УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

МОГУЋНОСТИ СУПРОТСТАВЉАЊА ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ У РЕПУБЛИЦИ СРБИЈИ

мастер рад

Ментор:
Проф. др Ненад Путник

Студент:
Стефан Марковић, 22/18

Београд, 2021.

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

OPPORTUNITIES TO CONFRONT HIGH-TECH CRIME IN THE REPUBLIC OF SERBIA

master thesis

Mentor:
Prof. dr Nenad Putnik

Student:
Stefan Marković, 22/18

Belgrade, 2021.

МОГУЋНОСТИ СУПРОТСТАВЉАЊА ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ У РЕПУБЛИЦИ СРБИЈИ

Резиме: Примена рачунара у данашње време је веома распрострањена и скоро да нема области друштвеног живота где рачунар није нашао примену. Високотехнолошки криминал у Републици Србији, представља једну од највећих претњи за широко распростирање и коришћење информационо-комуникационих технологија. Под високотехнолошким криминалом подразумевају се кривична дела која се извршавају помоћу рачунара као средства извршења и објекта напада, и као таква су предвиђена кривичним или неким посебним законима и садрже сва специфична обележја која су везана за средства и начин њиховог извршења. Ова врста криминала је све заступљенија, добија нове форме и облике, и представља све већу опасност по друштво. У раду су приказани различити аспекти супротстављања високотехнолошком криминалу и технике заштите ИКТ ресурса, и дате су смернице за њихово унапређење. У будућности се може очекивати даље повећање стопе високотехнолошког криминала. Због тога треба константно радити на превенцији, заштити и сузбијању високотехнолошког криминала.

Кључне речи: високотехнолошки криминал, информационо-комуникационе технологије, превенција, супротстављање.

OPPORTUNITIES TO CONFRONT HIGH-TECH CRIME IN THE REPUBLIC OF SERBIA

Abstract: The use of computers nowadays is very widespread and there is almost no area of social life where the computer has not found application. High-tech crime in the Republic of Serbia, represents one of the biggest threats to the widespread and use of information and communication technologies. High-tech crime means crimes that are committed with the help of computers as a means of execution and the object of attack, and as such are provided by criminal or some special laws and contain all the specific features related to the means and manner of their execution. This type of crime is becoming more prevalent, gaining new forms and forms, and posing an increasing danger to society. The work shows different aspects of countering high-tech crime and ICT resource protection techniques, and guidelines have been issued for improving them. Further increases in the rate of high-tech crime can be expected in the future. Therefore, we need to work constantly on the prevention, protection and suppression of high-tech crime.

Key words: high-tech crime, information and communication technologies, prevention, countering.

САДРЖАЈ

1. УВОД

Високотехнолошки криминал (у даљем тексту: ВТК) у Републици Србији представља негативну друштвену појаву и његови кривичноправни и појавни облици у пракси Министарства унутрашњих послова (у даљем тексту: МУП) Републике Србије испољавају се као видови савременог криминала. У Републици Србији из године у годину расте степен ВТК. Држава са друге стране, покушава да му се супротстави, доношењем закона и стратегија.

У Републици Србији се под појам ВТК подводе компјутерски криминал и сајбер криминал. Са терминолошког аспекта може се поставити питање у колико мери је то оправдано и да ли су сајбер и компјутерски криминал подскупови ВТК? Проблем са којим се сусрећемо је управо то изједначавање високотехнолошког, сајбер и компјутерског криминала од стране законодавца у Републици Србији. Због тога ће главна истраживачка питања бити:

- Шта је ВТК у Републици Србији и какав је његов однос са другим сродним техничким појмовима: „компјутерски криминал“ и „сајбер криминал“?
- Које се мере превенције и заштите спроводе на сузбијању ВТК у Републици Србији?
- На који начин се може унапредити заштита од ВТК у Републици Србији?

Темељан и свеобухватан начин анализе ВТК захтева приступ који је најпре утемељен теоријским истраживањем, а затим и студијом о ВТК, као типу криминала с многобројним модалитетима испољавања. Значај предмета истраживања огледа се у потпунијем сагледавању овог сложеног типа криминала, чиме је усмерена његова темељна анализа, како би се у будућности повећало превентивно деловање, и кроз различите активности надлежних органа, образовног система, разних семинара и едукативних програма уз укључивање друштва дошло до његовог ефикасног откривања и сузбијања.

Предмет истраживања овог мастер рада је превенција, заштита и сузбијање ВТК у Републици Србији. Мастер рад, као прегледна студија, обухватио је сазнања о превенцији, заштити и сузбијању ВТК у Републици Србији. У циљу што ефикасније обраде теме користио сам докторске

дисертације, стручне и научне часописе, прегледне студије постојећих мастер радова, као и стручне теоријске изворе, научне радове, међународне документе, конвенције, протоколе, законе и друга акта.

2. ПОЈАМ, ФЕНОМЕНОЛОГИЈА И ЕТИОЛОГИЈА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

2.1. Појмовно одређење високотехнолошког криминала

Према дефиницији МУП Републике Србије, „ВТК обухвата скуп кривичних дела где се као објекат извршења и као средство за извршење кривичног дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови продукти у материјалном и електронском облику“ (МУП Републике Србије).

Што се више друштво буде развијало, веће су шансе да дође до појаве ове врсте криминала. Починиоци кривичних дела ВТК ће постајати временом стручнији и бројнији, а начини извршења кривичних дела ВТК ће постајати разноврснији. Prensky истиче да „комуникација на друштвеним мрежама и уопште дигитална комуникација доводи до креирања потпуно новог жаргонског језика, и дао му је назив дигитални језик или језик дигиталних урођеника“ (Prensky, 2001).

У својој докторској дисертацији Вида Вилић истиче да „ВТК подразумева и активно и пасивно коришћење компјутера, па чак и чување доказа о извршеном кривичном делу у рачунару или у електронској форми, а жртве и могуће жртве су сва физичка и правна лица која се служе рачунарима и базама података или зависе од њихове употребе“ (Вилић, 2016, стр. 93-95). Будући да не постоји потпуна сагласност у дефиницији ове врсте криминала, такође не постоји ни сагласност у имену ове врсте криминала. Употребљавају се различити термини, а неки од њих су нпр. високотехнолошки криминал, компјутерски криминал, интернет криминал, сајбер криминал, рачунарски криминал, информациони криминал, итд. У раду ћу користити два термина, и то: компјутерски криминал и високотехнолошки криминал. Ова два термина се најчешће користе у националним и међународним документима, а у нашем законодавству законодавац је прописао да у употреби буде термин високотехнолошки криминал.

Константиновић-Вилић, Николић-Ристановић и Костић тврде да се у литератури широм света често употребљава назив компјутерски криминал, због повезаности криминала са употребом компјутера (Константиновић-Вилић и сар., 2012, стр. 178). Занимљива је и констатација Спасића да се компјутерски криминал у правној литератури назива и криминалом сивих шешира (Спасић, 2006, стр. 107).

Шјолберг тврди да ћемо се сусрести са различитим дефиницијама компјутерског криминала, и истиче да је скоро свуда присутна јединственост и да је за реализацију ове врсте криминала потребно веома добро познавање рада на компјутерима. (Schjolberg, 2008).

Занимљива је дефиниција Виде Вилић, по којој „компјутерски криминал представља такав облик криминалног понашања где се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења" (Вилић, 2016, стр. 95). Такође можемо рећи да компјутерски криминал „представља противправну повреду имовине код које се рачунарски подаци с предумишљајем мењају, разарају, или се користе заједно са хардвером" (Вилић, 2016, стр. 95).

Поједини аутори, попут Паркера, сматрају да компјутерски криминал не може да се дефинише аутентичним појмом, и наводи да је управо ова врста криминала усмерена против безбедности информационих система како би се прибавила било која врста користи или како би се некоме нанела нека штета (Parker, 1983).

Занимљива је констатација Наташе Тањевић, по којој је „заједнички заштитни објекат кривичних дела која се често карактеришу као компјутерски криминал *безбедност рачунарских података*, при чему се под појмом рачунарских података подразумевају подаци који се уносе или користе ради несметаног рада рачунара, подаци који се уносе ради електронске обраде или који се преносе рачунарским мрежама" (Тањевић, 2009, стр. 154).

Занимљива је дефиниција Паркера, по којој је „компјутерски криминал дефинисан у најширем смислу као сваки злочин који се деси у оквиру неког компјутерског система, али и као врста криминала *белог оковратника* извршеног у оквиру неког компјутерског система, при чему се компјутер користи као средство извршења овог кривичног дела" (Parker, 1989).

У Практикуму о компјутерском криминалу, који је донет 1979. године у Сједињеним Америчким Државама (САД) од стране Националног правног института, дефинисан је компјутерски криминал. Bequai сматра да се „под компјутерским криминалом подразумева тачно одређен број кривичних дела која су Препоруком Савета Европе из 1989. године предложена на усвајање националним законодавствима" (Bequai, 1990).

2.2. Однос високотехнолошког, сајбер и компјутерског криминала

Криминал нема једноставну и универзално прихваћену дефиницију. Занимљива је дефиниција Родића, по којој је „криминал категорија дефинисана законом, тачније нешто је криминал ако је декларисано као такво релевантним и применљивим законом" (Родић, 2015). Борба против криминала се спроводи кроз његово спречавање, а један од главних задатака државног апарата је управо борба против криминала. Постоје превентивне и репресивне мере за сузбијање криминала. Мере које усмерене су на уклањање узрока криминала се називају превентивним, док се репресивне мере примењују према учиниоцу кривичног дела након што је дело извршено.

ВТК се скоро искључиво веже за компјутерски криминал. Заправо компјутерски криминал се, често у пракси, третира као синоним ВТК. Као да не постоје други појавни облици ВТК. Родић ову врсту криминала дефинише као криминал коме је средство или циљ извршења злочина висока технологија. Код компјутерског криминала као средство или циљ извршења кривичних дела користи се компјутер. Треба, дакле, разликовати компјутерски од сајбер криминала. Према Родићу сајбер криминал представља „криминал почињен на интернету (у сајбер простору) уз коришћење компјутера или сличног уређаја као средство или циљ кривичног дела" (Родић, 2015). Сајбер простор је домен који одликује употреба електронике и електромагнетног спектра за складиштење, мењање и размену података путем умрежених система и повезаних физичких инфраструктура.

„Кривични законик дефинише кривична дела против безбедности рачунарских података у члановима од 298. до (закључно) 304а. У тим члановима инкриминисана су следећа кривична дела:

- оштећење рачунарских података и програма
- рачунарска саботажа
- прављење и уношење рачунарских вируса

- рачунарска превара
- спречавање и ограничавање приступа јавној рачунарској мрежи
- неовлашћено коришћење рачунара или рачунарске мреже
- прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података" (Кривични законик, бр. 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019).

Очигледно је да су сајбер и компјутерски криминал прави подскупови ВТК. Такође се уочава да је само мали део сајбер криминала „непокривен" компјутерским криминалом. Као што, са друге стране, постоји велики део ВТК који нема никакве везе са сајбер криминалом. Овим је показано да је изједначавање ВТК са сајбер и компјутерским криминалом погрешно.

2.3. Појавни облици и карактеристике високотехнолошког криминала

Занимљива је подела компјутерског криминала од стране Наташе Тањевић, по којој се разликују две врсте компјутерског криминала: „*традиционални компјутерски криминал* и *савремени облици компјутерског криминала који су се развили због злоупотреба компјутера и компјутерских мрежа*. Традиционални компјутерски криминал најчешће обухвата кривична дела која су уз помоћ рачунара извршена против имовине (нпр. кривична дела крађе, проневере и сл.), док савремени облици компјутерског криминала који су се развили због злоупотреба компјутера и компјутерских мрежа обухватају само она кривична дела која могу да се изврше употребом рачунара и злоупотребом рачунарских мрежа без обзира на то да ли је мотив за њихово извршење стицање материјалне користи (нпр. интернет прогањање, сајбер тероризам и сл.)" (Тањевић, 2009, стр. 157).

Вида Вилић наводи да „појавни облици компјутерског криминала могу да буду: противправно коришћење услуга и неовлашћено прибављање информација, компјутерске крађе, компјутерске преваре, компјутерске саботаже, компјутерски тероризам итд." (Вилић, 2016, стр. 100).

Један познати немачки теоретичар, Зибер (Sieber), сматра да се оног тренутка када је први пут угрожена приватност корисника интернета појавио проблем компјутерског криминала (Sieber, 1998).

Занимљива је подела компјутерског криминала зависно од типа извршених кривичних дела од стране Виде Вилић, по којој „компјутерски криминал може бити:

- *политички* (нпр. компјутерска шпијунажа),
- *економски* (нпр. компјутерске преваре),
- *производња и дистрибуција недозвољених и штетних садржаја* (нпр. дечија порнографија),
- *манипулација забрањеним производима, супстанцама и робама* (нпр. дрога),
- *повреде приватности на интернету* (нпр. надгледање електронске поште)" (Вилић, 2016, стр. 100).

Компјутери када су конструисани било је практично немогуће да у већој мери дође до њихове злоупотребе. У то време компјутери нису били у толико великој употреби као данас, и тада је било потребно обучити лице за рад на компјутеру, да би то лице уопште могло да користи компјутер. Међутим, веома брз развој компјутера и компјутерске технологије довели су до тога да компјутерски криминал постане опасан вид криминала у данашње време. Свакодневна употреба компјутера, довела је до тога да компјутерски криминал из сфере будућности постане опасан и известан вид криминала данашњице.

Вида Вилић истиче да су најчешћи појавни облици компјутерског криминала: „компјутерске крађе, компјутерске преваре, неовлашћено прибављање информација уз помоћ компјутера, неовлашћено прибављање или уништење информација садржаних у компјутеру, онемогућавање или отежавање приступа таквим информацијама (компјутерска саботажа), компјутерски тероризам" (Вилић, 2016, стр. 101-102).

Занимљива је и подела понашања на интернету од стране Шиндер, према којој „понашања на интернету се деле на: насилна и потенцијално насилна дела, деструктивна понашања и на ненасилна понашања на интернету. У *насилна и потенцијално насилна понашања* на интернету убрајају се сајбер тероризам, претње преко интернета, интернет прогањање и дечија порнографија; у *деструктивна понашања* спадају дела приликом чијег извршења се уништавају или оштећују рачунарске мреже или подаци, а у *ненасилна понашања на интернету* спадају неовлашћени упад у базе података, интернет крађа, интернет превара, интернет

проституција, коцкање преко интернета и слично" (Littlejohn Shinder, 2002, pp. 19-33).

Према Јовашевићу и Хашимбеговићу починиоци кривичних дела компјутерског криминала представљају јединствену категорију људи. Најчешће се ради о људима који нису били деликвентни, насилни, и друштвено прилагодљиви појединцима. Те особе поседују одређени степен знања у домену информатике, компјутерске технологије и њима су таква средства доступна за извршење кривичних дела. Кривична дела компјутерског криминала се врше прикривено, без неке видљиве и блиске просторне повезаности учиниоца дела и жртве. Та дела се тешко откривају, а још теже доказују (Јовашевић и Хашимбеговић, 2004, стр. 3-4).

2.4. Потенцијални циљеви високотехнолошког криминала

Према Видојковићу, „потенцијални циљеви ВТК могу бити: хардвер, софтвер, програми, подаци, заштита, услуге. *Напад на хардвер* – уништење, оштећење или отуђење рачунарског система или његових компоненти. *Напад на софтвер* – уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење софтверских производа. *Напад на програм* – уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење програмских производа. *Напад на податке* – уништење, оштећење, отуђење и неовлашћена измена, објављивање или коришћење података. *Напад на заштиту система* – нарушавање или пробијање система заштите. *Напад на услуге* – неовлашћено коришћење информационих ресурса" (Видојковић, 2015, стр. 7-8).

Поједини аутори, као што је на пример Шиндер, тврде да је нове и драстичне промене у свим сферама савременог живота унела управо компјутерска технологија. Поред својих позитивних страна те промене су донеле и низ проблема везаних за појаву и ширење ВТК, разних облика, форми и видова испољавања и оне се могу свести на следеће: нове форме вредности, концентрација података, нови амбијент деловања, нове методе и технике деловања, сужавање временске скале деловања, ширење географског простора деловања, мобилност, и стабилност ризика и самим тим се повећава број потенцијалних и могућих циљева компјутерског криминала (Littlejohn Shinder, 2002).

2.5. Последице високотехнолошког криминала у Републици Србији

Бановић сматра да се штетна последица ВТК испољава као настала имовинска штета, а може да се испољи и у виду губљења поверења у сигурност и тачност добијених информација из компјутерског система, што може довести до различитог третирања и нарушавања пословног угледа многих привредних и ванпривредних субјеката и изазвати страх од појаве нових криминалних радњи везаних за све нивое функционисања компјутерског система (Бановић, 2002).

Игњатијевић и Матијашевић истичу да су последице које наступају вршењем кривичних дела ВТК по правилу штетне и веома велике. Поред последица финансијске природе које могу да настану када учинилац врши дело у циљу стицања противправне имовинске користи, па ту корист за себе или друго лице заиста и стекне, или је не стекне, али својим делом објективно причини одређену штету, или када учинилац не поступа ради стицања користи за себе или другога, али објективно учини финансијску штету, постоје и последице нематеријалне природе које се огледају у неовлашћеном откривању туђих тајни, нарушавању угледа, повреди моралног права или другом сличном поступању, као и комбиноване последице, које постоје када се откривањем одређене тајне, или повредом ауторског права, путем злоупотребе компјутера или информатичке мреже нанесе одређени вид нематеријалне штете, а истовремено проузрокује и конкретна финансијска штета (Игњатијевић и Матијашевић, 2010, стр. 854).

2.6. Профил компјутерских криминалаца

Због великог броја кривичних дела компјутерског криминала и различитих узрока који појединце подстичу на извршење оваквих кривичних дела, не можемо све починиоце подвести под јединствен профил. У већини случајева ради се о млађим мушкарцима који су високо образовани, који нису раније били гоњени и кажњавани, имају радно искуство и обезбеђују егзистенцију и углавном све виде као изазов. Углавном се починиоци кривичних дела ВТК деле на оне који врше дела ради стицања имовинске добити и починиоци којима новац није приоритет, него виде одређен степен изазова, узбуђења и забаве у продирању у системе и обарању њихове заштите.

Алексић и Шкулић истичу да је комплетан криминолошки профил починиоца који кривична дела врше ради стицања имовинске добити следећи: 80% њих кривично дело врши први пут, 70% њих је кривично дело извршило у фирми у којој су запослени, старости су између 16. и 30. година, претежно су мушког пола, веома су интелигентни, неки су запослени али доста њих нису, неки имају дугогодишње искуство у струци, квалификованији су и образованији него што потребе њиховог радног места то захтевају, нису осуђивани, себе не сматрају криминалцима. Овај профил починиоца је чест у великим пословним системима, попут финансијских организација, банака (Алексић и сар., 2016, стр. 348-349).

Занимљива је подела починилаца кривичних дела ВТК од стране Димовског, по којој се они деле на: „починиоце који су мотивисани искључиво на стицање противправне добити, и на хакере којима стицање добити није примарни циљ вршења кривичних дела" (Димовски, 2010, стр. 208). Димовски починиоце који кривична дела врше ради стицања противправне добити дели на *аматере* и *професионалне криминалце*. *Аматери* су слаби и подложни појединци, људи са пороком, и фрустрирани појединци, док су *професионални криминалци* индивидуални професионални криминалци, организоване групе и криминалне организације. *Аматери* обично имају имају легално занимање, али се повремено баве компјутерским криминалом, и углавном остају неоткривени. *Слаби и подложни појединци* – овој групи припадају починиоци који су производи њихове слабе личности, а и слабих инструмената контроле. *Људи са пороком* – дрога, алкохол, коцка, живот изнад сопствених новчаних могућности су фактори који знатно мотивишу починиоца да се бави компјутерским криминалом. *Фрустрирани појединци* – огорчени, незадовољни и разочарани појединци, представљају тип криминалаца који су најопаснији по друштво. *Професионални криминалци* су лица којима је бављење криминалом једино занимање и извор зараде, имају огромно искуство и представљају велику друштвену опасност. У оквиру ове групе разликујемо индивидуалне криминалце, организоване групе и криминалне организације. *Индивидуални криминалци* – наступају индивидуално у реализацији својих циљева. Могу бити у кооперацији са другим криминалцима, али углавном повремено. Делују у локалу и немају разрађен дугорочни план деловања. *Организоване групе* – скуп појединаца који ради остварења својих криминалних амбиција делују заједно. Локалног су карактера, али са израженом стратегијом и тактиком.

Потенцијал за извршење кривичних дела им варира, али је сходно бројности и организованости, далеко већи од индивидуалних криминалаца, али још не толики да би последице имале неки већи национални ефекат. *Криминалне организације* – представљају највиши облик организације, одликују се чврстом хијерархијом, строгом дисциплином, послушношћу, лојалношћу уз изграђену дугорочну стратегију и тактику, уз тајност као најзначајнији фактор опстанка (Димовски, 2010, стр. 208-209).

Поједини аутори, попут Илингворта, сматрају да се са развитком информационе технологије појавио нови тип криминалца – *хакер*. Хакер је особа која неовлашћено упада у туђе, заштићене системе. Њихов мотив је често само лична сатисфакција, али понекад и злонамерно чине штету или краду. Опседнути су технологијом. Свој ужитак налазе у самом изазову пробијања заштите система и упада у туђи систем. Воле да проналазе недостатке у програмима, а поготово у системима заштите (Илингворт, 1990, стр. 93). Профил хакера криминолози сагледавају на више начина и анализирају са различитих аспеката. Занимљиве су следеће карактеристике хакера: они су скоро 100% мушкарци; слично рачунарским програмерима, хакери су екстремно бистри, склони истраживачком и логичком размишљању и увек су такмичарски расположени; по природи су веома радознали; не воле цензуру јер то води једноумљу; воле да виде себе као ауторитете за рачунаром и над било ким ко је повезан са њим, што им даје осећај моћи и контроле, дакле они су заинтересовани за добијање осећаја моћи, него за последице својих радњи; имају мало респекта према онима који не знају ништа о њиховој омиљеној теми компјутерима (Chiesa et al., 2008, pp. 43-44).

2.7. Теорије узрочности високотехнолошког криминала

Џејшанкар (Jaishankar) је установио посебну теорију о компјутерском криминалу 2008. године, и назвао је „*теорија транзиције простора* (енгл. Space Transition Theory). Теорија објашњава природу понашања особе која испољава прилагођено или неприлагођено понашање у стварном простору и у кибернетичком простору. Према овој теорији људи се различито понашају приликом преласка из стварног простора у виртуелни простор“ (Jaishankar, 2007, p. 7).

Према *теорији стила живота*, онлајн начин живота директно утиче на виктимизацију од компјутерског криминала. Студенти који користе

компјутере и немају антивирус програме, имају далеко већу шансу да постану жртве компјутерског криминала.

„*Теорија диференцијалне асоцијације и теорија самоконтроле* објашњавају узроке појединих облика компјутерског криминала, сајбер тероризма, дечије порнографије и сајбер пиратерије. *Теорија самоконтроле* се везује за психолошке факторе криминала. *Теорија диференцијалне асоцијације* полази од утицаја криминалних и некриминалних понашања унутар групе и опредељивања чланова групе за једно или друго понашање, зависно од утицаја који преовлађује. Битан аспект успеха терористичких група, које су своје чланство омасовиле користећи интернет и друштвене мреже, управо су објашњења ове теорије о прихватању криминалних утицаја. Према *теорији рационалног избора* преступници ће увек тежити да изаберу оне мете које захтевају најмање напора, али које у исто време пружају високу награду и носе најмањи ризик у погледу откривања и последица неуспеха“ (Мирковић, 2017, стр. 75-76).

3. ЗАКОНОДАВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР У СУПРОТСТАВЉАЊУ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ У РЕПУБЛИЦИ СРБИЈИ

3.1. Конвенција о високотехнолошком криминалу Савета Европе са Додатним протоколом

Конвенција Савета Европе о ВТК 185 од 23. новембра 2001. године са Додатним протоколом усвојена је као резултат кампање Савета Европе покренуте 1996. године оснивањем Комитета стручњака за криминал у сајбер простору. Анализа кривичних дела која се могу извршити путем интернета био је главни задатак овог комитета. Међутим, у фебруару 1997. године основан је Комитет експерата о криминалу у сајбер простору. Главни задатак овог комитета био је да се дефинишу преступи, утврде надлежности, да се провери распрострањеност и појавни облици ВТК.

Вилић наводи да постоји много разлога за доношење Конвенције, а неки од њих су: остваривање међународне сарадње између држава, знатно лакше откривање, вршење истрага и гоњења кривичних дела ВТК на националном и међународном нивоу итд. Доношење Конвенције омогућило је националним законодавствима развијање мреже за борбу против компјутерског криминала (Вилић, 2016). Конвенцију је до сада потписало 47 држава чланица Савета Европе, а од тих 47 држава само две је нису ратификовале, и то: Ирска и Шведска. Значај овог документа за

сузбијање ВТК може се видети и по томе што су Конвенцију потписале и земље које нису чланице Савета Европе, као нпр. Израел, Јапан, Канада итд. У априлу 2005. године, тачније 07.04.2005. године, Република Србија, у тадашње време државна заједница Србије и Црне Горе, је у Хелсинкију потписала ову Конвенцију са Додатним протоколом. Народна скупштина Републике Србије 2009. године ратификовала је и Конвенцију и Додатни протокол, и исте године је почела обавеза примене ратификоване Конвенције са Додатним протоколом. Конвенција садржи материјалне и процесне кривичноправне одредбе. У Конвенцији у првом поглављу се дефинишу појмови, у другом поглављу се спомињу мере које треба предузети на нивоу појединих држава, треће поглавље се односи на међународну сарадњу у борби против ВТК, и четврто поглавље се односи на потписивање и ступање на снагу.

У Конвенцији у члану 1 су наведене дефиниције: *рачунарског система, рачунарског податка, даваоца услуга, податка о саобраћају.* Интересантно је споменути и постојање мреже 24/7, која представља мрежу контаката са свим земљама које су ратификовале ову Конвенцију. Свака земља, која је ратификовала ову Конвенцију, мора да одреди место са којим ће се моћи ступити у контакт у било ком тренутку дана, недеље, месеца, године. То место мора бити доступно 24 сата дневно свих седам дана у недељи целе године, како би се омогућио хитан одговор и помоћ у хитним истрагама.

3.2. Кривични законик и кривична дела против безбедности рачунарских података

„Кривични законик у оквиру главе XXVII предвиђа *кривична дела против безбедности рачунарских података*, али и друга кривична дела која се на основу Конвенције о ВТК и позитивно-правних законских прописа сматрају кривичним делима компјутерског криминала. Кривична дела компјутерског криминала предвиђена Кривичним закоником могу се сврстати у три групе: (1) сва кривична дела која за групни заштитни објекат имају безбедност компјутерских података; (2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају компјутери, компјутерске мреже, компјутерски подаци и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од милион динара и (3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и

безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалу" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019).

3.2.1. Кривична дела против безбедности рачунарских података

ВТК, у глави XXVII Кривичног законика, обухвата скуп „кривичних дела против безбедности рачунарских података, и то:

- оштећење рачунарских података и програма,
- рачунарску саботажу,
- прављење и уношење рачунарских вируса,
- рачунарску превару,
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података,
- спречавање и ограничавање приступа јавној рачунарској мрежи,
- неовлашћено коришћење рачунара или рачунарске мреже, и
- прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019).

По закону о ауторским и сродним правима, ауторским делима сматрају се „нарочито рачунарски програми у било ком облику њиховог изражавања, укључујући и припремни материјал за њихову израду, затим музичка дела са или без речи и припремни материјал за њихову израду, као и филмска дела" (Закон о ауторским и сродним правима, 104/2009, 99/2011 и 119/2012: чл. 2).

„*Оштећење рачунарских података и програма* је кривично дело против безбедности рачунарских података које врши свако лице које неовлашћено избрише, измени, оштети, прикрије, или на други начин учини неупотребљивим рачунарски податак или програм, и такво лице ће се казнити новчаном казном или затвором до једне године. Међутим, ако је кривичним делом проузрокована штета у износу који прелази четиристопедесет хиљада динара, учинилац ће се казнити затвором од три

месеца до три године. Ако је кривичним делом проузрокована штета у износу који прелази милион и петсто хиљада динара, учинилац ће се казнити затвором од три месеца до пет година. У ставу четири овог члана прописана је обавезна примена мере безбедности одузимања предмета којим је извршено ово кривично дело" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 298).

„*Рачунарска саботажа* је кривично дело против безбедности рачунарских података које врши свако лице које унесе, уништи, избрише, оштети, измени, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, и то лице ће се казнити затвором од шест месеци до 5 година" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 299). Лазаревић сматра да су кривична дела рачунарска саботажа и оштећење рачунарских података и програма слична према начину извршења и последицама које могу оставити. Такође наводи да се ова кривична дела разликују по тежини последица које проузрокују, јер су последице кривичног дела рачунарска саботажа много теже и имају знатно шири спектар последица и објеката и правних субјеката (Лазаревић, 2011, стр. 811). Комлен Николић са својим сарадницима тврди да се последице рачунарске саботаже манифестују у знатном онемогућавању или знатном отежавању функционисања државног органа за дужи временски период, заједно са огромном материјалном штетом и губицима (Комлен Николић и сар., 2010, стр. 94).

„*Прављење и уношење рачунарских вируса* је кривично дело против безбедности рачунарских података које врши свако лице које направи рачунарски вирус у намери његовог уношења у туђ рачунар или рачунарску мрежу, и то лице ће се казнити новчаном казном или затвором до шест месеци. Свако ко унесе рачунарски вирус у туђ рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године. Уређај и средства којима је учињено кривично дело одузеће се" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 300). „МУП Републике Србије је прву

кривичну пријаву за ово кривично дело поднело 2010. године против Огњена Цветковића из Београда. Он је направио вирус типа тројанац под називом OMEA који је имао функције сликања активног монитора зараженог компјутера, снимања куцања карактера на тастатури, као и функције постављања садржаја на "заражени" компјутер и скидања садржаја са компјутера преко ИРЦ канала. Огњен је представљајући се лажно као Ирена Милетић, Јохан Мајстер (Johan Meister) и др Мајер (dr Mayer), слао вирус као додатак текстуалном делу мејла који је био послат на преко 70 електронских адреса. Вирусом је успео да зарази три немачка држављанина. Један од заражених компјутера, припадао је лицу које је клијент "Баден-Виртемберг" банке. О.Ц. је његове податке искористио да би путем електронског налога на сајту банке, лажно приказао да је он корисник и власник рачуна и довео у заблуду службенике да на рачун једне банке у Београду, уплате износ од 2.600 евра, са сврхом уплате – помоћ пријатељу" (Радио-телевизија Војводине, 2010).

„*Рачунарска превара* је кривично дело против безбедности рачунарских података које је прописано чланом 301. Кривичног законика. Ово кривично дело врши свако ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, и то лице казниће се новчаном казном или затвором до три године. Ако је кривичним делом прибављена имовинска корист која прелази износ од четиристопедесет хиљада динара, учинилац ће се казнити затвором од једне до осам година. Ако је кривичним делом прибављена имовинска корист која прелази износ од милион и петсто хиљада динара, учинилац ће се казнити затвором од две до десет година. Свако ко ово кривично дело учини само у намери да другог оштети, казниће се новчаном казном или затвором до шест месеци" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 301). Лазаревић сматра да је нетачан податак онај податак који не одражава истинито оно на шта се односи. Прописивањем овог кривичног дела, намера законодавца је била усмерена ка заштити веродостојности и интегритета компјутерских података, који се електронским путем обрађују или се на овај начин врши њихово преношење (Лазаревић, 2011, стр. 884).

„Против М. Ц. (17) из Врања и његовог вршњака Д. Ч. у Посебном одељењу Окружног јавног тужилаштва у Београду за борбу против ВТК, стављен је захтев за покретање истраге због сумње да су починили рачунарску превару. Сумња се да су двојица Врањанаца платним картицама држављана САД наручивали и плаћали робу преко интернета. Поступак против Д. Ч. је издвојен, јер је саизвршилац. Све је почело када је Мајкрософт српској полицији упутио елаборат о опасној групи српских хакера који месецима харају интернет продавницама у САД. Изненађење полиције није било мало када је утврђено да је "опасна група хакера", у ствари голобради младић из Врања! У захтеву за спровођење истраге против М. Ц. пише да је куповао преко сајта њњњ.цомтрадесхоп.цом. Наручивао је углавном скупе мобилне телефоне, компјутере, игрице, лаптопове. Уносио је електронски налог предузећа "СТ RETAIL D.O.O.", оштетивши га за 270.238 динара. М. Ц. је купио шест "Нокиа" мобилних телефона вредних 194.700 динара, конзолу од 37.777 динара и лаптоп који је коштао исто толико. Укупно - 270.238 динара, мада би износ, с обзиром на то да је истрага још увек у току, могао да буде и много већи. М. Ц. је робу наручивао на име Милош Димитријевић из Улице Есперанто 10 у Врању. Користио је поштанске услуге ДХЛ или "Сити експреса". Пошиљке је увек преузимао Д. Ч. У почетку су телефоне поклањали девојкама, другарима и родбини, а онда су почели, наводно, и да их продају. Прича се да је М. Ц. и мајци продао лаптоп убедивши је да извесним младенцима за свадбу поклони лаптоп, а не микроталасну рерну као што је планирала. Лаптоп је, наравно, наручио из Америке, а мајци испоставио рачун" (С. В., 2009).

„*Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података* је кривично дело против безбедности рачунарских података које врши свако ко се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, и учинилац ће се казнити новчаном казном или затвором до шест месеци. Свако ко сними, или употреби податак добијен на начин предвиђен у претходном ставу овог члана, казниће се новчаном казном или затвором до две године. Ако је услед дела дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, учинилац ће се казнити затвором до три године" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 302).

„*Спречавање и ограничавање приступа јавној рачунарској мрежи* је кривично дело против безбедности рачунарских података које врши свако ко неовлашћено спречава или омета приступ јавној рачунарској мрежи, и то лице ће се казнити новчаном казном или затвором до једне године. Ако ово кривично дело учини службено лице у вршењу службе, казниће се затвором до три године" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 303).

„*Неовлашћено коришћење рачунара или рачунарске мреже* је кривично дело против безбедности рачунарских података које врши свако ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист, и свако ко то чини казниће се новчаном казном или затвором до три месеца. За разлику од осталих кривичних дела за која се поступак покреће и води по службеној дужности, за ово кривично дело поступак се покреће приватном тужбом" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019, чл. 304). „Посебна радња доказивања која је од 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 (БИА), Војнобезбедносна агенција (ВБА), царинске, пореске или друге службе или други државни орган, односно правно лице које на основу закона врши јавна овлашћења" (Милошевић и Путник, 2017, стр. 182).

„*Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података* је кривично дело против безбедности рачунарских података које врши свако ко производи, продаје, набавља ради употребе, увози, дистрибуира, и на други начин ставља на располагање:

- уређаје и рачунарске програме пројектоване или првенствено у сврхе извршења неког кривичног дела из чл. 298. до 303. овог законика казниће се затвором од шест месеци до три године, а свако ко поседује нека од средстава у намери да их употреби у сврху извршења неког од кривичних дела из чл. 298. до 303. овог законика,

– рачунарске шифре или сличне податке путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у извршењу неког од кривичних дела из чл. 298. до 303. овог законика, и то лице ће се казнити затвором од шест месеци до три године.

Свако ко поседује нека од средстава из претходног става овог члана, у намери да их употреби у сврху извршења неког од кривичних дела из чл. 298. до 303. овог законика, казниће се новчаном казном или затвором до једне године. Предмети из претходних ставова овог члана одузеће се" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 304а).

3.2.2. Остала кривична дела која припадају компјутерском криминалу

„Кривични законик у глави XVIII, која се односи на *кривична дела против полне слободе,* предвиђа кривична дела у вези са дечијом порнографијом, што у потпуности одговара чл. 9 Конвенције о ВТК и Конвенцији о заштити деце од сексуалне експлоатације и сексуалног злостављања. Злоупотреба малолетника и деце за порнографију је најчешћи појавни облик ВТК" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: глава осамнаеста).

У склопу овог подпитања биће обрађена нека од кривичних дела која се налазе у Кривичном законику, али која због њихове непосредне везе са злоупотребом компјутерске технологије спадају у представнике кривичних дела која се могу сматрати кривичним делима ВТК.

„Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију је кривично дело против полне слободе, и свако ко малолетнику прода, прикаже или јавним излагањем или на други начин учини доступним текстове, слике, аудио-визуелне или друге предмете порнографске садржине или му прикаже порнографску представу, казниће се новчаном казном или затвором до шест месеци. Свако ко искористи малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу, казниће се затвором од шест месеци до пет година. Ако је дело из ст. 1. и 2. овог члана извршено према детету, учинилац ће се казнити за дело из става 1. затвором од шест месеци до три године, а за дело из става 2. затвором од једне до осам година. Свако ко

прибавља за себе или другог, поседује, продаје, приказује, јавно излаже или електронски или на други начин чини доступним слике, аудио-визуелне или друге предмете порнографске садржине настале искоришћавањем малолетног лица, казниће се затвором од три месеца до три године. Свако ко помоћу средстава информационих технологија свесно приступи сликама, аудио-визуелним или другим предметима порнографске садржине насталим искоришћавањем малолетног лица, казниће се новчаном казном или затвором до шест месеци. Предметима порнографске садржине насталим искоришћавањем малолетног лица (дечија порнографија) сматра се сваки материјал који визуелно приказује малолетно лице које се бави стварним или симулираним сексуално експлицитним понашањем, као и свако приказивање полних органа детета у сексуалне сврхе. Предмети из ст. 1. до 4. овог члана одузеће се" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 185).

„*Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу* је кривично дело против полне слободе, које врши свако ко у намери извршења овог кривичног дела, користећи рачунарску мрежу или комуникацију другим техничким средствима, договори са малолетником састанак и појави се на договореном месту ради састанка, и то лице ће се казнити затвором од шест месеци до пет година и новчаном казном. Ко дело из става 1. овог члана изврши према детету, казниће се затвором од једне до осам година" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 185б).

„Кривични законик у глави XX предвиђа следећа кривична дела против интелектуалне својине: повреда моралних права аутора и интерпретатора - чл. 198, неовлашћено искоришћавање ауторског дела или предмета сродног права - чл. 199, неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима - чл. 200, повреда проналазачког права - чл. 201 и неовлашћено коришћење туђег дизајна - чл. 202" (Кривични законик, 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019: чл. 198-202). Од горе наведених кривичних дела против интелектуалне својине, кривична дела која су највише повезана са коришћењем интернета су повреда моралних права аутора и интерпретатора (чл. 198), неовлашћено искоришћавање ауторског дела

или предмета сродног права (чл. 199), неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200).

3.3. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала у Републици Србији

„Закон о организацији и надлежности државних органа за борбу против ВТК ступио је на снагу 25. јула 2005. године, а његове измене и допуне 11. децембра 2009. године. Самим тиме успостављена је организација и одређена надлежност државних органа у борби против ВТК. Закон уређује образовање, организацију, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела ВТК. ВТК у смислу овог закона представља 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 – рачунарски програми и ауторска дела која се могу употребити у електронском облику. У члану 3 овог закона прецизирано је да се његове одредбе примењују ради откривања, кривичног гоњења и суђења за сва кривична дела против безбедности рачунарских података одређена Кривичним закоником, за кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења јављају рачунари и за кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира, уставног уређења и безбедности Републике Србије, која због начина извршења или употребљених средстава несумњиво припадају компјутерском криминалу" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09).

„Овај закон примењује се ради откривања, кривичног гоњења и суђења за:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником;

2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара;

3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2. став 1. овог закона" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09: чл. 3).

Бејатовић сматра да формулацијом стварне надлежности нису обухваћена сва кривична дела која припадају ВТК, а пре свега мисли на следећа дела: „приказивање, прибављање, и поседовање порнографског материјала, искоришћавање малолетног лица за порнографију и кривично дело фалсификовање и злоупотреба платних картица" (Бејатовић, 2012). Предложено је да се прошири формулација стварне надлежности, и те измене закона су ступиле на снагу 01. јануара 2010. године.

3.4. Законик о кривичном поступку и процесне одредбе о компјутерском криминалу

У чл. 2. Законика о кривичном поступку Републике Србије постоје дефиниције следећих термина: „електронски запис", „електронска адреса", „електронски документ", „електронски потпис", али нема дефиниције „електронског доказа", који је за компјутерски криминал веома значајан. Ови докази се могу врло лако обрисати, изменити, или на било који други начин уништити. Могу бити смештени на рачунару, рачунарској мрежи или удаљеном серверу ван територијалне надлежности органа који их прикупљају, могу бити видљиви или невидљиви. Радуловић сматра да „принципи прибављања електронских доказа подразумевају да ниједном радњом овлашћених лица не сме бити измењен садржај података који се прегледају. Принципе је неопходно доследно примењивати у сваком конкретном случају како би се сачувао интегритет доказа који се прибављају, документовао процес њиховог прибављања који омогућава понављање процеса уколико се за тим укаже потреба у каснијем току поступка, чиме се обезбеђује њихова доказна снага пред законом" (Радуловић, 2008, стр. 17-18).

Конвенција о ВТК указује на значај електронског доказа, док Законик о кривичном поступку не придаје значај електронском доказу, што можемо закључити тиме што уопште не постоји његова дефиниција у Законику о кривичном поступку. У чл. 152. овог законика предвиђено је да предмет претресања могу да буду уређаји за аутоматску обраду података и опреме

на којој се чувају или се могу чувати електронски записи. Писарић наводи да „у случају да лице пронађе компјутер са подацима у вези са извршењем кривичног дела компјутерског криминала, то лице сме само да обезбеди тај компјутер, и не сме да изврши претресање компјутера све док не добије одлуку суда, јер је за претресање неопходна судска наредба" (Писарић, 2015, стр. 233). Друге одредбе Законика о кривичном поступку односе се на привремено одузимање предмета. Кнежевић тврди да у „предмете који се могу привремено одузети и послужити као доказ у кривичном поступку спадају и уређаји за аутоматску обраду података и уређаји и опрема на којој се чувају или се могу чувати електронски записи" (Кнежевић, 2015, стр. 318). Законик о кривичном поступку није предвидео примену ових правила на рачунарске податке, али би се и они такође могли привремено одузети.

Прикупљањем доказа помоћу компјутерске технологије важно је указати на рачунарско претраживање података (чл. 178 - 180 Законика о кривичном поступку). „На образложени предлог јавног тужиоца суд може одредити рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело (чл. 178). Посебну доказну радњу из члана 178. овог законика одређује судија за претходни поступак образложеном наредбом. Наредба из става 1. овог члана садржи податке о осумњиченом, законски назив кривичног дела, опис података које је потребно рачунарски претражити и обрадити, означење државног органа који је дужан да спроведе претрагу тражених података, обим и време трајања посебне доказне радње. Рачунарско претраживање података може трајати највише три месеца, а због неопходности даљег прикупљања доказа може се изузетно продужити још највише два пута у трајању од по три месеца. Спровођење рачунарског претраживања података се прекида чим престану разлози за његову примену (чл. 179). Наредбу из члана 179. став 1. овог законика извршава полиција, Безбедносно-информативна агенција (БИА), Војнобезбедносна агенција (ВБА), царинске, пореске или друге службе или други државни орган, односно правно лице које на основу закона врши јавна овлашћења. По завршетку рачунарског претраживања података државни орган, односно правно лице из става 1. овог члана доставља судији за претходни поступак извештај који садржи: податке о времену почетка и завршетка рачунарског претраживања података, податке који су претражени и обрађени, податке о службеном лицу које је спровело посебну доказну радњу, опис примењених техничких средстава,

податке о обухваћеним лицима и резултатима примењеног рачунарског претраживања података. Судија за претходни поступак ће извештај из става 2. овог члана доставити јавном тужиоцу (чл. 180)" (Законик о кривичном поступку, 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 и 35/2019: чл. 178-180).

3.5. Институционални оквир супротстављања високотехнолошком криминалу у Републици Србији

Правни оквир државних органа надлежних за борбу против ВТК уређен је Законом о организацији и надлежности државних органа за борбу против ВТК ("Сл. гласник РС", бр. 61/2005 и 104/2009). Овим законом је уређено образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела ВТК. „Више јавно тужилаштво у Београду надлежно је за поступање по кривичним делима ВТК за територију Републике Србије. У Вишем јавном тужилаштву у Београду образује се посебно одељење за борбу против високотехнолошког криминала, које чини посебни тужилац за ВТК, заменици тужиоца, портпарол, секретар тужилаштва и остало тужилачко особље (у даљем тексту: Посебно тужилаштво). Ако овим законом није другачије одређено, на Посебно тужилаштво примењују се одредбе закона којим се уређује јавно тужилаштво" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09: чл. 4).

„Радом Посебног тужилаштва руководи посебни тужилац за високотехнолошки криминал (у даљем тексту: Посебни тужилац). Посебног тужиоца поставља Републички јавни тужилац из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља. Предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија. Посебни тужилац поставља се на четири године и може бити поново постављен. Републички јавни тужилац пре постављења Посебног тужиоца доноси решење о упућивању тог лица у Посебно тужилаштво. Посебног тужиоца Републички јавни тужилац може разрешити и пре истека времена на које је постављен. По престанку функције Посебни тужилац враћа се на функцију коју је вршио пре постављења. Посебни тужилац има права и дужности као јавни тужилац. Кад дође до сазнања да се у једном кривичном предмету ради о

случајевима предвиђеним у члану 3. овог закона, Посебни тужилац се у писменој форми обраћа Републичком јавном тужиоцу, захтевајући од њега да му повери или пренесе надлежност" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09: чл. 5-6). „Ради обављања послова органа унутрашњих послова у вези са кривичним делима из члана 3. овог закона, образује се у оквиру министарства надлежног за унутрашње послове служба за борбу против високотехнолошког криминала (у даљем тексту: Служба). Служба поступа по захтевима Посебног тужиоца, у складу са законом. Министар надлежан за унутрашње послове, по прибављеном мишљењу Посебног тужиоца, поставља и разрешава старешину Службе и ближе уређује њен рад, у складу са законом" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09: чл. 9)

„За поступање у предметима кривичних дела из члана 3. овог закона надлежан је Виши суд у Београду, за територију Републике Србије. За одлучивање у другом степену надлежан је Апелациони суд у Београду" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 61/05, 104/09: чл. 9). У оквиру Вишег суда у Београду за поступање по кривичним делима ВТК образовано је Одељење за борбу против ВТК. Ово одељење има одличну сарадњу са безбедносним службама Републике Србије, и са Одсеком за прикупљање и обраду дигиталних доказа, а постоји и сарадња са службама у иностранству. Судије у одељењу, на период од две године уз могућност продужења, распоређује председник Вишег суда у Београду из реда судија наведеног и других судова.

4. МЕСТО И УЛОГА МЕЂУНАРОДНИХ ПОЛИЦИЈСКИХ ОРГАНИЗАЦИЈА У СУЗБИЈАЊУ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

4.1. Интерпол

Међународна криминалистичка полицијска организација, (*Organisation internationale de police criminelle*) познатија као „ИНТЕРПОЛ", је организација која се бави међународном полицијском сарадњом. Основана је 7. септембра 1923. године у Бечу на међународном конгресу удружења криминалистичких полиција и од 1989. године седиште се налази у француском граду Лиону. Поред тога што треба да осигура и унапређује

узајамно помагање свих органа криминалистичке полиције у границама важећих закона различитих држава и у духу Универзалне Декларације о правима човека Уједињених нација из 1948. године, Интерпол треба и да успоставља и развија све институције које могу ефикасно доприносити превенцији и репресији злочина и кривичних дела из општег права.

Активност Интерпола подразумева и предузимање корака ка сузбијању компјутерског криминала. Интерпол своје активности врши у координацији са националним полицијским службама преко Бироа за сарадњу који се налазе у свакој држави чланици. „Влада Сингапура је Интерполу поклонила у септембру 2014. године савремени центар за борбу против компјутерског криминала, који је почео са радом у априлу 2015. године. Центар се налази у Сингапуру и представља посебну организациону јединицу Интерпола под називом Интерполов глобални комплекс за иновације (енг. IGCI – Interpol Global Complex for Innovation) у оквиру кога је посебно Одељење за борбу против компјутерског криминала (енг. IDCC – Interpol Digital Crime Center) и Одељење за развој (енг. CIO – Cyber Innovation and Outreach)“ (Видојковић, 2015, стр. 25-26). У рад центра укључиле су се и многе ИТ компаније које су помогле формирање центра и материјално и кадровски. Основне активности центра су да ради на јачању међународне полицијске сарадње, да пружа помоћ у вештачењима и истрагама националним полицијским службама, да прикупља и обрађује податке, процењује и упозорава националне полицијске службе на потенцијалне криминалне претње, да открива кривична дела и њихове починиоце, да ради на превенцији компјутерског криминала, да пружа помоћ у обуци полицијских службеника, и да ради на развоју нових технологија ради супростављања компјутерском криминалу. У оквиру Одељења за борбу против компјутерског криминала данонoћно раде и дежурни тимови стручњака који обавештавају националне полицијске службе о свакој могућој криминалној претњи. Од формирања центра, Интерпол је заједно за националним полицијским службама спречио много случајева хакерских напада, открио много случајева компјутерских превара и проневера, и открио доста случајева сексуалне експлоатације деце на интернету. „Захваљујући центру односно Одељењу за борбу против компјутерског криминала само на Филипинима је у 2015. години откривено више организованих криминалних група које су се бавиле дечјом порнографијом и ухапшено је преко сто особа и заплењено је преко хиљаду рачунара који су садржали експлицитни сексуални садржај“ (Interpol, 2015, p. 28).

4.2. Европол

Европол је агенција Европске уније (у даљем тексту: ЕУ) која је основана Уговором о ЕУ из Мастрихта 1992. године, и то Конвенцијом Европског Савета о Европолу. Конвенција је ступила на снагу 1. октобра 1998. године. Европол је почео са радом 1. јула 1999. године, са седиштем у Хагу, и представља специфичан вид сарадње полицијских служби држава чланица ЕУ. Видојковић сматра да је циљ формирања Европола да побољша сарадњу полицијских служби и ефикасност надлежних органа у борби са најтежим облицима криминала, који погађају две или више држава чланица. Главни задаци Европола су лакша размена информација између држава чланица, оперативна анализа, аналитичка обрада података о кривичним делима, одржавање информационог система и његов развој, обављање сложених вештачења и логистичке помоћи криминалистичким истрагама полиције (Видојковић, 2015, стр. 27). Битно је нагласити да Европол нема овлашћења за хапшење криминалаца, већ захваљујући бази података коју поседује омогућава полицијским службама да кроз специјализован информациони систем имају брз увид, размену и обраду података. Информационим системом Европола полицијске службе држава чланица су међусобно повезане, а део информационог система су и државе које имају потписане споразуме са Европолом. Базе података Европола се формирају захваљујући подацима које достављају полиције земаља ЕУ и свих трећих држава. МУП Републике Србије сарађује са Европолом од 2009. године и то на основу Закона о потврђивању споразума о оперативној и стратешкој сарадњи између Републике Србије и Европске полицијске канцеларије.

Једна од главних области деловања Европола је борба против ВТК и у ту сврху основан је Центар за борбу против ВТК – European Cybercrime Centre (EC3). Центар је у јануару 2013. године почео да ради и има задатак да помогне у заштити државних органа, привредних субјеката и грађана од ВТК у ЕУ. Главне области деловања центра су борба против организованих криминалних група, борба против дечје порнографије и сексуалне експлоатације на интернету, заштита података од крађе, и заштита виталних информационих система ЕУ. Центар пружа помоћ полицијским службама као: обавештајни и логистички центар, централна база података, центар за обуку, центар за вештачење, центар за сарадњу са невладиним сектором и привредом.

На нивоу ЕУ сваке године се због злоупотребе платних картица направи штета од више од милијарду евра, и због тога центар пажњу усмерава и на сузбијању злоупотреба платних картица. „Најпознатија акција Европола била је „Плави ћилибар“ (енг. Blue Amber), у којој је учествовало преко педесет полицијских служби. У овој операцији је ухапшено преко 130 лица која су у вишегодишњем периоду, злоупотребом платних картица куповала и препродавала авио карте преко интернета и на тај начин оштетила 38 авио компанија и стекла противправну добит у износу преко милијарду евра“ (Ashford, 2015).

Као део Европола, центар је учинио доста и у борби против дечје порнографије и до сада је захваљујући центру разбијено више криминалних група и ухапшено на стотине педофила. „Пример једне у низу успешних акција центра је када је у сарадњи са америчком федералном полицијом и румунском полицијом у фебруару 2015. године, центар спасао двогодишњу бебу из Румуније коју је њен отац злостављао и слике и видео записе злостављања постављао и продавао на интернету“ (Europol, 2015).

Центар је заслужан и за формирање Европске финансијске коалиције за борбу против сексуалне експлоатације деце на интернету која ради под патронатом Европске Комисије. Коалицију чине представници полицијских служби као и представници невладиног сектора, привреде и истакнути појединци који се боре против злоупотребе деце и њихове експлоатације на интернету. Захваљујући центру и коалицији годишње се обради преко милион сумњивих порнографских садржаја на интернету. Центар за борбу против ВТК бави се и обавештајним активностима, тако да у оквиру центра ради и тим специјализован за прикупљање информација на интернету, њихову анализу и препознавање потенцијалних претњи по безбедност ЕУ. „По дигиталној агенди Европске Комисије за ЕУ за 2020. годину информациона технологија је кључ привредног развоја и безбедност на интернету је један од приоритета обезбеђивања тог развоја“ (European Commission, 2015, p. 5). Центар у циљу спровођења агенде интензивно сарађује са компјутерским тимом за реаговање у хитним ситуацијама (енг. CERT – Computer Emergency Response Team) који представља службу ЕУ задужену за безбедност органа ЕУ од претњи које долазе са интернета.

5. ПРЕВЕНЦИЈА, ЗАШТИТА И СУЗБИЈАЊЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ

5.1. Стратешке концепције, опредељења и препоруке

Поједини аутори, попут Мирковића, сматрају да „супротстављање ВТК обухвата два механизма: превентивно и репресивно деловање, одвраћање од злоупотребе компјутера и стварање услова за брзо откривање и доказивање у случајевима када је злоупотреба извршена“ (Мирковић, 2017, стр. 98). Бошковић и Ивановић сматрају да су за „супротстављање ВТК значајне регионалне међувладине организације, као што је нпр. Организација за европску безбедност и сарадњу – ОЕБС, у оквиру које је оформљена радна група за безбедност информација и приватност“ (Бошковић и Ивановић, 2012, стр. 80).

Препоруке Савета министара Европског савета су посебно важне за изградњу превентивног система заштите од компјутерског криминала. У препорукама се наводи да је веома битно бити информатички образован и проширити своје знање из информатике, како бисмо смањили број кривичних дела ВТК на најмању могућу меру. У препорукама се предлаже да се предузму правне мере спречавања и заштите од ВТК.

„Стратегија развоја информационог друштва у Републици Србији до 2020. године (у даљем тексту: Стратегија) јесте акт Владе којим се на целовит начин дефинишу основни циљеви, начела и приоритети развоја информационог друштва и утврђују активности које треба предузети у периоду који обухвата ова стратегија. Циљ је да Република Србија до 2020. године по показатељима развијености информационог друштва достигне просек ЕУ“ (Стратегија развоја информационог друштва у Републици Србији до 2020. године, 51/10). „Општи циљ Стратегије развоја информационе безбедности у Републици Србији до 2020. године (у даљем тексту: Стратегија) је развој и унапређење информационе безбедности у Републици Србији и њено одржавање на адекватном нивоу, а с обзиром да су доношењем прописа у овој области дефинисани ИКТ системи од посебног значаја, мере заштите, надлежни органи, изазов за остварење циља налази се у стварању предуслова за континуирано унапређење кадрова, како кроз увођење посебних програма на универзитетима из области информационе безбедности, тако и кроз континуирано обучавање и усавршавање запослених у релевантним институцијама који се баве информационом безбедношћу. Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са

употребом информационо-комуникационих технологија, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца. Република Србија је препознала информациону безбедност као једну од шест приоритетних области развоја информационог друштва и предузела кораке у циљу успостављања свеобухватног оквира информационе безбедности. У складу са тим, Стратегија развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС", број 51/10) предвиђа да развој и унапређење информационе безбедности треба постићи кроз унапређење правног и институционалног оквира, заштиту критичне информационе инфраструктуре, борбу против високотехнолошког криминала и научно-истраживачки рад" (Стратегија развоја информационе безбедности у Републици Србији до 2020. године, 53/17).

5.2. Физичко-технички аспект заштите

Да бисмо успешно реализовали заштиту од ВТК и сузбијање ВТК, прво требамо подићи колективну свест грађана о свим опасностима и последицама до којих може довести ВТК. У остварењу овог циља најзначајнију улогу имају образовне институције кроз константне едукације и семинаре као и сами медији путем објективног и непристрасног извештавања.

Мандић, Путник и Милошевић сматрају да формулисање техничког аспекта заштите у оквиру безбедносне политике подразумева активности на осмишљавању и имплементацији система заснованог на средствима логичке заштите опреме (антивирусни програми, фајервол системи и др.), средствима техничке заштите опреме (противпожарни апарати, детектори дима, мерачи температуре и др.) и средствима забране, односно контроле приступа штићеном простору (механичке браве, временске браве, магнетне картице и др.) (Мандић и сар., 2017, стр. 206).

Физичко-техничка заштита се спроводи контролом приступа, коју спроводи служба физичког обезбеђења и сви запослени, затим применом техничких средстава заштите и на крају унапред дефинисаним процедурама, које прецизно одређују мере, поступке и обавезе свих запослених у спровођењу ове заштите (Мандић, 2015, стр. 241).

Поједини аутори, попут Мандића, Путника и Милошевића, сматрају да су за процес непосредног функционисања физичко-техничке заштите одговорни интерни субјекти заштите који кроз своје свакодневне радне активности спроводе и део послова који се односи на физичко-техничку

заштиту информација. Физичко-техничка заштита се односи на опрему, мере и поступке којима се спречавају или одвраћају неовлашћена лица да физички приступе пословном простору, односно местима и опреми на којој се користе, обрађују, складиште и чувају информације, као и самим информацијама, без обзира да ли су у електронском или папирном облику. Под физичким приступом подразумева се и лични приступ, као и удаљени приступ коришћењем електронских комуникација (Мандић и сар., 2017, стр. 346).

За ефикасно сузбијање ВТК битно је на време пријавити сваки облик злоупотребе и онлајн напада на приватност лица како би надлежни органи благовремено деловали. Нажалост, иако је од изузетног значаја благовремена пријава жртве и делотворна сарадња са надлежним органима у току поступка, у случају кривичних дела ВТК у великим корпорацијама, широко је распрострањена пракса интерног решавања. Мирковић сматра да су неки од разлога: могућност да се губици од компјутерског криминала пренесу са жртве на купца умањује интерес за његово пријављивање; већина жели да одржава низак ниво информисаности о томе шта се код њих дешава, због могућих потенцијалних проблема који могу настати пријављивањем криминалног дела; страх руководства од покретања питања и њихове одговорности због пропуста у предузимању одговарајућих мера заштите, што би могло спречити њихов професионални опстанак и напредовање унутар организације; компјутерски криминалац, чак и ако је осуђен, често добија условну казну, па ниска казна дестимулише жртву да дело пријављује. Због наведених разлога корпорације најчешће прибегавају дискретном премештају извршиоца дела на друго радно место или давању отказа (Мирковић, 2017).

5.3. Логички аспект заштите

Мандић, Путник и Милошевић тврде да сфере логичке, техничке и физичке заштите „представљају прву линију одбране информационих система. Сфере логичке, техничке и физичке заштите уобичајено се називају техничким аспектом заштите. Овај, односно ови аспекти заштите, подразумевају коришћење мера које имају за циљ регулисање начина и техничких поступака којима се може умањити ризик од злонамерног нарушавања функционалности информационих система. У циљу спречавања приступа штићеном систем, у употреби су различити

технички уређаји и средства, али и разноврсни информатички алати“ (Мандић и сар., 2017, стр. 200-206).

Поједини аутори сматрају да је у погледу спречавања појаве ВТК од стране појединачног корисника компјутера, осталих компјутерских уређаја и интернета, могуће издвојити неколико начина спречавања појаве ВТК:

– Увек укључен заштитни програм на компјутеру штити компјутер од покушаја извршилаца дела компјутерског криминала да приступе компјутерском систему, оштете или чак избришу важне податке.

– Инсталиран и редовно ажуриран антивирусни програм спречава продирање компјутерског вируса у компјутерски систем корисника.

– Неки од садржаја на интернету осмишљени су и направљени тако да могу да заобиђу и најсавременију антивирусну заштиту. Електронска пошта која је приспела од непознатих особа не би се требало отварати.

– Опрезност приликом коришћења бесплатног бежичног интернета на јавним местима, посебно приликом коришћења услуга електронског банкарства и провере електронске поште.

– Пажљив одабир лозинки које служе да ограниче приступ компјутерским ресурсима.

– Складиштење важних података на одговарајућим уређајима у случају неовлашћеног брисања истих са централног компјутерског система. Постојање неколико примерака копија важних података на више различитих уређаја додатно обезбеђује њихово очување. Као најпоузданији уређаји издвајају се екстерни хард дискови најновије генерације (Мирковић, 2017).

5.4. Међународна сарадња на сузбијању високотехнолошког криминала у Републици Србији

Оно што несумњиво произилази из карактеристика ове врсте криминала јесте неопходност међународног повезивања државних органа у целом свету који се баве откривањем и кривичним прогоном извршилаца кривичних дела ВТК. Прво на шта асоцира појам међународне помоћи јесте институт кривичног процесног права, а то је међународна правна помоћ. Међутим, овај институт је спор и папиролошки захтеван тако да у већини случајева доводи до одустанка од прикупљања доказа. Стога, потенцира се непосредан контакт између државних агенција у циљу што брже размене информација. Основни циљ је фиксирање доказа, како би се

пружила могућност, и оно што је најбитније, време, како би се покренуо званични поступак међународне правне помоћи. Један од најефикаснијих начина да се успостави контакт са представницима других држава јесте учествовање представника тужилаштва на различитим конференцијама, како у Србији, тако и у иностранству. Београд је у марту 2007. био домаћин Регионалне конференције о ВТК, где су присуствовали представници десет земаља у окружењу. „Представници Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ) су учествовали на конференцији под називом Повежи се сигурно. Ова конференција је одржана од 20. до 21. септембра 2018. године у Београду, у организацији МУП Републике Србије. Конференцију је отворио потпредседник Владе и министар унутрашњих послова др Небојша Стефановић. Поред домаћина конференцији су присуствовали и представници ОЕБС-а, Европола, Федералног истражног Бироа (ФБИ), Савета Европе, Европске Агенције за безбедност мрежа и података (ENISA), Форума безбедносних тимова за одговоре на инциденте (FIRST), затим представници националних CERT-ова из земаља региона, компаније Huawei, Центра за демократску контролу оружаних снага (DCAF), Посебног тужилаштва за ВТК, Канцеларије за информационе технологије и е-управу и осталих институција које се у нашој земљи баве информационом безбедношћу. Теме конференције су биле борба против ВТК и безбедност информационих система као стратешки приоритети, али и неопходност размене информација и искустава у циљу континуираног унапређења знања и вештина за борбу против ВТК и одбрану од напада на информационо-комуникационе системе. Гости на званичном отварању конференције су били и европски комесар за унутрашња питања и миграције Димитрис Аврамопулос, затим министар унутрашњих послова Републике Турске Сулејман Сојлу, министар унутрашњих послова Мађарске Шандор Пинтер, министар унутрашњих послова Црне Горе Мевлудин Нухоцић и министар унутрашњих послова Македоније Оливер Спасовски" (РАТЕЛ, 2018).

Другог дана конференције о ВТК и информационој безбедности под називом „Повежи се сигурно!", тачније 21. септембра 2018. године, одржана је сесија у којој су представљени примери успешних међународних операција у борби против ВТК. Виши стратешки аналитичар у Европском центру за ВТК (Европол), Никол ван дер Мејлен, рекла је да је са Србијом 2014. године потписан оперативни уговор и сарадња српског Одељења за борбу против ВТК и Европола је до сада на

задовољавајућем нивоу. Мејлен је нагласила да је задатак Европола, који сарађује и са 14 чланица Европске уније, да јача операције које воде државе чланице ЕУ и да је њихово деловање подељено у три главна дела која се баве сајбер криминалом, картицама и е-плаћањима, као и онлајн порнографијом. Такође, почетком маја 2018. године оформљен је тим за мрачни веб који је у почетној фази, а поред тога Европол има велики број форензичних стручњака, који помажу у операцијама. „Мејлен је изјавила да Европол покушава да има вишестрани приступ проблему сајбер криминала, те тако имају и академску саветодавну мрежу. Нагласила је да су 2014. имали само три операције, а од тада расте број операција које су подржали. Мејлен је нагласила да број ренсомвер напада стално расте, преваре са картицама и скидање средстава са њих, као и криптовалуте које су постале мета сајбер напада, хакују се новчаници, а криминалци користе криптовалуте за трансакције. Такође је рекла да раде на актуелизацији података, као и на њиховој енкрипцији, и сматра да би ти подаци које прикупљају могли да побољшају законодавне оквире. Нагласила је да је циљ Европола да створе кампању за подизање свести шире публике о сајбер нападима" (Печић, 2018).

Владимир Вујић из Одељења за борбу против ВТК МУП Републике Србије ушао је у детаље операције Power OFF, о којој ће бити речи у студији случаја Webstresser. Управо ова операција је била обарање једног од највећих сервиса за дистрибуцију DDoS напада у читавом свету.

Агент ФБИ, Питер Травен, који ради од 2005. године искључиво на питањима сајбер криминала на позицији је легал аташеа и смештен је у Букурешту. Травен сматра да је сарадња са приватним сектором битна, као и да су сајбер напади можда и значајнији од физичких с обзиром да су нападачи углавном скривени. Травен је рекао да је криминал сада глобализован. Нагласио је да сајбер криминалци имају више времена и средстава, из чега произилазе увек нове врсте криминала, па представници власти и органа реда морају стално да се удружени боре како би превазишли њихову почетну предност. Травен је нагласио да ФБИ нема буџет за представнике у свакој земљи, али имају 64 амбасаде где имају представнике, те и у Србији имају свог амбасадора. Имају референтне тачке где имају око четири човека који покривају све захтеве које има ФБИ за ту земљу. У последњих четири до пет година захтеви који стижу из Америке су везани за сајбер криминал. Када је реч о дељењу података и размени информација, Травен је био мишљења да ФБИ то ради добро, јер је размена обавештајних података кључна. ФБИ поседује

Центар за притужбе где грађани пријављују да су жртве одређених сајбер напада и те информације се даље деле. Нагласио је да је тешко носити се са ситуацијама где се рецимо користи српска инфраструктура да би се напала румунска банка, а да је решење јача међусобна повезаност. Рекао је да треба да радимо заједно, а то можемо кроз неформалне канале, а наравно када треба и званично (Печић, 2018).

Сваке године у Стразбуру, под покровитељством Савета Европе, одржава се конференција на којој се из године у годину повећава број учесника из различитих земаља. Тај податак је одличан показатељ пораста свести у великом броју земаља у циљу што ефикасније борбе против ВТК. „На конференцији посебна пажња се посвећује проблему контакт тачке 24/7 и њеном функционисању у различитим земљама. Учествовање на конференцији је одлична прилика за размену и расправљање о проблемима који настају у току кривичног поступка. Кад разматрамо питање међународне сарадње, она може да се посматра кроз однос са државним институцијама страних држава или кроз сарадњу са тзв. невладиним сектором, а ту пре свега мислимо на велике међународне компаније као што је Мајкрософт. Последњих неколико година све више се истиче значај партнерства између државе и привредних субјеката. Тужилаштво за ВТК остварило је сарадњу и на нивоу државних органа, као и на релацији држава–привреда“ (Комлен Николић и сар., 2010, стр. 248-249).

Република Србија има одличну сарадњу са представницима амбасада САД, Француске и Велике Британије у Београду. Тужилаштво има установљен партнерски однос са жандармеријом Републике Француске, која је од јануара 2009. године у саставу Француског министарства унутрашњих послова. На тужилачком нивоу успостављена је сарадња са Енглеским краљевским тужилаштвом. Сарадња са привредом одвија се преко америчке привредне коморе, чија се канцеларија налази у Београду, као и са канцеларијом Мајкрософта. Одлична сарадња успостављена је са Саветом Европе, кроз пројекат за борбу против економског криминала у Републици Србији, чија је основна тема била економски криминал, са две подгрупе питања: прањем новца и ВТК. Имајући у виду намеру Републике Србије да постане део ЕУ, тужилаштво је у контактима са мисијом ОЕБС у Републици Србији, као и са Европском комисијом.

5.5. Тенденције кретања високотехнолошког криминала у Републици Србији

Према подацима интернет светске статистике, број корисника интернет услуга у свету 30. септембра 2020. године износио је 4.929.926.187 од укупне светске популације. Интернет у Републици Србији један је од најпопуларнијих система масовне комуникације. У Републици Србији према подацима интернет светске статистике број корисника интернет услуга закључно са 30. септембром 2020. године износи 6.406.827 од укупне популације.

Овакав развој може друштву да пружи велике могућности као што су сви модерни процеси пословања попут електронског банкарства, електронске трговине, интернет телефонирања, итд. Међутим, овакав развој и прелазак друштва из индустријске у информациону еру са собом носи и велику претњу друштвеном и економском животу, јер данашња модерна друштва умногоме зависе од расположивости информационих технологија, нарочито њене инфраструктуре.

Већ сада са сигурношћу може да се закључи да је највећа светска глобална мрежа, *интернет*, постала уточиште криминала, те да је ВТК профитабилна незаконита активност у којој учествују структуриране организоване групе, чак и појединци који се никад нису срели уживо, али који сарађују преко интернета. Оно што је сигурно јесте да Република Србија у корак прати светске трендове у области ВТК, те да ћемо у блиској будућности бити сведоци извршења све већег броја кривичних дела из области ВТК.

Неки од разлога због којих ће се ВТК повећавати у будућности су:

- технологија за извршење дела ВТК је постала приступачна свима и потребни алати за извршење криминалних активности су доступни широком спектру људи, а не само информатичким стручњацима, и

- „у неразвијеним регионима света број корисника интернета је у сталном порасту, а број потенцијалних богатих жртава у развијеним регионима је углавном непроменљив, што ће изазвати повећан број напада на њих, када ће сваки нови преступник имати могућности да експоненцијално повећа број напада кроз све већу аутоматизацију коју омогућавају алати и интернет“ (UNODC, 2010, pp. 203-204).

У будућности, све ћемо чешће виђати рансомвер нападе. Управо ови напади биће усмерени на финансијске институције, велике компаније, итд., а процењује се да ће нападнути имати огромне губитке. Број фамилија рансомвера се сваке године повећава. Посебно су опасни рансомвер напади на болнице. Током пандемије корона вируса, било је пар случајева рансомвер напада на болнице. Напади на болнице јављају се услед коришћења повезаних уређаја и система у здравству, а исти су углавном минимално заштићени. Нападачи приликом рансомвер напада на болнице имају приступ великом броју личних података, и управо узимају те податке и закључавају им рачунаре у болницама и самим тим онемогућавају запосленима приступ подацима који су им неопходни. У оваквим ситуацијама мора се брзо реаговати, јер су лекарима и медицинским радницима, посебно за време пандемије корона вируса, неопходни подаци о пацијентима, дијагнозе пацијената, резултати тестова на корона вирус итд. Једини начин да се поново добије приступ рачунарима је да се плати откупнина, и то у крипто валутама, што се мора и урадити, јер нема времена да се ухвате и лоцирају починиоци, а поготово нема времена да појединци ИТ стручњаци покушају сами да реше рансомвер напад, поврате податке и омогуће поновни приступ рачунарима. Подаци о пацијентима у болницама неопходни су у сваком тренутку и управо то је разлог због ког имамо све више случајева рансомвер напада на болнице, јер криминалци нападима на болнице имају загарантовану и брзу зараду. Рансомвер напади ће се и даље убрзано развијати, и биће их све више и биће све чешћи. Очекује се све више инцидената везаних за нападе рансомвером са циљем енкрипције података као и блокирања медицинских уређаја и опреме. Медицинска опрема је често скупа, а понекад и животно потребна, што је чини главном метом напада и изнуђивања. У примени рансомвер напада је укључено више организованих криминалних група и повећаће се коришћење инсајдера у изабраним компанијама и државним институцијама.

На основу истраживања Републичког завода за статистику (у даљем тексту: РЗС), употреба информационо-комуникационих технологија и интернета на територији Републике Србије у сталном је порасту на нивоу државних институција, привреде, домаћинстава и појединаца. „У Републици Србији 81% домаћинстава поседује интернет прикључак, што чини повећање од 0,9% у односу на 2019. годину. Заступљеност рачунара у домаћинствима је 74,3%, што представља повећање од 1,2% у односу на 2019. годину. Што се тиче интернет конекције – 90,5% корисника

интернета користи фиксну широкопојасну интернет конекцију и то је најзаступљенији тип конекције, мобилну широкопојасну интернет конекцију има 71,9% домаћинстава. Широкопојасну интернет конекцију поседује 80,8% домаћинстава у Републици Србији. У последњих неколико месеци компјутер је користило 72,4% лица, што чини повећање од 0,5% у односу на 2019. годину. Истраживање је показало да је интернет користило 78,4% лица, док га 17,4% лица никада није користило. Преко 3 750 000 лица користи интернет сваког или скоро сваког другог дана. За потребе пословања, интернет користи 100% предузећа, док веб-сајт поседује њих 84,4%. Током 2019. године 27,9% предузећа продавало је производе/услуге путем интернета. 98,4% предузећа користи широкопојасну интернет конекцију, 82,8% малих предузећа поседује веб-сајт, и 18,6% предузећа користе клауд" (RZS, 2020).

ВТК у Републици Србији према броју пријава у Републичком јавном тужилаштву (у даљем тексту: РЈТ) у сталном је порасту. У складу са Конвенцијом о ВТК предузете су мере ради побољшања ефеката борбе против ВТК. Посебна одељења за борбу против ВТК формирана су 2006. године у оквиру РЈТ, МУП и Вишег суда у Београду. У посебном одељењу РЈТ – Посебном тужилаштву за борбу против ВТК од њеног оснивања до данас, број уписаних предмета у току године је у сталном порасту. Само у 2020. години број уписаних предмета од почетка године до данас износи већ преко 2.500 предмета. Највећи број пријава које се подносе су управо пријаве за неовлашћени приступ рачунарским мрежама и за преваре.

5.6. Едукација у превенцији високотехнолошког криминала

У 2020. години велики пораст криминалних дела ВТК забележен је у рансомвер нападима, јер управо ови напади доносе веома лаку и малтене сигурну зараду криминалцима, при томе да они остају анонимни и не буду лоцирани. Митић сматра да би се спречио рансомвер напад, систем мора увек да има најновије закрпе (исправке пропуста у систем), јер по обичају вируси искоришћавају те безбедоносне пропусте у систему, исти је случај и код рансомвер напада. Још 2017. године, када се појавио први рансомвер напад - WannaCry, Мајкрософт је закрпио чак и оне системе којима је званично истекла подршка годинама пре, зато јер је постојала претња да стану битне институције попут болница или аеродрома (Митић, 2020). Након тога, 2018. године појавио се нови пропуст погодан за рансомвер програме и тада се такође појавио још један patch који је такође понуђен власницима застарелих система без званичне подршке, тако да су

стварно сви имали довољно времена да се спреме. То би требало да буде познато особи која се бави одржавањем система, међутим све закрпе и ажурирања не вреде пуно уколико корисници нису едуковани у смислу сајбер сигурности и упознати са сигурносним протоколима као и да адекватно реагују на сумњиве мејлове и ситуације. За све такве ситуације треба да постоји интерна процедура коју прописује ИТ администратор или фирма која је задужена за безбедност институције или предузећа. Митић сматра да је свака заштита непотпуна, уколико корисници система нису прошли макар основну едукацију по питању сигурности која би минимално требало да садржи теме као што су правилан избор и употреба лозинки, размена лозинки на сигуран начин, као и чување истих. Затим у тој едукацији би требало да се упознају са сигурним приступањем сервисима и ауторификационим формама, да знају да препознају лажне од правих, а посебан део едукације треба да буде сигуран приступ и сигурност на друштвеним мрежама. Имејл је по обичају најкоришћенији алат хакера за убацивање вируса и злонамерних програма, а у скорије време чешћи примери су злоупотреба идентитета имејл порука у сврху наплаћивања лажних фактура. То је што се тиче обуке крајњих корисника основа (Митић, 2020).

Други ниво едукације би укључивао ИТ подршку у фирмама и државним институцијама која би требало да води рачуна о томе да су системи увек закрпљени са последњим закрпама као и да воде рачуна о бекапу, као и начину његовог складиштења, јер бекап не вреди ништа уколико се и оригинал и бекап копија нпр. базе налазе на истом хард диску, чак и у истој просторији или у истој згради. Митић сматра да је једини сигуран бекап када резервну копију података и базе имате „off-site" или на удаљеној локацији. Многи се у данашње време одлучују за опцију складиштења бекапа онлајн или у клауду што је мање сигурна опција. У том случају такви подаци морају бити енкриптовани пре слања. Међутим, добра сигурносна пракса је да се битни подаци, посебно лични, уколико није неопходно не држе онлајн (Митић, 2020).

Не треба заборавити да било који злонамерни софтвер, укључујући и уцењивачки, можемо зарадити на много начина. Зато не треба да скидамо сумњиве фајлове са интернета, не треба да отварамо насумично линкове, треба да користимо стандардни кориснички налог уместо администраторског, не треба да експериментишемо на систему и увек треба да правимо и имамо резервне копије важних фајлова. „Једног дана, из било ког разлога, нешто лоше ће се десити нашем компјутеру. Тога дана

ћемо или имати резервну копију, или га нећемо имати. Од нас зависи" (Систем Нови Сад, 2020).

6. СТУДИЈА СЛУЧАЈА „WEBSTRESSER"

Webstresser важио је за највећу платформу која је нудила клијентима – од којих су неки ухапшени у Холандији, Италији, Шпанији, Хрватској, Аустралији, Великој Британији и Хонг Конгу – да у замену за новчану накнаду, која је почињала од 15 евра и кретала се до 999 евра, изврше DDoS напад на одређени веб-сајт или платформу и тако их учине недоступном корисницима. „Сам домен webstresser.org регистрован је у Панами, која је изабрана јер су закони такви да држава не надзире интернет, а домен је изгледао као да су га направили прави професионалци. Његов изглед презентован је на конференцији, где су се могле видети цене које су администратори нудили корисницима за своје услуге, затим пакети вишемесечних услуга, а хакери су чак ишли и до те границе да корисницима нуде попуст од 15 одсто уколико плате криптовалутама. Поносно су се хвалили и статистиком успешних напада" (Бркић, 2018).

„Сајтом webstresser.org управљао је хрватски држављанин Кристиан Р. из Запрешића, крај Загреба, и означен је као власник овог сајта. Ухапшен је у међународној полицијској акцији, и приведен је на Жупанијски суд у Великој Горици 24. априла 2018. године. Како се наводи у саопштењу суда, осумњичени се терети да је починио тешко кривично дело против рачунарских система, програма и података. Према оптужници, Кристиан је од неутврђеног дана 2015. године до 24. априла 2018. године, из породичне куће у Запрешићу, управљао рачунарским системом доступним на интернет адресама webstresser.co и webstresser.org. Кристиан је прибавио противправну имовинску корист у износу од најмање 163,75124693 биткоина. Један је од четири администратора илегалног интернет сервиса за сајбер нападе webstresser.org, а ухапшен је у склопу оперативне акције кодног имена „Мануфактура". Једна комшиница, испричала је да је он још у основној школи хаковао систем једне банке због чега је као малолетник био и осуђен. Како је испричала, био је веома надарен за информатику, али због лоших оцена није могао да се упише у информатичку школу коју је желео да упише" (Телеграф, 2018).

DDoS напад (*Distributed Denial of service*) је врста напада у коме огроман број координисаних уређаја "циља" одређену мету чија инфраструктура не може да поднесе тај саобраћај па престаје са нормалним радом. DDoS напади функционишу тако што усмере огромну количину интернет саобраћаја на жељене интернет странце, чиме их успоре до тачке неупотребљивости или оборе са мреже. Webstresser је, према наводима Европола, функционисао као „сервис за унајмљивање“ који је за клијента обављао овај посао. У разговору за VICE, Андреј Петровски, сајбер форензичар из Share Conference, каже да је „проблем са DDoS нападима то што су примитивни у својој природи јер DDoS не експлоатише недостатак, него регуларно функционисање интернета. То значи да ће серверу бити упућен огроман број захтева и он ће бити "запослен" до те мере да неће моћи да функционише, а кад је DDoS у питању, то значи да се захтеви шаљу синхронизовано из више извора, ради амплификације, односно јачег ефекта“ (Бошковић, 2018).

Путник наводи пример DDoS напада који се десио 27. априла 2007. године био је усмерен на опструкцију званичних интернет сајтова Естоније. Неколико недеља је трајао овај напад. Сајтови естонске владе, министарства иностраних послова и министарства правде, медија и банака били су блокирани услед напада за који су окривљени руски хакери. Естонски министар одбране захтевао је примену члана 5. НАТО-а, који предвиђа колективну одбрану нападнуте земље (Путник, 2009). Као што смо могли видети на примеру Естоније може се закључити да последице ове врсте напада нису безначајне и да је ова врста напада веома озбиљна претња што можемо видети и у примеру Webstresser.

„У операцији **„Power OFF“** 24. априла 2018. године, обустављен је рад **webstresser.org**, а администратори тог сервиса су приведени. Међу њима, поред држављана Велике Британије, Канаде и Хрватске, била су и два држављанина Републике Србије. Како је саопштено из МУП-а Републике Србије, дводневна акција хапшења извршилаца овог кривичног дела започета је у Србији. Ухапшени су М. Ј. (19) из Прокупља и Д. В. (21) из Руме, због сумње да су били администратори Webstresser-а, док је платформом управљао њихов вршњак из Хрватске“ (Бошковић, 2018). Приликом претресања стана једног осумњиченог пронађен је компјутер који је био укључен и ту су видели како је изгледао Webstresser пре пар година, што значи да је он радио и дизајн те странице, пронађене су листе IP адреса које су служиле за DDoS нападе. Одузете су и крипто валуте. На сајту су откривена и корисничка имена која су осумњичени из Србије

користили и која је била њихова улога. Први је имао корисничка имена „m1rk" и „m1rk000oogdf" као и „Мирковик Бабс" под којим је и имао Фејсбук страницу. Испод последње његове објаве на тој страници пре акције „Power OFF", људи су остављали коментаре „RIP" док и сама Фејсбук страница није укинута. Он је био главна техничка особа када је у питању организација и функционисање сервиса. Поједини домаћи медији, представили су Мирковића као неког ко је у родном граду важио „за Сноудена из Прокупља" који је имао „кликер за технику". Међутим, иако се увек развија велика фама о сајбер нападима, DDoS напади нису претерано софистицирани и није потребно велико техничко знање за њихово извршење. Други осумњичени користио је корисничко име „Vule Graphic" и био је главна особа за плаћање путем PayPal-a. Хапшењем тинејџера који су били чланови у хакерској групи и откривањем крипто валута које су зарадили нападима на странице, први пут у Србији једна државна институција одузела је крипто валуте. Од једног осумњиченог одузето је 1,87 биткоина у вредности од око 15.000 долара и замрзнуто је 10.000 долара средстава осумњичених које су користили путем PayPal-a. „Штаб за команду и координацију дводневне акције био је постављен у седишту Европола, а акција је почела у Србији хапшењем М.Ј. и Д.В. Након тога, на већем броју локација широм света ухапшени су и остали администратори и чланови овог криминалног сервиса, док су сервери преко којих су изводили нападе преузети од стране полиције. Поменути сервис је затим оборен и угашен и његова серверска инсфраструктура је заплењена од стране полиција Немачке, САД и Холандије" (Николић, 2018).

У првој половини ове деценије, ако сте желели да учествујете у DDoS нападу, било је потребно само да преузмете мали програм чијим инсталирањем ваш компјутер постаје део мреже која напада одређену мету. Временом, начини DDoS напада су се мењали, сам Webstresser вам је, пре укидања, омогућавао да уместо да организујете огромну групу истомишљеника, једноставно само платите да бисте извршили DDoS напад. Међутим, како Петровски каже, начини одбране су постајали бољи, тако да је ово хапшење и затварање сајта готово „ретро". Наравно постоје технике и алати да се смањи могућност од DDoS напада, као што су конфигурисање перзистентних конекција или блокирање одређене IP адресе уколико она пошаље одређени број захтева серверу, или сервиси као cloudflare, који имају дистрибуирану мрежу кроз коју амортизују утицај DDoS напада. Иако су двојица приведених из Србије, медији су

пренели да ниједна мета није била на територији наше земље. „Оно што се јако често спомиње као разлог због чега до сада нисмо били мета неког већег напада, јесте чињеница да вероватно напад на државне институције у Србији која није геополитичка сила. DDoS је кривично дело рачунарска саботажа. Према члану 186б Кривичног Законика Републике Србије, предвиђена казна за то дело је од једне до осам година затвора“ (Бошковић, 2018).

Како пише BBC, webstresser.org је одговоран за напад на седам највећих банака у Великој Британији из новембра 2017. године. Иако никада званично признат, напад је банке коштао више стотина хиљада фунти, преноси BBC. Извор из Интерпола рекао је магазину Форбс да је највећи број напада са овог сајта и изведен и наручен у САД. „Џо Годел, главни истраживач британске националне агенције за криминал (енг. NCA – National Crime Agency), за BBC је изјавио да је сајбер криминал по дефиницији претња која надилази границе појединих држава. Хапшења која су извршена показала су да интернет не пружа стопроцентну анонимност онима који крше закон и ми очекујемо да у наредним недељама и месецима идентификујемо и остале осумњичене који се повезују са овим сајтом, казао је Годел“(B. J., 2018).

7. СТУДИЈА СЛУЧАЈА „РЕНСОМВЕР“

Занимљива је дефиниција Владимира Митића, по којој „ренсомвер напад чине злонамерни програм, малвер (енг. malware), који енкриптује податке жртве, и нападач, који касније тим жртвама тражи својеврсну откупнину за њихово откључавање (ransom - откупнина)” (Митић, 2020). Жртва нема више приступ подацима док не плати откупнину од хакера или док не врати бекап (резервну копију података), што може потрајати и данима, у зависности од комплексности система и количине података. Откупнина се плаћа криптовалутама, најчешће биткоином, јер се такве трансакције не могу пратити, и жртва не зна коме је отишао новац. Наравно да проблем настаје када жртва нема бекап, па је приморана да хакерима плати тражену суму. Након уплате хакерима, жртва добија кључ којим откључава (декриптује) своје податке и опет им има приступ. Делује као сцена из филма, али ово је већ пар година реалност са којом се сусрећемо све чешће. Ово се наравно лако може избећи коришћењем прописних сигурносних протокола и мера заштите, а такође увек треба да постоји бекап. Штета ће увек постојати чак и у случају да жртва има бекап, јер

поновно успостављање система од нуле захтева доста времена, а за то време су недоступни сервиси које жртва пружа.

Бојан Перков сматра да постоји много начина, чак и веома софистицираних, да неко зарази ваш уређај малициозним софтвером који ради као ренсомвер. Ренсомвер можете „закачити" преко линкова или прилога у мејловима, заражених флеш меморија, тако што је „спакован" у оквиру софтвера који сте инсталирали или рецимо путем недовољно безбедних веб страница. „Мајкрософт истиче најчешће две врсте ренсомвера: оне који закључавају екране (енг. lockscreen) и енкрипцијске (енг. encryption). Код верзија које закључавају екране се прикаже екран који вам не дозвољава да приступите фајловима и садржи поруку са упутствима за плаћање откупа, док енкрипцијски ренсомвер мења постојеће фајлове тако да не можете да их покренете јер су заштићени шифром коју је нападач поставио (Перков, 2017).

Државе са највећим бројем регистрованих ренсомвер напада, према извештају компаније „Malwarebytes", су: САД, Италија, Немачка, Велика Британија и Француска. Аутори Malwarebytes извештаја такође наводе да је међу корпоративним метама највише оних са седиштем у Северној Америци, док се напади на потрошаче и кућне рачунарске системе чешће дешавају у Европи. Међутим, Перков тврди да смо могли да се уверимо да ренсомвер, у офанзивном и дефанзивном смислу, није заобишао ни Србију. У јануару 2017. године су се у јавности појавиле информације да је најмање један грађанин Србије добио мејл од трговинског ланца Макси, са поруком о наводној наградног игри који је у прилогу садржао текстуални документ из кога се покретао ренсомвер назван Marlboro. Макси је упозорио грађане да мејл није потекао од компаније и да не отварају фајл у прилогу. Такође, почетком фебруара 2017. године откривен је први ренсомвер за који постоји веровање да долази из Србије – SerbRansom, што показује да домаћи хакери не заостају у домишљатости (Перков, 2017).

WannaCry (WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) ренсомвер је програм односно криптовирус који напада оперативне системе Мајкрософт Виндоус. Хакери, након што енкриптују податке, траже плаћање декрипције у криптовалути биткоин. Ренсомвер обично зарази рачунар након што корисник отвори фишовани мејл, а иако се сматрало да су наводно и у овом случају били коришћени овакви мејлови за инфекцију рачунара овај метод напада заправо није потврђен. Када се инсталира, WannaCry користи EternalBlue exploit, који је развила америчка Национална сигурносна агенција (енг. NSA – National Security Agency), да

би се преко локалних мрежа и удаљених хостова извршио директан напад на рачунаре који користе оперативне системе Мајкрософт.

Прошло је још мало па четири године од како је WannaCry рансомвер правио хаос у технолошком свету, а процењује се да је направио штету од око осам милијарди долара. WannaCry се свету представио 12. маја 2017. године, а сигурносни стручњаци су за кратко време утврдили разлог због којег се напади брзо шире – рањивост EternalBlue. Милан Живановић сматра да тада ситуација није била потпуно јасна, будући да су стручњаци из Мајкрософта ову рањивост санирали пре него што су почели WannaCry напади. Ипак, иако су из Мајкрософта издали званично саопштење о томе да су корисници безбедни, WannaCry напади су се догодили баш захваљујући пропусту под именом EternalBlue, преко система који нису применили закрпе. Експерти упозоравају да се последице напада осећају и данас, те да WannaCry и даље изазива проблеме, а они који плаћају тражени откуп изгледа нису упознати са чињеницом да ни они који плате не добијају натраг своје податке. Проблем указује и на то да још увек постоје корисници који нису применили закрпе против EternalBlue рањивости, што их чини рањивим не само на WannaCry кампању, већ и на друге малвер нападе (Живановић, 2020).

Оснивач и генерални директор компаније Касперски, Јуџин Касперски, верује да су сајбер напади на болнице током COVID-19 пандемије на истом нивоу као и терористички напади. Док здравствени радници широм света улажу напор како би заштитили човечанство од тренутне кризе коју је изазвао вирус корона, злочинци циљају потенцијално рањиве медицинске установе у циљу спровођења својих опасних активности. „На онлајн конференцији, одржаној 22. априла 2020. године, Јуџин Касперски, Костин Раиу – директор GReAT тима и Јури Наместников – директор GReAT тима за подручје Русије, дискутовали су о сајбер безбедносним последицама COVID-19 пандемије. Касперски је изјавио да ће, без обзира на тренутне мере социјалног дистанцирања које су уведене широм света, бити веома мало утицаја на целокупну сајбер безбедносну слику. Такође је истакао да ће сајбер криминалци највероватније остати активни. Они су навикли да раде од куће и њихове околности се нису драстично промениле. Они ће наставити са покушајима напада на предузећа и појединце и наш је посао да наставимо да радимо посвећено и да бранимо наше клијенте. Било који напад на болницу се у овим временима може посматрати као терористички напад" (персоналмаг, 2020).

Према истраживању компаније Касперски, „укупно 767.907 корисника је нападнуто од стране енкриптора у 2019. години – са готово трећином њих (30%) у предузећима. Од свих породица енкриптора, WannaCry је и даље била најчешћа – у 2019. години, напала је 164.433 корисника и чинила је 21% свих детектованих напада. Са значајном разликом, пратиле су је друге породице као што су GandCrab (11%) и Stop (4%). Прва је добро позната ренсомвер-као-услуга (ransomware-as-a-service), коју је развио тим криминалаца и изнајмљена је широј заједници и дистрибуирана годинама. Стоп ренсомвер кампања је такође добро позната претња која се шири путем компромитованих софтвера и веб-сајтова, као и адвера" (персоналмаг, 2020).

У марту 2020. године извршен је ренсомвер напад на Нови Сад. „Током једног викенда у марту криптовани су сервери градских управа и неколико других јавних служби преко ЈКП Информатика. Градске камере нису биле у функцији, а запосленима у градским службама речено је да не могу да приступе својим мејловима. Градска управа Новог Сада је одбила да плати откупнину. Нападачи су првобитно тражили 50 биткоина (око 400.000 евра), а касније спустили цифру на 20 биткоина. С обзиром на то да је и резервна копија података заражена вирусом, односно закључана, Нови Сад ће остати без свих криптованих података. Није саопштено шта је све нестало и које су размере напада. Градоначелник Новог Сада Милош Вучевић је изјавио да је упад у систем извршен преко мејла" (ит-клиника, 2020).

Са појавом вируса SARS-COV2, који изазива болест COVID-19, приморани смо да бројне радне активности пренесемо на онлајн режим. Значајно више проводимо времена испред рачунара, мобилних уређаја, користећи интернет најпре у пословне сврхе, али и за комуникацију, куповину и информисање о свим нама релевантним темама. С обзиром на све те активности, морамо да предузмемо и одређене акције како бисмо најбоље заштитили наше рачунаре, нарочито у случајевима када се повезујемо на мрежу компаније. Пошто је COVID-19 тренутно тема број један у свету, хакери у великој мери користе ту ситуацију, што је довело и до значајног пораста сајбер криминала. Бројни хакери користе COVID-19 ситуацију, како би навели кориснике да инсталирају различите малициозне

софтвере, све у циљу долажења до осетљивих података корисника, лозинки, праћења активности корисника на систему и слично.

„Различити су начини које хакери користе како би спровели своје акције у дело, само неке од њих су нпр. фишинг кампање и дистрибуција злонамерног софтвера, спам, злонамерни сајтови, рансомвер итд. Неки од примера злонамерних софтвера су:

Corona Virus Trojan – циљајући на Windows, овај тројански програм опонаша стварну мапу глобалних локација инфекција COVID-19 како би навели кориснике да преузму злонамерни софтвер, који потом краде корисничке акредитиве и друге личне податке.

CovidLock Android Ransomware – андроид апликација која се претвара да корисницима пружа начин да пронађу пацијенте COVID-19 у близини и прате ширење вируса широм света. Инсталирањем апликације закључава се уређај и тражи од корисника да плати 250 долара откупнине за биткоине.

Corona Safety Mask SMS Scam – претварајући се да је апликација која помаже корисницима да пронађу сигурносне маске, прикупља контакте и СМС поруке корисника, а затим шаље неистините поруке контактима жртве.

Мере заштите које се препоручују су да будемо опрезни са мејловима и фајловима које добијамо од непознатих пошиљаоца, да будемо опрезни са линковима и фајловима у мејловима који стижу од непознатих извора, да поручујемо производе онлајн само од проверених извора, да информације о COVID-19 тражимо само на провереним и званичним страницама, да своје податке нипошто и никоме не откривамо, јер званичне институције никада неће тражити такве податке путем имејла" (сага, 2020).

Болнице широм света под додатним су притиском због COVID-19 и то је нешто што сајбер криминалци желе да искористе. Било је бројних напада рансомвера који су били усмерени на болнице јер су нападачи покушали да у кључном тренутку виталну инфраструктуру држе као таоца да би могли да траже откуп, ризикујући животе људи. „Напад за који се претпоставља да је изазвао рансомвер погодио је Универзитетску болницу Брно у Чешкој, тест центар за COVID-19. Рачунарски системи у болници били су затворени због напада, што одлаже пуштање резултата испитивања COVID-19. Болнице, медицински центри и јавне установе су главне мете напада рансомвером, јер су установе окупиране здравственом

кризом и не могу да приуште да буду изван својих система, а криминалци верују да ће им се вероватно платити откупнина, јер управо лекарима су потребни подаци о пацијентима који се лече од корона вируса и који тек треба да почну са лечењем" (информација, 2020).

Тим састављен од безбедносних експерата из 65 земаља окупљен је у циљу спречавања рансомвер напада у време пандемије коронавируса. Понели су име COVID-19 CTI League, а главни циљ им је да осетљиве структуре у болничким установама заштите од сајбер напада. Живановић тврди да се ради о томе да су болнице широм света бележиле повећан број хакерских напада у претходних годину дана, у оквиру којих су кључни ИТ системи били енкриптовани уз помоћ малвера. Медицинске установе су често мета, а због застарелих система, те осетљивости посла којим се баве, због које морају да плате откупнине у рекордном року. Недавно је објављено да Ryuk рансомвер, на пример, и даље циља болнице у САД, без обзира на то што је читав свет у ванредном стању. Оснивач одбрамбене сајбер лиге је Охад Зајденберг (Ohad Zaidenberg), а око себе је окупио бројне експерте чији је циљ да заштите болнице у овом осетљивом периоду. Јасно је да напади на болнице угрожавају животе и у нормалним условима, али су у време пандемије постали још опаснији, највише због тога што медицинске установе и без њих имају проблема да се организују и изађу у сусрет свима којима је помоћ потребна (Живановић, 2020).

„Сајбер криминалци који стоје иза рансомвера **Maza** напали су ИТ мрежу „Hammersmith Medicines Research" (HMR), медицинске установе која је у стању приправности да помогне у испитивању могућих вакцина против корона вируса, и објавили су личне податке о хиљадама бивших пацијената након што је компанија одбила да плати откупнину. До напада је дошло након што је криминална група дала јавно обећање да неће нападати медицинске истраживачке организације током пандемије" (информација, 2020).

Компанија Гармин 23. јула 2020. године је искључила неколико својих услуга због напада рансомвера који је шифровао њихову интерну мрежу и неке производне системе. „Портпарол компаније Гармин одбио је да потврди да је прекид рада изазван рансомвер нападом, али је рекао да је истрага у току. Међутим, откад се инцидент десио, неколико запослених у компанији се јавило на друштвеним мрежама где су поделили детаље о нападу, а сви су говорили о рансомвер нападу. Појединци међу њима инцидент су приписали новом рансомверу који се појавио ове године, под називом **WastedLocker**, али у овом тренутку то су само нагађања.

Међутим, чини се да је инцидент много већи и погубнији него што је Гармин најавио у својој првој изјави" (информација, 2020). У дуго очекиваном саопштењу које је објавио Гармин, потврђен је ренсомвер напад, али компанија није рекла који је ренсомвер у питању, што је уобичајена пракса у оваквим случајевима док траје истрага. Гармин није именовао кривца за напад, али незванично иза напада стоји руска хакерска група **Evil Corp**. Човек који стоји иза ове хакерске групе је Максим Јакубец (Maksim Yakubets). „У децембру 2019. године, ФБИ је расписао награду у износу од пет милиона долара за информације о Максиму које би довеле до његовог хапшења. То је највећа награда која је икада понуђена за неког ко је повезан са сајбер криминалом. Верује се да је Максим одговоран за нападе на десетине америчких компанија. Максим, који и даље живи у Русији, стекао је огромно богатство од ренсомвер напада, а познат је по животу на високој нози. Према извештајима који нису потврђени, хакерска група која је компромитовала Гарминове сервере тражила је откуп од 10 милиона долара. **WastedLocker** се повезује са криминалном групом **Evil Corp** која је препознатљива по томе што у нападима користи банкарског тројанца **Dridex**. Након што су САД подигле оптужницу против чланова групе Evil Corp, група је променила своје тактике и технике и увела у игру WastedLocker који користи за изнуду новца од компанија које нападне" (информација, 2020).

Велика епидемија ренсомвер напада погодила је кинеске кориснике интернета у априлу 2020. године. Отприлике недељу дана, ренсомвер познат као **WannaRen** инфицирао је уређаје на десетине хиљада људи, али и локалних кинеских и тајванских компанија. Као и у случају ренсомвера WannaCry, аутори WannaRen ренсомвера уградили су EternalBlue exploit у ланац инфекције, омогућавајући WannaRen-у да се шири без ограничења унутар корпоративних мрежа пре шифровања фајлова. Баш као и WannaCry, и WannaRen се проширио попут пожара, далеко више од онога што су аутори ренсомвера наумили, узрокујући много већи проблем него што су они предвидели, и то је разлог зашто су се на крају аутори ренсомвера бесплатно одрекли мастер кључа за дешифровање, тако да све жртве могу да врате своје фајлове (информација, 2020).

Сада се са сигурношћу може рећи да су WannaCry створили севернокорејски хакери који раде за владу ове државе, имајући на уму мањи број жртава, од којих ће узети откупнину и употребити је за финансирање режима у Пјонгјангу. Аутори WannaCry никада нису имали велике амбиције, а изазивање глобалне епидемије никада није била

њихова намера, јер је то само привукло више пажње и указало на њихове криминалне активности. Нешто слично се може рећи и за ауторе WannaRen рансомвера, групу за коју је кинески произвођач антивируса Qihho 360 рекао да је прати под именом Hidden Shadow. Ова група је активна годинама, умешана је у дистрибуцију низа малвера (злонамерних софтвера), обично преко пиратских сајтова на којима се нелегално може преузети софтвер. Досадашње деловање групе било је ограничено на дистрибуцију малвера који краду лозинке, тројанаца за даљински приступ и малвера за рударење криптовалута. WannaRen је додат у арсенал групе 4. априла 2020. године. Према више извора, почетна тачка дистрибуције WannaRen-а била је модификовани инсталациони програм за уређивач текста Notepad++ који се дистрибуира преко Xixi софтвер центра. Пошто је приступ званичном веб сајту за преузимање Notepad++ у Кини често блокиран због анти-кинеског става произвођача софтвера, а и зато што је Xixi један од највећих кинеских сајтова за преузимање софтвера, логично је што је одмах дошло до великог скока броја инфицираних. На рачунарима на којима су корисници инсталирали ову инфицирану верзију Notepad++, инсталациони фајл је остављао backdoor тројанца, активирао EternalBlue exploit како би се проширио по мрежи и користио PowerShell скрипту за преузимање и инсталирање WannaRen рансомвера или модул за рударење криптовалуте Monero. Када би блокирао рачунаре корисника, рансомвер је приказивао поруку о откупнини са сликом севернокорејског председника Ким Џонг Уна и тражио од жртава да плате накнаду за дешифровање од 0,05 биткоина (око 550 долара) да би њихови фајлови били дешифровани. Сви рачунари које је заразио овај рансомвер били су препознатљиви по томе што је називима шифрованих фајлова додавана екстензија **.wannaren** (информација, 2020).

С обзиром на циљеве напада и откупнину, било је прилично јасно да група није намеравала да се њихов рансомвер шири тако много и тако брзо. Вероватно се плашећи реакције кинеских власти, мање од недељу дана након што је почела дистрибуција WannaRen-а, група Hidden Shadow контактирала је локалну кинеску фирму за сајбер безбедност под називом Huorong Security. У низу мејлова које је компанија објавила, аутори WannaRen-а проследили су мастер кључ за дешифровање рансомвера, тражећи од компаније да направи и подели бесплатни програм за дешифровање са зараженима. Huorong Security, 9. априла 2020. године, објавио је свој програм за дешифровање WannaRen-а, након чега је неколико сати касније објављен сличан програм за дешифровање који је

направила компанија QiAnXin Technology, која је такође пратила брзо ширење рансомвера широм Кине. Међутим, иако је велика већина корисника WannaRen-а била у Кини, екстремна виралност рансомвера је такође омогућила да се малвер путем интерних мрежа прошири из кинеских огранака у неке стране компаније. С обзиром да нису све ове компаније можда знале да постоји бесплатан алат за дешифровање или можда не верују алатима које су направиле две кинеске фирме, румунски произвођач антивируса Bitdefender објавио је свој алат за дешифровање WannaRen-а. У овом тренутку WannaRen више није активан, али жртве које су априла 2020. године можда направиле копије шифрованих фајлова сада их могу бесплатно дешифровати (информација, 2020).

Рансомвер **NetWalker** појавио се 2019. године, али је тек 2020. године постао озбиљно име у свету сајбер криминала, с обзиром да је од изнуда зарадио око 29 милиона долара и то само од марта 2020. године. Међутим, стручњаци за безбедност из компаније McAfee који су објавили анализу малвера сматрају да је криминална група која стоји иза рансомвера зарадила више, пошто немају комплетан увид у њихове трансакције. NetWalker је први пут примећен у августу 2019. године, а његова прва верзија појавила се под именом **Mailto**, али је до краја 2019. рансомвер преименован у NetWalker. Интензивно је почео да се користи од марта 2020. године, показала је анализа компаније McAfee. Пораст броја инфекција се поклопио са имплементацијом модела рансомвер-као-услуга, који привлачи технички напредне криминалне групе. Хакерске групе пријављују се и пролазе кроз поступак провере, након чега им је омогућен приступ веб порталу на којем могу направити прилагођене верзије софтвера. Дистрибуција је препуштена тим групама, и свака група користи рансомвер на начин који сматра прикладним. NetWalker рансомвер-као-услуга даје предност квалитету пре него квантитету и тражи људе који говоре руски језик и имају искуства са великим мрежама. Углавном је коришћен за нападе на велике компаније и институције, у Европи и Северној Америци. Неке од његових жртава су транспортна компанија Тол Група, Универзитет Калифорније, Сан Франциско, а недавно је нападнута и једна француска компанија која производи паметне батерије. Такође, федерални истражни биро, ФБИ, упозорио је да они који стоје иза рансомвера NetWalker сада циљају државне институције у САД, али и у другим државама (информација, 2020).

Један од разлога зашто је NetWalker толико популаран је и веб сајт на коме група објављује имена и податке жртава које одбијају да плате откупнину.

Када NetWalker компромитује мрежу, они најпре краду податке компаније, а затим шифрирају фајлове. Ако жртва одбије да плати за дешифровање фајлова током почетних преговора, група креира унос на њиховом веб сајту који има тајмер, а ако жртва и даље одбија да плати, група објављује фајлове које је украла из мреже жртве. Сајт помаже овом ренсомверу да изврши додатни притисак на жртве, јер се многи плаше да ће њихово интелектуално власништво или осетљиви кориснички подаци завршити на интернету, док се други боје да ће њихово име бити у медијима, а многе компаније ће платити само да се њихово име не појави у медијима у том контексту.

Универзитет у Јути, у Солт Лејк Ситију, такође је жртва напада ренсомвером. Хакерима су на крају исплатили скоро пола милиона долара да не би објавили осетљиве информације о студентима и запосленима на интернету. Иако детаљи о самом ренсомверу који је коришћен у нападу на универзитет нису објављени, универзитет је потврдио да је ренсомвер шифровао око 0,02% података сачуваних на његовим серверима, као и да украдене информације припадају и запосленима и студентима. Универзитет је вратио податке користећи сигурносне копије, али је плаћање било неопходно јер су хакери претили да ће објавити украдене податке студената на интернету, што је натерало менаџмент универзитета да преиспита своју одлуку о плаћању нападачима. Универзитет је на крају платио хакерима више од 457 000 долара, а део откупнине покривен је полисом сајбер осигурања. За откуп нису коришћена средства од школарина. Званичници универзитета су такође изнели и друге детаље о нападу, као што је датум када се догодио (19. јул 2020.) и на који део мреже је утицао (мрежа Факултета друштвених и бихејвиоралних наука на Универзитету). Међутим, универзитет није открио ко стоји иза напада. Брет Калов, аналитичар из фирме Емсисофт, изјавио је да, иако недостају конкретни докази, иза напада највероватније стоји криминална група која користи ренсомвер NetWalker. Ова група, за коју се верује да је ове године зарадила од ренсомвера више од 25 милиона долара, одговорна је и за недавни талас напада на универзитетске мреже, попут напада на Универзитет у Калифорнији у Сан Франциску (плаћено 1,14 милиона долара) и Градског универзитета у Сијетлу (информација, 2020).

Када је покренута 2016. године, No More Ransom иницијатива имала је свега четири члана, оснивача. No More Ransom нуди бесплатне алате за дешифровање фајлова на уређајима зараженим ренсомвером. No More Ransom има 163 партнера из области кибернетичке безбедности, полиције

и сектора финансијских услуга. No More Ransom је објавио бесплатне алате за дешифровање за више од 140 ренсомвера, који су преузети више од 4,2 милиона пута. Међу најзаслужнијим сарадницима пројекта су Емсисофт који је обезбедио 54 алата за дешифровање за 45 ренсомвера, компанија Касперски, која је оснивач пројекта No More Ransom, пет алата за 32 ренсомвера и Тренд Микро који је пројекту дао два алата за дешифровање за 27 ренсомвера. Остале компаније које су иницијативи допринеле са више алата су Аваст, Битдефендер, Чек Поинт, ESET и још један оснивач - компанија McAfee. No More Ransom доступан је на 36 језика и има посетиоце из 188 земаља широм света. Највећи број посетилаца долази из Јужне Кореје, САД, Бразила, Русије и Индије (информација, 2020).

Иако се No More Ransom показао корисним жртвама ренсомвера, сам Европол и даље препоручује превенцију као најбоље средство за заштиту од напада, нарочито имајући у виду природу ренсомвера који непрекидно еволуира, што значи да постоје многи ренсомвери за које нема бесплатног алате за дешифровање и можда га никада неће ни бити. Мере превенције које препоручује Европол укључују прављење резервних копија важних фајлова које треба чувати на сигурном, дакле ван мреже, тако да се у случају напада фајлови могу одмах преузети, без обзира да ли је доступан алат за дешифровање или не. Европол такође препоручује да корисници не преузимају програме из сумњивих извора или отварају прилоге непознатих пошиљалаца, како не би постали жртве напада ренсомвера.

Министарство унутрашњих послова Белорусије објавило је да је почетком августа 2020. године 31-годишњи мушкарац ухапшен под оптужбом да је дистрибуирао ренсомвер GandCrab. Власти су саопштиле да ухапшени раније није осуђиван. Ухапшени је био део операције дистрибуције ренсомвера GandCrab, а за дешифровање рачунара, тражио је од жртава око 1200 долара које је требало платити биткоинима. Он је потенцијалним жртвама слао фајлове који би, ако би их жртве отвориле, заразили њихове уређаје, да би им после тога био испостављен захтев да плате откупнину да би добиле програм за дешифровање и вратиле своје фајлове. Део новца које је узимао од жртава осумњичени је морао да преда администраторима ренсомвера GandCrab. Дистрибутери ренсомвера су добијали 60% од прве три откупнине за које су били заслужни, а након тога, њихов удео у приходима би се повећао на 70%. То значи да је осумњичени који је добијао 1200 долара од сваке жртве, зарађивао 840 долара за сваку

инфекцију, а програмери рансомвера GandCrab по 360 долара (информација, 2020).

Рансомвер наставља да буде једна од науспешнијих интернет претњи због тога што у основи функционише, а хакери на крају дођу до неке суме новца, што их мотивише да иду напред. Просечна „зарада“ се увећала за 33% у првом кварталу 2020. године, те износи око 111 хиљада долара. Највећи проблем је период који прође од почетка напада до исплате откупнине, а који у просеку износи 15 дана. Управо се због тога све чешће циљају осетљиви системи, те читави градови, будући да жртве раније плаћају уколико су подаци важнији, а посебно ако су у питању информације о становницима целог града. Градић Флоренс у Алабами, 5. јуна 2020. године, постао је жртва једног рансомвер напада, а од града се тражило да уплати суму од 300 хиљада долара. Градски оци су изјавили да ће новац највероватније уплатити, како би се спречило да информације грађана заврше на интернету. Само месец дана пре тога друга нападачка група угрозила је једну њујоршку адвокатску канцеларију, а за повраћај података се тражило чак 42 милиона долара. Власници су о плаћању морали озбиљно да размисле, будући да су се међу украденим подацима нашле и информације о америчком председнику (инвеститор, 2020).

Жртва напада постала је и компанија Хонда, а у питању је безбедносни инцидент који подсећа на рансомвер, а који је погодио производне погоне. И ту се уочава прва разлика у односу на старије рансомвер стратегије – крађа података је једно, а заустављање производње нешто сасвим друго. Тако преузимање виталних система које утиче на заустављање производње полако постаје водећа сајбер претња, што се показало ефектнијим, будући да одмах скреће пажњу кључних лица у некој компанији, што утиче и на то да се откупнине брже исплаћују. Напади на виталне инфраструктуре су тако много већа претња, јер наносе више штете, па такве стратегије могу да униште неки бизнис. Овакви напади често циљају и јавни сектор, те владине организације, а како би се дошло до података које ни једно владино тело не жели да остави у рукама сајбер криминалаца. Рансомвер ће наставити да се развија, будући да се ради о озбиљном извору зараде, а експерти истичу да су преговори са нападачима исто што и било која друга пословна трансакција, само што жртве из тога не добијају ништа осим онога што је већ било њихово, док нападачи не улажу ништа осим сопственог времена (инвеститор, 2020).

„Четворочлана група „Pentaguard“ основана почетком 2020. године намеравала је да у блиској будућности изврши рансомвер нападе на неке болнице у Румунији, користећи социјални инжењеринг слањем злонамерне извршне апликације, скривене у мејлу и у облик датотеке који би очигледно дошао из других владиних институција, у вези са претњом COVID-19. Овом врстом напада постоји могућност блокирања и озбиљног нарушавања функционисања ИТ инфраструктуре тих болница, дела здравственог система, који у овом тренутку игра пресудну улогу у борби против коронавируса” (Muncaster, 2020).

„Технолошка инфраструктура медицинског центра Parkview са седиштем у Колораду погођена је рансомвер нападом 21. априла 2020. године, што је проузроковало бројне прекиде ИТ мреже. Болница поред тога што опслужује пацијенте током пандемије COVID-19, мора да ради и на опоравку од напада. Открившши сајбер напад, званичници су рекли да су ступили у контакт са независним форензичким тимом како би ублажили и истражили инцидент. Обавештење не наводи детаљно на који начин су системи били погођени када је започео напад, као ни то да ли је то утицало на податке о пацијентима. Болница користи папирне записе за праћење и лечење пацијената, док раде на обнављању погођених система” (Davis, 2020).

Криминалне групе које раде са рансомњареом прошле године су од откупнина зарадиле најмање 350 милиона долара, открила је компанија *Chainalysis* у извештају објављеном прошле недеље. До те бројке дошло се праћењем трансакција ка блокчејн адресама повезаним са рансомвер нападима. Иако *Chainalysis* има вероватно најсвеобухватније податке о сајбер-криминалу повезаном са криптовалутама, компанија је рекла да је њена процена само доња граница стварног укупног профита. *Chainalysis* каже да нису све жртве прошле године открилe нападе рансомвера и накнадне исплате, и да је стварна укупна зарада сајбер криминалаца била вишеструко већа од онога што је компанија могла да види. Према подацима објављеним у извештају, плаћања повезана са рансомвером чинила су 7% свих средстава која су завршила на рачунима сајбер криминалаца у 2020. години. Бројка је већа за 311% у поређењу са 2019. годином, а *Chainalysis* сматра да је за овај нагли пораст крив “број нових малвера који узимају велике суме од жртава” и “неколико већ постојећих који драстично повећавају зараду”. На основу података компаније, међу онима који су прошле године најбоље зарађивали су групе као што су Ryuk, Maze (која сада не постоји), Doppelpaymer, Netwalker (чији је

опстанак доведен у питање после недавног хапшења), Conti i REvil (познат и под називом Содинокиби). И други ренсомвери попут Snatcha, Defray777 (RansomExx) и Dharme такође су извукли добит која се процењује у милионима долара. *Chainalysis* је рекао да на основу начина на који су жртве плаћале откупнине и како су зараде од одређених ренсомвера расле и падале, постоје и докази који указују да је на ренсомвер сцени много мање актера него што се раније веровало, и да су се многе од ових група пребацивале са једне ренсомвер услуге на другу јер су их привукле боље понуде. *Chainalysis* је рекао да је такође пратио како преваранти премештају исплаћене откупнине кроз блокчејн. Нова открића нису се превише разликовала од оних из претходних година. *Chainalysis* каже да су криминалци обично прали новац преко услуга „мешања биткоина", а затим их конвертовали у стварну валуту. *Chainalysis* је такође открио да ренсомвер групе често користе иста та средства за плаћање услуга других сајбер криминалаца: такозваним bulletproof hosting провајдерима, продавцима exploit-а и сервисима који врше пенетрацијске тестове (брокери почетног приступа). *Chainalysis* каже да су многе од ових група често користиле исте посредничке услуге прања новца.

8. ЗАКЉУЧАК

По неким прогнозама експерата и међународних безбедносних агенција очекује се даљи развој ВТК, првенствено због све веће приступачности технологија широком спектру људи и могућности да се за криминалне активности ангажује велики број неквалификованих појединаца, као и због повећаног броја напада који ће бити последица велике аутоматизације коју омогућавају алати и интернет. По неким проценама губици услед деловања ВТК, појединачно или кроз различите организационе форме, у 2021. години достићи ће шест милијарди долара.

Постоје, слободно можемо рећи два аспекта са којих можемо посматрати претње. То су организације, са једне и, појединци тј. физичка лица, са друге стране. Када је реч о организацијама, били смо сведоци напада рансомвером на ЈП „Информатика“ из Новог Сада, који је онемогућио рад многих јавних служби у том граду. На самом почетку пандемије корона вируса, у Чешкој је криптовирусом била нападнута COVID-19 болница у Прагу што је онемогућило њен рад. Оваква врста напада је за правна лица једна од највећих претњи. Исто тако су распрострањени и тзв. фишинг напади. Тако је, на пример, 2017. године извршен фишинг напад на Народну банку Србије. Банка је са фишинг имејла са наводним новим инструкцијама за плаћање, уплатила велику суму новца нападачу. Када је реч о томе како се заштити, постоји сет мера које би организације требало да примењују. То није само инсталација антивирус програма, већ употреба читавог низа алата. Да бисмо успешно реализовали заштиту од ВТК и сузбијање ВТК, прво требамо подићи колективну свест грађана о свим опасностима и последицама до којих може довести ВТК. У остварењу овог циља најзначајнију улогу имају образовне институције кроз константне едукације и семинаре као и сами медији путем објективног и непристрасног извештавања.

Током 2020. године значајно се увећао број рансомвер напада, па је број инцидената седам пута већи него 2019. године. Рансомвер напади последњих година постају све опаснији, будући да нападачи покушавају да енкриптују што већи број пословних мрежа, како би што пре добили тражене откупнине у биткоину. Само један напад може да донесе зараду од неколико стотина хиљада, па чак и неколико милиона долара. Од почетка пандемије корона вируса број напада се увећао, будући да велики број запослених ради од куће, што утиче и на безбедносне протоколе. Проблем није само у повећаном броју напада, већ и у томе што тактике

константно еволуирају, те старе верзије овог малициозног кода брзо нестају, како би уступиле место новим, још увек непознатим варијантама. Тако ови напади све више угрожавају организације и компаније свих профила. Са друге стране, експерти истичу да ови напади могу да се спрече у само неколико једноставних корака. Наиме, довољно је да се безбедносне мере примењују на време, како хакери не би могли да користе познате рањивости, те да се примењује вишефакторска аутентификација, будући да спречава нападаче да добију потпуно контролу над погођеним системима.

Недостатак поузданих емпиријских података о ВТК и даље доприноси његовом недовољном разумевању. Такође су и димензије ВТК мало познате, углавном због виртуелности и „невидљивости" криминала, сложености дигиталних трагова и отежане или онемогућене сарадње жртава, као и ограничености деловања органа закона у откривању и гоњењу починилаца, што ствара велику тамну бројку неоткривених, непријављених, неистражених или нерешених случајева.

Република Србија је у настојању да се супростави ВТК уредила Кривични законик у складу са Европским, и донела Стратегију за борбу против ВТК за период од 2019-2023. године као и Акциони план који омогућава државним институцијама да се боре против виртуелних криминалаца који причињавају штету и за собом остављају озбиљне последице у реалном простору. Будућност ВТК у Републици Србији узима све већи замах, јер корисници интернета који су са друге стране закона користе његове слабости и на брз и јефтин начин долазе до циља, што органима поступка може представљати потешкоћу да се ухвате у коштац са овим проблемом ако не иду у корак са временом и константно раде на едукацији и побољшању електронске опреме која омогућава бољи и ефикаснији рад у борби против ВТК.

Већ сада са сигурношћу може да се закључи да је највећа светска глобална мрежа, *интернет*, постала уточиште криминала, те да је ВТК профитабилна незаконита активност у којој учествују структуриране организоване групе, чак и појединци који се никад нису срели уживо, али који сарађују преко интернета. Оно што је сигурно јесте да Република Србија у корак прати светске трендове у области ВТК, те да ћемо у блиској будућности бити сведоци извршења све већег броја кривичних дела из области ВТК. Република Србија има одличну сарадњу са представницима амбасада САД, Француске и Велике Британије у Београду. Тужилаштво има установљен партнерски однос са жандармеријом Републике

Француске, која је од јануара 2009. године у саставу Француског министарства унутрашњих послова. На тужилачком нивоу успостављена је сарадња са Енглеским краљевским тужилаштвом. Сарадња са привредом одвија се преко америчке привредне коморе, чија се канцеларија налази у Београду, као и са канцеларијом Мајкрософта. Имајући у виду намеру Републике Србије да постане део ЕУ, тужилаштво је у сталним контактима са мисијом ОЕБС у Републици Србији, као и са Европском комисијом.

9. ЛИТЕРАТУРА

Алексић, Ж., и Шкулић, М. (2016) *Криминалистика* (9. издање). Београд: Правни факултет Универзитета у Београду.

Ashford, W. (2015). *Police arrest 130 in global cyber fraud operation.* Преузето 10. јула 2020., са: http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation

Бановић, Б. (2002). *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета.* Београд: Виша школа унутрашњих послова.

Бејатовић, С. (2012). Високотехнолошки криминал и кривичноправни инструменти супротстављања. У: *Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал: зборник радова међународна научностручна конференција.* (стр. 17-30). Бања Лука: Висока школа унутрашњих послова.

Бошковић, Г., и Ивановић, З. (2012). Стратешке концепције у супротстављању високотехнолошком криминалу. У: *Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал: зборник радова међународна научностручна конференција.* (стр. 79-92). Бања Лука: Висока школа унутрашњих послова.

Бошковић, В. (2018). *Шта су DDoS напади за које су ухапшени тинејџери из Србије.* Преузето 17. јула 2020., са: https://www.vice.com/rs/article/evq3ve/sta-su-ddos-napadi-za-koje-su-uhapseni-tinejdzeri-iz-srbije

Бркић, М. (2018). *"МИРКО" И "ВУЛЕ" Како су двојица младића из Србије постала део МЕЂУНАРОДНЕ ХАКЕРСКЕ БАНДЕ која је срушила 4 МИЛИОНА САЈТОВА.* Преузето 17. јула 2020., са: https://www.blic.rs/vesti/hronika/mirko-i-vule-kako-su-dvojica-mladica-iz-srbije-postala-deo-medjunarodne-hakerske/p7glsgk

Bequai, A. (1990). Computer-related crime. *Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems.* Strasbourg: Council of Europe. Преузето 28. јуна 2020., са: http://www.oas.org/juridico/english/89-9&final%20Report.pdf

Видојковић, М. (2015). *Компјутерски криминалитет.* Мастер рад. Ниш: Правни факултет.

Вилић, В. (2016). *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета.* Докторска дисертација. Ниш: Правни факултет.

B., J. (2018). *Американци изнајмљивали хакере у Србији за 1000 долара.* Преузето 17. јула 2020., са: https://www.danas.rs/drustvo/amerikanci-iznajmljivali-hakere-u-srbiji-za-1-000-dolara/

Димовски, Д. (2010). *Компјутерски криминалитет.* Зборник, LV, (стр. 197-214.) Ниш: Правни факултет.

Davis, J. (2020). *Ransomware Shuts Down Colorado Hospital IT Network Amid COVID-19.* Преузето 16. септембра 2020., са: https://healthitsecurity.com/news/ransomware-shuts-down-colorado-hospital-it-network-amid-covid-19

European Commission. (2015). Digital agenda for Europe - European Commission Directorate-General for Communication Citizens information. Luxembourg: Publications Office of the European Union.

Europol. (2015). *International police action leads rescue 22 month old Romanian sex abuse.* Преузето 08. јула 2020., са: https://www.europol.europa.eu/content/international-police-action-leads-rescue-22-month-old-romanian-sex-abuse-victim

Живановић, М. (2020). *Global Cybersecurity League: Одбрана болница током пандемије.* Преузето 12. септембра 2020., са: https://pcpress.rs/global-cybersecurity-league-odbrana-bolnica-tokom-pandemije/

Живановић, М. (2020). *WannaCry ransomware: Три године касније.* Преузето 16. септембра 2020., са: https://pcpress.rs/wannacry-ransomware-tri-godine-kasnije/

Живановић, М. (2020). *Ransomware: Повећан број напада у односу на прошлу годину.* Преузето 16. септембра 2020., са: https://pcpress.rs/ransomware-povecan-broj-napada-u-odnosu-na-proslu-godinu/

Игњатијевић, С., и Матијашевић, Ј. (2010). *Компјутерски криминалитет у правној теорији, појам, карактеристике, последице.* Vol. 9, Ref. E-VI-8, pp. 852-856. Источно Сарајево: Електротехнички факултет.

Илингворт, В. (1990). *Оксфордски речник рачунарства.* Београд: Нолит.

Инвеститор. (2020). *Крађа података се не исплати, ransomware напади све чешћи.* Преузето 16. септембра 2020., са: https://investitor.me/2020/06/20/kradja-podataka-se-ne-isplati-ransomware-napadi-sve-cesci/

Информација. (2020). *Криминалци користе пандемију да би зарадили од својих апликација за Андроид и малвера.* Преузето 14. септембра 2020., са: https://www.informacija.rs/Vesti/Kriminalci-koriste-pandemiju-da-bi-zaradili-od-svojih-aplikacija-za-Android-i-malvera.html

Информација. (2020). *Гармин претрпео напад ransomware-а, компанија обуставила неке услуге и производне линије.* Преузето 14. септембра 2020., са: https://www.informacija.rs/Vesti/Garmin-pretrpeo-napad-ransomwarea-kompanija-obustavila-neke-usluge-i-proizvodne-linije.html

Информација. (2020). *Од Гармина после напада тражено да плати 10 милиона долара, иза напада стоје руски хакери*. Преузето 14. септембра 2020., са: https://www.informacija.rs/Vesti/Od-Garmina-posle-napada-trazeno-da-plati-10-miliona-dolara-iza-napada-stoje-ruski-hakeri.html

Информација. (2020). *Гармин потврдио напад ransomware-a, сервиси компаније поново доступни*. Преузето 14. септембра 2020., са: https://www.informacija.rs/Vesti/Garmin-potvrdio-napad-ransomwarea-servisi-kompanije-ponovo-dostupni.html

Информација. (2020). *Ухапшен хакер који је инфицирао више од 1000 рачунара ransomware-ом GandCrab*. Преузето 15. септембра 2020., са: https://www.informacija.rs/Sajber-hronika/Uhapsen-haker-koji-je-inficirao-vise-od-1000-racunara-ransomwareom-GandCrab.html

Информација. (2020). *Бесплатни алати из програма No More Ransom сачували жртвама ransomware-a 650 милиона евра.* Преузето 15. септембра 2020., са: https://www.informacija.rs/Vesti/Besplatni-alati-iz-programa-No-More-Ransom-sacuvali-zrtvama-ransomwarea-650-miliona-evra.html

Информација. (2020). *Canon претрпео напад ransomware-a, хакери тврде да су украли 10 терабајта података.* Преузето 15. септембра 2020., са: https://www.informacija.rs/Vesti/Canon-pretrpeo-napad-ransomwarea-hakeri-tvrde-da-su-ukrali-10-terabajta-podataka.html

Информација. (2020). *Зашто су аутори WannaRen ransomware-a одлучили да жртвама бесплатно дају кључ за дешифровање.* Преузето 15. септембра 2020., са: https://www.informacija.rs/Vesti/Zasto-su-autori-WannaRen-ransomwarea-odlucili-da-zrtvama-besplatno-daju-kljuc-za-desifrovanje.html

Информација. (2020). *Универзитет платио хакерима пола милиона долара после напада ransomware-ом.* Преузето 15. септембра 2020., са: https://www.informacija.rs/Vesti/Univerzitet-platio-hakerima-pola-miliona-dolara-posle-napada-ransomwareom.html

Информација. (2020). *Криминалци стоје иза ransomware-a NetWalker само од марта зарадили најмање 29 милиона долара.* Преузето 15. септембра 2020., са: https://www.informacija.rs/Virus/Kriminalci-koji-stoje-iza-ransomwarea-NetWalker-samo-od-marta-zaradili-najmanje-29-miliona-dolara.html

ИТ-клиника. (2020). *Пажња: Нови опасни ransomware pwndlocker и у Србији, нападнут Нови Сад!* Преузето 16. септембра 2020., са: https://www.it-klinika.rs/blog/paznja-novi-opasni-ransomware-pwndlocker-i-u-srbiji

Interpol. (2015). *Annual report 2014 – INTERPOL.* General Secretariat Lyon: INTERPOL.

Interpol. (2015). *Supporting digital crime investigations – INTERPOL.* General Secretariat Lyon: INTERPOL.

Јовашевић, Д., и Хашимбеговић, Т. (2004). *Кривичноправна заштита безбедности рачунарских података.* Тара: Научно стручно саветовање ЗИТЕХ.

Jaishankar, K. (2007). Editorial: Establishing a Theory of Cyber Crimes, *International Journal of Cyber Criminology*, Vol 1 (2): pp. 7-9. Преузето 08. јула 2020., са: http://www.cybercrimejournal.com/Editoriaijccjuly.pdf

Комлен Николић, Л., Гвозденовић, Р., Радуловић, С., Милосављевић, А., Јерковић, Р., Живковић, В., Живановић, С., Рељановић, М., и Алексић, И. (2010). *Сузбијање високотехнолошког криминала.* Београд: Удружење јавних тужилаца и заменика јавних тужилаца Србије.

Константиновић-Вилић, С., Николић-Ристановић, В., и Костић, М. (2012). *Криминологија.* Ниш: Правни факултет.

Лазаревић, Љ. (2011). *Коментар Кривичног законика.* Београд: Правни факултет Универзитета Унион.

Littlejohn Shinder, Debra. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* Rockland: Syngress Publishing.

Мандић, Ј. Г. (2015). *Систем обезбеђења и заштите правних лица.* Београд: Факултет безбедности Универзитета у Београду.

Мандић, Ј. Г., Путник, Н., и Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти.* Београд: Факултет безбедности Универзитета у Београду.ф

Миладиновић, Ж. (2016). *Кривично дело преваре као модел остваривања сајбер криминала.* Докторска дисертација. Београд: Факултет за право, јавну управу и безбедност.

Милошевић, М., и Путник, Н. (2017). Сајбер безбедност и заштита од високотехнолошког криминала у Републици Србији - стратешки и правни оквир, *Култура полиса*, год. XIV, бр. 33, стр. 177-191. Београд: Факултет безбедности.

Мирковић, Д. (2017). *Криминолошки аспект компјутерског криминалитета.* Мастер рад. Ниш: Правни факултет.

Митић, В. (2020). *Ransomware – пример као упозорење*. Преузето 13. септембра 2020., са: https://www.021.rs/story/Novi-Sad/Vesti/235930/Ransomware-primer-kao-upozorenje.html

МУП Републике Србије. *Високотехнолошки криминал*. Преузето 10. јула 2020., са: http://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski%20kriminal/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zi_S19zQzdDYy8LUwMDA0czRzdLQxMLYzcDY31vfSj8CsAmmBU5Ovsm64fVZBYkqGbmZeWrx8Rllmcn51fkpqRl5-TX5ydqZBdlJmbCbKxIDsqEgAXi0v_/

Muncaster, P. (2020). *Police Catch Suspects Planning #COVID19 Hospital Ransomware.* Преузето 16. септембра 2020., са: https://www.infosecurity-magazine.com/news/police-catch-hackers-covid19/

Николић, Д. (2018). *Младићи из Руме и Прокупља ухапшени због високотехнолошког криминала.* Преузето 17. јула 2020., са: https://www.dnevnik.rs/hronika/mladici-iz-rume-i-prokupla-uhapseni-zbog-visokotehn-kriminala-26-04-2018

Перков, Б. (2017). *Како се одбранити од ransomware напада и отмице на интернету.* Преузето 16. септембра 2020., са: https://startit.rs/kako-se-odbraniti-od-ransomware-otmice-na-internetu/

Печић, М. (2018). *Други дан конференције о ВТК-у: Хакери у Србији нису безбедни*. Преузето 25. септембра 2020., са: https://pcpress.rs/drugi-dan-konferencije-o-vtk-u-hakeri-u-srbiji-nisu-bezbedni/

Писарић, М. (2015). *Претресање рачунара ради проналаска електронских доказа.* Зборник радова Правног факултета у Новом Саду, стр. 233. DOI: 10.5937/zrpfns49-8135

Прља, Д., Рељановић, М., и Ивановић, З. (2011). *Кривична дела високотехнолошког криминала.* Београд: Институт за упоредно право.

Путник, Н. (2009). *Сајбер простор и безбедносни изазови.* Београд: Факултет безбедности.

Parker, D. (1983). *Fighting computer crime.* New York: Scribner.

Parker, D. (1989). *Computer Crime: Criminal Justice Resource Manual.* US Department of Justice: National Institute of Justice. Преузето 01. јула 2020., са: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

Персоналмаг. (2020). *Дан борбе против ransomware-а.* Преузето 13. септембра 2020., са: http://www.personalmag.rs/ransomware/

Персоналмаг. (2020). *Сајбер напади на болнице током COVID-19 пандемије налик су терористичким нападима.* Преузето 13. септембра 2020., са: http://www.personalmag.rs/sajber-napadi-na-bolnice-tokom-covid-19-pandemije-nalik-su-teroristickim-napadima/

Prensky, M. (2001). Digital Natives, Digital Immigrants, *MCB University Press,* Vol. 9 No. 5, pp. 1-6. Преузето 03. јула 2020., са: https://marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Радио-телевизија Војводине. (2010). *Прва српска кривична пријава за уношење компјутерских вируса.* Преузето 09. јула 2020., са: http://www.rtv.rs/sr_lat/hronika/prva-srpska-krivicna-prijava-za-unosenje-kompjuterskih-virusa_187640.html

Радуловић, С. (2008). *Специфичност прибављања електронских доказа о извршењу кривичних дела високотехнолошког криминала.* Ревија за безбедност, *2* (12), стр. 17-22. Београд. Центар за безбедносне студије.

РАТЕЛ. (2018). *Конференција о високотехнолошком криминалу и информационој безбедности*. Преузето 25. септембра 2020., са: https://www.cert.rs/rs/vest/259-Konferencija+o+visokotehnolo%C5%A1kom+kriminalu+i+informacionoj+bezbednosti+-+%27%27Pove%C5%BEi+se+sigurno%27%27.html

Републички завод за статистику (РЗС). (2020). Годишње истраживање о употреби информационо-комуникационих технологија, 2020. Београд: Републички завод за статистику Србије. Преузето 24. септембра 2020., са: https://www.stat.gov.rs/sr-latn/vesti/20200922-godisnje-istrazivanje-o-ikt/?a=27&s=

Родић, Б. (2015). *Однос високотехнолошког, кибер и компјутерског криминала*, *2* (1). Primus Global. DOI 10.7251/PMG0115031R.

С. В. (2009). *Голобради хакери ојадили Американце.* Преузето 15. септембра 2020., са: http://www.novosti.rs/vesti/naslovna/aktuelno.69.html:258582-Golobradi-hakeri---ojadili-Amerikance

Сага. (2020). *Cyber kriminal i COVID-19*. Преузето 15. септембра 2020., са: https://saga.rs/blog/cyber-kriminal-i-covid-19/

Сервис компјутера систем Нови Сад. (2020). *Ransomware напади на болнице.* Преузето 13. септембра 2020., са: https://servis-kompjutera-novi-sad.weebly.com/blog/ransomware-napadi-na-bolnice

Спасић, В. (2006). *Актуелна питања у области сајбер криминала.* Билтен судске праксе Врховног суда Србије. Београд: Интермекс.

Schjolberg, S. (2008). *The History of Global Harmonization on Cybercrime legislation - The Road to Geneva.* Преузето 09. јула 2020., са: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf

Sieber, U. (1998). Legal Aspects of Computer-related crime in the Information society-COMCRIME Study, *The European Comission*. Преузето 09. јула 2020., са: https://www.law.tuwien.ac.at/sieber.pdf

Тањевић, Н. (2009). *Компјутерски криминал − правна заштита на националном нивоу,* Вол. 51, број 1-2, стр. 152-166.

Телеграф. (2018). *Вођа Балканских хакера зарадио више од 200 000 евра у биткоинима: Хрватски тинејџер у основној школи упао у систем банке.* Преузето 18. јула, 2020., са: https://www.telegraf.rs/vesti/jugosfera/2954042-vodja-balkanskih-hakera-zaradio-vise-od-200000-evra-u-bitkoinima-hrvatski-tinejdzer-u-osnovnoj-skoli-upao-u-sistem-banke-video

United Nations Office on Drugs and Crime (UNODC). (2010). *The globalization of crime - A transnational organized crime threat assessment.* Vienna: United Nations publication.

Chiesa, R., Ducci S., Ciappi S. (2008). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking.* United States: Boca Raton FL.

Правни извори:

Закон о ауторским и сродним правима. („Службени гласник РС", бр. 104/2009, 99/2011 и 119/2012). Београд: Службени гласник Републике Србије.

Закон о информационој безбедности. („Службени гласник РС" бр. 6/16 и 94/17). Београд: Службени гласник Републике Србије.

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. („Службени гласник Републике Србије" бр. 61/05, 104/09). Београд: Службени гласник Републике Србије.

Законик о кривичном поступку. („Службени гласник Републике Србије" бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 и 35/2019). Београд: Службени гласник Републике Србије.

Конвенција о високотехнолошком криминалу Савета Европе. („Службени гласник РС" број 19, од 19. марта 2009. године). Београд: Службени гласник Републике Србије.

Кривични законик. („Службени гласник РС", бр. 85/2005, 88/2005 – исправка, 107/2005 - исправка, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019). Београд: Службени гласник Републике Србије.

Стратегија за борбу против високотехнолошког криминала за период од 2019-2023. године. („Службени гласник РС", број 71/2018). Београд: Службени гласник Републике Србије.

Стратегија развоја информационе безбедности у Републици Србији до 2020. године. („Службени гласник РС", број 53/2017). Београд: Службени гласник Републике Србије

Стратегија развоја информационог друштва у Републици Србији до 2020. године. („Службени гласник РС", број 51/2010). Београд: Службени гласник Републике Србије.

10. БИОГРАФИЈА АУТОРА

Стефан Марковић рођен је 11. новембра 1994. године у Неготину. Завршио је основну школу „Вера Радосављевић" у Неготину са одличним успехом (5.00), средњу школу, „Неготинску гимназију" у Неготину са одличним успехом (4.93) и Војну академију у Београду са просеком 8.93. Као најбољи у виду ратног ваздухопловства и противваздухопловне одбране (РВиПВО), 2017. године, добио је пиштољ са посветом од министра одбране господина Александра Вулина. Од страних језика познаје енглески језик, а веома мало познаје и немачки језик.