Проф. др *Саша МИЈАЛКОВИЋ*[1]
Криминалистичко-полицијска академија, Београд

UDK – 343.321
Примљено: 24.06.2015.

Trash Intelligence као метод обавештајно-безбедносног рада

Апстракт: *Од степена значаја, квантитета и квалитета неопходних обавештајних сазнања (индиције, подаци, информације, истражни докази), као и од могућности и сложености њиховог стицања, али и од националних правних стандарда у области обавештајног и безбедносног рада, зависи и избор метода за њихово прикупљање. Сматра се да обавештајна сазнања имају већу вредност уколико су прикупљена из више различитих обавештајних извора. Такође, сматра се и да имају већи значај уколико се до њих дошло традиционалним и софистицираним обавештајним методама. Међутим, некада се до значајних обавештајних сазнања може доћи на наизглед једноставан начин који не захтева примену нарочито сложених обавештајних метода, ни посебних знања из области методике обавештајног рада и употребе техничких средстава. Реч је о методу прикупљања обавештајних сазнања анализом садржаја смећа и отпада који остаје за лицима која поседују извесна обавештајна сазнања, односно која су предмет извесне безбедносне обраде – тзв. trash intelligence. Овај метод могу да користе како државне безбедносне агенције, тако и субјекти недржавног сектора безбедности за прикупљање политичких, војних, економских, технолошких, личних и других података.*

Кључне речи: *обавештајни и безбедносни рад, обавештајне и безбедносне службе, шпијунажа, прикупљање обавештајних података анализом садржаја смећа и отпада.*

Увод

Обавештајно (са)знање је знање које је стечено током обавештајног или безбедносног рада, употребом обавештајних и безбедносних метода. Оно, као уосталом и обавештајни и безбедносни

[1] E – mail: Sasa.mijalkovic@kpa.edu.rs

рад, може али и не мора да буде везано за националне или наднационалне обавештајне и/или безбедносне агенције. Напротив, неки видови обавештајног и безбедносног рада све више постају делатност приватних безбедносних агенција и предузетника, али и других субјеката цивилног друштва који у свом раду могу да дођу до обавештајних сазнања.[2]

У односу на значај, квантитет и квалитет, могуће је разликовати више нивоа обавештајног знања, и то: обавештајну индицију, обавештајни податак и обавештајну информацију (Мијалковић, Милошевић, 2013: 115-116; види и: Образовно-истраживачки центар Безбедносно-информативне агенције, 2004). Посебан ниво обавештајног сазнања је доказ у кривичнопроцесном смислу речи, што је обавештајна информација која је задокументована у процесној форми.

Обавештајна индиција (индикатор) је почетно сазнање о предмету интересовања, степен њене тачности и потпуности у тренутку њеног стицања није познат. Прикупљањем, провером и укрштањем више индиција о предмету интересовања добија се податак који је употребљив у даљем оперативном или аналитичком раду.

Обавештајни податак је виши ниво знања који је естрахован из обавештајних индиција, супстрат и сировина из које се производи обавештајна информација . У тренутку стицања, за обавештајни податак се најчешће не зна да ли је тачан и да ли је потпун. Стога је најбоље да се о предмету интересовања стекне већи број података из више различитих извора. Као такви, подаци су извор обавештајних информација.

Обавештајне информације су посебно знање, естраховано из обавештајних података, неопходно за решавање конкретних безбедносних проблема и реализовање конкретних безбедносних циљева. Отуда је јасно да је циљ обавештајне делатности заправо − прикупљање обавештајних података на основу бројних индиција, који ће кроз известан аналитички процес прерасти у сврсисходну обавештајну информацију.

Најзад, обавештајно сазнање може да има значај **доказа** у кривичнопроцесном смислу речи који, уколико се фиксира у

This is the result of the Scientific Research Project entitled *„The Development of Institutional Capacities, Standards and Procedures for Combating Organized Crime and Terrorism in the International Integration Conditions*". The Project is financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia (No 179045), and carried out by the Academy of Criminalistics and Police Studies in Belgrade (2011−2014). The leader of the Project is Associate Professor Saša Mijalković, PhD.

[2] Готово свуда у свету, па и код нас, строго је забрањено недржавним актерима да оснивају обавештајне службе и да примењују оперативне методе и средства која су у искључивој надлежности државних органа (види: члан 1 *Закона о основама уређења служби безбедности Републике Србије*; члан 2 *Закона о приватном обезбеђењу* и члан 2 *Закона о детективској делатности*; види и: Петровић, Синковски, 2012).

кривичнопроцесној форми, очигледно може да послужи као доказ о нечијој кривици или невиности у кривичном поступку за извршено кривично дело.

Обавештајна сазнања се стичу применом обавештајних метода, из извесних обавештајних извора. Начелно, **обавештајна делатност** се реализује: тајним методима (метод тајног уграђивања припадника службе у структуре противника, агентурни метод и метод тајног коришћења техничких средстава), прикривеним методима (метод прикривеног анкетирања, метод прикривеног опсервирања и метод прикривеног научног истраживања) и легалним методима (метод прикупљања података испитивањем лица, метод прикупљања података извиђањем, прикупљање података методом сарадње са субјектима државног и цивилног сектора у земљи и иностранству, прикупљање података из средстава јавног информисања) (Мијалковић, Милошевић, 2011: 150-155).[3]

У најширем смислу, извори обавештајних сазнања су људи (тзв. живи извори) и ствари, које даље могу да се поделе на предмете, техничка средства и документе (Милошевић, 2001: 83-84).

Са аспекта овог рада посебно су интересантни предмети и документа који се могу пронаћи у смећу лица које поседује обавештајна сазнања, а до којих се може доћи применом више наведених метода обавештајне делатности.

Појам Trash Intelligence

Trash Intelligence (TrashInt), односно Garbage Intelligence, је жаргонски назив за активности прикупљања обавештајних сазнања претраживањем, изузимањем и анализирањем садржаја смећа и отпада који за собом остављају (праве или одлажу) лица која су предмет обавештајно-безбедносне обраде, односно корисници или поседоваоци значајних обавештајних сазнања.

У основи примене овог метода су две генералне претпоставке: прва, да одређено лице поседује обавештајно сазнање у форми документа или предмета који ће случајно или намерно, у оригиналној или у деформисаној (исцепаној, поломљеној, наизглед неупотребљивој) форми, случајно или намерно, одложити у смеће; и друга, да ће се поменути извор обавештајних сазнања пронаћи у смећу, да ће моћи да

[3] Међутим, некада се прибегава и примени специфичних (нестандардних) метода прикупљања обавештајних података, као што су тзв. „секс-шпијунажа“, „контејнер шпијунажа“ итд. (Mijalković, 2014).

се узме и анализира или фиксира у прописаној оперативној или кривичнопроцесној процедури.

Наравно, могуће су и извесне варијације ових претпоставки: прва, ствари-изворе обавештајних сазнања у смеће не мора да баци лице које их поседује, већ неко треће лице које са њим има контакт (нпр., хигијеничарка током чишћења канцеларије, члан породице током сређивања куће, дете током играња итд.); друга, ствари-изворе обавештајног сазнања у смећу не мора да пронађе лице које спроводи обавештајно-безбедносну делатност, већ треће лице које ће тај материјал предати служби безбедности (нпр., бескућник који претражује контејнере у потрази за остацима хране); најзад, у смећу не мора да се пронађе ствар-извор обавештајних сазнања који се тражи, већ извор других сазнања која нису предмет актуелне обавештајно-безбедносне обраде, а који ће се предати надлежним службама и јединицама (нпр., истражујући шпијунску делатност, припадници службе безбедности у смећу проналазе документацију која је доказ финансијских малверзација предузећа које је параван за обавештајни пункт, па се такав извор обавештајних сазнања предаје надлежним службама царине, пореских органа, финансијске полиције итд. Тада обрада финансијских малверзација постаје параван за обавештајно-безбедносну обраду шпијунског пункта.).

Посебно је интересантна дилема о легалности примене овог метода у односу на место складиштења смећа.[4] Наиме, уколико је реч о претраживању смећа (корпи и канти за отпатке) у кући лица које поседује изворе обавештајних сазнања, што подразумева и његово двориште и помоћне објекте око куће, у службеној просторији организације у којој је то лице запослено, и у другом објекту за чије је претраживање (претресање и надзор) неопходно одобрење надлежног правосудног органа, онда је такав начин прибављања обавештајних сазнања легалан само уколико постоји одобрење или наредба надлежног правосудног органа. У осталим случајевима овакве обавештајне активности су незаконите.

С друге стране, уколико се претражује смеће које је привремено (канта за смеће, контејнер на улици) или трајно (депонија) смештено на отвореном јавном простору, онда није неопходно одобрење надлежног правосудног органа. У оваквим случајевима Trash Intelligence (тзв. Dump Intelligence – DumpInt) има карактер легалног прикупљања обавештајних података из отворених извора (тзв. legal open source intelligence). Међутим, уколико је реч о депонији приватног комуналног

[4] О неким од ових дилема видети: Kahaner 1997.

предузећа на којој је ограничено или забрањено кретање незапосленим лицама (пословно-приватни посед), онда је за прикупљање обавештајних података неопходна наредба правосудног органа, односно одобрење руководећих органа депоније.

Посебно је интересантно питање прибављања докумената на овај начин у случајевима када су они јасно класификовани као тајни подаци заштићени законом којим се штите тајни подаци (нпр., документ владе који има ознаку „државна тајна“). Уколико је реч о подацима државних органа домаће државе, они се морају предати државном органу којем припадају и не смеју се користити у оперативној обради без посебног одобрења надлежног државног органа у чијој је надлежности заштита тајности података.

На крају елаборирања појма прикупљања обавештајних сазнања претраживањем смећа ваљало би поменути и у које се сврхе прибегава овом методу. Наиме, овај метод је погодан за прикупљање обавештајних сазнања свих врста, до којих се иначе долази и применом свих других обавештајних метода о којима је већ било речи.

Међутим, имајући у виду да државни органи земље која нас обавештајно интересује имају процедуре за поступање са тајним подацима, за њихово складиштење и уништавање, мало је вероватно да се у контејнеру за смеће може пронаћи документ са ознаком државне тајности. Исто је и са безбедносно интересантним лицима која имају виши степен развијености безбедносне културе.

Без обзира на све, Trash Intelligence се до сада показао као погодан за прикупљање података који се могу искористити за:

- **обавештајно-безбедносне операције** откривања, спречавања и сузбијања: обавештајне и субверзивне делатности страних обавештајних служби; угрожавајуће делатности чији су носиоци унутрашњи екстремисти и припадници екстремне политичке емиграције; унутрашњег и међународног тероризма; угрожавања носилаца највиших државних функција, и најтежих облика привредног, финансијског, имовинског и криминалитета против добара и вредности заштићених међународним правом (опширније, у – Мијалковић, Бајагић, 2012: 257-266; 488-515);
- **криминалистичку обраду и кривичну истрагу** наведених облика угрожавања безбедности (проналажење предмета и трагова кривичних дела, реконструкција кривичног дела, вршење увиђаја лица места кривичног дела, идентификовање лица и сл.);
- **безбедносно проверавање лица и проверавање његове искрености у процесу оперативне сарадње** (утврђивање његових контаката са одређеним лицима на бази бележака које

је одбацио у смеће, утврђивање неискрености лица (нпр., лице тврди да га у стану нико није посећивао, а у корпи за смеће су опушци цигарета иако је лице непушач; лице тврди да је било на викенд одмору у конкретном месту, а у корпи за смеће су рачуни плаћених путарина који одговарају предметном датуму, али са саобраћајница које не воде ка месту које је наведено у изјави итд.));

- **социјални инжењеринг, односно профилирање лица** које је безбедносно интересантно (нпр., утврђивање његових склоности, мана, опсесија, предмета интересовања, навика, слабости и свега што може да га компромитује или да укаже на најефикасније методе за његово вербовање ради добијања обавештајних података и информација);
- **субверзивно деловање против лица које је безбедносно интересантно**, када је на бази његовог профила могуће закључити како га је најлакше компромитовати у средини у којој живи, ради и креће се (изношењем неистина на бази извесних истина), како је најлакше извршити његову физичку ликвидацију (на основу утврђивања рутина у његовом кретању и понашању), како га компромитовати код групе чији је члан а која непријатељски делује против земље (фингирањем ситуације из које се може извести закључак да је лице непријатељ групе којој припада), како га медијски „сатанизовати“, како га лажно представити као извршиоца кривичног дела (потплаћивањем проститутке да лажно оптужи лице за силовање, при чему ће крунски доказ бити сперма која је са презервативом узета из канте за смеће лица; убиство које је извршено ножем за отварање писама које је лице случајно испустило у канту за смеће приликом читања поште, а на коме се налазе његови отисци) итд.;
- **крађу и злоупотребу идентитета лица** (види: Harwood, 2008) на основу материјала из смећа у коме су садржани лични подаци лица (име и презиме, име родитеља, матични број грађана, адреса становања, број рачуна у банци, број социјалног осигурања и сл.), а то су пре свега кућни рачуни, документација из банака, рачуни платних картица и сл..

На крају, прикупљање обавештајних сазнања претраживањем смећа треба разликовати од: прикупљања обавештајних сазнања из извора које је лице случајно изгубило или заборавило (на јавном месту, у средствима јавног превоза, у парку, у угоститељском објекту, у хотелу, на свечаностима и сл.), као и од прикупљања обавештајних сазнања крађом докумената (посебно техником џепарења лица), па

њиховим одбацивањем у смеће и фингирањем њиховог случајног одлагања. У оба случаја лице које поседује обавештајна сазнања није одбацило извор у смеће, ни намерно ни случајно.

Најзад, Trash Intelligence треба разликовати и од неовлашћеног упадања у заштићене рачунарске мреже поседоваоца обавештајних сазнања, и претраживања тих мрежа (тзв. хакерисање, хакинг, Hacking), што подразумева и претраживање обрисаних докумената који су у тзв. „канти за смеће“ (Recycle Bin), односно у простору за складиштење обрисаних докумената и и-мејлова (*Trash*).[5] Прибављање обавештајних података хакерисањем је познатије као HackInt (Hackers Intelligence) и представља један од метода злоупотребе савремених информационих технологија у обавештајном раду (тзв. ItInt – Information Technology Intelligence). Иако је реч о електронским материјалима који су обрисани и смештени у „канту за смеће“, овај метод се не може сматрати обликом *Trash Intelligence* јер не подразумева класично претраживање смећа и отпадака поседоваоца обавештајних сазнања. Напротив, реч је о форми тзв. TechInt (Tehnical Intelligence) који подразумева прикупљање обавештајних података коришћењем најмодерније информационе технологије (види: Бајагић, 2010: 135-137).

Иначе, TrashInt је метод који је традиционално веома заступљен али који, због свеукупне технотронизације друштва, постаје све заступљенији и мање актуелан у односу на све развијенији метод Hack-Int.

Феноменологија Trash Intelligence

Према природи података који се прикупљају, Trash Intelligence може да буде део метода који се примењују у оквиру (упореди са: Ђорђевић, 1987: 89-91):

1. **политичке шпијунаже**, када се обавештајни подаци прикупљају за потребе доносилаца политичких одлука и заштите националних интереса сопствене земље (политичке прилике и околности у оквиру конкретне земље; планови и одлуке страних влада; планови и одлуке органа међународних организација; планови реформе државне администрације; одлуке земље у вези са међународним интеграцијама; одлуке о увођењу економских, политичких и других санкција; смернице и ставови у погледу вођења спољне политике; процене о стању унутрашње политичке сцене конкретне

[5] О оваквим врстама злоупотребе опширније у: Петровић (2001); Матић, Миљковић (2013).

државе; лични подаци о политичким, војним и економским лидерима земље и сл.);

2. **економске шпијунаже**, када се обавештајни подаци прикупљају за потребе пројектовања националне економије и реализовања националних интереса сопствене земље (економско стање, економски и буџетски проблеми предметне земље; спољна и унутрашња дуговања земље; задуженост грађана и привреде код домаћих и страних банака; планирано учествовање у међународним економским пројектима; пројектована инфлација, приходи и расходи државе и сл.);
3. **војне шпијунаже**, када се обавештајни подаци прикупљају за потребе пројектовања и планирања система одбране сопствене земље (састав, квалитет, обученост, опремљеност и комуникације војске конкретне државе; тајни програми развоја савременог наоружања и опреме; мобилизацијски планови; планови ангажовања у мултинационалним мировним операцијама и војним блоковима итд.);
4. **индустријске шпијунаже**, када се обавештајни подаци прикупљају за потребе пројектовања планова и реализовања интереса појединих привредних субјеката (патенти, иновације и нова техничка решења; нови технолошки процеси; нови материјали; пројекти нових производа; планови освајања нових тржишта итд.);
5. **приватне истражитељске делатности**, које спроводе приватни истражитељи (детективи) на захтев одређених клијената, по комерцијалном основу („брачне истраге, породичне истраге, парничне истраге, истраге дисциплине на раду и истраге осигурања, ради утврђивања ванбрачних веза, нестанка члана породице, пратње и присмотре деце, утврђивања контакта родитеља и деце када је то судски забрањено, истражне услуге у оквиру парница, прикупљање доказа за потребе одбране оптуженог, истраживање дисциплине на раду, истраживање оправданости захтева за накнаду штете, утврђивање стварног имовинског стања лица итд.“ (Кесић, 2008: 61−63), али и проналажење изгубљених или украдених ствари, безбедносно проверавање лица, расветљавање кривичних дела која се гоне по приватној тужби и службеној дужности) итд.

Следеће важно питање је шта се све може пронаћи у смећу, а да може да буде значајно за безбедносно-обавештајни рад. Пре свега, то могу да буду извори обавештајних сазнања о приватном животу или у вези са службеним ангажманом лица које је предмет обраде или лица са

којим предмет обраде има контакте (упореди са: Wilding, 2006: 88). Наиме, лице које поседује обавештајна сазнања, лице које је са њим у непосредном контакту у његовом дому (члан породице) или канцеларији (колега, радник на одржавању чистоће) могу случајно или намерно да баце у канту за смеће извесне предмете или документе који су извор важних сазнања. Пре свега, реч је о:

- поверљивим документима државних органа на којима предметно лице ради (оригинали/копије; радне/завршне верзије; у штампаном/електронском облику; индига која су коришћена за прављење дупликата докумената, а са којих је могуће прочитати садржај документа итд.);
- службеним документима државних органа, привредних субјеката, научних и сличних институција на којима предметно лице ради, а који не морају да буду поверљиве природе (извештаји, планови, процене, спискови радника и сл.);
- документацији са личним подацима предметног лица (кућни рачуни, фактуре, банковна документација, обавештења члановима клубова, економско-пропагандни материјал који се доставља на кућну адресу, медицинска документација итд.);
- личним предметима лица (фотографија, ручни часовник са посветом, личне забелешке, лични дневник, телефонски именик итд.);
- предметима са којих је могуће изузети ДНК, као што су делови одеће, обуће и хигијенских средстава (веш, чарапе, капа, хигијенски улошци, пелене, чешаљ, четкица за зубе, презервативи, марамице, хигијенски папир, хигијенски штапић и сл.), на којима се налазе телесне течности и други ДНК материјал (зној, пљувачка, крв, сперма, измет, мокраћа, коса, длаке, крвни угрушци, кожне огуљотине, прљавштина из каде итд.). Овај вид Trash Intelligence познатији је као Ordure Intelligence (OrdInt);
- осталим предметима (рачуни из ресторана, хотела, са наплатних рампи, празне лименке и флаше, опушци цигарета, цедуље са забелешкама, игле, шприцеви, кутије лекова и сл.) са којих је могуће изузети отиске прстију лица, анализирати кретање, склоности, навике и пороке појединаца, али и њихове планове.

Најзад, ваља поменути и начине прикупљања обавештајних података методом Trash Intelligence.

Начелно, подаци се прикупљају узимањем из посуде за смеће или са депоније и одношењем на даљу анализу, односно оперативним или истражним (кривичнопроцесним) фиксирањем.

У првом случају, материјал се узима тако што се:

- односи цела посуда за смеће, а уместо ње поставље посуда идентичног изгледа;
- односи садржај посуде за смеће, а уместо њега у посуду убацује други садржај;
- односи садржај посуде за смеће која остаје празна, тако да се стиче утисак да су радници на одржавању хигијене или радници градске чистоће „обавили свој посао“;
- односи само садржај који је носилац извесних обавештајних сазнања, што се ретко примењује (јер лице може да потражи материјал који је бацило у смеће).

У наведеним ситуацијама лице које поседује обавештајна сазнања која је одложило у смеће може да посумња да су она дошла у посед трећих лица. Ипак, у то не може да буде апсолутно сигурно, јер за то не постоје недвосмислени показатељи.

У другом случају материјал се проналази и фиксира у оперативној или у истражној (кривичнопроцесној) форми. У оперативној форми материјал се фиксира: снимањем (фото, видео, копирањем), преписивањем садржаја, узорковањем дела биолошког материјала из посуде за смеће или са депоније ради анализе и вештачења и враћањем фиксираног садржаја на место са кога је узето. Овде је најмања могућност да лице које поседује обавештајна сазнања која је одложило у смеће „провали“ да су она дошла у посед трећих лица, јер ће тај материјал пронаћи у посуди за смеће уколико се присети да га је грешком тамо одложило.

Међутим, уколико се материјал фиксира у процесној (истражној) форми (претресање просторија, увиђај лица места, узорковање материјала приликом увиђаја или претресања просторија и његово слање на вештачење), лицу које је обавештајна сазнања одложило у смеће биће јасно да је предметни материјал у поседу државног органа.

У улози „копача по смећу“ поседоваоца значајних обавештајних сазнања могу да се нађу разна лица. То могу да буду оперативци безбедносно-обавештајних агенција прерушени у раднике градске чистоће или раднике на одржавању хигијене у објектима; заврбовани радници градске чистоће или радници на одржавању хигијене у објектима којима је то задатак; заврбована „трећа лица“ (скитнице, просјаци, вандали итд.).

До неких материјала из посуда за смеће могу да дођу само лица која су запослена у објекту у коме настаје извор обавештајних сазнања и

у коме се он уништава (нпр., само радник (хигијеничар, административац, оперативац, радник службе обезбеђења и сл.) може да дође до отпада који настаје у тзв. „сецкалицама“ – машинама за уништавање (сецкање) документације, односно у тзв. „горионицама“ – уређајима за спаљивање докумената, који посебним методима могу да се реконструишу, односно да се очита садржај текстова са њихових остатака).

Даље, прикупљању обавештајних сазнања претраживањем смећа редовно прибегавају приватни истражитељи и новинари (Wilding, 2006: 87).

Најзад, посебно су значајни припадници организованих криминалних група и терористичких организација које помоћу Trash Intelligence настоје да дођу до података о току и резултатима обавештајно-безбедносних обрада и истрага које спроводе државни органи, о припадницима сектора безбедности и правосуђа који учествују у таквим акцијама итд. (види: Мијалковић, 2010).

Овај метод може да се примени на различитим локацијама. Најпогоднији је за примену у објекту становања, односно запослења лица које поседује обавештајна сазнања. Међутим, ту је и најризичнији у погледу деконспирисања обавештајног рада, с обзиром на то да многе куће, зграде, пословни објекти и владине зграде имају видео надзор и службу физичког обезбеђења.

Такође, овај метод може да се примени и на јавном месту, како на отвореном (улица, трг, парк, шеталиште, излетиште, аутопаркинг, аеродром итд.), тако и у затвореном простору (хотел, резиденција, одмаралиште, одмориште, ВИП салони, галерије, опере, позоришта, музеји, дипломатско-конзуларна представништва, конференцијске сале итд.).

Уместо закључка: осврт на заштиту од Trash Intelligence

Trash Intelligence је метод који користе готово све обавештајне и безбедносне службе, независно од тога да ли су оне државне или приватне. С једне стране, могућност доласка до обавештајних сазнања је велика, а могућности да та сазнања буду значајна су реалне. С друге стране, примена овог метода не носи велику опасност од деконспирисања лица која имају задатак да прикупе обавештајна сазнања, а прикупљање материјала из посуда за смеће и јавних депонија најчешће није незаконито. Стога ће примена овог метода прикупљања обавештајних сазнања вероватно још дуго бити актуелна у обавештајно-безбедносном раду.

Најзначајније место у заштити од Trash Intelligence има безбедносна култура лица која поседују обавештајна сазнања, односно изворе обавештајних сазнања.

Безбедносна култура подразумева усвојена знања, ставове, вештине и искуства у руковању материјалом који је стварни или потенцијални носилац обавештајних сазнања. У том смислу, материјал који је носилац обавештајних сазнања ни у ком случају не би смео да буде доступан трећим лицима, па ни посредством отпада и смећа које настаје приликом израде тог материјала, његовог складиштења, транспорта, коришћења или уништавања. У том смислу, руковаоци изворима значајних обавештајних сазнања морали би да воде рачуна о томе како њима манипулишу, складиште их и чувају, а посебно како их уништавају.

Када је реч о државницима и радницима у државној администрацији, за њих је посебно важно да испуњавају прописане услове безбедносних квалитета (да задовољавају услове „безбедносне провере“), да поштују постојеће безбедносне режиме заштите тајности докумената и да поседују професионалну безбедносну културу.

Следећи је ниво техничке заштићености тајних података, просторија у којима се налазе и лица која њима манипулишу. То подразумева извесне безбедносне режиме израде, приступа, коришћења, умножавања, складиштења и уништавања извора обавештајних сазнања.

У погледу уништавања тајних података, лица која спроводе ове активности морала би да буду лица од интегритета, а безбедносни режими такви да документи буду уништени до нивоа од ког се ни на који начин не могу репродуковати, ни они, нити садржај њихових остатака.

Најзад, садржај отпада и смећа лица која поседују извесна обавештајна сазнања морао би да се посебно уништава, на начин на који није могуће доћи до његовог садржаја.

Литература

1. (2004). *Извори, технике и технологије прикупљања информација за потребе корисника обавештајних података*, Образовно-истраживачки центар Безбедносно-информативне агенције, Београд.
2. Бајагић, М., (2010). *Методика обавештајног рада*, Криминалистичко-полицијска академија, Београд.
3. Ђорђевић, О. Ж., (1987). *Основи државне безбедности − општи део*, ВШУП, Београд.

4. Harwood, M., (2008). *Annapolis Police Teach Residents "Trash Intelligence"*, http://www.securitymanagement.com/news/annapolis-police-teach-residents-trash-intelligence-004630, доступно 22. јуна 2014.
5. Kahaner, L., (1997). *Competitive Intelligence: How To Gather Analyze And Use Information To Move Your Buisiness to the Top*, Touchestone, New York.
6. Кесић, З., (2008). *Место и улога недржавног сектора у контроли криминалитета* (магистарска теза), Криминалистичко-полицијска академија, Београд.
7. Матић, Г., Миљковић, М., (2013). *Прилог дефинисању и класификацији нападаних и обавештајних информација у сајбер простору*, Безбедност, год. 55, бр. 3, стр. 130-147.
8. Мијалковић, С., (2010). *Обавештајне структуре терористичких и криминалних организација*, НБП – Журнал за криминалистику и право, год. 15, бр. 2, стр. 101-114.
9. Мијалковић, С., Милошевић, М., (2011). *Обавјештајно-безбједносна дјелатност и службе,* Висока школа унутрашњих послова, Бања Лука.
10. Мијалковић, С., Бајагић, М., (2012). *Организовани криминал и тероризам*, Едиција Asphaleia, књ. 3, Криминалистичко-полицијска академија, Београд.
11. Мијалковић, С., Милошевић, М., (2013). *Савремене обавјештајне службе: организација и методика обавјештајног, безбједносног и субверзивног дјеловања*, Висока школа унутрашњих послова, Бања Лука.
12. Mijalković, S., (2014). *'Sex-Espionage' as a Method of Intelligence and Security Agencies*, Безбедност, год. 56, бр. 1, стр. 5-22.
13. Мијалковић, С., Бајагић, М., Вучковић, Г., (2014). *Актуелни домети реформе недржавног сектора безбедности Републике Србије*, Супротстављање савременом организованом криминалу и тероризму V, едиција Asphaleia, књ. 7, Криминалистичко-полицијска академија, Београд, стр. 185-201.
14. Милошевић, М., (2001). *Систем државне безбедности*, Полицијска академија, Београд.
15. Павлићевић, П., (2012). *Обавештајне агенције и обавештајна сарадња у концепту контратероризма Европске уније*, НБП – Журнал за криминалистику и право, год. 17, бр. 1, стр. 107-121.
16. Петровић, С., (2001). *Компјутерски криминал*, МУП РС, Београд.

17. Петровић, Л., Синковски, С., (2012). *Корпоративна безбедност – основа заштите бизниса и предузетништва*, Безбедност, год. 54, бр. 3, стр. 86-109.
18. Wilding, E., (2006). *Information Risk and Security: Preventing and Investigating Workplace Computer Crime*, Gower Publishing Ltd, Aldershot.
19. *Закон о основама уређења служби безбедности Републике Србије*, Службени гласник Републике Србије, бр. 116/2007, са каснијим изменама и допунама.
20. *Закон о детективској делатности*, Службени гласник Републике Србије, бр. 104/2013.
21. *Закон о приватном обезбеђењу*, Службени гласник Републике Србије, бр. 104/2013.

Abstract: The choice of methods for gathering the necessary intelligence findings (indications, data, information, investigation evidence) depends on their degree of importance, their quantity and quality, as well as on the opportunities and complexity of their acquisition, but also on the national legal standards in the field of intelligence and security work. It is believed that the intelligence findings have a greater value if they are gathered from multiple intelligence sources. Also, they are considered to have greater significance if they were obtained using traditional and sophisticated intelligence methods. However, sometimes a significant intelligence findings can be obtained in a seemingly easy manner that does not require the use of particularly complex intelligence methods, special knowledge in the field of methodology of intelligence and the use of technical means. It is a method of gathering intelligence findings by analysing the contents of garbage and waste that remains after persons who have certain intelligence information, i.e. who are the subject of certain security processing – the so-called "Trash intelligence". This method can be used by both state security agencies, and non-state actors of the security sector to gather political, military, economic, technological, personal and other data.

Keywords: intelligence and security work, intelligence and security services, espionage, intelligence collection by analysing the contents of garbage and waste.

Prof. Saša Mijalković, PhD
The Academy of Criminalistic and Police Studies, Belgrade

"TRASH INTELLIGENCE" AS A METHOD IN INTELLIGENCE AND SECURITY

ABSTRACT: The choice of methods for gathering the necessary intelligence findings (indications, data, information, investigation evidence) depends on their degree of importance, their quantity and quality, as well as on the opportunities and complexity of their acquisition, but also on the national legal standards in the field of intelligence and security work. It is believed that the intelligence findings have a greater value if they are gathered from multiple intelligence sources. Also, they are considered to have greater significance if they were obtained using traditional and sophisticated intelligence methods. However, sometimes significant intelligence findings can be obtained in a seemingly easy manner that does not require the use of particularly complex intelligence methods, special knowledge in the field of methodology of intelligence and the use of technical means. It is a method of gathering intelligence findings by analysing the contents of garbage and waste that remains after persons who have certain intelligence information, i.e. who are the subject of certain security processing – the so-called "Trash intelligence". This method can be used by both state security agencies, and non-state actors of the security sector to gather political, military, economic, technological, personal and other data.

Keywords: intelligence and security work, intelligence and security services, espionage, intelligence collection by analysing the contents of garbage and waste.

Introduction

Intelligence findings represent knowledge gained during intelligence or security activities, using the intelligence and security methods. It, like the intelligence and security activities, may or may not be related to national or supranational intelligence and/or security agencies. On the contrary, some aspects of intelligence and security activities are increasingly becoming the area of private security agencies and entrepreneurs, but also other members of civil society, who can get intelligence findings in the course of their work[6].

This is the result of the Scientific Research Project entitled *The Development of Institutional Capacities, Standards and Procedures for Combating Organized Crime and Terrorism in the International Integration*

In relation to the importance, quantity and quality, it is possible to distinguish several levels of intelligence knowledge, namely: an intelligence indication, intelligence data and intelligence information (Mijalković, Milošević, 2013: 115−116; see also: Obrazovno-istraživački centar Bezbednosno-informativne agencije, Beograd, 2004). A particular level of intelligence findings is evidence in the criminal procedural sense, which is an intelligence information filed in the process form.

Intelligence indication (indicator) is the initial knowledge about the object of interest, the degree of accuracy and completeness of which are not known at the time of its acquisition. By gathering, verifying and crossrefferencing several indications about the object of interest, the information usable in further operational and analytical work is obtained.

Intelligence is a higher level of knowledge that is extracted from intelligence indications, substrate and material that produces intelligence information. At the time of acquisition, most often it is not known whether the intelligence data is accurate and whether it is complete. Therefore, it is best to acquire more data on the object of interest from multiple sources. As such, the data is a source of intelligence information.

Intelligence information is particular knowledge that is extracted from the intelligence data, necessary to solve specific security problems and for the implementation of specific security goals. Hence it is clear that the purpose of intelligence activities actually is – intelligence gathering on the basis of numerous indications, which will turn into meaningful intelligence information through certain analytical process.

Finally, if collected according to the criminal procedural form, the intelligence findings may have the significance of *evidence* in the criminal procedural sense and apparently can serve as proof of someone's guilt or innocence in criminal proceedings of an offence.

Intelligence findings are obtained using intelligence methods, from certain intelligence sources. Generally, *field of intelligence activity* consists of: secret methods (method of placing members of the secret services in the structure of the opponent, espionage methods and the secret use of technical means), undercover methods (undercover survey, method of covert observation and undercover methods of scientific research) and legal methods

Conditions. The Project is financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia (No 179045), and carried out by the Academy of Criminalistics and Police Studies in Belgrade (2011−2014). The leader of the Project is Associate Professor Saša Mijalković, PhD.

[6] Almost everywhere in the world, and so in our country too, non-state entities are strictly forbidden to establish intelligence services and to implement operational methods and means that are within the exclusive jurisdiction of the state authorities (see Article 1 of the Law on the Basic Provisions on the Security Services of the Republic of Serbia (Zakon o osnovama uređenja službi bezbednosti Republike Srbije); Article 2 of the Law on Private Security (Zakon o privatnom obezbeđenju) and Article 2 of the Law on Detective Work (Zakon o detektivskoj delatnosti). See also: Petrović, Sinkovski, 2012).

(method of gathering data by examining persons, method of gathering data through reconnaissance, method of gathering data through cooperation with entities of the state and civil society in the country and abroad, gathering data from the media) (Mijalković, Milošević, 2011: 150−155)[7].

In the broadest sense, sources of intelligence findings are the people (i.e. *living sources*) and items, that can further be divided into objects, technical means and documents (Milošević, 2001: 83−84).

From the perspective of this paper, what is particularly interesting are objects and documents that can be found in the garbage of the person who has the intelligence, and which can be obtained by using more of the mentioned methods of the intelligence activities field.

1. The notion "*Trash Intelligence*"

"Trash Intelligence" ("TrashInt") i.e. "Garbage Intelligence" is a slang term for the activities of gathering intelligence findings by searching, obtaining, and analysing the contents of garbage and waste left behind (made or disposed of) by persons who are the subject of intelligence and security processing, i.e. users or holders of relevant intelligence findings.

In the basis of the application of this method there are two general assumptions: first, that a certain person possesses intelligence in the form of documents or objects that he/she will dispose of in the trash, accidentally or intentionally, in original form or deformed (torn, broken, seemingly useless). Second assumption is that the said source of intelligence findings will be found in the trash, that it will be possible to take and analyse it or to collect according to the regulated operational or criminal procedural procedure.

Of course, some variations of these assumptions are also possible: first, the items-sources of intelligence do not need to be thrown in the trash by the person who owns them, but a third person who has contact with him (eg., the hygienist while cleaning offices, a family member while tidying up the home, a child while playing, etc.); secondly, the items-sources of intelligence do not need to be found in the trash by a person who conducts intelligence-security activities, but a third party who will deliver this material to security services (eg., a homeless man who searches the containers for discarded food); finally, the item-source of the intelligence findings that is looked for does not need to be found in the trash, but there can be a source of other findings that are not the subject of the current intelligence and security processing, which will be submitted to the relevant departments and units (eg., investigating the espionage activities, members of the security service

[7] However, sometimes one will resort to the use of specific (nonstandard) methods of intelligence data gathering, such as the so-called "Sex-espionage", "container espionage" and so on (Mijalković, 2014).

find in the trash documentation that is the evidence of embezzlement of the company which is the front for intelligence point, so this source of intelligence findings is submitted to the competent departments of customs, tax authorities, financial police, etc. Then the processing of financial malfeasance becomes a cover for intelligence and security processing of the espionage point.).

Particularly interesting is the dilemma about the legality of applying this method in relation to the place of storing the garbage.[8] Namely, in regard to searching garbage (waste baskets and garbage bins) in the house of the person who has the sources of intelligence findings, which also includes his yard and ancillary facilities around the house, the official premises of the organisation in which that person is employed and any other facility for the search (examination and supervision) of which the approval of the competent judicial authorities is required, then this way of obtaining intelligence information is legal only if there is the authorisation or order of the competent judicial authorities. In other cases, this kind of intelligence activities is illegal.

On the other hand, if the trash searched is temporarily (garbage bin, container on the street) or permanently (landfills) located in the open public space, the approval of the competent judicial authorities is not necessary. In such cases, the "Trash Intelligence" (aka. "Dump Intelligence" – "DumpInt") has the character of legal intelligence gathering from open sources (i.e. legal open source intelligence). However, if it is a landfill owned by a private waste disposal company with limited or prohibited approach to unemployed persons (commercial and private property), then in order to gather intelligence, it is necessary to have the order of the judicial authority i.e. the approval of the governing bodies of the landfill.

Especially interesting is the question of obtaining documents in this way in cases when they are clearly classified as secret data, protected by the law regulating classified information (e.g. government document marked "top secret"). When talking about the data of state bodies of the host state, they must be submitted to the state body to which they belong and should not be used in operational processing without specific approval of the competent state body in charge of the protection of classified information.

At the end of elaborating of the notion of intelligence findings by searching the garbage, one should mention the purposes for resorting to this method. Namely, this method is suitable for the collection of intelligence findings of all kinds, which are usually also obtained by applying all other intelligence methods which have already been discussed.

[8] About some of these dilemmas, see: Kahaner (1997).

However, bearing in mind that the state authorities of the country the intelligence of which we are interested in has procedures for dealing with classified information, for their storage and destruction, it is unlikely that a document marked as state secret would be found in a trash container. Same goes for the persons interesting security-wise, who have developed a higher level of security culture.

No matter what, "Trash Intelligence" has so far proved to be suitable for collecting data which can be used for:

− *Intelligence and security operations* for detection, prevention and suppression of: intelligence and subversive activities of foreign intelligence services; threatening activities internal extremists and members of extreme political emigration are responsible for; domestic and international terrorism; endangering highest state officials and the most severe forms of economic, financial, property crime and crime against goods and values protected by international law (for more details, see – Mijalković, Bajagić, 2012: 257–266; 488–515);

− *Criminal processing and criminal investigation* of the said forms of security threats (finding objects and traces of criminal offences, reconstruction of criminal offences, crime scene investigation, identifying persons, and the like);

− *Security checking of persons* and *checking their sincerity in the process of operational cooperation* (determining their contacts with certain persons based on the notes that were thrown in the garbage, determining persons' dishonesty (eg., a person claims that no one has visited him at the apartment, but there are cigarette butts in the garbage bin, although the person is a non-smoker; the person claims to have been on a weekend vacation at a particular place, however, in the garbage bin there are receipts of paid tall fees corresponding to the date in question, but from the roads that do not lead to the place specified in the statement, etc.));

− *Social engineering*, i.e. *profiling a person* who is interesting security-wise (eg., determining his aptitudes, faults, obsessions, interests, habits, weaknesses and anything that can compromise him or point to the most effective methods for his recruitment for the purpose of obtaining intelligence data and information);

− *Subversive action against a person who is interesting security-wise*, when on the basis of his profile, it can be concluded what the easiest way to compromise him is in his living and working environment and areas of movement (by stating untruths on the basis of certain truths), what the easiest way is to execute his physical liquidation (on the basis of establishing routines in his movements and behaviour), how to compromise him in the group whose member he is, and which undertakes hostile acts against the country (arranging a situation from which it may be inferred that the person is

the enemy of the group to which he belongs), how to "demonise" him in media, how to present him falsely as the perpetrator of a criminal offence (paying a prostitute to falsely accuse the person of rape, where the crucial evidence will be the sperm taken with condom out of the person's trash; the murder that was committed with a letter opener the person has accidentally dropped into a garbage bin when reading mail, with his fingerprints all over it) etc.;

− *Theft and abuse of a person's identity* (see: Harwood, 2008), based on materials from the trash that contain his personal data (name, parent's name, personal identification number, address, bank account number, social security number, etc., data primarily found on household bills, documents from banks, credit cards receipts and so on);

In the end, gathering intelligence by searching the garbage should be distinguished from gathering intelligence from sources which the person was accidentally lost or forgotten (in public places, on public transport, in a park, at a restaurant, in a hotel, at a ceremony, and the like) as well as from gathering intelligence by stealing documents (particularly using pick pocketing technique), then throwing them in the trash and arranging that it looks like they were thrown accidentally. In both cases, the person who has the intelligence has not thrown the source in the trash, neither deliberately nor accidentally.

Finally, "Trash Intelligence" should be distinguished from unauthorised accessing protected computer networks of the person who has intelligence, and searching through these networks (i.e. "hacking"), which includes the search of deleted documents that are in the so-called Recycle Bin, i.e. in the storage of deleted documents and e-mails (Trash)[9]. Obtaining intelligence by hacking is also known as "HackInt" (Hackers Intelligence) and is one of the methods of absuse of modern information technology in the field of intelligence (the so-called "ItInt" - Information Technology Intelligence). Although we speak of electronic materials which have been deleted and placed in the "Racycle Bin", this method can not be considered a form of "Trash Intelligence" because it does not imply a classical search of garbage and waste of a person who has intelligence. On the contrary, it is a form of so-called "Techint" (Technical Intelligence) which includes intelligence data gathering by using the latest information technology (see: Bajagić, 2010: 135−137).

In addition, "TrashInt" is a method that is traditionally very present but which, because of the overall technologisation of the society, is becoming more common and less talked about compared to the more developed method of "HackInt".

[9] About these types of abuse in more detail, see: Petrović (2001); Matić, Miljković (2013).

2. Phenomenology of "*Trash Intelligence*"

According to the nature of the data being gathered, "Trash Intelligence" can be a part of the methods applied in the framework of (compare: Đorđević, 1987: 89−91):

− *Political espionage*, when intelligence data is gathered for the purposes of political decision-makers and the protection of national interests of one's own country (political conditions and circumstances within a specific country, plans and decisions of foreign governments; plans and decisions of the bodies of international organisations; plans for reforming administration of the country; decisions of the country in relation to international integration; the decision on introducing economic, political and other sanctions; guidelines and standpoints in terms of conducting foreign policy; assessment of the situation on the political scene of a particular country; personal data of a political, military and economic leaders of the country, etc.);

− *Economic espionage*, when intelligence data is gathered for the purpose of planning national economy and fulfilling national interests of one's own country (economic situation, economic and budgetary problems of the country; external and internal debt of the country; indebtedness of citizens and businesses with domestic and foreign banks; planned participation in the international economic projects; projected inflation, income and expenses of the country, etc.);

− *Military espionage*, when intelligence data is gathered for the purpose of designing and planning the defence system of one's own country (composition, quality, training, equipment, and communications of the military of that country; secret programmes of modern weapons and equipment development; mobilisation plans; plans of engagement in multinational peacekeeping operations and military blocks, etc.).

− *Industrial espionage*, when intelligence data is gathered for the purpose of designing plans and fulfilling the interests of certain business entities (patents, innovations and new technical solutions; new technological processes; new materials; projects for new products; plans for the conquest of new markets, etc.).

− *Private investigation activities*, conducted by private investigators (detectives), at the request of certain clients, on commercial basis ("marital investigation, family investigations, civil law investigations, investigations of work discipline and related to insurance, investigations to determine extramarital relationships, the disappearance of a family member, escort and surveillance of children, establishing contact between parents and children when this is prohibited by the court, investigative services in a court procedure, gathering evidence for the defence of the accused, investigating work discipline, investigating validity of the request for compensation, establishing ac-

tual financial situation of a person etc." (Kesić, 2008: 61–63), but also the retrieval of lost or stolen items, security checks of persons, resolving criminal cases that are processed by private and public prosecution), etc.

The next important question is what can be found in the trash, and that may be significant for the security-intelligence activities. First of all, that can be sources of intelligence findings about the private life or related to the official involvement of the person subject to processing or persons with which threat person has contacts (compare: Wilding, 2006: 88). The person who possesses the intelligence, the person who is in direct contact with him/her at home (family member) or at the office (fellow worker to hygienist) can accidentally or deliberately throw in the trash certain items or documents that are the source important findings. First of all, these are:

− *Confidential documents of government authority* on which the person in question works (originals/copies; working/final versions; printed/electronic form; carbon papers used to create duplicates of documents, from which it is possible to read the contents of the document, etc.).

− *Official documents* of state bodies, business entities, scientific and similar institutions on which the person in question works, which do not have to be of a confidential nature (reports, plans, estimates, lists of employees, etc.);

− *Documents with personal data* of the person in question (household bills, invoices, bank documents, information to members of clubs, advertisement materials delivered to home address, medical records, etc.).

− *Personal belongings of the person* (photos, a wristwatch with a dedication, personal notes, a diary, telephone directory, etc.).

− *Objects from which it is possible to extract DNA*, such as items of clothing, footwear and personal hygiene items (underwear, socks, hat, sanitary napkins, diapers, comb, toothbrush, condoms, tissues, toilet paper, cotton swabs, etc.) that contain bodily fluids and other DNA material (sweat, saliva, blood, semen, faeces, urine, hair, other bodily hairs, blood clots, skin abrasions, dirt from the bathtub and so on). This form of "Trash Intelligence" is better known as "ordure Intelligence" ("OrdInt");

− *Other items* (receipts from restaurants, hotels, from pay toll booths, empty cans and bottles, cigarette butts, papers with notes, needles, syringes, boxes of medicines, etc.) from which it is possible to lift fingerprints, analyse movements, preferences, habits and vices of an individual, but also their plans.

Finally, we should mention the ways of intelligence data gathering by using "Trash Intelligence" method.

In general, data is gathered by taking the garbage from waste disposal containers or landfill sites and sending it for further analysis, i.e. by operational or investigative (criminal procedure) collecting.

In the first case, the material is taken in the following way:

- the whole trash container is taken away, and instead of it, the container that looks identical is put;
- the content of the garbage container is taken, and instead of it, some other content is put;
- the content of the garbage container is taken, and it remains empty, so that one gets the impression that the cleaning lady or city sanitation workers "did their job";
- only the content that has certain intelligence information is taken, which is rarely used (because a person can look for the things thrown in the trash).

In these situations, the person who has the intelligence that has been thrown in the trash, can suspect that it came into the possession of third parties. Yet, one cannot be absolutely sure of that, because there are no straightforward indicators.

In the second case, the material is found and collected according to operational or investigative (criminal procedure) form. In the operational form, the material is collected by: recording (photo, video, copying), rewriting the content, sampling a part of the biological material from garbage bins or landfills for analysis and getting an expert opinion, and restoring the collected contents to the place from which it was taken. Here the chance is lowest that the person who has the intelligence and has thrown it in the trash will "figure out" that it came into the possession of third parties, because he/she can find that same material in the trash container if he/she remembers that he/she has thrown it out there by mistake.

However, if the material is collected in the process (investigation) form (search of premises, crime scene investigation, sampling materials during the investigation or the search of premises and sending it for the expert analysis), the person who has thrown the intelligence in the trash will be clear that the material in question has come in possession of the state authority.

In the role of "the garbage diggers" of the one who has important intelligence information, various persons can be found. They may be the operatives of security-intelligence agencies disguised as sanitation workers or cleaning ladies at firms; recruited workers of municipal sanitation service or cleaning ladies at firms where the task is; recruited "third parties" (vagrants, beggars, vandals etc.).

Some materials from the trash container can be accessed only by persons who are employed in the facility in which the source of intelligence findings is created and in which it is destroyed (eg., only the employee (hygienist, administrative service employee, operative, security service employee, etc.) can get to the waste generated in the so-called "shredders" – machines for destroying (shredding) documentation, or the so-called "burners" -

devices for burning documents, which can be reconstructed using special methods, that is, the content can be read from their residues).

Further on, gathering intelligence findings by searching the garbage is regularly used by private investigators and journalists (Wilding, 2006: 87).

Finally, what is especially important is that the members of organised criminal groups and terrorist organisations use "Trash Intelligence" trying to obtain information about the progress and results of intelligence-security processing and investigations carried out by state authorities, of members of the security and justice sector who participate in such actions, etc. (see: Mijalković, 2010).

This method can be applied in different locations. It is most suitable for residential or employment facilities of the person who has intelligence. However, it is there that the risk is also the highest, in terms of exposing intelligence work, given that many houses, buildings, office buildings, government buildings have video surveillance and physical security service.

Also, this method can be used in a public place, both outdoors (street, square, park, walkway, picnic area, auto parking, airport, etc.) and indoors (hotel, residence, resort, resting area, VIP lounges, galleries, opera houses, theatres, museums, diplomatic and consular offices, conference rooms, etc.).

Instead of conclusion: a look into the protection from "Trash Intelligence"

"Trash Intelligence" is a method used by almost all intelligence and security services, regardless of whether they are public or private. On the one hand, the possibility of getting to intelligence findings is great, and the possibility that these findings are important is real. On the other hand, using this method does not carry a great risk of exposing persons who have the task to gather intelligence findings and gathering materials from garbage containers and public landfills is usually not illegal. Therefore, applying this method of gathering intelligence findings is likely to be present for a long time in the course of the intelligence and security activities.

What is most important about the protection from "Trash Intelligence" is the security culture of persons who possess the intelligence or sources of intelligence findings.

Security culture includes adoption of knowledge, attitudes, skills and experience in handling materials, which are actual or potential holders of intelligence findings. In this sense, the material holding intelligence findings should not, in any case, be accessible to third parties, not even through the trash and waste that is produced when creating this material, storing it, transporting, using or destroying it. In this regard, persons handling significant sources of intelligence findings would have to take care about how they ma-

nipulate them, store and preserve them, and especially how they destroy them.

When it comes to state officials and state administration employees, for them it is especially important to meet the prescribed requirements regarding security qualities (that they meet the requirements of "vetting"), that they adhere to the existing security regulations to protect the confidentiality of documents and that they have professional safety culture.

Next is the level of technical protection of classified information, of premises in which they are kept, and of people who handle them. This implies certain security regimes of creating, accessing, use, multiplication, storing and destroying the sources of intelligence findings.

With regard to destroying classified information, persons conducting these activities would have to be persons of integrity, and security regimes such that the documents are destroyed to that extent that they can not in any way be reproduced, neither the documents, nor the content of their remains.

Finally, the content of waste and garbage of persons who have certain intelligence findings would have to be specifically destroyed, in the way in which it is not possible to get to its contents.

REFERENCES

1. (2004). *Izvori, tehnike i tehnologije prikupljanja informacija za potrebe korisnika obaveštajnih podataka*, Obrazovno-istraživački centar Bezbednosno-informativne agencije, Beograd.
2. Harwood, M. (2008). *Annapolis Police Teach Residents "Trash Intelligence"*, http://www.securitymanagement.com/news/annapolis-police-teach-residents-trash-intelligence-004630, accessed on June 22 2014.
3. Kahaner, L. (1997). *Competitive Intelligence: How To Gather Analyze And Use Information To Move Your Buisiness to the Top*, Touchestone, New York.
4. Mijalković, S. (2014). *'Sex-Espionage' as a Method of Intelligence and Security Agencies,* Bezbednost, broj 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2014, pp. 5−22.
5. Wilding, E. (2006). *Information Risk and Security: Preventing and Investigating Workplace Computer Crime*, Gower Publishing Ltd, Aldershot.
6. Bajagić, M. (2010). *Metodika obaveštajnog rada*, Kriminalističko-policijska akademija, Beograd.
7. Đorđević, O. Ž. (1987). *Osnovi državne bezbednosti − opšti deo*, VŠUP, Beograd.
8. Zakon o detektivskoj delatnosti, Službeni glasnik RS, broj 104/2013.
9. Zakon o osnovama uređenja službi bezbednosti Republike Srbije, Službeni glasnik RS, broj 116/2007, sa kasnijim izmenama i dopunama.
10. Zakon o privatnom obezbeđenju, Službeni glasnik RS broj 104/2013.
11. Kesić, Z. (2008). *Mesto i uloga nedržavnog sektora u kontroli kriminaliteta* (magistarska teza), Kriminalističko-policijska akademija, Beograd.
12. Matić, G.; Miljković, M. (2013). *Prilog definisanju i klasifikaciji napadanih i obaveštajnih informacija u sajber prostoru*, Bezbednost, broj 3, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, str. 130−147.
13. Mijalković, S. (2010). *Obaveštajne strukture terorističkih i kriminalnih organizacija*, Nauka – bezbednost – policija, broj 2, Kriminalističko–policijska akademija, Beograd, str. 101–114.
14. Mijalković, S., Milošević, M. (2013). *Savremene obavještajne službe: organizacija i metodika obavještajnog, bezbjednosnog i subverzivnog djelovanja*, Visoka škola unutrašnjih poslova, Banja Luka.

15. Mijalković, S.; Bajagić, M. (2012). *Organizovani kriminal i terorizam*, Kriminalističko-policijska akademija, Edicija Asphaleia, knj. 3, Beograd.
16. Mijalković, S.; Bajagić, M.; Vučković, G. (2014). *Aktuelni dometi reforme nedržavnog sektora bezbednosti Republike Srbije, Suprotstavljanje savremenom organizovanom kriminalu i terorizmu V* (edicija Asphaleia – knjiga 7), Kriminalističko-policijska akademija, Beograd, str. 185–201.
17. Mijalković, S.; Milošević, M. (2011). *Obavještajno-bezbjednosna djelatnost i službe*, Visoka škola unutrašnjih poslova, Banja Luka.
18. Milošević, M. (2001). *Sistem državne bezbednosti*, Policijska akademija, Beograd.
19. Pavlićević, P. (2012). *Obaveštajne agencije i obaveštajna saradnja u konceptu kontraterorizma Evropske unije*, Nauka – Bezbednost – Policija, broj 1, Kriminalističko-policijska akademija, Beograd, str. 107−121.
20. Petrović, L.; Sinkovski, S. (2012). *Korporativna bezbednost – osnova zaštite biznisa i preduzetništva*, Bezbednost, broj 3, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, str. 86−109.
21. Petrović, S. (2001). *Kompjuterski kriminal*, MUP RS, Beograd.