Ненад Р. Путник[1]
Младен М. Милошевић[2]
Владимир Н. Цветковић[3]
Универзитет у Београду, Факултет безбедности
Београд (Србија)

343.533::004
004.738.5.056
Оригинални научни рад
Примљен 07/03/2022
Измењен 27/03/2022
Прихваћен 28/03/2022
doi: 10.5937/socpreg56-36845

РЕНСОМВЕР КАО ПРЕТЊА БЕЗБЕДНОСТИ – ДРУШТВЕНИ И КРИВИЧНОПРАВНИ АСПЕКТИ[4]

Сажетак: Рад је посвећен анализи друштвених и кривичноправних аспеката феномена злоупотребе рачунарског рансомвер (*ransomware*) малвера. Основна хипотеза аутора је да нису развијени адекватни механизми безбедносне и кривичноправне заштите од ове специфичне технике напада на рачунарске системе и податке који су у њима садржани.

Прегледом научне и стручне литературе и коришћење правно-догматског и нормативног метода аутори су установили да криминалитет везан за употребу рансомвер-малвера има потенцијал да озбиљно угрози поједине сегменте савременог друштва – привреду, осетљиве личне податке, националну и наднационалну критичну инфраструктуру, а указали су и на недостатке важећих законских решења.

Аутори закључују да је неопходно спровођење циљаних едукација корисника рачунарских система и предузимање мера за унапређење безбедносне културе, и износе конкретне предлоге за унапређење кривичноправног оквира.

Кључне речи: рансомвер-малвер, друштвени аспекти злоупотребе рансомвер-малвера, кривичноправна заштита од високотехнолошког криминала, критична инфраструктура.

УВОД

Рансомвер (енгл. *ransomware*) представља врсту малвера, из поткатегорије уцењивачког малициозног софтвера, који ауторизованом кориснику ограничава приступ рачунарском систему или у њему похрањеним подацима и тражи откупнину

[1] nputnik@fb.bg.ac.rs
[2] milosevic@fb.bg.ac.rs.
[3] vcvetkovic@fb.bg.ac.rs.
[4] Рад је настао у оквиру пројекта Фонда за науку Републике Србије „Идеје” – Пројекат акцелерације иновација и подстицања раста предузетништва у Републици Србији – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D.

како би корисник повратио приступ свом систему и/или подацима (Fruhlinger, 2020). Откупнина се по правилу тражи и исплаћује у криптовалутама, најчешће у биткоину. Трансакцијама у криптовалутама је тешко пратити траг, те је њихово коришћење у функцији очувања анонимности нападача.

Неке врсте рансомвера могу да блокирају рачунар на начин да се на екрану појави уцењивачка порука коју корисник не може да склони без плаћања откупнине. Друге врсте овог малвера могу да криптују (шифрују) појединачне или системе датотека у рачунару. Ако је рачунар повезан са локалном мрежом, рансомвер се, такође, може проширити на друге рачунаре или уређаје за складиштење на мрежи или у интернет облаку. У том случају се од корисника чији је рачунар заражен тражи откупнина у замену за откључавање (дешифровање) закључаних података.

Од 2016. године рансомвер-напади изазивају велику забринутост не само корпоративног менаџмента већ и влада држава. Разлог лежи у томе што ови напади проузрокују велике финансијске губитке са једне стране док, са друге, могу онемогућити функционисање здравствених установа и тиме, посредно, угрозити могућност лечења пацијената. Од почетка пандемије вируса SARS-CoV-2, здравствене установе широм Америке и Европе суочавају се, паралелно, и са пандемијом рансомвер-напада.

Напади овог типа, уколико циљају на ИКТ системе од посебног значаја, представљају озбиљан изазов не само за национално законодавство већ и за доносиоце политичких одлука и креаторе националних безбедносних политика. ИКТ системи од посебног значаја су системи који се користе у обављању послова у органима јавне власти, за обраду података о личности и у обављању делатности од општег интереса (član 6, Zakon o informacionoj bezbednosti, „Službeni glasnik RS", 6/2016 i 94/2017). Ови системи се у англосаксонском говорном подручју уобичајено називају критичном информационом инфраструктуром која представља једну од посебно осетљивих критичних инфраструктура државе. Појам критичне инфраструктуре се може одредити на различите начине. Члан 4 став 1 српског Закона о критичној инфраструктури (Zakon o kritičnoj infrastrukturi, „Službeni glasnik RS", broj 87/18) гласи: „Критична инфраструктура су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије". Дакле, наш законодавац сматра критичним оне „системе, мреже, објекте или њихове делове" чије функционисање у битној мери утиче на остваривање виталних државних или друштвених циљева и интереса (безбедност, привреда, живот, здравље, животна средина, имовина).

Савремено теоријско одређење појма критичне инфраструктуре односи се на имовину која укључује физичке и рачунарске системе који су од есенцијалног значаја за обезбеђивање економске и политичке стабилности земље (Radvanovsky & McDougall, 2010). У суштини, оне представљају оквир међузависних мрежа и система који обухватају одређене индустрије, институције (укључујући људе и процедуре) и капацитете за дистрибуцију који пружају поуздан проток производа и услуга који су неопходни за одбрамбену и економску сигурност земље, неометано функционисање власти на свим нивоима, као и друштва у целини (Rakić, 2015, str. 10). Критичне инфраструктуре обухватају здравствене системе, енергетске системе, телекомуникације, саобраћај, воду,

храну, банкарске системе и финансије, цивилну администрацију, укључујући и владини приватни сектор, али нису искључиво на њих ограничене (Radvanovsky & McDougall, 2010). Ниједна подела критичних инфраструктура није апсолутна и углавном је заснована на проценама стручњака и/или доносиоца политичких одлука одређене државе.

Данас све већи број инфраструктурних сектора поприма транснационални карактер. Сектор информационих и комуникационих технологија је одавно превазишао националне границе држава, а такви су и сектори саобраћаја (друмски, железнички, ваздушни, водни), хемијске, као и нуклеарне индустрије (Rakić, 2015, str. 48). Слично је и са финансијским сектором, који је у великој мери транснационализован (Global Economic Crisis, 2013). Ипак, у односу на све критичне инфраструктуре једне државе, информационо-комуникациона и електроенергетска се сматрају посебно осетљивим, будући да прожимају све остале, те прекид у њиховом исправном функционисању производи и дисфункционалност свих осталих инфраструктура (Putnik, 2009, str. 41).

Растућа зависност система који омогућавају основне услуге од информационо-комуникационе инфраструктуре представља елемент ризика, с обзиром на то да прожима све остале и намеће им сопствене рањивости, не само на националном већ и на регионалном, па и глобалном нивоу.

РЕНСОМВЕР КАО ПРЕТЊА КОРПОРАТИВНОЈ И НАЦИОНАЛНОЈ БЕЗБЕДНОСТИ

Рансомвер-напади представљају вид високотехнолошког криминалитета који годинама уназад бележи највишу стопу раста. Процењује се да сваких 11 секунди једно правно лице постане жртва рансомвер-напада (Morgan, 2019). Штета од ове врсте напада је у 2015. години износила 325 милиона долара на глобалном нивоу, а у 2017. години је увећана чак 15 пута и износила је 5 милијарди долара. У 2018. години она је порасла на 8 милијарди долара, а у 2019. години на 11,5 милијарди долара (Morgan, 2019). У 2021. години штета од ове врсте напада процењена је на чак 20 милијарди долара (Acronis Cyberthreats Report, 2022).

Практично да нема државе која није осетила последице ове врсте напада. Индија је била једна од најтеже погођених у 2017. години, уз Велику Британију, Руску Федерацију, Сједињене Америчке Државе, НР Кину и Канаду (Mohurle & Patil, 2017).

На мети напада била је национална критична инфраструктура али и велике мултинационалне компаније. Последице напада осетиле су компаније Федекс (*FedEx*), Нисан (*Nissan*), железничке компаније у Немачкој и Русији, телекомуникациона компанија Мегафортелефоника (*Megafortelefonica*) у Шпанији и многе друге, али и академске установе, о чему сведоче пријављени случајеви напада на кинеске колеџе и рачунаре студената (Mohurle&Patil, 2017).

Друштвене последице које узрокује рансомвер-напад су пак много озбиљније када су на мети нападача здравствене установе.

Илустративан је податак да је у 2017. години овом врстом напада погођено чак 60 здравствених установа у Великој Британији, а да се малициозни код након тога проширио на више од 200.000 болничких рачунарских система у 150 земаља (Collier, 2017).

Током 2020. године, у САД десила су се 92 појединачна напада рансомвер-вирусом на здравствене и медицинске научноистраживачке установе. У нападима је погођено преко 600 клиника, болница и установа и закључано више од 18 милиона медицинских досијеа пацијената (Davis, 2020).

Напади су за последицу имали не само финансијске губитке здравствених установа и компромитацију личних података о пацијентима већ су онемогућили процес лечења пацијената али и нормално функционисање установа – довели су до значајних застоја у раду. Застоји су варирали од минималних, код система који су правили честе резервне копије дигиталних података, до дуготрајних који су се мерили недељама, па чак и месецима, у системима који су резервне копије докумената имали само у папирној форми (Bischoff, 2021).

Као последица инфекције рансомвер-малвером сервери могу бити ван функције сатима, недељама, па чак и месецима. У неким случајевима се подаци и/или рачунари уопште не могу обновити. Збирно гледано, просечно време застоја износило је 15, 16, 19 или 21 дан за Q1, Q2, Q3, односно Q4 2020. године. То значи да се у четвртом кварталу, у односу на први квартал, време застоја узрокованог нападима повећало за скоро недељу дана. Збирна статистика говори да је рансомвер проузроковао 1.669 дана застоја у здравству САД у 2020. години (Coveware, 2021).

У 2020. години је, такође, био изражен растући тренд покушаја двоструке изнуде у којој нападачи не закључавају само рачунаре уз захтев за откупнину већ и контактирају жртве са доказима о прикупљеним подацима. Објављивање украдених података на јавним сајтовима повећава притисак на организације да плате накнаду за откуп (као примери оваквих случајева наводе се: *Beacon Health Solutions*, *Wilmington Surgical Associates* и *Riverside Community Care*) (Bischoff, 2021).

Изражено повећање броја напада у 2020. години може се довести у везу са пандемијом вируса SARS-CoV-2. Оптерећење здравствених установа је од почетка пандемије било велико. То их је учинило још рањивијима на сајбер-нападе јер је заштита здравствене ИКТ инфраструктуре била у другом плану у односу на повећан обим посла у условима пандемије. То је вероватно и додатно мотивисало нападаче јер су претпостављали да болнице, у тим околностима, неће себи приуштити застој ИКТ система већ ће, вероватније, прибећи плаћању откупнине.

На крају, тешко је сумирати укупну штету од рансомвер-напада током пандемије SARS-CoV-2. Поред финансијских трошкова проистеклих од застоја у раду здравствених установа, ту је и штета која се огледа у нарушеном здрављу па чак и изгубљеним животима људи, будући да правовремено лечење пацијената није било могуће. Иако би било тешко утврдити укупан утицај сајбер напада на здравље и живот пацијената, једно истраживање сугерише да је блокада медицинских досијеа пацијената током пандемије повећала стопу смртности од срчаних удара на годишњем нивоу - 36 смртних исхода више на 10.000 срчаних удара сваке године (Bischoff, 2021). Ови напади су, осим тога, довели и до успоравања истраживања самог вируса SARS-CoV-2. Тако је, на пример, јуна 2020. године Калифорнијски универзитет у Сан Франциску платио откуп у износу од 1,14 милиона долара како би повратио приступ својим подацима који су били део истраживања вируса SARS-CoV-2 (Bischoff, 2021).

Па ипак, највећа штета није она финансијска већ она која се очитује у последицама сајбер-напада на здравље и живот пацијената. Због тога не изненађује

иницијатива лекара, научника, експерата за сајбер-безбедност и политичких представника неколико држава да се рансомвер-напади на здравствене установе инкриминишу као чин терористичког напада (Bing, 2021).

Рансомвер-напад заиста има сличности са традиционалним терористичким нападима јер циља на цивилно становништво и може проузроковати нарушавање здравља, па чак и смрт људи. Такође, путем изазивања страха приморава жртву да поступи по захтеву нападача. Но ипак, основна мотивација нападача се разликује. Док је крајњи циљ терориста идеолошке или политичке природе, циљ који желе да остваре извршиоци рансомвер-напада своди се на стицање финансијске користи, те је прављење ове врсте аналогије тренутно прилично „натегнут" конструкт. Са друге стране пак ову иницијативу не би требало олако одбацити будући да се захтеви извршилаца, хипотетички гледано, могу лако преоријентисати са финансијских на политичке. Осим тога, рансомвер-напади могу представљати начин за сакупљање новчаних средстава у сврху финансирања терористичких организација, што свакако усложњава проблем и тражи приправност не само практичара на пољу безбедности, већ и истраживача, као и доносилаца политичких одлука.

И у будућности се може очекивати исти, ако не и већи тренд напада на здравствене установе. Будући да злонамерни актери на здравствене установе често гледају као на „лаку мету", рансомвер ће и даље представљати опасност како за установе, тако и за пацијенте. Иако је већина рансомвер-напада до сада циљала на досијее пацијената у болничким информационим системима, не могу се искључити ни много гори сценарији. Без осмишљавања и имплементације нових безбедносних алата, мера и процедура, здравствене установе би се ускоро могле суочити са рансомвер-нападима на медицинску опрему и уређаје од којих директно зависе животи пацијената.

На крају, важно је истаћи да штета коју изазива рансомвер-напад није ограничена само на цену откупа. Она обухвата и трошкове који настају услед оштећења или губитка података, губитка продуктивности, опоравка система након напада, форензичке анализе, поновног „хостовања" података који су били ускладиштени у облаку, губитка репутације правног лица, као и циљане едукације запослених и њихове обуке за реаговање у случају поновљеног напада.

Повећање безбедносне културе код запослених и њихова циљана едукација за препознавање безбедносних претњи и одбрану од сајбер-напада представља најважнији корак у борби против рансомвер-напада (Kovačević, Putnik &Tošković, 2020). Будући да 91% сајбер напада започиње ширењем фишинг (*phishing*) и-мејлова који имају за циљ уношење рансомвер-кода у корпоративни рачунарски систем, едукација би требало да буде усмерена на препознавање технике фишинга и адекватну и правовремену реакцију запослених (Morgan, 2019).

КРИВИЧНОПРАВНИ АСПЕКТ

Након приказа феноменологије злоупотребе рансомвер-вируса, намеће се питање њиховог кривичноправног третмана у домаћем законодавству. Да ли је национално кривично право у својим одредбама предвидело кажњавање ових, очигледно друштвено опасних понашања?

Кривична дела високотехнолошког криминала – кратак приказ

Ренсомвер-напади се изводе преко рачунарских мрежа и њихов објекат су рачунарски подаци и програми. Стога, анализу кривичноправног третмана започињемо са прегледом инкриминација високотехнолошког криминала.

Дела високотехнолошког криминала обухватају инкриминације из главе 27 Кривичног законика – кривична дела против безбедности рачунарских података (Krivični zakonik Republike Srbije, „Sl. glasnik RS", br. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19; даље: КЗ), али и друга, неспецифична кривична дела, која се такође могу извести уз коришћење високих дигиталних технологија (Милошевић, Путник, 2019: 74). Опсег кривичних дела високотехнолошког криминала можемо да сагледамо кроз анализу одредби посебног закона намењеног утврђивању организације и расподели надлежности између компетентних државних органа (Zakon o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala, „Sl. glasnik RS", br. 61/05, 104/09.2009; у даљем тексту: Закон о ВТК).

Закон о ВТК је донет ради испуњења међународноправних обавеза преузетих ратификацијом Конвенције о високотехнолошком криминалу Савета Европе из 2001. године и додатног протокола уз њу (Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, 2009; у даљем тексту: Конвенција ВТК; Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, 2009). И измене и допуне КЗ-а којим су уведена кривична дела против безбедности рачунарских података (глава 27) донете су из истог разлога – ради хармонизације са Конвенцијом, иако су оне усвојене пре него што је наша земља ратификовала овај међународни уговор.[5] Из наведеног разлога, опште карактеристике ових кривичних дела треба посматрати у светлу и контексту Конвенције о ВТК и Закона о ВТК.

Конвенција дефинише мере које би национална законодавства требало да предузму у области кривичног права, пре свега кроз инкриминисање радњи наведених у члановима 2–10 (незаконит приступ; незаконито пресретање; ометање података; ометање система; злоупотреба уређаја; фалсификовање у вези са рачунарима; превара у вези са рачунарима; дела у вези са дечјом порнографијом и дела у вези са кршењем ауторских и сродних права) (Mandić, Putnik, Milošević, 2017, str. 310; Stojanović & Delić, 2015; Stojanović, 2012; Đorđević, 2014).

Члан 13 Конвенције захтева да државе предузму законодавне и друге правне мере како би се осигурало да наведена друштвено опасна понашања подлежу делотворним, пропорционалним и одвраћајућим санкцијама. Глава 27 КЗ-а у највећој мери следи препоруке Конвенције.

Закон о ВТК углавном решава питања процесног карактера (надлежност, организација итд.). Ипак, овај пропис садржи и одредбе од значаја за материјално право, јер једини у домаћем законодавству садржи посредну дефиницију појма

[5] Ипак, занимљиво је да радње пресретања комуникације, које Конвенција сврстава у облике кажњивог понашања у сајбер-простору, наш законодавац није увео у биће ниједног од новоуведених кривичних дела (Stojanović & Perić, 2011, str. 251).

„високотехнолошки криминал", кроз набрајање круга кривичних дела и потребних услова да би се иста квалификовала као ова врста криминалног деловања: „под високотехнолошким криминалом подразумева се вршење кривичних дела код којих се као објекат или средство извршења[...] јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику" (члан 2 став 1 Закона о ВТК). Члан 3 Закона о ВТК одређује да надлежност за откривање, гоњење и суђење припадају специјализованим одељењима полиције, тужилаштва и суда у случају следећих кривичних дела:

- против безбедности рачунарских података (глава 27 КЗ-а) – по правилу, односно **без додатних услова**;
- против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије – уз додатни **услов**: да се могу сматрати високотехнолошким криминалом имајући у виду начин извршења и коришћена средства (сходно члану 2 став 1 Закона о ВТК);
- против интелектуалне својине, имовине, привреде и правног саобраћаја – уз **два услова**: 1. да број примерака ауторских дела прелази 2.000 (овај услов се односи на кривична дела против интелектуалне својине, попут повреде проналазачког права или неовлашћеног искоришћавања ауторског дела или предмета сродног права) или да настала материјална штета прелази износ од 1.000.000 динара и 2. да се могу сматрати високотехнолошким криминалом имајући у виду начин извршења и коришћена средства (сходно члану 2 став 1 Закона о ВТК).

Кривична дела која не потпадају под посредне дефиниције из чл. 2 и 3 Закона о ВТК, не могу се сматрати високотехнолошким криминалом у Републици Србији.

Законом о ВТК установљено је одељење Вишег јавног тужилаштва у Београду, надлежно за читаву територију Републике Србије, које законодавац означавао као *посебно тужилаштво*; одељење за борбу против високотехнолошког криминала у склопу Министарства унутрашњих послова – Управе криминалистичке полиције (које се у овом закону назива: *Служба за борбу против високотехнолошког криминала*) и, у оквиру Вишег суда у Београду, Веће за борбу против високотехнолошког криминала (законодавац га назива *Одељење*), задужено за територију Републике. Министарству правде је поверено обезбеђивање услова и средстава за реализацију задатака и послова специјализованих служби/одељења у полицији, тужилаштву и суду (Milošević & Putnik, 2017).

У глави 27 Кривичног законика се налазе следеће инкриминације (чл. 298–304а КЗ): оштећење рачунарских података и програма (члан 298); рачунарска саботажа (члан 299); прављење и уношење рачунарских вируса (члан 300); рачунарска превара (члан 301); неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302); спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303); неовлашћено коришћење рачунара или рачунарске мреже (члан 304); прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а). Последња наведена инкриминација представља врсту припремне радње уздигнуте на ниво радње извршења. Знајући значај превенције и степен друштвене опасности високотехнолошог криминала, законодавац се одлучио за кривичноправну репресију

у раној фази. Тачније, законодавац је имплементирао препоруке Конвенције, која експлицитно захтева кажњавање ових припремних радњи.

Занимљиво је да је наш законодавац пропустио да предузме легислативне мере за кажњавање само једног облика друштвено опасног понашања према рачунарским подацима. Реч је о незаконитом пресретању података, које није предвиђено као посебно кривично дело. Члан 3 Конвенције захтева од страна потписница да кривично санкционишу „противправно пресретање преноса рачунарских података који нису јавне природе, ка рачунарском систему, од њега или унутар самог система, укључујући и електромагнетна емитовања из рачунарског система којим се преносе такви подаци, када је учињено са намером и уз помоћ техничких уређаја".

Имајући у виду изнети сумарни приказ кривичноправне регулативе високотехнолошког криминала, питамо се да ли постојеће инкриминације обухватају злоупотребу рансомвер-малвера односно малициозних кодова. Међу набројаним кривичним делима, оно из члана 300 се очито односи на употребу рачунарских вируса, па ћемо се на њега и фокусирати. Након тога, размотрићемо и друге, неспецифичне инкриминације, које се могу испољити у форми високотехнолошког криминала.

Прављење и уношење рачунарских вируса и остале могуће кривичноправне квалификације

Прављење рачунарског вируса уз намеру његовог уношења у туђ рачунар или рачунарску мрежу, инкриминисано је чланом 300 КЗ-а. Запрећена је новчана казна алтернативно са затвором од шест месеци. Уколико учинилац унесе рачунарски вирус и проузрокује штету, остварен је квалификовани облик, прописан ставом 2 овог члана, за који је прописана новчана казна или затвор до две године. Законом је прописана обавезна мера безбедности, којом се одузимају уређаји и средства намењени за или настали извршењем кривичног дела.

Члан 112 став 20 КЗ одређује значење појма рачунарског вируса, описујући га као врсту рачунарског програма (или другог скупа налога, односно наредби) који одликује тенденција самоумножавања и деловања на друге програме и податке. Вирус делује на друге рачунарске програме и податке тако што им се придодаје и мења начин на који они функционишу.

Основни облик показује намеру законодавца да реагује у раној фази, јер је прављење рачунарског вируса уз дату намеру, по својој суштини, само припремна радња. С обзиром на то да је припремање кривичног дела начелно некажњиво, законодавац је прописивањем основног облика омогућио примену кривичних санкција и за припремне радње, које су овим добиле карактер радње кривичног дела.

Тежи облик је, по природи ствари, основни облик, који је законодавац „вештачки" трансформисао у квалификовани, јер је припремну радњу прогласио за основни облик дела. Овде се основано може поставити питање оправданости постојања облика из става 1, након што је ЗИД КЗ из 2009. године увео кривично дело из члана 304а. Тим кривичним делом, уз прецизирање и допуне учињене доношењем ЗИД КЗ из 2016. године, инкриминишу се различите припремне радње за извршење кривичних дела против безбедности рачунарских података. Уз евентуално додатно прецизирање

одредби члана 304а, потреба за постојањем основног облика из садашњег члана 300 став 1 би потпуно нестала, што би било оправдано и са становишта законодавне технике.

У вези садашње регулативе, поставља се још питања. Наиме, јасно је да ако неко направи рачунарски вирус а затим га унесе у туђ рачунар или мрежу, чини само дело из става 2. Међутим, дело из става 2 је последично, што значи да је свршено када наступи штета (Stojanović & Delić, 2020). У случају да је рачунарски вирус унет а штета изостала, реч је о покушају, који је некажњив по општим одредбама.

Дакле, само прављење рачунарског вируса у намери стављања у туђ рачунар или мрежу је кажњиво, док би уношење вируса без наношења штета било некажњиво. Ово је очигледна нелогичност, која је последица чињенице да је припремна радња кажњива, а покушај „правог" дела некажњив. Припремне радње би требало да се кажњавају када се припрема теже кривично дело, а ово дело је у категорији лакших, што и доводи до спорних решења.

Занимљиво је да ово кривично дело нема више квалификованих облика. Уколико би се *de lege ferenda* приступило изменама ове главе КЗ-а, требало би размотрити брисање члана 300 става 1 (уз његово јасно „припајање" члану 304а) и додавање тежих облика, који би се односили на извршење дела из садашњег става 2 (који би постао став 1) уз одређене квалификаторне околности. Те околности би могле да буду: наношење имовинске штете у одређеном износу; привремени или потпуни застој или поремећаји у раду (ако је пасивни субјект орган/организација).

Пре даљег разматрања *de lege ferenda* пак потребно је одговорити на питање: да ли се злоупотребе малициозних кодова у виду рансомвер-напада могу квалификовати искључиво по овом члану КЗ-а или у обзир долазе и друге кривичноправне квалификације?

У том смислу, ваља испитати могућност да се радња злоупотребе рансомвер-вируса подведе под кривично дело уцене из члана 215 КЗ-а. Уцена постоји уколико учинилац, у намери стицања противправне имовинске користи за себе или другог, прети да ће против пасивног субјекта „или њему блиског лица открити нешто што би њиховој части или угледу шкодило". Према томе, употреба рансомвер-кода, би, хипотетички, могла да представља кривично дело уцене само у случајевима када се оштећени уцењује откривањем „заробљених" података, чијим обелодањивањем може да се нашкоди части или угледу. То, ипак, код рансомвер-напада углавном није случај, те већински неће бити основа да се дело квалификује по члану 215 КЗ-а.

Међутим, могуће су и ситуације у којима учинилац зароби рачунарске податке и уцењује жртву њиховим откривањем (нпр. стекне контролу над рачунарским системом и оствари приступ фотографијама, чијим откривањем би наудио угледу пасивног субјекта). Тада би се дело квалификовало као уцена. С обзиром на то да је уцена изведена помоћу уношења рачунарског вируса, поставило би се и питање стицаја дела из чл. 215 и 300 КЗ-а. У теорији и судској пракси се слично питање постављало у вези односа кривичних дела преваре и фалсификовања исправе. У вези са тим делима заузет је став да ако је фалсификовање исправе био једини начин да се изведе превара, стицај је привидан (Stojanović & Perić, 2011, str. 153). Такво становиште је оправдано у овом случају, али једино уколико је заиста била реч о једином могућем начину извршења уцене. У свим осталим ситуацијама, постојао би реални

стицај, посебно имајући у виду да је реч о кривичним делима са врло различитим заштитним објектима.

Дакле, поједини случајеви злоупотребе ренсомвер-кодова могу да се квалификују као кривично дело уцене. Међутим, ти случајеви су релативно ретки и остаје проблем подвођења осталих друштвено опасних радњи изведених употребом малициозних кодова под одговарајућу кривичноправну квалификацију.

Кривично дело принуде, из члана 135 КЗ-а, постоји ако се друго лице, употребом силе или претње, принуди на одређено чињење, нечињење или трпљење. Поступање код ренсомвер-напада се поклапа са законским описом основног облика овог дела, јер се жртви упућује претња и иста је принуђена на чињење или нечињење. Ипак, покушај основног облика овог кривичног дела је некажњив, јер је запрећена казна затвора до три године.

Такође, поставља се питање да ли је овде присутан стицај са кривичним делом из члана 300 или је он привидан (Delić, 2021; Vuković, 2021; Stojanović, 2018). Закључак је исти као код уцене. У већини случајева овде ће бити реч о реалном стицају два кривична дела. Уосталом, законодавац није без разлога инкриминисао уношење рачунарских вируса у туђ рачунар или рачунарску мрежу, већ је имао у виду посебну друштвену опасност ових радњи. Стога не би било оправдано „багателисати" дело из члана 300 његовим свођењем на начин извршења другог кривичног дела.

На крају, али никако најмање важно, остаје да се размотри могућност правне квалификације ренсомвер-напада као изнуде (члан 214 КЗ-а). Изнуда, као имовинско кривично дело, представља специјалан случај принуде и од ње се разликује по субјективном елементу (намера стицања противправне имовинске користи) и последици (пасивни субјект је принуђен да нешто учини или не учини на штету своје или туђе имовине). Имајући у виду да учиниоци који користе ренсомвер-вирус по правилу имају лукративне (имовинске) мотиве, јасно је да би далеко већи број ових напада могао да се квалификује као изнуда. Принуда би била исправна квалификација само у ситуацијама када учинилац није имао намеру стицања противправне имовинске користи. Проблем стицаја треба решавати на исти начин као код излагања о уцени и принуди. С обзиром на запрећену казну за кривично дело из члана 214 КЗ-а, овде би покушај био кажњив.

Имајући све наведено у виду, сматрамо да би већину појавних облика злоупотребе ренсомвер-малвера требало квалификовати као стицај кривичних дела изнуде и прављења и уношења рачунарских вируса. Тамо где не би постојала намера стицања противправне имовинске користи нити би се последица огледала у имовинској штети, радило би се о стицају принуде и дела из члана 300, док би у најређим случајевима претње обелодањивањем података постојао стицај уцене и прављења и уношења рачунарских вируса.

De lege ferenda

Имајући у виду изнете тешкоће у вези са правном квалификацијом, потребно је размотрити могућност уподобљавања законских решења савременим начинима извршења кривичних дела у сајбер-простору, односно проблем коришћења ренсомвер-малвера.

Овде би кривичноправна заштита могла да буде унапређена увођењем допунских облика кривичног дела из члана 300 или новог кривичног дела. Овај нови облик/дело би постојао ако би учинилац унео рачунарски вирус или други малициозни код у туђ рачунар или рачунарску мрежу и тако стекао контролу над радом рачунара, што би искористио тако што би ставио у изглед оштећеном да ће му коришћење тих програма и података на даље бити онемогућено уколико не поступи по његовим захтевима. Дакле, учинилац „заробљава" туђ рачунар, односно програме и податке који се налазе на њему и принуђава оштећеног на одређено чињење или нечињење, јер ће у супротном рачунар остати закључан или ће подаци бити злоупотребљени.

Сама законска формулација бића кривичног дела могла би да гласи: ко са намером да принуди другог да нешто учини, не учини или трпи, унесе рачунарски вирус или сличан рачунарски програм или скуп наредби у туђ рачунар или рачунарску мрежу и тиме стекне контролу над радом рачунара или појединих података или програма, казниће се...

Уз то, било би оправдано да се уведе и још тежи облик, који би гласио: уколико је извршењем дела из претходног става учинилац стекао противправну имовинску корист или проузроковао имовинску штету у износу од ..., или су наступиле друге тешке последице, казниће се...Могући најтежи облик би се односио на изазивање опасности по живот или здравље грађана или угрожавање функционисања привреде или критичне инфраструктуре (снабдевање природним енергентима, саобраћај итд.).

Првопоменути облик би инкриминисао само употребу рансомвер-програма у одређеној намери, док би тежи облик прописивао строже казне уколико је дошло до наношења штете, стицања противправне имовинске користи или других тешких последица (нпр. последица по приватни живот, здравље, углед и част или радно место оштећеног, односно, у случају да је пасивни субјект правно лице – блокаду рада, репутациону штету, одговорност према трећим лицима и сл.).

Запрећена казна би требало да буде адекватна и сразмерна стварној друштвеној опасности. Сматрамо да тренд коришћења ове врсте малвера и потенцијалне консеквенце његове употребе, оправдају увођење новог кривичног дела или стварање допунских облика дела из члана 300.

Такође, овако би се избегле практичне тешкоће приликом примене права, јер би се решиле недоумице око правне квалификације. Ново дело – рачунарска изнуда/принуда (или, евентуално, нови облици кривичног дела из члана 300), јасно би се разликовало у односу на остала кривична дела и имало би адекватан распон казне, посматрајући из аспекта апстрактне друштвене опасности ових противправних понашања. Увођењем квалификованих облика које предлажемо, обухватио би се читав делокруг радњи којима се пасивни субјекти угрожавају помоћу рансомвер-вируса, односно малициозних кодова.

ЗАКЉУЧАК

Ефикасна заштита критичних инфраструктура, међу којима посебно важно место заузима информационо-комуникациона инфраструктура, намеће се као императив савременог умреженог и информатизованог друштва.

За постизање тог циља неопходан је координиран приступ који подразумева константну активност на (ре)дефинисању, имплементацији и хармонизацији националних и међународних безбедносних политика и стратегија, закона и стандарда. Заштита критичних инфраструктура, осим тога, захтева и конзистентно, кооперативно партнерство између јавног и приватног сектора – између власникâ и управљачâ инфраструктуре и влада држава.

Све већа зависност критичних инфраструктура од информационо-комуникационе инфраструктуре доводи до повећања могућности за угрожавање безбедности не само на националном већ и глобалном нивоу. О томе сведоче и последице које је последњих година рансомвер-малвер проузроковао по безбедност и здравље људи широм света.

Сходно томе, сматрамо да је потребно пронаћи оптималне начине за унапређење заштите критичне информационе инфраструктуре. За почетак, мислимо да законско решење које идентификацију критичне инфраструктуре поставља секторски (свако надлежно министарство и други субјекти одређују засебно шта је у њиховом сектору критична инфраструктура) треба променити тако што би се увели јединствени критеријуми. Такође, ниво безбедносне културе и свести мора да буде знатно унапређен, првенствено кроз додатне едукације запослених задужених за заштиту критичне инфраструктуре. Сајбер-простор нам је донео низ предности, али нас је и учинио рањивијим, те су врло потребне легислативне, организационе и образовне мере како бисмо се адекватно супротставили изазовима, ризицима и претњама савременог доба.

Важеће кривичноправне норме не пружају адекватну заштиту од злоупотребе рачунарских малвера у форми рансомвер-напада. Постојеће одредбе доводе до озбиљних тешкоћа у тумачењу, односно компликују правну квалификацију дела, а и не обухватају сва друштвено опасна понашања која заслужују кривичноправну реакцију. Изменом постојеће инкриминације из члана 300 КЗ-а или увођењем новог кривичног дела (рачунарска изнуда/принуда) које предлажемо, ове противречности и непотпуности би биле отклоњене, а кривичноправна заштита од савремених начина извршења кривичних дела у сајбер-простору значајно побољшана.

Nenad R. Putnik[1]
Mladen M. Milošević[2]
Vladimir N. Cvetković[3]
University of Belgrade, Faculty of Security Studies
Belgrade (Serbia)

RANSOMWARE AS A SECURITY THREAT – SOCIAL AND CRIMINAL LEGISLATION ASPECTS[4]

(Translation In Extenso)

Abstract: This article focuses on the analysis of social and criminal aspects of the phenomenon of ransomware-malware abuse. The authors' basic hypothesis is that the optimal mechanisms in terms of security and Criminal Code protection against this specific form of attacks on computer systems and data stored therein are still underdeveloped.

The review of scientific and professional literature and the use of legal-dogmatic and normative methods by various authors have shown that crime related to the use of ransomware- malware has a potential to seriously endanger certain segments of modern society - economy, sensitive personal data, national and supranational critical infrastructure. The authors have also noted the shortcomings of currently available legal solutions.

The authors conclude that it is necessary to conduct tailored educations of computer system users and also to undertake appropriate activities for the purpose of improving security culture. The authors additionally present concrete proposals for improving the legal framework for criminal legislation.

Keywords: ransomware-malware, social aspects of ransomware-malware attacks, Criminal Code protection against cybercrime, critical infrastructure.

INTRODUCTION

Ransomware is a type of malware. It falls under the subcategory of ransom malicious software, which allows to the authorised user only limited access to the computer system or

[1] nputnik@fb.bg.ac.rs
[2] milosevic@fb.bg.ac.rs
[3] vcvetkovic@fb.bg.ac.rs
[4] This paper was created as part of the Science Fund of the Republic of Serbia project *Ideas*. This is an innovation acceleration project which also aims to encourage entrepreneurship in the Republic of Serbia – Management of New Security Risks – Research and Simulation Development – NEWSIMR&D.

data stored therein and demands that ransom is paid, and thus the user regains access to the system and/or data (Fruhlinger, 2020). As a rule, ransom is demanded and paid in cryptocurrency, in most cases Bitcoin. Cryptocurrency transactions are hard to trace back to the attacker, so the reason for their use serves the purpose of maintaining the attacker's anonymity.

Some types of ransomware can block the computer in a way that an extortion message pops up on the screen and the message cannot be removed by the user until the ransom is paid. Other types of this malware can encrypt (code) individual files or systems of files stored on a computer. If the computer is connected to a local network, ransomware may also spread to other computers or data storage devices in the same network, the Internet cloud included. In this case, a ransom is demanded form the user whose computer is infected, in exchange for decrypting encrypted data.

Since 2016, ransomware attacks have been a cause of major concern not only of corporate management, but also of various countries' governments. The reason for this is that such attacks result in enormous financial losses on the one hand while on the other hand they could potentially disable the functioning of healthcare institutions and, as a consequence, indirectly deny patients possibility to be treated for their health conditions. Since the commencement of the SARS-CoV-2 pandemic, healthcare institutions throughout the United States and Europe have in parallel been faced with the challenge of ransomware attacks pandemic.

Attacks of this type, if they target information and communication technologies (ICT) of special importance, represent a major challenge not only for the national legislation but also for political decision-makers and creators of our national security policies. ICT systems of special importance are the systems that are used for: the performance of tasks in public authorities, the processing of special categories of personal data, the performance of activities of general interest (Article 6 of the Law on Information Security, "Official Gazette of the Republic of Serbia", No. 6/2016 and 94/2017). In English speaking countries, these systems are called critical information infrastructure, which stands for one of especially sensitive critical infrastructures of a state. The term critical infrastructure may be defined in different manners. Article 4, Paragraph 1 of the Serbian Law on Critical Infrastructure ("Official Gazette of the Republic of Serbia" No. 87/18) reads as follows: "Critical infrastructure are systems, networks, facilities, or parts thereof, whose interrupted functioning and cessation of delivery of goods or services may result in serious consequences on national security, heath and lives of people, property, the environment, citizens' safety, economic stability, i.e. this may threaten the functioning of the Republic of Serbia". Hence, the local legislator deems as critical those "systems, networks, facilities or parts thereof" whose functioning to a large extent affects the achievement of vital state and social objectives and interests (safety, economy, life, health, the environment, property).

Modern theoretical determining of the term critical infrastructure refers to property, which includes physical and computer systems that are essentially important for ensuring economic and political stability of a state (Radvanovsky & McDougall, 2010). They basically represent a framework of interdependent networks and systems which cover certain industries, institutions (including people and procedures) and capacities for the distribution, which provide a reliable flow of products and services that are necessary for homeland security and economic security of the country, smooth functioning of state authorities at all levels, as well as society as a whole (Rakić, 2015, p. 10. Critical infrastructures include

healthcare systems, energy systems, telecommunications, traffic, water, food, banking systems and finance, civil administration, including public and private sectors, but are not limited solely to these (Radvanovsky & McDougall, 2010). No division of critical infrastructures is absolute, and such divisions are mainly based on assessments made by experts and/or political decision-makers of a particular state.

Nowadays, there is an increasing number of infrastructure sectors which adopt a transnational character. The ICT sector has long gone beyond national boundaries, and the same goes for the sector of traffic (road, railroad, air, water), chemical sector as well as nuclear industries (Rakić, 2015, p. 48). A similar situation is in the finance sector, which has been substantially trans-nationalised (Global Economic Crisis, 2013). Still, compared to all other critical infrastructures of a state, the ICT and energy infrastructures are considered particularly sensitive, since some segments of the two are present in all other infrastructures and consequently any disruption in their functioning leads to dysfunctions in all other infrastructures (Putnik, 2009, p. 41)

Growing dependence on the systems which allow the provision of basic services from ICT infrastructure represents an element of risk, given the fact that it is present in all other infrastructures, thus transferring to them its own vulnerabilities, not only on a national but also regional and global levels.

RANSOMWARE AS A THREAT TO CORPORATE AND HOMELAND SECURITY

Ransomware attacks are a form of cybercrime which for a number of years have been the fastest growing type of cybercrime. It is estimated that every 11 seconds a business is a victim of ransomware attack (Morgan, 2019). In 2015, ransomware damages stood at 325 million dollars globally, while in 2107 these damages recorded an increase of as many as 15 times, thus reaching 5 billion dollars. The damages went up to 8 billion dollars in 2018, while in 2019 the figure was 11.5 billion dollars (Morgan, 2019). In 2021, the estimated amount of damages was as high as 20 billion dollars (Acronis Cyberthreats Report, 2022).

There is virtually not a single state which has not suffered the consequences of cyberattacks. India was one of the most severely affected countries in 2017, along with Great Britain, the Russian Federation, the United States of America, the People's Republic of China, and Canada (Mohurle & Patil, 2017).

Critical national infrastructures were targeted by cyberattacks but also large multinationals. Some of these were *FedEx*, *Nissan*, railway companies in Germany and Russia, the Spanish telecommunications provider *Megafortelefonica* and many others. Academic institutions did not remain unaffected either, which is confirmed by reported cases of cyberattacks on Chinese colleges and students' computers (Mohurle & Patil, 2017).

However, consequences caused by ransomware attacks are far more serious when cyber attackers target healthcare institutions.

Illustrative information in this regard is that as many as 60 healthcare institutions in Great Britain were affected in 2017 while the malicious code then spread in more than 200,000 hospital computer systems across 15 countries (Collier, 2017).

In 2020, there were 92 individual ransomware attacks on US healthcare institutions as well as medical research institutions. More than 600 clinics, hospital and institutions were affected, with more than 18 million decrypted patients' medical records (Davis, 2020).

The cyberattacks resulted not only in financial losses incurred by healthcare institutions and compromised personal patient data but this also prevented the process of treating patients and normal functioning of the institutions because significant disruptions in their operations occurred. Disruption lengths ranged from minimum ones, with systems which frequently made backup copies of digital data, to very long disruptions that lasted for weeks, even months, for systems which had hardcopies as backup for files (Bischoff, 2021).

As a consequence of ransomware-malware infections, servers may be out of order for hours, weeks, even months. In some cases, data and/or computers cannot be retrieved. Overall, the average downtime after a cyberattack was 15, 16, 19 and 21 days for Q1, Q2, Q3 and Q4 respectively. This means that in Q4, compared to Q1, the downtimes caused by cyberattacks increased by almost one week. Cumulative statistics shows that in 2020 ransomware caused 1.669 disruptions in the US healthcare system (Coveware, 2021).

In 2020, there was also a noticeable growing trend of attempts at double extortion in which cyber attackers not only decrypted computer and demanded a ransom but also contacted victims and presented proof of collected data. Releasing stolen data on public webpages resulted in stronger pressure on attacked organisations to pay the ransom (examples of this situation are *Beacon Health Solutions*, *Wilmington Surgical Associates* and *Riverside Community Care*) (Bischoff, 2021).

A significant increase in the number of cyberattacks in 2020 may be correlated with the outbreak of the SARS-CoV-2 pandemic. The burden on healthcare institutions from the outset of the pandemic was enormous. This made them even more vulnerable to cyberattacks because security and protection of the ICT infrastructure became secondary compared to a large-scale engagement of staff in the pandemic situation. This probably served as additional motivation for cyber attackers because their assumption was that under those circumstances, hospitals could not afford any disruptions of the ICT system and that instead they would be willing to pay a ransom.

When all is said and done, it is difficult to summarise the total damage caused by ransomware attacks during the SARS-CoV-2 pandemic. In addition to financial loss incurred as a result of disruptions in healthcare institutions, there is also damage reflected in deteriorated health, even fatalities, of people because timely treatment was impossible. Although it would be difficult to establish the overall impact of cyberattacks on patients' health and lives, there is research which suggests that the decryption of patients' medical records during the pandemic increased the annual heart condition mortality rates – 36 fatalities more for every 10,000 heart attacks every year (Bischoff, 2021). Additionally, the cyberattacks lead to a slowdown in research into the SARS-CoV-2 virus itself. As an example, in June 2020 the University of California in San Francisco paid a ransom of 1.14 million dollars in order to retrieve its data which were a part of their research into the SARS-CoV-2 virus (Bischoff, 2021),

Still, the biggest damage is not financial one but damage which is reflected in the consequences of cyberattacks on patients' health and lives. Therefore, it does not surprise that medical doctors, scientists, cyber-security experts and political representatives in

several states had an initiative to declare ransomware attacks on healthcare institutions acts of terrorism (Bing, 2021).

Ransomware attacks are indeed similar to terrorist attacks because they target civilians and my cause deterioration in the overall health condition even death of individuals. Furthermore, by provoking fear, such attacks force the victim to do as required by the cyber attacker. Nevertheless, motivations of cyber attackers are different. While the ultimate goal of terrorists is ideologically and politically motivated, the goal which cyber attackers want to achieve comes down to financial gain and therefore such an analogy is currently something of "stretch". On the other hand, this initiative should not be dismissed offhand since demands of cyber attackers, hypothetically speaking, can easily be redirected from financial to political. In addition to this, the ransomware attack may constitute a form of raising funds for the purpose of financing terrorist organisations, which certainly makes the problem more complicated and calls for preparedness of not only cybersecurity practitioners but also researchers and political decision-makers.

It is reasonable to expect that in the future there will be the same, if not a more intensive, trend of cyberattacks on healthcare institutions. Given the fact that malicious cyber attackers on healthcare institutions often see them as "easy marks", ransomware will still pose a threat both to such institutions and patients as well. Although so far the majority of ransomware attacks targeted patient records in hospital information systems, for more sinister scenarios cannot be excluded. Without designing and implementing new cybersecurity tools, measures and procedures, healthcare institutions could be faced with ransomware attacks on medical equipment and machines on which patients' lives directly depend.

Finally, it is important to point out that damage caused by a ransomware attack is not limited solely to the amount of ransom that is demanded. The attacks also include costs incurred as a result of damage or loss of data, loss of productivity, system recovery following the attack, IT forensics analysis, rehosting data which were stored on the cloud, loss of reputation of the attacked legal entity, as well as tailored educations of staff and their training as to how to respond in the event of a repeated attack.

The most important step in fighting ransomware attacks is stronger cybersecurity culture of employees and tailored education provided to them, which will ensure that cyberthreats are recognised and teach what protection measures are to be undertaken in the event of a cyberattack (Kovačević, Putnik & Tošković, 2020). Given the fact that 91% of cyberattacks start by sending phishing emails, whose purpose is to introduce a ransomware code into a corporate computer system, education should be aimed at identifying phishing techniques and appropriate and timely reaction of the employees (Morgan, 2019).

CRIMINAL LEGISLATION ASPECT

Following a review of phenomenology of the abuse of a ransomware virus, the question now is how it is treated in the local legislation. Do the provisions of the national criminal legislation envisage that such forms of obviously socially dangerous behaviour are punishable?

Cybercrime offences – an overview

Ransomware attacks are carried out through computer networks, and they target data and programmes stored on computers. Therefore, we will commence the analysis of criminal legislation treatment with an overview of cybercrime charges.

Offences relative to cybercrime are covered by charges mentioned in Chapter 27 of the Criminal Code – criminal offences against security of computer data (Criminal Code of the Republic of Serbia, "Official Gazette of the Republic of Serbia", No. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19, hereinafter: the CC) but also other, non-specific criminal offences which may also be committed with the use of sophisticated digital technologies (Milošević, Putnik, 2019:74). The scope of criminal offences that involve cybercrime may be seen through an analysis of the provisions of a specific law whose objective is to define organisations and allocate responsibilities among competent state authorities (Law on the Organisation and Competences of Government Authorities Combating Cybercrime, "Official Gazette of the Republic of Serbia", No. 61/05, 104/09.2009, hereinafter: the Law on CC)

The Law on CC was passed for the purpose of fulfilling legal obligations undertaken through ratification of the Council of Europe Convention on Cybercrime of 2011 and the accompanying Protocol (Law on Ratifying the Convention of Cybercrime, 2009; hereinafter: the Convention on CC; Law on Ratifying the Accompanying Protocol to the Law on Ratifying the Convention of Cybercrime, in the segment thereof which is pertinent to charges relative to criminal offences that are of racist and xenophobic nature, such criminal offences being committed through computer systems, 2009). Changes in and amendments to the CC, pursuant to which criminal offences against security of computer data were introduced (Chapter 27), were passed for the same reason – harmonisation with the Convention, although they had been passed even before our country ratified this international treaty.[5]For the mentioned reasons, general feature of these criminal offences should be observed in the light of the Convention on CC and the Law on CC.

The Convention defines measures that national legislations should undertake in the field of criminal legislation, mainly by incriminating activities stated in Articles 2-10 (illegal access; illegal interception; data interference; system interference; abuse of devices; forgery committed with the help of computers; criminal offences relative to child pornography and criminal offences entailing breaches of intellectual property rights and ancillary IP rights) (Mandić, Putnik, Milošević, 2017, p. 310; Stojanović & Delić, 2015; Stojanović, 2012; Đorđević, 2014).

Article 13 of the Convention requires that Parties to the Convention adopt such legislative and other measures to ensure that the said socially dangerous behaviours are punishable by effective, proportionate, and dissuasive sanctions. Chapter 27 of the CC to the greatest extent adheres to recommendations stipulated in accordance with the Convention.

The Law on CC mainly deals with the procedural issues (responsibilities, competences, organisation, etc.). Nevertheless, this Law also contains provisions that are of relevance for

[5] Still, it is worth noting that our legislator failed to include in any of the newly introduced criminal offences such activities which involve interception of communication, which the Convention categorises as criminal behaviour in cyberspace (Stojanović & Perić, 2011, p. 251).

material right, because this is the only law in the local legislation that contains an indirect definition of the term "cybercrime", and so by listing the scope of criminal offences and conditions for such offences to be qualified as this form of criminal activity: "cybercrime is considered to be the commitment of criminal offences whereby as the object or means of committing[...]the following are used: computer, computer systems, computer networks, computer data, as well as any and all of their products, either in hard or soft form (Article 2, Paragraph 1 of the Law on CC). Article 3 of the Law on CC stipulates responsibilities for identifying, investigating and taking appropriate legal action, and those are assigned to specialised divisions of the Police Department, Public Prosecutor's Office and courts, in the event of the below listed criminal offences:

- against computer data security (Chapter 27 of the CC) – as a rule, i.e. **without additional conditions**;
- against civil liberties and rights, gender liberty, public order and constitutional order and homeland security of the Republic of Serbia – with an additional **condition**: that they may be construed to mean cybercrime given the manner of perpetration and utilised means (pursuant to Article 2, Paragraph 1 of the Law on CC) ;
- against intellectual property, property, economy and legal transactions – with **two conditions**: 1) the number of copies of an intellectual property item shall not be in excess of 2,000 (this condition applies to criminal offences against intellectual property, such as a breach of patent rights or unauthorised rights or subject of an IP ancillary right), or if incurred damage is in excess of 1 million dinars and 2) they can be considered cybercrime given the manner of their perpetration and utilised means (pursuant to Article 2, Paragraph 1 of the Law on CC).

Criminal offences that are not covered by this indirect definition set out in Articles 2 and 3 of the Law on CC cannot be considered cybercrime in the Republic of Serbia.

In line with the Law on CC, it is stipulated that a special department within the Higher Public Prosecutor's Office in Belgrade was established, which department is responsible for the entire territory of the Republic of Serbia, and it is designated by the legislator as the *special prosecutor's office*; Department for Cybercrime Combating within the Ministry of Interior –Criminal Police Directorate (which in the said Law is called: *Department for Cybercrime Combating*), and within the Higher Court of Belgrade, there is a Council for Cybercrime Combating (the legislator calls it in the Law: *Department*), which is in charge of the entire territory of the Republic of Serbia. The Ministry of Justice is responsible for ensuring conditions and means for realising tasks and activities of specialised directorates/departments of the Police Department, Public Prosecutor's Office and Court (Milošević & Putnik, 2017).

Chapter 27 of the Criminal Code includes the following charges (Articles 298-304a of the CC): damage to computer data and programmes (Article 298); computer sabotage (Article 299); creating and introducing of computer viruses (Article 300); computer fraud (Article 301); unauthorised access to computer, computer network or electronic data processing (Article 302);preventing or restricting access to public computer network (Article 303); unauthorised use of a computer or a computer network (Article 304); creating, obtaining and providing another person with means for the committing of criminal offences against the security of computer data (Article 304a). The last incrimination stands for a form of preparatory activity which has been elevated to the level of committing. Being aware

of the importance of prevention and level of danger of cybercrime to society, the legislator opted for early-stage criminal legislation suppression.

It should be noted that our legislator failed to undertake legislative penal measures just for one form of socially dangerous behaviour when handling computer data. This issue is illegal interception of data, which is not defined as a separate criminal offence. Article 3 of the Convention requires from the signatory parties to impose that such offences are criminally punishable as "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data."

Given that the presented summary overview of criminal legislation relative to cybercrime, we raise the question of whether existing incriminations also include the abuse of ransomware-malware, i.e. malicious codes. Among the mentioned criminal offences, the one set out in Article 300 obviously applies to the use of computer viruses, and we will therefore focus on it. After this, we will consider other, non-specific incriminations, which can be manifested in the form of cybercrime.

Creating and introducing of computer viruses and other possible qualifications in terms of criminal legislation

Creating a computer virus with intent to introduce it into another's computer or computer network is stipulated pursuant to Article 300 of the Criminal Code. Punishment for such offences is fine, alternatively imprisonment of up to six months. If the offender introduces a computer virus or causes damage, as defined in accordance with Paragraph 2) of this Article, punishment is fine or imprisonment up to two years. The Law specifies a mandatory security measure of seizing equipment and devices intended or used for the committing of such offences.

Article 112 of the Criminal Code specifies the meaning of the term computer virus and describes it as a type of computer programme (or a set of accounts, or commands) which are characterised by the ability to multiply, by adding themselves to other computer programmes and data, or to alter the way in which they function.

The basic form demonstrates the legislator's intention to act in the early stages because creating a computer virus with intent is, in essence, merely a preparatory activity. Since, generally speaking, preparation for a criminal offence is not punishable, by stipulating this basic form the legislator ensured that even preparatory activities are punishable, whereby they acquired the status of a criminal offence.

A graver form is, by definition, the basic form, which the legislator "artificially" transformed into an offence that qualifies as criminal because the legislator declared a preparatory action the basic form of the criminal offence. It is reasonable to ask here whether the existence of the form defined in accordance with Paragraph 1 after the Law on Changes in and Amendments to the CC of 2009 introduced the criminal offence defined in Article 304a. With this criminal offence, in addition to specifying and amending that occurred upon the passing of the Law on Changes in and Amendments to the CC of 2016, various forms of preparatory activities relative to committing criminal offences against computer data safety were defined. If the provisions of Article 304a were to be additionally specified,

then the need for the existence of the basic form of current Article 300, Paragraph 1, would completely cease to exist, which would be also justified in terms of legislative techniques.

More questions can be raised with regard to the currently prevailing regulations. Namely, it is clear that if a person creates a computer virus and then introduces it into another computer or network, he/she commits only criminal offence pursuant to Paragraph 2. Nevertheless, criminal offence from Paragraph 2 is consequential, which means that it is completed once damage has been suffered (Stojanović & Delić, 2020). In the event that a computer virus is introduced, and no harm is caused, then it is just attempted offence, which is not punishable in accordance with the general provisions.

So, the very fact that a computer virus is created with intent to introduce it into another's computer or network is punishable, while introducing the virus without any damage being caused would not be punishable. This is a strikingly illogical and is result of the fact that a preparatory activity is punishable whereas attempted "actual" offence is not. Preparatory activities should be punishable when a graver criminal offence is prepared, while this specific criminal act falls into the category of minor offences, which leads to disputable solutions.

We find it interesting that this criminal offence does not have multiple forms. If this chapter of the CC were to be made *de lege ferenda*, then striking out of Article 300, Paragraph 1 should be considered (with its clear "merging into" Article 304a), as well as addition of graver forms, which would refer to the committing of criminal offences mentioned in the present Paragraph 2 (which would become Paragraph 1), with certain qualifying circumstances. Such circumstances could be: inflicting damage to property in a certain amount; temporary or complete disruption or suspension in operation (if the injured party is an authority/organisation).

Nevertheless, before we further look into *de lege ferenda*, it is necessary to answer this question: can the abuse of malicious codes in the form of ransomware attacks be qualified solely under this Article of the CC or are there any other criminal qualifications that are also applicable in this case?

In this context, we should explore a possibility of the criminal offence – ransomware virus abuse – being included in the criminal offence of blackmail, as per Article 215 of the CC. Blackmail exists if the offender, with intent to acquire unlawful property gain for himself or another, by force or threat to the passive subject "or a person close to such passive subject disseminates something which may harm his honour or reputation". Accordingly, the use of a ransomware code could hypothetically be the criminal offence of blackmail only in cases when the injured party is blackmailed with dissemination of "captured" data, the dissemination of which could harm honour and reputation. However, this is hardly ever the case with ransomware, so in the majority of cases there will be no grounds for this offence to qualify under Article 215 of the CC.

However, it is possible to have situations in which the offender "holds hostage" computer data and blackmails the victim with dissemination thereof (e.g. acquires control of a computer system and gains access to photos, dissemination of which would harm reputation of the passive subject). This would qualify as blackmail. Since blackmail was committed by introducing a computer virus, a reasonable question here is possible existence of the offence stipulated in Articles 215 and 300 of the CC. In theory and court practice, a similar

question has been raised in connection with the relationship between fraud and a forged document. The position taken with regard to these offences is that if forging the document was the only way to commit fraud, concurrence of offences is ostensible (Stojanović & Perić, p. 153). Such a position is justified in this case solely if it really entailed only one possible manner of committing blackmail. In all other situations, there would be a real concurrence of offences, especially bearing in mind that these are criminal offences with very diverse protective objects.

So, just some individual cases of the abuse of ransomware codes may qualify as the criminal offence blackmail. Nevertheless, such cases are relatively rare, and the issue remains in which category in appropriate crime legislation qualification to include other socially dangerous activities committed through the use of malicious codes.

The criminal offence of coercion, as defined in Article 135 of the CC, exists if whoever, with the use of force or threat coerces another to do or refrain from doing something or to suffer something. Acting in terms of ransomware attacks corresponds to the legal description of the basic form of this offence because the injured party is threatened and coerced into doing or refraining from doing. Still, attempted basic form of this criminal offence is not punishable because the punishment is imprisonment of up to three years.

Additionally, the question is whether here we have a concurrence of offences with the criminal offence from Article 300 or is it just seemingly there (Delić, 2021; Vuković, 2021; Stojanović, 2018). The conclusion is the same as with blackmail. In most cases, this will be a real concurrence of two criminal offences. Admittedly, there is a reason why the legislator specified introducing computer viruses into another's computer or computer network, the reason being particular social danger that such activities entail. Therefore, it would not be justified to minimise the importance of the offence mentioned in Article 300 by reducing it merely to the manner in which a different criminal offence was committed.

Last, but by no means least, what we have to look into is a possibility of legal qualification of ransomware attacks as extortion (Article 214 of the CC). Extortion, as a property-related criminal offence, represents a special case of extortion and it is different from it in terms of the subjective element (intent to acquire unlawful property gain) and consequence (passive subject is forced to do something or refrain from doing something to the detriment of his or another's property). Bearing in mind that the offenders who use ransomware viruses as a rule have lucrative (financial gain) motivation, it is clear that a much higher number of these attacks could qualify as extortion. Extortion would be the accurate qualification only in situations when the offender did not have the intent to acquire unlawful property gain. The issue of concurrence of offences should be resolved in the same manner as was the case with blackmail and coercion. Given the defined punishment for the criminal offence set out in Article 214 of the CC, this attempt would be punishable.

Taking into account all of the above presented, we believe that the majority of manifestations of the abuse of ransomware-malware should be qualified as a concurrence of the criminal offence extortion and creating and introducing computer viruses. In the event that there was no intent to acquire unlawful property gain, then it would be a case of concurrence of offences – extortion and the offence from Article 300, where in a very few cases threat to disseminate information would be a concurrence of offences–blackmail and creating and introducing computer viruses.

De lege ferenda

Given the presented difficulties with regard to a suitable legal qualification, it is necessary to consider a possibility of adapting legislative solutions in a manner that suits ways in which criminal offences are committed in cyberspace, i.e. issue of the use of ransomware-malware.

Protection specified by criminal legislation could in this case be improved with the introduction of additional forms of the criminal offence set out in Article 300 or a completely new criminal offence. This new form/offence would exist if the offender introduced a computer virus, or some other malicious code, into another's computer or computer network thereby acquiring control over the operation of the computer, which the offender would use by warning the injured party that the use of such programmes and data would no longer be possible unless the injured party did what the offender required. So, the offender "holds hostage" another computer, i.e. programmes stored in it, thus coercing the injured party to act or refrain from acting in a certain manner and that unless that is the case, the computer remains decrypted, or data will be misused.

The wording of this criminal offence in the law could be as follows: whoever with intent to coerce another to do something, refrain from doing something or suffer something, introduces a computer virus or any such similar computer programme or a group of commands into another's computer or computer network, thereby acquiring control over the functioning of such computer or specific data or programmes, shall be punished by etc.

Additionally, it would seem justifiable to introduce an even graver form which would read as follows: if by committing the offence mentioned in the Paragraph above the offender were to acquire unlawful property gain or cause damage to property in the amount of …, or if any severe consequences occurred, the offender shall be punished by… A possible gravest form would apply to causing life-threatening damage to health of the citizens or potential threat to the functioning of economy or critical infrastructure (supply of energy products, traffic, etc.).

The former would incriminate just the use of ransomware-programme with intent, while the graver form would stipulate a more severe punishment, if damage were actually suffered, property acquired unlawfully or if other serious consequences occurred (e.g. consequences to private life, health, reputation and honour or workplace of the injured party, i.e. in the event that the passive subject is a legal entity –disruption of work processes, reputational harm, responsibility towards third parties, etc.).

Defined punishment should be adequate and proportionate to the actual danger to society. We believe that the trend of the use of this type of malware and potential consequences of its use justify the introduction of a new criminal offence or introduction of additional forms of the offence set out in Article 300.

Furthermore, in this manner practical difficulty in applying the law would be avoided, because this would resolve concerns over the legal qualification. The new criminal offence – computer extortion/coercion (or, possibly, new forms of the criminal offence described in Article 300), would be clearly distinguishable from other criminal offences and would have an adequate range of punishments, if observed from the perspective of social danger of such criminal behaviours. With the introduction of qualified forms which we suggest,

an entire range of activities would be included, such activities being a threat to the passive subjects when ransomware-virus, i.e. malicious codes are used.

CONCLUSION

Efficient protection of critical infrastructures, among which a particularly important position holds the information-communication infrastructure, imposes itself as an imperative of modern networked and computerised society.

In order to accomplish this objective, it is necessary to have a coordinated approach which entails continuous activity in terms of (re)defining, implementation and harmonisation of national and international security policies and strategies, as well as laws and standards. The protection of critical infrastructures, additionally, requires a consistent, cooperative partnership between the public and private sectors – between the owners and handlers of the infrastructures and state governments.

The ever-increasing dependence on critical infrastructures and the information-communication infrastructure leads to growing possibilities to breach security not only nationally but globally as well. This is confirmed by consequences which ransomware-malware has caused in terms of safety and health of people worldwide.

Accordingly, we believe that it is necessary to come up with optimum ways in which to improve protection of critical information infrastructure. To begin with, we deem that the legislative solution according to which the identification of critical infrastructure is sectoral (every competent ministry and other institutions decide for themselves what critical infrastructure in their sector is) should be changed by introducing uniform criteria. Furthermore, the level of security culture and awareness should be significantly improved, mainly through additional education of staff in charge of the protection of critical infrastructure. Cyberspace has brought us multiple benefits, but it has made us more vulnerable, so this is why legislative, organisational and educational measures are much needed in order to adequately confront challenges, risks and threats of modern times.

The currently prevailing criminal legislation norms do not provide suitable protection against the abuse of computer malware, in the form of ransomware attacks. The existing provisions lead to serious difficulties in interpretation, thus complicating qualification of the criminal offence, while they fail to include all socially dangerous behaviours which require to be treated by criminal legislation. With a change of the existing incrimination from Article 300 of the CC or introduction of a new criminal offence (computer extortion/coercion) which we suggest, these contradictions and incompleteness would no longer be the case, and at the same time criminal legislation would provide significantly stronger protection against modern ways of committing criminal offences in cyberspace.

REFERENCES / ЛИТЕРАТУРА

Acronis Cyberthreats Report (2022). Acronis Cyberthreats Report 2022 unveils cyber threat predictions. Available at: https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/

Bing, C. (2021). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. Available at: https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

Bischoff, P. (2021). Ransomware attacks on US healthcare organizations cost $20.8bn in 2020. Available at: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, *189*(22), 786-787

Coveware. (2021). Available at: https://www.coveware.com/ransomware-blog

Criminal Code, *Official Gazette of the Republic of Serbia*, No. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 [In Serbian]

Davis, J. (2020). UPDATE: The 10 Biggest Healthcare Data Breaches of 2020. Available at: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

Đorđević, Đ. (2014). *Criminal Law – a Special Part*, 3rd edition. Beograd: Kriminalističko-policijska akademija [In Serbian]

Fruhlinger, J. (2020). Ransomware explained: How it works and how to remove it. Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Global Economic Crisis (2013). Available at: https://www.sciencedirect.com/topics/economics-econometrics-and-finance/global-economic-crisis

Kovačević, A., Putnik, N. & Tošković, O. (2020). Factors Related to Cyber Security Behaviour. *IEEE Access*, *8*, 125140-125148. doi: 10.1109/ACCESS.2020.3007867

Law on Critical Infrastructure, *Official Gazette of the Republic of Serbia*, No. 87/18 [In Serbian]

Law on IT Security, *Official Gazette of the Republic of Serbia*, No. 6/2016, 94/2017 [In Serbian]

Law on the Organization and Competencies of State Bodies in the Fight against Cyber Crime, *Official Gazette of the Republic of Serbia*, No. 61/05, 104/09 [In Serbian]

Mandić, G., Putnik, N., Milošević, M. (2017). *Data protection and social engineering - legal, organizational and security aspects*. Beograd: Fakultet bezbednosti Univerziteta u Beogradu [In Serbian]

Milošević, M., Putnik, N. (2017). Cyber security and protection against high-tech crime in the Republic of Serbia – strategic and legal framework. *Kultura polisa*, *14*(33). 177-191 [In Serbian]

Milošević, M., Putnik, N. (2019). Specifics of committing the crime of fraud with the use of information and communication technologies. *Bezbednost*, 2/2019, 68–89 [In Serbian]

Mohurle, S., Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Morgan, S. (2019). Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021. *Cybercrime magazine*. Available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Putnik, N. (2009). *Cyberspace and security challenges*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti [In Serbian]

Radvanovsky, R. & McDougall, A. (2010). *Critical Infrastructure, Homeland Security and Emergency Preparedness. Second edition.* New York: CRC Press, Taylor & Francis Group.

Rakić, M. (2015). *Crisis management in the function of the protection of the critical infrastructures in the transition countries* (doctoral dissertation). Fakultet bezbednosti Univerziteta u Beogradu, Beograd. Available at: https://nardus.mpn.gov.rs/bitstream/handle/123456789/4220/Disertacija52.pdf?sequence=6 [In Serbian]

Stojanović, Z., Perić, O. (2011). *Criminal Law - a Special Part*, 14th edition. Beograd: Pravna knjiga [In Serbian]

Stojanović, Z. (2018). *Commentary on the Criminal Code*. Beograd: Službeni glasnik [In Serbian]

Stojanović, Z., Delić, N. (2020). *Criminal Law - a Special Part*, 7th edition. Beograd: Službeni glasnik [In Serbian]

Vuković, I. (2021). *Criminal Law – General Part*. Beograd: Pravni fakultet Univerziteta u Beogradu [In Serbian]