МИЛЕНА КОЈИЋ*
Филозофски факултет
Нови Сад

УДК 004:343.9
Монографска студија
Примљен: 25.04.2015
Одобрен: 17.05.2015

ИЗАЗОВИ КОМПЈУТЕРСКОГ КРИМИНАЛА

Сажетак: Циљ овог рада је да расветли проблем компјутерског криминала, да укаже на његову јединственост и специфичан контекст унутар ког се одвија, као и да предложи могуће начине правне регулације у овој области. Феноменолошка разноврсност овог појма отежава разумевање компјутерског криминала као јединствене појаве, а неразликовање од криминала белог оковратника и од традиционалног криминала ствара додатне концептуалне проблеме. Правни инструменти за борбу против сајбер преступништва варирају од државе до државе, а међународна иницијатива превенције и борбе против компјутерског криминала напредује споро у односу на развој технологије и све софистицираније форме испољавања ове врсте криминала. Поред неопходних законских мера у овој области, у раду ће се скренути пажња и на друге начине регулисања понашања у сајбер простору - друштвене норме, тржиште и архитектуру (технологију) виртуелног простора.

Кључне речи: компјутерски криминал, хакери, криминал белог оковратника, виртуелно окружење, правни инструменти, регулатори

Историја интернета је прагматичан пример развоја технологије кроз креативну апропријацију њених корисника [1] Многи рани корисници интернета видели су себе као хакере, међутим хаковање само по себи није имало негативну конотацију каква му се данас придаје (Петровић, 2012). Оригинално, овај израз је био повезан са слободом информација и истраживањем нових технологија, док се данас најчешће односи на врсту компјутерског криминала која се повезује са хакерима „друге генерације" (Morris, 2011; Turgeman - Goldschmidt, 2011).

Архитектура отворености раног интернета омогућила је развој специфичне хакерске културе коју су сачињавали млади људи посвећени извођењу елегантних хакова, односно проналажења начина да рачунар учини различите,

* milena.kojic.ns@gmail.com, телефон: 0603301171

[1] Креативна апропријација би се најједноставније могла дефинисати као способност или могућност корисника да мењају или изнова стварају техничка средства кроз њихову креативну примену.

до тад незамисливе, ствари (Петровић, 2012). Према њиховом мишљењу, слободне и свима доступне информације омогућавају ефективнији и ефикаснији напредак технологије, што је један од аргумената у служби данашње „хакерске етике„" (Morris, 2011). Ова етика експлицира принцип да би све информације требало да буду слободне и да је подела информација друштвена одговорност, док се чување информација сматра правим злочином (Turgeman-Goldschmidt, 2011). Данас хакерска етика у потпуности добија негативну конотацију која упућује на компјутерски криминал и „електронске вандале", док је све јасније да отворена размена информација доведи до брзог развоја технологије, али исто тако отвара могућности онима који желе да је злоупотребе (Morris, 2011).

Дефинисање и типологија компјутерског криминала

Тешкоће у дефинисању компјутерског криминала произилазе из чињенице да се ради о релативно новој врсти криминала чије је обележје велика феноменолошка разноврсност. Самим тим је проблематично обухватити све облике ове појаве једном дефиницијом или једном типологијом. Из тог разлога овде су представљене дефиниције за које се сматра да су најобухватније и најрепрезентативније.

„Енциклопедија компјутерског криминала" одређује компјутерски криминал као све незаконите активности које се врше на компјутеру или код којих је компјутер средство извршења. Наведено обухвата незаконит приступ другом компјутерском систему, крађу компјутерских података или коришћење онлајн система за вршење или помоћ у извршењу превара. (McQuade, 2009). На десетом Конгресу Уједињених Нација за превенцију криминалитета и третман делинквената, компјутерским криминалом су обухваћена „кривична дела која се врше посредством компјутерског система или мреже, у компјутерском систему или мрежи, или против компјутерског система или мреже. У принципу он укључује било које кривично дело које се врши у „електронском амбијенту" (Матијашевић и Игњатијевић, 2010:853). Према *Закону о организацији и надлежности државних органа у борби против високотехнолошког криминала*, компјутерски криминал „представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику" (члан 2, став 1. Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала).

Постоји више типологија компјутерског криминала. Поједини аутори (Straub and Nance, 1990; Durham and Skousen, 1990) сматрају да се основна подела заснива на томе да ли је компјутер субјекат или објекат криминалне радње, док други сматрају да је кључна подела она која разликује да ли је компјутерски криминал извршен од стране инсајдера или аутсајдера (Harrington, 1996). С обзиром на танку границу између типова компјутерског криминала, постаје очигледно да једно кривично дело може претходити другом, а такође је могуће исто кривично дело сврстати под два различита типа компјутерског

криминала (Bequai, 1990). Комбинација компјутерских кривичних дела зависи од креативности починиоца дела. Из тог разлога би најобухватнија типологија захтевала објашњење начина на који се одређено кривично дело у сфери компјутерског криминала врши. Иако је за регулисање компјутерског криминала неопходно да се што детаљније опишу сва понашања која се сматрају криминалним, исцрпне типологије нису могуће узимајући у обзир ограничења у обухвату овог рада. Из тог разлога биће представљена једна од репрезентативнијих типологија на којој је заснована студија „Кривично право у сајбер простору". Компјутерски криминал у овој студији обухвата (Katyal, 2001):

1. Неовлашћени приступ компјутерским програмима и фајловима
2. Пуштање у оптицај штетних садржаја и програма
3. Крађа идентитета
4. „Традиционална" кривична дела изведена уз помоћ компјутера.

Неовлашћени приступ компјутерским програмима и фајловима

Неовлашћеним приступом компјутерским програмима и фајловима сматра се сваки приступ без дозволе у циљане фајлове или програме. Починилац може бити особа или други компјутер, а приступ може бити електронски (кроз лозинке и друге механизме) или физички (крађа персоналног идентификационог броја- ПИН). Електронски приступ је чешћа претња сигурности и изводи се путем крађе лозинки (комјутерским генерисањем насумичних лозинки све док се не добије права којом се врши приступ), или постављање „замки" (*trap doors*) које на брз начин добијају податке којима се врши приступ (Katyal, 2001). „Замке" се постављају тако што се при хаковању поставља код који хакерима омогућује да у више наврата приступају одређеном фајлу или програму. Корисници програма или фајла на којима је постављена „замка" су принуђени да куцају лозинку два пута (Schell and Martin, 2006). Злоупотреба фајлова или програма и непримерено коришћење података се третирају као различити злочини. (McQuade, 2009).

Пуштање у оптицај штетних садржаја и програма

Ова група кривичних дела сподразумева ситуацију када одређени ентитет без овлашчења управља функцијама компјутерског хардвера или софтвера. У наведено спадају „вируси", „црви", „логичке бомбе", „тројански коњи", и „онемогућавање вршења услуга" (DdoS). (Katyal, 2001)

„Вирус" је програм који модификује друге компјутерске програме. Модификације су направљене на начин да када је компјутерски програм „заражен" „вирусом", он га репликује. Другим речима, оригинални програм (аналогно здравој ћелији у организму) је измењен „вирусом" тако да „вирус" може да се мултипликује. „Заражени" програм прикривено захтева од компјутерског оперативног система да копира „вирус" на програм који је мета (McQuade,

2009). Када је компјутер повезан са другим компјутером кроз интернет, директном компјутерском везом или кроз обичан УСБ, „вирус" се шири. „Вирус" не мора нужно бити штетан, већ ниво штетности зависи од алгоритма којим је „вирус" програмиран (Schell and Martin, 2006). Неки „вируси", међутим, производе огромне штете[2] (Katyal, 2001).

Компјутерски „црви" су програми који се самостано репликују, као и „вируси". Међутим, разлика је у томе што „вирус" захтева и људску акцију. Компјутерски „црви" са друге стране, користе компјутерску мрежу како би се умножавали[3] (Katyal, 2001; Schell and Martin, 2006).

„Логичке бомбе" налажу компјутеру да изврши одређене инструкције у одређено време под јасно одређеним околностима. Такве команде могу бити бенигне (порука од програмера сваке године на ваш рођендан) или штетне (команда да се уништи хард диск у одређено време) (McQuade, 2009). „Логичка бомба" може да постоји непримећена у хардверу или софрверу до детонације.Она може да служи и као помоћ у нападу ван сајбер простора. (Schell and Martin, 2006).

„Тројански коњ" је, са друге стране, компјутерски програм који извршава неку корисну функцију, али који истовремено садржи и штетни код (McQuade, 2009). Тај штетни код може да садржи „вирус", „црв" или може да дозволи неовлашћени приступ (Katyal, 2001). „Тројански коњ" је заправо најчешћи начин на који „вируси" доспевају до компјутерских система. Неки од познатијих су „NetBus" и „Zevs" (Lockwood et al, 2003).

„Онемогућавање вршења услуга" (Ddos) се односи на нападе на сајтове путем преплављивања информацијама и онемогућавање сајтовима да комуницирају са другим компјутерима (Katyal, 2001). Овакав напад подразумева неовлашћени приступ компјутерском систему и постављање стофтверског кода у компјутерски систем који тада постаје „Господар". Затим, да би се извршио овакав напад, потребно је неовлашћено приступити другим мрежама да би се поставио код који те друге системе претвара у агенте (познатије као „зомбије" или „робове"). Сваки „Господар" контролише више агената и активира се путем интерног програмирања (команда за почетак напада у одређено време) и истовремено шаље информације агентима. Након што приме информације, агенти шаљу понављане захтеве за повезивањем са метом напада (нпр. одређена ИП адреса) (McQuade, 2009). На тај начин мета напада не може да разликује који захтеви су прави а који лажни. Агенти делују истовремено и стварају „закрчење саобраћаја", чиме сајтови постају преплављени информацијама (Katyal, 2001). На тај начин сајтови не могу да врше услуге с обзиром на то да

[2] На пример, од средине новембра 2014. године, Интернет је под нападом најбрже растућег "вируса" у историји познатог као "SoBig.F". Кроз само деведесет и шест сати овај "вирус" се раширио у сто тридесет и четири земље, генеришући десетине милиона е-мејл налога. Штета коју је направио мери се у милионима неуспелих извршења услуга и падова система (Lockwood et al, 2003).

[3] Најпознатији пример је "ILoveYou" "црв" који је заправо поседовао карактеристике и "црва" и "вируса". Ширио се првенствено кроз листу контаката са е-мејла, али се преносио и кроз интернет четове и интернет системе компанија (Lockwood et al, 2003).

не успевају да изврше трансакције са сваким агентом који је послао захтев. Овакве нападе су доживели сви већи сајтови (Yahoo!, Amazon.com, Buy.com, CNN.com) што је резултирало огромним финансијским губицима (Schell and Martin, 2006).

Крађа идентитета

Под крађом идентитета подразумева се вршење „традиционалне" крађе идентитета посредством компјутера (нпр. крађа кредитних картица). Сајбер простор омогућава лакше извршење овог криминалног дела (Schell and Martin, 2006). Са друге стране крађа идентитета у сајбер простору не мора бити аналогна „традиционалној" крађи идентитета. Могуће је украсти идентитет сајтова путем постављања кодова на сајт који тада постаје жртва напада (Katyal, 2001). Кодови омогућавају да сајт шаље информације независно од воље оних који поседују сајт (*cross-site scripting*). Такође, могуће је и изменити адресу на коју води линк или лого сајта. Ово се назива отимање сајтова (*pagejacking*) (Schell and Martin, 2006).

„Традиционална" кривична дела изведена уз помоћ компјутера

Иако у ову групу спадају сви злочини који се дешавају у реалном простору, а који се изводе путем или уз помоћ компјутера, фокус ће бити на четири примера криминалне активности у овој категорији: дечјој порнографији, ауторским и сродним правима и виртуелном ухођењу (Katyal, 2001). Из перспективе починиоца криминалног дела свака од ових активности има предности које се тичу широке и брзе дистрибуције и минимализације трошкова (Schell and Martin, 2006).

Починилац кривичног дела дечје порнографије има разне врсте трошкова продукције оваквог материјала у реалном простору (снимање, штампање, дистрибуција), док у виртуелном простору ове тешкоће за починиоца нестају. Лакоћа дистрибуције је стандардна одлика компјутерског криминала (Матијашевић и Игњатијевић, 2010). Чак и фининсијски криминал, као што је манипулација берзом, има предности у виртуелном у односу на реални простор (McQuade, 2009). Тако дечју порнографију није лако спречити, јер је овакав материјал могуће послати са једног краја света на други, за веома кратко време. Починиоци овог криминалног дела су углавном стационирани у земљама где нема закона о дечјој порнографији или земљама које немају законе који спречавају дистрибуцију оваквог материјала преко националних граница.(Стефановић, 2009).

Са друге стране, виртуелни простор олакшава улогу информатора (Schell and Martin, 2006). У реалном простору, особе које поседују информације о потенцијалним криминалним делима углавном избегавају да дају такве информације полицији, због страха од освете која може да се одрази на њихову по-

родицу, здравље или имовину (Katyal, 2001). Виртуелни простор може да помогне у спречавању такве врсте освета, јер ни полиција не мора да зна ко је информатор, а самим тим ни криминалац. Одавање овакве врсте информација постало је једноставно колико и писање е-маила (Schell and Martin, 2006).

Кршење ауторских права се односи на крађу интелектуалног власништва (Katyal, 2001). Ако бисмо замислили да је 1970. година и да желимо да копирамо албум Битлса (*Beatles*) „*Let it be*", процес би био много захтевнији него што је то случај данас. У најмању руку би подразумевао куповину легитимне копије албума и куповину скупе опреме за снимање. Осим што је читав подухват изузетно тешко извести, свака следећа копија би била лошијег квалитета, а највише бисмо могли да направимо двадесет и пет копија у једном дану. Када бисмо и успели да направимо те копије, морали бисмо да одлучимо на који начин бисмо их продавали. Врло вероватно бисмо их проследили трговцима на велико који би их затим проследили трговцима на мало. Међутим, ако бисмо продају извршили на улици, ризиковали бисмо да нас ухвати полиција. Све ово је превазиђено у компјутерском добу. Чак и копије копија звуче скоро савршено, трошкови копирања не постоје, време које нам је потребно да копирамо албум своди се на неколико минута, а за исто толико времена можемо да дистрибуирамо албум по целом свету. Ниједан од наших купаца не мора да зна наш идентитет, а чак и да органи гоњења дођу до нашег сајта, не морају нужно да знају наш прави идентитет (Schell and Martin, 2006).

Ухођење путем интернета се односи на претње и злостављања која се дешавају у виртуелном простору. Иако претње путем интернета звуче безопасно, проблем наступа када ухођење из виртуелног простора изазове ухођење у реалном простору (Ковачевић-Лепојевић и Лепојевић, 2009). Дакле, као и у претходним типовима компјутерског криминала, и ухођење је олакшано путем интернета (чему доприноси анонимност особе која уходи) (Schell and Martin, 2006). Чак и ако не постоји каузалност између ухођења у виртуелном и реалном простору, постоји вероватноћа да су они који уходе путем интернета склони извршењу кривичног дела као што је злостављање у реалном простору (Katyal, 2001).

Компјутерски криминал као криминал белог оковратника

Компјутерски криминал је обично класификован као криминал белог оковратника који је дефинисан као незаконита активност коју карактеришу обмане, огромне финансијске штете, непостојање директног насиља и ниска стопа пријављивања (Benquai, 1990; Mc Ewen, 1989). Са друге стране, Даф и и Гардинер (Duff and Gardiner, 1996) сматрају да хаковање не треба сматрати криминалитетом и да већина форми хаковања не потпада под криминал белог оковратника.

Термин „криминал белог оковратника" има корене у раду Едвина Сатерленда (Edwin Shutherland) који је акцентовао појединце високог статуса и

угледа који крше закон у оквиру својих професија. Овом новом кованицом Сатерленд је желео да укаже на пристрасност кривичноправног система у Америци тог времена, тако што је идентификовао тип криминала који није типичан за ниже класе друштва, а који је тадашње правосуђе занемаривало (Sutherland, 1940). Временом је значење овог концепта почело да обухвата бројна ненасилна дела чији је суштински елемент обмана и непоштење у контексту уобичајених и легалних друштвених трансакција. Обмана се у овом смислу односи на превару, прикривање, довођење у заблуду, манипулацију итд (Croall, 1992). У колоквијалном смислу, израз криминал белог оковратника се разуме као дело фундаментално различито од уличног криминала. За улични криминал је типично конфронтирање са жртвом или њеном имовином, док се већина дела криминала белог оковратника односи на криминал који подразумева одређену дозу софистицираности (Булатовић, 2010). Ово дело је релативно лако прикрити, а жртве су тешко уочљиве. Доминантно обележје нормативног регулисања криминала белог оковратника је да му се у савременим демократијама не придаје иста тежина као другим врстама криминала, тачније, да су казне обично блаже (Braithwaite, 1985).

Колман у свом раду објашњава да Сатерлендов концепт наилази на тешкоће у дефинисању која тачно понашања елите се сматрају девијантним. Због одсуства јасне формулације друштвеног стандарда за понашање елите, социолози користе приступе девијантности који се обично ослањају на њихове личне вредности и предрасуде (Coleman, 1987). Сва понашања која спадају у криминал белог оковратника подразумевају кршење закона од стране особа угледних позиција и високог друштвеног статуса. Такође, односи се на рационално калкулисане злочине, а не злочине из страсти (Булатовић, 2010). Циљ већине понашања која спадају у ову категорију је економски добитак или професионални успех који може довести до економског добитка. Употреба насиља у оквиру криминала белог оковратника обично је нус продукт, а не циљ оваквог понашања (Sutherland, 1940). И поред ових заједничких особина, концепт криминала белог оковратника није кохерентан аналитички конструкт (Pontel and Rossof, 2009) .

Сатерленд је објаснио криминално понашање са интеракционистичке позиције, међутим, он није препознао контрадикторност тог становишта (Coleman, 1987). Према интеракционистичкој позицији симболички конструкти који мотивишу криминално понашање уче се у интеракцији са другима. Значење које појединци придају одређеној ситуацији и друштвеној реалности уопштено структуирано је њиховим искуствима. На тај начин су одређене акције перципиране као прикладне, док су друге игнорисане или перципиране као неприкладне (Akers, 1985). Симболичка конструкција осим што дефинише реалност, омогућава појединцима да антиципирају реакције на њихово понашање и самим тим да ускладе своје понашање према одређеној ситуацији. Дакле, мотивација подразумева симболичку конструкцију, дефиницију ситуације као пожељне или као непожељне и очекивања у вези са реакцијама које узрокује индивидуално понашање. Међутим, генерализовани други као централни елемент понашања представља проблем у интеракционистичком објашњењу

криминала белог оковратника јер већина криминалних активности нарушава друштвена очекивања. Зато се Колман ослања на теорију о „техникама неутрализације" Сајкса и Марце (Sykes and Martza). Они који чине криминално дело имају потребу да оправдају тј. рационализују своје понашање (Coleman, 1987).

Теорија о техникама неутрализације је покушај објашњења криминалног понашања који се заснива на хипотези да иако већина људи дели конвенционална веровања о криминалу као непожељном понашању, с времена на време људи чине кривична дела тако што рационализују своје понашање и на тај начин одрже слику о себи као о неделинквентним индивидуама. Сајкс и Марца су развили своју теорију преко истраживања малолетничке делинквенције и на тај начин дошли до закључка да се индивидуални ставови о криминалу не могу одвојити од контекста. Према овој теорији, индивидуе прихватају криминално или девијантно понашање као пожељно тако што развијају рационализације или неутрализације својих дела.

Сајкс и Марца наводе пет техника неутрализације (Sykes and Martza, 1957):

1. Порицање одговорности - када користи ову технику, индивидуа преусмерава сваку потенцијалну оптужбу на неки алтернативни извор или на околности.
2. Порицање штете - индивидуа може да рационализује криминално дело тако што закључи да то дело не наноси ни имовинску ни личну штету, па је према томе такво понашање безопасно.
3. Порицање постојања жртве - ова техника неутрализације се обично користи када жртва није физички присутна, или је непозната или апстрактна починиоцу дела. Из те перспективе лако је закључити да, ако нема жртве, нема ни злочина.
4. Осуда оних који осуђују - ова врста оправдања се користи када је перспектива починиоца дела неусклађена са перспективом правних ауторитета. У овом случају индивидуа сматра да су они који стварају законске одредбе лицемери и да с тога немају право да осуђују њене акције. Према тој логици, те акције нису непримерене.
5. Виши циљ - последња техника неутрализације коју наводе Сајкс и Марца се односи на оправдавање акција које индивидуа сматра важнијим од сопственог интереса или интереса онога коме је штета начињена. На пример, у традиционалним криминалним делима ово би се односило на проневеру компанијског новца због лечења детета и слично.

Ових пет техника не покривају експлицитно све врсте оправдања која се примењују при извршењу криминалних дела, па из тог разлога постоје покушаји проширења и допуне ове листе. На пример Мајнор (Minor) наводи и шесту тачку „одбрана из неопходности" која се састоји из оправдања да одређено дело које се перципира као неопходно, чак и ако се сматра неморалним, мора бити извршено (Minor, 1981). Скот и Лајман (Scott and Lyman, 1968) додају још две врсте оправдања: „тужна прича" и „самоиспуњење".

Колман наводи да су најчешће технике неутрализације криминала белог оковтатника „порицање нанете штете" и оправдања која се тичу кршења „непотребних закона" тј, осуда оних који осуђују (Coleman, 1987). Са друге стране, неколико истраживања је утврдило везу између неутрализација и кримина-

ла, укључујући и хаковање (Morris, 2011). У истраживању израелских хакера и студената (Turgeman-Goldschmidt, 2011) откривено је да је најчешћа техника неутрализације коју хакери користе „порицање постојања жртве". Као што је наведено, до ове врсте рационализације долази када је жртва непозната или апстрактна починиоцу дела.

Осим коришћења техника неутрализације, криминалци белог оковратника и хакери имају доста тога заједничког:

1. Социо-демографске карактеристике хакера и криминалаца белог оковратника су веома сличне. Најчешће су то бели мушкарци, млади, ненасилни, који потичу из средње класе (Turgeman-Goldschmidt, 2011).
2. Друштвена перцепција ове две врсте криминала је слична. Хакери су обично представљени као генији или хероји (Turkle, 1984). Са друге стране, криминалци белог оковратника обично нису перципирани као „прави" криминалци, у смислу да се на пример неплаћање пореза не посматра као озбиљан злочин (Braithwhite, 1985). Према Веисбурду и Шлегалу (Weisburd and Schlegel, 1992) већина јавне пажње је посвећена уличном криминалу, док криминал белог оковратника није ништа мање илегалан, само није онај тип криминала који нас чини несигурним у нашим кућама и квартовима . Јавна перцепција је један од разлога зашто закон у већој мери не обраћа пажњу на ову врсту криминала. Ни хакери ни криминалци белог оковратника не доживљавају себе као криминалце, већ уживају симпатије друштва (Turgeman-Goldschmidt, 2011).
3. Сличност ове две врсте криминала лежи и у тешкоћи њиховог идентификовања од стране органа гоњења и правосуђа. Поред тога, значајну улогу игра и мањак ресурса за истраживање и кривично гоњење ових врста криминала (Turgeman-Goldschmidt, 2011). Веисбурд и Шлегал верују да три основна концепта раздвајају криминал белог оковратника од „обичног" криминала: организација, жртве (које обично нису свесне да су жртве) и казнени систем (Weisburd and Schlegel, 1992). Ова три концепта се такође могу применити и на хаковање. Тешко идентификовање хакованих компјутера и компјутерских мрежа је последица непријављивања ових злочина. Наиме, велике компаније и владине агенције се суздржавају од пријављивања овакве врсте криминала јер то пријављивање истовремено подразумева и негативан публицитет (Harrington, 1996).
4. Поред тога, сличност између хаковања и криминала белог оковратника се огледа и у огромним финансијским штетама које обе врсте криминала наносе (Turgeman-Goldschmidt, 2011; Katyal, 2001).

Поред наведених сличности, постоје и разлике између ове две врсте криминала. При употреби техника неутрализације хакери не користе „порицање одговорности" нити „тужну причу" као оправдања за своја дела (Turgeman-Goldschmidt, 2011). Разлог томе је чињеница да хакери желе да преузму одговорност за оно што су учинили јер извршена кривична дела перципирају као успех и очекују награду од својих „колега" (Turkle, 1984). Интереси и вредности хакера су усмерени ка увећању сопственог статусног положаја међу „колегама". Они стварају идентитет дистинктивне групе која има сопствену субкултуру и тиме шаље поруку „ми смо другачији". Овакве субкултуре постоје свуда у свету и оне обезбеђују подршку, експертизу, професионални развој, литературу, веб сајтове и конференције (Turgeman-Goldschmidt, 2011). Са друге

стране, криминалци белог оковратника не развијају сопствену културу или мрежу на основу својих криминалних понашања. Управо супротно, они покушавају да оправдају своја дела и да докажу да су они „обични људи". Криминална дела која извршавају су у циљу искључиво личне економске добити (Pontel and Rossof, 2009).

Евидентно је да поистовећивање криминала белог оковратника и компјутерског криминала није увек оправдано. Велики део компјутерског криминала извршавају хакери који не врше криминална дела искључиво ради економске добити. Постоји читава нова култура која се јавља у потпуно новом специфичном окружењу, тзв сајбер простору.

Виртуелно окружење (сајбер простор)

Неопходно је размотрити специфичности виртуелног окружења у коме се сва наведена кривична дела извршавају. Сам појам сајбер простора потиче из романа „*Neuromancer*" Вилијама Гибсона. Овде се под тим термином подразумева нешто што је виртуелно, невидљиво, неограничено, базирано на технологији тј. универзум рачунарских мрежа, свет у коме се мултинационалне компаније, друштва и други субјекти боре за освајање података и информација (Lessig, 2000). Слично, светски речник енглеског језика сајбер простор дефинише као „електронски медиј рачунарских мрежа, у којем се остварује онлајн комуникација" и као „нематеријални простор заснован на информационо комуникационој технологији" (Вулетић, 2009:64)

Карактеристике специфичног сајбер окружења у коме се одвија компјутерски криминал су висока концентрација информација на малом простору, претходно проверених и уређених података, доступних како овлашћеним, тако и неовлашћеним корисницима; знатно проширен простор криминалног деловања, који, за разлику од традиционалних видова криминалитета, не захтева присуство извршиоца на месту извршења кривичног дела; скраћено време криминалног деловања, с обзиром на аутоматизовани амбијент, чија брзина спречава надзор и управљање (McQuade, 2009). На тај начин, време потребно за извршење кривичног дела скраћује се на делове секунде, што имплицира висок ниво прикривености и значајне тешкоће у откривању такве делатности. На ово се надовезују и суптилне технике и методи које се извршавају истим механизмима као и легалне, не остављају трагове, нити ометају редован рад система, па је самим тим могућност откривања сведена на најмању меру (Матијашевић и Игњатијевић, 2010). За разлику од традиционалног криминала, компјутерски карактерише стабилност ризика (с обзиром на то да се једном изграђен модус може веома дуго користити, са потпуно истим, ниским ризиком откривања) и све једноставније могућности употребе компјутерске технологије од стране све већег броја корисника, којима више није нужно посебно техничко образовање (Вулетић, 2009).

Правни инструменти за борбу против компјутерског криминала

Тешкоћа усклађивања правне регулативе међународне заједнице произилази из проблема третирања одређеног понашања као илегалног у једној земљи и третирање истог типа понашања као легалног у некој другој земљи. Тако се оставља велики простор за избегавање кривичне одговорности (Shah, 2005). Друга тешкоћа која се јавља је проблем надлежности. Када се користи технологија која омогућава рад са удаљених локација, односно употреба ресурса у једној земљи за обављање активности у другој, док се оперативни рад обавља у трећој, проблематично је дефинисати докле досеже надлежност органа гоњења, а докле надлежност органа правосуђа (Adoption of Convention of Cybercrime, 2001). Управо због неопходне координације и ефикасне борбе против криминала, неопходно је успоставити законску регулативу, а потом ускладити процесе прикупљања и анализирања дигиталних доказа (Weber, 2003).

Савет Европе је већ 1976. године препознао неколико облика злоупотребе рачунара, међутим, од препознавања проблема до преузимања иницијативе и састављања стручне комисије прошло је пуних девет година, а до састављања акта спремног за потписивање на међународном нивоу, прошло је још једанаест година. Прва међународна иницијатива потекла је са Конференције Савета Европе о криминолошким аспектима привредног криминала. Стручна комисија је образована 1985. године у сврху давања кључних смерница националним законодавствима у регулисању ових појава. Још тада је утврђен минимални списак кривичних дела која спадају у ову категорију. Те смернице су касније преточене у Конвенцију о компјутерском криминалу која је усвојена и отворена за потпис 2001. године, а на снагу је ступила 2004. године[4] (Писарић, 2011). Овај документ у четири поглавља дефинише основне појмове, легислативне мере, прописује међународну сарадњу и на крају оставља могућност захтевања нових елемената (Adoption of Convention of Cybercrime, 2001). Ратификовањем овог документа држава се обавезује да ће материјалне одредбе (описана кривична дела) и процесуалне одредбе (поступци неопходни за истрагу и кривично гоњење таквих кривичних дела) Конвенције бити имплементиране у домаће законодавство[5]. На овај начин је свакој земљи омогућено да

[4] До данас, 43 земље чланице Савета Европе су приступиле Конвенцији, међу којима је и наша земља. Иако Русија, Монако, Сан Марино и Андора нису приступиле Конвенцији, постоје и државе ван Европе (Јапан, САД, Канада, Јужноафричка република) које су је потписале, чиме овај документ добија универзални значај . С друге стране, четрнаест земаља које су потписале Конвенцију нису ратификовале овај међународни инструмент, па самим тим он није ни ступио на правну снагу (Weber, 2003).

[5] Република Србија је априла 2005. године у Хелсинкију потписала Конвенцију о компјутерском криминалу, а током марта 2009. године Народна Скупштина Републике Србије је ратификовала овај међународни правни инструмент. Основни значај Конвенције је формирање посебних државних органа који су специјализовани за борбу против компјутерског криминала (Писарић, 2011). Законодавство Републике Србије је у периоду од потписивања до ратификације (април 2005-март 2009.) усвојило низ закона којима се Конвенција о компјутерском криминалу имплементира у наш правни систем. Међу њима су најважнији: Закон о организацији и надлежности државних органа за борбу против компјутерског криминала, Кривични законик, Закон о одговорности

препозна врсту злочина и као такву је уврсти или дефинише у свом правосудном систему (Писарић, 2011). Савет Европе није дао смернице за санкционисање ових злочина, већ је само омогућио да починиоци могу бити кажњени „ефективним, пропорционалним и оштрим санкцијама које укључују лишавање лица слободе" у случају када је починилац правно лице. Предвиђена је и мера новчане казне (Weber, 2003).

Савет Европе није ишао даље у дефинисању, већ је оставио свакој својој чланици да своју правну регулативу уреди на начин на који она сматра одговарајућим. Такав приступ доводи до разлика које су прихватљивије у смислу различитости средина и система државног уређења (Писарић, 2011).

На нивоу Европске уније постоји низ докумената који се баве овом проблематиком. (Weber,2003). Кључан документ који утврђује јасну опредељеност супротстављању компјутерском криминалу на нивоу Европске уније је „Оквирна одлука о нападима на информационе системе" из 2005.године. Оквирном одлуком изражена је стратешка подршка Конвенцији и настојање да се државе чланице подстакну на ратификацију Конвенције (Ruyver et al, 2002). Ова два правна инструмента имају исти циљ иако се њихова правна природа и домет разликују, а то је да се ублаже разлике између националних законодавстава, да се уведу нова овлашћења у откривању и доказивању компјутерског криминала и да се побољша међународна сарадња у борби против високотехнолошког криминала (Стаменковић и др, 2014)

Ограничења кривичног права

Надлежни органи морају константно да уче и да буду у кораку са развојем информационих и комуникационих технологија. Само високоспецијализовани стручни кадрови могу ефикасно вршити истрагу догађаја који представљају злоупотребу у информационим технологијама. Стручни кадрови у интервентним тимовима морају имати и одговарајуће ресурсе за овакве истраге. Без константне обуке и будног праћења догађаја и промена у свету технологије биће веома тешко контролисати раст компјутерског криминала (Shah, 2005).

Са друге стране, превише агресивно право је опасно у виртуелном окружењу. Сваки нови облик компјутерског криминала изазива органе гоњења и правосуђа да врше промене техничке инфраструктуре како би створили што боље механизме за праћење и надгледање (Durham and Skousen, 1990). Проблем који се односи на начин како ће се право носити са развојем технологије је ужи од проблема компјутерског криминала. Компјутерски криминал нам указује на недостатке и ограничења кривичног права, као што и кривично право указује на ограничења технологије. Међутим, компјутерски криминал није

правних лица за кривична дела, Закон о кривичном поступку, Закон о полицији, Закон о ауторским и сродним правима, Закон о телекомуникацијама, Закон о електронском потпису, Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине и Правилник о условима за пружање интернет услуга и садржају одобрења (Стаменковић и др, 2014).

одређен искључиво правом. Право је само један од механизама којим се он сузбија (Katyal, 2001). Лоренс Лесиг објашњава да је свако понашање осим законом ограничено са бар још три фактора који га регулишу: друштвеним нормама, тржиштем и архитектуром. Регулација тог понашања је резултанта та четири ограничења. Промена у било ком од ових фактора утиче на целину. Такође, нека ограничења подупиру а нека поткопавају друга ограничења. Ограничења су различита, али међузависна. Закон ограничава путем прописане казне, друштвене норме путем стигматизације коју намеће заједница, тржишта ограничавају путем цене, а архитектуре ограничавају путем физичких терета које намећу (Лессиг, 2000).

Закључак

Евидентно је да су мере превенције и санкције могуће тек након што се се компјутерски криминал схвати као реалан проблем данашњице и као јединствена и посебна врста криминала која има своје карактеристике у специфичном контексту виртуелног окружења. Механизми сузбијања компјутерског криминала нису на завидном нивоу. Напредак технологије сваким даном указује на ограниченост мера закона, док је стигматизација компјутерских криминалаца од стране (он и офлајн) заједнице практично непостојећа. У *онлајн* заједницама се извршиоцима преступа чешће придаје херојски карактер него што се они стигматишу, а у *офлајн* заједницама је изузетно тешко идентификовати преступнике (услед псеудонима којима сакривају свој идентитет) (Билиновић, 2014). Са друге стране, чак и када су преступници идентификовани, не сматрају се „правим" криминалцима (Turkle, 1984; Katyal, 2001; Turgeman-Goldschmidt, 2011). Према томе, поред стварања правних инструмената и низа закона на државном и међународном нивоу, неопходно је подизати свест како у *онлајн* тако и у *офлајн* заједницама о компјутерском криминалу и његовим последицама.

Литература:

1. Adoption of Convention on Cybercrime (2001). The American Journal of International Law. 95(4): 889-891.
2. Akers, L. Ronald (1985). Deviant Behavior: A Social Learning Approach. Belmont.
3. Bequai, August (1990). Computer-related crime. Strasburg, Germany: Council of Europe.
4. Bilinović, Ana (2014). Primena koncepta socio-kulturne integracije u analizi devijantnosti i procesa etiketiranja.Zbornik Instituta za kriminološka i sociološka istraživanja, God. 33, br. 1, str. 177-191.
5. Braithwhite, John (1985). White collar crime. Annual Review of Sociology. 11: 1-25.
6. Bulatović, Aleksandra (2010). Pitanje o javnom ovlašćenju-koren kriminala belog okovratnika. Socijalna misao. 4:75-86.

7. Coleman, J. William (1987). Toward an integrated theory of white-collar crime. American Journal of Sociology. 93(2):406–439.
8. Croall, Hazel (1992). White collar crime. Philadelphia and Buckingham, PA: Open University Press.
9. Duff, Liz, and Gardiner, Simon (1996). Computer crime in the global village: Strategies for control and regulation--in defence of the hacker. International Journal of the Sociology of Law, Vol. 24, no. 2, pp. 211–228.
10. Durham, W. Cole and Russel C. Skousen (1990). The law of computer-related crime in the United States. The American Journal of Comparative Law. Supplement. U.S. Law in an Era of Democratization. 38:557-580.
11. Harrington, J. Susan (1996). The effects of codes of ethics and personal denial of responsibilityon computer abuse judgments and intentions. MIS Quartetly. 20(3): 257-278
12. Katyal, K. Neal (2001). Criminal law in cyberspace. University of Pensilvania Law Review. 149(4):1003-1114.
13. Kovačević-Lepojević, Marina i Borko Lepojević (2009). Žrtve sajber proganjanja u Srbiji. Temida.3: 89-108.
14. Lessig, Lawrence (2000). Code and other laws of cyberspace. New York: Basic Books.
15. Lockwood, John, James Moscola, David Reddick, Mathew Kulig and Tim Brooks (2003). Application of hardware accelarated extensible network modes for Internet worm and virus protection. Kyoto, Japan: IWAN
16. Matijašević, Jelena i Svetlana Ignjatijević (2010). Kompjuterski kriminal u pravnoj teoriji, pojam, karakteristike, posledice. Infoteh-Jahorina . 9: 852-856.
17. McEwen, J. Thomas (1989). Dedicated computer crime units. Washington, DC: National Institute of Justice.
18. McQuade, C. Samuel (2009). Encyclopedia of cybercrime. Westport, Conneticut: Greenwood Press.
19. Minor, W. William (1981). Techniques of neutralization: A re-conceptualization and empirical examination. Journal of Research in Crime and Delinquency . 18 (2): 295–318.
20. Morris, G. Robert (2011). Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. In: T. J. Holt and B. H. Shell (Eds.), Corporate hacking and tehnology-driven crime: Social dynamics and implications. New York, NY: Information Science Reference, pp. 1-17.
21. Petrović, M. Dalibor (2012). Novi oblici društvenog umrežavanja: Uloga interneta u uspostavljanju interpersonalnih odnosa u Srbiji. Beograd: Filozofski fakultet - doktorska disertacija.
22. Pisarić, Milana (2011). Stanje i tendencije u suprotstavljanju kompjuterskom kriminalu na evropskom nivou. Zbornik radova Pravnog fakulteta u Novom Sadu. 1: 487-505.
23. Pontell, N. Henry and Stephen M. Rossof (2009). White-collar delinquency. Crime, Law and Social Change. 51(1): 147-162.
24. Ruyver, Brice, Gert Vermeulen, Tom Beken (2002). Strategies of the EU and the US in combating transnational organized crime. Antwerp, Belgium: Maklu-Publishers.
25. Schell, Bernadette and Clemens Martin (2006). Webster's New World Dictionary. Indianapolis,IN: Whiley Publishing Inc.
26. Scott, B. Marvin and Stanford M. Lyman (1986). Accounts. American Sociological Review. 33: 46-62.
27. Shah, R. Monica (2005). The Case of Staturory Suppression Remedy to Regulate Illegal Private Party Searchers in Cyberspace. Columbia Law Review. 105(1): 250-278.
28. Stamenković, Branko, Adis Balota, Valentina Pavličić, Bojana Paunović i Jakša Backović (2014). Visokotehnološki kriminal: Praktični vodič kroz savremeno krivično pravo i primjere iz prakse. Podgorica : OEBS Misija u Crnoj Gori.

29. Stefanović, Ivana (2009). Krivična dela vezana za iskorišćavanje dece u pornografske svrhe zloupotrebom računarskih mreža (međunarodni i domaći pravni okvir). Temida. 3: 27-42.
30. Straub, W. Detmar and William D. Nance (1990). Discovering and disciplining computer abuse in organizations: A feild study. MIS Quarterly, 14(1): 45-60.
31. Sutherland, H. Edwin (1940). White-collar criminality. American Sociological Review, 5(1): 1-12.
32. Sykes, M. Gresham, and Matza, David (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22: 664–670.
33. Turgeman-Goldschmidt, Orly (2011). Between Hackers and White-Collar Offenders. In: T. J. Holt and B. H. Shell (Eds.), Corporate hacking and tehnology-driven crime: Social dynamics and implications. New York, NY: Information Science Reference: 18-38.
34. Turkle, Sherry (1984). The second self: Computers and the human spirit. New York, NY: Simon and Schuster.
35. Vuletić, Dejan (2009). Trgovina ljudskim organima u sajber prostoru. Temida , 3: 63-74.
36. Weber, M. Amelie (2003). The Concil of Europe's Convention on Cybercrime. Berkeley Technology Law Journal. 18(1): 425-446.
37. Weisburd, David, and Schlegel, Kip (1992). Returning to the mainstream. In: K. Schlegel & D. Weisburd (Eds.), White-collar crime reconsidered. Boston, MA: Northeastern University Press.
38. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, „Službeni glasnik Republike Srbije" br. 61/2005 i 104/2009.

THE CHALLENGES OF CYBERCRIME

Summary: This paper aims to illuminate the problem of cybercrime, to point to its uniqueness and a specific context in which it appears, as well as to suggest possible ways of legal regulations in this field. The phenomenal diversity of this term complicates the understanding of cybercrime as a unique phenomenon, while inability to differentiate it from white-collar crime and traditional crime brings additional conceptual problems. The legal instruments for fighting cybercrime vary widely depending on the countries, and the fact is that international initiatives for preventing and fighting cybercrime is developing slowly in comparison to the development of technology and increasingly sophisticated forms of manifestation of this type of crime. In addition to the required legislative measures in this field, this paper will also describe the other ways of regulating behavior in cyberspace - social norms, market and architecture (technology) of virtual space.

Key words: cybercrime, hackers, white collar crime, virtual environment, legal instruments, regulators