УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови

(мастер рад)

Ментор:
проф. Др Дарко Димовски

Кандидат:
Дарко Александров
M007/23-UP

Ниш, 2025.

САДРЖАЈ

Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови

АПСТРАКТ: *Сајбер простор представља ново и динамично криминогено окружење у којем криминални облици добијају један нови, дигитални облик. Сајбер простор је је основа овога рада, а сам рад у свом целокупном облику истражује теоријске основе сајбер криминала и сајбер претњи, анализирајући њихов утицај на државу, приватни сектор и појединце. Поред дефинисања појма и класификације претњи, рад се бави слабијим тачкама информационо-комуникационих система и мерама заштите података. Такође, приказан је правни и институционални оквир борбе против сајбер криминала на међународном нивоу и у Републици Србији, као и практични изазови кроз анализу студија случаја, укључујући глобални ransomware напад „WannaCry“ и Dark Web операцију „Silk Road“.*

КЉУЧНЕ РЕЧИ: *Сајбер простор, сајбер криминал, сајбер претње, информационо-комуникациони системи.*

I. УВОД

Савремени човек данас живи у дигиталном свету много више него што је тога свестан. Огроман део наших свакодневних активности – од комуникације и информисања, преко пословања и образовања, па све до куповине – одвија се у сајбер простору. Сајбер простор, за који слободно можемо рећи да је невидљив, неопипљив, да је готово имагинаран, постао је саставни део живота људи, ствар навике - да ретко ко помисли шта се заправо налази иза свега тога, какви ризици постоје и колико је сваки корисних заправо изложен. Другим речима, сајбер простор, колико год био користан и неопходан, носи у себи једну другу страну – страну у којој делују појединци и групе које користе анонимност, техничке могућности и рањивости дигиталних система како би остварили противправне циљеве. То, чиме се они баве – назива се сајбер криминал. Сајбер криминалитет се развија неупоредиво брже него традиционални облици криминала, јер се

технолошке иновације јављају из дана у дан. Оно што је јуче била савремена мера заштите, данас може бити превазиђено. О томе нам сведоче и бројни апдејтови (унапређивања) различитих антивирусних система. Нама сумње да је сајбер простор једно сложено и динамично окружење које омогућава масовну размену података, висок степен повезаности и готово тренутан проток информација. Ми, наравно, од свега тога имамо огромне користи које су у тој мери промениле животе људи да данашњи живот човек са почетка 20. века не би могао ни да замисли. Међутим, сви ти бенефити, све те поменуте карактеристике које омогућавају бројне позитивне ефекте у свим областима људског деловања чине овај простор привлачним и за различите облике злонамерних активности. Зато је разумевање ове области не само научно занимљиво, већ и практично неопходно. Свако ко данас управља рачунарима мора да има основно знање о њима, а пре свега о заштити и безбедности, како би уопште могао на нормалан и функционалан начин њима да се служи. Сајбер напад може у истом тренутку да погоди велики број корисника, институција и система, без обзира на географске границе. Зато се данас са правом каже да сајбер криминал представља глобалну претњу која захтева глобални одговор, а не само реакцију појединачних држава. Управо из тог разлога, у овом раду настојим да прикажем ширину и комплексност сајбер простора, као и да покажем како правни и технички системи реагују на претње које су све софистицираније. Разлози за избор ове теме су и личне природе. У једном тренутку схватио сам да, иако свакодневно користим интернет, врло мало размишљам о томе шта се дешава „иза екрана“ и где су границе безбедности. Чини ми се да већина грађана дели исту ситуацију: ослањамо се на технологију без истинског разумевања ризика. Са порастом броја сајбер напада, не само на велике системе и институције, већ и на обичне људе, постало ми је јасно да је важно дубље разумети функционисање овог окружења. Рад на овој теми био је, у том смислу, не само академско истраживање већ и лични изазов – да боље разумем простор у којем свакодневно боравим, иако је невидљив и нематеријалан, те да себе, као што се обезбеђујем у физичком простору, обезбедим и у сајбер простору.

Рад је структуиран тако да прво уведе појам и дефиниције сајбер простора, затим анализира различите облике криминала у њему, са посебним освртом на криминал усмерен против државе и против приватног сектора. Након тога, представљене су

различите сајбер претње, њихова класификација, као и субјекти који их покрећу. Посебна пажња посвећена је заштити у сајбер простору, анализи слабијих тачака информационо-комуникационих система и мерама заштите које се примењују. Рад такође разматра правни и институционални оквир борбе против сајбер криминалитета на међународном, европском и националном нивоу, уз конкретне студије случаја, попут глобалног „WannaCry“ напада и Dark Web операције „Silk Road“. На крају, рад се бави могућностима унапређења система борбе против сајбер криминала и даје закључак који сажима резултате истраживања. Циљ овог рада је да пружи свеобухватнији увид у природу сајбер криминалитета, да укаже на постојеће слабости система и да, на основу анализе, понуди препоруке које могу допринети унапређењу система сајбер безбедности.

II. САЈБЕР ПРОСТОР – ПОЈАМ И ДЕФИНИЦИЈА

Није прошло много времена од појаве првог рачунара. Међутим, од тада па до данашњег дана, променило се много тога. Промена коју је узроковао настанак и развој информационих технологија може да се пореди са проналаском точка или пак са проналаском парне машине. Речју, десила се револуција. То је резултирало чињеницом да се рачунари данас користе у свим областима људског деловања. Наравно, није се развио само рачунар, већ и нове технологије уопштено. Развојем рачунара, развика се наравно и глобална рачунарска мрежа, односно интернет. Међутим, треба истаћи чињеницу да је тај брзи развој информационо-комуникационих технологија омогућио масовну употребу, па да је самим тим дошло и до злоупотребе поменуте технологије. Тако се јавио и појам сајбер криминала, који се разликује од других облика криминалитета по томе што је простор криминалног деловања значајно проширен а тај простор не захтева присуство извршиоца на месту извршења кривичног дела.[1] Другим речима, сајбер криминал је криминал који се догађа у сајбер простору. Шта је, дакле, сајбер простор?

Иако се термин *сајбер простор* везивао за рад америчког математичара Норберт Винера и његов термин кибернетике, право значење овог термина дао је Вилијам Гибсон у свом роману *Neuromancer* из 1984. године код којег је термин сајбер подразумевао „виртуелно, невидљиво, неограничено, базирано на технологији".[2] Саму синтагму сајбер простор поменути Вилијам Гимбсон посматра као „универзум рачунарских мрежа, свет у којем се мултинационалне компаније, друштва и други субјекти боре за освајање података и информација".[3] Другим речима, сајбер простор је нека врста заједнице која је „сачињена од мрежа рачунара у којој се елементи класичног друштва налазе у облику битова и бајтова, односно, простор који креирају рачунарске мреже".[4] Сајбер простор је дакле онлајн свет рачунарских мрежа, али и дигитални свет уопште. У том свету врше се и кривична дела. У таквом амбијенту, тј. у сајбер простору, криминал се извршава лакше, брже, разноврсније, али и анонимније, у односу на класичне облике криминала. Такође, важно је поменути да је сајбер простор препун различитих могућности. Могућности у

[1] Ј. Матијашевић-Обрадовић, С. Зарубица, Интернет и злоупотребе у сајбер простору, *Европско законодавство*, бр. 67/19, Београд, 2019, стр. 247
[2] Д. Вулетић, Сајбер безбедност, *Интегрална безбедност Републике Србије*, Београд, стр. 174.
[3] Исто, стр. 174.
[4] Исто, стр. 174.

сајбер простору су готово бесконачне. То значи да у сајбер простору постоје различити облици комуницирања, различити садржаји, бесплатне информације, могућности пословања, итд...[5] Ипак, као најзначајнија карактеристика сајбер простора је то што је у питању глобални, транснационални простор и он превазилази територијалну контролу националних држава. Зато Мајкл Бенедикт посматра сајбер простор као „нови универзум, паралелни створен универзум, који је одржаван помоћу 'светских рачунара' и комуникационих линија".[6] Са друге стране, Кевин Хјуз „дефинише сајбер простор као међусобно спојено, окружење посредством компјутера у коме су представљени сви претходно настали медији".[7] Дакле, сајбер простор је једна нова стварност која је настала из рачунарских мрежа, а посебно интернета. Сходно наведеном, може се рећи да је сајбер простор „вештачка творевина која захтева високу техничку опремљеност, добру информациону инфраструктуру која је ничија и свачија својина, у коме паралелно коегзистирају виртуелно и реално и код кога је комуникација колективна".[8]

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

На основу извршеног појмовног одређења сајбер простора може се закључити да се у њему, помоћу субјеката и објеката информационих технологија, спроводе активности које имају и апстрактни, али и конкретни смисао и сврху. Те активности могу бити и

[5] Ј. Матијашевић-Обрадовић, С. Зарубица, нав. дело, стр. 248.
[6] Исто, стр. 248.
[7] Исто, стр. 248.
[8] Исто, стр. 249.

углавном и јесу афирмативне и корисне за појединце или друштво у целини, али могу имати и свој негативни карактер, односно могу наносити штету лицима која учествују у дигиталним активностима у сајбер простору. Ради организације и спровођења мера заштите дигиталне активности, са развојем и применом информационих технологија, настаје и успешно се развија и сајбер безбедност.

Класичном афирмативном дефиницијом, сајбер безбедност можемо појмовно одредити као скуп организационих, техничких и оперативних мера људске делат- ности у сајбер простору, усмерених на заштиту сајбер инфраструктуре и материјалне и нематеријалне имовине појединца, група и заједница. На основу ове дефиниције, може се уочити да сајбер безбедност обухвата: мере заштите формиране на основу корисничких упутстава за употребу сајбер алата (организационе мере), мере заштите уграђене кроз сам производни процес дизајнирања хардверских, софтверских и дигиталних комуникацијских информационих решења (техничке мере) и мере заштите коју мора да спроводи сам корисник у току дигиталних активности како би унапредио сајбер безбедност (оперативне мере).

Вера Тасић и Иван Бауер у свом *Речнику компјутерских термина* описују сајбер простор као „окружење виртуелне реалности у коме особе комуницирају помоћу повезаних (умрежених) рачунара”.[9] Слично томе, америчко *Министарство одбране (Department of Defence – DoD)* сагледава сајбер простор као део ширег информационог екосистема. Оно сматра да је у питању подручје информационог система које је састављено од мноштва независних информационих инфраструктура, попут интернета, рачунарске мреже, процесора, контролера, телекомуникационих мрежа.[10] Овакво одређење посебно истиче сложеност и хетерогеност инфраструктуре која омогућава функционисање сајбер простора. Поједини аутори истичу и одређене нетехнолошке карактеристике при дефинисању сајбер простора. Тако Аљоша Мимица и Марија Богдановић сајбер простор виде као специфичну, нову менталну димензију људског

[9] Д. Вулетић, нав. дело, стр. 174.
[10] Исто, стр. 174.

постојања у којој настаје симулирана стварност проистекла из интеракције човека и технолошког интерфејса.[11]

Иако потичу из различитих извора, све наведене дефиниције у суштини повезују појам сајбер простора са рачунарским мрежама као његовим темељним носиоцем. Сајбер простор се може разумети као нематеријално, интерактивно и практично неограничено окружење створено умреженим дигиталним технологијама. Он представља производ технолошког развоја и друштвених потреба, нудећи изузетно широк спектар могућности и делујући као доминантан канал комуникације у савременом информационом друштву. Његов развој довео је до шире појаве дигиталних услуга и производа који су у многим областима заменили своје традиционалне еквиваленте, чиме су омогућени нови модели економских односа и дигиталне трговине. Такође, сајбер простор би се могао упоредити са оним што је некада у античкој Грчкој био *форум* – место окупљања, трговине, итд... Дакле, сајбер простор је дословно вид јавног простора који омогућава индивидуално изражавање и слободно кретање, за разлику од физичког простора ограниченог димензијама, географијом и материјалним препрекама.[12] Тако се данас у сајбер простору стварају нови друштвени односи, образују се форуми, сарађује се, играју се игре, људи се удружују ради пословних подухвата или просто забаве, налазе своје брачне партнере, итд... Ипак, поједини аутори истичу да такве групе не могу у потпуности заменити традиционалне заједнице, док други сматрају да виртуелне заједнице могу допунити и ојачати везе у физичком свету. Неке анализе истичу опасност да претерана укљученост у виртуелне заједнице може довести до смањене повезаности са стварним социјалним окружењем. Ипак, модеран сајбер простор омогућава очување и јачање односа међу људима који се физички ретко сусрећу, што је веома значајно будући да, барем код нас, многи људи одлазе у иностранство на рад, па управо кроз сајбер простор одржавају везу и контакт са својим најмилијима. Међутим, оно што разликује дигиталну од реалне заједницијe јесте то што се у дигиталном окружењу блискост чешће остварује преко заједничких интересовања него преко традиционалних социјалних фактора као што су пол, статус или економски положај. Стога су ове заједнице често хомогене по вредностима и интересима, али истовремено веома разнолике у погледу узраста, порекла и

[11] Исто, стр. 174.
[12] Исто, стр. 175.

друштвених идентитета.[13] Један од најистакнутијих атрибута сајбер простора је изузетна брзина и разноврсност протока информација, што је приметно другачије у односу на материјални простор и класично схватање времена. Такође, поједини аутори сматрају да постоје и друге особености. За Томаса Ериксена, сајбер простор је квалитативно нова појава по томе што је овај простор децентрализован и огроман. Он нема хијерархију нити распоред, он је отворен али то пружа и ризик од експлицитних и проблематичних садржаја. Такође, иако је глобалан и отворен, сајбер простор је могуће користити за ширење свог утицаја. У том смислу битно је поменути енглески језик који је доминантан језик у сајбер простору и на тај начин западне државе могу да имају јачи утицај. Другим речима, сајбер простор је тековина глобализације и самим тим је његова природа глобалистича па утиче на многе области живота, обликује идентитете, обликује забаву, комуникацију, образовање, политичку мисао, свакодневно понашање, итд... Све наведене карактеристике сајбер простора упућују нас на то да је у питању простор где је и те како могућа појава криминала – такозваног сајбер криминала, али о томе у наредном поглављу...

[13] Исто, стр. 175.

III. КРИМИНАЛ У САЈБЕР ПРОСТОРУ – САЈБЕР КРИМИНАЛ

3.1. Појам и дефиниција

Савремено друштво данас у великој мери зависи од информатичких и комуникационих технологија, што је последица њиховог интензивног развоја и све шире доступности. Масовна употреба рачунара и интернета, поред бројних предности, отворила је простор и за нове облике злоупотреба. Могућност слободног приступа огромној количини података омогућила је настанак различитих криминалних радњи у дигиталном окружењу, али и изменила начин извршења већ познатих противправних дела. Сајбер криминал данас представља једну од значајних претњи модерном друштву, али се мора нагласити да интернет није узрок самог криминала, већ средство које омогућава његово манифестовање у новом простору. Технолошки развој је људима приближио информације и ресурсе који су раније били недоступни, чиме су створени услови за формирање специфичног вида криминалитета који се одвија у дигиталном окружењу.[14] Иако се на први поглед чини да је реч о сасвим новој појави, многи облици криминалног деловања у сајбер простору представљају само модификоване форме традиционалних кривичних активности.[15] На тај начин дигитална сфера функционише као нови простор извршења, који се у бројним случајевима преплиће са класичним облицима криминалитета.

Дакле, у сајбер простору догађа се сајбер криминал. Шта је сајбер криминал?

Сајбер криминал представља облик криминалних активности које се одвијају путем дигиталних технологија и комуникационих мрежа. Као такав, сајбер криминал обухвата различите облике противправних радњи у дигиталном окружењу, као што су неовлашћено приступање информационим системима, крађа идентитета, ширење злонамерних програма, фишинг, финансијске злоупотребе и бројне друге активности усмерене на угрожавање података и дигиталних ресурса. При анализи ове појаве важно је правити разлику између сајбер криминала и компјутерског криминала. Компјутерски криминал

[14] Р. Антовић, *Сајбер криминалитет као криминалитет данашњице - научна монографија*, Београд, 2023., стр. 9.
[15] Исто, стр. 9.

најчешће подразумева традиционалне облике противправног деловања у којима је рачунар употребљен као средство или мета извршења, што може укључивати крађу информација, ширење штетног софтвера или нападе на рачунарске мреже. Супротно томе, сајбер криминал обухвата много шири спектар активности које се одвијају у оквиру дигиталних комуникационих мрежа. Он не обухвата само радње усмерене на рачунарске системе, већ и различите облике злоупотреба које се реализују путем интернета, друштвених мрежа, мобилних уређаја и других платформи које функционишу у дигиталном простору.

Радомир Антовић у својој монографији наводи дефиницију *Европске комисије* која каже да сајбер криминал чине „кривична дела почињена коришћењем електронских комуникационих мрежа и информационих система или против таквих мрежа и система".[16] Сајбер злочин се примењује на три категорије криминалних активности. Прва група обухвата традиционалне облике противправног деловања, као што су превара или фалсификовање, али у контексту сајбер криминала односи се на њихово извршење путем дигиталних комуникационих мрежа и информационих система. У другу категорију спадају дела која се тичу дистрибуције незаконитих садржаја путем електронских медија, укључујући материјал који се односи на сексуалну експлоатацију деце или садржаје који подстичу расну нетрпељивост. Трећа група обухвата облике криминала специфичне за дигитални простор, као што су напади на информационе системе, онемогућавање приступа услугама и различити облици хакерских активности. Ови напади могу бити усмерени и на критичну инфраструктуру, што представља посебан безбедносни ризик, јер нарушавање таквих система може довести у питање функционисање механизама за хитно реаговање и проузроковати озбиљне последице по читаво друштво.[17]

Важно је напоменути и чињеницу да је сајбер кримилан повезан са другим гранама криминала. Тако на пример**,** тероризам користи насиље и страх за остваривање политичких циљева, а сајбер простор омогућава анонимност и тешко откривање починилаца. Чланови терористичких организација као што су „Ал Каида" и ИСИС користе интернет за пропаганду, комуникацију и обуку хакера, док аматери учествују ради сензационализма.

[16] Исто, стр. 9.
[17] Исто, стр. 10.

Такође**,** дечја порнографија је кривично дело које се сада односи на лица до 18 година, а интернет омогућава лаку дистрибуцију материјала и експонирање деце. Савремена технологија и мобилни телефони олакшавају снимање и ширење овог садржаја, чиме се повећава ризик од злоупотребе. Поред овога, сајбер простор је везан и за имовински криминал. Када високо-технолошки криминал доноси противправну имовинску корист, она се често легализује кроз прање новца. Сајбер криминал омогућава прикривање порекла средстава и њихову интеграцију у легалне токове.

3.2. Развој сајбер криминалитета у историјском контексту

Као што се логички може закључити, предуслов за сајбер криминал је постојање ИКТ који опет условљава постојање сајбер простора. То нас упућује на чињеницу да је недуго после појаве првог рачунара уследила његова злоупотреба. Наиме, први потпуно функционалан електронски програмски дигитални рачунар био је ENIAC. а како наводи Радомир Антовић „први објављени извештаји о употреби компјутера за вршење злочи-на датирају из шездесетих година прошлог века".[18] Криминал тога доба прилично се разликује од криминала каквог данас познајемо, односно од савременог криминала. Тада још није било интернета, тј. није постојала умреженост рачунара. Такође, рачунари у то доба нису били масовни, као што је то случај данас. У оно време, поседовати рачунар била је права реткост. За рачунар је требала велика просторија, пре свега, а потом и неколико милиона долара, будући да је толико коштао један рачунар. Такође, веома мало људи је могло да приступи главном рачунару, па је самим тим и број људи који су били у позицији да почиње компјутерски криминал, био веома мали. Тај мали број људи који је имао приступ рачунарима унутар компаније у којој су били запослени, а који су учинили злоупотребу - називао се једноставним именом - инсајдер. Инсајдери су, као одговор или као освету на отказ који су добили, шпијунирали друге запослене, саботирали рачунар или податке. Претходно речено представља први облик сајбер криминала, а мотивација за такву врсту криминалне делатности у највећем броју случајева била је метријална користи. Како наводи Радомир Антовић „средином шездестих година 20. векарачуновођа у САД је користио компјутер за проневеру вредну милиондолара. Откривен је тако што је

[18] Исто, стр. 15.

направио намерну грешку и осуђен на 10 година затвора".[19] Од овог случаја, број злопутреба рачунара за финансијски криминал је у порасту. Али, прави проблем настаје оног тренутка какда су се крајем 20. века појавили лични (персонални) рачунари, такозвани PC. Са њиховом појавом, појавили су се и хакери о којима ће више бити речи у засебном одељку. Реч *хакер* је први пут употребљена 1950-их година да опише студенте Универзитета МИТ којима је било дозвољено да користе централни рачунар факултета, и овај појам није био нужно везан за негативно значење већ се односило на људе који су користили рачунаре креативно.[20]

Дакле, од најранијих дана развоја рачунарских технологија, хакери су креирали сопствене програме и размењивали их међусобно. Оснивање ARPANET-a 1969. године омогућило је да се већи број хакера повеже у ширу мрежу, иако је та заједница у то време и даље била малобројна.[21] Ситуација се значајно променила 1979. године када су се на тржишту појавили први масовно доступни персонални рачунари – Apple II, PET 2001 и TRS-80. Продати у више стотина хиљада примерака, они су подстакли нагли пораст броја људи који су се упуштали у хаковање. Убрзо након тога, почетком осамдесетих, појавиле су се и прве познате хакерске афере. Група из Милвокија позната као „414-s" успела је да провали у више рачунарских система и да при том уништи део података, што је довело до њиховог хапшења.

Током деведесетих година 20. века персонални рачунари постали су много јефтинији и доступнији, а заједно са њима ширио се и софтвер који је олакшавао упаде у системе. Како је интернет растао, хакери су добијали приступ огромном броју потенцијалних мета широм света. Паралелно са тим развијао се и читав спектар заштитних механизама, као и институције задужене за борбу против сајбер напада. Један од познатијих хакера из тог периода био је Кевин Полсен (Kevin Poulsen), у хакерским круговима познат као „Мрачни Данте". Још као тинејџер, са свега седамнаест година, 1983. године провалио је и у базу података америчког Министарства одбране. Касније је, након сукоба са законом, ангажован да ради на унапређењу безбедносних система.

[19] Исто, стр. 15.
[20] Исто, стр. 15.
[21] Исто, стр. 16.

Новинари су га у то време описивали као „последњег хакера“, јер је управо у тим годинама хаковање престало да се посматра као интелектуално надметање и све јасније је прерастало у област организованог сајбер криминала.[22]

Треба, наравно, споменути и компјутерске вирусе, који су се иначе појавили 1972. године. Од те године, број вируса расте рапидно. До 1990. било је познато око двестотинак вируса, док је до 2008. та бројка премашила милион. Црви, као још један значајан тип малвера, почели су да се развијају почетком осамдесетих. Један од првих познатијих случајева је и црв који је студент Роберт Морис (Robert Morris) направио 1988. године са идејом да тестира рањивости раних интернет система.[23] Како наводи Радомир Антовић поменути „црв је заразио више од 6000 компјутерских система, односно 10% корисника интернета у САД у том тренутку. Процене су биле да је учињена штета достигла скоро 100 милиона америчких долара”.[24]

Крајем двадесетог века хакерске активности све више прерастају у организовани сајбер криминал. Међу најпознатијим фигурама тог доба био је Кевин Митник (Kevin Mitnick), који је деведесетих година извео серију упада у значајне институције као што су NASA, NATO и бројне војне и научне организације.[25] Ипак, у том периоду делују и такозвани „хакери старе школе“, који у систем упадају из радозналости или личних разлога, док све већи број напада спроводе професионалци са јасном финансијском или политичком (идеолошком) мотивацијом. У том смислу треба поменути случај хакера под називом СМАК. СМАК је хакер који је упадом на сервер провајдера дошао до великог броја кредитних картица. Код њега је приликом хапшења пронађен CD са више од сто хиљада украдених података. Средином деведесетих појављују се и макро вируси – први је био *Concept* из 1995, који се ширио е-поштом и преко интернета и за мање од месец дана стигао до готово свих корисника *Microsoft Word*-а, иако није правио директну штету.[26] Крај деведесетих обележили су малвери, комбијације црва и вируса, попут *Melisse*, која је

[22] Исто, стр. 16.
[23] Исто, стр. 16.
[24] Исто, стр. 16.
[25] Исто, стр. 16.
[26] Исто, стр. 17.

за неколико сати успела да преоптерети мејл сервере широм света и изазове вишемилионске губитке.

Годину 2000. обележио је *Love Bug*, вирус способан да краде лозинке и да за мање од недељу дана зарази више од 45 милиона рачунара. Штета коју је проузроковао процењена је на око осам милијарди долара. Иако је аутор откривен на Филипинима, није осуђен за сам вирус, јер тада још није постојао закон који би такав злочин санкционисао.

После тога уследили су напади малвера као што су *Code Red, Nimda, Slammer* и *Sasser*, од којих је сваки нанео вишемилијарске штете.[27] Малвери све чешће постају производ професионалних програмера, а намера се јасно усмерава на крађу, продају или уцену подацима. Уместо ширења преко е-поште, напади се све више ослањају на заражене веб-сајтове. У другој деценији 21. века сајбер криминал прераста у глобалну, високо исплативу делатност. Процењује се да приходи криминалних група премашују сто милијарди долара годишње. Рачунари и интернет постају средства за преваре, крађе, изнуде и читав низ других противправних радњи. Данас је веома специфична ситуација: хакери нису фокусирани на појединце већ на компаније, посебно након пандемије COVID-19. Како се све већи део пословања ослања на дигиталне системе (услед карантина), криминалне групе добијају више прилика да упадају у мреже, краду податке и ометају рад организација. Само у прва четири месеца 2020. године забележено је скоро милион spam порука и више стотина малвер инцидената.[28]

Али, ми данас не смемо заборавити мобилне телефоне. Данас су мобилни телефони у употреби више него рачунари и готово свака особа на земљи их има. То је променило и мету напада. Мете су данас највише паметни телефони јер и они као и рачунари могу бити заражени вирусима, црвима и тројанцима. Пад цена телефона, заједно са брзим растом броја корисника, створио је ново и веома профитабилно поље деловања за сајбер криминалце. Поред телефона, велика популарност уређаја као што су паметни сатови, фитнес траке и таблети додатно је проширила „простор напада“. Сви ови уређаји су повезани на интернет и комуницирају једни са другима, што омогућава да се инфекција са

[27] Исто, стр. 17.
[28] Исто, стр. 17.

једног пренесе на читаву мрежу. Управо та међусобна повезаност олакшава злоупотребу – од крађе података до преузимања контроле над уређајем. Савремени корисници у својим телефонима чувају огромну количину осетљивих података – од банковних информација, е-банкинг апликација и лозинки, до личних фотографија и докумената. Многи користе и апликације за мобилна плаћања или вођење финансија. Са становишта криминалаца, то значи лак приступ вредним подацима које могу злоупотребити за финансијску добит, крађу идентитета или даље ширење малвера.

3.3. Подела сајбер криминала

Радомир Антовић, када говори о сајбер криминалу, дели га на две групе:

- Сајбер криминал против државе, и на
- Сајбер криминал усмерен на приватни сектор.

3.3.1. Сајбер криминал против државе

Сајбер тероризам је концепт који се јавља крајем 20. века као резултат сајбер револуције која је покренула питања о безбедности информација и могућности терориста да користе интернет за своје активности. „Већ 1991. године амерички *National Research* Council је упозорио да будући терористи могу учинити више штете тастатуром него бомбом”.[29] Безбедносне службе дефинишу га као „планирани, намерни, политички мотивисан напад на информације, комјутерске системе и податке са циљем изазивања страха и претње насиљем цивилима”, да би дефиниција била допуњења временом са следећом констатацијом: циљ сајбер напада је да се угрози пружање услуга, створи конфузија и неизвесност унутар циљне популације како би се утицало на владу и становништво да прихвате одређену политичку, друштвену или идеолошку агенду”.[30] Овај облик тероризма се разликује од конвенционалног јер укључује офанзивне могућности информационих технологија које могу деловати самостално или у комбинацији са другим средствима, а мрежа постаје средство које олакшава сајбер напад. Мете могу бити разне,

[29] Исто, стр. 44.
[30] Исто, стр. 44.

могу се напасти информације, базе података, па и доступност услуга. Напади на ове елементе могу изазвати губитак поверења у ИКТ и државне институције, уз директан утицај на функционисање енергетског сектора, здравствених служби и других виталних процеса. Један од раних примера је „хакерски упад у базу података болнице за време конфликта у Нагорно-Карабаху 1999. године", кад су хакери „изменили крвне групе у картонима пацијената како би се угрозила безбедност трансфузије".[31] Сајбер тероризам је привлачан за терористе јер се изводи без оружја и економичнији је од конвенционалног, а истовремено ови напади привлаче већу медијску пажњу захваљујући начину извршења.

У сајбер свету, критична инфраструктура представља главну мету напада јер садржи структуре и функције од виталног значаја за функционисање друштва. Информационо-комуникационе технологије (ИКТ) подржавају рад јавног сектора, здравство, енергију и друге виталне системе, а грађани се све више ослањају на њих, па је очување и јачање безбедности ИКТ-а веома значајно. Поред ИКТ-а, веома су важни енергетски системи. Они су идентификовани као критична инфраструктура јер стабилно снабдевање енергијом омогућава економски раст, али њихова дигитализација повећава изложеност сајбер нападима. Колико је ово значајан сектор сведочи и сајбер напад на украјинску електроенергетску мрежу, 2015. и 2016. године или сајбер напад на петрохемијску фабрику у Саудијској Арабији у августу 2017. године.[32]

Сајбер ратовање је савремени облик конфликта који користи информационо-комуникационе технологије као средство за постизање војних, политичких и психолошких циљева. У медијском рату „злоупотребљавају се информације, а дезинформацијама и лажима манипулише се ради остваривања неоколонијалних циљева и интереса великих моћних земаља".[33] Нове технологије у комбинацији са когнитивним техникама омогућавају да масовни медији постану „високо ефикасно психолошко оружје."[34] ИКТ су омогућиле да појединци и групе имају утицај који је раније био резервисан само за државе и велике институције. Тако су терористичке организације попут Ал-Каиде успеле да добију простор и прилику те се укључе у глобалну комуникацију. На платформама, тј. на

[31] Исто, стр. 46.
[32] Исто, стр. 47.
[33] Исто, стр. 51.
[34] Исто, стр. 51.

интернету се обесмишљава дипломатија јер се сада и недржавним актерима олакшава утицај на унутрашњу политику других земаља.

Али, сајбер ратовање има и свој садржај. Медијска пропаганда представља управо тај садржај хибридног ратовања. Сајбер рат се дефинише као чин „ратовања у сајбер простору или кроз сајбер простор," користећи ИКТ за постизање ефеката у физичком, информационом и сајбер простору.[35] Сајбер трупе, које делују у интересу влада или политичких партија, манипулишу јавним мњењем кроз видео садржаје, мимове и лажне вести. а недовољан капацитет држава за откривање напада, идентификацију нападача и благовремену реакцију повећава рањивост.

Код нас је данас актуелна тема ботова. За многе се тврди да имају своје ботове који "ботују" у сајбер простору у корист онога који их је ствари. Ти ботови су аутоматски налози, или просто плаћени људи, који подржавају пропагандне поруке или масовно се боре против порука које су за власт неприхватљиве. Они тако креирају тренд. Током протеста у Кини, власт је тако користила бот налоге и пропаганду. Побуњенике тј. демонстранте власт је кроз медије представила као терористе који су под утицајем запада. На твитеру је отворено јако пуно налога да подрже ову пропаганду. И тако је пропагандни рат против сопственог народа успео, а Твитер (данас мрежа Икс) је обуставио промоцију огласа на мрежи од стране државних медија.[36]

Када говоримо о анти-државним нападима у сајбер простору, важно је поменути и сајбер шпијунажу. У најширем смислу, сајбер шпијунажа подразумева прибављање поверљивих информација од различитих субјеката, укључујући државе, организације и појединце, са циљем остваривања политичких, војних или економских користи, уз употребу недозвољених метода у дигиталном окружењу.[37] Ова активност је континуирана и спроводе је сајбер организације различитих земаља које настоје да хакују системе потенцијалних противника. Међутим, „то не представља вандализам, већ подразумева професионалну активност којом се откривају информације од значаја на стратешком

[35] Исто, стр. 51.
[36] Исто, стр. 54.
[37] Исто, стр. 54.

нивоу противника".[38] Најактивније у овом домену су велике светске силе попут Сједињених Америчких Држава, Кине и Русије.

Поред шпијунаже, имамо и организовани сајбер криминал. У питању је деловање криминалних група које користе ИКТ за извршење злочина, укључујући интернет коцкање, преваре са кредитним картицама или нападе на критичну инфраструктуру. Групе могу бити потпуно онлајн, хибридне (онлајн и офлајн) или искључиво офлајн уз подршку ИКТ-а. Сајбер криминал је све више доступан као услуга („cybercrime-as-a-service"), где се хакери ангажују за нападе, одбране система или шпијунажу, а клијенти могу бити владе, корпорације или појединци. Ове групе развијају различите услуге, укључујући крађу идентитета, дизајн малвера, рансомвар, DDoS алате, прање новца и криптовалуте, као и прикупљање и продају поверљивих информација. Важно је наравно поменути и хактивисте, тј. хактивизам који представља спој хаковања и активизма, често са мањим последицама и ретким гоњењем. Групе попут Anonymous-а користиле су DDoS нападе, крађу и објављивање података током протеста и друштвених покрета.

3.3.2. Сајбер криминал усмерен против приватног сектора

Као и државни сектор, тако је и безбедност приватног сектора на удару. У овом смислу није згорег поменути филм *IT*, у којем Бирс Броснан игра главну улогу. Наиме, он води авиокомпанију, међутим, запошљава хакера који задобија поверење због начина на који се представио, а када дође до првих несугласица између њих двоје, хакер почиње да се свети тако што упада у мрежу и уништава му компанију. Тако, у приватном сектору, сајбер криминал може да подразумева:

- крађу података,
- крађу ресурса и услуга,
- фалсификовање,
- пиратерију,
- шпијунажу и надзор,
- манипулацију информацијама,
- разне преваре.

[38] Исто, стр. 55.

Када већ говоримо о авиокомпанијама, није згорег поменути и *British Airways* који је био мета напада на безбедносни систем, при чему су украдени подаци везани за 380,000 трансакција. Појединци су такође често на удару тако што хакери покушавају да упадну у њихове телефоне, украду им картице, итд...

Такође, није згорег поменути и пиратерију. Пиратерија је на друштвеним мрежама широко распрострањена, углавном због функција апликација које олакшавају дељење и недостатка техничких ограничења за ширење нелегалног садржаја. Иако закон забрањује ову активност, платформе за друштвене мреже и даље омогућавају лако распрострањивање пиратског музичког, филмског, видео или сличног материјала, што представља озбиљну претњу за ауторска права. Многи корисници интернета посећују сајтове као што су BitTorrent, IsoHunt, PirateBay итд, и на њима преузимају садржај за који би иначе морали да плате, па тако бесплатно преузимају, односно даунлоадују, филмове, музику, серије, итд...

Када говоримо о крађи података, можемо споменути америчку компанију Yahoo која је два од највећих цурења података у историји између 2013. и 2014. године. Посебно је проблематично што је компанија знла за цурење података али их је чувала у тајности. Прво цурење догодило се у августу 2013. године на Yahoo серверима и погођени су сви кориснички налози, укупно три милијарде. Друго цурење 2014. године обухватило је више од 500 милиона налога. Оба инцидента укључивала су имена, адресе е-поште, бројеве телефона, датуме рођења и безбедносна питања – и у шифрованом и у нешифрованом облику. Због ових инцидената, четири особе су оптужене за учешће у другом цурењу, укључујући канадског хакера Карима Баратова, који је осуђен на пет година затвора.

3.3.3. Остали облици сајбер криминала или Сајбер криминал усмерен против грађана

Будући да смо према Антовићевој класификацији рекли реч више о сајбер криминалу против државе и привантог сектора, одлучили смо да у оквиру овог поглавља додамо још једно, а то је управо оно које ће се бавити осталим облицима (онима који нису поменути) сајбер криминала или оним који је усмерен против грађана. То чинимо из разлога што је овај сегмент сајбер криминала веома важан. Наиме, сајбер криминал усмерен против грађана обухвата све врсте незаконитих активности које угрожавају личне

податке, приватност, имовину или безбедност појединца, као што су крађа идентитета, финансијске преваре, онлајн узнемиравање, лажни и хаковани профили, малвер и онлајн сексуално злостављање. Неке од ових облика већ смо споменули у самом раду, а неке ћемо тек споменути у даљем тексту. Услед тога, у овом делу раду, тј. у овом поглављу рећи ремо реч више о дигиталном насиљу, приватности и угрожавау личних података. Наиме, можемо рећи да су често приватна лица на удару на друштвеним мрежама као што *су Facebook, Instagram, X, TlkTok*, итд. Злопутреба друштвених мрежа дефинише се као „девијантно понашање које се састоји у нелегалном коришћењу друштвених мрежа противно правилима о заштити приватности, протоколима о електронској комуникацији, препорукама и утврђеним правилима која постојена друштвеним мрежама, чиме се друштву и појединцима корисницима друштвених мрежа, али и онима који то нису, наноси материјална и нематеријална штета".[39] Због све већег и лакшег приступа личним подацима корисника, често долази до њихове озбиљне злоупотребе. Неретко, појединци који се баве програмирањем или неовлашћеним упадима у системе успеју да наруше безбедност и корисника и администратора мрежа. Посебно су рањиви малолетници, па многе платформе уводе посебне механизме који им омогућавају безбедније коришћење сервиса. У последње време све су учесталији напади усмерени на нарушавање приватности, са циљем да се лични подаци злоупотребе. На основу таквих података могу се утврдити различити аспекти нечијег живота – од свакодневних навика и кретања, до личних обележја и припадности одређеним групама – што у крајњој линији омогућава стварање детаљне слике о било ком кориснику. Многи критичари данас сматрају да приватност, услед горепоменутог, више и не постоји. Према њима, приватност је мртва. Приватност је мит. Само привилеговани имају потпуну приватност. Како наводи Вида Вилић: „интересантан пример могуће злоупотребе друштвене мреже за извршење неког другог кривичног дела представља објављивање података 2010. године на интернет порталу www.PleaseRobMe.com[40], где је приказан преглед свих профила корисника друштвене мреже Twitter који су отишли на одмор, на викенд или н апосао и оставили свој дом празан. Циљ оснивача овог сајта био је да покаже корисницима сајтова за друштвено умрежавање како њихов дом може лако бити опљачкан због информација које пласирају

[39] В. Вилић, Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета, Универзитет у Нишу, Правни факултет, Ниш, 2016., стр 107.
[40] Што у преводу значи: Молим те, опљачкај ме (прим. аут.)

преко друштвене мреже, да упозоре људе на последице које могу да имају информације које остављају на Интернету, а не да ти корисници буду опљачкани."[41]

Потребно је, наравно, поменути и дигитално насиље. Дигитално насиље се још назива и електронско насиље или интернет насиље, али и cyberbulling. Дигитално насиље, сајбер насиље или cyberbullying је сваки вид насиља које које настаје употребом дигиталних технологија. Дигитално насиље је нешто са чиме се свакодневно сусрећемо, а да ни не приметимо да је реч о насиљу и злостављању које треба санкционисати и спречити, поготово када су у питању деца и дигитално злостављање међу њима. Дигитално насиље може се испољити на више различитих начина, а најчешћи облици укључују cyberbullying, злоупотребу личних података, узнемиравање, претње, уцене, говор мржње, злоупотребу фотографија, лажне или хаковане профиле, дечију порнографију, онлајн сексуално злостављање и интернет преваре. А оно што је важно јесте да као траг остаје дигитални запис и стога је могуће говорити о дигиталном насиљу када говоримо о криминалу у сајбер простору. Међутим, посебно се данас усмерава пажња на сексуално дигитално насиље. У сајбер простору најчешће се као облици сексуалног насиља јављају *родно засновано злостављање* и *нежељена сексуална пажња*, док је *сексуално задовољење* ретко због немогућности физичког контакта. *Узнемиравање* на интернету може укључивати слање претњи, фотографија или личних података жртве, објављивање адреса или других информација с циљем застрашивања и повреде особе.

Када говоримо о родно заснованом злостављању у сајбер простору, можемо говорити о више облика узнемиравања. Активно сексуално узнемиравање манифестује се кроз слање увредљивих порука сексуалног карактера. Пасивно, са друге стране, изгледа мање наметљиво, а суштина је да се злостављач не обраћа дикретно, већ својим надимком или корисничким именом вређа морал. Активно графичко сексуално родно засновано узнемиравање подразумева слање еротских или порнографских садржаја путем различитих платформи, а пасивно значи објављивање таквог садржаја а не директно слање.

[41] Исто, стр. 108.

Када говоримо о нежељеној сексуалној пажњи у сајбер простору можемо споменути да она укључује директну вербалну комуникацију са циљем успостављања сексуалног контакта, било виртуелног или реалног, често уз наношење емоционалне патње жртви. Сајбер сексуална принуда подразумева коришћење онлајн канала за наметање сексуалног контакта, где жртва осећа притисак и страх од последица.

Када пак говоримо о сексуалном насиљу у сајбер простору, можемо истаћи да сексуално насиље може да се јави као „порнографија из освете“, када се без сагласности жртве објављују њене експлицитне фотографије или видео снимци, често са именом, бројем телефона или радним местом, а понекад и у циљу уцене. Најчешће су жртве жене, а снимци настају различитим начином – добровољно, тајно снимање или крађа путем упада у рачунаре и телефоне. Ризично понашање које може довести до сајбер сексуалног злостављања укључује секстинг (размена интимних порука и фотографија) и сајберсекс (симулацију сексуалних односа путем технологије), јер материјал постаје потенцијално видљив свима, може бити трајно доступан и подложан злоупотреби, укључујући објављивање на порнографским сајтовима.[42]

Посебно треба споменути сексуалну експолатацију и сексуално злостављање деце у сајбер простору. У савременом електронском добу, деца све више времена проводе за рачунаром и на интернету, који им, поред забавних и едукативних садржаја, доноси и бројне опасности скривене у облицима онлајн дружења. Вера Вилић наводи податке *Националног центра за несталу и злостављану децу* који показују да је око једно од седморо деце узраста од 10 до 17 година било изложено нежељеној сексуално експлицитној комуникацији или онлајн сексуалном злостављању.[43] Овај облик девијантног понашања у сајбер простору испољава се у четири облика:

- *Дечија порнографија* - обухвата сваки визуелни приказ, укључујући и дигитално генерисане форме, у коме је дете представљено на сексуализован начин или у контексту који има сексуалну конотацију, без обзира да ли је ситуација стварна или симулирана.

[42] Исто, стр. 159.
[43] Исто, стр. 164.

- *Груминг (Grooming)* представља процес у коме одрасла особа намерно гради поверење и емоциону блискост са дететом како би створила услове за каснију сексуалну злоупотребу.
- *Сексуални туризам усмерен на децу и дечија проституција* добијају нову димензију у сајбер простору, где интернет постаје средство за рекламирање и посредовање у незаконитим сексуалним услугама које укључују малолетнике.
- *Излагање детета непримереним садржајима на интернету против његове воље* честа је последица широке доступности порнографије у дигиталном простору. Деца се са таквим материјалом могу сусрести ненамерно па тако виде садржаје који нису прикладни за њихов узраст..

Када говоримо о грађанима, они често могу бити и жртве прогањања у сајбер простору. У традиционалном криминалу, прогањање и сексуално узнемиравање захтевало је близак физички контакт али је интернет омогућио да се ова врста злочина догађа и у виртуелном свету. „Прогањање путем коришћења интернет мреже дефинише се као упорно и циљано злостављање појединца путем електронских начина комуникације или као употреба нових технологија у циљу прогањања неке особе".[44] Сајбер прогонитељ надгледа активности жртве, проналази податке о њој, контактира људе са којима је жртва блиска, све у свему, прогонитељ прати online активност своје жртве а жртва постаје уплашена и несигурна. На тај начин прогонитељ стиче моћ и контролу над жртвом и може да је злупотреби. Интернет прогањање може да се јави у два основна облика. Први подразумева прогањање које се у потпуности одвија онлајн, без било каквог физичког контакта, најчешће кроз слање порука, учешће у причаоницама, форумима, блоговима или на друштвеним мрежама, док други облик представља мешовити модел, а овај облик започиње у виртуелном простору, док временом прелази и у стварни свет, када прогонитељ покушава да успостави лични контакт са жртвом, или обрнуто – када особа која је у реалности изложена прогањању бива настављена да се прати и онлајн.[45]

[44] Исто, стр. 127.
[45] Исто, стр. 131.

IV. САЈБЕР ПРЕТЊЕ

Сајбер претње су различити облици напада и опасности у дигиталном окружењу који могу угрозити интегритет, поверљивост и доступност података.

4.1. Класификација претњи у сајбер простору

Сајбер претње класификују се, према Ненаду Путнику, на следећи начин:

- „Сајбер напади
    - Сајбер напади уз коришћење обмане (социјални инжењеринг и сајбер напади техничког типа и фишинг)
    - Сајбер напади техничког типа (напади помоћу малициозних програма — malwer, напади усмерени на опструкцију услуга — Denial of Service или Distributed Denial of Service)
- Злоупотреба сајбер простора као средства масовне комуникације
    - Информационо ратовање
    - Пропаганда
    - Психолошки рат
    - Обавештајна делатност.”[46]

4.1.1. Сајбер напади

Сајбер напади техничког типа

У дигиталном окружењу могу се уочити различити облици угрожавања безбедности, који се у најширем смислу могу сврстати у две основне групе. У прву спадају ненамерне рањивости настале као последица грешака приликом развоја софтвера. Такви пропусти, иако релативно ретки, могу омогућити неовлашћеним лицима приступ подацима који би морали бити заштићени и поверљиви, чиме се индиректно ствара простор за злоупотребу. Другу, много распрострањенију групу чине намерно креирани штетни програми чији је циљ нарушавање функционалности информационо-комуникационих система или компромитовање података. У ову категорију спадају различите врсте малвера, као што су вируси, црви (worms), тројански коњи, „споредна

[46] Н. Путник, *Сајбер простор и безбедносни изазови*, Београд, 2009., стр. 73.

врата“, затим програми за нежељено оглашавање (adware), ботови, отмичарски софтвер и шпијунски програми (spyware).

Вирус представља врсту злонамерног програма који се везује за извршне датотеке и приликом њиховог покретања умножава се тако што инфицира друге датотеке, истовремено извршавајући активности које могу нанети штету систему. Поред механизма саморепликације, поједини вируси садрже и додатне елементе[47]:

- Механизам активације, односно скуп услова на основу којих вирус процењује када ће покренути своје деструктивне функције;
- Једну или више компоненти задужених за извођење штетних радњи, као што су брисање података, оштећење диска, приказивање непожељних порука или друге форме ометања нормалног рада система.

Тројански коњ је облик малвера који се представља као легитиман програм, а након инсталације прикрива своје деловање и омогућава нападачу приступ осетљивим подацима, као што су лозинке или информације о банковним рачунима. У појединим државама, попут САД и Аустралије, овакви програми се уз судско одобрење користе и у оквиру полицијских истрага, како би се прикупили докази у случајевима високотехнолошког криминала.

Црви представљају самосталне злонамерне програме који користе рањивости софтвера или оперативног система како би се ширили. Најчешће се дистрибуирају путем електронске поште, а након активирања умножавају се и шаљу своје копије другим рачунарима у мрежи, без икаквог учешћа корисника. Њихово деловање углавном доводи до преоптерећења мреже и успоравања њеног рада.

Споредна врата су посебан тип злонамерног софтвера који се обично комбинује са тројанцима или црвима. Њихова функција је да омогуће тајни приступ зараженом систему, заобилазећи уобичајене механизме заштите. На овај начин нападач може преузети

[47] Д. Тепавац, *Заштита пословних информација у функцији националне безбедности*, Београд, 2018., стр. 144.

контролу над системом, често само на основу познавања IP адресе уређаја на који је тај канал приступа инсталиран

Постоје различити програми који се користе за неовлашћено праћење активности корисника:[48]

- Adware представља софтвер који без дозволе корисника приказује рекламе на рачунару, генеришући приход за његовог аутора. Често се дистрибуира као тројанац или црв и може се инсталирати различитим каналима.
- Spyware је злонамерни програм намењен прикупљању информација о кориснику и његовом понашању на рачунару. Може бележити посећене веб сајтове, електронску пошту, па чак и откуцане карактере на тастатури, чиме открива лозинке и личне податке. Сакупљене податке могу примити централни сервери и злоупотребити их. Често се крију у бесплатним програмима, најчешће играма, и праћење корисника се реализује без његове свести.
- Spam се односи на нежељене поруке, најчешће рекламног карактера, чијим слањем спамери остварују профит. Ове поруке ометају рад корисника и могу бити средство за крађу идентитета, јер се шаљу у име невиних особа или организација.
- Лишавање услуге (DoS) и дистрибуирано лишавање услуге (DDoS**)** представљају нападе усмерене на онемогућавање приступа рачунарским услугама, мрежама или ресурсима. Напад се фокусира на доступност информација, а не на њихову поверљивост или садржај, и обично погађа системе који обезбеђују функционалност, као што су сервери електронске поште.

Сајбер напади уз коришћење обмане

Неки од најизраженијих облика сајбер напада уз коришћење обмане су:

- *Мрежна крађа идентитета — Фишинг* (енгл. *Phishing*) „користи се за описивање илегалног прикупљања осетљивих информација обманом (бројеви кредитних картица, корисничка имена, лозинке, PIN кодови и слично), при којој се нападач представља као неко вредан поверења и као неко ко има право и потребу за таквом

[48] Исто, стр. 144-145.

врстом података (нпр. лажне поруке наводно послате из банке или друге финансијске организације)".[49] Нападач на овај начин може слати лажне поруке користећи измишљено име, представљајући се као банка или нека друга установа. Фишинг се, у већини случајева, може лако уочити ако корисник има основно познавање рачунарских система. Пре свега, такве поруке одликује захтевање личних података, наглашавање хитности, коришћење лажираних линкова, тело поруке које је често у облику слике, као и разна нереална обећања и слично.[50] „Спровођење Фишинг напада врши се коришћењем различитих техника, маскирање URL адреса, пресретање комуникације, пропусти у web-апликацијама, лажиране HTML email поруке."[51] Како наводи Кристина Кишановић у свом дипломском раду: „напад се започиње тако што нападач настоји да усмери жртву ка одређеној интернет страници и на њој оставља личне поверљиве информације. На тај начин нападач преузима идентитет жртве, да би извршио незаконите радње односно незаконите финансијске трансакције. Мета напада трпи значајне финансијске губитке, а исто тако и губитак електронског идентитета".[52] Заштита од ове врсте напада пре свега обухвата едукацију корисника, примену јаче корисничке аутентификације, пажљивији приступ безбедности при развоју веб-апликација, унапређење сигурности имејл налога, као и коришћење дигиталног потписа у електронској пошти.

- Као што је крајњи циљ фишинга долажење до одређене информације, исто тако је то и крајњи циљ социјалног инжењеринга. У питању је напад којим се заобилазе различите заштите, те власници одају своје лозинке и поверљиве информације нападачу. „Социјални инжењеринг означава врсту напада при којој се нападач не служи информатичким техникама, већ путем комуникација наводи жртву да учини безбедносне пропусте и прекрши норме и процедуре, а да не примети да је изманипулисана".[53] Речју, суштина је да нападач дође до жељени информација у

[49] Исто, стр. 147-148
[50] Пре неког времена сам сведочио једном покушају фишинга, где се нападач представљао као мајкрософт компанија и покушао лажним мејлом да наговори корисника да пошаље своје податке. Нападач је том приликом користио мејл адресу која гласи: rnicrosoft.com. Ако читаоца буни шта је спорно, спорно је у томе што пише rn (RNicrosoft), а не Microsoft, а поменута слова rn изгледају као да пише m.
[51] Исто, стр. 148.
[52] К. Киштановић. *Безбедносне претње у сајбер простору* - дипломски рад, Београд, 2021., стр. 32.
[53] Д. Тепавац, нав. дело. стр. 148.

наизглед необавезном разговору. На тај начин, дошавши до жељених информација, он их користи и пропбија мехизме заштите које је корисник поставио. Реч је дакле о једној врсти манипулације. Углавном се ради о прибављању бројева кредитних картица па се њима врши плаћање украденом картицом на мрежи. Наиме, људски фактор је најслабији део система безбедности и заштите, па стога нападачи често ударају управо на ту карику – на људски фактор. Како наводи Дејан Тепавац: „најчешће методе преваре које се користе у социјалном инжењерингу су уверавање (које се сматра најважнијим предусловом), лажно представљање, стварање одговарајуће ситуације, искоришћавање моралне одговорности, жеља за помагањем и коришћење старих веза из пословних контаката”.[54]

4.1.2. Злоупотреба сајбер простора као средства масовне комуникације

Злоупотреба сајбер простора као средства масовне комуникације може да се поистовети са поглављем који смо већ радили а који се односи на сајбер нападе усмерене против државе. У наставку ћемо видети и зашто је то тако. Наиме, злоупотреба сајбер простора као средства масовне комуникације односи се на злоупотребу сајбер простора због тога што се тим путем деле информације. Информационо ратовање је чест облик злоупотребе сајбер простора. Информационо ратовање представља активност којом се путем информација слабе непријатељи. Насупрот томе, сопственим снагама се да је предност у оном домену у којем се информациона активност спроводила. Тако се информационо ратовање може спровести у многим пољима, као што су поље економије, политике, културе, итд... Стога, да би се иформациони рат добио, потребно је остварити власт над каналима за проток информација. Поред тога, потребно је спроводити пропаганду, односно ширити свој поглед на свет, сопствене вредности и те исте вредности наметати другима. Како наводе Ненад Путник и Милан Миљковић, информационо ратовање спроводи се и у приватном домену, па тако они кажу да „велике привредне корпорације користе интернет да би се обавестиле о пословним кретањима,

[54] Исто, стр. 148-149.

али, исто тако, и да би дезинформисале своје конкуренте. У конкурентским секторима прикупљање података и избор тражених профила противника од изузетног су значаја".[55]

Поред информационог ратовања, када говоримо о злоупотреби сајбер простора као средства масовне комуникације, можемо говорити и о сајбер тероризму (о коме смо већ говорили у једном од претходних поглавља) који се односи на пропаганду и психолошки рат. Наиме, сајбер тероризам се веома често спроводи у областима индустрије (нпр. хемијска, прехрамбена, итд...), водоснабдевања, енергетике, итд... Застрашујућа је чињеница коју наводи Вајман (Weimann): наиме, он „констатује да готово све активне терористичке организације (...) имају по један или више интернет-сајтова, и то, углавном, доступних на неколико језика. Оно што сајбер терористи покушавају да ураде јесте да наруше безбедност како грађана тако и оних институција или субјеката који обезбеђују безбедност и нормално функционисање друштва. Када успеју у овом циљу, отвара има се простор за даље деловање јер је нападнути тада дезоријентисан и нестабилан. Тако се путем сајбер напада шире страх и паника, па и насиље, што је опет погодно да се рат побеђује на неком новом пољу. Како наводи Дејан Тепавац: „путем сајбер простора терористи теже да допру до три аудиторијума:

- постојећих и потенцијалних бораца и подржавалаца,
- међународног јавног мњења које није директно укључено у конфликт, али је заинтересовано за његове кључне елементе,
- непријатељске или противничке јавности."[56]

4.2. Субјекти претњи у сајбер простору

Када говоримо о сајбер криминалцима, потребно је истаћи чињеницу да је присуство починиоца у сајбер криминалу удаљено од места злочина, за разлику од традиционалног криминала где криминалац оставља физичке трагове доказа и присутан је на месту извршења злочина. Сајбер криминалци приступају интернету и са њега врше своје нападе, па тако нападају како персоналне рачунаре обилних људи, тако и корпораије и драве. Сајбер криминалац се крије иза интернета. Жртва може бити било ко. А како

[55] Н. Путник, М. Миљковић, Злоупотреба кибер простора као средства масовне комуникације, *Војно дело*, јесен/2012, стр. 168
[56] Д. Тепавац, нав. дело, стр. 150.

наводи Маја Вукман: „јединствени профил учиниоца кривичног дела компјутерског криминалитета не постоји, али се сви они означавају заједничким називом - хакер".[57] Дакле, „хакер је особа која ствара изван стандардних техничких лимита, користећи сопствене вештине, са циљем да надмудри и креативно превазиђе ограничења која му се намећу, не само у пољима његових интересовања већ и у свим осталим аспектима живота".[58] Са друге стране, оно што хакер чини је хакерски напад, а ти напади „представљају продор у ИС корисника са намером манипулисања и прибављања заштићених података и информација, пословних тајни и других поверљивих података".[59]

Када говори о карактеристикама хакера, Маја Вукман истиче да код хакера „доминирају припадници мушког пола, екстремно су бистри, склони истраживачком и логичком размишљању и увек такмичарски расположени, са сваком успешном реализацијом на тастатури они виде себе као афирмисане ауторитете над рачунаром и над било ким ко је повезан са њим, што им даје осјећај снаге и контроле, теже да се информатичким производима баве површно, имају мало респекта према онима који не знају ништа о њиховој омиљеној теми – компјутеру".[60]

Такође, треба истаћи чињеницу да постоји више врста хакера. Једна од њих су такозвани *крекери* који остварују интерес за искључиво за себе а мотиви напада, поред придобијања имовинске користи, могу бити разни (ширење извитопирених идеја и ставова који су националне, расне, верске природе).

Поред крекера имамо и *хактивисте*, који су већ помињани у нашем раду. Они користе исте технике као и хакери, али су им циљеви другачији и односе са задобијање публике, односно на привлачење пажње јавност ина неки проблем. Дакле, они су хакери и активисти. Хактивисти тако могу да хакују веб сајт неке државе и да окаче на насловну страну паролу која не иде на руку владајућим структурама те државе.

Поред крекера и хактивиста, имамо и *инсајдере*, који су део организације или неке групе, међутим, они делују против те организације, другим речима – делују прикривено,

[57] М. Вукман, *Cyber криминалитет и профилисање починилаца* - мастер рад, Ниш, 2022., стр. 48.
[58] Д. Тепавац, нав. дело. стр., 152.
[59] Исто, стр. 152.
[60] М. Вукман, *Cyber криминалитет и профилисање починилаца*, нав. дело. стр. 48.

као агендији, и раде против ње. Мотови за овакво дело су различити, а неки од њих су просто новац (могуће је да је инсајдер плаћен од неке друге службе или организације), мотив може бити и личан, на пример освета.

Хакере је могуће поделити и по другој подели, која додатно описује разлике које постоје међу њима. Тако познајемо *беле капе, црне капе* и *сиве капе* а основа ове поделе је однос хакера према хакерској етици.

White Hat Hackers (Беле капе) су хакери познати по томе што се придржавају начела хакерске етике. Њихов основни задатак јесте заштита рачунарских система и мрежа. Поред тога, беле капе за свој циљ имају и унапређење безбедносних механизама како би се предупредиле могуће штете настале услед упада у систем. Ови хакери су често ангажовани од стране различитих компанија како би тестирали њихове системе заштите, па се на тај начин откривају начини на које се може извршити сајбер напад. Услед тога, наравно, долази се до спознаје слабости система заштите, те се те слабости отклањају што доводи до тога да се самим тим повећава ниво заштите и гради јачи систем заштите.[61]

Black Hat Hackers (Црне капе) представљају групу хакера, која се - за разлику од претходно поменуте групе белих капа – бави крађом и уништавањем података у рачунарским мрежама и системима. Црне капе хакерску етику тумаче онако како им одговара и често оправдавају своје поступке ставом да све информације треба да буду доступне свима. Током својих упада неретко оштећују делове система. Поред тога, баве се и стварањем и пуштањем штетних програма као што су вируси и црви, који наносе значајну штету корисницима.[62]

Grey Hat Hackers (Сиве капе) представљају групу која се налази између црних и белих капа, као нијанса. То значи да сиве капе настоје да се издвоје од стручњака за безбедност који раде у компанијама, али и да се дистанцирају од штетног деловања црних

[61] М. Вукман, *Cyber криминалитет и профилисање починилаца*, нав. дело. стр. 55.
[62] Исто, стр. 55.

капа. У почецима су неретко нарушавали хакерску етику, али су током времена одлучили да своје знање користе у складу са важећим правилима..[63]

Препознавање разлога због којих се неко упушта у сајбер криминал представља кључни део профилисања починиоца. Иако се чини да је одговор једноставан – да криминалци чине кривична дела зато што су криминалци – у стварности је мотивација много сложенија. Разумевање мотива важно је и за креирање профила починиоца и за доказивање његове кривице. Мотиви могу бити различити: потреба за изражавањем, забава, лична корист или корист за трећу страну, емоционални разлози, политички или сексуални мотиви, па чак и озбиљни психијатријски поремећаји.

[63] Исто, стр. 55.

V. ЗАШТИТА У САЈБЕР ПРОСТОРУ

5.1. Слабе тачке информационо-комуникационих система

Да би се умањио ризик, неопходно је препознати могуће претње и слабе тачке информационо-комуникационог система. Претња представља сваку активност која може угрозити поверљивост, интегритет или доступност података, док се слаба тачка односи на недостатак у систему заштите. Контрола ризика у области ИКТ заснива се на њиховом препознавању, процени и идентификовању извора претњи и слабих тачака, као и на предузимању мера које ће потенцијалну штету у потпуности отклонити или свести на најнижи ниво. Ризиком се сматра могућност настанка губитака или оштећења. Тачке упада могу бити интерне и екстерне. Унутрашње тачке приступа најчешће обухватају системе који нису смештени у контролисаном простору и немају адекватну локалну заштиту. Супротно томе, спољашње тачке приступа везане су за све елементе који омогућавају комуникацију са интернетом – као што су мрежне компоненте, интернет апликације и комуникациони протоколи. Мрежна инфраструктура обухвата каблове, мрежне уређаје и сервисе који омогућавају повезивање рачунара међусобно и са удаљеним системима изван организације. Управо преко тих тачака могућ је неовлашћен приступ мрежи и информацијама које се у њој налазе. Али, често је човек најслабија карика и њега је лакше обманути него ИКТ, али о томе је већ било речи. Због тога је неопходно стално обучавање кадрова. Континуирана едукација, организовање обука и семинара у оквиру организације, као и развијање свести о последицама које непажња или недовољна стручност могу имати по безбедност ИКС-а, доприносе бољој заштити података и умањују ризик од неовлашћеног приступа.

5.2. Спречавање напада и заштита података

У оквиру рачунарских мрежа, ради спречавања потенцијалних напада и заштите података од оштећења, примењују се различити безбедносни сервиси, међу којима су најважнији:

- Аутентификација (authentication);
- Тајност података (data confidiality);
- Непорицање порука (nonrepudation);
- Интегритет података (data integrity);

- Контрола приступа (access control) и
- Расположивост ресурса (resource availability).[64]

Ради унапређења IT безбедности, државни органи и организације, као и приватна предузећа, најчешће се ослањају на шест основних група заштитних мера. Конкретан одабир мера зависи од тога који ниво безбедности је потребно обезбедити:

- софтвер за заштиту од вируса,
- дигитални потписи,
- шифровање (енкрипција)
- заштитни и (противпожарни) зидови и
- прокси сервери.

За постизање високог нивоа заштите подаци се углавном шифрују, тј. врши се енкрипција. Основна сврха шифровања је да информације учини нечитљивим за неовлашћене особе и да их заштити од покушаја дешифровања у случају напада. Процес шифровања се обавља помоћу „случајно генерисаних криптографских кључева“ који обезбеђују сигурност шифрата и отежавају неовлашћен приступ. Кључеви се углавном чувају такође у шифрованој форми.

Пакетски филтери (Firewalls) - представљају системе који не дозвољава појединим типу информације да се креће између непоузданих мрежа (читај: интернет) и мреже корниска. Пакектски филтери могу да буду софтверски, хардверски или њихова комбинација, а функција ових филтера је да блокирају неовлашћени приступ локалној мрежи од стране корисника интернета. Софтверски филтер се користи за кућну употребу, док организације користе сложеније системе.

Системи против злонамерног софтвера (Anti-Malware Systems) – су софтверски пакети који откривају вирусе, црве и друге малциозне апликације. Најбоља заштита је коришћење специјализованих апликација:

[64] Г. Матић, *Основе обраде и заштите података* - Приручник, Београд, 2014, стр. 29.

- Антивирусни софтвер препознаје злонамерне програме упоређивањем са базом антивирусних дефиниција. Редовно ажурирање софтвера је неопходно јер хакери непрестано раде на пробијању у мрежу. Антивирусни софтвер функционипе тако што он препозна претњу, па се кориснику обично нуде опције „обрисати“, „очистити“, „карантин“ или „игнорисати“.
- Програми за детекцију шпијунског кода (Anti-Spyware) откривају spyware, adware и друге апликације које могу угрозити приватност или изазвати финансијску штету. Разлика између антивирусног софтвера и овог програма јесте у томе што је антивирус стално активиран, док се овај програм активира на захтев корисника рачунара.
- Програми за детекцију тројанаца (Anti-Trojan) допуњују антивирусну заштиту откривањем тројанаца, backdoor програма и keylogger-a (програм који бележи редослед коришћења тастатуре), тако да се систем чини отпорнијим на нападе.
- Лични заштитни зид (Personal Firewall) надгледа комуникацију између рачунара и мреже, ограничавајући приступ само на предвиђену употребу и спречавајући злонамерне покушаје преузимања контроле.

VI. ПРАВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР БОРБЕ ПРОТИВ САЈБЕР КРИМИНАЛА

Будући да су већ одређени појмови сајбер простора и криминала, али и да су утврђене претње, време је да се каже реч више о борби против сајбер криминала, а то ће бити учињено управо у овом поглављу. Наиме, ивде ће бити речи о међународним и националним оквирима борбе против сајбер криминала.

6.1. Међународни оквир

Као што је речено на самом почетку рада, ИКТ су условиле глобализам. Та глобална повезаност указује на неминовност глобалне, односно заједничке, односно међународне акције поводом решавања питања и проблема безбедности у сајбер простору. Међународне организације и форуми споревели су низ активности путем скупова, иницијатива, директива, итд... Када говоримо о међународном нивоу сајбер безбедности, важно је споменути Уједињене нације, Европску унију, и друге организације.

Уједињене нације

Уједињене нације имају значајну улогу у развоју глобалних стандарда, политика и механизама сарадње у борби против сајбер криминала и очувању безбедности дигиталног простора. Како је сајбер криминалитет по природи прекограничан и често подразумева актере из више држава, УН представљају кључну платформу за усаглашавање ставова, доношење међународних докумената и подстицање држава да усклађују своје законодавство и институционалне капацитете. „У оквиру ОУН постоје четири главне међународне инситуције, које су укључене у активности постављања законодавних стандарда у сајбер простору. Те институције су следеће:

- Светски самит о информационом друштву;
- Група владиних стручњака за безбедност информација под комитетом Генералне скупштине УН
- Група експерата УН за сајбер криминал и
- Међународна унија за телекомуникације".[65]

[65] Ј. Гордић, Сајбер напади са аспекта међународног и унутрашњег права, *БАШТИНА*, Приштина – Лепосавић, св. 57, 2022, стр. 279.

Светски самит о информационом друштву (WSIS) настао је на основу одлуке Генералне скупштине Уједињених нација. Светски самит о информационом друштву је реализован први пут (прва фаза) у Женеви 2003. године, док је друга фаза била у Тунису 2005. године. Од тада, WSIS Forum се одржава сваке године као међународни дијалог о развоју дигиталног друштва и очувању сајбер безбедности. Овај облик међународног деловања битан је између осталог због тога што је заслужан за усвајање Женевске декларације принципа и Плана акције и за усвајања Туниске агенде за информационо друштво.

Из Генералне скупштине УН настала је и горепоменута *Група владиних стручњака за безбедност информација (UN Group of Governmental Experts – UN GGE).* Поменуту групу чине експерти које именују владе држава-чланица а који имају задатак да анализирају ризике и претње у сајбер простору, да разматрају међународни правни оквир и примену међународног прав ау сајбер простору, али и да формулишу норме, правила и принципе одговорног државног понашања. Ова група формирана је 2004. године а као послебно значајан подвиг треба истаћи да је ова група одговорна за признавање међународног права у оквиру сајбер простора.

Група експерата УН за сајбер криминал (UN Expert Group on Cybercrime) је радно тело Уједињених нација формирано са циљем да анализира, истражи и предложи моделе сарадње држава у борби против сајбер криминала.

„Значају улогу у оквиру Организације уједињених нација имају *Посебне снаге за информационо-комуникационе технологије (United Nations Information and Communication Technologies Task Force – UN ICT TF)* које су формиране новем- бра 2001. године. Основна намена UN ICT TF је да се владама и међународним организацијама обезбеди саветодавна политика ради превазилажења дигиталне поделе на глобалном нивоу”.[66]

Међународна унија за телекомуникације (International Telecommunication Union – ITU), која се налази у Женеви и окупља више од 190 држава чланица, представља специјализовану агенцију Уједињених нација задужену за област информационо-

[66] Д. Вулетић, Одбрана од претњи у сајбер простору, Институт за стратегијска истраживања, Београд, 2011, стр. 57.

комуникационих технологија. Ово тело спроводи широк спектар активности усмерених на унапређење телекомуникационе инфраструктуре, израду и усаглашавање међународних стандарда, као и на подстицање размене техничких решења, стручних знања и иновација између држава.[67]

Европски стандарди и пракса

Када говоримо о Европи и њеном доприносу сајбер безбедности, важно је напоменути правни оквир. „Један од најважнијих међународних докуметната за борбу против сајбер напада, а који је усаглашен са више националних законских оквира, и који побољшава методе истраге и унапређује сарадњу међу земљама по питањима сајбер безбедности је Конвенција о сајбер криминалу".[68] Ову конвенцију, познату и као Будимпештанска конвенција о сајбер криминалу донео је Савет Европе (Council of Europe) 2001. године. Наиме, Савет Европе је међувладина организација са седиштем у Стразбуру, која окупља 46 држава-чланица. Како наводи Јован Гордић „у оквиру ове конвенције проучавана су и идентификована питања као што су државни суверенитет у сајбер простору, легално коришћење сајбер простора и методе и средства борбе против сајбер криминала".[69] Поред Савета Европе, ова конвенција је остварена уз сарадњу САД, Канаде и Јапана. У питању је први међународни документ и први међународни покушај да се дефинишу злочини у сајбер простору и да са се развије политика спречавања одређених кривиних дела у сајбер постору. Потписана је 23. новембра 2001. годиен у Будимпешти а ступила је на снагу 1. јула 2004. године. Све земље могу приступити и једини је обавезујући међународни споразум за област кримилана у сајбер простору. Овај Споразум, тј. Конвенција садржи 4 поглавља и свако поглавље има 48 чланова. Прво поглавље садржи опште дефиниције, друго се фокусира на услађивање националних закона у вези сајбер криминала, трећи говори о међународној сарадњи, а четврто поглавља везано је за потписивање, извршење и ратификовање Уговора. Конвенција дефинише девет кривичних дела у области сајбер криминала, која су груписана у четири главне категорије:

[67] Исто, стр. 57-58,
[68] Ј. Гордић, нав. дело, стр. 280.
[69] Исто, стр. 280.

- Прва категорија обухвата дела против поверљивости, интегритета и доступности рачунарских података и система, као што су неовлашћени приступ, пресретање и ометање података, саботажа система и злоупотреба уређаја.
- Друга категорија се односи на прекршаје извршене уз употребу рачунара, укључујући рачунарске фалсификате и преваре.
- Трећа категорија обухвата кривична дела повезана са садржајем, као што су материјали који се тичу дечје порнографије или расистичког и ксенофобичног садржаја.
- Четврта категорија односи се на прекршаје који се односе на кршење ауторских права.

Поред *Будимпештанске конвенције* важно је поменути *NIS директива (Directive on Security of Network and Information Systems)* – први свеобухватни правни оквир ЕУ за сајбер безбедност. *NIS директива* усвојена је 2016. године, а циљ ове директиве је био да се успоставе минимални стандарди безбедности за критичне секторе као што су енергија, транспорт, здравство и дигитална инфраструктура. *NIS директива* је увела обавезу за државе-чланице да успоставе националне стратегије сајбер безбедности, органе за координацију и механизме обавештавања о инцидентима. Међутим, обзиром на брз развој сајбер претњи и дигиталне трансформације, *NIS директива* је 2022. године замењена *NIS2 директивом*. *NIS2* доноси оштрије стандарде и проширује обавезе на више сектора и организација, укључујући и средња предузећа која управљају критичном инфраструктуром. Директива такође јача надзор и примену прописа, уводи строжије казне и подстиче бољу размену информација и сарадњу између држава-чланица.

Треба, наравно, поменути и *eIDAS регулатив*у која представља уредбу којом су постављена јединствена правила за електронску идентификацију (eID) и услуге поверења широм Европске уније. Поменута регулатива омогућава да државе-чланице безбедно размењују дигиталне податке што има за последицу стварање поверења у сајбер простору. Захваљујући овој регулативи, електронска идентификациона средства се признају преко граница, а приступ јавним и приватним интернет услугама је знатно олакшан.

Дејан Вулетић спомиње *Акциони план* из 2009. године који је усвојила Европска Комисија. Вулетић спомиње да је он аснован је на пет кључних стубова[70]:

- спремност и превенција,
- детекција и реаговање,
- ублажавање последица и опоравак,
- међународна сарадња и
- критеријуми за идентификацију европских критичних информационих инфраструктура у области ИКТ.

Акције планиране овим планом допуњују *Европски програм за заштиту критичних инфраструктура (EPCIP)*, чији је централни део директива о идентификацији и означавању критичних инфраструктура. Директива јасно истиче да је ИКТ сектор посебно важан и да му треба посветити посебну пажњу. Све предложене мере осмишљене су тако да подрже сарадњу полиције и правосудних органа у откривању, спречавању и процесуирању криминалних и терористичких дела која угрожавају критичну информациону инфраструктуру. Европска комисија је 2011. године усвојила саопштење *„Достигнућа и следећи кораци: према глобалној сајбер безбедности“*, у којем се наводе планирани кораци за сваку од акција на европском и међународном нивоу. Посебан акценат је стављен на глобалну димензију реаговања и значај сарадње између држава-чланица и приватног сектора, како на националном, тако и на европском и међународном плану.[71]

До сада смо говорили о правном оквиру унутар ЕУ што се тиче сајбер простора, а сада ћемо рећи реч више о институционалној инфраструктури. У том смислу важно је споменути агенцију под називом *ENISA (European Union Agency for Cybersecurity)* – која има за циљ да пружи подршку државама чланицама у стратешком и оперативном плану за сајбер безбедност. Наиме, ENISA је почела са радом 2004. године а седиште ове агенције је у Грчкој.

Поред агенције ENISA, у оквиру Европске уније значајну улогу у заштити критичних информационих инфраструктура има и *Информациона мрежа за упозоравање критичних инфраструктура (CIWIN)*. Ова мрежа пружа подршку државама-чланицама,

[70] Д. Вулетић, нав. дело, стр. 58.
[71] Исто, стр. 58.

институцијама ЕУ, као и корисницима и оператерима критичних система, омогућавајући размену података о могућим претњама, рањивостима и најбољим мерама за смањење ризика и ефикасну заштиту критичних информационих инфраструктура.

Поред ENISA и CIWIN-а, важну улогу у заштити критичних информационих инфраструктура у Европској унији има и *CERT-EU (Computer Emergency Response Team for the EU Institutions, Bodies and Agencies)*. Овај тим је задужен за откривање, анализу и реаговање на сајбер инциденте који угрожавају ИТ системе институција ЕУ. *CERT-EU* такође пружа смернице и подршку у превенцији сајбер напада, као и размену информација о претњама и најбољим праксама међу државама-чланицама и другим релевантним актерима у области сајбер безбедности.

6.2. Национални правни оквир – Република Србија

Безбедност у сајбер простору најпре је регулисана кроз Закон. Наиме, „Кривични законик Републике Србије у глави Двадесет седмој регулише кривична дела против безбедности рачунарских података. У ову категорију кривичних дела се убрајају следећа кривична дела:

- оштећење рачунарских података и програма (чл. 298.),
- рачунарска саботажа (чл. 299.),
- прављење и уношење рачунарских вируса (чл. 300.),
- рачунарска превара (чл. 301.),
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302.),
- спречавањеи ограничење приступа јавној рачунарској мрежи (чл. 303.),
- неовлашћено коришћење рачунара и рачунарске мреже (чл. 304.) и
- прављење, набављање и давање другим средства за извршавање кривичних дела против безбедности рачунарских података (чл. 304а).”[72]

Поред Законика, важно је истаћи *Одељење унутрашњих послова задужено за високотехнолошки криминал* које спроводи истрагу и спречава кривична дела у сајбер

[72] Р. Антовић, нав. дело, стр. 75.

простору. Постоји и посебно *Тужилаштво за високотехнолошки криминал* који процесуира сајбер кривична дела. Другим речима, у одељењу за високотехнолошки криминал у оквиру МУП-а „обављају се послови и задаци из надлежности Републичког јавног тужилаштва у вези са кривичним делима високотехнолошког криминала, извршавање обавеза преузетих Законом о потврђивању Конвенције о високотехнолошком криминалу, остварује координација рада са посебним одељењем Вишег јавног тужилаштва у Београду за високотехнолошки криминал, као и координација рада са тужилаштвима опште надлежности, а у вези са кривичним делима високотехнолошког криминала."[73] Србија, наравно, будући да је чланица УН, укључена је у поменуту Међународно телекомуникациону унију и друге активности УН. Што се тиче Европског дела, Србија је део иницијатива *NIS* и *NIS2* директива, али и *eIDAS*.

6.3. Националне стратегије САД, Немачке и Велике Британије за обезбеђење сајбер простора

Стратегије обезбеђења сајбер простора представљају оквир за организовање безбедносних мера, утврђивање приоритета и смањење националне рањивости критичних информационих инфраструктура.

У САД, „Национална стратегија за обезбеђење сајбер простора" дефинише приоритете за владина министарства, агенције, локалне власти, приватни сектор и грађане у циљу заштите критичних инфраструктура као што су енергетика, транспорт, здравство, финансије, телекомуникације и владина управа. Стратегија наглашава потребу за динамичким прилагођавањем и сталним ажурирањем мера због брзих промена у сајбер окружењу. Основни циљеви укључују спречавање сајбер напада, смањење рањивости и минимизирање последица у случају инцидента. Приоритети су успостављање националног система за одговор на инциденте, смањење рањивости, обука и подизање свести, заштита владиних система и међународна сарадња.[74]

Велика Британија у својој стратегији сајбер безбедности такође истиче значај интегрисаног приступа, укључујући улогу владе, јавних институција, приватног сектора,

[73] Ј. Гордић, нав. дело, стр. 280.
[74] Д. Вулетић, *Одбрана од претњи у сајбер простору*, нав. дело, стр. 73.

грађана и међународних партнера. Главни циљеви обухватају смањење мотивације и способности нападача, унапређење заштите критичних система, прикупљање обавештајних података и развој компетенција и свести о ризицима. Постављени су и оперативни механизми као што су Уред за сајбер безбедност и Оперативни центар за надзор и координацију реаговања на инциденте.[75]

Немачка стратегија сајбер безбедности наглашава виталну улогу интегритета, доступности и поверљивости података, као и све већу комплексност и рањивост информационих инфраструктура. Основни принципи обухватају свеобухватан приступ, координацију и размену информација. Стратегијски циљеви укључују заштиту критичних инфраструктура, ИТ система у државној администрацији, успостављање националних тела за одговор и саветодавних тела, ефикасну контролу сајбер криминала и развој људских и техничких капацитета.[76]

Све у свему, стратегије се разликују чисто формално, али у суштини све су усмерене на исто. Може се рећи да је свим стратегијама заједничко да се прилагођавају континуираним променама у сајбер простору и да обухватају интегрисан и мултидимензионалан приступ који укључује превенцију, детекцију, реаговање и обуку као основу за осигурање безбедности у дигиталном окружењу.

[75] Исто, стр. 73-74.
[76] Исто, стр. 74-75.

VII. ДИГИТАЛНА ФОРЕНЗИКА

Пре него што кажемо реч више о дигиталној форензици, потребно је написати и коју реч о дигиталној безбедности. Наиме, дигитална безбедност подразумева технологије и процесе који су осмишљени у циљу протекције рачунара, хардвера, софтвера, мреже, података, итд... Дигитална безбедност може бити нарушена, а то се дешава када су „угрожена информациона средства и поверљивост, интегритет или доступност система".[77] Последњих година у свету се све чешће јављају различити облици злонамерних радњи у дигиталном окружењу, које су проузроковале огромну материјалну штету и довеле до трагичних последица по људске животе. Због тога је питање дигиталне безбедности постало једно од кључних усмерења како националних држава, тако и међународних организација, премда је о томе већ било речи у претходним поглављима. Као реакција на пораст кривичних дела која се врше уз употребу високих технологија, појавила се потреба за формирањем нове научне области која би се систематично бавила овим видом криминалитета, као и за успостављањем јасних правних правила која омогућавају ефикасно вођење поступака против учинилаца таквих дела.[78] Отуда се јавила дигитална форензика. Дигитална форензика се као посебна научна област формирала тек крајем деведесетих година, тачније 1999. године, и од тада представља дисциплину која пружа поуздане методе и средства за откривање рачунарских злоупотреба, за правилно чување и управљање електронским подацима, за њихову стручну анализу, као и за стручно представљање дигиталних доказа у судским поступцима.[79] Када се догоди инцидент у оквиру ИКТ система, било да је реч о злоупотреби или неком облику рачунарског криминала, или када постоји потреба да се таква ситуација правилно сагледа и разреше сви њени аспекти, управо дигитална форензика пружа неопходна објашњења и процедуре за његово решавање. Дакле, дигитална форензичка истрага представља поступак који се, ослањајући се на научне методе и савремене технолошке алате, бави обликовањем и проверавањем теоријских претпоставки путем хипотеза, анализирајући при том електронске уређаје који могу служити као релевантни докази у судским процесима. Основна сврха оваквог поступка јесте утврђивање чињеница о противправној радњи, као и

[77] Д. Ружић, *Дигитална форензика - појам, циљ и карактеристике*, специјалистички рад, Универзитет у Београду, Факултет Безбедности, Београд, 2023, стр. 8
[78] В. Кораћ, А. Дилигенски, Д. Прља, *Дигитална форензика*, Београд, 2016., стр. 57.
[79] Исто, стр. 57.

свих битних околности које се односе на починиоца и начин извршења кривичног или прекршајног дела. У том смислу, дигитални доказ подразумева електронски објекат који садржи поуздане податке способне да потврде или оповргну постављену хипотезу.[80]

У оквиру класификације дигиталне форензике, посматрано према врсти објекта који је предмет истраживања, ова област се може разграничити на више потдисциплина. Тако разликујемо[81]:

- форензику рачунарских система,
- форензику мобилних уређаја,
- форензику база података,
- као и форензику рачунарских мрежа, у шта спада и интернет форензика, односно сајбер форензика.

Погледајмо сада шта је дигитална форензичка истрага и како она изгледа. Како наводе аутори књиге *Дигитална форензика* (2016), дигитална форензичка истрага „подразумева прикупљање чињеница и њихову проверу. Затим се формира хипотеза и врше тестирања кроз тражење доказа, који могу да је потврде или оповргну. То може да утиче на промену закључака уколико се пронађу нови докази (што би изазвало и нови циклус обраде доказа)”.[82]

У средишту сваке дигиталне истраге налази се одређени електронски уређај који је био предмет или средство незаконитог деловања. Такав уређај може бити искоришћен тако да осумњичени путем интернета спроведе различите припремне кораке за извршење кривичног дела или обави другу дигиталну активност у виртуелном простору која је у супротности са важећим законским нормама одређене државе или са унутрашњим правилима неког правног лица.[83] То може обухватати, на пример, неовлашћено приступање систему, поседовање или ширење забрањеног садржаја, као и различите облике злоупотребе електронске поште, попут уцена и претњи, или било који други облик сајбер криминала који је већ раније поменут у самом раду. Даље, када надлежни органи утврде да је дошло до противправне радње, они покрећу поступак преткривичне истраге.

[80] Исто, стр. 57.
[81] Исто, стр. 58.
[82] Исто, стр. 68.
[83] Исто, стр. 68.

Дигитална форензичка анализа се у ширем смислу дели на две основне врсте:

- званичне истраге и
- корпоративне истраге.

Званична истрага подразумева испитивање уређаја, алата и метода које је починилац користио приликом извршења недозвољене радње. У оквиру такве истраге утврђује се мотив, дефинише се врста незаконите активности и спроводи се даље кривично процесуирање. Ову врсту истрага спроводе државни истражни органи, који делују као организован тим са јасно одређеним вођом поступка и чији рад захтева постојање судских налога.

Код *корпоративних форензичких истрага*[84] на инцидент најчешће реагује једна особа, а овакви поступци се углавном сврставају у истраге нижег нивоа. Њихов предмет нису кривична дела, већ различите врсте инцидентних ситуација унутар система. У одређеним случајевима могу се посматрати и као нека врста припремне фазе која претходи званичној истрази високотехнолошког криминала. Истрага у оквиру организације спроводи се у контролисаним условима и најчешће обухвата покретање поступка, утврђивање природе насталог рачунарског инцидента и анализу свих доступних података. Прикупљање и предаја дигиталних доказа надлежним државним органима или надлежним службама унутар саме организације могућа је искључиво уз сагласност власника система који је био компромитован и након формалне одлуке организације.

Али, оно што је најзначајније, јесте чињеница да и званичне и корпоративне истраге почивају на истим форензичким принципима и стандардима. Потребно је истаћи и то да постоје различити модели форензичке истраге. Постоје модели истраге физичког места кривичног дела, модели истраге дигиталног места кривичног дела (који користе методологију физичке истраге) и интегрисани модели у којима је рачунар сам по себи

[84] Није згорег поменути компанију Target, у којој се 2013. године десио и био откривен неовлашћени приступ њиховим платним системима, што је покренуло корпоративну дигиталну форензичку истрагу. Наиме, тим поводом, ИТ тим компаније анализирао је логове, активности мрежних уређаја и POS система како би утврдио природу инцидента и идентификовао начин компромитације. Након интерне анализе, Target је предузео мере за јачање безбедности и обавестио надлежне органе, а истрага је служила као пример корпоративног поступка у реаговању на дигитални инцидент.

дигитално место кривичног дела.[85] Истраживање физичког места ослања се на Локардов закон размене материје, где контакт између објеката оставља физичке трагове (нпр. длаке починиоца на месту злочина), док дигитално место кривичног дела садржи трагове активности у систему, као што су привремени фајлови, RAM меморија или подаци на хард диску.[86]

Када говоре о кључним доказима форензичке истраге, аутори књиге Дигитална форензика истичу следеће најважније појмове:

- „*Физички докази* – представљају физичке објекте на основу којих се може утврдити извршење кривичног дела. Могу да докажу везу између починиоца кривичног дела и жртве или везу између извршиоца и самог злочина. Примери физичких доказа су: рачунар, DVD, хард диск, мобилни телефон.
- *Дигитални доказ* – представља дигитални податак који може потврдити рачунарски криминал и доказати везу између починиоца и кривичног дела. Примери дигиталних доказа су: подаци на хард диску (нпр. лог фајл), подаци у меморији мобилног телефона.
- *Физичко место кривичног дела* – представља физичко окружење у коме се налазе физички докази злочина. Окружење где се догодила прва недозвољена активност назива се примарно физичко место кривичног дела, а сва остала физичка места називају се секундарним физичким местима кривичних дела.
- *Дигитално место кривичног дела* – представља дигитално (виртуелно) окружење које чине системски програми, апликације и хардвер у коме се налазе дигитални докази недозвољене активности. Окружење где се догодила прва недозвољена активност назива се примарно дигитално место кривичног дела, а сва следећа дигитална места називају се секундарна дигитална места кривичних дела”.[87]

Све у свему, када говоримо о дигиталној форензичкој истрази, да би она била успешна кључно је обезбедити неколико основних корака. Прво, потребно је утврдити да ли је дошло до недозвољене активности или рачунарског инцидента. У случају званичне

[85] Исто, стр. 76.
[86] Исто, стр. 76.
[87] Исто, стр. 76-77.

истраге, неопходан је судски налог за приступ систему, док у интерним истрагама унутар организације налог није потребан ако постоји важећа процедура коју је запослени потписао. Затим се спроводи форензички одговор на инцидент и правилно прикупљају дигитални докази. Једнако важан је и безбедан транспорт доказа до лабораторије, уз употребу антистатичких торбица, футрола за блокирање wireless сигнала и посебну пажњу код SSD дискова, јер су подложни уништењу услед електромагнетног зрачења.

VIII. ПРАКТИЧНИ ИЗАЗОВИ БОРБЕ ПРОТИВ САЈБЕР КРИМИНАЛИТЕТА – СТУДИЈЕ СЛУЧАЈА

8.1. Global ransomware напад „WannaCry“

Пре него што пређемо на сам напад који је светски познат, рећи ћемо реч више о ренсомвер-у. Како наводе Путник, Милошевић и Цветковић: „Ренсомвер (енгл. ransomware) представља врсту малвера, из поткатегорије уцењивачког малициозног софтвера, који ауторизованом кориснику ограничава приступ рачунарском систему или у њему похрањеним подацима и тражи откупнину како би корисник повратио приступ свом систему и/или подацима. Откупнина се по правилу тражи и исплаћује у криптовалутама, најчешће у биткоину. Трансакцијама у криптовалутама је тешко пратити траг, те је њихово коришћење у функцији очувања анонимности нападача”.[88] Неке варијанте рансомвера у потпуности онемогућавају употребу рачунара тако што на екрану приказују уцењивачку поруку која се не може уклонити без уплате траженог износа. Други типови овог злонамерног софтвера не блокирају сам систем, већ шифрују одређене датотеке а таквим ситуацијама нападачи од жртве захтевају новчану накнаду како би омогућили приступ закључаним, односно шифрованим датотекама. Процене су да се сваких 11 секунди деси један овакав напад. А многе државе и приватне компаније сусреле су се са овим типом напада. Индија је претрпела напад 2017. године, а прептпеле су папад и Велика Британија, Русија, САД, Кина и Канада. Као што је речено, поред националне критичне инфраструктуре, нападају се и велике мултинационалне компаније, као што су Федекс, Нисан, итд...[89] WannaCry представља рансомвер, тј. криптовирус који је напао ОС Мајкрософт виндоуз. Овај сајбер напад је био глобалан и почео је 12. маја 2017. године. Сам напад је погодио преко 150 земаља а било је заражено преко 300.000 рачунара. Као што је већ речено, овај тип вируса тражи новчану накнаду да би се обуставио. Тако је било и у овом нападу у којем су хакери енкриптовали податке, те тражили да се декрипција плати у најпознатијој криптовалути - биткоину. Нападом су биле погођене многе организације и институције. Тако је у Шпанији на удару била компанија Телефоника, у

[88] Н. Путник, М. Милошевић, В. Цветковић, Реномвер као претња безбедности - друштвни и кривичноправни аспекти, *Социолошки преглед*, vol. LVI (2022), no. 1, стр. 328-329.
[89] Исто, стр. 330.

Британији су нападнуте Националне здравствене службе, Дојче банка у Немачкој, итд... Посебно су биле погођене земље истока, као што су Русија, Украјина, Индија и Тајван. Удар је почео на нападом на Велику Британију и њене здравствене установе а одатле се малициозни код проширио на више од 200.000 болничких рачунарских система у 150 земаља.[90] Наиме, овај вирус се широм света рапидно проширио користећи рањивост у Windows системима познату као EternalBlue. Међутим, ширење овог малвера заустављено је када је примећено да вирус, пре него што активира шифровање, покушава да приступи одређеном, наизглед случајно генерисаном домену. Та адреса у тренутку напада није била регистрована. Када је истраживач регистровао тај домен, WannaCry је почео да „верује“ да се налази у контролисаном окружењу (sandbox), па је аутоматски престајао да се извршава. На тај начин је ненамерно активирана килсвич механика која је била уграђена у сам малвер. Другим речима, регистрација тог домена практично је зауставила даље ширење рансомвера. Након тога, Microsoft је објавио хитне закрпе, укључујући и закрпу за старије, званично неподржане верзије Windows-а, како би се спречиле будуће инфекције.

Није згорег поменути и напад који се десио 2020. године у САД. Тада су се десила 92 појединачна напада овим вирусом, такође на здравствене установе. Скоро 600 клиника, болница и институција уоштено је било погођено. Међутим, нису само финансијски губици били последица овог напада. Нападом се компромитовао велики број података о пацијентима па је тако онемогућено њихово лечење, а саме институције нису могле нормално да функционишу.[91] Оно што је важно споменути код ренсомвер напада јесте да он има сличности са традиционалним терористичким нападима будући да се напада цивично становништво, а последица напада може бити нарушавање здравља или чак смрт. На тај начин изазива се страх и паника, па се тако манипулише жртвама те се приморавају да поступе по захтеву нападача. Али, оно што се разликује од традиционалног терористичког напада јесте мотивација нападача. Док је у првом случају крајњи циљ терориста политички или идеолошки, ренсомвер напад се своди на стицање новца.

[90] Исто, стр. 330.
[91] Исто, 331.

8.2. Dark Web операција „Silk Road“

Посебна опасност у сајбер простору прети од стране такозваног даркнета. Наиме, даркнет је на неки начин подземље сајбер простора, а у питању је мрежа домена који нису индексирани. То значи да се они не могу пронаћи преко класичних интернет предраживача (нпр. Гугл). За приступање Даркнету користи се Тор. Тор је систем који омогућава анонимну и заштићену комуникацију на интернету. Путем тора прикрива се локација и активност на интернету. Сам Тор није нелегалан, будући да се он користи у многим државама. Тако је Даркнет, због могућности које пружа, постао простор на којем се тргује различитом незаконитом робом и услугама, укључујући дроге, оружје, фалсификована документа (као што су пасоши, возачке дозволе, картице социјалног осигурања и рачуни за комуналне услуге), као и фалсификовани новац. Поред материјалних добара, преко ових мрежа се такође нуде разноврсне илегалне услуге. Silk Road или Пут свиле је платформа која је била присутна на Даркнету. Пут свиле на Даркнету је покренут 2011. године а служио је управо за илегалну трговину. Поменуту платформу основао је Рос Улбрих, познат под псеудонимом Dread Pirate Roberts. Оно што је занимљиво, јесте да се на овој платформи (исто као и у претходном поглављу код рансомвер напада) биткоин користио као платежно средство. На тај начин је додатно обезбеђена анонимност. Међутим, две године од оснивања ове платформе, Америчка Федерална служба (FBI) је спровела истрагу. Служба је пратила Тор саобраћај, користила техничке пропусте на самом сајту, пратила трансакције и успела да дође до важних информација те да ухапси поменутиг Роса Улбрихта, осуди га на доживотну робију, да угаси сајт, заплени сервер и конфискује велики број биткоина.

8.3. Blackshades и сексуално насиље

Да бисмо се боље упознали са садржајем, потребно је рећи више о појму Blackshades. Наиме, Blackshades је злонамерни тројанац који хакери користе за даљинско управљање зараженим рачунарима. Малвер је усмерен на рачунаре који користе оперативне системе базиране на Microsoft Windows. Према подацима америчких званичника, више од 500.000 рачунарских система широм света је заражено овим софтвером. Један од најпознатијих случајева злоупотребе малвера Blackshades јесте случај америчке тинејџерске Кесиди Вулф. Она је више месеци била на мети нападача Џереда Џејмса Абрахамса (20), који је уз помоћ овог програма тајно приступао њеном рачунару и надзирао је без њеног знања. Абрахамс је у марту 2014. године осуђен на 18 месеци затвора због неовлашћеног упада у рачунарске системе и изнуде. Према подацима тужилаштва у Калифорнији, он је продирао у уређаје више жена – како оних које је познавао, тако и потпуно непознатих, чије је профиле проналазио на Facebook-у. Процењује се да је током две године компромитовао око 150 корисничких налога. „Када би злонамерним софтвером преузео контролу над компјутером жртве, Абрахамс је могао да даљински укључи веб камеру и слика жртву док се пресвлачи, а да то жртва ни не слути. Затим је фотографије које би на овај начин направио користио је да би уцењивао своје жртве претећи им да ће компромитујуће фотографије или видео снимке објавити на друштвеним мрежама ако му не пошаљу своје још интимније фотографије и видео снимке или ако не пристану на петоминутни разговор преко Скајпа (Skype) са њим током кога ће морати даураде све што им нареди”.[92]

[92] В. Вилић, Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета, Универзитет у Нишу, Правни факултет, Ниш, 2016., стр. 160.

IX. УНАПРЕЂЕЊЕ СИСТЕМА БОРБЕ ПРОТИВ САЈБЕР КРИМИНАЛА

Да би очување сајбер безбедности имало смисла, потребно је повећати финансијска улагања и обезбедити стручне људске ресурсе. Стога је веома важно да се едукују кадрови за сајбер безбедност. То значи да је неопходно школовати, регрутовати и задржати стручњаке. Добра пракста у овом смислу је примењена у Сенегалу где је основана Национална школа за сајбер безбедност 2018. године. На овај начин се ојачала одбрана Западне Африке у сајбер простору. Поред тога, јавност треба информисати и подизати свест о претњама у сајбер простору, јер већина људи још увек потцењује ризике и опасности које постоје. Такође, држава треба да појача подршку институтима у истраживањима у области сајбер безбедности. То је неопходно зато што се свет у сајбер простору развија муњевитом брзином, нови млавери, нови проблеми и нови облици претњи јављају се сваког дана, па је неопходно бити у току са временом и дешавањима и имати увек спреман одговор на потенцијалне претње. Дејан Вулетић наводи и да је веома важан корак у унапређењу сајбер безбедности и процена спремости и попис ресурса, како на националном нивоу, тако и код савезника и потенцијалних претњи.[93] Он наводи и да је веома важно да постоји тим за одговор на инцидент који би координирао реакцију на сајбер напад.[94] Тај тим чине стручњаци за информациону безбедност који проучавају рањивости, анализирају мрежне системе и пружају обуку и информације ради унапређења безбедности. Поред државник актера, постоје и недржавни актери у сајбер простору који обухватају представнике цивилног друштва, невладине организације, академске истраживачке групе, медије, приватни сектор, посебно компаније и привредна удружења. Да би заштита била спроведена на најбољи могући начин, неопходно је да сарадња приватног и државног сектора буде на одговарајућем нивоу. Шта више, ова сарадња је од пресудног значаја за очување безбедности. Пример сарадње приватног и државног сектора откривен је када је Евдард Сноуден обелоданио документа која су била државна тајна. Он је открио да су безбедносне службе Велике Британије и Америке спроводиле масовну шпијунажу. Управо је овим државним актерима у овоме помогао приватан сектор, и то Гугл и Јаху - приватне компаније. На овај начин је откривена размена обавештајних података између једне организације и других земаља, међути, углед САД и Велике

[93] Д. Вулетић, нав. дело, стр. 53.
[94] Исто, стр. 53.

Британије у свету је много опао после обелодањивања шпијунаже. Што се тиче технологије, неопходно је користити више слојева заштите: firewall као филтер за овлашћене кориснике, лозинке за идентификацију, енкрипцију да би се спречило одливање података, као и редовно бекаповање и рикавери опције за случај пробоја система. Важно је и стално праћење трендова и претњи на Интернету. Организације као што су *CERT, Internet Storm Center* и *CAIDA* пружају податке и алате за праћење сајбер претњи, док ЕУ развија пројекте попут *Lobster*-а за мониторинг кључне Интернет инфраструктуре. Све у свему, пред нама је велика борба која ће бити непрестана, будући да се сајбер простор сваког дана шири и јављају се нови облици угрожавања безбедности и сигурности.

X. ЗАКЉУЧАК

На основу анализе изложене у овом раду може се закључити да је сајбер простор постао од суштинског значаја за функционисање савременог друштва, али и једно од најризичнијих подручја са становишта безбедности. Другим речима, традиционални облици сузбијања криминалитета, овде нису довољно, већ је потребно унапредити их и додатно развити стратегије и технологију која ће омогућити и потпомогнути поменуто сузбијање криминалитета. Дакле, традиционални облици контроле и заштите тешко могу да се примене у сајбер простори и управо из тог разлога, сајбер криминалитет се развио у један од најзначајнијих изазова модерног доба. Као што смо имали прилике да видим оу раду, сајбер претње су разнолике, технички напредне и често добро организоване. Од малвера и фишинга (пецања), преко рансомвера и DDoS напада, па до сложених криминалних мрежа које делују на дарквеб-у, савремени облици дигиталног криминала показују висок степен прилагодљивости и креативности. Кажем креативности, јер ко би могао претпоставити да ће једног дана бити развијена платформа попут "пута свиле", али за интернет, тј. за дарквеб и да ће ту моћи да се наручују разноразне илегалне активност и и супстанце. Горепоменуте претње попут малвера, рансомвера и других видова напада нарушавају не само приватност и финансијску сигурност појединаца, већ и стабилност институција, функционисање критичне инфраструктуре и поверење у целокупни дигитални екосистем, па самим тим и у државе. О томе нам сведочи и горепоменути напад „WannaCry“ или случај тржишта „Silk Road“ тј. пут свиле,. Два поменута случаја су показала да последице сајбер криминала могу бити огромне — од блокирања болница и јавних установа, преко финансијских губитака, па до ширења организованог криминала у онлајн окружењу. Ипак, ова искуства такође показују да успешан одговор на сајбер претње постоји, али захтева комбинацију правних, техничких, организационих и образовних мера, али и среће! Кажем среће, јер је први напад делимично обесмишљен тако је случајно откривено решење, док је у другом случају - случају црног тржишта - најпре била потребна добра обавештеност – коју су тајне службе Америке успеле да издејствују. Наравно, све ове акције треба да буду потпомогнуте правним оквиром. Он се, наравно, посепено унапређује, али и даље постоје бројне празнине. Брзина технолошких промена је често већа од брзине којом се правне норме могу прилагодити. Поред тога, сајбер криминал по својој природи превазилази националне границе, што ствара потребу

за широм међународном сарадњом, што је делимично и остварено још од оснивања *Будимпештанске Конвенције* 2001. године. Правни оквир и међународна сарадња није довољна, већ је потребно и улагање у модернизацију како дигиталне форензике тако и стручних кадрова како би се развио ефикаснији заштитни систем. Наравно, не смемо заборавити корисника и његову свест. Човек је, као што је то већ речено у раду, најслабија карика у безбедности. Потребно је подићи свест корисика ИКТ-а да неопрезно кликтање, слабе лозинке, непажљиво дељење података могу бити почетак много већег безбедносног проблема. Зато је едукација, иако делује једноставно, један од кључних механизама заштите. Све у свему, радом на свом мастер раду успео сам да схватим и разумем колико је сајбер простор истовремено и прилика и ризик, и колико је важно да се у њему крећемо свесно, а не механички. Оно што ми је најинтригантије, јесте да је је борба против сајбер криминалитета процес који никада неће бити окончан, јер је сајбер простор увек у развоју и увек се појављују нове претње, стога је потребно увек смишљати нове одговоре који ће бити ефикасни.

XI. ЛИТЕРАТУРА

1. Антовић Радомир, *Сајбер криминалитет као криминалитет данашњице - научa монографија*, Београд, 2023, Центар за стратешку анализу;
2. Вилић Вера, *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета*, Ниш, 2016, Универзитет у Нишу, Правни факултет.
3. Вукман Маја, *Cyber криминалитет и профилисање починилаца*, Ниш, 2022, Правни факултет, Универзитет у Нишу;
4. Вулетић Дејан, *Одбрана од претњи у сајбер простору*, Београд, 2011, Институт за стратегијска истраживања.
5. Вулетић Дејан, Сајбер безбедност, *Интегрална безбедност Републике Србије*, Београд, 2017;
6. Гордић Јован, Сајбер напади са аспекта међународног и унутрашњег права, *БАШТИНА*, Приштина – Лепосавић, св. 57, 2022.
7. Киштановић Кристина, *Безбедносне претње у сајбер простору,* - дипломски рад, Београд, 2021., Факултет безбедности, Универзитет у Београду;
8. Кораћ Вањам Дилигенски Андреј, Прља Драган, *Дигитална форензика*, Центар за нове технологије, Београд, 2016.
9. Матић Горан, *Основе обраде и заштите података* - Приручник, Београд, 2014, Канцеларија савета за националну безбедност и заштиту података;
10. Матијашевић-Обрадовић Јелена, Зарубица Сара, Интернет и злоупотребе у сајбер простору, *Европско законодавство*, бр. 67/19, Београд, 2019;
11. Путник Ненад, Миљковић Милан, Злоупотреба кибер простора као средства масовне комуникације, *Војно дело*, јесен/2012, стр. 157-183;
12. Путник Ненад, *Сајбер простор и безбедносни изазови*, Београд, 2009, Факултет безбедности, Универзитет у Београду;
13. Путник Ненад, Милошевић Милан, Цветковић Владимир, Реномвер као претња безбедности - друштвни и кривичноправни аспекти, *Социолошки преглед*, vol. LVI (2022), бр. 1, стр. 328–353;

14. Ружић Душка, *Дигитална форензика - појам, циљ и карактеристике*, специјалистички рад, Београд, 2023, Универзитет у Београду, Факултет Безбедности.
15. Тепавац Дејан, *Заштита пословних информација у функцији националне безбедности*, Београд, 2018, Факултет безбедности, Универзитет у Београду.

САЖЕТАК

Примена информационо-комуникационих технологија суштински мења природу савремене безбедности, трансформишући дигитални простор из платформе за напредак у примарни амбијент за развој софистицираних облика криминалитета. Основна напетост коју овај рад анализира лежи у сукобу између незадрживе експанзивности дигиталних претњи и рестриктивне природе законодавства у вези са сајбер безбедношћу. Док савремени облици криминала (малвери, фишинг, рансомвер, DDoS напади) показују изузетан степен техничке софистицираности, правни поредак, кроз Будимпештанску конвенцију и домаћи Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминалитета, покушава да ухвати корак са динамиком виртуелног простора. Овај сукоб престаје да буде само теоријски у тренутку када асиметричне претње попут „WannaCry" напада паралишу критичну цивилну инфраструктуру или када се у оквиру Дарк веба операционализују платформе попут „Silk Road", претварајући дигитално подземље у глобално тржиште за илегалне супстанце, чиме се de facto забилазе традиционални механизми полицијске контроле и надзора.

Кључни механизам заштите пронађен је у концепту дигиталне форензике и операционализацији вишеслојне одбране система. Савремени безбедносни стандарди, предвођени европском NIS2 директивом, пребацују терет са реактивног деловања на проактивно управљање ризицима. Посебан фокус истраживања стављен је на очување интегритета дигиталних доказа током форензичке претраге. Идентификација, прикупљање и испитивање података са рачунарских система и мрежа морају бити усклађени са најстрожим процедуралним стандардима, при чему класични криминалистички принципи попут Локардовог закона о размене материје добијају нову форму у контексту ИКТ система, омогућавајући материјализацију дигиталног трага на суду.

У домаћем правном и институционалном контексту, рад идентификује специјализоване јединице (CERT) и Национални центар за превенцију безбедносних ризика као примарне бране којима се спречавају масовни инциденти. Међународна кривичноправна помоћ и сарадња између државног и приватног сектора појављују се као

неопходан сигурносни вентил код сузбијања прекограничних напада. Ипак, поред техничких баријера попут заштитних зидова и енкрипције, човек остаје најслабија карика безбедности, што едукацију корисника чини суштинским делом сваког одбрамбеног кода. Борба против сајбер криминалитета мора остати перманентан процес у служби заштите појединца и друштва. Само кроз симбиозу правних норми, техничких стандарда и јачања безбедносне културе може се осигурати да мушевити развој технологије не потисне фундаментално право на личну сигурност, приватност и дигитални суверенитет у модерном добу.

Кључне речи: сајбер криминалитет, сајбер безбедност, дигитална форензика, Будимпештанска конвенција, Дарк веб.

SUMMARY- Cyber space as a new criminogenic environment: Theoretical foundations and practical challenges

The application of information and communication technologies fundamentally alters the nature of contemporary security, transforming the digital space from a platform for progress into the primary environment for the evolution of sophisticated forms of crime. The core tension analyzed in this paper lies in the conflict between the unstoppable expansiveness of digital threats and the restrictive nature of legislation regarding cybersecurity. While modern forms of crime (malware, phishing, ransomware, DDoS attacks) demonstrate an exceptional level of technical sophistication, the legal order, through the Budapest Convention and the domestic Law on Organization and Competence of State Organs in Suppressing High-Tech Crime, attempts to keep pace with the dynamics of the virtual space. This conflict ceases to be merely theoretical the moment asymmetric threats like the "WannaCry" attack paralyze critical civilian infrastructure, or when Dark Web platforms such as the "Silk Road" are operationalized, turning the digital underworld into a global marketplace for illegal substances, thereby de facto bypassing traditional mechanisms of police control and surveillance.

The key mechanism of protection is identified in the concept of digital forensics and the operationalization of a multi-layered system defense. Contemporary security standards, led by the European NIS2 Directive, shift the burden from reactive response to proactive risk management. A special focus of the research is placed on preserving the integrity of digital evidence during forensic examination. The identification, collection, and analysis of data from computer systems and networks must comply with the strictest procedural standards, whereby classic criminalistic principles, such as Locard's exchange principle, take on a new form within the context of ICT systems, enabling the materialization of digital traces in court.

Within the domestic legal and institutional context, the paper identifies specialized units (CERT) and the National Center for the Prevention of Security Risks as primary barriers preventing mass incidents. International mutual legal assistance and cooperation between the public and private sectors emerge as an indispensable safety valve for suppressing cross-border attacks. Nevertheless, alongside technical barriers like firewalls and encryption, the human factor

remains the weakest link in security, making user education an essential part of any defense protocol. The fight against cybercrime must remain a permanent process dedicated to protecting individuals and society. Only through a symbiosis of legal norms, technical standards, and the strengthening of security culture can it be ensured that the rapid advancement of technology does not overshadow the fundamental rights to personal safety, privacy, and digital sovereignty in the modern era.

Keywords: cybercrime, cybersecurity, digital forensics, Budapest Convention, Dark Web.

БИОГРАФИЈА

Дарко Александров је рођен 28.08.1997. године у Врању, Републици Србији. Завршио је основну школу „Бранко Радичевић“ у Врању где је био носилац Вукове дипломе, а након тога је завршио Медицинску школу „др Изабел Емсли Хатон“- смер Зубни техничар, такође у Врању. Након завршене средње школе 2017. године уписао је Факултет за правне и пословне студије „др Лазар Вркатић“ у Нишу – смер Безбедност и криминалистика који је завршио у року дана 17.12.2021. године. Током студирања, био је председник студентског парламетна одсека наведеног факултета у Нишу, где је учествовао у бројним студентским активностима а између осталог учествовао и у процесу реакредитације факултета.

Након завршених студија, 2022. године креће на основну полицијску обуку у Сремској Каменици, и након успешно завршене обуке, у јулу 2023. године постаје припадник Министарства унутрашњиих послова на радном месту Полицајац. Завршио је интерну обуку у МУП-у и сертификовани је полицијски службеник за рад и поступање са малолетним лицима.

Уписао је мастер студије 2023. године на Правном факултету Универзитета у Нишу – смер Унутрашњи послови, са циљем да додатно унапреди своја знања из области правних и других сродних наука.

Дарко Александров
Е-маил: darko.aleksandrov.flv@gmail.com

ИЗЈАВА О ИСТОВЕТНОСТИ ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: _____

Наслов мастер рада:_____
_____

Ментор: _____

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом _____

_____

пријављен и одбрањен на Правном факултету Универзитета у Нишу: • резултат сопственог истраживачког рада; • да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима; • да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: _____

У Нишу, _____

Потпис аутора

_____