Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo

(COM(2010) 517 galutinis – 2010/0273 (COD))

(2011/C 218/27)

Pagrindinis pranešėjas **Peter MORGAN**

Taryba, vadovaudamasi Sutarties dėl Europos Sąjungos veikimo 114 straipsniu, 2011 m. sausio 20 d. nusprendė pasikonsultuoti su Europos ekonomikos ir socialinių reikalų komitetu dėl

Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo

COM(2010) 517 galutinis – 2010/0273 (COD).

2011 m. vasario 15 d. Europos ekonomikos ir socialinių reikalų komiteto biuras pavedė Transporto, energetikos, infrastruktūros ir informacinės visuomenės skyriui atlikti Komiteto parengiamąjį darbą šiuo klausimu

Europos ekonomikos ir socialinių reikalų komitetas, atsižvelgdamas į tai, kad darbas skubus (Darbo tvarkos taisyklių 59 straipsnis), savo 471-ojoje plenarinėje sesijoje, įvykusioje 2011 m. gegužės 4–5 d. (gegužės 4 d. posėdis), pagrindiniu pranešėju paskyrė Peter Morgan ir priėmė šią nuomonę 173 nariams balsavus už, 1 – prieš ir 7 susilaikius.

1. **Išvados ir rekomendacijos**

1.1 Komitetas palankiai vertina Komisijos komunikatą dėl pasiūlymo priimti Europos Parlamento ir Tarybos direktyvą dėl atakų prieš informacines sistemas. Komitetas, kaip ir Komisija, yra labai susirūpinęs dėl elektroninių nusikaltimų mąsto Europoje ir šio didėjančio grėsmingo reiškinio daromos ir galimos žalos ekonomikai ir piliečių gerovei.

1.2 Komitetas, kaip ir Komisija, yra nusivylęs, kad kol kas tik 17 iš 27 valstybių narių ratifikavo Europos Tarybos konvenciją dėl elektroninių nusikaltimų (Elektroninių nusikaltimų konvenciją) ([1]). Komitetas ragina likusias valstybes nares ([2]) (Austriją, Belgiją, Čekiją, Graikiją, Airiją, Liuksemburgą, Maltą, Lenkiją, Švediją ir Jungtinę Karalystę) kuo skubiau ratifikuoti šią Elektroninių nusikaltimų konvenciją.

1.3 Komitetas pritaria Komisijai, kad reikia skubiai priimti direktyvą, kurioje būtų atnaujintos nusikalstamų veikų, vykdomų rengiant atakas prieš informacines sistemas, apibrėžtys, ir, siekiant efektyviai spręsti šią opią problemą, padidintas ES baudžiamosios teisenos koordinavimas ir bendradarbiavimas.

1.4 Kadangi būtinai reikia priimti specialiai atakoms prieš informacines sistemas skirtą teisės aktą, Komitetas pritaria Komisijos sprendimui politikos priemone pasirinkti direktyvą, kuri būtų papildyta įstatymo galios neturinčiomis priemonėmis, skirtomis šiai konkrečiai elektroninių nusikaltimų rūšiai.

1.5 Tačiau, kaip jau nurodyta ankstesnėje nuomonėje ([3]), EESRK norėtų, kad Komisija paraleliai rengtų visuotinius ES teisės aktus kovai su elektroniniais nusikaltimais. Komitetas mano, kad skaitmeninė darbotvarkė ir strategija „Europa 2020“ bus sėkmingos tik tuo atveju, jeigu bus parengtas visuotinis kovos su elektroniniais nusikaltimais pagrindas ([4]). Šis pagrindas turėtų apimti prevencijos, nustatymo ir švietimo klausimus, taip pat teisėsaugą ir sankcijas.

1.6 EESRK norėtų apsvarstyti Komisijos pasiūlymus dėl visuotinio pagrindo imtis priemonių sprendžiant bendrą interneto saugumo klausimą. Po 10 metų, kai dauguma gyventojų naudosis internetu, didžioji dalis ekonominės ir socialinės veiklos bus priklausoma nuo interneto, sunku patikėti, kad vis dar galėsime pasikliauti esamu įprastiniu ir nestruktūrizuotu požiūriu į naudojimąsi internetu, visų pirma todėl, kad šios veiklos ekonominė vertė bus neapskaičiuojama. Iškils daugybė klausimų, susijusių su kitomis problemomis, pavyzdžiui, asmens duomenų apsauga, privatumu ir elektroniniais nusikaltimais. Skrydžių saugą kontroliuoja centrinė valdžios institucija, nustatanti orlaivių, oro uostų ir oro vežėjų veiklos standartus. Atėjo laikas įsteigti analogišką valdžios instituciją, nustatančią saugių galinių įrenginių (kompiuterių, planšetinių kompiuterių, telefonų), tinklo saugumo, tinklaviečių ir duomenų saugumo standartus. Svarbi apsaugos nuo elektroninių nusikaltimų priemonė – fizinė interneto konfigūracija. ES reikės reguliavimo institucijos, galinčios valdyti internetą.

1.7 Direktyvoje daugiausia dėmesio bus skiriama nusikalstamos veikos apibrėžimui ir gresiančioms sankcijoms. EESRK prašo kartu atkreipti dėmesį į prevenciją taikant veiksmingesnes

([1]) 2001 m. lapkričio 23 d. Budapešte pasirašyta Europos Tarybos konvencija dėl elektroninių nusikaltimų, CETS Nr. 185.

([2]) Žr. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

([3]) EESRK nuomonė dėl saugios informacinės visuomenės, OL C 97, 2007 4 28, p. 21.

([4]) COM(2010)245, COM(2010) 2020.

saugumo priemones. Įrangos gamintojai turėtų laikytis standartų, kad užtikrintų įrenginių saugumą. Tai, kad įrenginių ir galiausiai tinklo saugumas priklauso nuo savininko užgaidų, yra nepriimtina. Reikėtų apsvarstyti europinės elektroninės asmens tapatybės sistemos galimybę, tačiau ji turėtų būti kuriama atsargiai, kad nebūtų pažeidžiamas asmenų privatumas; reikėtų pradėti visiškai išnaudoti IPv6 saugumo galimybes, o gyventojų informavimas apie asmeninį elektroninį saugumą, įskaitant duomenų saugumą, turėtų būti esminė visų skaitmeninio raštingumo programų dalis. Komisija turėtų atsižvelgti į ankstesnes Komiteto nuomones, kuriose buvo nagrinėjami šie klausimai ([5]).

1.8 Komitetas džiaugiasi, kad pasiūlytoje direktyvoje adekvačiai aptariamos atakos prieš informacines sistemas naudojant botnetus (angl. k. *botnet*) ([6]), įskaitant atsisakymo aptarnauti (angl. *denial of service* (DoS)) atakas ([7]). Komitetas taip pat mano, kad direktyva padės valdžios institucijoms kovoti su elektroniniais nusikaltimais, kuriais bandoma pasinaudoti tarptautiniu tinklų susietumu, ir baudžiamojon atsakomybėn patraukti pažeidėjus, kurie bando veikti anonimiškai, ką leidžia padaryti rafinuotos elektroninių nusikaltimų priemonės.

1.9 Komitetas taip pat teigiamai vertina pateiktą nusikalstamos veikos, kuriai taikoma direktyva, sąrašą, pirmiausia tai, kad į tą sąrašą įtrauktas „neteisėtas duomenų perėmimas“ ir aiškiai apibūdintos „nusikaltimams daryti naudojamos priemonės“.

1.10 Tačiau atsižvelgiant į tai, koks svarbus yra pasitikėjimas skaitmenine ekonomika ir jos saugumas, taip pat atsižvelgiant į milžiniškus elektroninių nusikaltimų kasmet padaromus nuostolius ([8]), Komitetas mano, kad direktyvoje sankcijų griežtumas turėtų atspindėti nusikaltimo rimtumą ir būti realia atgrasomąja priemone nusikaltėliams. Siūloma direktyva numato minimalias dvejų ar penkerių metų laisvės atėmimo bausmes (penkerius metus už sunkinančias aplinkybes). EESRK siūlo taikyti sankcijų skalę atsižvelgiant į nusikaltimo sunkumą.

1.11 EESRK siūlo pasinaudoti proga ir nustatyti dar griežtesnes sankcijas, aiškiai parodant nusikaltėliams, kas jų laukia, ir nuraminant piliečius. Pavyzdžiui, Jungtinėje Karalystėje ([9]) už didelio masto atakas prieš informacines sistemas numatomos iki 10 metų laisvės atėmimo bausmės, o Estijoje padidintos nuobaudos ir didelio masto atakos terorizmo tikslais jau gali būti baudžiamos 25 metais laisvės atėmimo ([10]).

1.12 Komitetas teigiamai vertina Komisijos pasiūlymą papildyti direktyvą įstatymo galios neturinčiomis priemonėmis siekiant toliau skatinti veiksmų koordinavimą ES lygmeniu ir efektyviau taikyti priimtas nuostatas. EESRK taip pat pabrėžia, kad reikia išplėsti koordinavimą įtraukiant glaudų bendradarbiavimą su visomis ELPA šalimis ir NATO.

1.13 Komitetas labai pritaria mokymo programoms ir geriausios praktikos sklaidos rekomendacijoms, kuriomis tikimasi padidinti šiuo metu ištisą parą be poilsio dienų veikiančių teisėsaugos institucijų informacinių punktų efektyvumą.

1.14 Be pasiūlyme minimų įstatymo galios neturinčių priemonių Komitetas ragina Komisiją kuriant ankstyvo nustatymo ir reagavimo sistemas, kurios padėtų spręsti informacinių sistemų atakų problemą, atkreipti ypatingą dėmesį į MTTP fondus. Nuotolinių kompiuterinių išteklių paslaugų (angl. k. *cloud computing*) ([11]) ir sudėtinių kompiuterinių tinklų (angl. k. *grid computing*) ([12]) technologijų modernumas Europai gali suteikti geresnę apsaugą nuo daugelio grėsmių.

1.15 Komitetas siūlo, kad, neapsiribojant teisėsaugos priemonėmis, Europos tinklų ir informacijos apsaugos agentūra (ENISA) remtų tikslinę kvalifikacijos kėlimo programą, kurios paskirtis būtų sustiprinti Europos informacinių ir ryšių technologijų saugumo pramonę ([13]).

1.16 Komitetas norėtų pakartoti, kad siekiant geriau apsaugoti Europą nuo elektroninių atakų, svarbu kurti Europos viešąją ir privačią partnerystę atsparumui užtikrinti ir ją integruoti į ENISA ir Europos tarpvyriausybinės kompiuterinių incidentų tyrimo tarnybų grupės (EGC) darbą.

([5]) EESRK nuomonė dėl saugios informacinės visuomenės, OL C 97, 2007 4 28, p. 21. EESRK nuomonė „Interneto tobulinimas“, OL C 175, 2009 7 28, p. 92. EESRK nuomonė „Ypatingos svarbos informacinės infrastruktūros apsauga“, OL C 255, 2010 9 22, p. 98. EESRK nuomonė „Europos skaitmeninė darbotvarkė“, OL C 54, 2011 2 19, p. 58. EESRK nuomonė „Naujasis“ ENISA reglamentas“, dar nepaskelbta Oficialiajame leidinyje. EESRK nuomonė „Skaitmeninio raštingumo didinimas, įgūdžių gerinimas ir įtraukties stiprinimas“, dar nepaskelbta Oficialiajame leidinyje.

([6]) Sąvoka „botnetas“ (angl. k. *botnet*) reiškia kompiuterių, kuriuose įdiegta kenkimo programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams, pavyzdžiui, atakoms prieš informacines sistemas (t. y. kibernetinėms atakoms) rengti. Šie „zombiai“ gali būti kontroliuojami iš kito kompiuterio, dažnai užkrėstų kompiuterių naudotojams apie tai nieko nežinant. Nusikaltėlius susekti labai sunku, nes botnetui priklausantys kompiuteriai, kurie naudojami atakoms rengti, gali būti visai kitoje vietoje nei pats pažeidėjas.

([7]) Atsisakymo aptarnauti (angl. *denial-of-Service* (DoS)) ataka yra ataka, kai kompiuterinis subjektas (pavyzdžiui, tinklavietė arba interneto tarnyba) nebeteikia paslaugų ir tampa neprieinama savo tiksliniams vartotojams. Vartotojams, kurie kreipiasi į tarnybinę stotį arba tinklalapį, nurodoma, kad ši yra „neprieinama“. Dėl tokių atakų, pavyzdžiui, internetinės mokėjimo sistemos gali nebeveikti ir padaryti nuostolių savo vartotojams.

([8]) Kaip rodo 2009 m. atliktas ir Pasaulio ekonomikos forumui pateiktas tyrimas, pasauliniai internetinių nusikaltimų nuostoliai siekia vieną trilijoną dolerių ir sparčiai auga. Žr. tolesnius 2.5 ir 2.7 punktus.

([9]) http://www.legislation.gov.uk/ukpga/2006/48/contents.

([10]) SEC(2010) 1122 galutinis. Komisijos tarnybų darbo dokumentas ir poveikio įvertinimas, pateikiami kartu su pasiūlymu dėl direktyvos dėl atakų prieš informacines sistemas

([11]) **Nuotolinių kompiuterinių išteklių paslaugos** – internetu paprašius arba automatiškai teikiami kompiuteriniai ištekliai. Šios paslaugos vartotojams teikiamos paprastai ir suprantamai ir vartotojai neturi žinoti, kaip tos paslaugos yra teikiamos. Pasinaudojant nuotolinių kompiuterinių išteklių platforma kiekvieną prie interneto prisijungusį Europos vartotoją būtų galima aprūpinti galutiniam vartotojui skirta antivirusine ir interneto saugumo programine įranga.

([12]) **Tinklai** yra paskirstytų skaičiavimo sistemų forma, kai „virtualus superkompiuterį“ sudaro daug į tinklą sujungtų ir laisvai susietų kompiuterių, kurie veikia kartu, kad atliktų labai dideles užduotis. Sudėtinių kompiuterinių tinklų technologijos gali tapti elektroninių atakų analizės ir atsako realiu laiku platforma.

([13]) EESRK nuomonė dėl naujojo Europos tinklų ir informacijos apsaugos agentūros (ENISA) reglamento, dar nepaskelbta Oficialiajame leidinyje OL C 107, 2011 4 6, p. 58.

1.17 Europoje turėtų būti skatinama stipri informacijos saugumo pramonė, kad būtų galima konkuruoti su labai gerai finansuojama JAV pramone ([14]). Reikėtų daug daugiau investuoti į elektroninei apsaugai skirtus mokslinius tyrimus, technologijų plėtrą ir švietimą.

1.18 Komitetas atkreipia dėmesį į Jungtinei Karalystei, Airijai ir Danijai pagal Sutarties protokolus suteiktas išimtis netaikyti siūlomos direktyvos. Nepaisant išimčių, Komitetas ragina šias valstybes nares kiek galima labiau bendradarbiauti įgyvendinant direktyvos nuostatas, kad nusikaltėliams būtų užkirstas kelias pasinaudoti politikos spragomis ES.

2. **Įžanga**

2.1 Kurdama savo piliečių gerovę ir užtikrindama gyvenimo kokybę Europa jau dabar yra labai priklausoma nuo informacinių sistemų. Svarbu, kad mūsų didėjanti priklausomybė būtų derinama su vis rafinuotesnėmis saugumo priemonėmis ir griežtais įstatymais informacinėms sistemoms nuo atakų apsaugoti.

2.2 Internetas yra skaitmeninės visuomenės pagrindas. Skaitmeninės visuomenės ir skaitmeninės ekonomikos vystymuisi ypač svarbu užkirsti kelią pavojams informacinių sistemų saugumui. Internetu remiasi didžioji dalis Europos ypatingos svarbos informacinės infrastruktūros – būtiniausių prekių ir paslaugų tiekimo informacijos ir komunikacijos platformos. Išpuoliai prieš informacines sistemas – vyriausybės sistemas, finansų sistemas, socialines paslaugas ir ypatingos svarbos infrastruktūros sistemas, pavyzdžiui, elektros energijos tiekimo, vandentiekio, transporto, sveikatos ir skubios pagalbos paslaugas teikiančius subjektus – tapo didele problema.

2.3 Interneto infrastruktūrą sudaro milijonai tarpusavyje susijusių kompiuterių, kurie apdoroja, perduoda ir kontroliuoja duomenis visame pasaulyje. Ši decentralizuota architektūra sudaro interneto stabilumo ir atsparumo pagrindą ir iškilus problemoms padeda greitai atstatyti interneto ryšio tiekimą. Vis dėlto tai taip pat reiškia, kad didelio masto elektronines atakas gali surengti bet kas turintis tokių kėslų ir elementarių žinių iš bet kurios atokiausios tinklo vietos, pasinaudojęs, pavyzdžiui, botnetais.

2.4 Dėl informacinių technologijų raidos tokių problemų dar pagausėjo, nes vis lengviau kuriamos ir platinamos priemonės (kenksminga programinė įranga ([15]) ir botnetai), pažeidėjai gali išlikti anonimiški, o atsakomybės klausimus spręsti priklauso skirtingoms valstybėms. Dėl sunkumų baudžiamojo persekiojimo srityje organizuoti nusikaltėliai gali gauti daug naudos mažai rizikuodami.

2.5 Kaip rodo 2009 m. atliktas ir Pasaulio ekonomikos forumui pateiktas tyrimas ([16]), pasauliniai internetinių nusikaltimų nuostoliai siekia vieną trilijoną dolerių ir sparčiai auga. Neseniai Jungtinės Karalystės vyriausybės ataskaitoje ([17]) buvo nurodyta, kad vien Jungtinėje Karalystėje tokie nusikaltimai kainuoja 27 milijardus svarų. Didelė internetinių nusikaltimų kaina verčia imtis griežtų veiksmų, griežtai taikyti dideles nuobaudas pažeidėjams.

2.6 Kaip teigiama Komisijos tarnybų darbo dokumente, kuris pridedamas prie pasiūlymo priimti direktyvą ([18]), organizuoti nusikaltėliai ir priešiškų valstybių vyriausybės naudojasi destruktyviomis atakų prieš informacines sistemas ES galimybėmis. Tokių botnetų atakos gali būti labai pavojingos visai nukentėjusiai šaliai, jomis teroristai ir kiti asmenys gali naudotis kaip priemone daryti politinį spaudimą valstybei.

2.7 Išpuolis prieš Estiją 2007 m. balandžio–gegužės mėnesiais atkreipė dėmesį į šią problemą. Po atakos iš rikiuotės išėjo nemaža ypatingos svarbos informacinės infrastruktūros dalis valstybės ir privačiame sektoriuje. Dėl didelio atakų masto suirutė tęsėsi keletą dienų ir padarė nuostolių už 19–28 milijonus eurų, taip pat ir nemažą politinę žalą. Panašios destruktyvios atakos surengtos prieš Lietuvą ir Gruziją.

2.8 Pasauliniai komunikaciniai tinklai pasižymi nemažu tarpvalstybiniu susietumu. Labai svarbu, kad visos 27 ES valstybės narės kartu imtųsi vienodų veiksmų kovoti su elektroniniu nusikalstamumu ir ypač atakomis prieš informacines sistemas. Ši tarptautinė tarpusavio priklausomybė verčia ES ieškoti kompleksiškos politikos, skirtos apsaugoti informacines sistemas nuo atakų ir nubausti pažeidėjus.

2.9 Savo 2007 m. nuomonėje dėl saugios informacinės visuomenės strategijos ([19]) Komitetas pareiškė, kad reikėtų visuotinių ES teisės aktų kovai su elektroniniais nusikaltimais. Toks visuotinis teisinis pagrindas turėtų apimti ne tik atakas prieš informacines sistemas, bet ir finansinius elektroninius nusikaltimus, neteisėtą interneto turinį, elektroninių įrodymų rinkimą, saugojimą, perkėlimą ir išsamesnes nuostatas dėl jurisdikcijos.

2.10 Komitetas pripažįsta, kad parengti visuotinį teisinį pagrindą yra labai sunki užduotis, kurią dar labiau apsunkina politinio konsensuso trūkumas ([20]) ir pakankamai skirtingos valstybių narių nuostatos dėl elektroninių įrodymų tinkamumo teismuose. Tačiau toks visuotinis teisinis pagrindas maksimaliai

([14]) Oficialūs Baltųjų rūmų duomenys rodo, kad JAV vyriausybė elektroninio saugumo tyrimams, technologijų plėtrai ir švietimui šioje srityje 2010 m. išleido 407 milijonus dolerių ir siūlo 2012 m. tam skirti 548 milijonus dolerių. http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([15]) Kenksminga programinė įranga (angl. *„malware“* - *„malicious software“* sutrumpinimas) yra programinė įranga, kuri naudojama slapta, be informuoto savininko sutikimo įsibraunant į kompiuterinę sistemą.

([16]) Tyrimą „Neapsaugota ekonomika: gyvybiškai svarbios informacijos apsauga“ (*„Unsecured Economies: Protecting Vital Information“*) „McAfee“ bendrovei atliko Perdju universiteto informacijos apsaugos mokslo ir tyrimų centro mokslininkai (2009 m.), http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf

([17]) http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.

([18]) SEC(2010) 1122

([19]) EESRK nuomonė dėl saugios informacinės visuomenės, OL C 97, 2007 4 28, p. 21 (TEN/254).

([20]) SEC(2010) 1122, COM(2010) 517 poveikio vertinimas.

padidintų įstatymo galią turinčių ir neturinčių priemonių naudingumą sprendžiant įvairiausias elektroninių nusikaltimų problemas. Tai taip pat leistų išspręsti baudžiamosios teisės sistemos klausimus ir tuo pat metu pagerintų teisėsaugos bendradarbiavimą ES. Komitetas ragina Komisiją ir toliau siekti tikslo sukurti visuotinį teisinį pagrindą elektroniniams nusikaltimams.

2.11 Kovoti su elektroniniais nusikaltimais reikia specialių gebėjimų. Komiteto nuomonėje dėl siūlomo ENISA reglamento ([21]) buvo atkreiptas dėmesys į tai, kaip svarbu paruošti teisėsaugos pareigūnus. Komitetas teigiamai vertina faktą, kad Komisija daro pažangą kurdama mokymų kovoti su elektroniniais nusikaltimais platformą teisėsaugai ir privačiam sektoriui, kaip pasiūlyta 2007 m. komunikate COM (2007) 267 ([22]).

2.12 Kibernetinis saugumas aktualus visiems ES piliečiams, kurių gyvenimas gali priklausyti nuo ypatingos svarbos paslaugų. Patys piliečiai turi stengtis kiek galima geriau apsaugoti savo interneto ryšį nuo atakų. Dar didesnė atsakomybė turi tekti informacinių ir ryšių technologijų ir paslaugų, sudarančių informacines sistemas, teikėjams.

2.13 Ypač svarbu, kad visi suinteresuotieji subjektai būtų tinkamai informuojami apie kibernetinį saugumą. Taip pat svarbu, kad Europa turėtų pakankamai kompetentingų ekspertų elektroninio saugumo srityje.

2.14 Europoje turėtų būti skatinama stipri informacijos saugumo pramonė, kad būtų galima konkuruoti su labai gerai finansuojama JAV pramone ([23]). Reikėtų daug daugiau investuoti į elektroninei apsaugai skirtus mokslinius tyrimus, technologijų plėtrą ir švietimą.

3. **Svarbiausios direktyvos projekto nuostatos**

3.1 Šio pasiūlymo tikslas – pakeisti 2005 m. vasario 24 d. Tarybos pamatinį sprendimą 2005/222/TVR dėl atakų prieš informacines sistemas ([24]). Kaip nurodyta šio pamatinio sprendimo konstatuojamosiose dalyse, sprendimu siekta gerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policijos ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą derinant valstybių narių baudžiamosios teisės nuostatas atakų prieš informacines sistemas srityje. Pradėti taikyti ES teisės aktai, skirti kovoti su tokiais nusikaltimais, kaip neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemą ir neteisėtas įsikišimas į duomenis, taip pat nustatytos specialios taisyklės dėl juridinių asmenų atsakomybės, jurisdikcijos ir keitimosi informacija. Valstybių narių reikalauta imtis būtinų priemonių, kad iki 2007 m. kovo 16 d. būtų pradėta laikytis šio pamatinio sprendimo nuostatų.

3.2 2008 m. liepos 14 d. Komisija paskelbė Pamatinio sprendimo įgyvendinimo ataskaitą ([25]). Išvadose buvo pasakyta, kad „po to, kai priimtas Sprendimas, visoje Europoje įvykdytos atakos parodė, kad kyla naujų pavojų: vienu metu įvykdytos itin didelio masto atakos prieš informacines sistemas ir padidėjo vadinamųjų botnetų naudojimas nusikalstamiems tikslams“. Priimant pamatinį sprendimą šioms atakoms nebuvo skirta daug dėmesio.

3.3 Šiame pasiūlyme atsižvelgiama į naujus elektroninių nusikaltimų metodus, visų pirma botnetų panaudojimą ([26]). Pažeidėjus susekti labai sunku, nes botnetui priklausantys kompiuteriai, naudojami atakoms rengti, gali būti visai kitoje vietoje nei pats pažeidėjas.

3.4 Botneto atakos dažnai būna didelio masto. Didelio masto atakos yra tokios atakos, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala, pavyzdžiui, dėl sutrikusių sistemos paslaugų, finansinių nuostolių, prarastų asmens duomenų ir t. t. Didelio masto atakų padaryta žala daro didelį poveikį pačiam taikinio darbui ir (arba) paveikia jo darbo aplinką. Šiame kontekste „didelis botnetas“ yra tinklas, galintis padaryti didelę žalą. Sunku nustatyti botnetų dydį, tačiau apskaičiuota, kad prisijungimų prie didžiausių nustatytų botnetų (t. y. užkrėstų kompiuterių) skaičius buvo nuo 40 000 iki 100 000 per 24 valandas ([27]).

3.5 Pamatiniame sprendime yra keletas trūkumų, nes pažeidimų (kibernetinių atakų) mastas ir skaičius kinta. Sprendimu suderinamos tik ribotą skaičių nusikalstamų veikų reglamentuojančios nuostatos, tačiau nėra visapusiškai sprendžiama didelio masto atakų visuomenei keliamos potencialios grėsmės problema. Sprendime neatsižvelgiama į nusikaltimų sunkumą ir už juos taikomas sankcijas.

3.6 Šios direktyvos tikslas yra suderinti valstybių narių baudžiamosios teisės nuostatas atakų prieš informacines sistemas srityje ir pagerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policiją ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą.

([21]) EESRK nuomonė dėl naujojo Europos tinklų ir informacijos apsaugos agentūros (ENISA) reglamento, dar nepaskelbta Oficialiajame leidinyje (OL C 107, 2011 4 6, p. 58).

([22]) COM(2007) 267 „Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme“.

([23]) Oficialūs Baltųjų rūmų duomenys rodo, kad JAV vyriausybė elektroninio saugumo tyrimams, technologijų plėtrai ir švietimui šioje srityje 2010 m. išleido 407 milijonus dolerių ir siūlo 2012 m. tam skirti 548 milijonus dolerių. http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([24]) OL L 69, 2005 3 16, p. 68.

([25]) Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas, COM (2008) 448, 12 straipsnį.

([26]) Žr. 6 išnašą.

([27]) Prisijungimų skaičius per 24 valandas yra dažnai naudojamas matavimo vienetas botneto dydžiui nustatyti.

3.7 Atakų prieš informacines sistemas grėsmė didėja, ypač dėl organizuoto nusikalstamumo, todėl vis didesnį susirūpinimą kelia galimi teroristų išpuoliai ar atakos dėl politinių motyvų prieš informacines sistemas, kurios yra valstybių narių ir Sąjungos ypatingos svarbos infrastruktūros dalis. Kyla grėsmė, kad nebus sukurta saugesnė informacinė visuomenė ir laisvės, saugumo bei teisingumo erdvė, todėl reikia imtis Europos Sąjungos lygmens veiksmų.

3.8 Akivaizdu, kad daugėja pavojingų ir pakartotinių didelio masto atakų prieš informacines sistemas, kurios yra ypatingai svarbios valstybėms arba konkrečioms viešojo ar privataus sektoriaus funkcijoms. Be šios tendencijos taip pat pastebėta, kad kuriamos vis modernesnės priemonės, kurias nusikaltėliai gali naudoti įvairaus pobūdžio elektroninėms atakoms rengti.

3.9 Šioje srityje bendros, ypač informacinių sistemų ir kompiuterinių duomenų, sąvokų apibrėžtys yra svarbios, kad valstybėse narėse būtų užtikrintas nuoseklus šios direktyvos taikymas.

3.10 Reikia susitarti dėl bendro požiūrio į nusikalstamos veikos sudėties požymius numatant, kad neteisėta prieiga prie informacinės sistemos, neteisėtas įsikišimas į sistemą, neteisėtas įsikišimas į duomenis ir neteisėtas duomenų perėmimas yra bendrai laikomi nusikalstama veika.

3.11 Valstybės narės turėtų nustatyti sankcijas už atakas prieš informacines sistemas. Nustatytos sankcijos turėtų būti veiksmingos, proporcingos ir atgrasančios.

3.12 Direktyvoje, kuria panaikinamas pamatinis sprendimas 2005/222/TVR, išliks šio sprendimo nuostatos ir bus įtraukti šie nauji elementai:

(a) reglamentuojamos sankcijos už nusikalstamai veikai daryti naudojamų įrenginių ir (arba) priemonių gamybą, pardavimą, įsigijimą naudojimuisi, importą, platinimą arba galimybių jais naudotis sudarymą kitu būdu;

(b) įtraukiamos nuostatos dėl sunkinančių aplinkybių:

— didelio masto atakų rengimo, botnetų ar panašių priemonių naudojimo problema būtų sprendžiama įtraukiant naujas nuostatas dėl sunkinančių aplinkybių, t. y. botneto kūrimas arba panašių priemonių naudojimas darant pamatiniame sprendime išvardytus nusikaltimus būtų laikomas sunkinančia aplinkybe,

— kai tokios atakos rengiamos slepiant tikrąją pažeidėjo tapatybę ir daroma žala teisėtam tapatybės turėtojui;

(c) įtraukiamos nuostatos, pagal kurias neteisėtas duomenų perėmimas laikomas nusikalstama veika;

(d) nustatomos priemonės bendradarbiavimui baudžiamosios teisenos srityje gerinti stiprinant ištisą parą be poilsio dienų veikiančių informacinių punktų struktūrą ([28]);

(e) reaguojama į būtinybę parengti statistinius duomenis apie elektroninius nusikaltimus, įskaitant nusikaltimus, kurie minimi galiojančiame pamatiniame sprendime ir naujai įvestą „neteisėtas duomenų perėmimą“;

(f) šioje direktyvoje pateiktos 3, 4 ir 5 straipsniuose išvardytų nusikalstamų veikų (neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemas ir neteisėtas įsikišimas) apibrėžtys, į kurias įtraukta nuostata, pagal kurią perkeliant direktyvą į nacionalinę teisę kaip už nusikalstamą veiką leidžiama bausti tik „tais atvejais, kurie nėra nereikšmingi“.

2011 m. gegužės 4 d., Briuselis

Europos ekonomikos ir socialinių reikalų komiteto pirmininkas

Staffan NILSSON

([28]) Informaciniai punktai sukurti Konvencija ir pamatiniu sprendimu 2005/222/TVR dėl atakų prieš informacines sistemas.