УДК: 004.738.5+343.9
Примљено: 3. марта 2010.
Прихваћено: 25. маја 2010.
Оригинални научни рад

Српска политичка мисао
број 2/2010.
год. 17. vol. 28.
стр. 233-250.

Душан Васић
Универзитет АЛФА, Београд

НЕКА ОТВОРЕНА ПИТАЊА ПРИМЕНЕ КОНВЕНЦИЈЕ САВЕТА ЕВРОПЕ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Сажетак

Приближавање Србије Европској унији претпоставља и њено интегрисање у јединствени концепт борбе против високо-технолошког криминала. Платформа за заједничко деловање на овом плану формулисала је Конвенција Савета Европе о сајбер криминалу. Ову Конвенцију досад је потписала 41 чланица Савета Европе и 5 држава изван Европе. Међутим, тек нешто више од половине потписница спровело је поступак ратификације. Показало се да су нека питања и даље остала спорна да би једноставно могла бити преточена у националне законе највећег броја држава. Тим питањима и разлозима застоја у процесу ратификације Конвенције посвећен је овај рад, уз закључак да је, упркос одређених резерви, неопходно да се на глобалном плану обликује платформа за заједнички рад на превенцији, сузбијању и кажњавању сајбер криминала.

Кључне речи: Конвенција о сајбер криминалу; високо-технолошки криминал; заштита података о личности, Мрежа 24/7; Национални центар за рачунарску безбедност (НЦРБ);

ЗАБРИЊАВАЈУЋИ ПОРАСТ ВИРТУЕЛНИХ ФОРМИ КРИМИНАЛА

Злоупотреба рачунара постала је једна од масовних нус-појава савремене цивилизације. Парадокс је театралан. Што је свет ин-

тегрисанији, то су ризици од високо-технолошког криминала распрострањенији. Човечанство је закорачило у виртуелни простор електронских пулсација, у коме се обликују дигитални производи нематеријалне природе, комуницира планетарно, послује глобално и информише тренутно, мимо свих граница, временског или просторног и језичког, па и других ограничења. То је на једној страни подстакло најсмелија научна маштања а на другој пробудило многе негативне пориве и ниске страсти.

Уз то, период удвостручавања светске компјутерске мреже са првобитних 20 година (за период 1970 до 1990) , смањио се на 10 (период 1990-2000. године), а потом на само 5,2 године (период 2000-2006). Темпо криминализације *кибер простора*[1)] је много бржи, због чега се број криминалних дела увећава геометријском прогресијом.

Рачунар, тај синоним технолошког прогреса, постепено се претвара у средство повећане рањивости модерних друштава. Дигиталним путем лако се може угрозити добробит сваке државе, без обзира на величину, војну моћ, политички утицај и економску снагу. У мери у којој се брзина електронске комуникације, просторна удаљеност између субјеката општења и обухватност Интернет мреже увећавају, у тој мери расту и ризици од виртуелних форми криминала, чије материјалне последице у појединим државама већ надмашују остале врсте криминала.

Још 2004. години власти САД су упозориле да је „приход“ од *сајбер* криминала у тој земљи први пут премашио годишњи приход од продаје дроге, који се процењује на око 300 милијарди долара[2)]. Због тога су САД заоштриле казнену политику у овој области. У току фискалне 2007. године (март 2007- март 2008) у САД је поднето 2.470 кривичних пријава против *сајбер* криминалаца. Чак 95,39 одсто оптужених је осуђено на различите казне. Највећа казна изречена је за *on-line* превару једне финансијске институције и износила је 9 година затвора[3)]. За крађу идентитета преко интерне-

1) Израз *кибер*, на енглеском *сајбер* (*cyber)*, води порекло од грчке речи Κυβερνήτης (латиничним писмом: kybernētēs), а означава особу која управља, кормилари или предводи. Од те речи, писац научно-фантастичних романа *William Gibsont* је 1982. године сачинио кованицу *киберпростор* (cyberspace) да би описао итерактивни глобални домен у коме се одвија дејства посебних уређаја који преносе елекормагнетну енергију у сврху одвијања комуникација и у сврху контроле. Савремени смисао овом појму дао је пионир кибернетике, стручњак за област електронике N*orbert Wiener*, који је оформио посебну научну дисциплин-кибернетику.

2) Valerie McNiven, U.S. Department of the Treasury (Riad, 28. Nov 2005)

3) *US v. Simbaqueba,* Southern District of Florida, Department of Justice Release, avgust 5, 2008, доступно на сајту www.usdoj.gov

та највећа изречена казна је 66 месеци затвора[4], док је по основу загушивања *spam* порукама највећа затворска казна износила 47 месеци[5] итд.

На *Првој светској конференцији о сајбер-криминалу*, која је у јануару 2009. године одржана у Њујорку, уз присуство преко 400 учесника из 37 земаља, упозорено је да су не само софистицираност већ и „пословичност" *сајбер* криминалаца у порасту. „Предузетничка слобода" криминалаца иде чак дотле да користе *on-line* форуме за оглашавање нелегалних производа, куповину и продају компјутерских вируса, трговину украденим идентитетом и друге забрањене радње, све у циљу стицања профита.[6]

Услед раста конкуренције у прљавим пословима, знатно су појефтиниле „услуге" преварног карактера. За око 30 долара било где у свету може се купити бланко кредитна картица, заједно са холограмским заштитним ознакама, које иначе користе овлашћене компаније за издавање кредитних картица. Вешти криминалци на исти начин могу прибавити опрему за кодирање, којом на бланко картицу могу унети компјутерски украдени идентитет неке особе. Поврх тога, они могу купити софтвер, који ће на пристигли упит са места чекирања картице одговорити да је тако „клонирани" купац кредитно способан.[7]

РЕГУЛАТИВА У СРБИЈИ

Процењује се да Србија око осетно заостаје у развоју информатичког друштва у односу на Европу.[8] То има своју добре страну, јер су хакери дуго заобилазили Србију. Међутим, три околности домаћи информатички простор сада чине посебно рањивим: (1) уведен је брзи приступ Интернету, (2) већином се користе рачунари ниског нивоа заштите а (3) степен знања у овој области је раван масовној неписмености.

4) *US v. Brown,* Disrict of Arizona, Department of Justice Release, Avgust 5, 2008, (www.usdoj.gov)

5) *US v. Soloway,* Western District of Washington, Department of Justice Release, Avgust 5, 2008, (www.usdoj.gov)

6) *Shawn Henry*, Head of FBI Cyber Division, address to the Conference at Fordham University in New York City, January 14, 2009.

7) Ибид.

8) Митровић, Ђорђе: „Могућности и проблеми будућег развоја информатичког друштва у Србији у процесу придруживања ЕУ", *Економске теме,* Ниш**,** 2007, вол. 45, бр. 3, стр. 164-165.

Србија је посебно атрактивна за компјутерску пиратерију свих врста. Почев од тога да се на улици и даље за свега сто динара могу купити најновији филм или видео-игре чија је израда коштала пар милиона долара, до тога да се злоупотребом банкарских картица и рачуна може електронским путем доћи до замашних новчаних сума или вредних материјалних добара, нарочито ако се те картице користе у другим земљама. Са ширењем интернета и повећањем броја рачунара Србија ће све више постајати и мета *сајбер* деликвената, најразличитијих амбиција и намера.

Институције система у Србији су на самом почетку процеса оспособљавања за супротстављање различитим видовима *сајбер* криминала и за откривање појединаца или група који су њихових главни носиоци. У пролеће 2007. године при *Окружном јавном тужилаштву* у Београду је основано посебно *Одељење за борбу против високотехнолошког криминала* (у закону означено још и као Посебно тужилаштво). Истовремено, именован је први специјални тужилац за ову област, у рангу заменика јавног тужиоца. Паралелно са тим, у Окружном суду формирано је и посебно судско веће, *Веће за поступање у кривичним делима високо-технолошког криминала.*. После реконструкције правосудне мреже у Србији, од првог јануара 2010. године, Више тужилаштво је постало онај орган који је надлежан за покретање истраге против сајбер криминалаца, а Виши суд је постао она судска инстанца, чије Одељење (а не више Веће) пресуђује починиоцима кривичних дела из области високотехнолошког криминала.[9] Међутим, број тужилаца специјализованих за борбу против високотехнолошког криминала је преполовљен – са четири на два. Овај податак убрзо је пао у очи стручној јавности која је на то критички реаговала.

Министарство унутрашњих послова је у оквиру Службе за борбу против организованог криминала формирала *Одсек за сузбијање компјутерског криминала*. Међутим, према слову закона, у ту сврху требало је формирати посебну службу, а не само одсек. Ово одељење засад једино постоји у Београду, а у другим градовима на полицијским пословима у вези сајбер криминала најчешће ради само по једна особа. Наше је мишљење да ће у будућности бити потребно да се у МУП-у Србије чак формира посебна управа за сузбијање високо-технолошког криминала, једнако као што је пораст других природних и друштвених ризика наметнуо потребу формирања посебне Управе за ванредне ситуације.

9) "Закон о измени и допуни закона о организованости државних органа за борбу против високотехнолошког криминала", *Службени гласник Републике Србије*, бр. 104/2009, чланови 3-9.

Што се тиче оспособљености за вештачење информационих спорова, досад су тек три особе добила лиценцу сталног судског вештака за ову врсту спорова. Истина, постоји на десетине експерта за ову област, али недостаје им лиценца Министарства. Коначно, Влада Србије је пре три године усвојила *Стратегију развоја информационог друштва* и потписала *Агенду за развој информационог друштва у Југоисточној Европи* за период од 2007. до 2012. године али се у њиховој имплементацији није далеко одмакло.

Не изненађује отуд што је у Србији 2007. године због високотехнолошког криминала процесуирано тек 103 лица, а подигнуто је 11 оптужница (извештаји за 2008. и 2009. још нису објављени, напомена Д.В.). Од укупног броја предмет, а 85 се односило на дела против интелектуалне својине, седам против безбедности рачунарских података и 10 против имовине[10]. Од почетка 2008. године до почетка 2010. године за кривична дела против рачунара или њиховим коришћењем у Србији је правоснажно осуђено 129 лица, којима је одузета противзаконито стечена корист од 1.100 000 динара и 80 рачунара[11].

Високотехнолошки криминал у Србији засад се најчешће манифестује у форми пиратерије. Иза њега стоје организоване, или полуорганизоване групе, које путем Интернета, коришћењем сателитских, кабловских, или бежичних брзих веза долазе у посед филмова, музике и програма. Уз помоћ моћних и брзих рачунара *сајбер* криминалци ове електронске производе копирају а затим преко уличне мреже препродаваца дистрибуирају широм Србију.

У оквиру процеса приближавања Европској унији, Народна Скупштина Републике Србије је већ усвојила низ значајних закона. Међу првима су донети су *Закон о електронском потпису*[12], нови *Кривични законик Србије*[13], *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*[14] и *Закон о путним исправама*[15] са биометријским подацима, као и читав сет закона из области правосуђа (укупно седам)[16]. Крајем 2008. и почетком 2009. године донети су *Закон о заштити*

10) *Годишњи извештај Окружног суда у Београду за 2007 годину*, *www.okruznisudbg.org.yu*

11) http://www.beograd.vtk.jt.rs/index.php?option=com_content&view=article&catid=34:naslovna&id=53:tuzilastvo-za-borbu-protiv-visokotehnoloskog-kriminala&Itemid=53&lang=yu

12) *Службени гласник Републике Србије,* бр. 135/2004.

13) *Службени гласник Републике Србије*, бр. 85/2005.

14) *Службени гласник Републике Србије*, бр. 61/2005.

15) *Службени гласник Републике Србије*, бр. 90/2007.

16) *Службени гласник Републике Србије*, бр. 116/2008.

података о личности[17], *Закон о одузимању имовине проистекле из кривичних дела,*[18] *Закон о међународној правној помоћи у кривичним стварима,*[19]. *Закон о електронској трговини*[20] *и Закон о ауторским и сродним правима*[21].

Највише недоумица било је око Закона о заштити података о личности. Упркос озбиљних замерки, Закон је усвојен крајем 2008. године, а ступио је на снагу 1. јануара 2009. године. Нека од усвојених решења и данас су предмет расправе и критике, тим пре што још нису донета сва подзаконска акта за његово спровођење. Највећи проблем је то што још није успостављен објективан и поуздан механизам за надзор над применом стандарда који су прописани законом.

У већини бивших југословенских република у просеку око двадесетак људи се професионално бави надзором у овој области, независно да ли у оквиру агенција или посебних управних служби. У Србији је та обавеза пребачена на институцију Повереника за информације. Практично, иста служба која треба да надзире и обезбеђује слободан приступа грађана информацијама од јавног значаја, сада је задужена да спроводи надзор над спровођењем норми из Закона о заштити података о личности. То се на неки начин чини немогућом мисијом, па не изненађује што досад ни једна особа званично није задужена за послове надзора. По свему судећи, надзор ће се свести на импровизацију, а о развоју свести, културе и едуковању кадрова за послове надзора очигледно још се не размишља[22]

Више је примера који показују да се личним подацима грађана у Србији данас понегде произвољно барата, независно од доношења Закона. Један дневни лист је у више наврата објављивао спискове грађана са њиховим матичним бројем. Неким медијима су достављени матични бројеви судија појединих судова. Где год да грађанин крене сви управни органи увек изнова траже копију личних докумената, од личне карте, пасоша, возачке дозволе и слично, независно од тога што је тражење ових података законом ограничено.

17) *Службени гласник Републике Србије*, бр. 97/2008.

18) *Службени гласник Републике Србије*, бр. 97/2008.

19) *Службени гласник Републике Србије*, бр. 20/2009.

20) *Службени гласник Републике Србије*, бр. 41/2009.

21) *Службени гласник Републике Србије*, бр. 104/2009.

22) Родољуб Шабић: «Крадљивци личних података», *Данас, дневни лист*, Београд, 21.06.2009.

Да би стала на пут томе, Словенија је средином 2008. године забранила да се од грађана тражи да достављају копије личних докумената, осим ако се они изричито с тим сложе. Уједно, забранила је скенирање и чување личних докумената грађана. Хрватска је од јануара 2009. године увела нови идентификациони број грађана који не садржи личне податке укључене у општепознати ЈМБГ (јединствени матични број грађана).

Србија ни једно од ових решења које треба да предупреди ризик од злоупотребе личних података није нормирала. Могућности за крађу електронски забележеног идентитета грађана у основи нису запречене, јер су ти подаци стационирани на разним местима, у различитим установама и на бројним знаним и незнаним фајловима. Злоупотребе личног идентитета у финансијске сврхе могу имати тешке материјалне последице, али и други облици штета нису за потцењивање, као на пример повреда угледа, повређивање емоција, нарушавање породичног живота, угрожавање интиме, изазивање јавног одијума против неких особа и слично. Без успостављања независних државних органа или агенције која ће се професионално и аутономно бавити овим осетљивим питањима надзора и контроле, без допуне правила о јасном поступању са личним подацима грађана, без прецизнијег ограничавања права појединаца и служби да приступају туђим подацима излазак на пут европских стандарда у информационој сфери неће бити тако брз.

Најзначајнији процедурални помак на мапи пута ка белој шенгенској листи представљало је ратификовање три конвенције Савета Европе -*Конвенције сузбијању високотехнолошког криминала*, као и протокола уз ову конвенцију, *Конвенције о спречавању тероризма* и *Конвенције о борби против трговине људима*[23].

Усвајањем горе наведених закона Србија се прикључила кругу држава које ефективно располажу основним правним инструментима, законском регулативном, државним институцијама и стручним тимовима за супротстављање високо технолошком криминалу. Њени капацитети за борбу против рачунарског криминала сада могу стављени у функцију заједничког ангажовања држава потписница Конвенције, које чине трећину чланица УН.

Сматрамо ипак да ће време показати неопходност доношења посебног закона о сузбијању високо-технолошког криминала. С обзиром на размере пораста ове врсте криминала свету и перспективу укључивања Србије у различите форме регионалних интеграција, реално је закључити да ће се одредбе Главе XXVII

23) *Службени гласник Републике Србије*, бр. 19/2009.

Кривичног законика Србије ускоро показати недовољним да захвате сва питања, проблеме, друштвене активности, државну политику и институционално деловање против високо-технолошког криминала. Координација деловања свих институција система као и координација међународне сарадње са суседним држава и њено проширивање према свим државама Југоисточне Европе и онима које следе дух европског заједништва зацртан у пројектима Савета Европе тим више ће захтевати далеко већи степен институционалне и нормативне оспособљености Србије за заједничко деловање и на плану сузбијања сајбер криминала.

НЕДОУМИЦЕ КОЈЕ ПРАТЕ КОНВЕНЦИЈУ О САЈБЕР КРИМИНАЛУ

Пре него што је ратификована, већ поменута *Конвенције Савета Европе о борби против компјутерског криминала*[24] из 2001. године (ступила на снагу 2004. године) пуне три године је у Србији имала статус закона у припреми. Она је брзо уведена у скупштинску процедуру, али се ту предуго задржала. Велики део стручне јавности сматра да *Конвенција* представља врхунац досадашњих међународних напора да се заједничким снагама стане на пут сајбер-криминалу. Она је дефинисала седам нових кривичних дела и значајно допринела успостављању заједничке казнене политике, као и усвајању низа националних прописа (материјалног и процедуралног карактера) и подстицању међународне сарадње у овој области.

Међутим, упркос великим почетним надама, ентузијазам за њеним спровођењем је донекле опао. Неке одредбе *Конвенције* учиниле су се упитним и оним државама које су је међу првима потписале, али је још нису ратификовале. Према званичним подацима, од укупно 46 држава чланица *Савета Европе*, *Конвенцију* је до сада потписала 41 држава, и још пет држава изван Европе (Канада, Јапан, Јужна Африка и САД). Међутим, поступак ратификације досад је довршило само 28 чланица *Савета Европе*. Из било ког угла гледано, са становишта територије, са становишта броја држава и према обиму светске популације, ово је неочекивано мали број[25].

24) *Конвенција о сајбер криминалу*, Будимпешта, 23. новембар 2001.

25) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG (16.05.2010)

Међу 13 држава које су потписале *Конвенцију* али се нису одлучиле да је ратификују су и такве значајне државе као што су Велика Британија, Шведска, Швајцарска, Аустрија, Белгија, Грчка, Шпанија, Пољска итд. Поред тога, још пет држава чланица Савета Европе, до средине марта 2010. године, уопште није потписало Конвенцију, нити има намеру да то учини у догледној будућности. Међу њима су и тако утицајне и велике државе као што су Русија и Турска, али и три микро државе: Сан Марино, Монако и Андора. Србија је конвенцију потписала 7. априла 2005. године, али је требало да прође готово четири пуне године до њене ратификације (18. март 2009.). Од држава које нису чланице Савета Европе, једино су САД спровеле поступак ратификације (крајем 2007. године), а Канада, Јапан и Јужна Африка то нису учиниле.

Неколико решења из *Конвенције* наишло је на озбиљно оспоравање. Критици је подвргнут пре свега део 2, у оквиру Поглавља II, који се односи на процедурално право. Одредбе *Конвенције* су тако еластично формулисане да омогућавају државним органима да у току истражног поступка приступе свим приватним подацима који су електронски ускладиштени, без да је грађанима обезбеђена основна заштита од произвољног мешања у приватност, осигурано да ти подаци неће бити злоупотребљени или бар да је стриктно ограничена њихово коришћење[26].

Конвенција даље дозвољава државама да преносе и међусобно размењују податке о свим лицима која су уведена у било какву казнену евиденцију, а не само о лицима која су осумњичена за учешће у сајбер криминалу. На тај начин у току примене *Конвенције* могло би се изићи из оквира компјутерског криминала, што није била њена почетна идеја нити предмет њеног регулисања. Због тога се стручна јавност и браниоци грађанских права у појединим државама супротстављају њеној ратификацији.

Управо је Русија изразила највећу забринутост у погледу могућности да страни истражни органи слободно улазе у туђи виртуелни простор и вршљају по подацима у потрази за потенцијалним или осумњиченим прекршиоцима на међународном плану. Неконтролисани и слободни упади иностраних истражитеља у туђи информационо-комуникациони систем за ауторе у Русији представљали би вид угрожавања националне безбедности, тим пре што Конвенција реално даје право страним органима да у реалном времену "јуре" починиоце електронског криминала свуда по свету без

26) *Конвенција о сајбер криминалу*, Будимпешта, 23. новембар 2001, чланови 14-21.

да о томе претходно обавештавају локалне органе власти или траже њихову сагласност.

Одредбе *Конвенције* о екстрадицији такође су биле повод за нове полемике. Наиме, овде је предвиђено да се екстрадицијом могу обухватили и она лица чије изручење није експлицитно наведено у посебној, *Европској конвенцији о екстрадицији* из 1957. године. На одређени начин, проширене су и одредбе *Европске конвенције о узајамној помоћи у кривичним стварима* из 1959. године и Доданог протокола уз ову Конвенцију из 1978. године.

С тим у вези јавила се и дилема да ли се ратификацијом *Конвенције о сајбер криминалу* једноставно могу променити раније ратификовани међународни уговори или је потребно извршити допуну тих закона, као и да ли су нови процесни поступци усклађени са националним прописима о кривичном поступку. Исто тако, отворено је и питање сукоба норми националног законодавства у појединим државама, а у пракси се показало и донекле спорним питање јурисдикције над лицима из више земаља која учествују у јединственом криминалном подухвату.

Опаске се износе и у погледу правне логике и генералног приступа на којима који *Конвенција* почива. У том смислу замера се да *Конвенција* не уважава друге правне културе и да не води довољно рачуна о постојању структуралне диспропорција у развоју информационо-комуникационих система. Осим мањег броја технолошки развијених земаља постоји и убедљива већина оних које су технолошки недовољно развијене, а *Конвенција* није ту чињеницу узеле у обзир.

На тој линији приговорено је да је *Конвенција* писана у оквиру Савета Европе, уз снажан утицај САД, Канаде и Јапана, због чега више одсликава њихове интересе, него потребе већине осталих земаља а посебно оних у развоју. Те мање утицајне државе имају одређене резерве према *Конвенцији* које нису искључиво правног карактера, утолико што је доживљавају и као политички инструмент у рукама војно-политички и технолошки најутицајнијих држава.

Простим уграђивањем одредби *Конвенције* у национално законодавство технолошки неразвијених држава, а због недовољног знања и необучености, велики број корисника компјутера би, врло лако и нехотице потпао под удар одређених казнених одредби Конвенције. Због непознавања прописа и без да су они тога свесни, они би постали технолошки деликвенти, односно могли бити затечени у вршењу криминалних дела.

Огромна већина рачунара тамо је набављена или склопљена илегално, софтверски пакети су мултипликовани без дозволе, антивирус лиценце су клониране тако да исту шифру користи на стотине појединаца и слично. Други начин за набавку тих уређаја, осим овог илегалног или недовољно легалног најчешће није ни постојао. Све то због рестриктивног односа власти, непостојања регулативе, одсуства морала у трци за профитом појединих предузетника и мултинационалних компанија али и због низа других разлога.

У Србији није вођена расправа о могућим импликацијама и недоумицама око примене Конвенције. Једино је у току полемике око нових прописа о личним исправама, заснованим на биометријским подацима, било неслагања око оцене ризика неовлашћеног задирања у личне податке и опасности да ти подаци доспеју у нежељене руке. Искристалисала су се два опречна мишљења. По једном, примена чипова на идентификационим документима представља хватање корака са светом, а по другом, она представља Орвеловску предају душе и разума технолошком ђаволу.

Истина, низак ниво информатичко-компјутерске повезаности и опремљености српског друштва, а пре свега привредних субјеката, још не омогућава да се на домаћем терену препознају проблеми које примена *Конвенције* у одређеним сегментима може изазвати. Ти проблеми објективно још нису доспели у видокруг ни тужилаштва, ни судства, а још мање полиције, из простог разлога што је и степен откривености високо-технолошког криминала још далеко испод оног у западним државама. Разуме се, правна наука ће овим питањима поклонити потпунију пажњу тек када у практичној примени буду настале недоумице и када се појави проблем тумачења и колизије одређених прописа.

ИНТЕГРАЛНО СУПРОТСТАВЉАЊЕ САЈБЕР КРИМИНАЛУ

Технолошки развијене државе прве су уочиле значај усклађеног и организованог деловања против рачунарског криминала и са њим повезаним облицима нарушавања информационо-комуникационе безбедности. Оне су још средином последње деценије прошлог века осмислиле механизам сталног дежурства, међусобног обавештавања и синхронизовног деловања, под називом „Мрежа 24/7". Тај механизам је први пут успостављен 1997. године у

оквиру Групе осам (Г-8) најразвијенијих земаља, да би 2001. године била уграђена у *Конвенцију* о *сајбер* криминалу.

Мрежи су се придружиле и неке државе које нису чланице Савета Европе, као и поједине које су потписале али још нису ратификовале *Конвенцију*. На тај начин мрежа је проширена изван оквира држава уговорница *Конвенције*, тако да данас обухвата 55 земаља.

Поменути механизам сталног дежурства и међусобне повезаности, омогућава државама које су га прихватиле да промптно и синхронизовано реагују на покушаје напада од стране *сајбер*-криминалаца, да замрзну њихове електронске поруке и друге стациониране податке, и то у реалном времену и материјално препознатљивој форми. Брзина реаговања на упад је најважнија претпоставка онемогућавања „интрудера" да уклоне дигиталне отиске својих криминалних радњи. Истрага у таквим условима траје свега неколико сати, уместо неколико недеља или месеци, а поступак против криминалаца постаје техничко-технолошки доказив и процедурално комплетан.

Суштина свих ових међународних напора је да се *сајбер* криминалцима да до знања да ће за своје штетне радње сносити једнаке консеквенце на свим меридијанима и да их географска удаљеност од места извршења виртуелног злочина неће сачувати од мача правде.

За Србију ће посебно бити значајно да примени члан 35 Конвенције, који налаже да се формира посебна служба, односно "да одреди место за контакте које ће бити доступно 24 сата, свих 7 дана у недељи, да би омогућила моменталну помоћ у истражне сврхе или за процедуре у вези кривичних дела која се односе на компјутерске системе и компјутерске податке, или ради прикупљања доказа за кривична дела у електронском облику"[27]. Због природе електронског криминала, његово сузбијање и спречавање може бити ефикасно само уколико се одвија у реалном времену, а не са неколико месеци или година закашњења, и под условом да државе међусобно сарађују.

У складу са предвиђеним механизмом узбуне, уколико би се трагови, извршилац, или било шта друго у вези са једним кривичним делом налазило на територији Србије, одговарајући орган стране државе имао би право да одмах позове и затражи поступање државних органа Србије. Наведени захтев неодложно би мора бити извршен од стране потписника *Конвенције*, јер је то једини на-

27) *Конвенција о сајбер криминалу*, Поглавље 3, члан 35.

чин за спречавање међународно организованог криминала и његово избављење од одговорности пред националним законодавством.

Први ефекти примене овог механизма осетиће криминалци који су се већ повезали на нивоу Балкана. Досад је у Србији ухваћено десетак мањих група, које су се бавиле клонирањем банкарских платних картица или њиховом крађом у једној, а коришћењем у суседној земљи. Али то је само врх леденог брега. Не само да поједина криминална дела у овој области није лако открити због њихове софистицираности, већ се понекад и сазнања о „успесима" криминалаца крију од јавности, нарочито када се ради о банкама, да се не би довео у сумњу кредибилитет појединих емитера платних, кредитних и сличних картица. Све до 2003. године таква кривична дела у домаћем законодавству уопште нису ни постојала, па се за њих није могло ни одговарати.

У Србији се на високотехнолошки криминал још гледа као на нешто периферно. Републички завод за статистику је прва и једина институција која је почетком 2009. године спровела истраживање у вези са информационом безбедношћу. Других истраживања није било, док се у свету редовно спроводе анкете анонимног карактера о покушајима упада, превара, крађе, фалсификовања података и других рачунарских злоупотреба или напада међу домаћим предузећима. Привредна друштва и предузетници највећим делом, осим ако изузмемо велике системе, банке и слично, немају стручно знање, одговарајуће службе или навику заједничког деловања у супротстављању електорнским упадима. Шта више нема ни одговарајуће институције републичког карактера преко којих се могу обавештавати о проблемима са високо-технолошким криминалом и едуковати за његово спречавање.

Уз Македонију, Босну и Херцеговину и Албанију, Србија спада у малобројне државе у региону која још није формирала такозвани национални центар за рачунарску безбедност. Тај центар у већини земаља носи назив ЦЕРТ (према енглеској скраћеници *Computer Emergency Response Team*[28]), а његов је основни задатак да посредује у решавању рачунарско безбедносних инцидената у којима учествује неко правно или физичко лице из одређене државе, да прикупља и одашиље савете у вези заштите рачунара, упућује препоруке, даје обавештења о најприкладнијим алатима, образује и информише кориснике, као и најширу јавност, о неопходности и начину побољшања заштите рачунарских система и мрежа од разних злоупотреба, а пре свега од оних криминалне природе. Чла-

28) У САД је овај центар функционише под називом *US- Computer Emergency Readiness Team*.

нови ЦЕРТ су како индивидуални тако и колективни корисници рачунара, а пре свега јавне установе, пословне асоцијације, привредна друштва, предузетници и други субјекти.

У Србији пословни свет не размишља довољно о томе да електронски стациониране информације, дигитализоване пословне тајне, нови пројекти и студије изводљивости, налози за електронско плаћање и други подаци или инструменти који су похрањени у рачунарима лако могу постати плен виртуелних крадљиваца и злонамерне конкуренције. Системи заштите сопствене мреже од криминалних радњи недовољно су познати, а предузетници немају коме да се обрате уколико и открију да неко покушава упад у њихову интерну компјутерску мрежу. О култури информационе безбедности говори се само спорадично, по правилу једном годишње, као о 8. марту или Дану штедње.

Приликом коришћења Интернета, привредници готово не воде рачуна о безбедности информација које размењују преко мреже, депонују у одређена дигитална складишта или преузимају са бизнис портала. Они лако заборављају да многи подаци који путују Интернет каналима садрже информације поверљиве (на пр. лични подаци) или осетљиве природе (на пр. финансијски извештаји). Податке те врсте потребно је заштитити како би се спречио њихов преглед, измена или злоупотреба. Један од првих облика заштите била је примена ССЛ (енг. *Secure Sockets Layer*) протокола. Данас је ова заштита прерасла у нови, виши стандард чија је ознака ТЛС (енг. *Transport Layer Security*) протокол. Основна улога наведеног протокола је да заштити податке приликом комуникације, као и да осигура аутентификацију учесника пословних операција путем рачунарске мреже.

НЕУЈЕДНАЧЕНОСТ РЕГИОНАЛНИХ СИСТЕМА ЗАШТИТЕ

Напад на информационо комуникационе системе врши се на различит начин од земље до земље и од континента до континента, што такође отежава уједначавање активности на планетарном супротстављању високотехнолошком криминалу.

У Азији тако доминирају „*spam*" напади, који чине 34,1 одсто од укупног броја сајбер деликата. На Европу одлази 31,9 одсто, Северну Америку 24,2 одсто, Јужну Америку 8,3 одсто, Африку 1 одсто и Аустралију 0,5 одсто. По инфицираности „ *botnet* " предњаче системи у САД са 26 и Великој Британији са 22 одсто, док је

ова пошаст у Кини присутна са свега 9 одсто, а у Јапану са 2 одсто. Борба против сајбер криминала може бити успешна и на националном и на међународном плану. Ту се као позитиван пример најчешће помиње Холандија. Употреба одговарајуће (и скупе) опреме и одбрамбених филтера пете генерације смањила је тамошње „ *spam*"- нападе за чак 85 одсто. У Финској су ови напади смањени за 80—30 одсто и тсл.[29)]

Готово све регионалне организације здушно су се ангажовале у том правцу. *Државе Комонвелта* (окупљене око „британске круне") утврдиле су 2002. године „Модел закон", као образац за реформу сопствених закона о сајбер криминалу. *Државе чланице ASEAN* (асоцијације земаља Јужне Азије) приступиле су билатералним формама стратешког партнерства у овој области и одржале низ важних конференција, на министарском и на оперативном полицијском нивоу.

Европска унија је прве директиве које су се тицале заштите електронских података донела још 1995. године[30)], а после 2001. године читав низ докумената о јединственој борби против различитих облика злоупотреба компјутера, укључујући оне са терористичким намерама. Последња у низу била је *Оквирна одлука у вези напада на информационе системе* из 2005. године[31)], а 2008. године је „*антитерористичка" директива*[32)] амандирана забраном јавних провокација, регрутовања и обуке путем коришћења компјутерске технологије. *Савет Европе* не само да је 2001. године донео већ поменуту *Конвенцију о борби против сајбер криминала* већ редовно годишње одржава састанке на којима се сумирају резултати укупних активности на овом плану.

*Чланице АПЕК (*Азијско-пацифичке кооперације) су такође успоставиле специфичне облике сарадње (на пример „Телекомуникациона радионица о политици и техници приступања борби против *botnet*-а" 2008 године у Токију) и одржали низ важних скупова (међу којима је последњи Министарски скуп у Банкоку 2008. године). *Организација америчких држава* (OAS) је још 1999. године формирала „Експертску групу за супротстављање сајбер-криминалу". Од 2005. године се одржавају редовни годишњи састанци министара правде држава чланица, а до краја 2008. године усвојено је пет скупова правних препорука (*Set of Recommendations*) које има-

29) http://www.ic3.gov/media/annualreports.aspx/1/3/2010.

30) Directive 95/46/EC

31) 2005/222/JNA

32) 2002/475/JNA

ју сличну улогу као директиве у систему ЕУ. Веома значајни рад на сузбијању сајбер криминала као једну од редовних активности обавља и *Међународна телекомуникациона унија* (ITU). Огроман допринос пружају и такве професионалне организације као што је међународна полицијска асоцијација (*Интерпол).*

Хармонизација прописа о сајбер криминалу на регионалном нивоу имала је своје специфичности, па је, осим добрих, показала и једну лошу страну. Наиме, она је резултирала у паралелном постојању више правних концепата за сузбијање *сајбер* криминала, који су међусобно недовољно конзистентни. Зато се сада намеће потреба њиховог приближавања и уједначавања. Али разлике постоје око начина на који се може доћи до транснационалног решења.

Две су тенденције засад присутне. Једна, коју заговара Савет Европе, да „његова" Конвенцију из 2001. године буде „протегнута" на све државе света, што се образлаже како разлозима уједначавања праксе и прописа, тако јачања поверења у информационе и комуникационе технологије. Тај став је посебно дошао до изражаја на петој годишњој конференцији о спровођењу Конвенције СЕ о „сајберкриминалу" (такозвана OCTOPUS конференција), која је од 23 до 25 марта одржана у Стразбуру.[33)] Друга иницијатива иде за тим да се донесе нова конвенција, под окриљем УН, како због слабости које садржи сама Конвенција Савета Европе, тако и због превазиђености неких њених решења. Ову иницијативу подржавају Међународна конвенција за телекомуникације, Русија, Бразил и значајан број латиноамеричких држава. Свој глас у прилог израде нових глобалних глобалних стандарда УН у овој области, дали су 19 априла 2010 и учесници Конгреса УН о спречавању криминала и јачању правде (UNDOC). Истина, иницијатива да се започне рад на изради посебне конвенције УН још није формално усвојена, али се та опција чини прихватљивијом од проширивања дејства Конвенције Савета Европе на остали део свет.[34)]

ЗАКЉУЧАК

Упркос недоумицама око појединих одредби, као и половичној ратификацији, *Конвенција Савета Европе о сајбер криминалу* представља досад најзначајнији међународно-правни оквир и

33) Messages from the Octopus conference, Strasbourg, March 25, 2010, www.coe.int/cybercrime;

34) UNDOC, A/CONF.213/1., Salvador, Brazil, 12-19 April 2010, PDF document.

упутство за супротстављање растућем високо-технолошком криминалу. Она идентификује све кључне тачке на којима корисници рачунара могу прећи линију законом дозвољеног понашања и јасно маркира оне ситуације и активности кроз које се генерише *сајбер*-криминал. Инструменти на којима се заснива Конвенција, а посебно механизам 24/7, представљају платформу за интегрисање међународних напора и активности на превенцији, сузбијању и кажњавању *сајбер* криминала.

За Србију је ратификовање *Конвенције* представљало много више од формалног укључивања у међународне активности на сузбијању *сајбер* криминала. Оно је представљало обавезну степеницу која се морала проћи на "мапи пута" ка белој Шенгенској листи. Сматрамо да ће пуно интегрисање Србије у ове заједничке напоре на сузбијању сајбер криминала временом наметнути потребу да се донесе и посебан закон о закон о овој проблематици, као и да се у оквиру Министарства унутрашњих послова оформи посебна Управа за борбу против високо-технолошког криминала.

За неке друге земље већ само потписивање *Конвенције* било је довољно да се оне у пуној мери укључе у заједничку борбу против виртуелног криминала. Одлажући ратификацију Конвенције, оне су за себе задржале могућност да у националном законодавству на другачији начин уреде питања око којих постоје озбиљне разлике унутрашњих политичких снага. Та питања ће вероватно у скорој будућности тражити допунска разјашњења или измену појединих одредби *Конвенције*, али покретање истих неће довести у питање привржености заједничком деловању против свих облика високо-технолошког криминала. Мало је при том вероватно да ће се Конвенција Савета Европе наметнути као глобални стандард. Много је вероватније да ће се приступити изради нове конвенције под окриљем Уједињених нација. Поред осталог и зато што Русија, Бразил, Индија, Кина, Велика Британија као и огромна већина држава у свету не показује спремност да прихвате Конвенцију Савета Европе.

ЛИТЕРАТУРА

Митровић, др Ђорђе: "Могућности и проблеми будућег развоја информатичког друштва у Србији у процесу придруживања ЕУ", *Економске теме*, Ниш, 2007, вол. 45, бр. 3.

Службени гласник Републике Србије, 2004-2009.

Безбедност информационих система, Зборник радова, издавач Академија за дипломатију и безбедност, Београд, 2009.

Васић, др Душан: "Информациони рат и међународно право", *Правни живот*, бр. 13/2009, Том V.

Stein Schjolberg**,** Chief Judge: "International Pathways to Cybersecurity", A presentation at the *EastWest Institute 7th Worldwide Security Conference*, February 17, 2010.

Cybercrime and Security, general editor Pauline C. Reich, Oxford University Press, London, 2010, Vol I, II, III.

Dusan Vasic

CERTAIN OPEN ISSUES REGARDING THE IMPLEMENTATION OF THE COUNCIL OF EUROPE CONVENTION ON CYBER CRIME

Summary

Advancement of Serbia toward the European Union requires its integration into the common Europe-wide concept of combating high technology criminal. The platform for this concept was laid down by the Council of Europe Convention on cyber crime. To this date, there are 46 states signatories to the Convention, but only 28 have completed the process of ratification. The reason is that some provisions of the Convention remain contestable and therefore, difficult to transpose into national laws. This paper will focus on those open issues, concluding that all the parties to the Convention remain dedicated to the common concept of prevention, suppression and penalization of cyber crime regardless of the delay in the ratification process. Furthermore, in the author's opinion, the current halt in the process of the Convention ratification and some of its shortcomings could be overcome by the adoption of a new universal convention under the auspices of the United Nations.

Key words: Convention on cyber crime; high-tech criminal; personal data protection; 24/7 Network; Computer Emergency React Team (CERT);