Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Priekšlikums Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām, un ar ko atceļ Padomes Pamatlēmumu 2005/222/TI"

COM(2010) 517 galīgā redakcija – 2010/0273 (COD)

(2011/C 218/27)

Galvenais ziņotājs: ***MORGAN* kgs**

Eiropas Savienības Padome 2011. gada 20. janvārī saskaņā ar Līguma par Eiropas Savienības darbību 114. pantu nolēma konsultēties ar Eiropas Ekonomikas un sociālo lietu komiteju par tematu

"*Priekšlikums Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām, un ar ko atceļ Padomes Pamatlēmumu 2005/222/TI*"

COM(2010) 517 galīgā redakcija – 2010/0273 (COD).

Eiropas Ekonomikas un sociālo lietu komitejas Birojs 2011. gada 15. februārī uzdeva Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētajai nodaļai sagatavot Komitejas atzinumu par šo jautājumu.

Ņemot vērā jautājuma steidzamību (saskaņā ar Reglamenta 59. pantu), Eiropas Ekonomikas un sociālo lietu komiteja 471. plenārajā sesijā, kas notika 2011. gada 4. un 5. maijā (4. maija sēdē), iecēla *Morgan* kgu par galveno ziņotāju un ar 173 balsīm par, 1 balsi pret un 7 atturoties, pieņēma šo atzinumu.

1. **Secinājumi un ieteikumi**

1.1 Komiteja atzinīgi vērtē Komisijas priekšlikumu Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām. Komiteja pievienojas Komisijas bažām par Eiropas kibernoziegumu plašo mērogu un kibernoziegumu pieaugošo draudu reālo vai iespējamo kaitējumu ekonomikai un iedzīvotāju labklājībai.

1.2 Tāpat kā Komisija, arī Komiteja izsaka nožēlu par to, ka līdz šim brīdim tikai 17 no 27 dalībvalstīm ir ratificējušas Eiropas Padomes konvenciju par kibernoziegumiem ("Kibernoziedzības konvenciju" [1]). Komiteja aicina arī pārējās dalībvalstis [2] — Austriju, Beļģiju, Čehiju, Grieķiju, Īriju, Luksemburgu, Maltu, Poliju, Zviedriju un Apvienoto Karalisti — cik drīz vien iespējams ratificēt Kibernoziedzības konvenciju.

1.3 Komiteja piekrīt Komisijai, ka efektīvam minētās būtiskās problēmas risinājumam ir steidzami jāpieņem direktīva, lai atjauninātu definīciju nodarījumiem, kas saistīti ar uzbrukumiem informācijas sistēmām, un lai uzlabotu ES koordināciju un sadarbību krimināltiesību jomā.

1.4 Lai tieši risinātu jautājumus, kas saistīti ar uzbrukumiem informācijas sistēmām, steidzami vajadzīgi jauni tiesību akti, tāpēc Komiteja atbalsta Komisijas lēmumu izstrādāt direktīvu, papildus nosakot neleģislatīvus pasākumus, kas vērsti konkrēti uz minēto kibernoziegumu veidu.

1.5 Tomēr EESK atkārto jau agrāk izstrādātā atzinumā [3] pausto aicinājumu Komisijai vienlaikus turpināt izstrādāt visaptverošu ES tiesisko regulējumu kibernoziedzības apkarošanai. Komiteja uzskata, ka visaptverošs regulējums ir būtiski svarīgs Digitālās programmas un stratēģijas "Eiropa 2020" [4] veiksmīgai īstenošanai. Visaptverošajam regulējumam jāaptver ne vien tiesībaizsardzības un sodīšanas, bet arī prevencijas, atklāšanas un izglītības jautājumi.

1.6 EESK vēlētos, lai Komisija drīzumā nāktu klajā ar priekšlikumiem visaptverošam rīcības plānam, kurā risināts vispārējais jautājums par drošību internetā. Pēc desmit gadiem lielākā daļa iedzīvotāju lietos internetu un saimnieciskā darbība un sabiedriskā dzīve būs lielā mērā atkarīga no interneta. Nav iedomājams, ka arī tad varēs turpināt pret interneta lietošanu izturēties tikpat pavirši un nestrukturēti kā šobrīd, jo īpaši tādēļ, ka interneta lietošanas ekonomiskā vērtība būs neiedomājami augsta. Aktualizēsies daudz dažādu jautājumu, un to vidū bez kibernoziedzības būs arī citas problēmas, piemēram, personas datu drošība un privātās dzīves aizsardzība. Pašlaik aviolīniju drošību kontrolē centrālā iestāde, kas izdod noteikumus par gaisa kuģiem, lidostām un aviosabiedrībām. Vajadzētu izveidot līdzīgu iestādi, kas noteiktu standartus attiecībā uz galiekārtu (personālo datoru, planšetdatoru, tālruņu) drošumu un tīklu, tīmekļa vietņu un datu drošību. Galvenais faktors, no kā atkarīga aizsardzība pret kibernoziegumiem, ir interneta fiziskā konfigurācija. Eiropas Savienībai būs vajadzīgs pilnvarots regulators interneta jomā.

1.7 Direktīvas priekšlikumā galvenā uzmanība pievērsta noziedzīgu nodarījumu definēšanai un iespējamām soda sankcijām. EESK aicina vienlaikus koncentrēties arī uz novēršanu,

---

([1]) Eiropas Padomes konvencija par kibernoziegumiem, Budapešta, 23.11.2001, *CETS* Nr. 185.

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

([3]) EESK atzinums par tematu "Drošas informācijas sabiedrība", OV C 97, 28.04.2007, 21. lpp.;

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

uzlabojot drošības pasākumus. Iekārtu ražotājiem ir jānodrošina ierīču atbilstība drošuma standartiem. Nav pieļaujams, ka ierīču drošums un tādējādi arī tīkla drošība ir atkarīga no ierīču īpašnieku izvēles. Jāapsver Eiropas elektroniskās identifikācijas sistēmas ieviešana, tomēr minētā sistēma būtu jāveido uzmanīgi, lai nepieļautu, ka tiek pārkāpts personu privātums. Jāsāk pilnībā izmantot drošības iespējas, ko sniedz interneta protokola 6. versija (*IPv6*), un par neatņemamu digitālo prasmju mācību programmu daļu jākļūst apmācībai personīgajā kiberdrošībā, tostarp datu drošībā. Komitejai vajadzētu ņemt vērā Komitejas iepriekšējos atzinumus, kuros iztirzāti minētie jautājumi ([5]).

1.8 Komiteja ir gandarīta, ka ierosinātā direktīva pienācīgi aptver uzbrukumus informācijas sistēmām, kuros izmanto robottīklus ([6]), tostarp arī pakalpojuma atteikuma uzbrukumus ([7]). Komiteja arī uzskata, ka direktīva palīdzēs iestādēm veikt kriminālvajāšanu par kibernoziegumiem ar mērķi izmantot tīklu starptautiskos savienojumus, kā arī saukt pie atbildības noziegumu izdarītājus, kuri cenšas izmantot anonimitāti, ko iespējams nodrošināt ar augstu attīstītiem kibernoziegumu izdarīšanas rīkiem.

1.9 Komiteja atzinīgi vērtē direktīvā ietverto noziedzīgu nodarījumu sarakstu, īpaši to, ka iekļauta "nelikumīga pārtveršana", kā arī to, ka precizēti noteikumi par "noziedzīgu nodarījumu izdarīšanas rīkiem".

1.10 Tomēr, ņemot vērā to, ka digitālajā ekonomikā liela nozīme ir uzticamībai un drošībai, un ievērojot arī ārkārtīgi lielos zaudējumus, ko ik gadu rada kibernoziegumi ([8]), Komiteja uzskata, ka direktīvas priekšlikumā ierosināto sodu apmēriem ir jāatspoguļo noziegumu smagums un sodiem jābūt tik stingriem, lai tie patiešām atturētu no noziegumu izdarīšanas. Direktīvas priekšlikumā ierosināts par minimālo sodu noteikt brīvības atņemšanu uz diviem gadiem vai — atbildību pastiprinošos apstākļos — uz pieciem gadiem. EESK ierosina sodu smagumu samērot ar pastrādāto noziegumu smagumu.

1.11 EESK ierosina noteikt stingrākus sodus, lai izmantotu iespēju dot skaidru vēstījumu gan noziedzniekiem, gan iedzīvotājiem, kuriem nepieciešama papildus drošības sajūta. Piemēram, Apvienotajā Karalistē ([9]) noteikti sodi līdz 10 gadiem par plaša mēroga uzbrukumiem informācijas sistēmām, savukārt Igaunija ir noteikusi stingrākus sodus, par plaša mēroga uzbrukumu veikšanu terorisma nolūkos paredzot brīvības atņemšanu līdz pat 25 gadiem ([10]).

1.12 Komiteja atzinīgi vērtē Komisijas ierosinājumu papildus direktīvai noteikt arī neleģislatīvus pasākumus, lai vēl vairāk veicinātu koordinētu sadarbību ES līmenī un efektīvāku piemērošanu. EESK uzsver, ka minēto sadarbību vajadzētu paplašināt, cieši sadarbojoties arī ar visām Eiropas Brīvās tirdzniecības asociācijas valstīm un ar NATO.

1.13 Komiteja atbalsta ieteikumus par apmācības programmām un paraugpraksi, lai palielinātu tiesībaizsardzības iestāžu pastāvošo 24/7 kontaktpunktu efektivitāti.

1.14 Komiteja aicina Komisiju papildus priekšlikumā minētajiem neleģislatīvajiem pasākumiem piešķirt pētniecībai un izstrādei paredzētos līdzekļus īpaši tam, lai izstrādātu agrīnas diagnosticēšanas un reaģēšanas sistēmas, ar kurām novērst uzbrukumus informācijas sistēmām. Jaunākās tehnoloģijas mākoņdatošanas ([11]) un režģiskās skaitļošanas ([12]) jomās sniedz iespējas daudz labāk aizsargāt Eiropu no daudziem draudiem.

1.15 Komiteja ierosina Eiropas Tīkla un informācijas drošības aģentūrai (*ENISA*) finansēt prasmju veidošanas programmu, lai Eiropas informācijas un komunikācijas tehnoloģiju drošības nozari stiprinātu arī ar citiem, ne tikai ar tiesībaizsardzības līdzekļiem ([13]).

1.16 Komiteja atkārtoti uzsver: lai stiprinātu Eiropas aizsardzības mehānismu pret kiberuzbrukumiem, ir ļoti svarīgi veidot Eiropas publiskā un privātā sektora partnerību infrastruktūru noturības jautājumos (*EP3R*) un saskaņot tās darbību ar darbu, ko veic Eiropas Tīkla un informācijas drošības aģentūra un Eiropas Valdību reaģēšanas grupa datorapdraudējumu gadījumos.

([5]) EESK atzinums par tematu "Drošas informācijas sabiedrība", OV C 97, 28.04.2007., 21. lpp.; EESK atzinums par tematu "Interneta modernizācija", OV C 175, 28.07.2009., 92. lpp.; EESK atzinums par tematu "Informācijas kritiskās infrastruktūras aizsardzība", OV C 255, 22.09.2010., 98. lpp.; EESK atzinums par tematu "Digitālā programma Eiropai", OV C 54, 19.02.2011., 58. lpp.; EESK atzinums par regulu, kas attiecas uz Eiropas Tīklu un informācijas drošības aģentūru, vēl nav publicēts Oficiālajā Vēstnesī; EESK atzinums par tematu "Digitālo prasmju, iemaņu un iekļautības uzlabošana", vēl nav publicēts Oficiālajā Vēstnesī.

([6]) Ar terminu "robottīkls" apzīmē ar destruktīvu programmatūru (datorvīrusu) inficētu datoru kopumu. Šādam inficētu datoru ("spoku") kopumam var likt veikt īpašas darbības, piemēram uzbrukt informācijas sistēmām (kiberuzbrukumi). Šos "spokus" var kontrolēt kāds cits dators, bieži vien bez inficēto datoru lietotāju ziņas. Ir grūti izsekot nodarījuma izdarītājus, jo datori, kas veido robottīklu un veic uzbrukumu, un nodarījuma izdarītājs var atrasties dažādās vietās.

([7]) Pakalpojumu atteikuma uzbrukums ir uzbrukums ar mērķi padarīt datorresursu (piemēram, tīmekļa vietni vai interneta pakalpojumu) nepieejamu lietotājiem, kam tas paredzēts. Kad lietotāji mēģina piekļūt attiecīgajam serverim vai tīmekļa vietnei, viņi saņem paziņojumu, ka pakalpojums nav pieejams. Minētā veida uzbrukumi var padarīt lietošanai nederīgas, piemēram, tiešsaistes maksājumu sistēmas, radot zaudējumus to lietotājiem.

([8]) Saskaņā ar 2009. gadā veikto pētījumu, ar ko iepazīstināja Pasaules ekonomikas forumā, kibernoziegumi pasaulē radījuši aptuveni vienu triljonu ASV dolāru lielus zaudējumus, un šī summa turpina strauji augt. Sk. 2.5. un 2.7. punktus.

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

([10]) *SEC(2010)1122 final* — Komisijas dienestu darba dokuments un ietekmes novērtējums, kas pievienots direktīvas projektam par uzbrukumiem informācijas sistēmām.

([11]) **Mākoņdatošana** ir datorresursu nodrošināšana internetā — pēc pieprasījuma vai automātiski. "Mākoņpakalpojumi" ir pieejami lietotājiem vienkāršā un saprotamā veidā, un viņi tos var izmantot, neiedziļinoties pakalpojumu darbības specifikā. Ikvienam lietotājam Eiropā ar "mākoņplatformas" starpniecību varētu nodrošināt tiešajiem lietotājiem paredzētas jaunākās pretvīrusu un interneta drošības programmas, tādējādi mazinot lietotāju vajadzību pašiem rūpēties par drošību.

([12]) **Režģiskā skaitļošana** ir dalītās skaitļošanas veids, daudziem tīklā savienotiem un vāji saistītiem datoriem kopīgi veicot ļoti liela apjoma uzdevumu un tādējādi veidojot vienu "virtuālo superdatoru". Ar režģiskās skaitļošanas tehnoloģijas starpniecību varētu reālajā laikā analizēt kiberuzbrukumus un nodrošināt reaģēšanas sistēmas.

([13]) EESK atzinums par regulu, kas attiecas uz Eiropas Tīklu un informācijas drošības aģentūru *ENISA*, OV C 107, 6.04.2007, 58. lpp.

1.17 Eiropā jāveido spēcīga informācijas drošības nozare, kas atbilstu tam kompetences līmenim, kāds raksturīgs šai nozarei ASV, kur tā saņem ļoti labu finansējumu ([14]). Ievērojami jāpalielina ieguldījumi kiberdrošības jomas pētniecībā, izstrādē un izglītībā.

1.18 Komiteja norāda, ka Līguma Protokolos noteikti izņēmumi attiecībā uz Apvienoto Karalisti, Īriju un Dāniju, kurām nebūs jāīsteno direktīvas noteikumi. Neatkarīgi no izņēmumiem, Komiteja aicina attiecīgās dalībvalstis tomēr sadarboties un cik vien iespējams ievērot direktīvas noteikumus, lai nepieļautu, ka noziedznieki ļaunprātīgi izmanto Eiropas Savienības valstu politiskās atšķirības.

2. **Ievads**

2.1 Labklājības un dzīves kvalitātes nodrošināšanā Eiropa pašlaik ir lielā mērā atkarīga no informācijas sistēmām. Ir svarīgi, palielinoties mūsu atkarībai, arvien vairāk attīstīt arī drošības pasākumus un tiesību aktus, lai aizsargātu informācijas sistēmas no uzbrukumiem.

2.2 Internets ir digitālās sabiedrības galvenā platforma. Digitālās sabiedrības un digitālās ekonomikas attīstībai ir ārkārtīgi svarīgi novērst draudus informācijas sistēmu drošībai. Internetu izmanto lielākajai daļai Eiropas īpaši svarīgas informācijas infrastruktūras: tas ir pamatā informācijas un sakaru platformām, ko lieto pirmās nepieciešamības preču un pakalpojumu nodrošināšanai. Par ievērojamu problēmu kļuvuši uzbrukumi informācijas sistēmām — pārvaldes sistēmām, finanšu sistēmām, sociālo pakalpojumu sistēmām un īpaši svarīgām infrastruktūras sistēmām, piemēram, energoapgādes, ūdensapgādes, transporta, veselības aizsardzības un avārijas dienestu sistēmām.

2.3 Interneta arhitektūras pamatā ir miljoniem savienotu datoru un globāls datu apstrādes, sakaru un kontroles funkciju dalījums. Šī dalītā arhitektūra ir galvenais faktors, kas nodrošina interneta stabilitāti un elastīgumu, problēmu gadījumā ļaujot ātri atjaunot datu apriti. Tomēr tas arī nozīmē, ka ikviens, kas to vēlas un kam ir vajadzīgās pamatzināšanas, no jebkuras tīkla vietas var veikt liela mēroga kiberuzbrukumus, piemēram, izmantojot robottīklus.

2.4 Informācijas tehnoloģiju attīstība ir saasinājusi minētās problēmas, jo pašlaik ir vieglāk izgatavot un izplatīt nodarījumu izdarīšanas rīkus (destruktīvu programmatūru ([15]) un robottīklus) un likumpārkāpēji var saglabāt anonimitāti, turklāt atbildība tiek sadalīta dažādām jurisdikcijām. Ņemot vērā grūtības saukt pie atbildības par minētajiem nodarījumiem, organizētās noziedzības aprindas var gūt ievērojamus ienākumus bez liela riska.

2.5 Saskaņā ar 2009. gadā veikto pētījumu ([16]), ar ko iepazīstināja Pasaules ekonomikas forumā, kibernoziegumi pasaulē radījuši aptuveni vienu triljonu ASV dolāru lielus zaudējumus, un šī summa turpina strauji augt. Nesenais Apvienotās Karalistes valdības ziņojums ([17]) liecina, ka Apvienotajā Karalistē vien ikgadējie zaudējumi sasniedz 27 miljardus sterliņu mārciņu. Kibernoziegumu lielās izmaksas pieprasa izlēmīgu rīcību, efektīvu piemērošanu un stingrus sodus likumpārkāpējiem.

2.6 Kā paskaidrots Komisijas dienestu darba dokumentā, kas pievienots ierosinātās direktīvas projektam ([18]), organizētās noziedzības pārstāvji un naidīgi noskaņotas valdības ļaunprātīgi izmanto iespējas veikt uzbrukumus informācijas sistēmām visā Savienībā. Robottīklu uzbrukumi var ievērojami kaitēt visai valstij, pret kuru tie vērsti, un tos var izmantot arī teroristi vai citi likumpārkāpēji, lai uz valsti izdarītu politisku spiedienu.

2.7 Uzbrukums Igaunijai 2007. gada aprīlī un maijā lika pievērst īpašu uzmanību minētajai problēmai. Minētajā uzbrukumā cieta īpaši svarīgas informātikas infrastruktūras daļas valsts pārvaldes un privātajā sektorā, kuru darbība vairākas dienas bija paralizēta, radot no 19 līdz 28 miljoniem *euro* lielus zaudējumus un nodarot lielu politisko kaitējumu. Līdzīgus postošus uzbrukumus veica arī pret Lietuvu un Gruziju.

2.8 Starptautiskajiem sakaru tīkliem ir raksturīga augstas pakāpes pārrobežu savienojamība. Ir būtiski, lai visas 27 dalībvalstis kibernoziegumus un jo īpaši uzbrukumus informācijas sistēmām apkarotu kopīgi un vienoti. Starptautiskās savstarpējās atkarības dēļ Eiropas Savienībai ir pienākums izstrādāt integrētu stratēģiju informācijas sistēmu aizsardzībai pret uzbrukumiem un uzbrukumu izdarītāju sodīšanai.

2.9 Komiteja 2007. gada atzinumā par drošas informācijas sabiedrības stratēģiju ([19]) aicināja izstrādāt visaptverošu ES tiesisko regulējumu kibernoziedzības apkarošanai. Vajadzētu izstrādāt visaptverošu tiesisko regulējumu, kas attiektos ne vien uz uzbrukumiem informācijas sistēmām, bet arī uz finanšu kibernoziedzību, nelikumīgu interneta saturu, elektronisko pierādījumu vākšanu/glabāšanu/pārsūtīšanu, un ietvertu sīki izstrādātus noteikumus par jurisdikciju.

2.10 Komiteja atzīst, ka ir visaptveroša regulējuma izstrāde ir ļoti sarežģīts uzdevums, ko vēl vairāk apgrūtina politiskās vienprātības trūkums ([20]) un tas, ka stipri atšķiras dalībvalstu noteikumi par elektronisko pierādījumu pieļaujamību tiesā. Tomēr

([14]) Saskaņā ar Baltā nama oficiālo statistiku ASV valdība 2010. gada iztērējusi 407 miljonus ASV dolāru pētniecībai, izstrādei un izglītībai kiberdrošības jomā un ierosinājusi 2012. finanšu gadā minētajam nolūkam atvēlēt 548 miljonus ASV dolāru, http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([15]) Destruktīva programmatūra (angliski — *malware*, saīsinājums no "*malicious software*") ir programmatūra, kas izstrādāta, lai slepus piekļūtu datorsistēmai bez tās īpašnieka apzinātas piekrišanas.

([16]) Pētījums "*Unsecured Economies: Protecting Vital Information*" (2009), ko pēc *McAfee* pasūtījuma veica *Purdue* universitātes Informācijas nodrošinājuma un drošības izglītības un pētniecības centrs, 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]) EESK atzinums par drošas informācijas sabiedrību, OV C 97, 28.04.2007, 21. lpp. (*TEN/254*).

([20]) *SEC(2010) 1122*, ietekmes novērtējums Komisijas priekšlikumam *COM(2010) 517*.

visaptverošs regulējums ļautu maksimāli efektīvi izmantot priekšrocības, ko sniedz tiesību akti un neleģislatīvie akti, lai risinātu plašo ar kibernoziegumiem saistīto problēmu klāstu. Visaptverošā regulējumā varētu ņemt vērā arī krimināltiesību sistēmu, un tas vienlaikus uzlabotu arī tiesībaizsardzības sadarbību Eiropas Savienībā. Komiteja mudina Komisiju turpināt strādāt pie visaptveroša tiesiskā regulējuma izstrādes kibernoziedzības apkarošanai.

2.11 Kibernoziegumu apkarošanai ir vajadzīgas īpašas prasmes. Komitejas atzinumā par priekšlikumu regulai, kas attiecas uz *ENISA* ([21]), uzsvērts, ka tiesībaizsardzības iestāžu darbinieku apmācība ir ļoti svarīga. Komiteja ir gandarīta, ka Komisija, atbilstoši tās ierosinājumam paziņojumā par vispārīgo politiku cīņai ar kibernoziedzību ([22]), jau ir daudz paveikusi, lai izveidotu apmācības platformu kibernoziedzības apkarošanai, iesaistot tiesībaizsardzības iestādes un privāto sektoru.

2.12 ES kiberdrošībā ieinteresētās personas ir ikviens iedzīvotājs, kura dzīvība var būt atkarīga no pamatpakalpojumu pieejamības. Iedzīvotāji ir arī atbildīgi par sava interneta pieslēguma aizsargāšanu pret uzbrukumiem, ciktāl tas ir viņu spēkos. Vēl lielāka atbildība ir informācijas un komunikācijas tehnoloģijas un pakalpojumu sniedzējiem, kas nodrošina informācijas sistēmas.

2.13 Ir ārkārtīgi svarīgi, lai visas iesaistītās puses būtu pienācīgi informētas par kiberdrošības jautājumiem. Svarīgi arī, lai Eiropai būtu daudz kvalificētu ekspertu kiberdrošības jomā.

2.14 Eiropā jāveido spēcīga informācijas drošības nozare, kas atbilstu tam kompetences līmenim, kāds raksturīgs šai nozarei ASV, kur tā saņem ļoti labu finansējumu ([23]). Ievērojami jāpalielina ieguldījumi pētniecībā, izstrādē un izglītībā kiberdrošības jomā.

3. **Direktīvas projekta kopsavilkums**

3.1 Priekšlikuma mērķis ir aizstāt Padomes 2005. gada 24. februāra Pamatlēmumu 2005/222/TI par uzbrukumiem informācijas sistēmām ([24]). Pamatlēmuma mērķis, kā norādīts tā apsvērumos, bija uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībaizsardzības dienestu sadarbību, tuvinot dalībvalstu krimināltiesību noteikumus, kas attiecas uz uzbrukumiem informācijas sistēmām. Ar to tika ieviests ES līmeņa tiesiskais regulējums attiecībā uz tādiem nodarījumiem kā nelikumīga piekļuve informācijas sistēmām, nelikumīga iejaukšanās sistēmā un nelikumīga iejaukšanās datos, kā arī īpaši noteikumi par juridisko personu atbildību, jurisdikciju un informācijas apmaiņu. Dalībvalstīm bija jāveic vajadzīgie pasākumi, lai līdz 2007. gada 16. martam īstenotu minētā pamatlēmuma noteikumus.

3.2 Komisija 2008. gada 14. jūlijā publicēja ziņojumu par pamatlēmuma īstenošanu ([25]). Ziņojuma secinājumos norādīja, ka "nesenie visā Eiropā notikušie uzbrukumi kopš Pamatlēmuma pieņemšanas ir parādījuši, ka ir radušies vairāki jauni draudi, jo īpaši plašu vienlaicīgu uzbrukumu informācijas sistēmām parādīšanās un tā saukto robottīklu (*botnets*) aizvien pieaugošā izmantošana noziedzīgiem mērķiem". Pamatlēmuma pieņemšanas laikā šiem uzbrukumiem nebija pievērsta galvenā uzmanība.

3.3 Komisijas priekšlikumā ir ņemtas vērā kibernoziegumu izdarīšanas jaunākās metodes, jo īpaši robottīklu izmantošana ([26]). Ir ļoti grūti izsekot nodarījuma izdarītājus, jo datori, kas veido robottīklu un veic uzbrukumu, un nodarījuma izdarītājs var atrasties dažādās vietās.

3.4 Robottīklu veiktie uzbrukumi bieži vien ir plaša mēroga uzbrukumi. Plaša mēroga uzbrukumi ir vai nu tādi, ko var veikt, izmantojot rīkus, kas ietekmē ievērojamu skaitu informācijas sistēmu (datoru), vai kas rada ievērojamu kaitējumu, proti, sistēmas pakalpojumu pārtraukumu, finansiālas izmaksas, personas datu zudumu utt. Plaša mēroga uzbrukumi ievērojami kaitē uzbrukuma tiešajam mērķim un/vai tā darba videi. Šajā saistībā "liels robottīkls" it tāds, kas spēj radīt nopietnu kaitējumu. Ir grūti definēt robottīklu lielumu, taču tiek lēsts, ka lielākie līdz šim pieredzētie robottīkli aptver 40 000 līdz 100 000 savienojumu (tas ir, inficētu datoru) 24 stundu laikposmā ([27]).

3.5 Pamatlēmumā ir vairākas nepilnības, ņemot vērā nodarījumu (kiberuzbrukumu) apjomus un skaita pieaugumu. Tā tuvina tiesību aktus tikai attiecībā uz dažiem nodarījumiem, bet pilnībā nerisina jautājumu par liela mēroga uzbrukumu iespējamiem draudiem sabiedrībai. Turklāt nav pievērsta pietiekama uzmanība šo nodarījumu smagumam un sankcijām.

3.6 Direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību normas attiecībā uz uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp dalībvalstu policijas un citu specializētu tiesībaizsardzības dienestu sadarbību.

([21]) EESK atzinums par regulu, kas attiecas uz Eiropas Tīklu un informācijas drošības aģentūru, OV C 107, 6.04.2007, 58. lpp.

([22]) "Vispārīgā politika cīņai ar kibernoziedzību", *COM(2007) 267*.

([23]) Saskaņā ar Baltā nama oficiālo statistiku ASV valdība 2010. gada iztērējusi 407 miljonus ASV dolāru pētniecībai, izstrādei un izglītībai kiberdrošības jomā un ierosinājusi 2012. finanšu gadā minētajam nolūkam atvēlēt 548 miljonus ASV dolāru, http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([24]) OV L 69, 16.03.2005., 68. lpp.

([25]) Komisijas ziņojums Padomei, pamatojoties uz 12. pantu Padomes 2005. gada 24. februāra pamatlēmumā par uzbrukumiem informācijas sistēmām, *COM (2008) 448*.

([26]) Sk. 6. zemsvītras piezīmi.

([27]) Savienojumu skaits 24 stundu laikposmā ir parasti izmantota robottīklu lieluma mērvienība.

3.7 Uzbrukumi informācijas sistēmām, jo īpaši organizētas noziedzības aktivitāšu rezultātā, kļūst arvien draudīgāki, un pieaug bažas par iespējamiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tādējādi ir nepieciešama rīcība Eiropas Savienības līmenī.

3.8 Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas ir īpaši svarīgas valstīm vai īpašām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Šo tendenci pavada aizvien modernāku rīku attīstība, ko noziedznieki var izmantot dažādu kiberuzbrukumu izdarīšanai.

3.9 Definīciju, jo īpaši informācijas sistēmu un datorizētu datu definīciju, vienotība šajā jomā ir svarīga, lai nodrošinātu saskaņotu pieeju šīs direktīvas piemērošanai dalībvalstīs.

3.10 Jāpanāk kopīga pieeja noziedzīgu nodarījumu pazīmēm, ieviešot vienotus noziedzīgu nodarījumu sastāvus attiecībā uz nelikumīgu piekļuvi informācijas sistēmai, nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datos un nelikumīgu pārtveršanu.

3.11 Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām. Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas.

3.12 Ar direktīvu atceļ Pamatlēmumu 2005/222/TI, pārņemot tā noteikumus un pievienojot turpmāk minētos elementus.

(a) Direktīva nosaka par sodāmu nodarījumu izdarīšanai izmantojamo ierīču/rīku ražošanu, pārdošanu, iepirkšanu izmantošanai, importu, izplatīšanu vai citāda veida pieejamības nodrošināšanu.

(b) Ar direktīvu ievieš atbildību pastiprinošus apstākļus:

— ja veikts plaša mēroga uzbrukums — ieviešot jaunu atbildību pastiprinošu apstākli, tiktu aptverti robottīkli vai tamlīdzīgi rīki tādā nozīmē, ka robottīkla vai tamlīdzīga rīka izveide būtu atbilstību pastiprinošs apstāklis, ja tiek izdarīti pamatlēmumā uzskaitītie nodarījumi;

— ja uzbrukums izdarīts, slēpjot izdarītāja patieso identitāti un kaitējot identitātes likumīgajam īpašniekam.

(c) Ar direktīvu ievieš "nelikumīgas pārtveršanas" noziedzīga nodarījuma sastāvu.

(d) Ar direktīvu ievieš pasākumus, lai uzlabotu sadarbību Eiropā krimināltiesību jomā, stiprinot 24/7 kontaktpunktu struktūru ([28]).

(e) Direktīvā risina jautājumu par kibernoziedzības statistikas datu sniegšanu, tostarp par pamatlēmumā minētajiem nodarījumiem un pievienoto "nelikumīgo pārtveršanu".

(f) Direktīvā noziedzīgu nodarījumu definīcijās, kas uzskaitītas 3., 4., 5. pantā (nelikumīga piekļuve informācijas sistēmai, nelikumīga iejaukšanās sistēmā, nelikumīga iejaukšanās datos) ir iekļauts noteikums, kas, transponējot direktīvu valsts tiesību aktos, ļauj paredzēt, ka krimināltatbildība iestājas tikai "gadījumos, kas nav mazsvarīgi".

Briselē, 2011. gada 4. maijā

Eiropas Ekonomikas un sociālo lietu komitejas priekšsēdētājs

Staffan NILSSON

([28]) Ieviesta pamatojoties uz Konvenciju un Pamatlēmumu 2005/222/TI par uzbrukumiem informācijas sistēmām.