БЕЗБЕДНОСНА ПОЛИТИКА

UDK: 343.533::004
Biblid 1451-3188, 14 (2015)
Год XIII, бр. 51, стр. 318–335
Изворни научни рад

др Владимир УРОШЕВИЋ[1]
мр Сергеј УЉАНОВ[2]

ЗНАЧАЈ ДЕКЛАРАЦИЈЕ МИНИСТАРА И ВИСОКИХ ФУНКЦИОНЕРА О СТРАТЕШКИМ ПРИОРИТЕТИМА У БОРБИ ПРОТИВ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

ABSTRACT

Countries of South-East Europe (SEE) going through the process of political and economic transition, and in recent years they are challenged by threats of cyber crime and removing consequences caused by cybercrime. The joint regional project of the European Union and the Council of Europe on cooperation against cybercrime under the Instrument of Pre-Accession (Cybercrime@IPA) started on 1 November 2010 and had duration of two years. Under the umbrella of this project, the Ministers and Senior Officials of Ministries of Interior and Security, of Ministries of Justice and of Prosecution Services of the countries and areas participating in the CyberCrime@IPA project adopted in 2013. in city of Dubrovnik, Republic of Croatia declaration named: "Strategic Priorities in the Cooperation against Cybercrime". The authors are about to make review on this Declaration and its long term significance for the Republic of Serbia in the area of cyber crime suppression.

Key words: Cyber crime, regional cooperation, European Council, European Union.

[1] Министарство унутрашњих послова Републике Србије, Институт за упоредно право, Београд. Е-маил: vladimir.urosevic@mup.gov.rs.

[2] Министарство унутрашњих послова Републике Србије.

I) УВОД

Карактеристике високотехнолошког криминалитета као што су: анонимност, брзина, потенцијал за виктимизацију великих размера, као и мултијурисдикциона природа, посебно усложњавају борбу против високотехнолошког криминала. Високотехнолошки криминал представља једну нову форму транснационалног организованог криминала, и неопходно је, стога, разматрати, како улоге, тако и приоритете у овој области. Решавање проблематике ове области изискује поштовање међународних обавеза, квалитетну координацију и прецизно одређену сарадњу. Постоји неопходност познавања нових вештина, технологија и истражних криминалистичких метода које се морају применити у циљу превенције, регистровања и адекватног одговора и заштите критичних инфраструктура. У протеклим годинама широм света уочени са јаки таласи напада високотехнолошког криминала који су по свом карактеру били високософистицирани и досезали су неслућене размере на глобалном нивоу. Приликом извршења кривичних дела извршиоци су показали да имају довољно знања и вештина да нпр. рачунарским вирусима заразе милионе персоналиних рачунара који припадају државним институцијама, приватним предузећима, као и обичним грађанима. Ови напади јасно су указали и на потребу да се у процене безбедносних ризика укључи шира друштвена заједница.

Подручје Југоисточне Европе је веома специфично када је у питању борба против високотехнолошког криминала. На Интернету се појављују сервиси и пружају се услуге које су по својој природи регионалне (као пример chat rooms, IRC канали, Интернет сајтови, форуми, блогови). Регион југоисточне Европе је део европског континента, али земље у овом региону имају (у великој већини) сличан језик, културну и етничку припадност итд. Посебна забринутост ЕУ када је овај регион у питању је чињеница да постоје историјска и традиционална "пријатељства" међу криминалцима у овом региону која би могли да утичу на формирање регионалних организованих криминалних групе које ће деловати у области високотехнолошког криминала.

Неки од проблема на подручју Југоисточног Блакана у који могу да утичу на формирање таквих организованих криминалних групе су:

– Ефекти глобалне економске кризе у региону.

– Успорен процес европских интеграција.

– Погоршање билатералних политичких односа у региону.

– Крхкост установљених регионалних структура.

– Недостатак узајамног поверења.[3]

II) СВРХА

На регионалној Конференцији о стратешким приоритетима у борби против високотехнолошког криминала која је одржана у Дубровнику у Хрватској од 13. до 15. фебруара 2013. године у сарадњи држава потписница Декларације са Саветом Европе и Европском унијом наведено је више разлога за усвајање Декларације. Министри и високи функционери који су на наведеној конференцији представљали министарства унутрашњих послова и безбедности, министарства правде и државна тужилаштва земаља и подручја који учествују у пројекту CyberCrime@IPA[4] истакли су неколико битних разлога за усвајање Декларације, као што су:

– Корист од информационих и комуникационих технологија које трансформишу друштва Југоисточне Европе;
– Забринутост због ризика од високотехнолошког криминала који негативно утиче на сигурност и поверење у информационе технологије, као и на права и безбедност лица, укључујући нарочито децу;
– Изричита обавеза влада региона Југоисточне Европе да штите грађане од високотехнолошког криминала.
– Потреба да се поштују основна права и слободе, укључујући заштиту грађана у вези са обрадом података о личности приликом заштите друштва од криминала.
– Потреба за сарадњом између јавног и приватног сектора ради спречавања и сузбијања високотехнолошког криминала и заштите рачунарских система; делотворне мере против високотехнолошког криминала захтевају ефикасну регионалну и међународну сарадњу.
– Вредност Будимпештанске конвенције о високотехнолошком криминалу као смернице за домаће законодавство и правног оквира за међународну сарадњу;

[3] S. Uljanov, V. Urosevic, "The role of regional organizations in combating cybercrime in the Western Balkans", International scientific conference *Western Balkans: from stabilization to integration*, Institute of International Politics and Economics, Belgrade, 07-08.07.2011., Belgrade, pp. 468-480.

[4] Савет Европе: „Стратешки приоритети сарадње у области високотехнолошког криминала" Интернет: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project 20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_SRB_final_adopted.pdf (приступљено 15.12.2014. године)

– Све већи значај који Европска унија придаје безбедности рачунарских система и деловању против високотехнолошког криминала.
– Потреба за партнерствима између Европског центра за борбу против високотехнолошког криминала (EC3) у Европолу и наших органа за спровођење закона.
– Подршку коју су пружиле Европска унија и Савет Европе кроз регионални пројекат CyberCrime@IPA.
– Остварени напредак и на мере против високотехнолошког криминала које су већ предузете у земљама и подручјима региона, уз истовремено констатовање да су потребни додатни напори.

III) МЕРЕ ЕУ

Данас, у 21. веку јасно је уочљива потреба за развојем иновативних приступа, као и нових стратегија и технологија које ће бити адекватне за спречавање ових по много чему софистицираних и друштвено штетних напада. Управљање информацијама, координација и интеракција са кључним факторима у друштву постали су незаобилазан фактор у решавању ових проблема. Многи појавни облици високотехнолошког криминала остали су исти, али свакога дана неслућеном брзином мењају своје појавне облике прилагођавајући се на новонастале промене у информационом окружењу. Појава нових услуга и Интернет сервиса са собом носи ризик од масовних злоупотреба на глобалном нивоу. Појава злоупотреба у области нових типова Интернет сервиса као што су социјалне мреже, *P2P* сервиси (*Peer-to-Peer*), *VoIP* технологије, *cloud computing*, нови начини електронског пословања и електронског банкарства, бежичне технологије, сервиса који пружају анонимност на Интернету итд. јасно је указала на чињеницу да је Интернет све рањивији на овакве нападе. Са развијањем Интернет технологија и услуга и омасовљењем његовог коришћења дошло је до нагле експанзије високотехнолошког криминала и такав тренд се предвиђа и у будућности... Подручје Југоисточне Европе је, када је високотехнолошки криминал у питању, веома специфично, а многе државе су у процесу придруживања Европској унији. Помоћ ЕУ и Савета Европе у борби против овог вида криминала је кључна. Пројекат *Cybercrime@IPA* започет је 01.11.2010 године а завршен је 1.11.2012. године. Пројекат је финансиран је из *IPA* фондова и заједнички је регионални пројекат Европске уније и Савета Европе о сарадњи против високотехнолошког криминала у оквиру Инструмента за претприступну помоћ (*IPA*). Државе и територије које су учествовале у

пројекту су: Албанија, Босна и Херцеговина, Хрватска, Црна Гора, Србија, Македонија, Турска и Аутономна покрајина Косово и Метохија. Пројекат је спроводи Савет Европе. Кроз овај регионални пројекат, Европска унија и Савет Европе пружили су подршку властима да побољшају своје способности за спречавање и контролу високотехнолошког криминала, а на основу постојећих алата и инструмената, што се нарочито односи на Будимпештаанску конвенцију о компјутерском криминалу (*CETS 185*)[5] и њен протокол о ксенофобији и расизму (*CETS 189*)[6].

IV) САДРЖАЈ

У Декларацији министара и високих функционера о стратешким приоритетима у борби против високотехнолошког криминала која је усвојена акламацијом у Дубровнику у Хрватској, 15. фебруара 2013. године наведено је да представници држава и територија учесница подржавају стратешке приоритете у области високотехнолошког криминала представљене на тој конференцији и да су опредељени да:

– Спроводимо стратегије борбе против високотехнолошког криминала ради осигурања делотворне реакције кривичног правосуђа на кривична дела против рачунара и помоћу рачунара, као и било које кривично дело које укључује електронске доказе;
– Усвоје потпуно и делотворно законодавство о високотехнолошком криминалу које испуњава захтеве у погледу људских права и владавине права;
– Јачају специјализоване јединице за спровођење закона и специјализацију тужилаштава у вези са високотехнолошким криминалом и електронским доказима;
– Спроводе одрживе стратегије обуке органа за спровођење закона;
– Подржавају обуку судија и тужилаца о високотехнолошком криминалу и електронским доказима;
– Спроводимо свеобухватне стратегије ради заштите деце од сексуалног искоришћавања и сексуалног злостављања преко интернета у складу са Ланзаротском конвенцијом;[7]

[5] "Convention on Cybercrime", CETS No.185, Councile of Europe, Budapest, 2001.

[6] "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", CETS No.189, Councile of Europe, Strasbourg, 2003.

[7] "Convention for the protection of children against sexual exploitation and sexual abuse", CETS No.201, Councile of Europe, Lanzarote, Spain, 2007.

– Унапређују финансијске истраге и спречавање и сузбијање превара и прања новца преко интернета;
– Јачају сарадњу са приватним сектором, нарочито између органа за спровођење закона и добављача интернет услуга;
– Укључују се у ефикасну регионалну и међународну сарадњу;
– Деле своје искуство са другим регионима света ради подршке изградњи капацитета за борбу против високотехнолошког криминала;
– Промовишу придржавање Будимпештанске конвенције о високотехнолошком криминалу на глобалном нивоу.

У прилогу наведеног документа налази се листа осам стратешких приоритета у области високотехнолошког криминала и то:

1) Стратешки приоритет: „*Политике и стратегије у области високотехнолошког криминала*“. У оквиру овог стратешког приоритета наведено је безбедност информационо-комуникационих технологија постала приоритет политика многих влада будући да информациона и комуникациона технологија трансформише друштва. То се одражава у усвајању стратегија безбедности рачунарских система с првенственим фокусом на заштиту критичне информационе инфраструктуре. Међутим, владе имају и изричиту обавезу да штите људе и њихова права од високотехнолошког криминала и да приводе починиоце кривичних дела правди. У тексту се даље наводи и да владе држава треба да размотре припрему посебних стратегија борбе против високотехнолошког криминала или да унапреде компоненте везане за високотехнолошки криминал у оквиру стратегија односно политика безбедности рачунарских система (*cybersercurity*).

Према Декларацији надлежни органи би требали да размотре следеће мере:

– Усвојити политике односно стратегије борбе против високотехнолошког криминала с циљем осигурања делотворне реакције кривичног правосуђа на кривична дела против рачунара и помоћу рачунара као и било које кривично дело које укључује електронске доказе. Као елементе таквих политика односно стратегија размотрити превентивне мере, законодавство, специјализоване јединице за спровођење закона и тужилаштва, међуагенцијску сарадњу, обуку органа за спровођење закона и правосуђа, сарадњу јавног и приватног сектора, делотворну међународну сарадњу, финансијске истраге и спречавање превара и прања новца, и заштиту деце од сексуалног насиља.

– Обезбедити да се поштују захтеви у погледу људских права и владавине права приликом предузимања мера против високотехнолошког криминала.
– Успоставити платформе на интернету за подношење пријава од стране јавности о високотехнолошком криминалу. То би требало да обезбеди боље разумевање претњи и трендова високотехнолошког криминала и да олакша деловање кривичног правосуђа. Такве платформе могу да се користе и за информисање јавности и упозорења о претњама.
– Подизати свест и промовисати превентивне мере на свим нивоима.
– Укључити се у сарадњу јавног и приватног сектора, укључујући нарочито сарадњу између органа за спровођење закона и пружаоца интернет услуга.
– Укључити се у највећем могућем степену у међународну сарадњу. То обухвата пуно коришћење постојећих билатералних, мултилатералних и регионалних споразума, нарочито Будимпештанске конвенције о високотехнолошком криминалу. Треба спровести мере и обуку за убрзање међународне правне помоћи. Владе (потписнице Конвенције и посматрачи) треба да активно учествују у раду Комитета Конвенције о високотехнолошком криминалу (*T-CY*) и треба да се укључе у сарадњу са Европским центром за борбу против високотехнолошког криминала (*EC3*) и другим иницијативама Европске уније.
– Редовно оцењивати делотворност реакције кривичног правосуђа на високотехнолошки криминал и водити статистику. Такве анализе би помогле да се утврди и побољша успешност деловања кривичног правосуђа и да се ефикасно распоређују ресурси.Декларација о стратешким приоритетима борбе против високотехнолошког криминала

2) Стратешки приоритет: *„Потпун и делотворан правни основ за деловање кривичног правосуђа“*. У оквиру овог стратешког приоритета наведено је да је адекватно законодавство је основ за мере кривичног правосуђа против високотехнолошког криминала и коришћење електронских доказа у кривичним поступцима. У тексту декларације се даље наводи да су државе и подручја која учествују у пројекту *CyberCrime@IPA* остварили велики напредак у усклађивању свог законодавства са Будимпештанском конвенцијом, као и са сродним стандардима Савета Европе и Европске уније о заштити података, о заштити деце од сексуалног насиља или о имовини проистеклој из кривичног дела и прању новца. Међутим, спомиње се и да је потребнододатно јачање, а да законодавство често тек треба да прође кроз

проверу у пракси. Усвајање потпуног и делотворног законодавства које испуњава захтеве у погледу људских права и владавине права према Декларацији треба да буде стратешки приоритет.

Према Декларацији надлежни органи би требали да размотре следеће мере:

– Додатно побољшати одредбе процесног права о приступу органа за спровођење закона електронским доказима. То треба да обухвати законе и прописе за њихово спровођење у вези са применом одредаба Будимпештанске конвенције о хитној заштити (следећи корак после процене Комитета Конвенције о високотехнолошком криминалу), али и друга правила односно смернице о приступу подацима које поседују лица из приватног сектора.
– Оценити делотворност законодавства. Примена законодавства и прописа у пракси треба да се редовно оцењује. Треба водити статистичке податке о предметима који се истражују, гоне и по којима је донета пресуда и треба документовати примењене процедуре. Постарати се да овлашћења органа за спровођење закона подлежу условима и заштитним механизмима у складу са чланом 15. Будимпештанске конвенције. То треба да обухвати судски надзор интрузивних овлашћења, али и поштовање начела сразмерности и нужности. Оснажити законодавство о заштити података у складу са међународним и европским стандардима. ладе се подстичу да осигурају да њихово национално законодавство о заштити података буде усклађено с принципима Конвенције Савета Европе о заштити података ETS 108 и да учествују у актуелном модернизацијском процесу Конвенције. Исто важи за будуће стандарде Европске уније о заштити података. То ће олакшати прекогранично дељење података и за потребе спровођења закона.
– Употпунити законодавство и предузети превентивне и заштитне мере у вези са заштитом деце од сексуалног насиља преко интернета. Мада су имплементиране многе одредбе Ланзаротске конвенције, у неким земљама односно подручјима још увек се треба позабавити питањима као што су „поседовање дечје порнографије“, „свесно приступање садржају“ и „придобијање деце“ (grooming).
– Прилагодити законодавство о финансијској истрази, одузимању имовине проистекле из кривичног дела и о прању новца и финансирању тероризма у интернет окружењу.

Правила и прописи нарочито треба да предвиде брзу домаћу и међународну размену информација.

3) Стратешки приоритет: „Специјализоване јединице за борбу против високотехнолошког криминала“

У тексту Декларације је наведено и да високотехнолошки криминал и електронски докази захтевају специјализовану реакцију кривичних правосудних органа. Органи за спровођење закона и тужилаштва треба да буду у стању да истражују и гоне кривична дела против рачунарских података и система, кривична дела помоћу рачунара, као и електронске доказе у вези са било којим кривичним делом. У свим земљама и подручјима који учествују у пројекту CyberCrime@IPA у време усвајања Декларације у току је било формирање или јачање јединице полицијског типа за борбу против високотехнолошког криминала, а у некима се разматра и специјализација тужилаца. Тај процес како се у Декларацији наводи треба наставити. Битно је схватити да се технологија мења из дана у дан и да се стално повећава радно оптерећење јединица за борбу против високотехнолошког криминала и форензичких јединица. Прибављање ресурса (особља, опреме, софтвера) и одржавање специјализованих вештина и прилагођавање таквих јединица новонастајућим условима представља непрекидан изазов. Непрекидно јачање специјализованих јединица за борбу против високотехнолошког криминала треба да буде стратешки приоритет.

Надлежни органи, према Декларацији, треба да размотре следеће мере:

– Основати – где то још није учињено – специјализоване јединице за борбу против високотехнолошког криминала у оквиру кримииналистичке полиције. Тачна организација и функције треба да буду резултат пажљиве анализе потреба и да се заснивају на закону.
– Унапредити специјализацију тужилаца. Размотрити оснивање специјализованих јединица тужилаштва или, као другу могућност, групе специјализованих тужилаца да усмеравају или помажу другим тужиоцима у случајевима који укључују високотехнолошки криминал и електронске доказе.
– Редовно преиспитивати функције и обезбеђивање ресурса специјализованих јединица. То треба да омогући прилагођавања, а тако и одговоре на нове изазове и све веће захтеве.
– Олакшати сарадњу и размену добрих пракси између специјализованих јединица на регионалном и међународном нивоу.
– Побољшати процедуре за истраге високотехнолошког криминала и поступање са електронским доказима. Испитати и размотрити имплементацију националних и међународних стандарда и добрих

праксе по том питању. Размотрити коришћење „ водича о електронским доказима“ који је израђен у оквиру пројекта CyberCrime@IPA.

4) Стратешки приоритет: „Обука органа за спровођење закона“

У Декларацији се наводи да органи за спровођење закона треба да буду у стању не само да истражују кривична дела против и помоћу рачунарских система већ и да поступају са електронским доказима у вези са било којом врстом кривичног дела. Са експоненцијалним растом коришћења информационих технологија у друштву, у једнакој мери су порасли и изазови за органе за спровођење закона. Сви службеници органа за спровођење закона – од органа који први реагују до високоспецијализованих рачунарских форензичких истражитеља – треба да буду оспособљени да поступају са високотехнолошким криминалом и електронским доказима свако на свом нивоу. Идентификовани су, али још нису потпуно имплементирани елементи стратегија обуке органа за спровођење закона. Имплементација одрживих стратегија обуке за обучавање службеника за спровођење закона на одговарајућем нивоу треба да буде стратешки приоритет.

Надлежни органи би према Декларацији треба да размотре следеће мере:

– Имплементацију домаће стратегије обуке органа за спровођење закона. Циљ треба да буде да се обезбеди да органи за спровођење закона имају вештине и компетенције неопходне да истражују високотехнолошки криминал, обезбеђују електронске доказе, врше рачунарску форензичку анализу за кривичне поступке, помажу другим органима и доприносе безбедности мреже. Улагање у такву обуку је оправдано с обзиром на ослањање друштва на информационе технологије и с тим повезане ризике.
– Укључити правила и протоколе о поступању са електронским доказима на свим нивоима националне обуке. ажно је препознати да електронски докази утичу на све криминалне активности и да потребу за обуком за препознавање електронских доказа и поступање с њима имају сви службеници органа за спровођење закона који оперативно поступају, а не само они у специјализованим јединицама. Та обука би могла да буде базирана на „ одичу о електронским доказима“ који је израђен у оквиру пројекта CyberCrime@IPA.
– Размотрити увођење индивидуалних планова обуке за специјализоване истражитеље. Промене у технологији и начину на који починиоци кривичних дела злоупотребљавају ту технологију значе да постоји

потреба за одговарајућим бројем високообученог особља које је компететно и способно да спроводи истраге и/или испитивања дигиталних доказа на највишем нивоу. То ће побољшати и њихов статус у оквиру кривичног правосудног система.

– Размотрити имплементацију процедура да би се обезбедило да се максимално искористи улагање у обуку о високотехнолошком криминалу. Обука о високотехнолошком криминалу и рачунарској форензици веома је скупа. Како би обезбедиле да се улагање адекватно исплати, земље треба да се постарају да се чланови особља поставе и задрже на положајима који одражавају ниво знања и вештина које они поседују. У том циљу, стратегије обуке и стратегије управљања људским ресурсима треба да буду комплементарне.

5) Стратешки приоритет: *„Обука правосудних органа“*

У Декларацији је даведено да све судије и тужиоци треба да буду спремни да поступају са електронским доказима посебно зато што, поред кривичних дела против и помоћу рачунара, све већи број других врста кривичних дела укључује доказе на рачунарским системима или другим уређајима за чување података. У земљама и подручјима који учествују у пројекту CyberCrime@IPA учињен је напредак у смислу да су припремљени модули за обуку, да су обучени инструктори и да су одржани основни и напредни пилот курсеви. Поред тога, оснива се Регионални пилот центар за обуку правосудних органа о високотехнолошком криминалу и судским доказима. Та достигнућа треба институционализовати. Оспособљавање свих судија и тужилаца да врше гоњење и пресуђују у области високотехнолошког криминала и користе електронске доказе у кривичним поступцима треба да остане стратешки приоритет.

Надлежни органи треба да размотре следеће мере:

– Интегрисати обуку правосудних органа о високотехнолошком криминалу и електронским доказима у редовне програме. Домаће институције за обуку судија и тужилаца треба да интегришу основне и напредне модуле обуке о високотехнолошком криминалу и електронским доказима у своје редовне програме обуке за почетну обуку и обуку уз рад.

– Јачати Регионални пилот центар за обуку правосудних органа основан у Загребу у Хрватској. Домаће институције за обуку правосудних органа из региона треба да сарађују са Регионалним пилот центром за обуку

правосудних органа ради ажурирања материјала за курс, документовања и ширења добрих пракси и пружања регионалне обуке.

– Увести мере како би се обезбедило да обука правосудних органа о високотехнолошком криминалу и електронским доказима буде обавезна. Током пројекта је било очигледно да је обука за судије и тужиоце добровољна у већини области пројекта. То је довело до многих случајева у којима су учесници похађали обуку само веома кратко време током курсева и нису имали пуну корист од обуке која је пружена.
– Увести евиденцију обуке за појединачне судије и тужиоце. Како би се обезбедило да се обука која се пружа судијама и тужиоцима искористи на најбољи начин, препоручљиво је да се води евиденција о целој обуци коју добијају појединци како би се прикупиле информације о потребама за даљом специјализованом обуком и обезбедило да буду обучени прави људи и да се њихове вештине искористе на одговарајући начин.

6) Стратешки приоритет: *„Финансијске истраге и спречавање и сузбијање превара и прања новца на интернету“*

Највећи део криминала који укључује интернет и друге информационе технологије усмерен је на остваривање економске добити путем различитих врста превара и других облика привредног и тешког криминала. Тако се стварају и циркулишу на интернету велики износи користи проистекле из кривичног дела. Стога финансијске истраге које су усмерене на тражење, трајно и привремено одузимање имовине проистекле из кривичног дела и мере за спречавање превара и за спречавање и сузбијање прања новца на интернету треба да постану стратешки приоритет.

Према Декларацији Владе држава потписница треба да размотре следеће мере:

– Успоставити платформу на интернету за подношење пријава од стране јавности о превари на интернету и о високотехнолошком криминалу уопште. Коришћење стандардизованих образаца пријава омогућиће бољу анализу претњи и трендова, криминалних послова и организација, као и уобичајених модела новчаних токова и прања новца. То ће олакшати мере кривичних правосудних органа и финансијских обавештајних служби за гоњење починилаца кривичних дела и трајно и привремено одузимање имовине проистекле из кривичног дела. Платформа треба да врши и превентивне функције (подизање свести и образовање јавности, упозорења о претњама, инструменти и савети). Што су домаће платформе

усклађеније с платформама других земаља и подручја, то ће се више олакшати регионалне и међународне анализе и деловање. Промовисати проактивне паралелне финансијске истраге приликом истраге високотехнолошког криминала или кривичних дела која укључују информационе технологије/интернет. То захтева повећану међуагенцијску сарадњу између органа надлежних за борбу против високотехнолошког криминала и за финансијске истраге као и финансијских обавештајних служби. Такву међуагенцијску сарадњу може олакшати заједничка обука.

– Направити поуздане форуме (домаће и регионалне) за размену информација између јавног и приватног сектора о претњама рачунарским системима у вези са финансијским сектором. Домаћи форуми треба да буду на располагању кључним заинтересованим странама (као што су представници финансијског сектора, пружаоци интернет услуга, јединице за борбу против високотехнолошког криминала, финансијске обавештајне службе, тимови за реаговање на рачунарске безбедносне инциденте). Њихова намена је да идентификују претње, трендове, инструменте и решења за заштиту финансијског сектора од високотехнолошког криминала. Регионални форум треба да се састоји од форума основаних на домаћим нивоима.
– Успоставити правни оквир за привремено и трајно одузимање имовине проистекле из кривичног дела и дигиталних средстава, као и за спречавање прања новца преко интернета. То треба да обухвати дигитална средства као што је е-новац и виртуелне валуте. Правила, прописи и процедуре за спречавање прања новца треба да се примењују и на системе за плаћање преко интернета.
– Искористити могућности за ефикаснију међународну сарадњу. Повезивање мера за спречавање прања новца и финансијских истрага са истрагама високотехнолошког криминала и рачунарском форензиком пружа додатне могућности за међународну сарадњу. Владе држава потписница треба да искористе могућности које су им на располагању по Будимпештанској конвенцији о високотехнолошком криминалу, Конвенцији о прању, тражењу, привременом и трајно одузимању имовине проистекле из кривичног дела и финансирању тероризма (*CETS 198*) Савета Европе и 40 прерађених препорука Радне групе за спречавање прања новца Декларација о стратешким приоритетима борбе против високотехнолошког криминала (*FATF*). Осим тога треба размотрити налазе *MONEYVAL*-ове студије типологије токова новца проистеклог из кривичних дела на интернету из марта 2012. године.

7) Стратешки приоритет: *„Сарадња између органа за спровођење закона и пружалаца интернет услуга“*

Према тексту ове Декларације сарадња између органа за спровођење закона и пружалаца интернет услуга и других лица из приватног сектора битна је за заштиту права корисника интернета и за њихову заштиту од криминала. Делотворне истраге високотехнолошког криминала често нису могуће без сарадње интернет сервис провајдера. Међутим, таква сарадња треба да узме у обзир различите улоге органа за спровођење закона и интернет сервис провајдера, као и права корисника на приватност. Унапређена сарадња органа за спровођење закона и ИСП и размена информација између јавног и приватног сектора у складу са прописима о заштити података треба да постане стратешки приоритет.

Како се у тексту Декларације наводи Владе држава потписница би требале да размотре следеће мере:

– Установити јасна правила и процедуре на домаћем нивоу за приступ органа за спровођење закона подацима које поседују интернет сервис провајдера и друга лица из приватног сектора у складу са прописима о заштити података. Јасан правни основ у складу са одредбама процесног права и заштитним механизмима и условима Будимпештанске конвенције о високотехнолошком криминалу помоћи ће да се испуне захтеви у погледу људских права и владавине права. Смернице усвојене на конференцији Савета Европе „Octopus“ 2008. године могу помоћи да органи за спровођење закона и ИСП организују и структурирају своју сарадњу. ладе треба да олакшају коришћење одредаба о хитној заштити (чл. 16, 17, 29. и 30) Будимпештанске конвенције узимајући у обзир резултате процена Комитета Конвенције о високотехнолошком криминалу.
– Неговати културу сарадње између органа за спровођење закона и интернет сервис провајдера. У том погледу основни инструмент су меморандуми о разумевању између органа за спровођење закона и пружалаца интернет услуга. Регионална координација олакшала би способност органа за спровођење закона да спроводе истраге преко регионалних граница на основу сазнања да су у другим земљама и подручјима усвојени слични стандарди. Регионална сарадња би требала да поспеши и сарадњу у обелодањивању података који се чувају у иностраној јурисдикцији или на „cloud“ серверима којима управљају ти интернет сервис провајдери.
– Олакшати размену информација између јавног и приватног сектора преко граница. Лица из приватног сектора поседују велике количине података

о рачунарским безбедносним инцидентима. Прекогранична размена таквих података помогла би унапређењу безбедности информационе инфраструктуре, као и истрази починилаца кривичних дела. Ладе треба да размотре законодавство и закључивање споразума који омогућавају размену информација између јавног и приватног сектора и да подстичу развијање смерница за олакшавање размене информација унутар и преко граница, укључујући процесне, техничке и правне заштитне механизме и заштитне механизме у смислу заштите података.

8) Стратешки приоритет: *„Ефикаснија регионална и међународна сарадња“*

У тексту Декларације се даље наводи и да су високотехнолошки криминал и електронски докази по природи транснационални, те стога захтевају ефикасну међународну сарадњу. Потребно је неодложно деловање да се обезбеде електронски докази у иностраним јурисдикцијама и да се обезбеди обелодањивање таквих доказа. Међутим, неефикасност међународне сарадње, нарочито међународне правне помоћи, и даље се сматра једном од главних препрека које спречавају делотворну акцију против високотехнолошког криминала. Стварање ефикасније међународне сарадње по питању високотехнолошког криминала и електронских доказа треба да буде стратешки приоритет.

У Декларацији се наводи и да Владе треба да размотре следеће мере:

– Искористити могућности Будимпештанске конвенције о високотехнолошком криминалу и других билатералних, регионалних и међународних споразума о сарадњи у кривичним стварима. То укључује пуно коришћење чл. 23. до 35. Будимпештанске конвенције у вези са сарадњом између полицијских органа и између правосудних органа, укључујући прилагођавања прописа и унапређене процедуре. Владе (потписнице и посматрачи Конвенције) треба да у потпуности учествују у оцени одредаба Будимпештанске конвенције о међународној сарадњи коју ће 2013. године предузети Комитет Конвенције о високотехнолошком криминалу (*T-CY*). Оне треба да се надовежу на оцену *T-CY* из 2012. године и да промовишу коришћење чл. 29. и 30. Будимпештанске конвенције о међународним захтевима за заштиту података.
– Обезбедити обуку и размену најбољих пракси. Органи надлежни за сарадњу полицијских и правосудних органа треба да се укључе у домаћу, регионалну и међународну обуку и размену најбољих пракси. То треба да олакша сарадњу засновану на поверењу.

– Оценити делотворност међународне сарадње. Министарства правде и унутрашњих послова и тужилаштва треба да прикупљају статистичке податке о захтевима за међународну сарадњу у вези са високотехнолошким криминалом и електронским доказима, укључујући врсту захтева за помоћ, благовременост одговора и коришћене процедуре. То треба да помогне да се идентификују добре праксе и уклоне препреке за сарадњу. Она могу да сарађују са регионалним партнерима на анализирању питања која негативно утичу на међународну сарадњу.
– Ојачати делотворност контакт тачака доступних 24 сата дневно, 7 дана у недељи. Такве контакст тачке успостављене су у свим земљама и подручјима у складу са чланом 35. Будимпештанске конвенције, али треба да се унапреди њихова улога и можда треба да постану проактивније и потпуно функционалне.
– Редовно прикупљати статистичке податке о контакт тачкама доступним 24 сата дневно, 7 дана у недељи, и другим облицима међународне сарадње и преиспитивати њихову делотворност.

V) ИЗВОРИ

"Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" CETS No.189, Councile of Europe, Strasbourg, 2003.

"Convention for the protection of children against sexual exploitation and sexual abuse", CETS No.201, Councile of Europe, Lanzarote, Spain, 2007.

"Convention on Cybercrime", CETS No.185, Councile of Europe, Budapest, 2001

Uljanov S., Urosevic V.: *„The role of regional organizations in combating cybercrime in the Western Balkans"*, International scientific conference Western Balkans: from stabilization to integration, Institute of International Politics and Economics, Belgrade, 07-08.07.2011., Belgrade, pp.468-480.

Институт за стратешке студије и прогнозе МОНЕТ: „Црногорски економски трендови", вол. бр. 34, 2013. Интернет: http://issp.me/wp-content/uploads/2012/10/monet34se.pdf (доступно 03.01.2015. године).

Интернет: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project 20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_SRB_final_adopted.pdf (приступљено 15.12.2014. године)

Савет Европе: „Стратешки приоритети сарадње у области високотехнолошког криминала"

Урошевић В., Уљанов С., Ивановић З.: „Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције“, зборник радова Інтернационалне асоцијације криминалиста, *Међународна и национална сарадња и координација у супротстављању криминалитету*, Бања Лука 2010. стр. 530-541.

Урошевић В., Уљанов С., Ивановић З.: „Мач у *World Wide Web-y* – Изазови високотехнолошког криминала“, Етернал мих, Београд, 2012. стр.129.

VI) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Поред утицаја и препорука из ОЕБС-а у правном систему Србије није била покривена област високотехнолошког криминала и информационо комуникационих технологија све до ступања на снагу Кривичног законика Републике Србије из 2006. године, а као израз обавезе потписивања и ратификовања (истина тек 2009) *CEST* 185. Од тог тренутка се правни систем Републике Србије модификовао врло често, а неке измене су биле и веома темељне. Томе је такође допринела и улога радне групе у оквиру хармонизације у примени прописа *CEST* 185 и *CEST* 189, као део *CyberCrime@IPA* пројекта.[8] Развој борбе против високотехнолошког криминала је гледајући стање законодавства и укупне пратеће инфраструктуре у области међународне сарадње у погледу високотехнолошког криминала у Србији постигао висок степен али још увек није на задовољавајућем ступњу. Стратешки концепт супротстављања високотехнолошког криминалу дефинисан у Декларацији посебно добија на значају уз помоћ Савета Европе и Европске уније. Организовање регионалне сарадње у овој области, од стране Савета Европе и Европске уније као медијатора за остваривање хармонизованог одрживог развоја свих земаља *ЈИЕ* у наведеном документу има свој посебан значај за све државе потписнице. Могуће је предвидети да ће приказана Декларација у будућности подстаћи још искреније и ефикасније покушаје сарадње и иницирања дубљих контаката и одрживих размена информација на стратешком нивоу, које ће овим путем бити много лакше трасирати и каналисати. Група земаља која је у оквиру пројекта *Cybercrime@IPA SEE* одабрана веома је блиска према свим критеријумима и могуће је да је у оваквој средини много лакше укључити све неопходне

[8] В. Урошевић, С. Уљанов, З. Ивановић, „Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције“, зборник радова Интернационалне асоцијације криминалиста *Међународна и национална сарадња и координација у супротстављању криминалитету*, Бања Лука 2010. стр. 530-541.

чиниоце и остварити хармонизовану развојну структуру за ову веома видно прогресивну област. Основни смисао је да се у свим државама Југоисточне Европе, па самим тим и у Републици Србији, постигне сличан ниво спремности за реаговање на високотехнолошки криминал у свим структурама, као и да се у супротстављању ВТК пронађе модус који ће довољно брзо и довољно адекватно одговорити на надолазеће претње.[9] То укључује стратешку акцију на регионалном нивоу и могућност да структура која се налази испод прве капе одбране буде довољно флексибилна да прими први удар и анализира нападе и предузме неопходне мере на расветљавању и откривању дела и извршилаца. Процес хармонизације прописа у области ВТК под покровитељством Савета Европе и Европске уније у оквиру пројекта указује на значај активности свих актера у друштвеном животу сваке земље укључене у пројекат, а Декларација представља стратешки документ којом државе региона потврђују своју вољу и спремност да учествују проактивно на решавању овог проблема. Декларација јасно указује и друштвима наведених држава да се очекује укључивање широког фронта различитих институција постепено. Учешће широког спектра институција не само да би допринело квалитету резултата, већ обогаћује смисао самог рада на овој проблематици која је једна од најваријабилнијих и најразноврснијих. Имајући у виду да је регион Југоисточне Европе један од најугроженијих у Европи по питању деловања организованог криминала, те да је такође у интензивном процесу повећања друштвене зависности од информационо-комуникационе технологије, ово је добар почетак за проналажење адекватних регионалних одговора на претеће сајбер опасности у будућности.[10] Декларација би у региону требала да има много већи значај, пошто би се њеним поштовањем и спровођењем у дело проблематика високотехнолошког криминала у региону сигурно унапредила а сарадња на спречавању подигла на знатно виши ниво од постојећег...

[9] В. Урошевић, С.Уљанов, З. Ивановић: „Мач у *World Wide Web-y* – Изазови високотехнолошког криминала“, Етернал мих, Београд, 2012. p.129.

[10] Институт за стратешке студије и прогнозе МОНЕТ: „Црногорски економски трендови“, волумен бр. 34, 2013. година. Интернет: http://issp.me/wp-content/uploads/2012/10/monet34se.pdf (доступно 03.01.2015. године.