UDK: 004.738.5:061.1
Biblid 1451-3188, 10 (2011)
Год X, бр. 35–36, стр. 224–235
Изворни научни рад

Бранимир ЂОКИЋ[1]

ИНТЕРНЕТ НАПАДИ РЕГУЛАТИВА НА НИВОУ ЕВРОПСКЕ УНИЈЕ

ABSTRACT

Member states of European Union are among the most developed countries whose population, commerce and administration use internet extensively in their own affairs. Concerning cyber attacks, several documents have been adopted on the EU level within the fight against cyber crime. The most significant among them is the Framework Decision on attacks against information system of 2005. After the internet attacks on Estonia in 2007 and Lithuania in 2008, the emergence of Conficer and Stuxnet computer worms as well as the entry into force of the Lisbon Treaty, the European Union decided to respond to the new challenges by announcing a Proposal for a Directive on attacks against information systems.

Key words: cyber attack, botnet, information system, European Union, Framework Decision, Directive proposal.

I) СВРХА

Живот без интернета данас за многе постаје непојмљив. У Финској је право на доступност широкопојасног интернета чак предвиђено као законско право сваког грађанина.[2] У последњих пет година број интернет корисника у свету удвостручио се са једне на две милијарде.[3] Повећање броја корисника прати и повећање информационих система који су доступни преко интернета, али и њихов значај. Наиме, увидевши

[1] Судијски приправник у Првом основном суду у Београду.

[2] Mbit Internet access a universal service in Finland from the beginning of July, Интернет: *http://www.government.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=301979*, 17.03.2011.

[3] The World in 2010: ICT facts and figures, Интернет: *http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf*, 17.03.2011, стр. 4.

могућности уштеде и убрзања административних послова, државе масовно уводе е-управу и подстичу грађане да је што више користе. Банке данас највећи део својих трансакција и послова обављају управо преко интернета. Повећање броја корисника, услуга и капитала на интернету неминовно за собом повлачи и пораст како учесталости тако и озбиљности криминалитета у тој области. Напади на информационе системе су од појаве интернета еволуирали од сајбер вандализма, преко сајбер криминала до данас све изгледнијег сајбер ратовања. Један од највећих интернет напада на подручју Европе изведен је у Естонији 2007. године. Напад је био усмерен пре свега на државне и комерцијалне информационе системе. За последицу *e-mail* сервиси нису радили, бројне интернет странице државних институција нису биле доступне грађанима, а банке су биле принуђене да обуставе скоро све видове пословања преко интернета. Напад је значајно погодио Естонију јер је те године у Естонији 98% свих банкарских трансакција вршен преко интернета, док је чак 82% пореских пријава вршено електронским путем.[4] Такође, још 2008. године Светски економски форум проценио је да постоји 10 до 20% вероватноће да ће доћи до значајног слома критичне информационе инфраструктуре у наредних десет година, са потенцијалном глобалном економском ценом од приближно 250 милијарди америчких долара.[5] Европска унија, свесна зависности свог даљег просперитета од безбедности информационих система, овај проблем је увидела и предузела значајне кораке у циљу борбе против напада на информационе системе.

II) МЕРЕ ЕУ

Први корак који је начињен на нивоу Европске уније био је доношење Оквирне одлуке Савета Европске уније о нападима против информационих система из 2005. године (у даљем тексту: Одлука). Циљ доношења овог документа је да се унапреди сарадња између правосудних власти, полиције и других специјализованих државних органа држава чланица кроз приближавање њихових кривичних законодавства у области напада против информационих система. Наиме, постојала је оправдана бојазан да би разлике између законодавстава држава чланица могле да отежају борбу против организованог криминала и тероризма, који све више користе

[4] Cyber Security Strategy 2008 – 2013, http://www.kmin.ee/files/kmin/img/files/Kuber julgeoleku_strateegia_2008-2013_ENG.pdf, 17.03.2011, стр. 12.

[5] Global Risks 2008: A Global Risk Network Report, Интернет: *https://members.weforum.org/pdf/globalrisk/report2008.pdf*, 17.03.2011, стр. 48.

интернет за остваривање својих циљева. У изради Одлуке се умногоме ослањало на Конвенцију Савета Европе о високотехнолошком криминалу из 2001. године (у даљем тексту: Конвенција), чиме је олакшано и убрзано усаглашавање националних законодавстава како садашњих, тако и будућих чланица Уније које су већ потписнице овог документа.

Европска комисија (у даљем тексту: Комисија), саставила је *Извештај* 2008. године, на основу члана 12 Одлуке о напретку имплементације одредаба из Одлуке у национална законодавства држава чланица (у даљем тексту: Извештај) којим је дала велики допринос у разјашњењу недоумица у тумачењу одређених одредби и тиме додатно допринела даљој хармонизацији. Такође је указано да се начин вршења напада преко интернета технолошки унапредио и попримио много веће размере чиме је доведена у питање даља ефикасност Одлуке у борби са новим изазовима. Пре свега је скренута пажња на све већу злоупотребу ботнета као и на нападе из 2007. године.[6] На нове изазове, где су посебно наведени Конфикер и Стукснет који су се појавили после ступања на снагу Одлуке, Европска унија је одговорила обелодањивањем *Предлога Директиве о нападима против информационих система крајем 2010. године* (у даљем тексту Директива).[7] Циљ Директиве је да се унапреди регулатива предвиђена Одлуком и допуни у складу са новим изазовима али и новом реалношћу. Наиме, 1. децембра 2009. године ступио је на снагу Лисабонски споразум који је у многим сегментима изменио начин функционисања ЕУ. Промене које су се десиле утицале су и на легислативу. Новим споразумом су између осталог укинуте оквирне одлуке. Једини начин да се мења оно што је до тада регулисано оквирним одлукама јесте да се оне дерогирају доношењем директиве о истој материји.

---

[6] Ботнет представља мрежу рачунарских система са којих се напад истовремено врши на један или више рачунарских система. Ове мреже могу да садрже и преко 100.000 рачунарских система. Треба напоменути да се овде не ради о 100.000 људи који учествују у нападу, већ су у питању рачунарски системи заражени вирусом који исте претвара у тзв. „зомбије", а који по наређењу контролног рачунарског система симултано почињу напад на циљни рачунарски систем или више њих.

[7] Конфикер (*Conficker,* такође познат и као *Downup* и *Kido*) представља малициозни програм (компјутерски црв) откривен крајем 2008, који се користећи пропусте Windows оперативног система инфилтрирао у многе рачунарске системе и створио један од тада највећих ботнет-а. Стукснет *(Stuxnet)* такође је комјутерски црв који се слично Конфикеру инфилтрира у рачунарске системе али за разлику од њега бира које ће од њих инфицирати.

Наиме он је програмиран да се активира искључиво на рачунарским системима индустријских постројења и омогућава нападачу да врши саботажу истих.

III) САДРЖАЈ

Оквирна одлука Савета Европске уније

Дефиниције у Одлуци (члан 1)

„Информациони систем" означава било који уређај или групу међусобно повезаних или зависних уређаја од којих један или више њих, у циљу извршења одређеног програма, врши аутоматску обраду рачунарских података; уз њих и рачунарске податке ускладиштене, обрађене, преузете или послате од њих у циљу њиховог рада, употребе, заштите и одржавања.[8]

„Рачунарски податак" означава свако представљање чињеница, информација или концепата у облику који је подесан за обрађивање у информационом систему, укључујући и одговарајући програм на основу кога информациони систем обавља своју функцију.

„Правно лице" означава сваки ентитет који има такав статус у складу са позитивним правом, искључујући државе или друге јавне субјекте са државним овлашћењима, као и међународне организације.

„Неовлашћено" означава приступ или утицај који није дозвољен од стране власника, другог држаоца права на систему или његовом делу, или који није дозвољен националним законодавством.

Незаконит приступ информационом систему (члан 2)

Овим нападом се угрожава поверљивост и приватност информационог система односно података на њему. Напад се најчешће врши применом специјализованих програма који искоришћавају пропусте у заштити информационих система омогућавајући приступ нападачу. Одлуком је предвиђено да намеран неовлашћени приступ информационом систему у целини или његовом делу треба да буде кажњив као кривично дело, бар у случајевима који не представљају дело малог значаја.[9] Уношењем појма

[8] У Конвенцији, с друге стране, користи се термин „Рачунарски систем" који је ужи појам од информационогсистема. Рачунарски ситем обухвата само уређаје који обављају одређене функције, док информациони систем поред уређаја обухвата и саме податке које тај уређај тј. рачунарски систем користи у свом раду.

[9] Оквирна одлука је инструмент ЕУ који је служио за хармонизацију националних законодавстава држава чланица. Обавезна је за све државе чланице у смислу остваривања одређеног циља, али су начин и форма имплементације препуштени самим државама чланицама. Стога се свим члановима Одлуке, државе чланице позивају да предузму неопходне мере у циљу спровођења дате одредбе.

„дело малог значаја" омогућено је државама чланицама да инкриминишу само дела која представљају озбиљнију повреду поверљивости. У Извештају је изнет став да се делом малог значаја сматрају случајеви незаконитог приступа који су од мање важности или кад је повреда поверљивости информационог система мањег степена. Одређене државе чланице су се, према Извештају, ове одредбе погрешно имплементирале јер су својим законодавствима ограничиле тј. сузиле инкриминацију на само одређене случајеве. Тако нпр. Аустрија је предвидела кривичну одговорност само у случајевима кад постоји намера да се врши шпијунажа и да се прибављени подаци користе у циљу остваривања профита или проузроковања штете. Овим је ограничена инкриминација само на ова дела. У свим другим случајевима, без обзира на степен повреде поверљивости информационог система, починилац неће кривично одговарати. Управо ту се отвара простор за изигравање закона путем *forum shopping-a*. Наиме, тада би свако ко би потпао под надлежност аустријског проавосуђа био ослобођен ако његове намере не би могле бити подведене под три наведене. Такође аустријско решење је супротно циљу ове одредбе, а то је да се остави могућност државама чланицама да не инкриминушу само неовлашћене приступе информационом систему где су последице по поверљивост информационог система биле мањег степена или врло малог значаја. Ипак је у ставу 2 овог члана остављена могућност државама чланицама да сузе инкриминацију само на случајеве када је дело извршено нарушавањем заштитних мера.[10] Поново, за разлику од примера са Аустријом, која је инкриминацију ограничила само на она дела која су вршена у одређеном циљу (шпијунажа, профит и штета), овде су инкриминисана сва дела, без обзира на циљ, која су извршена савлађивањем мера заштите. Овим се, сасвим оправдано, искључују из кривично–правне заштите они информациони системи које њихов власник није ни сам покушао да заштити.

Незаконито ометање рада система (члан 3)

Овом одредбом се штите како интереси самог власника информационог система тако и трећих лица, тј. корисника да им информациони систем буде увек доступан. Као најзаступљенији облици вршења овог напада су тзв. дифејсинг (defacing) напади ускраћивањем

[10] У питању су мере као што су постављање заштитног зида (firewall), рачунарских шифри, итд. (прим. аут.)

услуге.[11] У Одлуци је предвиђено да намерно озбиљно ометање или прекидање функционисања информационог система уношењем, преношењем, оштећењем, брисањем, погоршањем, мењањем, прикривањем или чињењем недоступним рачунарских података треба да буде кажњиво као кривично дело ако је почињено неовлашћено, бар у случајевима који не представљају дело малог значаја. Као и у претходном случају настао је проблем у тумачењу „дела малог значаја" приликом имплементације код одређених држава чланица. Према тумачењу Комисије делом малог значаја сматрају се случајеви када је ометање рада информационог система од мањег значаја, или када је интегритет информационог система повређен у мањем степену. Као пример добре имплементације се наводи између осталих и Естонија која је инкриминасала ово дело у случајевима *када је причињена значајна штета*. Као лош пример имплементације је наведена Немачка која је инкриминисала ово дело само онда када је систем који се омета од посебног значаја *за трећа лица*. Разлика је у томе што је у првом случају обухваћена било која радња која изазива значајну штету било коме, док су у другом случају фактички заштићени само јавни и комерцијални информациони системи. Иако је заштита ових информационих система несумњиво била првенствени циљ, ипак се не може сматрати оправданим овакво ограничавање заштите само на њих.

Незаконито манипулисање подацима (члан 4)

Овај вид напада је потенцијално најопаснији јер може да проузрокује највећу штету. Када нападач једном приступи информационом систему, било овлашћено или не, он може подацима са тог система слободно манипулисати. То може да чини непосредно или посредно, уношењем у информациони систем малициозних програма који то аутоматски чине тј. вируса. Према Одлуци, радње намерног брисања, оштећења, погоршања, мењања, прикривања или чињења недоступним рачунарских података треба

[11] Дифејсинг (Defacing) представља напад којим нападач, пошто је неовлашћено приступио информационом систему, неовлашћено мења било само почетну страницу било садржај целог сајта, са садржајем по жељи. Самим тим интернет сајт постаје недоступан трећим лицима. Напади ускраћивањем услуге или Дос (Denial of Service) напади се изводе онеспособљавањем било ресурса (као што су сервери) било сервиса (е-пошта) информационог система, тако што се они оптерећују великим бројем лажних захтева за успостављање везе. Тада систем, услед немогућности да одговори на све постављене захтеве, престаје да буде доступан трећим лицима, односно легитимним корисницима, па чак и самом нападачу. При томе сами подаци информационог система остају нетакнути.

да буду кажњиве као кривично дело ако су извршене неовлашћено, бар у случајевима који не представљају дело малог значаја. Иако ова одредба у опису садржи исте радње као и претходна, разлика је у томе што у претходном случају утицање на податке мора имати за последицу ометање рада информационог система. Овим чланом се штите сами подаци на информационом систему, без обзира на њихов значај за функционисање самог система. Наравно, с обзиром да се исте радње јављају у оба члана, многе државе чланице су ове две одредбе имплементирале у своја законодавства као једну, на шта Комисија није имала примедбе.

Подстрекивање, помагање и покушај (члан 5)

Подстрекивање, помагање и покушај извршења дела предвиђених члановима 2, 3 и 4 свака држава чланица треба да предвиди као кривично дело. Шведска је имплементирала ову одредбу тако што је својим законодавством предвидела да неће бити кажњавани покушај, помагање и подстрекивање извршења дела, ако је у питању дело малог значаја. Према Извештају овај приступ је погрешан и није у складу са захтевима из Одлуке јер у самој одредби нигде није предвиђена таква могућност сужавања инкриминације. С друге стране, остављена је могућност државама чланицама једино да не инкриминишу *покушај* и то искључиво *код дела незаконитог приступа информационом систему*.

Казне и квалификовани облик дела (чланови 6 и 7)

Државама чланицама је препуштено да саме одреде висину и врсту казни за дела из чланова 2, 3, 4 и 5 (у даљем тексту: дела предвиђена Одлуком) при чему те казне треба да буду „ефективне, пропорционалне и превентивне". Међутим, за дела незаконитог ометања информационог система и незаконитог манипулисања подацима, државе чланице треба да предвиде максималне казне затвора у трајању од најмање једне до три године. Квалификовани облик предвиђен је за дела незаконитог приступа информационом систему уз заобилажење заштитних мера, незаконитог ометања информационог система и незаконитог манипулисања подацима у случајевима кад их је извршила *организована криминална група*. За потребе Одлуке се под организованом криминалном групом подразумева *организована група која постоји одређено време и чине је више од две особе које делују споразумно у циљу вршења кривичних дела.*[12] За квалификовани

[12] 98/733/JHA, Article 1, Интернет: http://eurlex.europa.eu/smartapi/cgi/sga_doc? smartapi! celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998F0733&model=guichett.

облик државе чланице треба да предвиде максималну казну затвора у трајању од најмање две до пет година. Такође, државама чланицама је остављена могућност да као квалификовани облик предвиде и сходно казне свако дело које је изазвало значајне штете или је утицало на битне интересе.

Одговорност правних лица и санкције (Чланови 8 и 9)

Предвиђена је обавеза држава чланица да имплементирају у своја законодавства одговорност правних лица за дела предвиђена Одлуком, а која у њихову корист почини свако физичко лице, које делује самостално или као члан органа правног лица, ако има руководећу улогу у правном лицу, а на основу:

а) овлашћења да заступа правно лице;

б) овлашћења да доноси одлуке у име правног лица;

в) овлашћења да врши контролу унутар правног лица.

Даље, правно лице се може сматрати одговорним и у случају када због изостанка надзора или контроле од стране претходно наведеног физичког лица, другом физичком лицу, које поступа по овлашћењу правног лица, буде омогућено да изврши дела предвиђених Одлуком, а у корист правног лица. У сваком случају одговорност правног лица не искључује кривично гоњење физичких лица која учествују у извршењу дела као извршиоци, подстрекачи или саучесници. Државама чланицама је препуштено да саме изаберу санкције које ће предвидети за правна лица, докле год су ефективне, пропорционалне и превентивне. Санкције могу бити било кривичне било некривичне новчане казне, али државе чланице могу да предвиде и друге санкције, као што су:

а) одузимање права на јавне субвенције и помоћ;

б) привремено или трајно одузимање дозволе за рад;

в) стављање под судски надзор;

г) принудна ликвидација правног лица.

Надлежност (члан 10)

Успостављање надлежности у случајевима интернет напада може да буде изузетно компликована због саме природе овог дела. Наиме, починилац, жртва и средство извршења могу се налазити на различитим територијама. Због тога су Одлуком предвиђени критеријуми за успостављање надлежности као и правила у случају сукоба надлежности.

За дела предвиђена Одлуком свака држава чланица ће успоставити своју надлежност ако је дело почињено:

а) у целости или делимично на њеној територији; или

б) од стране њеног држављанина; или

в) у корист правног лица чија се управа налази на територији државе чланице.

Овде треба напоменути да је државама чланицама остављена могућност да не примењују или да примењују само у одређеним случајевима или околностима, правила о јурисдикцији наведена у тачкама б) и в). Из наведеног произилази да су државе чланице увек дужне успоставити своју надлежност кад је дело почињено у целости или делимично на њеној територији. Зато је тај критеријум ближе дефинисан у ставу 2. Наиме, када успоставља своју надлежност у овом случају, свака држава чланица ће осигурати да својом надлежношћу обухвати случајеве у којима:

а) починилац почини дело када је физички присутан на њеној територији, без обзира да ли је дело извршено против информационог система на њеној територији;

б) дело је почињено против информационог система на њеној територији, без обзира да ли је починилац био физички присутан на њеној територији кад је извршио дело.

У случајевима кад је дело починио држављанин државе чланице ван њене територије, предвиђено је да ће тада држава чланица, која према својим законима не изручује своје држављане, предузети неопходне мере да успостави своју надлежност и кад је могуће процесуира дела предвиђена Одлуком. У случају позитивног сукоба надлежности између више држава чланица, државе чланице у питању ће сарађивати у циљу доношења одлуке која ће од њих гонити починиоца, тежећи централизацији поступка у једној држави чланици, ако је то могуће. У овом циљу, предвиђено је да се државе чланице могу обратити било ком телу или механизму Европске уније ради олакшања сарадње између њихових правосудних органа и координације њихових поступака. За одређивање редоследа приоритета могу се користити следећи критеријуми:

– надлежна ће бити држава чланица на чијој територији су дела у целости или делимично почињена;

– надлежна ће бити држава чланица чији је држављанин починилац;

– надлежна ће бити држава чланица у којој је починилац пронађен.

Размена информација (члан 11)

С обзиром да је један од циљева ове одлуке и да се побољша комуникација и размена информација међу релевантним институцијама држава чланица, Одлуком је предвиђено да ће у том циљу државе чланице осигурати да постојећа мрежа оперативних контакт тачки буде доступна 24 часа дневно, седам дана у недељи. Све државе чланице су дужне да обавесте Генерални секретаријат Савета и Комисију о контакт тачки коју су одредиле за размену информација о делима везаним за напад на информационе системе. Потом ће Генерални секретаријат проследити ту информацију другим државама чланицама чиме би требало да се успостави мрежа за размену информација.

Према Извештају државе чланице су у испуњавању ове обавезе највише подбациле. Свега једанаест држава чланица је у потпуности испунило обавезу из овог члана. Овакав поражавајући резултат се врло лоше одражава на ефикасност борбе против интернет напада, јер брза размена информација код оваквих дела је од пресудног значаја.

2. Предлог Директиве о нападима против информационих система

Сама Директива ће начелно задржати постојеће одредбе Одлуке, пре свега кажњавање незаконитог приступа, незаконитог ометања информационог система и незаконитог манипулисања подацима, али ће и укључити неке нове елементе:

– кажњавање употребе алата (као што је злонамерни софтвер – нпр ботнет – или недозвољено прибављање рачунарских шифри) ради извршења кривичних дела;
– увођење „незаконитог прислушкивања" информационог система као кривичног дела;
– унапређење европске кривичне судске/полицијске сарадње кроз: ојачавање постојеће структуре мреже 24/7 тачака за контакт, уводећи обавезу давања одговора у року од осам сати на хитне захтеве;
– увођење обавезе прикупљања основних статистичких података о високотехнолошком криминалу.

Директивом се пооштрава казна за дела интернет напада на најмање две године затвора. Подстицање, помагање и покушај тих дела ће такође бити кажњавани.

Такође подиже се и висина казни за квалификоване облике дела на најмање пет година затвора, а то су дела:

– извршена у оквиру криминалне организације (већ предвиђено Одлуком);
– извршена употребом алата створеног да покрене нападе који утичу на значајан број информационих система или који проузрокују значајну штету у виду поремећаја системских услуга, финансијских трошкова или губитка личних података (није раније било предвиђено Одлуком). Ова одредба има за циљ да се ухвати у коштац са ширењем малициозног софтвера који се сада користи у великој мери да би се вршили најопаснији напади преко интернета;
– извршена прикривањем стварног идентитета извршиоца и стварањем погрешне представе о стварном власнику идентитета (није предвиђено Одлуком).

IV) ДАТУМ СТУПАЊА НА СНАГУ

Одлука је, у складу са чланом 13, ступила на снагу даном објављивања у Службеном листу Европске уније, 16. марта 2005. године. Рок за имплементацију је био 16. март 2007. године. Закључно са 1. јуном 2008. године, пошто је подсетник послат, укупно 20 држава чланица је испунило своју обавезу обавештавања Савета и Комисије о националним одредбама којима су имплементиране обавезе из Одлуке.

V) ИЗВОРИ

• Љиљана Комлен Николић, Радоје Гвозденовић и др., *Сузбијање високотехнолошког криминала,* Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010.
• Council of Europe, Convention on Cybercrime, Интернет: *http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm*, 17. mart 2011.
• Council of European Union, Framework Decision 2005/222/JHA on attacks against information systems, *Official Journal of the EU,* L 69, Интернет: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:L:2005:069:0067:0071:EN:PDF*, 17. mart 2011.
• Report from the Commission to the Council: Based on Article 12 Council Framework Decision of 24 February 2005 on attacks against information systems, COM/2008/0448 final, Интернет: *http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF,* 17. mart 2011.

• Commission staff working document: Impact assessment - accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA, SEC/2010/1122 final, Интернет: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1122:FIN:EN:PDF*, 17. mart. 2011.
• Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM/2010/0517 final – COD/2010/0279, Интернет: *http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463&format=PDF&aged=1&language=EN&guiLanguage=en*, 17. mart. 2011.

VI) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Као потписница Конвенције Република Србија је у Кривичном законику у глави 27 инкриминисала дела против безбедности рачунарских података. Упоредно гледано описи дела из Одлуке могу се подвести под одговарајућа дела предвиђена Закоником: делу из члана 2 Одлуке одговара дело из члана 302 Законика; делу из члана 3 Одлуке одговара дело из члана 303 Законика; делу из члана 4 Одлуке одговара дело из члана 298 Законика. Ипак постоје разлике, пре свега у висини запрећених казни, које су у Одлуци строже и код појма квалификованог облика дела, кад је дело извршила организована криминална група, што нашим законодавством није предвиђено. Такође постоји дискрепанца по питању одговорности правних лица за ова дела. Приликом усаглашавања нашег законодавства са законодавством ЕУ требало би обратити пажњу на примедбе које је комисија изнела у Извештају као и на предлог Директиве који не само да пооштрава казне већ и уводи нова дела. Тиме би Република Србија избегла почетничке грешке имплементације и много спремније би, бар законодавно, ушла у борбу против овог све значајнијег вида компјутерског криминала.