Прегледни рад
УДК: 343.85:004.738.5
159.98:004.738.5
DOI: 10.5937/zrffp52-33587

ФОРЕНЗИЧКА САЈБЕРПСИХОЛОГИЈА И ПРИСТУПИ КРИМИНАЛНОМ ПРОФИЛИСАЊУ

Душан Љ. ВЛАЈИЋ[1]
Универзитет у Нишу
Филозофски факултет
Департман за психологију

[1] dusan.vlajic@filfak.ni.ac.rs

Рад примљен: 20. 8. 2021.
Рад прихваћен: 30. 6. 2022.

ФОРЕНЗИЧКА САЈБЕРПСИХОЛОГИЈА И ПРИСТУПИ КРИМИНАЛНОМ ПРОФИЛИСАЊУ[2]

Кључне речи: криминално профилисање; индуктивно профилисање; дедуктивно профилисање; сајбер криминалитет; сајбер психологија; дигитални доказ.

Сажетак. Иако постоји велики број теорија које изучавају психолошке факторе криминалног понашања и без обзира на то што скоро свака криминална активност има дигитални аспект, криминално профилисање није популарна дисциплина међу форензичким психолозима, нарочито када је реч о сајбер криминалу. Стога ће циљ овог чланка бити да пружи кратки преглед стручне литературе која разматра психолошке факторе повезане са девијантним рачунарским и онлајн понашањем. Биће приказана два основна приступа криминалном профилисању, индуктивни и дедуктивни, њихове предности и недостаци, логика на којој се базирају и концепти на које се ослањају током анализе дигиталних доказа, а са циљем сужавања опсега осумњичених за одређено кривично дело. Биће укратко поменути и конкретни модели који су развијени у оквиру сваког приступа. Поврх тога, биће описани резултати студија спроведених у оквиру сајберпсихологије и дискутован њихов однос са криминалним профилисањем, нарочито са индуктивним приступом, што је и оригинални допринос овог рада. На самом крају, биће изнети предлози за превазилажење ограничења претходних студија и за приближавање дисциплина криминалног профилисања и сајберпсихологије.

[2] Припремљено у оквиру пројекта *Примењена психологија у функцији квалитета живота појединца у заједници*, који се изводи на Филозофском факултету Универзитета у Нишу (бр. 455/1-1-6-01).

Увод

У последње две деценије је дошло до рапидног развоја информационо-комуникационих технологија. Њихов велики комуникациони потенцијал, мултифункционалност и лакоћа са којом приступамо различитим садржајима отворила је могућност да се бројни облици интеракција из „офлајн“[3] пренесу у онлајн свет. Изузетак не представљају ни кривична дела. У модерном добу је тешко замислити кривично дело које нема макар мали удео дигиталног (Casey, 2011). Потврда изнете констатације се може наћи и у преамбули Конвенције Савета Европе (2001) о сајбер криминалу у којој се наводи да се документ доноси због темељних промена које дигитализација и континуирана глобализација рачунарских мрежа доносе са собом и због могућности да оне буду коришћене у почињењу кривичних дела и садрже доказе.

Основни циљ овог рада је да пружи кратки преглед литературе из дисциплина које изучавају криминално понашање у сајберпростору и трагове који том приликом остају. Биће приказана два основна приступа профилисању сајбер криминалаца, њихове предности и недостаци, као и фактори који утичу на сајбер понашање.

Основни појмови

Грана психологије која проучава начин на који људи ступају у међусобну интеракцију уз помоћ технологије, како технологија утиче на понашање, на који начин она може да се развија тако да се што боље прилагоди потребама корисника и како утиче на психичка стања носи назив *сајбер психологија* (Whitty & Young, 2016; Kirwan, 2016b). Међу бројним специјализованим гранама своје место налази и *форензичка сајберпсихологија*, која

[3] У овом раду се под термином „офлајн“ подразумева све оно што се дешава или налази у реалном, материјалном свету, без обзира да ли су у питању починиоци, кривична дела, окружење, понашање итд.

се првенствено бави изучавањем сајбер криминала, тј. широког спектра криминалног, незаконитог понашања које се реализује уз помоћ рачунара или рачунарских мрежа (Kirwan, 2016a).

Сајберпростор можемо дефинисати као „комплексно окружење које је резултат интеракције људи, софтвера и интернет сервиса, уз помоћ повезаних техничких уређаја и мрежа, а које не постоји у физичком облику" (Hogan & Newton, 2015). Под *криминалним профилисањем* се подразумева доношење закључака о карактеристикама починилаца кривичних дела на основу анализе њиховог понашања (Shaw, 2006; Woodhams & Toye, 2007). Профилисање помаже при одређивању броја починилаца, идентификацији осумњичених, откривању карактеристичних образаца понашања (modus operandi и потпис), остваривању увида у мотивацију и психичко стање преступника, његове опасности и откривању додатних информација о личности (Casey, 2012). Из претходног се може извести закључак да вредност профилисања највише долази до изражаја онда када је починилац непознат.

Психолошки фактори понашања људи на интернету

Бројна онлајн понашања могу да се протумаче као *агресивни акти*. Објашњење нуде социјалнопсихолошке теорије, чији аутори тврде да су људи склонији да се понашају агресивно онда када је починилац анониман и када постоји мала шанса да се жртва освети (Myers, 2005, према: Campbell & Kennedy, 2014). Оба услова су често задовољена у сајберпростору. На онлајн понашање утиче и *анонимност*, која се лако остварује коришћењем надимака, украдених налога или спуфинга. Сакривање идентитета резултује у *емоционалној дистанцираности* у односу на друге, која по себи представља додатни фактор агресивног онлајн понашања. Повезана са лажним представљањем је и *деиндивидуација*, тј. губитак самосвесности који даље резултује понашањем супротног нормама (Campbell & Kennedy, 2014). Иако се деиндивидуација често користи да објасни понашање људи у маси, попут агресивних навијачких група, може се употребити и за објашњење агресивног онлајн понашања. Разлог је што су многи фактори који доводе до деиндивидуације, попут анонимности, у великој мери присутни и на интернету. Затим, ту је и *социјална дистанцираност*, до које доводи то што сајбер криминалци често не виде непосредне негативне последице које њихово понашање има по жртву. Тако дистанцираност делује као тампон између починиоца и жртве, што олакшава испољавање агресивности (Campbell & Kennedy, 2014).

Криминолог Марк Роџерс наводи да бројни криминалци користе менталне поступке којима оправдавају своја онлајн понашања. У такве поступке спадају: упоређивање свог лошег са лошијим понашањем других,

минимизирање последица свог понашања, пребацивање одговорности и окривљавање жртве. Ови поступци су описани у Бандуриној теорији моралности, која каже да ће особе бескрупулозног понашања променити начин размишљања да би оправдали своје поступке (Campbell & Kennedy, 2014).

Став да се починиоци кривичних дела осећају безбедно на интернету, и поред тога што је њихово понашање лако уочљиво (Casey, 2011), може се објаснити *ефектом онлајн дезинхибиције*. Ефекат је дефинисао Сулер (2004) да би објаснио појаву да људи често говоре и раде ствари на интернету које не би говорили и радили у свакодневном животу. До дезинхибиције, између осталог, доводи дисоцијација селфа, када онлајн део селфа постаје одговоран за изражавање хостилности или других девијантних понашања. Тако особа поменута понашања одваја од остатка свог живота и скида одговорност са себе.

Други фактор који доприноси феномену дезинхибиције је међусобна невидљивост током комуникације путем мејлова, четова и блогова. Она обухвата и недостатак перцепције невербалних знакова који су обично присутни и који сузбијају неприхватљива понашања током комуникације „лицем-у-лице" (Suler, 2004). Невидљивост саговорника доводи и до тешкоће перципирања социјалних улога, структура и норми и тиме олакшава појаву агресивног онлајн понашања (Kiesler & Sproull, 1992, према: Campbell & Kennedy, 2014).

Сулер (2004) разликује *бенигну дезинхибицију*, која подразумева дељење личних информација о себи (емоција, жеља, страхова), од *токсичне дезинхибиције*, која обухвата употребу непристојних речи, грубо критиковање других, испољавање љутње, непријатељства и упућивање претњи у сајберпростору. Пример токсичне дезинхибиције је онлајн узнемиравање (Whitty & Young, 2016). Дезинхибиција смањује вероватноћу да ће особа преузети одговорност за узнемиравање и да ће доживети осећање кривице (Guitton, 2012).

Структура личности утиче на онлајн понашање, укључујући и испољавање сајберкриминала. Значајни за онлајн понашање су антисоцијални и нарцистички поремећај личности (Campbell & Kennedy, 2014). Склоност лагању и неискреност карактеришу *антисоцијални поремећај личности* (American Psychiatric Association [APA], 2013b). Поменуте црте би могле да стоје у основи криминалног онлајн понашања које доноси мало или нимало награде, али и опасност од казне (Campbell & Kennedy, 2014). Ове особе могу да имају мањак увида у своја понашања, да минимизирају његове последице или да криве жртву. Са друге стране, истраживања показују да сајбер криминалци не тумаче своја дела као штетна или илегална и да понекад рационализују своја понашања управо кривећи жртве (мрежне администраторе или креаторе софтвера) због пропуста у испуњавању радних задатака (Campbell & Kennedy, 2014).

У контексту сајбер криминала помиње се и *нарцистички поремећај личности*, са карактеристикама попут преувеличаног доживљаја сопствене вредности и доживљаја привилегованости, тј. веровања да им други дугују посебно повољан третман или да ће се аутоматски покорити њиховим захтевима (APA, 2013b). Шо и сарадници (1998, према: Campbell & Kennedy, 2014) тврде да је друга карактеристика присутна код ИТ специјалиста који изнутра нападају радне организације, онда када надређени не препознају њихов труд или остварене резултате на очекивани начин. Оба поменута поремећаја личности карактерише рационализација негативног понашања, која се среће и код сајбер криминалаца (Campbell & Kennedy, 2014).

Нађена је сличност *Аспергерової синдрома*[4] и карактеристика које се стереотипно приписују хакерима (Zuckerman, 2001, према: Campbell & Kennedy, 2014). Преокупираност математиком, науком, технологијом и машинама се често јавља код ове деце и одржава се до одраслог доба, што може да резултује каријерама које се директно ослањају на поменута интересовања. Међутим, ове налазе никако не треба протумачити као доказ да Аспергеров синдром узрокује хакерисање. Једино је оправдано закључити да постоји сличност особина двеју поменутих група.

Дигитални доказ

Без обзира на то да ли су рачунари окружење у коме је почињено кривично дело или средство за његову реализацију, на њима ће у готово свим случајевима бити похрањени трагови о онлајн понашању. Такав траг се назива *дигитални доказ*, а дефинише се као било који податак сачуван или трансмитован коришћењем рачунара (тј. у дигиталном формату), који подржава или побија теорију о томе како је дошло до почињења кривичног дела или се односи на битне елементе извршења дела попут намере или алибија (Casey, 2011).

Подаци о томе када је фајл креиран, ко га је креирао и на ком рачунару, информације о налозима између којих су размењене поруке путем имејла и времену када је порука послата, а које чувају лог фајлови на различитим серверима, и подаци о брзини и месту кретања возила у датом тренутку представљају примере дигиталних доказа (Henseler, 2000, према: Casey, 2011). Интернет и други комуникациони системи могу да обезбеде доказе чак и када нису директно повезани са почињењем дела. Пример би биле камере постављене дуж градских улица када забележе извршење неког дела (Casey, 2011).

[4] Аспергеров синдром према најновијем ДСМ 5 приручнику не постоји као одвојена нозолошка категорија, већ се дијагностикује као поремећај из спектра аутизма без оштећења језичких или интелектуалних способности (APA, 2013a).

Персонални рачунари, паметни телефони и слични уређаји садрже информације о посећеним сајтовима и разне мултимедијалне садржаје, који представљају значајну бихевиоралну архиву и извор података о интересовањима, мотивима, жељама, плановима и активностима особе (Casey, 2011). На пример, лични сајтови или профили дају увид у слику коју починилац има о себи, у тренутно психичко стање, мотиве или фантазије, а записи које оставља за собом могу да укажу на евентуално постојање жртава и/или локација на којима се налази још доказа (Casey, 2012). Дигитални доказ може да укаже и на мере предострожности починиоца како би сакрио свој идентитет и отежао откривање. Пример је да уместо „Enochian" као корисничко име користи „En0ch|an" јер базе података не препознају да нула представља слово „о", а знак „|" слово „и" (Casey, 2012).

Рачунари и интернет могу да буду коришћени у сврху одабира, праћења, контактирања, успостављања односа поверења, ухођења, узнемиравања потенцијалних жртава, крађе новца са банковних рачуна, интелектуалне својине и идентитета, затим оштећења мрежних функција, лоцирања, прикупљања и чувања поверљивих или недозвољених садржаја, сужавања или ширења могућности за даљу дистрибуцију материјала итд. (Turvey, 2011).

Докази уопште, па и дигитални докази, служе да се оствари основни циљ истраге, а то је идентификовање починилаца кривичних дела (Rogers, 2003). У оквиру криминалног профилисања разликујемо два модела: *дедуктивно* и *индуктивно*. *Дедуктивно профилисање* се фокусира на конкретан случај који се расветљава у датом тренутку. Прецизније, на основу доказа који остају на месту злочина, а који указују на одређена понашања, и на основу изјава сведока и других података, доносе се закључци о вероватним карактеристикама починиоца (Shaw, 2006). На крају се дефинише бихевиорални профил починиоца. Са друге стране, *индуктивно профилисање* се ослања на статистичке анализе података о осуђеним починиоцима или групама испитаника сличних карактеристика. Статистичком анализом се долази до општих закључака о понашањима, цртама личности и мотивима починилаца (Petherick, 2002, према: Rogers, 2003; Shaw, 2006). Овај приступ креће од генералног према специфичном следећи индуктивну логику. Сличан приступ се користи у истраживањима описаним у уџбеницима сајберпсихологије (Whitty & Young, 2016; Kirwan, 2016a). Разлика је у томе што истраживања на којима почива индуктивно профилисање као узорак обично користе групе осуђеника, а истраживања из сајберпсихологије проучавају углавном студенте. Ово не треба схватити као правило, јер не важи у свим случајевима.

Профилисање функционише на исти начин за „офлајн" и онлајн починиоце и предузима се са истим циљевима. Ту спада: развијање истражних стратегија, сужавање списка потенцијалних осумњичених, развој стратегија интервјуисања осумњичених итд. Специфичност сајбер профилисања се огледа у томе што дигитални докази, за разлику од физичких,

могу лако да се униште или измене и постоје у сајберпростору, тј. на меморији рачунара или сервера, па тиме рачунар некада добија улогу јединог сведока (Rogers, 2003). Током онлајн профилисања форензичар се усредсређује на индикаторе кључних понашања попут претраге специфичних речи, историје посећиваних сајтова итд. (Rogers, 2003).

Дедуктивно криминално профилисање

Дедуктивно профилисање акценат ставља на конкретан случај, тј. на трагове који остају иза починиоца. Пример модела дедуктивног профилисања је *анализа бихевиоралних доказа* (*BEA – Behavioral Evidence Analysis*), коју је развио Турви (Turvey). БЕА се састоји из 4 корака: 1) прикупљање што је могуће више података о догађају; 2) детаљна анализа карактеристика жртве (виктимологија); 3) анализа особености места злочина, које су повезане са одлукама и понашањем починиоца; 4) закључивање о вероватним карактеристикама (цртама личности и понашању) починиоца, што се ослања на податке прикупљене у прва три корака. БЕА се као метод препоручује за примену ван САД, јер не почива на карактеристикама узорака починилаца одређених кривичних дела прикупљених на територији једне државе (што је типично за индуктивно профилисање). Због тога се очекује да дедуктивно профилисање буде мање културолошки пристрасно (Rogers, 2003).

Да би се разумело понашање починиоца током извршења кривичног дела неопходно је упознати се са концептима *modus operandi*, *понашања потписа* и *мотива*. *Modus operandi* (*MO*) састоји се из понашања која су нужна да би злочин био успешно реализован, па су та понашања функционална за његово извршење. Другим речима, концепт објашњава како је починилац извршио злочин (Turvey & Freeman, 2012). МО се у истрагама најчешће користи у сврху повезивања злочина почињених од стране истог починиоца или групе починилаца. Његове функције су да заштити идентитет починиоца, осигура успешно почињење дела и олакша напуштање места злочина.

Када говоримо о МО понашањима релевантним за сајбер криминал, можемо навести (Turvey, 2011):

1) *степен планирања кривичног дела*, о коме сведоче белешке о одабраној локацији или прикупљеним информацијама о жртви, садржаних у мејлу или фајловима рачунара;
2) *средства уз помоћ којих је почињено дело* (врста оперативног система, тип конекције, софтвер итд.);
3) *надгледање жртве и/или потенцијалног места злочина* (праћење активности жртве на интернету, постова на друштвеним мрежама, личних информација које дели итд.);

4) *одабир места злочина* – слање претећих порука преко одређених сајтова, конверзација са жртвом у собама за ћаскање (тзв. *chat rooms*), како би се успоставио пријатељски контакт и емоционални однос, а са циљем да жртва лакше пристане на сексуални контакт (тзв. *grooming*), хостовање недозвољеног материјала на серверу са намером да се даље тајно дистрибуира итд.;
5) *коришћење оружја током почињења дела* – покушај убацивања вируса у рачунар жртве путем мејла;
6) *мере предострожности* – коришћење псеудонима од стране починиоца, упад на приватни рачунарски систем који се користи као база за даље операције, лажирање ИП адресе итд.

Проактивни карактер односа МО и сајбер криминала огледа се у томе што починиоци могу да користе постојећу технологију да унапреде свој МО како би постигли жељене циљеве или савладали препреке које им стоје на путу током почињења дела. Пример који показује на који начин дигиталне технологије могу да унапреде МО је случај једног швајцарског пара који је, путем интернета, са купцима из САД уговарао и на велико продавао фотографије деце која учествују у сексуалним активностима (Turvey, 2011). Дакле, МО је унапређен тако што су починиоци, уз помоћ информационо-комуникационих технологија, ступили у контакт са великим бројем купаца и зарадили више новца него да су слике продавали само „на локалу".

Треба имати у виду да се у контексту сајбер криминала може појавити *аутоматизовани МО*, тј. да починилац може аутоматизовати одређене активности уз помоћ специјализованих софтвера, што отежава доношење закључака о броју починилаца. Такође, већа техничка писменост пружа могућност починиоцу да намерно мења свој МО, па се тада он описује као *динамичан МО* (Casey, 2012).

Потпис се односи на понашања која нису неопходна да се почини злочин, а одражавају дубље психолошке потребе починиоца. Ова понашања у основи нису функционална за почињење датог дела. Она рефлектују психодинамику починиоца, која је релативно стабилна током времена (Turvey & Freeman, 2012). Пример потписа у контексту сајбер криминала би било додељивање идиосинкратичких ознака и назива фајловима или кодовима (Rogers, 2003). Препознавање овог типа понашања даје могућност истражитељима да савладају тешкоће до којих доводи аутоматизовани или динамични МО (Casey, 2012).

За разлику од МО, који одговара на питање како је злочин почињен, *мотиви* се односе на питање зашто је почињен. Они нагоне починиоце да чине кривична дела и независни су од технологије (Turvey, 2011). Роџерс (2001, према: Rogers, 2003) наводи да у основи сајбер криминалитета стоје мотиви попут похлепе, освете, беса, перверзности, жеље за моћи или политички мотиви. Сличне мотиве наводи социолог Пол Тејлор (1999, према: Campbell

& Kennedy, 2014), који је путем интервјуа установио да се мотивација сајбер криминалаца своди на 6 основних категорија: зависност, радозналост, досада, моћ, признање и политички мотиви. Једна група аутора наводи да су слични мотиви присутни код хакера (Chiesa, Ducci, Ciappi, 2009).

Познавање МО, понашања потписа и мотива сајбер криминалаца омогућује истражитељу да створи представу о вештинама које имају, да дефинише критеријуме за анализу онлајн садржаја (на пример, претрагу кључних речи или ранијих верзија фајлова), да га усмери на одређену категорију починилаца или део сајберпростора (на пример, на сајтове са одређеном тематиком) (Rogers, 2003). Такође, може да послужи као основа за доношење одлука о адекватности остваривања контакта са починиоцем у датом тренутку и најбољем начину приступања (Casey, 2012).

Иако исти мотиви покрећу сва понашања, њихово испољавање може да се мења у онлајн окружењу (Turvey, 2011). Ипак, типологије развијане на основу испитивања починилаца кривичних дела у физичком свету могу да се примене и на објашњење сајбер криминалитета. Пример је *бихевиорално-мотивациона типологија Николаса Грота* (Turvey, 2011; Freeman & Turvey, 2012). Он разликује 6 облика понашања починилаца: компензаторно, тј. понашања охрабривања моћи, понашање потврђивања моћи, гневно-осветничко понашање (одмазда), садистичко, опортунистичко и понашање оријентисано на профит. Типологија се примењује тако што се, на основу информација и доказа везаних за случај, класификују понашања починиоца.

За разлику од Гротове типологије, која је развијена пре појаве сајбер криминала, постоје новије методе дедуктивног профилисања. Једна таква (група) метода се назива *процена на даљину* (*Remote Assessment*). Њу описује Шо (2006) у контексту расветљавања случаја инсајдерских претњи упућиваних мејлом руководству једне компаније. Ове методе су психолингвистичке јер се баве анализом писаних трагова (Casey, 2012). Примењују се у ситуацијама када није пожељно или могуће остварити директан контакт и када циљ није само идентификовати починиоца већ и управљати његовим понашањем како би се истрага до краја успешно спровела. Централно место заузима анализа садржаја писаних трагова (Shaw, 2006).

Поменута анализа се користи у различите сврхе. На пример, може да послужи у одређивању броја аутора различитих мејлова. У том случају, поред контекста комуникације (одређивања ко је мета напада, времена када се напад догодио, догађаја који га прате, мрежног саобраћаја итд.) узимају се у обзир три индикатора. Сваки наредни пружа мању могућност за поуздано доношење закључака да је починилац једна конкретна особа. Најспецифичнији индикатор су *грешке у куцању*, тачније идиосинкратичка вербална понашања, која обухватају специфични стил писања, скраћивања речи, граматички неправилно или неуобичајено коришћење речи, организацију написаног итд. Други индикатор су делови написаног и речник који

указују на одређено емоционално стање, личне и интерперсоналне карактеристике. Иако и они могу бити специфични за појединца, истовремено могу бити и заједнички особама које имају сличну структуру личности и, сходно томе, доживљавају слична осећања у датом контексту. Трећи, најмање специфични индикатор је *доследно јављање одређених тема или описа проблема у тексту*. Овај индикатор има најмању поузданост јер велики број особа унутар једне организације може да дели слична искуства и пише о сличним темама.

Друга сврха анализе садржаја је процена степена опасности починиоца по друге. О томе се закључује на основу садржаја који указује на мотивацију и намере починиоца или у коме он описује своје виђење жртве, наводи примере сопственог агресивног понашања, закључује да се отуђио од других или на основу података о специфичним плановима за напад, сопствене виктимизираности од стране људи из непосредног окружења, менталном стању, изложености стресорима итд. (Shaw, 2006).

Трећа сврха коришћења методе је доношење закључака о карактеристикама починиоца. Овде разликујемо два приступа. Први је *квантитативни*, базиран на индикаторима, у које, поред већ поменутог стила писања, спадају и:

1) *фреквенција одређених речи* – може да укаже на неке психолошке карактеристике. На пример, постоји снажна веза између коришћења негација („не“, „никад“) и доживљаја беса или опозиционалности, као и веза коришћења заменице „ја“ и пасивности или склоности да се особа осети виктимизованом (Weintraub 1989, према: Shaw, 2006);
2) *комплексност и дужина речи* – указују на развијеност вокабулара, а представљају и добре индикаторе интелигенције (Pennebaker & King, 1999, према: Shaw, 2006);
3) *упоредна фреквенција више речи* – на пример, сразмера коришћења заменице „ја“ у односу на „ми“ указује на склоност особе да ради у тиму или самостално.

Осмишљени су и сложенији алгоритми за процену психолошких карактеристика. Утврђено је, на пример, да се склоност особе ка иницирању акције у односу на реагибилност када акцију покрене неко други може проценити када се сразмера коришћења „ја“ у односу на „ми“ подели учесталошћу коришћења заменице „мене (ме)“ (Weintraub, 1987, према: Shaw, 2006).

Још неки примери примене квантитативног приступа су: процена ароганције и грандиозности, када, на пример, самопоуздање надмашује сензитивност коју аутор има према другима или процена когнитивне ригидности, у ком случају аутор учесталије користи мање сложене речи (Shaw, 2006).

Квалитативни приступ се ослања на клиничку психологију, психолошке теорије и дијагностичке критеријуме. Често је незаменљив за

утврђивање психичких поремећаја. У индикаторе поремећаја спадају: значајно изражени проблеми са организацијом написаног, грешке, упадљиве варијације емоционалног тона и забринутост аутора због вулнерабилности према спољашњим факторима (Shaw, 2006). Што даље демонстрира да овакав приступ омогућује доношење закључака и о годинама и полу починиоца, проблемима у интерперсоналним односима, психопатолошким испољавањима (параноидне тенденције, опсесивност) итд. Као пример можемо узети закључивање о постојању опсесивних црта. У прилог њиховој присутности говоре преокупираност детаљима, правилима, листама, процедурама и наглашавање значаја одржавања контроле у животу. Сличну методологију су развили Рашид и сарадници (2013, према: Whitty & Young, 2016) како би детектовали онлајн превару и открили праве податке о полу и годинама аутора порука.

Индуктивно криминално профилисање

Индуктивно профилисање се ослања на статистичке податке о починиоцима кривичних дела. Оно даје добар увид у карактеристике починилаца претходних дела, а може да послужи у сврхе дијагностиковања и третирања пратећих поремећаја. Међутим, неки аутори сматрају да овакав приступ има ограничену вредност у истрази јер може да наведе на погрешан траг. То се дешава онда када се донесу неисправни закључци о типичним карактеристикама неке групе починилаца, а истражитељ се ослони на њих да би сузио круг осумњичених особа (Casey, 2012). Индуктивно профилисање, такође, обухвата неколико модела. Овде спада *Холмсова типологија* коју је даље развио ФБИ (FBI), па је због тога позната и под именом *ФБИ модел* (Rogers, 2003). Она разликује два типа починилаца: организоване несоцијалне и дезорганизоване асоцијалне, сваки са својим карактеристикама. Када се злочин догоди, на основу карактеристика места злочина се закључује о карактеристикама починиоца. Оне су утврђене претходним проучавањем релативно малог броја особа. Након установљавања ком типу починилац припада, трага се за особама које се уклапају у карактеристике тог типа, чиме се сужава опсег осумњичених. Овакво резоновање се одвија под претпоставком да ће особе на које ће се наилазити током истраге (у будућности) имати исте карактеристике као оне чијим се проучавањем дошло до карактеристика датог типа (Petherick & Turvey, 2012). Други модел у оквиру индуктивног профилисања је *истражна психологија*, коју је развио Кантер (Rogers, 2003). Иако другачије именује категорије починилаца, овај приступ у основи следи исту логику као ФБИ модел.

Истраживања на која се ослањају методе индуктивног профилисања углавном проучавају групе процесуираних починилаца за одређена дела, да

би утврдили њихове типичне карактеристике (Shaw, 2006). Истраживања у оквиру сајберпсихологије раде исто то, с тим да узорке углавном чине студенти, тј. припадници опште популације, који, попуњавајући упитнике самопроцене, саопштавају да ли су се ангажовали у одређеним, девијантним онлајн активностима. Примена упитника самопроцене је уједно и најједноставнији начин испитивања мотивације сајбер преступника и криминалаца (Campbell & Kennedy, 2014). И поред мишљења да су оваква истраживања ограничене вредности (Casey, 2012) важно је имати их у виду, јер поједини истраживачи истичу како разумевање мотива и психолошких корелата сајбер криминала омогућава превентивно и протективно делање (Campbell & Kennedy, 2014).

Две особине личности су се показале као предиктори предузимања и успешности хакерских напада (Bachmann, 2010). Прва је преференција према рационалном промишљању приликом доношења одлука, која је позитивни предиктор и предузимања и успешности напада. Друга особина је склоност ка преузимању ризика која доводи до већег броја, али мање успешних напада.

Група аутора је установила да студенти психологије који погађају шифре, користе туђе рачунаре, прегледавају и мењају фајлове без дозволе и користе или креирају вирусе имају слабије интернализовани морални компас и склони су манипулацији и експлоататорском понашању (Rogers, Smoak, Liu, 2006). Противно стереотипу који је присутан у медијима, истраживање је показало да особе склоне описаним активностима нису више интровертне у односу на оне које се не понашају на тај начин. Касније је спроведено истраживање у коме су учествовали студенти технолошког факултета (Rogers, Seigfried, Tidke, 2006), а које је дало дијаметрално супротне резултате. Још једно истраживање спроведено на узорку студената је показало да су моралне вредности у негативној корелацији са крађом идентитета, електронским булингом и креирањем вируса (Seigfried-Spellar & Treadway, 2014).

Истраживање повезаности сајбер криминала и психопатије је показало да су црте психопатије значајно повезане са: хаковањем, крађом идентитета, недозвољеним надгледањем мрежног саобраћаја, писањем вируса и уништавањем веб-сајтова. Показало се и да је сајбер криминалитет повезан са другим типовима антисоцијалног понашања, што сугерише да се може тумачити као индикатор опште тенденције ка криминалном понашању и да се опште теорије криминалитета могу користити у објашњењу сајбер криминала (Seigfried-Spellar, Villacís-Vukadinović, Lynam, 2017).

Психопатија на узорку студената значајно корелира са тенденцијама према хакерисању и порнографском садржају (Williams, McAndrew, Learn, Harms, Paulus, 2001, према: Seigfried-Spellar et al., 2017). Нађено је и да степен самоконтроле корелира са активностима хаковања (Bossler & Burruss, 2010) и дигиталном пиратеријом (Marcum, Higgins, Wolfe, Ricketts, 2011).

Конкретно, особе које су у стању да сагледају последице свог понашања биће мање склоне пиратерији.

Резултати једне метаанализе показују да су онлајн преступници нешто млађи од „офлајн" преступника и да их карактерише већа емпатичност према жртви, израженија сексуална девијантност и мања способност да се представе на (неоправдано) оптимистичан начин (Babchishin, Hanson, Hermann, 2010). Аутори су опажене разлике објаснили већим степеном контроле и израженијим психолошким баријерама онлајн починилаца, које им онемогућавају да реализују своје потребе.

Истраживања сексуалних преступника у оквиру дечије порнографије показују да њих карактерише емоционална неадекватност и високо изражена девијантност (Henry, Mandeville-Norden, Hayes, Egan, 2010), да су млађи, да живе сами, нису у вези и немају деце, што значи да су социјално изоловани (Reijnen, Bulten, Nijman, 2009).

Истраживање онлајн ухођења (*stalking*) показује да су починиоци често били изложени сексуалном злостављању у детињству (Ménard & Pincus, 2012), а Алекси и сарадници (2005, према: Whitty & Young, 2016) налазе да имају већу вероватноћу да повреде себе од оних који уходе у „офлајн" окружењу.

Закључак

Широко посматрајући, постоје два правца досадашњих промишљања и истраживања у области сајбер профилисања. Са једне стране, развијане су методе индуктивног и дедуктивног приступа, првенствено у оквиру форензичких дисциплина, укључујући и форензичку психологију. Са друге стране, аутори истраживања у сајберпсихологији су трагали за демографским и психолошким особинама испитаника, груписаних на основу девијантних сајбер активности у којима су се ангажовали. Њихов циљ је био да дефинишу типичне карактеристике, које би, када једном буду валидиране низом истраживања, могле да постану део „профила" дате групе. У том аспекту је логика истраживања у сајберпсихологији слична логици истраживања на којима почива индуктивно профилисање. Разлика је у томе што истраживачи у сајберпсихологији не наводе експлицитно да им је циљ дефинисање психолошког профила одређене групе испитаника, иако карактер њихових истраживања то имплицира.

Повећање интересовања форензичких сајберпсихолога за профилисање, којег актуелно мањка (Kirwan, 2016a), и прелазак са узорака студената на узорке осуђених починилаца потенцијално би довело до приближавања двеју истраживачких струја. Даље комбиновање резултата таквих истраживања са анализом места злочина би могло да допринесе идентификовању

специфичних трагова који остају иза починилаца одређених психолошких карактеристика, што би резултовало приближавањем индуктивног и дедуктивног приступа. Потребно је имати у виду и то да се подгрупе сајбер криминалаца разликују у погледу мотива и активности (Campbell & Kennedy, 2014), због чега не треба трагати за јединственим профилом.

Литература

American Psychiatric Association. (2013a). Neurodevelopmental Disorders. In: *Diagnostic and Statistical Manual of Mental Disorders* (5th ed.). American Psychiatric Association Publishing.

American Psychiatric Association. (2013b). Personality Disorders. In: *Diagnostic and Statistical Manual of Mental Disorders* (5th ed.). American Psychiatric Association Publishing.

Babchishin, K. M., Hanson, R. K., & Hermann, C. A. (2011). The Characteristics of Online Sex Offenders: A Meta-Analysis. *Sex Abuse*, 23 (1), 92–123.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, 4 (1–2), 643–656. Preuzeto sa: https://www.cybercrimejournal.com/bachmannjandec2010.htm

Bossler, A. M. & Burruss, G. W. (2010). The General Theory of Crime and Computer Hacking: Low Self-Control Hackers? In: T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (38–67). New York, NY: IGI Global.

Campbell, Q. & Kennedy, D. M. (2014). The Psychology of Computer Criminals. In: S. Bosworth, M. E. Kabay, E. Whyne (Eds.), *Computer Security Handbook* (387–419). New York, NY: John Wiley & Sons.

Casey, E. (2012). Cyberpatterns: Criminal Behavior on the Internet. In: B. E. Turvey (Ed.), *Criminal Profiling: An Introduction to Behavioral Evidence Analysis* (361–178). San Diego, CA: Academic Press.

Casey, E. (2011). Foundations of Digital Forensics. In: E. Casey (Ed.), *Digital Evidence and Computer Crime* (3–34). San Diego, CA: Academic Press.

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, FL: CRC Press.

Freeman, J. & Turvey B. E. (2012). Interpreting Motive. In: B. E. Turvey (Ed.), *Criminal Profiling: An Introduction to Behavioral Evidence Analysis* (311–330). San Diego, CA: Academic Press.

Guitton, C. (2012). Criminals and Cyber Attacks: The Missing Link Between Attribution and Deterrence. *International Journal of Cyber Criminology*, 6 (2), 1030–1043. Preuzeto sa: https://www.cybercrimejournal.com/guiton2012julyijcc.pdf

Henry, O., Mandeville-Norden, R., Hayes, E., & Egan, V. (2010). Do Internet-Based Sexual Offenders Reduce to Normal, Inadequate, and Deviant Groups?. *Journal of Sexual Aggression*, 16 (1), 33–46.

Hogan, M. D. & Newton, E. M. (2015). *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization*

to Achieve U.S. Objectives for Cybersecurity. (NISTIR 8074, Vol. 2). National Institute of Standards and Technology.

Kirwan, G. (2016a). Forensic Cyberpsychology. In: I. Connolly, M. Palmer, H. Barton, G. Kirwan (Eds.), *An Introduction to Cyberpsychology* (283–308). Oxfordshire: Routledge.

Kirwan, G. (2016b). Introduction to Cyberpsychology. In: I. Connolly, M. Palmer, H. Barton, G. Kirwan (Eds.), *An Introduction to Cyberpsychology* (29–50). Oxfordshire: Routledge.

Marcum, C. D., Higgins, G. E., Wolfe, S. E., & Ricketts, M. L. (2011). Examining the Intersection of Self-Control, Peer Association, and Neutralization in Explaining Digital Piracy. *Western Criminology Review*, 12 (3), 60–74. Preuzeto sa: http://www.westerncriminology.org/documents/WCR/v12n3/Marcum.pdf

Ménard, K. S. & Pincus, A. L. (2011). Predicting Overt and Cyber Stalking Perpetration by Male and Female College Students. *Journal of Interpersonal Violence*, 27 (11), 2183–2207.

Petherick, W. A. & Turvey B. E. (2012). Criminal Profiling: Science, Logic, and Cognition. In: B. E. Turvey (Ed.), *Criminal Profiling: An Introduction to Behavioral Evidence Analysis* (41–65). San Diego, CA: Academic Press.

Reijnen, L., Bulten, E., & Nijman, H. (2009). Demographic and Personality Characteristics of Internet Child Pornography Downloaders in Comparison to Other Offenders. *Journal of Child Sexual Abuse*, 18 (6), 611–622.

Rogers, M. (2003). The Role of Criminal Profiling in the Computer Forensics Process. *Computers & Security*, 22 (4), 292–298.

Rogers, M. K., Seigfried, K., & Tidke, K. (2006). Self-Reported Computer Criminal Behavior: A Psychological Analysis. *Digital Investigation*, 3, 116–120.

Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-Reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis. *Deviant Behavior*, 27 (3), 245–268.

Savet Evrope. (2001). *Konvencija o sajber kriminalu*. Preuzeto sa: https://rm.coe.int/1680081561

Seigfried-Spellar, K. C. & Treadway, K. N. (2014). Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behavior*, 35 (10), 782–803.

Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer Criminal Behavior Is Related to Psychopathy and Other Antisocial Behavior. *Journal of Criminal Justice*, 51, 67–73.

Shaw, E. D. (2006). The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations. *Digital Investigation*, 3 (1), 20–31.

Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior*, 7 (3), 321–326.

Turvey, B. E. (2011). Modus Operandi, Motive, and Technology. In: E. Casey (Ed.), *Digital Evidence and Computer Crime* (285–304). San Diego, CA: Academic Press.

Turvey, B. E. & Freeman J. (2012). Case Linkage: Offender Modus Operandi and Signature. In: B. E. Turvey (Ed.), *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*. (331–360). San Diego, CA: Academic Press.

Whitty, M. T. & Young, G. (2016). *Cyberpsychology: The Study of Individuals, Society, and Digital Technologies*. Hoboken, New Jersey: John Wiley & Sons.
Woodhams, J. & Toye, K. (2007). An Empirical Test of the Assumptions of Case Linkage and Offender Profiling with Serial Commercial Robberies. *Psychology, Public Policy, and Law*, 13 (1), 59–85.

Dušan Lj. VLAJIĆ
University of Niš
Faculty of Philosophy
Department of Psychology

Forensic Cyberpsychology and Approaches to Criminal Profiling

Summary

Although there are plenty of theories which consider psychological factors of criminal behaviour and almost every criminal act has a digital aspect, criminal profiling is not so popular among forensic psychologists, especially when it comes to cybercrime. Thus, the goal of this paper is to give a brief overview of literature considering psychological factors related to deviant computer and online behaviour. Two basic approaches of criminal profiling, inductive and deductive, will be presented, as well as their advantages, disadvantages, logic they follow and concepts they rely on when analysing digital evidence in order to narrow suspect pools. Concrete models developed under each approach will be briefly portrayed. Moreover, studies from the field of cyberpsychology will be presented and their relationship with profiling will be discussed, particularly with inductive approach, which is original contribution of this paper. At the very end, suggestions for overcoming limitations of previous studies and converging disciplines of criminal profiling and cyberpsychology will be offered.

Keywords: criminal profiling; inductive profiling; deductive profiling; cybercrime; cyberpsychology; digital evidence.