

Др Владимир УРОШЕВИЋ,  
УКП СБПОК, Одељење за сузбијање ВТК  
Мр Сергеј УЉАНОВ,  
УКП НЦБ ИНТЕРПОЛ, Београд  
Мр Звонимир ИВАНОВИЋ,  
Криминалистичко-полицијска академија, Београд

## Фокуси у сарадњи криминалистичких полиција са аспекта Националног централног бироа ИНТЕРПОЛ-а Београд

УДК: 351.746.2 : 061.1 (100)

*Апстракт:* Аутори покушавају да у раду прикажу и повежу стратешки, тактички и оперативни ниво рада у различитим областима комплексних делатности којима се бави НЦБ ИНТЕРПОЛ у Београду. Покушано је фузионисање расположивог суделовања многих линија рада, при чему је највећи акценат, због изузетног значаја, стављен на међународну полицијску сарадњу у области високотехнолошког криминала, са аспекта интеграције Републике Србије у ЕУ. Фокуси који су у раду приказани избор су аутора према оперативном значају у размени података и постојећој друштвеној опасности ових области криминала.

*Кључне речи:* ИНТЕРПОЛ, међународна полицијска сарадња, високотехнолошки криминал.

### Увод

Национални централни биро ИНТЕРПОЛ-а Београд чини тежиште Министарства унутрашњих послова Републике Србије преко кога се одвија међународна полицијска сарадња, у смислу размене информација од, пре свега, оперативног и тактичког, а у извесним случајевима и стратешког значаја. Поседујући атрибуте детерминисане међународним префиксом, Национални централни биро ИНТЕРПОЛ-а Београд представља нуклеус у методолошком, информатичком и комуникационом смислу, организационе јединице Министарства унутрашњих послова Републике Србије под називом Одељење за међународну полицијску сарадњу, која је формацијски смештена у Управу криминалистичке полиције наведеног Министарства.

У Одељењу за међународну полицијску сарадњу, поред помоћних техничких, информатичких, документалистичких и аналитичких, за-

ступљене су све главне линије рада криминалистичке полиције. Уз постојећу архиву, коју чини преко пола милиона досијеа, те самосталну интерну базу података, ИНТЕРПОЛ Београд у свом саставу има и дактилоскопску радну јединицу која омогућава утврђивање идентитета у реалном времену, у односу на захтев стране криминалистичке полиције.

Имајући у виду наведено, напомињемо да је ИНТЕРПОЛ Београд радно дефинисан као склоп информатичко-комуникационих и аналитичко-документалистичких система прожетих компактном базом података, коју чине сви криминалистичко релевантни институти, од личних података, до бројева шасија на возилу, телефонских бројева, чак и назива пловила. Као такав, ИНТЕРПОЛ Београд је прави пример оптималног коришћења конзистентног система кроз токове радног процеса засноване на стриктном поштовању задатих протокола.

У својим свакодневним активностима, оличеним у сменском извршавању константних радних задатака, Национални централни биро ИНТЕРПОЛ-а Београд, по природи ствари, прати трендове у настанку, развоју и сузбијању актуелних облика и врста криминалних активности. Уколико би дихотомно посматрали рад криминалистичке службе, са становишта његове сврхе, закључили би да ИНТЕРПОЛ Београд, као део националне криминалистичке службе, такође делује превентивно и репресивно, према начину на који реализује захтеве иностраних криминалистичких полиција. У зависности од методологије поступања у односу на акценат у кореспонденцији са страним партнерима, ИНТЕРПОЛ Београд вршећи провере лица *post delictum* реагује репресивно, доприносећи да полиције других држава, баш као и друге организационе јединице Министарства унутрашњих послова Републике Србије, формирају комплетан профил извршиоца и потенцијалних извршиоца криминалних активности. Са друге стране, проактивно обавештавајући домаћу и стране полиције о потенцијалним претњама страних и домаћих организованих криминалних група и појединих делинквената, ИНТЕРПОЛ Београд испуњава волумен превентивне димензије свога функционисања.

Дакле, на основу свега реченог можемо закључити да српски Национални централни биро ИНТЕРПОЛ-а на савремен начин држи корак са дневним светским збивањима на плану борбе против криминала. Као пример који ће са аспекта праксе поткрепити наведену тврдњу, направићемо осврт на фокусе у међународној сарадњи криминалистичких служби, који су *ipso facto* представљали приоритете у остваривању циљева Националног централног бироа ИНТЕРПОЛ-а Београд. С обзиром да је у тој сарадњи, због динамичне проблематике, од значаја обрадити поједине одабране линије рада, исте ће у даљем току бити појединачно обрађене и анализирани.

## ***Имовински деликти***

Најпре, Национални централни биро ИНТЕРПОЛ-а је допринео да се утврди идентитет више десетина лица која су повезана са серијама разбојништава учињених на штету златара и радњи са скупоценим ручним сатовима, дијамантима и другим драгоценостима на подручју Западне Европе. Поређењем отисака прстију и ДНК профила омогућено је да стране криминалистичке службе утврде идентитет особа које су лишиле слободе под лажним личним подацима. Та лица су уз коришћење лажних личних података, користила и путне исправе са уметнутом фотографијом и туђим генералијама, тако да су извештаји страних криминалистичких служби били пуни противречности, које су улогом ИНТЕРПОЛ-а Београд успешно отклоњене. То је учињено ефикасном координацијом рада подручних полицијских управа и коришћењем постојеће интерне архиве и базе података самог Бироа.

## ***Наркотици***

Такође су и бројне контролисане испоруке опојних дрога на релацији Немачка – Албанија – Немачка, Чешка – Турска – Чешка и Аустрија – Турска – Аустрија у свим случајевима транзитно, преко територије Србије и подручја Косова и Метохије, успешно реализоване у сарадњи криминалистичких служби суседних држава, те држава извора и дестинације посредством ИНТЕРПОЛ-ове заштићене комуникације, и у неким случајевима уз подршку официра за везу страних полиција, који су, ради међународне полицијске сарадње, деташирани у своја матична дипломатско-конзуларна представништва у Београду.

## ***Потражна делатност***

Активна потражна делатност ИНТЕРПОЛ-а Београд дала је резултата у бројним лишењима слободе домаћих и страних држављана који су се налазили у бекству у страним државама, по међународним потерницама издатим уз сагласност Министарства правде Републике Србије, а на захтев локалних надлежних правосудних органа и затворских установа.

## ***Организоване криминалне групе са етничком кохезијом***

Организоване криминалне етничке групе које на овим просторима врше кривична дела, а која чине лица претежно албанске националности, посебно у области кријумчарења опојних дрога, биле су посебан предмет интересовања ИНТЕРПОЛ-а Београд, с обзиром да је Србија члани-

ца ИНТЕРПОЛ-ове радне групе која се на оперативном нивоу бави сузбијањем илегалног промета хероина и кокаина, организованом од стране албанских криминалних група у свету, а пре свега у Југоисточној Европи, на потезу од Словеније до Молдавије. До сада је неколико лица из наведеног миљеа било лишено слободе, уз остварене заплене опојне дроге од стране суседних држава, чему је допринело активно учешће српске криминалистичке службе посредством Националног централног бироа ИНТЕРПОЛ-а Београд.

### ***Високотехнолошки криминал (ВТК)***

Уколико проучимо и значај који ЕУ придаје проблематици ВТК кроз признавање и широко прихватање Ковенције о ВТК<sup>1</sup> и додатног протокола о ксенофобији и расизму, видећемо да сузбијање ВТК, кроз међународну полицијску сарадњу, представља један од кључних услова за успешне интеграције у ЕУ. Природа те врсте криминала је веома одређујућа у креирању поступања свих актера у супростављању тој пошасту, која поприма пандемијске размере. Транснационалност, неограничена анонимност, значајна брзина *деловања*, неограничене могућности употребе нових технолошких достигнућа су само делић описаних елемената проблематике ове појаве. Сегменти полицијске сарадње који се односе на ВТК у садашњем тренутку најчешће су базирани на областима везаним за рачунарске преваре, преваре са платним картицама и дечију порнографију, али су такође присутни и други облици кривичних дела из области безбедности рачунарских података, као и кривичних дела која се врше уз помоћ рачунара и рачунарских мрежа. Код појединих случајева о којима ће се у раду расправљати неопходно је разумети да је због интереса одвијања поступка немогуће ући дубље у проблематику, већ је довољно приказати само сегменте који могу бити интересантни за тематику рада а неће штетити претходном и главном поступку. У последњих неколико месеци одиграли су се веома интересантни случајеви везани за ВТК у Србији, а у већем броју случајева било је и елемената транснационалности.

Како се у литератури наводи (Урошевић, et al., 2010:7-9), у току 2008. и 2009. године на територији Републике Србије од стране оштећених лица пријављено је десет случајева<sup>2</sup> са елементима „Нигеријских превара“ или „419 превара“<sup>3</sup> против непознатих учинилаца (Урошевић, 2009:145-

<sup>1</sup> На енглеском језику: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG> доступна 29. 3. 2010. год.

<sup>2</sup> У евиденцијама НЦБ ИНТЕРПОЛ-а Београд, у погледу превара путем интернета (лутрија, спортске преваре, варање колекционара, наручивање на туђе картице, све врсте превара), за период од 3. 8. 2001. до 1. 3. 2010. поступано је у укупно 256 предмета. У расподели по годинама то изгледа овако: 2001:9; 2002:15; 2003:13; 2004:16; 2005:35; 2006:30; 2007:41; 2008:34; 2009:52; 2010:11.

<sup>3</sup> Назив им долази из нигеријског кривичног закона којим превару дефинишу у члану бр. 419 (који је део поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“, који

157). Тим кривичним делима оштећени су држављани Републике Србије и предузећа са наше територије, а укупна имовинска штета износила је преко 60.000 ЕУР-а. Оштећена лица су извршиоцима кривичних дела новац слала преко сервиса Western Union и MoneyGram. У септембру (29. септембар) 2009. год. уследиле су и три нове преваре. У тим кривичним делима жртве су биле један грађанин и две фирме, а укупна штета износила је 9.500 долара.<sup>4</sup> *О могућим модалитетима тог облика рачунарске преваре може се више пронаћи у стручној литератури, на пример др Владимир Урошевић виšekратно је писао о томе, као и други стручњаци на том пољу.* Поменути облици преваре јесу стандардни облици тзв. нигеријске преваре, изведене на тај начин што је један грађанин примио електронску пошту – мејл у којем се моли да помогне у пребацивању веће суме новца из Сенегала у Африци. Пошиљаоци оваквих мејлова углавном се представљају као рођаци неких од званичника или државника страних земаља, који увек желе да пребаце велике своте новца, за шта им је потребан банковни рачун из друге земље, а за узврат обећавају одређену провизију. Процесуирање таквих дела велики је проблем, посебно зато што извршиоци долазе са подручја неких од афричких земаља са којима је сарадња у тој области веома слаба.

Описане преваре су углавном вршене помоћу SPAM<sup>5</sup> порука, уз интензивно коришћење метода социјалног инжењеринга, а комуникација је, након одговора од стране оштећених на SPAM поруку, углавном вршена преко бесплатних налога за електронску пошту отвораних на интернет сервисима Yahoo, Hotmail и др. Поред описаног употребљаване су и лажне интернет адресе на којима су се налазиле презентације постављене од стране извршилаца кривичних дела, са намером да обману наивне кориснике интернета. У реализацији превара коришћена је и фалсификована документација државних органа и предузећа Нигерије, Гане, Сенегала, Камеруна и других држава са територије Западне Африке. Утврђено је и да су за скривање идентитета на интернету извршиоци користили приступе на јавним местима, нпр. у *Cyber* кафеима.<sup>6</sup> У комуникацији са

дефинише ово кривично дело. Америчко друштво за дијалектику је утврдило да се израз „Превара 419“ користи од 1992. године.

<sup>4</sup> [http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=09&dd=29&nav\\_id=383854&nav\\_category=206](http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=09&dd=29&nav_id=383854&nav_category=206) доступан 27. 3. 2010. год.

<sup>5</sup> Што се тиче термина, сматра се да порекло води из једног скеча чувене енглеске групе комичара Monty Python flying circus. Више о томе на [http://en.wikipedia.org/wiki/Spam\\_\(electronic\)#Origin\\_of\\_the\\_term](http://en.wikipedia.org/wiki/Spam_(electronic)#Origin_of_the_term) доступан 20. 3. 2010. год. У питању су веће количине нежељене поште, незахтеване, љубре поште.

<sup>6</sup> Корисници тих сервиса се често идентификују јединственом ознаком која представља само идентификатор одређеног рачунара или места конекције, дакле у питању је групно а не идентификујуће обележје, али опет може представљати квалитетну индицију на располагању органима гоњења у расветљавању дела. Упоредити са Урошевић, В., Уљанов, С., Вуковић, Р., (2010). *Политиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије*, Зборник радова са саветовања, стр. 7-9.

оштећеним лицима са наше територије коришћена су лажна идентификациона обележја званичника наведених држава, свештеника, адвоката и сл. Коришћење интернет сервиса и програма на интернету, за прикривање IP адреса у овим случајевима било је веома распрострањено.<sup>7</sup> У случајевима „нигеријских превара“ чије су жртве држављани Републике Србије радило се о преварама извршеним на неколико начина и то: слањем обавештења о лажним добицима на лутрији помоћу којих су жртве превара методама социјалног инжењеринга навођене да поверују да су добитници награда, након чега су уплаћивали одређене суме новца да би им се омогућило подизање награде, и слањем обавештења о наследству помоћу којих су жртве превара методама социјалног инжењеринга навођене да поверују да су наследиле одређену количину новца, након чега су уплаћивали одређене суме да би им се омогућила исплата наслеђеног новца. Кривична дела су иницирана са подручја Нигерије, Сенегала и Бенина, а међународна полицијска сарадња са наведеним државама до данас није довела до значајнијих резултата. Такође су вршене и преваре везане за куповину различитих роба путем On-line куповине, након чега роба није испоручивана. Жртве тих видова преваре били су и наши, али и страни држављани, који су оштећени од стране извршилаца кривичних дела са наше територије. Након сазнања о извршењу те врсте преваре полицијски службеници прикупљају доказе и трагове у виду електронских података о оствареној комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца (Урошевић, et al., 2010:7-9). Након описаног, обављају се провере лог фајлова сервера у потрази за IP адресом, у циљу лоцирања сервиса преко којих су извршиоци кривичног дела слали електронске поруке оштећенима, као и преглед целокупне електронске поште коју је оштећени примио (уз упоређивање података са сервера и рачунара оштећеног), како би се уочили пропусти направљени од стране извршиоца а који могу указати на постојање кривичног дела и места одакле је извршена превара.<sup>8</sup> Након изоловања IP адресе и времена слања електронских порука из лог фајлова, преко ИНТЕРПОЛ-а се, у зависности од државе са чије је територије извршено кривично дело, врше провере у вези корисника коме је она била додељена у тренутку вршења кривичног дела (да се скрати и каже да се врше провере логова на основу прикупљених података са сервера, тј. да се направи нека „компилација“). Те провере се врше према расположивим

<sup>7</sup> Извршиоцима се омогућавало анонимно слање електронских порука, без остављања трага о правој IP (интернет протокол) адреси извршиоца кривичног дела, на тај начин што целокупан интернет саобраћај према одређеним интернет адресама и страницама иде преко сервиса који, потом, као траг оставља своју IP адресу, а адреса правог корисника се налази на серверу тих сервиса.

<sup>8</sup> Нпр. у случају да је извршилац поставио лажни интернет линк неке институције, провером места хостовања правог интернет сајта институције и лажног сајта може се уочити да се ради о превари.

подацима, уз захтеве према државама порекла нежељених или преварних порука, преко неког вида замолнице о предузимању појединих оперативнотактичких радњи. И такви захтеви, у зависности из које државе долазе преварне активности, морају бити тактички промишљени. Наиме, с обзиром на велики број захтева који стижу неким од поменутих држава Западне Африке, услед присутности великог броја извршилаца са тог подручја, из различитих земаља, па наравно и оних најразвијенијих, негде се мора вршити селекција захтева и одредити брзина одговора. У том смислу неопходно је прецизно и концизно формулисати захтеве, уз конкретне и проверено неопходне и изводљиве захтеве за одређеним активностима. Наравно, у сваком тренутку неопходно је водити рачуна о земљи којој се упућује захтев, карактеристикама постојећих претходних контаката и, уколико је могуће, контактирати неког официра за везу из дипломатског представништва те државе. Као што се може видети из досадашњих облика сарадње са државама из тог географског подручја, веома је слаба сарадња полиција у многим сегментима, па и у том. Наравно, на томе треба радити у многим сегментима захтева, али и контаката са свим званичницима тих држава. Неопходно је пребродити многе нелогичности и препреке а при том користити „стару славу“ СФРЈ која је још увек присутна на просторима тих држава. Посебно би требало имати у виду чињеницу да већина држава са територије афричког континента нема полицијске јединице које се баве спречавањем ВТК, а да и уколико их има, оне нису довољно добро опремљене техником, нити имају довољно обучене кадрове.

Коришћење метода социјалног инжењеринга је веома присутно када је извршење наведених кривичних дела у питању. Поред тих начина извршења, у порасту је и број кривичних дела чији је начин извршења познатији као „*card not present*“, у којима се преваре врше без физичког присуства платне картице. Таква кривична дела најчешће се врше преко интернета, а током 2009. године примећен је и пораст оштећених лица са територије Републике Србије (Урошевић, et al., 2010:6).

Преко интернет страница привредна друштва на нашој територији, користећи електронске продавнице, углавном за остваривање правног промета захтевају основне идентификујуће податаке као што су број телефона, име, презиме и адреса лица које ће преузети робу, електронска адреса и слично. Приликом креирања елемената *essentialia negotii* правног посла захтева се и број платне картице (у већини случајева само четири последња или прва броја) и њен безбедносни код (Card Security Code – CSC),<sup>9</sup> као

<sup>9</sup> Card Verification Value (CVV or CV2), Card Verification Value Code (CVVC), Card Verification Code (CVC), Verification Code (V-Code or V Code), или Card Code Verification (CCV). Постоји неколико шифара (кодова) – прва од њих је CVC1 или CVV1, она је унета на магнетну траку картице и користи се за плаћање када је и власник присутан ради упоређивања података из идентификационих докумената. Други код и најчешће цитирани, а који се у 99% користи у описаним преварама је CVV2 или CVC2 (у зависности од типа картице). Често се назива и идентификујућим кодом картице CCID – Credit Card ID, користи се у случајевима плаћања на даљину – обично путем интернета у

и лични подаци власника. Извршиоци кривичних дела углавном наручују тражену скупочену робу (мобилне телефоне, лап топ рачунаре, злато, аудио и видео технику и др.) која је „брзо утопива“ након извршења кривичног дела. Приликом наручивања робе извршиоци утичу на процес обраде података тако што уносе податке о платним картицама у поља за унос података на интернет сајту електронске продавнице, и дају лажне личне податке (име, презиме, адресу) представљајући се као да су они власници платне картице, а за евентуалне договоре око преузимања робе остављају бројеве мобилних телефона намењене само за ту сврху (Урошевић, et al., 2010:6). У току 2008. и 2009. године на територији Републике Србије откривено је више случајева рачунарских превара и злоупотреба платних картица на интернету, у оквиру којих су покушане и извршене злоупотребе података са више стотина платних картица, а прибављена имовинска корист износила је преко пет милиона динара (Урошевић, et al., 2010:6). Оперативним радом дошло се до седам лица која су се бавила тим кривичним делима и против којих су поднете кривичне пријаве Посебном тужилаштву у Београду (Урошевић, 2009:3). Злоупотребљаване су углавном платне картице страних банака издавалаца са територије САД, а за прибављање података коришћене су технике<sup>10</sup> SPAM-а, phishing-а и SQL ињекција<sup>11</sup>.

У наведеним случајевима сарадња је била много коректнија, садржајнија и бржа. Значајно је схватити да је вискоразвијеним државама веома битна сарадња са многим државама у свету, па и са нама, јер много је „јефтине“ да се проблем покуша одбити са своје територије или да се дозволи и „неким тамо у Србији“ да се баве делом проблематике која се ослања на кибер криминал на глобалном нивоу, кроз различите модалитете. Ти облици сарадње укључују: стручну обуку, облике личних контаката од стране за то задужених службених лица тих држава (путем којих на неформалне начине могу да се брзо и ефикасно реше многи проблеми), сарадњу у специфичним областима (нпр. дечије порнографије) и др. У питању нису само државе, већ и велике мултинационалне компаније чији су интереси у таквим случајевима угрожени. На малопређашњим примерима можемо препознати срж ових разлога – постојање „белих“ и „златних“ картица угрожава пословање великих фирми чији је основ егзистенције у функционисању ових безбедносних процедура и заштитних средстава.

случајима "card not present" трансакција. Неке нове картице, тзв. чип картице или Contactless могу имати сопствене електронски самогенеришуће кодове, као нпр. iCVV или динамички CVV.

<sup>10</sup> У једном од наведених случајева „card not present“ превара је дошло и до тзв. „преваре на основу романсе“, када је држављанин БиХ, мушког пола, путем једне од социјалних мрежа, преко интернета контактирао држављанку Републике Србије. Након више месеци дописивања и упознавања замолио је да му да адресу пребивалишта, фиксни телефон и своје податке како би за њега примила робу (компјутерске компоненте), пошто он није у могућности да пошљику прими у својој држави. Роба је била наручена фалсификованом платном картицом аустралијског држављанина. Више у: Урошевић В., Ивановић, З., 2010:91.

<sup>11</sup> RACO Serbia – Пројекат за борбу против економског криминала у Републици Србији: Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе, 2008, стр. 38.



Овде долазимо до најскоријих облика сарадње наше полиције у области ВТК – борбе против дечије порнографије.

Крајем марта 2010. године<sup>12</sup> у Србији је лишено слободе више лица на подручју Кикинде и Београда због растурања дечије порнографије. Припадници Министарства унутрашњих послова – Службе за борбу против организованог криминала, Одељења за борбу против високотехнолошког криминала, Одељења за борбу против високотехнолошког криминала, у заједничкој акцији са Посебним одељењем за високотехнолошки криминал Вишег јавног тужилаштва у Београду, лишили су слободе осумњичено лице из Кикинде због постојања основа сумње да је извршио кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију.<sup>13</sup> У наставку акције сузбијања дечије порнографије на интернету у току дана лишено је слободе и друго лице из Београда, због постојања основа сумње да је извршио кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију.

У склопу међународне полицијске акције у сузбијању дечије порнографије на интернету, СБПОК – Одељење за борбу против високотехнолошког криминала је у сарадњи са Немачком савезном полицијом (БКА), посредством ИНТЕРПОЛ-а, прикупило оперативне податке да већи број лица са територије Србије путем интернета врши дистрибуцију видео материјала порнографске садржине, настале искоришћавањем малолетних лица, особама са територије Немачке.

У наставку акције српска и немачка полиција су прибавиле део доказног материјала који је дистрибуиран путем интернета, као и податке који су послужили за идентификацију и проналажење извршилаца на територији Србије. Након размене и увида у прибављени материјал утврђено је да се ради о видео и другим материјалима у електронском формату који приказују вулгарно сексуално злостављање деце. На основу прикупљених података, у одвојеним акцијама, идентификовани су описани осумњичени. На основу наредби истражног судије извршено је претресање станова осумњичених. На рачунару једног од осумњичених пронађено је чак 262 видео снимка у разним видео форматима (avi, mpeg, wmv). Сви ти снимци садрже искључиво експлицитне сцене најгорег сексуалног злостављања деце. Укупна количина до сада пронађеног педофилског материјала код овог осумњиченог је преко 30 GB. Приликом претреса стана осумњиченог из Београда пронађен је већи број CD-а са видео снимцима у разним

<sup>12</sup> Према подацима НЦБ ИНТЕРПОЛ Београд, у периоду од 21. 9. 2001. до 30. 3. 2010. у погледу дечије порнографије (до 2005. год. то дело није било инкриминисано у КЗ РС, а који је ступио на снагу 2006. год.) поступано је у 93 случаја. У расподели по годинама то изгледа овако: 2001:4; 2002:8; 2003:7; 2004:9; 2005:12; 2006:15; 2007:14; 2008:11; 2009:10; 2010:3.

<sup>13</sup> Званично саопштење МУП-а РС, бр. 190/10 од 24. 3. 2010. године, доступно на [http://www.mup.gov.rs/javascript:popUp\('/cms\\_cir/saopstenja.nsf/saopstenja-MUP.h#25032010','600','400'\)](http://www.mup.gov.rs/javascript:popUp('/cms_cir/saopstenja.nsf/saopstenja-MUP.h#25032010','600','400')) 29. 3. 2010. год.

видео форматима (avi, mpreg, wmv), као и фотографијама, који садрже искључиво сцене директног и вулгарног сексуалног злостављања деце. Укупна количина до сада пронађеног педофилског материјала код овог осумњиченог је преко 5 GB.

Осумњиченима је одређено полицијско задржавање до 48 сати, након чега су, уз кривичну пријаву, предати дежурном истражном судији Вишег суда у Београду. Таква сарадња је у више случајева остварена и са SOCA у Великој Британији, као и са FBI у САД, о чему говоре лишења слободе педофилских група у тим земљама. О наведеним облицима сарадње говоре и званична саопштења МУП-а Републике Србије. Током састанка генерални директор британске Агенције за борбу против тешких облика организованог криминала, Вилијам Хјуз, изразио је задовољство досадашњом сарадњом са МУП-а Републике Србије и нагласио да је SOCA са Службом за борбу против организованог криминала МУП-а Републике Србије спровела низ успешних акција које су резултирале откривањем и хапшењем више организованих криминалних група које су се бавиле илегалном трговином наркотицима, високотехнолошким криминалом, прањем новца и другим тешким облицима криминала.<sup>14</sup> Хјуз је нагласио да је досадашња сарадња имала изузетно позитивне ефекте на плану борбе против организованог криминала, не само у региону, него и у свету. На основу информација које је српска полиција доставила британској и другим светским агенцијама заплена је велика количина дроге широм света.<sup>15</sup>

## Закључак

Битно је нагласити и да се међународна сарадња преко НЦБ ИНТЕР-ПОЛ-а Београд одвија и по питању заштите интелектуалне својине на интернету, кибер тероризма, угрожавања сигурности лица и објеката путем интернета, заштите животне средине везане за илегалну трговину ретким и угроженим животињским врстама, говора мржње на интернету и свих других кривичних дела која се врше путем интернета од стране поједина-

<sup>14</sup> Званично саопштење МУП-а Р Србије, бр. 177/1018. од 29. 3. 2010. доступно на [http://www.mup.gov.rs/javascript:popUp\('/cms\\_cir/saopstenja.nsf/saopstenja-MUP:h#25032010','600','400'\)](http://www.mup.gov.rs/javascript:popUp('/cms_cir/saopstenja.nsf/saopstenja-MUP:h#25032010','600','400')) 29. 3. 2010. год.

<sup>15</sup> Видећемо да то није јединствен случај у свету, као и да су скоро све полиције схватиле да, с обзиром на карактеристике интернета и могућности које пружа извршиоцима кривичних дела, постоји неопходност примена одредаба Конвенције о високотехнолошком криминалу Савета Европе (део о међународној сарадњи, чл. 23-36). Један од интересантних случајева је пољско-швајцарски пример. У јуну 2009. год. на основу сарадње швајцарске и пољске полиције лишено је слободе 31 лице – сви пољски држављани, због поседовања дечије порнографије. До пољских педофила су дошли припадници швајцарске полиције преко једног сајта са којег је те нелегалне садржаје скидало преко 2.000 људи из целог света, међу њима и људи са педесет IP адреса из Пољске. Наравно, овде је дат простор за сарадњу и са другим државама. У акцији је заплена 40 компјутера, 28 хард дискова, преко 1.400 CD и DVD носача. Међу ухапшенима су, као и у случајевима ранијих рација, људи различитих година, професија и социјалног статуса, од незапослених и радника на бензинској пумпи до информатичара и запослених у консталинг фирми. <http://www.blic.rs/Vesti/Svet/97640/Poljska-policija-uhapsila-31-osobu-zbog-decije-pornografije> доступно 29. 3. 2010. год.

ца или криминалних група широм света. Посебно би требало нагласити и чињеницу да се сарадња са другим полицијским службама интензивно одвија и по питању полицијских обука везаних за ВТК, али и размене информација о најсавременијим облицима извршења кривичних дела из области ВТК (фишинг напади, рачунарски вируси, ДДОС напади и слично). Појединачни случајеви су веома често са елементима прекограничног криминала, у којима наши извршиоци врше кривична дела над страним држављанима, па је улога ИНТЕРПОЛ-а кључна за прикупљање оперативних и других података везаних за ефекте извршења на страним територијама. Исто је и у обрнутом смеру.

На основу свега наведеног може се донекле створити слика о улози коју на стратешком, оперативном и тактичком плану рада националне криминалистичке службе има Национални централни биро ИНТЕРПОЛ-а Београд. Превасходно као ефикасан координатор напора домаће криминалистичке полиције, а потом и као поуздан партнер у међународној полицијској сарадњи.

## ***Литература:***

1. Комлен-Николић, Ј. et. al., (2010). *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд.
2. McQuade, S. C., (2009). *III Encyclopedia of cybercrime*, Greenwood Press, 88 Post Road West, Westport.
3. Furnell, S. M., (2001). *Problem of categorising cybercrime and cybercriminals*, 2nd Australian Information Warfare and Security conference.
4. Петровић, С., (2004). *Компјутерски криминал*, Војно-издавачки завод, Београд.
5. *RASO Serbia – Пројекат за борбу против економског криминала у Републици Србији*, (2008). Приручник за истрагу кривичних дела у области високотехнолошког криминала, Савет Европе.
6. Урошевић, В., Уљанов, С., Вуковић, Р., (2010). *Полиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије*, У: Зборник радова Научно-стручног саветовања, Удружење судских вештака за ИТ, стр. 7-9. ЗИТЕХ 10 (електронски извор).
7. Урошевић, В., (2009). „*Нигеријске преваре“ у Србији*, Безбедност, год. 51, бр. 3, стр. 145-157.
8. Урошевић, В., (2009). *Злоупотребе платних картица и рачунарске преваре*, Правни информатор, бр. 9/2010.
9. Урошевић, В., Ивановић, З., (2010). *Улога Интернета у ангажовању посредника за преузимање новца и робе која је противправно прибављена*

- вљена извршењем кривичних дела из области високотехнолошког криминала, Гласник права, часопис Правног факултета Универзитета у Крагујевцу, год. 1, бр. 1/2010, стр. 83-95.
10. Војковић, Г., Штамбук-Суњић, М., (2006). *Конвенција о кибернетичком криминалу и казни закон Републике Хрватске*, Зборник радова Правног факултета у Сплиту, год. 43, бр. 1(81), стр. 123-136.
  11. Newman, G. R., McNally, M. M., *Identity theft literature review*, доступан на интернету дана 12. 1. 2010. год. <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf>

### **Интернет извори:**

12. [http://www.mup.gov.rs/javascript:popUp\('/cms\\_cir/saopstenja.nsf/saopstenja-MUP.h#25032010','600','400'\)](http://www.mup.gov.rs/javascript:popUp('/cms_cir/saopstenja.nsf/saopstenja-MUP.h#25032010','600','400'))
13. <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>
14. <http://www.blic.rs/Vesti/Svet/97640/Poljska-policija-uhapsila-31-osobu-zbog-decije-pornografije>
15. [http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=09&dd=29&nav\\_id=383854&nav\\_category=206](http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=09&dd=29&nav_id=383854&nav_category=206)
16. [http://en.wikipedia.org/wiki/Spam\\_\(electronic\)#Origin\\_of\\_the\\_term](http://en.wikipedia.org/wiki/Spam_(electronic)#Origin_of_the_term)

## **CRUCIAL POINTS IN COOPERATION OF CRIME INVESTIGATING AGENCIES AS SEEN FROM THE ASPECT OF THE NATIONAL CENTRAL BUREAU OF INTERPOL IN BELGRADE**

**Abstract:** *The authors of this article are trying to present the strategic, tactical and operational levels of complex activities of the National Central Biro of Interpol in Belgrade. They attempted to merge participation of many operational lines of work of the NCB Interpol in Belgrade. The greatest attention was given to international police cooperation in cyber crime cases, because of its exceptional importance for EU integration of the Republic of Serbia. This article presents author's choices in relation to importance of the exchange of operational data and the existing social threats of these areas of a crime.*

**Key words:** *INTERPOL, international police cooperation, cybercrime.*