**MYKOLO ROMERIO UNIVERSITETAS**

**SOCIALINIŲ TECHNOLOGIJŲ FAKULTETAS**

**SKAITMENINIŲ TECHNOLOGIJŲ INSTITUTAS**

**ARNOLDAS DUOBA**

Naujųjų technologijų teisė

# TEISINĖS KOVOS SU ELEKTRONINIAIS NUSIKALTIMAIS PRIEMONĖS TARPTAUTINIU MASTU

**Magistro baigiamasis darbas**

**Darbo vadovas-**

**Prof. Darius Štitilis**

**Vilnius, 2014**

Turinys

# ĮVADAS

***Temos aktualumas***. Šių dienų pasaulyje internetinė erdvė ir tarptautinė erdvė yra persipynusios tarpusavyje. Informacinė sistema apjungia kontinentus, salas, tautas, bendruomenes ir pavienius asmenis į milžinišką virtualų tinklą, tačiau nepaisant to valstybės vis tiek išlaiko savo tradicinį imunitetą. Yra sakoma, kad pasaulyje turinčiame internetą nei viena sala nėra sala[1]. Interneto ir kasdieniniame gyvenime naudojamų technologijų vystymas sąlygojo ir įvairių nusikalstamo elgesio formų atsiradimą bei plitimą.[2] Visa jungiantis internetas suteikia naujų galimybių vykdyti nusikalstamas veikas, sudaro sąlygas naujiems nusikaltimų būdams atsirasti, bei sudaro galimybes įvykdyti naujas iki tol nežinomas teisinėje praktikoje nusikalstamas veikas.[3] Pastaruoju metu tokio pobūdžio nusikalstamos veikos tapo realybe, o elektroninių pajamos gaunamos iš elektroninių nusikaltimų pagal kai kuriuos vertinimus, yra trečioje vietoje po pajamų gaunamų iš prekybos narkotikais ir ginklais.[4]

Po 2001 metų rugsėjo 11 dienos įvykių buvo pradėta kalbėti, kad teroristiniai aktai gali būti vykdomi ir interneto pagalba.[5] Ilgai laukti po šios galimos prognozės pasitvirtinimo nereikėjo, nes jau 2007 metais Estijoje buvo įvykdytos masinės kompiuterinės atakos, kurias vieni prilygino teroristiniam išpuoliui, o kiti net kariniams veiksmams. Akivaizdu, kad elektroniniai nusikaltimai gali paveikti tiek konkretų asmenį, tiek visą konkrečią visuomenę kaip tokią.[6]

Elektroniniai nusikaltimai tapo nepriklausomi, nuo valstybių sienų, ar teritorijos ribų. Tuo tarpu kai teisės normos ir jų galiojimas yra ribojamas teritorinio principo, tai įrankiai, priemonės, ir elektroninių nusikaltimų subjektai yra nepriklausomi nuo valstybių sienų. Elektroniniai nusikaltimai gali būti vykdomi bet kurioje pasaulio šalyje, nepaisant fizinės nusikaltimą vykdančio asmens buvimo vietos. Prof. D. Štitilio nuomone globali elektroninių nusikalstamų veikų prigimtis apsunkina tokių nusikalstamų veikų tyrimą, sukelia jurisdikcijos problemas, bei apsunkina elektroninių įrodymų rinkimą. Priemonės priimamos valstybės viduje, yra labai svarbios kovojant su elektroniniais nusikaltimais, tačiau jų nepakanka norint susidoroti su šiuo pasauliniu iššūkiu. Todėl tarptautinis tarpvalstybinis bendradarbiavimas ir koordinavimas yra būtinas siekiant susidoroti su nusikalstamomis veikomis draudžiamomis didžiojoje dalyje pasaulio valstybių.

[1] McConnell International.Cyber Crime…and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December 2000, p. 8.
[2] Higgins G.E. Cybercrime:An introduction to an Emerging Phenomen.// Library of Congress Cataloging, 2010, p. 1.
[3] Štitilis D. Elektroniniai nusikaltimai.// Vilnius, Mykolo Romerio Universitetas, 2011, p. 2.
[4] Ten pat.
[5] Britz T.M. Computer Forensics and Cyber Crime: An Introduction.// Person Education, 2009, p. 155.
[6] Brenner S.W. Cybercrime. Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010, p. 3-5.

Laimei, per pastaruosius kelis dešimtmečius kovai su elektroniniais nusikaltimais buvo skiriamas vis didesnis dėmesys. Daugelis pasaulio valstybių pradėjo pildyti savo nacionalinius baudžiamuosius įstatymus naujomis, iki tol niekam nežinomomis su kompiuterinėmis elektroninėmis technologijomis susijusiomis, nusikalstamomis veikomis. Nacionalinės valstybių pastangos buvo pakankamai sustiprintos tarptautinių organizacijų, tokių kaip Ekonominio bendradarbiavimo ir plėtros organizacijos, Jungtinių Tautų, Pietryčių Azijos valstybių asociacijos, Amerikos valstijų asociacijos, G-8 valstybių, bei Interpolo. Be nacionalinių ir organizacinių pastangų kovojant su tarptautinio masto elektroninėmis nusikalstamomis veikomis 2001 metais Budapešte buvo pasirašyta Konvencija dėl elektroninių nusikaltimų[7]. Tačiau dėl mažo šią tarptautinę sutartį pasirašiusių, o vėliau ją ratifikavusių valstybių skaičiaus Konvencija iš esmės nesustabdė elektroninių nusikalstamų veikų plitimo.

Atsižvelgiant į tai, šiame darbe keliamas ***tyrimo tikslas -*** analizuojant esamas teisines kovos su elektroniniais nusikaltimais priemones tarptautiniu mastu atskleisti probleminius aspektus, taip pat nustatyti ar egzistuojančios priemonės yra pakankamos kovoti su elektroniniais nusikaltimais.

Siekiant užsibrėžto tikslo, keliami šie ***uždaviniai:***

1. Atskleisti esamas teisinės kovos priemones su elektroniniais nusikaltimais tarptautiniu mastu;
2. Nustatyti ar šiuo metu egzistuojančios tarptautinės teisinės kovos su elektroniniais nusikaltimais priemonės yra pakankamai efektyvios kovoje su elektroniniais nusikaltimais;
3. Atskleisti jurisdikcijos problemą kovojant su elektroninėmis nusikalstamomis veikomis;
4. Išanalizuoti tarptautinio teismo ir tribunolo reikalingumą kovojant su elektroniniais nusikaltimais;

Tyrimo ***objektas.*** Tyrimo objektas yra teisinės priemonės tarptautiniu mastu, kuriomis siekiama kovoti prieš neteisėtas elektronines veikas.

***Tyrimo naujumas.*** Darbe analizuojami Lietuvos teisės moksle nenagrinėti klausimai, bei tarptautiniu mastu mažai ištirti aspektai. 2001 m. Konvencija dėl elektroninių nusikaltimų[8] iki šiol nėra pilnai ir veiksmingai veikianti tarptautinė sutartis. Naujumą atspindi tai, kad darbe analizuojamas, esamuose moksliniuose darbuose nagrinėtas minėtos Konvencijos ir kitų tarptautinių teisės aktų įgyvendinimo klausimas.

***Temos ištirtumas.*** Didžiąją dalį su elektroniniais nusikaltimais susijusių temų yra išanalizavęs šios srities ekspertas Steinas Schjolbergas[9]. Savo moksliniuose leidiniuose ir rekomendacijose jis yra išanalizavęs elektroninių nusikaltimų rūšis, tarptautinius kovos su

[7] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2013-07-10]
[8] Ten pat.
[9] Biograpfhy of Stein Schjolberg. http://www.cybercrimelaw.net/biography.html [žiūrėta 2013-07-10]

elektroniniais nusikaltimais teisės aktus, bei teismų technologiniai sričiai klausimą. Todėl ,autoriaus nuomone, šiame darbe yra tikslinga atskleisti esamas tarptautines teisinės kovos su elektroniniais nusikaltimais priemones, teismo reikalingumą siekiant pažaboti elektronines nusikalstamas veikas, bei išanalizuoti Konvencijos dėl elektroninių nusikaltimų ir kitų juridinę galia turinčių tarptautinių teisės aktų efektyvumą. Prof. Summit Ghosh, leidyklos „Springer" išleistoje knygoje „Cybercrime: A Multidisciplinary Analysis", labai minimaliai atskleidė tarptautinių organizacijų, kovojančių su elektroniniais nusikaltimais veiklą, todėl šiame magistro baigiamajame darbe yra labai svarbu atskleisti tarptautinių organizacijų kovojančių su elektroninėmis nusikalstamomis veikomis problematiką. S.W. Brenner ir B.J. Koops naujųjų technologijų teisei skirtame žurnale išspausdino straipsnį pavadinimu „Approaches to Cybercrime Jusrisdiction", kuriame analizavo jurisdikcijos problemą tiriant elektroninio pobūdžio nusikalstamas veikas, todėl atsižvelgiant ir į kitų teisės mokslininkų darbus, autorius tikslingai atskleidžia esamą jurisdikcijos teoriją, išanalizuoja jurisdikcijos problemą tiriant nusikalstamas veikas, atskleidžia galimai kylančias jurisdikcijos kolizijas, bei atskleidžia jurisdikcijos problemą sparčiai populiarėjančioje debesų kompiuterijoje.

***Darbe naudoti metodai.*** Darbe naudojamas istorinis metodas analizuojant teisinių kovos su elektroniniais nusikaltimais priemonių raidą. Statistinis metodas naudojamas analizuojant prie tarptautinių sutarčių prisijungusių valstybių skaičių, vertinant elektroninių nusikaltimų paplitimą. Lyginamasis metodas naudojamas atskleidžiant tarptautinių sutarčių, skirtų kovotis su elektroniniais nusikaltimais, ypatumus taip pat lyginant atskirų tarptautinių organizacijų bei tarptautiniu mastu veikiančių institucijų veiklą, bei jų naudojamas teisines priemones. Lingvistinis ir analizės metodai naudojami aiškinant tarptautinių teisės aktų normas, atskirų teisinių kovos su elektroniniais nusikaltimais priemonių esmę. Remiantis sisteminiu bei loginiu metodu darbe bus daromos išvados ir apibendrinimai.

***Darbo struktūra.*** Magistro baigiamąjį darbą sudaro įvadas, 4 skyriai (8 poskyriai) ir išvados. Darbo pabaigoje yra literatūros sąrašas, bei darbo apibendrinimas lietuvių ir anglų kalbomis.

Magistriniame darbe yra remiamasi įvairiais literatūros ***šaltiniais*** – tiek teorine, tiek ir praktine medžiaga – teisminių institucijų formuojama praktika. Rengiant darbą naudota gausi mokslinė literatūra iš kurios išskiriama gerai žinomų teisės specialistų moksliniai darbai ir straipsniai. Remtasi aktualiais mokslinių žurnalų „International Journal of Marine and Coastal Law", „International & Comparative Law Quarterly", „American Business Law Journal", „Journal of High Technology Law" straipsniais.

## I. ELEKTRONIAI NUSIKALTIMAI IR JŲ PROBLEMA

Šiais laikais, kompiuterinė technika ir internetas yra neatsiejama beveik kiekvieno iš mūsų gyvenimo dalis. Tačiau tiek kompiuteris, tiek ir internetas gali būti naudojamas ne tik pramogoms, bet taip pat ir vykdant nusikalstamas veikas. Apie teisės pažeidimus, kurie padaromi naudojantis kompiuteriais plačiai diskutuojama tiek žiniasklaidoje, tiek ir moksliniu lygmeniu, tačiau prieš analizuojant elektroninius nusikaltimus būtina apsibrėžti jų sąvoką.

Teisės mokslininkai nurodo, kad šiuo metu universaliausia elektroninių nusikaltimų sąvoka pateikiama 2001 metų Budapešto konvencijoje dėl elektroninių nusikaltimų (toliau-Konvencija)[10]. Ši Konvencija[11] yra vienintelis privalomas tarptautinis teisės aktas, skirtas spręsti kompiuterinių nusikaltimų keliamas problemas. Minėtoje tarptautinėje sutartyje elektroniniai nusikaltimai skirstomi pagal įstatymo saugomą interesą, į šių nusikaltimų sąvoką patenka:

1. Nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui;
2. Kompiuteriniai nusikaltimai;
3. Turinio nusikaltimai;
4. Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais.

Dar prieš priimant šią Konvenciją G. Urbas išreiškė poziciją, kad kol kas neegzistuoja universali elektroninių nusikaltimų sąvoką[12]. Tuo pačiu buvo nurodoma, kokie neteisėti veiksmai turėtų būti laikomi elektroniniais nusikaltimais. Tai neteisėta prieiga prie kompiuterinės sistemos, neteisėtas kompiuterinės informacijos perėmimas, neteisėto turinio medžiagos siuntimas, taip pat tokie veiksmai, kuriais daromas poveikis kompiuterinei sistemai bei su turiniu susiję pažeidimai[13]. Visi šie veiksmai apibrėžti kaip neteisėti 2001 metais priimtoje Budapešto konvencijoje, kuri galima teigti, kriminalizavo platų spektrą veikų, kuriomis padaromi elektroniniai nusikaltimai.

Siekiant pateikti aiškų ir išsamų apibrėžimą, paminėtina pozicija, kad elektroniniai nusikaltimai yra laikomi kompiuteriniais nusikaltimais plačiąja prasme, tokiems nusikaltimams priskiriami ir nusikaltimai, kurie vykdomi panaudojant elektroninę erdvę[14]. Tokia nuomonei pritaria

---

[10] Civilka M., Lamanauskas T., Osinaitė G., Sauliūnas D. ir kt. Informacinių technologijų teisė.// Vilnius, NVO Teisės Institutas, 2004, p. 513.
[11] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2013-07-10]
[12] Urbas G. Cybercrime legislation in the Asia - Pacific Region. Regional conference of piracy and cyber crime. The university of Hong Kong, April 25-26, 2001.
[13] Broderic T. R. Regulation of the Information Technology in the European Union.// London, Kluver Law International, 2000, p. 67.
[14] Civilka M., Lamanauskas T., Osinaitė G., Sauliūnas D. ir kt. Informacinių technologijų teisė.// Vilnius, NVO Teisės Institutas, 2004, p. 512.

tiek G.Wahlertas,[15] tiek ir autorius. Ši pozicija nurodoma ir 2000 metų Europos Komisijos komunikate[16], bei paaiškinamajame Konvencijos dėl elektroninių nusikaltimų memorandume[17]. Taigi, šiuo metu elektroninių nusikaltimų sąvoka yra pakankamai plati.

Tačiau dar prieš priimant minėtą Konvenciją valstybės suprato, kad kompiuteriniai nusikaltimai yra tarptautinio lygmens ir norint efektyvaus būdo kovoti su jais, reikia priemonių, kurios būtų įgyvendinamos tarptautiniu mastu. Šiame magistriniame darbe tarptautinėmis priemonėmis yra laikomos visos priemonės skirtos kovoti su elektroniniais nusikaltimai, dėl kurių sutarė daugiau nei viena valstybė, arba kurios yra priimtos tarptautinės organizacijos. Tačiau, kovojant su šiais nusikaltimais pasitelkiamos ne tik teisinės, bet ir techninės bei kitos priemonės. Darbe analizuojamos tiktai teisinės kovos su elektroniniais nusikaltimais priemonės, priimtos tarptautiniu mastu. Teisės moksle prof. Summit Ghosh pateikė nuomonę, kad norint efektyviai kovoti su elektroniniais nusikaltimais, valstybės turi modernizuoti tiek materialiąsias tiek ir procesines teisės normas[18]. Materialioji teisės norma uždraudžia vienokį ar kitokį elgesį, o procesinės teisės normos sprendžia tokius klausimus kaip paieška ar sulaikymas, jurisdikcija, ekstradicija, duomenų perdavimas, tarptautinio bendradarbiavimo metodai. Siekiant užkardyti elektroninių nusikaltimų plitimą, valstybės bendradarbiauja, nemažai tarptautinių organizacijų, tokių kaip G-8 ir kitos, deda pastangas siekiant suvienodinti kompiuterinių nusikaltimų reguliavimą, taip pat siekiant išvengti tokių vietų, kurios būtų saugios kompiuterinių nusikaltimų darytojų atžvilgiu (angl. „computer crime havens“, „kompiuterinių nusikaltimų rojus“). Ekonominio bendradarbiavimo ir vystymosi organizacija (Organisation for Economic Co-operation and Development) jau 1986 m. paskelbė protokolą, kuriame buvo išvardintos penkios kategorijos nusikaltimų, į kurias jų manymu pateko pagrindiniai kompiuteriniai nusikaltimai[19]. Tai buvo pirmasis bandymas užkirsti kelią elektroniniams nusikaltimams tarptautiniu mastu. Nuo to laiko, nemažai tarptautinių priemonių, skirtų kovoti su elektroniniais nusikaltimai tarptautiniu lygiu, buvo priimta. Galima atkreipti dėmesį į tai, kad tarptautinės priemonės šioje srityje yra ne kas kitas kaip kovos su elektroniniais nusikaltimais priemonių harmonizavimas. Visas šias priemones-tarptautinius harmonizavimo veiksmus Li Xingan siūlo suskirstyti į tokius veiksmus, kurių ėmėsi:

- specializuotos organizacijos;

---

[15] Wahlert G. Crime in Cyberspace: trendsin Computer Crime in Australia. Paper presented at the conference, held in Melbourne, 16-17 February, 1998, by the Australian institute of Criminology;
Magnin C. J. The 2001 Council of Europe: Convention on Cybercrime: an efficient tool to fight crime in cyberspace. 2001.

[16] Cominication from the Commission to the Council, the Europien Parliament, the Economic and the Social Committee and Committee of the regions. Creating a Safer Information Infrastructures and Combating Computer-related Crime. Brussels, COM (2000) 890 final. https://www.conventions.coe.int [žiūrėta 2013-07-15]

[17] Explanatory Memorandum related to Convention on Cyber-Crime. http://www.conventions.coe.int [žiūrėta 2013-07-15]

[18] Summit G., Elliot T. Cybercrimes: a multidisciplinary analysis.// Vokietija, Springer, 2010. p. 320.

[19] Computer-Related Criminality: Analysis of Legal Policy in the OECD Area. Report DSTI- ICCP 84.22, 18 April 1986.

- regioninės organizacijos;
- įvairių valstybių sukurtos organizacijos;
- ir pasaulinės organizacijos;[20]

Prie specializuotų organizacijų reikėtų paminėti Interpolą, Tarptautinę telekomunikacijų sąjungą ir kitas. Tačiau ne visos specializuotos tarptautinės organizacijos, kurios prisideda koordinuojant saugumą elektroninėje erdvėje, kuria teisines priemones kovai su elektroniniais nusikaltimais. Dėl šios priežasties darbe didesnis dėmesys skiriamas tiktai Interpolo (Tarptautinės Kriminalinės Policijos Organizacijos)[21] įgyvendinamoms priemonėms.

Taip pat yra ir daugybės regioninių organizacijų, kurios savo veikloje skiria dėmesį kovai su elektroniniais nusikaltimais, reikia paminėti tokias kaip Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo organizacija, Pietryčių Azijos valstybių asociacija, Europos Taryba, Europos Sąjunga, Amerikos valstybių organizacija ir kt. Prie įvairių valstybių sukurtų organizacijų, kurios deda pastangas užtikrinant saugumą elektroninėje erdvėje priskirtinos tokios organizacijos kaip Tautų Sandrauga (Commonwealth of Nations), Didžiojo aštuoneto šalys (The Group of Eight), Ekonominio bendradarbiavimo ir vystymosi organizacija, taip pat pasaulinė organizacija Jungtinės Tautos. Šiame darbe nebus analizuojamos visos tarptautiniu mastu įgyvendinamos teisinės priemonės skirtos kovoti su elektroniniais nusikaltimais. Aptariamos priemonės pasirinktos dėl jų tarptautinės reikšmės, o dėl darbo apimties visi tarptautiniai veiksmai, kurių ėmėsi tarptautinės organizacijos, visuose lygmenyse nebus analizuojami.

Siekiant susisteminti priemones, kurių minėtos tarptautinių organizacijų grupės ėmėsi kovojant su elektroniniais nusikaltimais, galima išskirti pagrindines jų veiklos sritis. Jos imasi veiksmų skatinančių apsaugos stiprinimą tiek tarptautiniu, tiek ir nacionaliniu lygiu, imasi priemonių skirtų teisės harmonizavimui, taip pat veiksmų skirtų koordinuoti ir bendradarbiauti įgyvendinant teisės normas, bei imasi tiesioginių veiksmų skirtų kovoti su elektroniniais nusikaltimais. Visos šios priemonės įgyvendinamos priimant konvencijas, rekomendacijas, gaires, sudarant specializuotas darbo grupes ir kitais būdais skatinant valstybes imtis tiesioginių kovos su elektroniniais nusikaltimais priemonių.

Kalbat apie skatinimą užtikrinti saugumą tarptautiniu lygiu, tokių veiksmų ėmėsi Jungtinių Tautų Organizacija. Dvi šios organizacijos lygmeniu priimtos rezoliucijos (53/63 (2000) ir 56/121 (2001) priimtos siekiant susidoroti su nusikalstamu piktnaudžiavimu naudojant informacines technologijas pabrėžė Didžiojo aštuoneto organizacijos principų svarbą ir paragino valstybes atsižvelgti į šiuos principus. Kelios kitos JT rezoliucijos taip pat yra skirtos paskatinti daugiašalėms

[20]Xingan L. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology, Vol. 4, No 3, September 2007. http://www.webology.org/2007/v4n3/a45.html [žiūrėta 2013-07-20]
[21] Fooner, M. Interpol: Issues in World Crime and International Criminal Justice.// New York and London, Springer, 1989, p. 32-244.

deryboms apie egzistuojančias ir potencialias grėsmes informacijos saugumo srityje, taip pat aptariant priemones kuriomis galėtų būti apribojamos šios grėsmės. Reikia pastebėti, kad kitos tarptautinės organizacijos taip pat ėmėsi priemonių skatinant saugumo užtikrinimą tarptautiniu mastu. Pavyzdžiui po 09/11 įvykių Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo organizacijos (APEC) lyderiai skatino stiprinti organizacijos veiksmus apsaugant infrastruktūrą[22].

Skatinant apsaugos stiprinimą valstybiniu lygiu, šioje srityje pastangas deda visos tarptautinės organizacijos. Kaip pavyzdį galima pateikti jau autoriaus paminėtą Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo organizaciją. Ši organizacija nurodė valstybėms narėms ir regionams skatinti kibernetinę apsaugą ir stabdyti kibernetinių nusikaltimų grėsmes.

Aptariant tarptautines priemones skirtas teisinio reglamentavimo harmonizavimui, pabrėžtina, kad tai yra pagrindinė tarptautinių organizacijų, kovojančių su elektroniniai nusikaltimais veiklos sritis. Kaip jau minėta, teisinio reglamentavimo vienodinimas Europoje prasidėjo 1980 metais ir didžiausias pasiekimas šioje srityje buvo Konvencija dėl elektroninių nusikaltimų. Kitos tarptautinės organizacijos taip pat stengėsi vienodinti teisės normas. 1981 m. Interpolas su tikslu nustatyti trūkumus egzistuojančiame teisiniame reglamentavime ir jį suvienodinti apžvelgė valstybių narių baudžiamosios teisės normas. Šiuo metu Interpolo „African Working Party on Information Technology Crime Projects“ bando įkalbėti Afrikos šalis pasirašyti ir ratifikuoti Konvenciją dėl elektroninių nusikaltimų[23]. Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo organizacija taip pat deda pastangas norėdami paskatinti valstybes sukurti Konvencijai dėl elektroninių nusikaltimų prilygstantį ir Jungtinių Tautų rezoliucijas atitinkantį tarptautinį dokumentą. Europos Sąjungos sprendimu 2002 m. valstybėms narėms buvo suteikta atsakomybė kriminalizuojant neteisėtą prieigą ir neteisėtą kišimąsi į informacines sistemas. Amerikos valstybių organizacija paskatino valstybes kriminalizuoti kibernetinius nusikaltimus ir harmonizuoti valstybių narių teisės normas, taip pat apsvarstyti galimybę prisijungti prie Konvencijos dėl elektroninių nusikaltimų. Didžiojo aštuoneto šalys, Paryžiaus konferencijoje aptarė bendradarbiavimo galimybę, kuriant tarptautinį baudžiamąjį kodeksą skirtą kovoti su kompiuteriniais nusikaltimais. Iš pateiktos informacijos matyti, kad teisinio reglamentavimo harmonizavimo srityje yra siekiama kurti privalomus tarptautinius teisės aktus, tarptautines sutartis, kurių pagalba būtų užtikrinamas teisės normų skirtų kovoti su elektroniniais nusikaltimais vienodumas tarptautiniu mastu. Nes vien rekomendacinio pobūdžio priemonės, neįgalina valstybių imtis aktyvių veiksmų, užkertant kelią elektroniniams nusikaltimams, juos kriminalizuojant.

[22] Xingan L. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology, Vol. 4, No 3, September 2007. p. 11. http://www.webology.org/2007/v4n3/a45.html [žiūrėta 2013-07-20]
[23] http://www.interpol.net/Public/TechnologyCrime/WorkingParties/Default.asp [žiūrėta 2013-07-22]

Kita svarbi priemonių skirtų kovoti su elektroniniais nusikaltimais rūšis, tai priemonės skirtos koordinuoti ir bendradarbiauti įgyvendinant priimtas teisės normas. Priimant ir kuriant šias priemones, siekiama užtikrinti, kad nei viena valstybė netaptų prieglobsčio šalimi, asmenims įvykdžiusiems elektroninius nusikaltimus, siekiant, kad priimtos teisės normos būtų efektyvios ir veikiančios. Skatinamas bendradarbiavimas, įgyvendinat sukurtas normas skirtas kovoti su elektroniniais nusikaltimais. Interpolo Europos informacinių nusikaltimų darbo grupė šiuo tikslu sudarė Kompiuterinių nusikaltimų žinyną, kuriame pateiktos techninės gairės, kurių turėtų būti laikomasi įgyvendinant teisės normas. Konvencijoje dėl elektroninių nusikaltimų teisės normų įgyvendinimo srityje taip pat numatytas bendradarbiavimo mechanizmas, Europos Sąjungos mastu buvo diskutuota apie srauto duomenų išsaugojimą, o 2001 m. Amerikos teisingumo ir vidaus reikalų ministro įkurta elektroninių nusikaltimų ekspertų grupė dirbo siekdami atrasti bendradarbiavimo Amerikoje sistemą, kovojant su elektroniniais nusikaltimais. Didžiojo aštuoneto grupė taip pat peržiūrėjo egzistuojančius bendradarbiavimo mechanizmus, atrado spragas ir dėjo pastangas joms užpildyti. Valstybės narės buvo skatinamos padidinti kriminalizavimą, persekiojimą, tyrimą ir tarptautinį bendradarbiavimą.

Kovojant su elektroniniais nusikaltimais tarptautinės organizacijos taip pat imasi priemonių skirtų tiesiogiai užkirsti kelią šiems nusikaltimams. Prie šių priemonių priskiriamos dvi kategorijos: tai elektroninių nusikaltimų prevencijos ir elektroninių nusikaltimų tyrimo priemonės. Kaip nurodo L. Xingan jos yra labai vertingos, kol dar vyksta tarptautinis elektroninius nusikaltimus reglamentuojančios teisės harmonizavimas[24]. Skirtingos organizacijos imasi priemonių skirtingose srityse. Pavyzdžiui, Interpolas tiesiogiai bendradarbiauja su bankais, kovojant su nusikaltimais susijusiais su sukčiavimu apmokant[25]. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce 1999 apibrėžė vartotojų elektroninėje komercijoje apsaugą. Guidelines for the Security of Information Systems and Networks 2002 paskatino valstybes nares skirti daugiau dėmesio apsaugai ir skatinti saugumą tarp visų dalyvių, apsaugant informacines sistemas ir tinklus.

Kaip matoma, tarptautiniu lygmeniu dedamos didelės pastangos siekiant užkirsti kelią elektroniniams nusikaltimams bei kovoti su jais. Tačiau norint efektyvaus rezultato didžiausios pastangos turėtų būti dedamos teisinio reglamentavimo vienodinimui. Visose valstybėse, tiek ir ekonomiškai stipresnėse, tiek ir mažiau išsivysčiusiose, elektroniniai nusikaltimai ir elektroninės erdvės apsauga turėtų būti vienodai apibrėžtos. Kaip nurodo, vienas žymiausių šios srities

[24] Xingan L. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology, Vol. 4, No 3, September 2007. p. 12. http://www.webology.org/2007/v4n3/a45.html [žiūrėta 2013-07-20]
[25] Police Commissioners Conference Electronis Crime Working Party, 2000, p. 64. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.4966 [žiūrėta 2013-08-03]

mokslininkų Steinas Schjolbergas, tai būtų galima pasiekti priimant tarptautinį susitarimą ar protokolą Jungtinių Tautų lygmeniu[26].

Daugiau, labai svarbu išsiaiškinti elektroniniais nusikaltimais daromą žalą ir trumpai išanalizuoti esamą naujausią, praėjusių metų, statistiką. Remiantis internete pateikta informacinių technologijų specialistų pateikta 2013 metų statistika, elektroninių nusikaltimų žala praėjusiais metais siekė virš 100 milijonų JAV dolerių.[27] Nukentėjusių nuo šio tipo nusikalstamų veikų skaičius buvo 556.000000.[28] Tai reiškia, kad kiekvieną dieną nuo elektroninių nusikaltimų nukentėjo apie pusantro milijono žmonių, net aštuoniolika žmonių kas sekundę. Vieno nukentėjusiojo vidutinis padaromos žalos dydis buvo 298 JAV doleriai.[29] Remiantis ta pačia statistika vyrai beveik 1,5 karto dažniau nukenčia nuo elektroninių nusikaltimų, nei moterys. Net 59% darbuotojų išeidami iš savo buvusios darbovietės nusikopijuoja jos vidinius dokumentus, o verslo srityje dažnai net su komercine paslaptimi susijusią informaciją[30]. Net 38,9% tokių nusikalstamos veikos požymių turinčių veiksmų įvyksta medicinos ir sveikatos priežiūros srityje, tačiau bankų, finansų ir kredito įstaigų srityje tai pasitaiko net septynis kartus rečiau. Statistikos duomenimis per 2013 metus daugiausia elektroninių nusikalstamų veikų buvo įvykdyta iš Rusijos, Taivanio ir Vokietijos[31]. Tačiau nuo veikų daugiausia nukenčia Rusijos, Kinijos ir Pietų Afrikos piliečiai[32]. Taigi, autoriaus nuomone, pilno tiesioginio ryšio tarp nukentėjusių ir nusikaltėlių faktinių geografinių padėčių nėra, o tokia statistika egzistuoja dėl menko viso pasaulio visuomenės supratimo apie elektroninius nusikaltimus, pačios elektroninės nusikalstamos veikos latentiškumo ir menko kompiuterinio tinklo naudotojų apsaugos lygio.

Apibendrinant galima teigti, kad nepaisant autoriaus pateiktos statistikos ir kitų teisės mokslininkų paminėtos esamos teisinės padėties elektroninių nusikaltimų srityje su šia problema reikia kovoti. Reikia skatinti tiek tarptautinių organizacijų, tiek ir nacionaliniu interesu kuriamas naujas kovos priemones su elektroniniais nusikaltimais. Jokių būdu nepaliekant reikiamų sprendimų ateičiai. Todėl sekančiose darbo dalyje autorius bandys nustatyti esamas tarptautines teisinės kovos priemones ir ištirti priemonių efektyvumą.

[26] Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva.// December 2008, p. 2.
[27] Cyber Crime Statistics and Trends. http://www.go-gulf.com/blog/cyber-crime/ [žiūrėta 2014-03-20]
[28] Ten pat.
[29] 2013–The Impact of Cybercrime. http://resources.infosecinstitute.com/2013-impact-cybercrime/ [žiūrėta 2014-03-20]
[30] Cyber Crime Statistics and Trends. http://www.go-gulf.com/blog/cyber-crime/ [žiūrėta 2014-03-20]
[31] Ten pat.
[32] 2013–The Impact of Cybercrime. http://resources.infosecinstitute.com/2013-impact-cybercrime/ [žiūrėta 2014-03-20]

## II. JURIDINĘ GALIĄ TURINČIOS PRIEMONĖS

Statistikos duomenimis kompiuterinis internetinis tinklas per pastarąjį dešimtmetį kasmet vidutiniškai augo po kelis šimtus procentų pasauliniu mastu ir šiuo metu maždaug 2,5 milijardo žmonių yra šio tinklo vartotojai.[33] Interneto sklaida į visuomenę buvo tokia greita, kad iki šiol visuomenei priimtini etikos kodeksai, baudžiamieji teisės aktai ar kiti teisės aktai buvo priversti neatsilikti ir žengti koja kojon su šiuo nauju reiškiniu. Siekiant sukurti naujus etikos standartus kompiuterinėje erdvėje, baudžiamieji teisės aktai privalo būti priimti aiškūs ir konkretūs, be jokios galimybės juos interpretuoti. Nes tik tada nusikaltimus darantys asmenys gali būti sustabdyti, o teisinės kovos su elektroniniais nusikaltimais priemonės pasiektų viršūnės tašką.

Anot M. Gercke, pagrindinis pasaulinio masto klausimai šiuo metu yra platėjanti elektroninių nusikaltimų gama, informacijos arba kitaip sakant duomenų apsauga ir paties naudojamo internetinio tinklo saugumas[34]. Egzistuoja du skirtingi sprendimai į šiuos probleminius klausimus. M.Gercke teigimu sprendimai ir tarptautiniai metodai sprendžiami per tarptautines organizacijas, pavienių valstybių arba valstybių grupių, per geografinio regiono teisės aktus arba tarptautines sutartis. Tačiau abu šie metodai turi tiek privalumų, tiek trūkumų.[35]

Elektroniniai nusikaltimai yra neturi jokių juos ribojančių sienų ir dėl tos priežasties jie yra potencialiai tarptautiniai.[36] Nusikaltimus vykdantys asmenys ir nusikaltimo aukos gali būti bet kurioje, nebūtinai toje pačioje valstybėje, todėl tarptautinis teisėsaugos institucijų bendradarbiavimas yra būtinas, siekiant kovoti su nusikaltimais tarptautiniu mastu.[37] Tarptautinė kova su elektroniniais nusikaltimais priklauso nuo patikimų bendradarbiavimo priemonių ir vieningai suderintų valstybinių įstatymų. Remiantis bendru dvigubo baudžiamumo principu, efektyviam tarptautiniam bendradarbiavimui yra būtinas baudžiamosios teisės nuostatų suderinimas, su tikslu išvengti saugaus prieglobsčio bet kurioje valstybėje sukūrimu.[38] Be to, labai svarbu suderinti tyrimo priemones siekiant užtikrinti, kad visos valstybės, dalyvaujančios tyrime turėtų būtinas priemones tyrimui.

Todėl esamas teisines kovos priemones su elektroniniais nusikaltimais tarptautiniu mastu bandysime struktūrizuotai apžvelgti šiame skyriuje. Pabandysime plačiau ir struktūrizuotai atskleisti tarptautinių organizacijų teisines priemones, nei tai buvo padaryta pirmame skyriuje. Taip pat

[33] Internet Usage Statistics http://www.internetworldstats.com/stats.htm [žiūrėta 2014-01-05]
[34] Gercke M. National, Regional and International Legal Approacges in the Fight against Cybercrime.// 2008, p. 7-13.
[35] Ten pat.
[36] Sofaer A.D., Goodman S.E. Cyber Crime and Security The Transnational Dimension. http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf [žiūrėta 2014-01-05]
[37] ten pat.
[38] WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf [žiūrėta 2014-01-05]

atskleisti Konvencijos dėl elektroninių nusikaltimų efektyvumą, bei įvardinti mums aktualiausias Europos regionines teisines priemones ir jų svarbą.

## 2. 1. Tarptautinės sutartys

### 2. 1. 1. 2001 metų Konvencija dėl elektroninių nusikaltimų.

1989 metais Europos Taryba pradėjo aktyviai dirbti prie naujai augančios grėsmės, kurią kėlė įsilaužimai į kompiuterį ir kiti su kompiuteriais susiję nusikaltimai. 2001 metais priimta, o 2004 Liepos 1 dieną įsigaliojusi Konvencija dėl elektroninių nusikaltimų yra puikus regioninės iniciatyvos pavyzdys[39], kuriuo siekiama spręsti kompiuterinių nusikaltimų problemą, derinti nacionalinius teisės aktus, gerinti šio pobūdžio nusikalstamų veikų tyrimo metodus ir skatinti tarptautinį bendradarbiavimą.

Pagrindinis Konvencijos tikslas yra suvienodinti baudžiamąją politiką, siekiant apsaugoti visuomenę nuo elektroninių nusikaltimų, priimant tinkamus teisės aktus ir skatinant tarptautinį bendradarbiavimą. Konvencija buvo siekiama suderinti baudžiamosios materialinės teisės susijusios su elektroniniais nusikaltimais elementus. Taip pat sprendžiami procedūriniai teisiniai klausimai. Konvencija reikalauja valstybių narių nustatyti minimalias procesines priemones nacionaliniu lygmeniu, kurios vėliau per atitinkamas valstybės institucijas turėtų įgaliojimus vykdyti tam tikrų rūšių elektroninių nusikalstamų veikų tyrimus. Be to jos 22 straipsnyje yra įtraukta nuostata, suteikianti valstybėms jurisdikciją pažeidimams, padarytiems per tos valstybės teritoriją. Nors jurisdikcijos nuostatos Konvencijoje apibrėžtos išsamiai, tačiau tai valstybėms sukelia didžiulių problemų praktikoje. Todėl tai galima įvardinti, kaip pagrindinę kovos su elektroniniais nusikaltimais problemą, kurią autorius plačiau atskleis vėliau.

Konvencijoje numatyti vidaus baudžiamajam persekiojimui reikalingi įgaliojimai, tiriant ir persekiojant asmenis padariusius elektroninę nusikalstamą veiką. Tuo yra siekiama sukurti greitą ir veiksmingą tarptautinio bendradarbiavimo tvarką. Nepaisant to Konvencija dėl elektroninių nusikaltimų sukūrė teisinį pagrindą tarptautinės pagalbos dėl elektroninių nusikaltimų centrų tinklui 24/7. Todėl valstybės narės privalo paskirti kontaktinį punktą, prieinamą 24 valandas per parą, septynias dienas per savaitę, siekiant užtikrinti neatidėliotiną pagalbą tyrimams. Šio tinklo sukūrimas yra vienas iš svarbiausių Konvencijoje numatytų kovos priemonių, nes tik esant jam valstybės galėtų tinkamai reaguoti į teisėsaugos problemas, kylančias kovojant su elektroniniais nusikaltimais. Be to šis tinklas tūrėtų papildyti tarpvalstybinį bendradarbiavimą, nes kiekvienas toks

[39] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2014-01-05]

centras atliktų ne tik technines funkcijas, tai yra duomenų išsaugojimą ir įrodymų rinkimą, bet ir teisines konsultacijas. Sutartyje be visa ko yra reikalaujama, kad tokio nacionalinio centro darbuotojai būtų tinkamai apmokyti reaguoti į tokio pobūdžio nusikalstamas veikas ir kitų valstybių pagalbos kreipimusis.

Praėjus kiek laiko, Konvencija buvo papildyta papildomu protokolu dėl rasistinio ir ksenofobinio pobūdžio veikų, pasitelkiant kompiuterinius tinklus, kriminalizavimo.[40] Šio papildomo protokolo tikslas – kriminalizuoti rasistinio ir ksenofobinio pobūdžio veikas, atliktas kompiuterio pagalba naudojantis elektroniniais tinklais, įpareigoti valstybes bendradarbiauti tarpusavyje tiriant šias nusikalstamas veikas. Tačiau papildome protokole, kaip ir pačioje Konvencijoje numatyta, kad kiekviena valstybė siekiant sustabdyti tokio pobūdžio veikas priima tiesės aktus savo nuožiūra. 2007- 2008 metais Europos Taryba patikrino, ar yra reikalinga atskira teisinė priemonė kovojant su kompiuteriniu terorizmu, ir padarė išvadą, kad valstybės turi pilnai įgyvendinti visas Konvencijos dėl elektroninių nusikaltimų priemones, o tik po to kurti naujas tarptautines sutartis.[41] 2014 m. kovo mėnesį Konvenciją buvo pasirašiusios 50 valstybių, o ratifikavusios 41[42]. Kadangi iš viso yra beveik du šimtai valstybių autorius pritaria S. W. Brenner nuomonei, kad ši tarptautinė sutartis labai minimaliai įtakoja tarptautinę kovą su elektroniniais nusikaltimais[43]. Todėl autorius formuotų išvadą, kad Konvencija dėl šios priežasties nepasiekė savo juridinės populiarumo viršūnės.

Tačiau siekiant nustatyti Konvencijos dėl elektroninių nusikaltimų efektyvumą autorius savo pasirinkimu išanalizuos Konvencijos įtaką Didžiosios Britanijos, Jungtinių Arabų Emyratų ir JAV nacionaliniams įstatymams. Visų pirma bus nustatyta ar Konvencijos normos turi atitikmenis nacionaliniuose pasirinktų valstybių teisės aktuose. Taip pat ar nacionalinės normos keitėsi po Konvencijos įsigaliojimo ir, ar pilnai atitinka Konvencijos normas išdėstytas antrame - dešimtame Konvencijos straipsniuose.

Visų pirma tikslinga būtų trumpai apibudinti Konvencijos antrame – dešimtame straipsniuose įtvirtintas nuostatas:

- 2 – 6 straipsniai numato nusikalstamas veikas kompiuterinių duomenų ir sistemų konfidencialui, vientisumui ir prienamumui;
- 7 ir 8 straipsniai numato kompiuterinius nusikaltimus susijusius su klastojimu ir sukčiavimu;

[40] Additional Protocol to the Convention on Cybercrime, cornening the criminalisitaion of acts of a racist and xenophobic nature committes through computer systems. Strasbourg, 28.I.2003 http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm [žiūrėta 2014-01-05]
[41] Kostopoulos G.K. Cybercpace and Cybersecurity.// CRC Press, Taylor & Francis Group, 2013, p. 15.
[42] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-05]
[43] Brenner S.W. Cybercrime: Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010, p. 209.

- 9 straipsnis numato turinio nusikaltimus, arba tiksliau sakant nusikaltimus susijusius su vaikų pornografija;
- 10 straipsnis numato nusikalstamas veikas susijusias su autorių teisių ir gretutinių teisių pažeidimais;[44]

Be to svarbu atskleisti visų trijų valstybių su el. nusikaltimais susijusius nacionalinius teisės aktus, bei tai ar jos yra prisijungusios prie elektroninių nusikaltimų Konvencijos, jei taip tai - kaip ir kada jos tai padarė.

Didžioji Britanija pasirašė Konvencijos sutartį 2001 metais, tačiau ją ratifikavo tik praėjus dešimtmečiui.[45] D. Britanija buvo viena iš pirmųjų valstybių, kuri 1985 metais jau turėjo kompiuterinių nusikaltimų padalinį[46]. O 1990 metais priėmė Kompiuterių netinkamo naudojimo įstatymą (angl. Computer Misuse Act), kuris apibrėžė normas, procedūras ir sankcijas už veikas susijusias su neteisėta prieiga prie kompiuterinės sistemos[47]. O 1984 metais teisinė sistema jau turėjo duomenų apsaugos įstatymą, kuris aiškiai apibrėžė kaip duomenys privalo būti renkami, saugomi, atnaujinami ir naikinami. Tačiau kiek vėliau 2006 buvo pradėtas taikyti Policijos ir teisingumo aktas (angl. Police and Justice Act), kuris numatė su kompiuteriais susijusių nusikaltimų bausmių terminus, kriminalizavo DoS atakas ir nustatė programinės įrangos ir priemonių sąrašą, kuris gali būti naudojamas vykdant kompiuterinius nusikaltimus[48].

Jungtiniai Arabų Emyratai (JAE) yra federacinė valstybė, sudaryta iš septynių Emyratų. Ši valstybė nėra nei pasirašiusi, nei ratifikavusi 2001 Konvencijos dėl elektroninių nusikaltimų.[49] Teisinė JAE sistema yra grindžiama dviguba sistema, iš islamo, dar kitaip vadinamo šariatu, ir civilinės teisės. 2006 metais JAE priėmė pirmąjį savo nacionalinį teisės aktą dėl kovos su elektroniniais nusikaltimais pavadinimu JAE Federalinis Įstatymas Nr. (2) 2006 dėl prevencijos informacinių technologijų nusikaltimams.[50] Šį teisės aktą sudaro 29 straipsniai, nustatantys skirtingas nusikalstamas veikas.

---

[44] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2014-04-05]

[45] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-05]

[46] Computer Misuse Act 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents [žiūrėta 2014-04-05]

[47] Ten pat.

[48] Greek D. Change to Computer Misuse Act Worries Researchers. 2006. http://www.computeractive.co.uk/computeractive/news/2169530/changes-computer-misuse-act [žiūrėta 2014-04-06]

[49] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-06]

[50] United Arab Emirates, The Federal Law No. (2) on 2006 on The prevention of information Technology Crimes. http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf [žiūrėta 2014-04-06]

Jungtinės Amerikos Valstijos (JAV) yra sudarytos iš penkiasdešimties valstijų ir federalinė apygardos. Konvenciją jos pasirašė drauge su visomis kitomis pirmosiomis valstybėmis, tačiau ją ratifikavo tik 2006 metų rugsėjo pabaigoje.[51] Teisinė sistema JAV yra federalinė, kiekviena valstija turi savo unikalią teisinę sistemą ir galiojančius teisės aktus. Pagrindinis JAV teisės aktas dėl kompiuterinių nusikaltimų yra 1986 Kompiuterinio sukčiavimo ir piktnaudžiavimo aktas (Computer Fraud and Abuse Act 1986), dar žinomas, kaip JAV kodekso 1030 skirsnio 18 antraštė.[52] Šis teisės aktas pagrinde apima visas galimas nusikalstamas veikas, numatytas Konvencija dėl elektroninių nusikaltimų.

Nustačius pagrindinius visų trijų valstybių teisės aktus autorius pabandė surasti ir nustatyti ar Konvencijos 2-10 straipsniuose išdėstytos nusikalstamos veikos turi atitikmenis pasirinktų valstybių nacionaliniuose teisės aktuose. Todėl siekdamas lengviau atspindėti esamą situaciją autorius sudarė tikslią lentelę 2.1 su tikslia nuoroda į atitinkamos valstybės teisės aktą.

2.1 Lentelė pateikianti Konvencijos normų atitikmenis nacionaliniuose teisės aktuose.

| **2001 m. Konvencijos dėl elektroninių nusikaltimų straipsnis** | **Didžiosios Britanijos atitinkamas teisės aktas** | **Jungtinių Arabų Emyratų atitinkamas teisės aktas** | **Jungtinių Amerikos Valstijų atitinkamas teisės aktas** |
|---|---|---|---|
| 2 str. Neteisėta prieiga | Section 1 on Computer Misuse Act 1990 | Article 2 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Section 1030 (a) (1)- (5) |
| 3 str. Neteisėta perimtis | Regulation of Investigatory Powers Act 2000 | Article 8 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Sections 2510 - 2522 |
| 4 str. Poveikis duomenims | Section 3 on Computer Misuse Act 1990 | Article 6 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Section 1030 (a) (5) |
| 5 str. Poveikis sistemai | Section 3 on Computer Misuse Act 1990 | Article 5 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Section 1030 (a) (5) |
| 6 str. Netinkamas įtaisų naudojimas | Section 3A on Computer Misuse Act 1990 | _____ | USA Code Title 18 Sections 1029, 1030,1030 (a) (5) (A) |
| 7 str. Kompiuterinės klastotės | Section 2 on Computer Misuse Act 1990 | Article 7 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Sections 1029, 1037, 1028 |
| 8 str. Kompiuterinis sukčiavimas | Section 2 on Computer Misuse Act 1990 | Article 10, 11 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Sections 1029, 1030 (a) (4), 1343 |
| 9 str. Turinio nusikaltimai | Sexual Offences Act 2003 | Article 12, 23 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Sections 2251, 2252, 2252A |
| 10 str. Nusikaltimai susiję su autorių teisių ir gretutinių teisių pažeidimais | Copyright, Design and Patents Act 1988 | Article 23 on UAE Federal Law No 2 of 2006 | USA Code Title 18 Sections 1029, 1030, 2319 |

[51] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-06]

[52] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers http://www.law.cornell.edu/uscode/text/18/1030 [žiūrėta 2014-04-06]

Kaip matome iš pateiktos 2.1 lentelės didžioji dalis Konvencijoje įtvirtintų nusikalstamų veikų kriminalizuotos visose trijose valstybėse. Išimtis yra Jungtiniai Arabų Emyratai, kurie nėra apsibrėžę tokios draudžiamos veikos, kaip netinkamas prietaisų naudojimas. Bet tai vertinant derėtų dar kartą paminėti, kad Jungtiniai Arabų Emyratai nėra nei pasirašę, nei prisijungę prie autoriaus analizuojamas Konvencijos[53]. Visų antrą iš sudarytos 2.1 lentelės yra matoma, kad nėra nei vieno konkretaus teisės akto, kuris reglamentuotų visas nusikalstamas veikas iš elektroninių nusikaltimų Konvencijos.

Siekiant pilnai atskleisti ir įvertinti 2001 metais priimtos Konvencijos efektyvumą ir įtaką Didžiosios Britanijos, JAV ir JAE teisinei sistemai, buvo pasirinka įvertinti teisės aktų pasikeitimą po Konvencijos pasirašymo ir įsigaliojimo. Todėl atsižvelgiant į tai autorius pateikia 2.2 lentelę, kurioje pažymėta, kurios teisės normos keitėsi priėmus Konvenciją ir šiuo metu pilnai atitinką jos 2-10 straipsniuose pateiktas normas.

2.2 Teisės aktų keitimosi ir atitinkamumo Konvencijos normoms lentelė.

| **2001 m. Konvencijos dėl elektroninių nusikaltimų straipsnis** | **Didžioji Britanija** | **JAE** | **JAV** |
|---|---|---|---|
| 2 str. Neteisėta prieiga | *X* | *X* | *X* |
| 3 str. Neteisėta perimtis | | | *X* |
| 4 str. Poveikis duomenims | *X* | *X* | *X* |
| 5 str. Poveikis sistemai | *X* | | *X* |
| 6 str. Netinkamas įtaisų naudojimas | | | *X* |
| 7 str. Kompiuterinės klastotės | *X* | | *X* |
| 8 str. Kompiuterinis sukčiavimas | | | *X* |
| 9 str. Turinio nusikaltimai | *X* | *X* | *X* |
| 10 str. Nusikaltimai susiję su autorių teisių ir gretutinių teisių pažeidimais | *X* | *X* | *X* |

Iš pateiktos lentelės matyti, kad JAV nacionaliniuose teisės aktuose įtvirtintos normos atspindi pilną suderinamumą su Konvencijos dėl elektroninių nusikaltimų 2 – 10 straipsniuose pateiktomis normomis. Be to, Jungtinės Amerikos Valstijos yra viena iš keturių ne Europos Tarybos valstybių, kuri dalyvavo kuriant Konvenciją. Taip pat iš pateiktos lentelės matyti, kad Didžiosios Britanijos nacionalinės teisės normos įgyvendina tik pusę Konvencijos pateiktų teisės normų. Esant tokiai situacijai autorius daro prielaidą, kad tokia situacija yra dėl vėlyvo Konvencijos

[53] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-06]

ratifikavimo, t.y. tik 2011 metais.[54] UAE nacionalinės normos yra mažiausiai atitinkančios Konvencijos normas, bet vertinant efektyvumą į šią valstybę nereikėtų kreipti dėmesio, nes ji nėra prisijungusi prie Konvencijos.

Apibendrinant galime teigti, kad Konvencija nesukūrė tokių teisinės kovos priemonių su elektroniniais nusikaltimais, kokių iš jos buvo tikėtasi. Pagrindinės to priežastys yra santykinai mažas sutartį pasirašiusių ir ratifikavusių valstybių skaičius[55], sunkiai valstybių įgyvendinamos technologinės ir procesinės priemonės. Konvencijos efektyvumas santykinai proporcingas valstybės pasirašymo ir ratifikavimo momentui, bei įtakai šios srities tarptautinėje teisėkūroje.

### 2. 1. 2. Reakcija į elektroninių nusikaltimų Konvenciją.

Konvencijos dėl elektroninių nusikaltimų įsigaliojimui priešinosi daugelis civilinių laisvių grupių. Jos baiminosi, kad Konvenciją ratifikavusiose valstybėse naujai sukurtos tyrimų institucijos ir padidėjęs tarpvalstybinis bendradarbiavimas teisėsaugos srityje palies civilių privatumą ir kitas teises.[56] Kaip rašo J. Pryce privatus- verslo sektorius neturėjo konkretaus požiūrio.[57] Autorių teisių savininkai tvirtai palaikė Konvenciją, tačiau interneto paslaugų teikėjai ir kitų tinklų operatoriai išreiškė susirūpinimą, kad su šia Konvencija jiems galimai yra priskiriama našta, rinkti informaciją apie abonentus ir saugoti srauto duomenų informaciją[58]. Metams bėgant opozicija buvo prislopinta, tačiau neaišku, ar tai įvyko dėl nepasitvirtinusių išankstinių abejonių, ar dėl to, kad Konvencija ir po jos sekę veiksmai šiuo metu yra jau įvykę faktai daugelyje valstybių.

Tačiau viena iki šiol pastebima opozicijos lyderė yra Rusija. Nepaisant to, kad ji yra Europos Tarybos narė, ji nėra pasirašiusi Konvencijos dėl elektroninių nusikaltimų ir tuo labiau jos ratifikavusi[59]. 1990 metų viduryje Rusija Jungtinėms Tautoms pasiūlė kibernetinės ginklų kontrolės sutartį, siekiant apriboti valstybių kibernetinių ginklų panaudojimo ribas. Remiantis Konvencija, Rusija prieštaravo nuostatai, pagal kurią vienašalis tarpvalstybinis teisėsaugos institucijos priėjimas prie kompiuterių ar kompiuterinių duomenų yra galimas be kompiuterio ar kompiuterinių duomenų

[54] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-06]
[55] Ten pat.
[56] Pryce J. Convention on Cybercrime.// Privacy & Security Law Report. Vol 5, No. 1, BNA, Inc., 2006 October 16, p. 1451.
[57] Ten pat.
[58] International Cybercrime Treaty https://www.aclu.org/technology-and-liberty/international-cybercrime-treaty [žiūrėta 2014-01-06]
[59] Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG [žiūrėta 2014-04-06]

savininko sutikimo, interpretuodama tai, kaip nacionalinio suvereniteto pažeidimą.[60] Tačiau iki šiol egzistuoja nepaneigta nuomonė, kad tikroji Rusijos neprisijungimo prie Konvencijos dėl elektroninių nusikaltimų priežastis yra noras išvengti tarpvalstybinio bendradarbiavimo tiriant elektroninius nusikaltimus[61], atsižvelgiant į tai, kad daugybė elektroninių nusikalstamų veikų padaroma būtent iš šios valstybės.

Jungtinių Tautų narkotikų ir nusikalstamumo biuras išreiškė rekomendaciją, kad Konvencijos dėl elektroninių nusikaltimų plėtra turi būti svarstoma palankiai tik atsargiai įvertinus visus kriterijus.[62] Šio biuro teigimu Europos Tarybos Konvencijos pasirašymas atspindi visą valstybės tautos pažangą, o ne valstybė pritarimą ar nepritarimą[63]. Tarptautinė telekomunikacijų sąjunga (toliau – ITU), Jungtinių Tautų agentūra, atsakinga už informacijos ir komunikacijos technologijų klausimus, taip yra išreiškusi abejotiną nuomonę, ar Konvenciją reikėtų laikyti kaip pasaulinį standartą. ITU generalinis sekretorius H. Taure yra paminėjęs, kad Konvencija buvo išimtinai sukurta Europos Tarybos narių ir keturių stebinčių valstybių, todėl ji dabar „šiek tiek dulkėta".[64] Kaip alternatyvą, ITU parėmė „ITU įrankių rinkinys elektroninių nusikaltimų teisės aktams" kūrimą.[65] Rinkinio tikslas buvo suderinti nacionalinius teisės aktus, nereikalaujant tautos prisijungimo prie šios plačiai nagrinėjamos tarptautinės sutarties.

Europos Taryba atsiribojo nuo visos kritikos ir pasiūlė verčiau jungtis prie Konvencijos, nei „išradinėti dviratį".[66] Europos Tarybos generalinis sekretorius pareiškė, kad Konvencija susilaukė didelio pritarimo ir iniciatyvos iš Azijos ir Ramiojo vandenyno šalių bendradarbiavimo, Europos Sąjungos, Interpolo, JAV ir kitų organizacijų, taip pat privataus sektoriaus.[67] Be to, Europos Tarybos ekspertų su terorizmu komitetas nurodė, kad atskira tarptautinė sutartis, siekiant kovoti su kompiuteriniu terorizmu nėra reikalinga, nors tai reglamentuojančios teisinės kovos priemonės jau yra įtrauktos į Konvenciją dėl elektroninių nusikaltimų.[68] Komitetas pabrėžė, kad dabartiniame etape pagrindinis dėmesys turėtų būti skiriamas užtikrinti veiksmingą Konvencijos egzistavimą.

---

[60] Markoff J., Kramer A. In Shift, U.S Talks to Russia on Internet Security.http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0 [žiūrėta 2014-01-07]
[61] Ten pat.
[62] Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf [žiūrėta 2014-01-07]
[63] Ten pat.
[64] ITU will IP-Adressen verwalten http://www.heise.de/netze/meldung/ITU-will-IP-Adressen-verwalten-835928.html [žiūrėta 2014-01-07]
[65] ICT Regulation Toolkit http://www.itu.int/itudoc/gs/promo/bdt/flyer/87876.pdf [žiūrėta 2014-01-08]
[66] International Cyberspace Strategies http://www.nsci-va.org/WhitePapers/2010-06-28-InternationalCyberspaceStrategies-Stephens-McKee.pdf [žiūrėta 2014-01-07]
[67] Contribution og the Secretary general of the council of Europe. To the Twelfth United Nations Congress on Crime prevention and Criminal Justice. Salvador, Brazil, 12-19 April 2010 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf [žiūrėta 2014-01-07]
[68] Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyberterrorism and Use of Internet for Terrorist Purpose http://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf [žiūrėta 2014-01-08]

Todėl komitetas rekomendavo, Europos Tarybą aktyviau raginti valstybes prisijungti prie Konvencijos dėl elektroninių nusikaltimų.[69]

Apibendrinant, Konvencija dėl elektroninių nusikaltimų priešiško požiūrio į save susilaukė natūraliai proporcingai, kaip ir kiti panašūs tarptautiniai teisės aktai. Svarbu atsižvelgti į tai, kad kai kurių valstybių požiūris į šią tarptautinę sutartį yra įprastas atsakas į bet kokį ne jų inicijuotą veiksmą, kuris bent kiek mažintų jų galią. Verslo sektoriaus reakcija yra akivaizdžiai suprantama, nes kiekvienos naujos funkcijos įgyvendinimas reiškia pelno dalies atsisakymą.

### 2. 1. 3. Jungtinių Tautų Konvencija prieš tarptautinį organizuotą nusikalstamumą.

Jungtinių Tautų Konvencija prieš tarptautinį organizuotą nusikalstamumą (TOC) buvo patvirtinta 2000 metų lapkričio 15 dieną, Generalinės Asamblėjos rezoliucija 55/25.[70] Tai pagrindinė tarptautinė sutartis, kovojanti su tarptautiniu organizuotu nusikalstamumu. Ja siekiama skatinti tarptautinį bendradarbiavimą siekiant užkirsti kelią tarptautiniam organizuotam nusikalstamumui.

Ši konvencija nenumato vieningos organizuoto nusikalstamumo sąvokos, tačiau nustato sampratos elementus. Organizuota grupė apibrėžiama kaip trijų ar daugiau asmenų grupė, įsipareigojusi kartu atlikti vieną ar kelis sunkius nusikaltimus, su tikslu gauti finansinės arba kitokią materialinę išraišką turinčios naudos. Tarptautinis nusikaltimas apibrėžiamas, kaip nusikalstama veika atlikta daugiau nei vienoje valstybės teritorijoje. O sunkus nusikaltimas šioje sutartyje apibrėžiamas kaip veikla, kuria baudžiama maksimalia laisvės atėmimo bausme nuo keturių ir daugiau metų.

Konvencija prieš tarptautinį organizuotą nusikalstamumą kaip ir Konvencija dėl elektroninių nusikaltimų savaime pati yra teisinės kovos priemonė su elektroniniais nusikaltimais tarptautiniu mastu. Tačiau jos įgyvendinimas išlieka problematiškas, nes valstybėms ir toliau nurodoma vadovautis pagrindiniu vidaus teisės principu[71], kuris reiškia, kad valstybės Konvencijos nuostatas perkelia į nacionalinius baudžiamuosius teisės aktus savo nuožiūra. Todėl galima daryti išvadą, kad Jungtinių Tautų Konvencija prieš tarptautinį organizuotą nusikalstamumą yra tik papildanti priemonė Konvencijai dėl elektroninių nusikaltimų.

---

[69] Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyberterrorism and Use of Internet for Terrorist Purpose
http://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf [žiūrėta 2014-01-08]

[70] Jungtinių Tautų konvencija prieš tarptautinį organizuotą nusikalstamumą. Valstybės žinios. 2002-05-22, Nr. 51-1933. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=166679 [žiūrėta 2014-01-10]

[71] Ten pat.

## 2. 2. Regioniniai teisės aktai

Nors tai yra gana įgrisę, tačiau mes gyvename skaitmeniniame amžiuje. Kasdienis gyvenimas jau dabar neatsiejamas nuo išmaniųjų telefonų ar planšetinių kompiuterių, kurių pagalba mes ne tik bendraujame tarpusavyje vieni su kitais, bet ir apsipirkinėjame ar vykstame iš taško A į tašką B. Nors visa tai atrodo gana teigiamai, tačiau tai sudarė puikias prielaidas naujo pobūdžio nusikaltimams. Todėl su tokio pobūdžio „besieniais“ nusikaltimais J. Clough vienareikšmiškai siūlo kovoti pasitelkiant tik teisės aktus, galiojančius regioniniu arba tarptautiniu mastu.[72]

### 2. 2. 1. Europos Sąjungos teisės aktai ir regioninių priemonių problema

Norint išanalizuoti teisines priemones, kuriomis siekiama kovoti su elektroniniais nusikaltimais tarptautiniu mastu reikėtų apžvelgti Europos Sąjungos institucijų išleistus teisės aktus. 1989 metais Europos Taryba priėmė Rekomendaciją Nr. R(89)9, kuria Europos Tarybos valstybės narės kviečiamos atsižvelgti į ekspertų komiteto paruoštą ataskaitą kuriant įstatymus, susijusius su kompiuteriniais nusikaltimais. Šioje rekomendacijoje esminiu punktu buvo nusikalstamų veikų, susijusių su kompiuteriais, sąrašo pateikimas. Tačiau viskas buvo valstybių apsisprendimo laisvėje, valstybės narės nevaržomos galėjo apsispręsti, pasinaudoti šia rekomendacija ar ne.

Vėliau 1995 metų rugsėjį buvo priimta Rekomendacija Nr. R(95)13, kuria siekiama įtvirtinti naujus baudžiamojo proceso veiksmus, kurie būtų taikomi tiriant būtent elektroninius nusikaltimus.[73] Rekomendacijoje nurodyti šie nauji procesiniai principai: krata ir poėmis, telekomunikacijų kontrolė, pareiga bendradarbiauti, elektroninė įrodymų forma, šifravimo kūrimas ir panaudojimas, profesiniai mokymai ir tarpvalstybinis bendradarbiavimas. Tačiau praėjus beveik dviem dešimtmečiams efektyvus tarpvalstybinis bendradarbiavimas dar nėra pasiektas.

2001 metų sausio 26 dienos komunikatas – Saugesnės informacinės visuomenės kūrimas, gerinant informacinių infrastruktūrų saugą ir kovą su nusikaltimais, susijusiais su kompiuteriais. KOM (2000)890.[74] Komunikate be siūlomo nusikalstamų veikų klasifikavimo, buvo nurodytos ir konkrečios teisinės priemonės, kurių valstybės privalo imtis kovojant su elektroniniais nusikaltimais. Viena iš priemonių buvo nacionalinės baudžiamosios teisės harmonizavimas. Kita nurodyta teisinė priemonė buvo procesinės teisės suvienodinimas, kurio akivaizdi nauda atsiskleistų tiriant nusikalstamas veikas.

---

[72] Clough J. Principles of Cybercrime.// New York, USA, Cambridge University Pres, 2010, p. 3.
[73] Council of Europe Recommendation No. R(95) 13
http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp [žiūrėta 2014-01-10]
[74] Commission of the European Communities COM (2000) 890
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF [žiūrėta 2014-01-12]

2007 metų komunikatas KOM(2007)267 galutinis, Bendros politikos, skirtos kovoti su elektroniniais nusikaltimais linkme[75] buvo pagrindas skatinti Europos Sąjungos valstybes bendradarbiauti tarpusavyje ir taip efektyviau kovoti su plintančiais elektroniniais nusikaltimais. Tačiau komunikatas, susirūpinus esama bloga infrastruktūros apsauga buvo paskelbtas 2009 metais kovo 30 dieną. Tai buvo Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų Komitetui bei Regionų Komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos - „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo- geresnė parengtis, didesnis saugumas ir atsparumas" – KOM(2009)149 galutinis.[76] Kaip kibernetinių atakų pavyzdys buvo paminėtas 2007 metų antpuolis prieš Estiją, šį atvejį autorius plačiau išanalizuos kitoje dalyje. Komunikate dėmesys skiriamas prevencijai, parengčiai, informavimui ir veiksmų planams, jei tokio pobūdžio išpuoliai įvyktų valstybėje. Todėl jame buvo pateiktas veiksmų planas, kurio reikėtų imtis siekiant užkirsti kelią kibernetiniams išpuoliams, o jei nuo to nepavyktų apsisaugoti, tai veiksmams, kurių reikėtų imtis, siekiant pilnai išaiškinti tokio tipo nusikalstamą veiką.

2013 metų rugpjūčio 12 dieną priima Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas[77]. Ši direktyva pakeičia 2005 metų Europos Taryba priimtą pamatinį sprendimą, dėl atakų prieš informacines sistemas Nr. 2005/222/JHA. Direktyvos tikslas yra suderinti valstybių narių baudžiamosios teisės normas dėl atakų informacinių sistemų srityje, nustatant būtinąsias taisykles, susijusias su nusikalstamų veikų apibrėžtimi, ir atitinkamas sankcijas šioje srityje. Taip pat pagerinti valstybių narių atsakingų institucijų, policijos ir kitų teisėsaugos institucijų, Eurojusto, Europolo ir Europos kovos su elektroniniais nusikaltimais centro bei Europos tinklų ir informacijos apsaugos agentūros ENISA bendradarbiavimą.

Atsižvelgiant į tarptautinį šios rūšies nusikaltimų pobūdį, nacionalinių teisės aktų ir kovos metodų suderinimas yra gyvybiškai svarbus kovojant su visais elektroniniais nusikaltimais. Tačiau anot M. Gercke nacionalinis teisinis harmonizavimas turi vykti tik atsižvelgiant į esamą regioninę situaciją, iššūkius ir gebėjimus[78]. Vadinasi nei viena valstybė negali priimti tam tikrų nacionalinių teisės normų, neorientuodama jų į esamą kriminogeninę padėtį ar regioninę situaciją. Autorius su tokia nuomone nesutinka, nes tokia situacija būtų ironiška, jei tarkim viena valstybė tam tikrame regione būtų pastoviai atakuojama elektroninių nusikaltimų iš visų ją supančių kaimyninių valstybių, tačiau jos visos būtų tos pačios regioninės organizacijos narės. Regioninių kovos

[75] Europos Komisijos komunikas KOM (2007) 267 galutinis http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF [žiūrėta 2014-01-12]
[76] Europos Komisijos komunikas KOM (2009) 149 galutinis http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:LT:NOT [žiūrėta 2014-01-12]
[77] Europos Parlamento ir Tarybos direktyva 2013/40/ES http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT [žiūrėta 2014-01-12]
[78] Gercke M. Understanding Cybercrime: A Guide for Developing Coutries.// ITU Telecommunication Development Sector Second Edition. 2011.

priemonių svarba su elektroniniais nusikaltimais pabrėžiamas tik per tarptautines regionines organizacijas, tokias kaip EBPO, ES, AOS ir kt. Steino Schjolbergo manymu šiuo metu egzistuoja tik keturios privalomos regioninių organizacijų sukurtos teisinės kovos su elektroniniais nusikaltimais priemonės:

- Europos Tarybos Konvencija dėl elektroninių nusikaltimų;
- Arabų valstybių lygos Konvencija dėl kovos su informacinių technologijų nusikaltimais;
- Nepriklausomų valstybių sandraugos susitarimas dėl kovos su nusikaltimais, susijusiais su kompiuterine informacija;
- Šanchajaus bendradarbiavimo organizacijos susitarimas dėl informacijos saugumo;[79]

Remiantis šia S. Schjolbergo nuomone, net 82 valstybės yra pasirašiusios ir ratifikavusios privalomą kovos su elektroniniais nusikaltimais priemonę. Tačiau jo teigimu, jos privalo turėti ne tik normas perkeltas iš egzistuojančių regioninių priemonių, bet ir nacionalines, individualiai kiekvienai tautai pritaikytas baudžiamosios teisės normas.[80] Visų valstybių kriminogeninė situacija yra skirtinga, ją gali įtakoti tokie pašaliniai rodikliai, kaip pragyvenimo lygis, darbo užmokestis, ekonominė padėtis, bankų stabilumas ir kita. Todėl nevertėtų kovą su nusikaltimais vertinti padidintu masteliu, tai yra regioniniu mastu, taip apribojant nacionalines priemones.

Reziumuojant esamas regionines teisines kovos priemones, atsižvelgiant į labiausiai mums aktualias Europos Sąjungos sukurtas teisines priemones, galime teigti, kad pagrindinės akcentuojamos ir siekiamos teisinės kovos priemonės su elektroninėmis nusikalstamomis veikomis visuomet buvo tarptautinis bendradarbiavimas ir teisės normų harmonizavimas. Tačiau greta skatinamų priemonių egzistuoja teisinis savarankiškumo principas, kuris reiškia kad valstybės teisines priemones į nacionalinius įstatymus perkelia nepriklausomai, savo nuožiūra. Paantrinant jau išsakytai S. Scjolbergo nuomonei, greta tarptautinių-regioninių organizacijų kuriamų neprivalomų priemonių pasaulyje galioja tik keturios privalomos regioninės teisinės priemonės. Tačiau jomis apsiriboti negalima, nes kiekviena valstybė, tauta, ekonominiai ir socialiniai rodikliai, įtakojantys esamą kriminogeninę situaciją yra skirtingi.

[79] Schjolberg S. Crossing jurisdictional boundaries.// The Hague, The Netherlands, 2013, p 3.
[80] Ten pat.

### 2. 2. 2. Naujo teisės akto prieš elektroninius nusikaltimus tarptautiniu mastu svarstymas.

Praėjus daugiau nei dešimtmečiui po Konvencijos dėl elektroninių nusikaltimų priėmimo vis dažniau pradedama kalbėti apie naują pasaulinį teisės aktą, kuris galėtų būti veiksmingesnė teisinė priemonė kovojant su tarptautiniais elektroniniais nusikaltimais, nei esama 2001 metų Konvencija dėl elektroninių nusikaltimų. Pagrindinės to priežastys yra nepasitvirtinusi Konvencija dėl elektroninių nusikaltimų ir nesustabdomas vis naujos pažeidžiamos informacinės visuomenės formavimasis.

Naujo pasaulinio teisės akto pagrindinis uždavinys būtų tinkamai apibrėžti elektroninius nusikaltimus ir su jais susijusias nusikalstamas veikas. M. Kiškio ir D. Štitilio teigimu, elektroninės technologijos sparčiai vystosi ir keičiasi, todėl metodai ir modeliai tobulėja, esamos nusikalstamos veikos nebeatitinka Konvencijoje įtvirtintų nuostatų.[81] Tačiau, autoriaus nuomone, elektroninių nusikaltimų sąvoka negali būti apibrėžta per daug griežtai, atsižvelgiant į teisėje egzistuojančius atvirumo ir lankstumo principus. Visiems yra gerai žinoma, kad iki šiol nėra visuotinai priimtos vieningos elektroninių nusikaltimų sąvokos.[82] Tačiau pažodžiui, elektroniniai nusikaltimai reiškia nusikalstamą veiką, susijusią su elektronine erdve, internetu, kompiuteriu ir kompiuteriniais tinklais ar kita informacine sistema. Todėl elektroninis nusikaltimas nebegali būti siejamas tik su kompiuteriu ir internetu, kaip buvo anksčiau. Šiandien elektroninį nusikaltimą turėtų atspindėti žodžiai: informacinės sistemos ir duomenys. Informacinė sistema dažniausiai yra apibrėžiama kaip bet koks prietaisas arba tarpusavyje sujungti prietaisai, kuris pagal specialią programą vykdo automatinį duomenų apdorojimą.[83] O duomenys yra kokie nors faktai, pateikti tokia forma, kuri yra pritaikyta tvarkyti informacinėje sistemoje, įskaitant programą galinčią atlikti šią funkciją.[84] Remiantis šiais dviem labai svarbiais šiandienai apibrėžimais įtvirtintais Konvencijoje dėl elektroninių nusikaltimų, planšetinis kompiuteris, išmanusis telefonas ar išmanusis televizorius (angl. SMART TV) taip pat yra informacinės sistemos. Todėl galima daryti išvadą, kad riba tarp informacinės sistemos ir telekomunikacijų sistemos tampa visiškai menkavertė. Išmanieji mobilieji telefonai tikrai yra mini informacinės sistemos, gebančios apdoroti duomenis ir atlikti pilną spektrą kitų intelektualių veiksmų, todėl nusikalstamos veikos, susijusios su mobiliais telefonais, autoriaus nuomone, turėtų būti įtrauktos į naują elektroninių nusikaltimų apibrėžtį.

---

[81] Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. Teisės informatika ir informatikos Teisė.// Vilnius, Mykolo Romerio Universitetas, 2006, p. 230.
[82] Štitilis D. Elektroniniai nusikaltimai.// Vilnius, Mykolo Romerio Universitetas, 2011, p. 33-45.
[83] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2013-12-10]
[84] Ten pat.

Sekanti teisinė priemonė, kuriai reikėtų skirti didelį dėmesį, J. Vogel manymu, yra prevencija[85]. Tai yra naujas teisinis iššūkis elektroninių nusikaltimų srityje.[86] Valstybių teisėsaugos institucijos negali tirti ir patraukti baudžiamojon atsakomybėn mažareikšmių nusikalstamų veikų, todėl elektroninis saugumas priklauso beveik tik nuo prevencijos. Baudžiamoji teisė yra ta priemonė, kuri priverčia nuo aklos kovos su elektroniniais nusikaltimais judėti link apibrėžto ir aiškaus elektroninio saugumo stiprinimo.[87] Pastaraisiais metais J. Vogel teigimu vis didesnis dėmesys skiriamas:

- Informacinių sistemų „grūdinimui". Labai svarbu žinoti sistemų spragas ir elektronines nusikalstamas veikas atliekančių asmenų gebėjimus.
- Apsaugoti elektroninio bendradarbiavimo šifravimą pasitelkiant elektroninį parašą ir kitas saugos priemones.
- Didinti visuomenės sąmoningumą, taip kovojant su turinio nusikaltimais, tai yra vaikų pornografija ir šmeižtu. [88]

2001 metų Konvencija dėl elektroninių nusikaltimų, tai tarptautinė sutartis inicijuota Europos Tarybos, kuri nėra Europos Sąjungos institucija. Nepaisant to, dauguma prie šios sutarties prisijungusių ir ją ratifikavusių valstybių yra Europos valstybės, dabartinės Europos Sąjungos narės, tačiau neskaitant Rusijos, kur yra tik Europos Tarybos narė. ITU generalinio sekretoriaus Hamadoun Toure nuomone, galiojanti Konvencija yra daugiau regioninis teisės aktas[89]. Dėl tos priežasties prie Konvencijos jungėsi ir ją ratifikavo mažiau valstybių, nei buvo tikimasi. O ir pati Konvencija nepasiekė tokio efektyvumo, kokio buvo iš jos tikėtasi. Dauguma šios srities mokslininkų beveik vieningai pritarė Hamadoun Toure teiginiui, kad vargu ar kada nors vėliau pavyks sukurti kita tarptautinį teisės aktą, kuris bus veiksmingesnis nei dabar galiojanti Konvencija[90]. Visuomet išsiskirdavo valstybių interesai ir norai, taip bus ir ateityje, todėl autorius siūlytų apsiriboti esama Konvencija o ja tobulinti leidžiamais naujais papildomais protokolais. Thorbjorn Jagland teigia, kad Konvencija dėl elektroninių nusikaltimų susilaukė deramos paramos iš EBPO, AOS, Interpolo ir kitų tarptautinių organizacijų, priimdamos organizacinius teisės aktus ir rekomendacijas identiškai panašias į teisės normas įtvirtintas galiojančioje Konvencijoje[91]. Tokiai

[85] Vogel J. First World Conference of Penal Law// Mexico, November 2007.
[86] Europos Komisijos komunikas KOM (2007) 267 galutinis http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF [žiūrėta 2014-01-12]
[87] Vogel J. First World Conference of Penal Law// Mexico, November 2007.
[88] Ten pat.
[89] ITU will IP-Adressen verwalten http://www.heise.de/netze/meldung/ITU-will-IP-Adressen-verwalten-835928.html [žiūrėta 2014-01-12]
[90] Ten pat.
[91] Protecting Youyou're your Rights in Cyberspace: Minimising the Risks, Maximising the Freedom http://en.collaboratory.de/w/Protecting_You_and_Your_Rights_in_Cyberspace:_Minimising_the_Risks,_Maximising_the_Freedom [žiūrėta 2014-01-14]

nuomonei pritaria ir autorius, todėl tarptautinių organizacijų kuriamos teisinės kovos priemonės bus apžvelgtos vėliau.

Apibendrinant, galima teigti, kad elektroninė erdvė be pažeidimų yra mažai tikėtinas rezultatas, tačiau negalime pamiršti, kad saugumo didinimas ir prevencija informacinėse sistemose ar internete neturėtų pažeisti pagrindinių žmogaus teisių, tai yra teisės į judėjimo ir žodžio laisvę. Naujos tarptautinės sutarties ar tarptautinio teisės akto reikalingumas negali būti grindžiamas nepasiteisinusia Konvencija dėl elektroninių nusikaltimų, nes jokia teisėta teisės forma negali būti grindžiama prievarta, šiuo atveju priverstiniu prisijungimu o vėliau ir priverstine teisės normų harmonizacija. Todėl efektyviausia yra palikti galiojančią 2001 metų Konvencija dėl elektroninių nusikaltimų, o teisines spragas papildyti leidžiamais naujais papildomais protokolais.

### 2. 3. Tarptautinių organizacijų kuriamos priemonės

Didžiausias iššūkis yra sekti kartu su elektroninių nusikaltimų pažangą, taip kad nusikalstamų veikų tyrimas ir baudžiamasis persekiojimas žengtų su jais kartu. Kiekvienas nusikalstamos veikos atvejis yra unikalus, todėl su juo reikia kovoti individualiai, tai veikai pritaikytomis priemonėmis. Todėl kartais nacionaliniai teisės aktai ir juose įtvirtintos teisinės priemonės būna neveiksmingos ir reikia pasikliauti tarptautinių organizacijų siūlomomis priemonėmis. Nes būtent tarptautinės organizacijos nuolat stebi nusikalstamų veikų pokyčius, steigia darbo grupes, kuria strategijas, skirtas kovoti su šio pobūdžio nusikaltimais ir leidžia organizacinius aktus su įtvirtintomis nuostatomis dėl kovos su elektroniniais nusikaltimais tarptautiniu mastu. Todėl toliau autorius apžvelgs tarptautinių organizacijų kuriamas teisines kovos priemones.

#### 2. 3. 1. Jungtinės Tautos

1948 metais, Jungtinių Tautų Organizacija - JTO įsteigė savo pirmąjį biurą kovoti su tarptautiniu nusikalstamumu. O šiandien, JTO jau gali spręsti vis svarbesnes tarptautines problemas, įskaitant ir tas, kurias kelia organizuoto nusikalstamumo veikla. Remiantis EBPO pateikta ataskaita, kurią autorius aptars vėliau, JTO sušaukė aštuntą Jungtinių Tautų kongresą dėl nusikaltimų prevencijos ir elgesio su nusikaltimais, siekiant spręsti tarptautinius teisinius iššūkius kylančius iš elektroninių nusikaltimų. Kongresas sukūrė rezoliuciją, raginančią visas JTO valstybes nares dėti daugiau pastangų kovojant su elektroniniais nusikaltimais ir modernizuoti savo nacionalinius baudžiamuosius įstatymus, prireikus pagerinti kompiuterių saugumo ir prevencijos priemones,

skatinti baudžiamąjį persekiojimą, konfiskavimą ir restituciją neteisėtai įgytam turtui, iš kompiuterinių nusikaltimų veiklos.[92]

1995 metais, JTO paskelbė vadovą „Prevencija ir kontrolė su kompiuteriais susijusiems nusikaltimams".[93] Rinkinys reglamentavo kompiuterinius nusikaltimus, teisės aktus saugančius duomenų ir informacijos savininkus, privatumą, procesinę teisę ir tarptautinį bendradarbiavimą. JTO vadovas skirtas ne tik grėsmei kylančiai iš elektroninių nusikaltimų, bet ir kitoms nusikalstamoms veikoms, lengvai kertančioms valstybių sienas. Valstybės pripažindamos, kad organizuotas nusikalstamumas tapo ne vienos valstybės problema, JTO sujungė jėgas ir pasiūlė Jungtinių Tautų Konvenciją prieš tarptautinį organizuotą nusikalstamumą.[94] Konvencija nustato bendras sąlygas skirtingoms teisinėms sistemoms, kurios egzistuoja kiekvienoje valstybėje, ir pabrėžia, kaip svarbu yra kurti vieningas, teisiškai privalomas priemones, siekiant įveikti problemas, atsirandančias tarpusavyje susiduriant tarptautinio bendradarbiavimo ir savitarpio pagalbos situacijose.

Be to, JTO ėmėsi ir papildomų iniciatyvų kovoti su tarptautiniu kibernetiniu nusikalstamumu. 2000 metais Vienoje, Jungtinės Tautos savo dešimtąjį kongresą skyrė prevencijai ir elgesiui su nusikaltėliais, susijusiais su kompiuteriniai tinklais. Kongreso metu vyko techninis seminaras skirtas kompiuterinių nusikaltimų prevencijai. Tačiau šio kongreso metu pasiūlytos kovos ir prevencijos priemonės, kaip ir kitos JTO kuriamos priemonės į priekį judėjo labai lėtai. Dažnai tarptautinių sutarčių, tokių kaip konvencija kūrimas ir ratifikavimas užtrunka dešimtmečius, todėl jų kaip priemonių efektyvumas yra menkas. Tačiau nepaisant to, S. Ghosh nuomone, Jungtinių Tautų kova su elektroniniais nusikaltimais tarptautiniu mastu yra itin svarbi siekiant sveikos civilizacijos[95] .

Tarptautinė telekomunikacijų sąjunga - ITU buvo įkurta Jungtinių Tautų, kaip specializuota telekomunikacijų agentūra[96]. Ši agentūra prižiūri pasaulinį telekomunikacijų naudojimąsi ir gerina telekomunikacijų infrastruktūrą besivystančiose šalyse[97]. ITU aptariami kompiuterinio saugumo stiprinimo klausimai. Remiantis Jungtinių Tautų Generaline rezoliucija dėl kovos su nusikaltimais informacinių technologijų srityje. 2009 metais ITU išleido savo teisės aktų elektroniniams nusikaltimams rinkinį, siekiant suteikti valstybėms pamatinės teisėkūros medžiagos, kuria remiantis

[92] Eight U.N. Congress on the Prevention of Crime and the Treatment of Offenders. 1990 September 4. http://www.asc41.com/UN_congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf [žiūrėta 2014-01-08]
[93] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime http://www.uncjin.org/Documents/EighthCongress.html [žiūrėta 2014-01-15]
[94] U.N and Cybercrime http://www.ictparliament.org/node/2128 [žiūrėta 2014-01-15]
[95] Ghosh S, Turrini E. Cybercrimes: A Multidisciplinary Analysis.// Springer, 2010, p. 328.
[96] International Telecommunication Union. http://www.itu.int/net/about/ [žiūrėta 2014-01-15]
[97] Ten pat.

gali būti sukurti nauji įstatymai reglamentuojantys elektronių nusikaltimų sritį.[98] Tačiau 2010 metų balandį Jungtinių Tautų narės atmetė sutarties pasiūlymą, dėl pasaulinės kovos su elektroniniais nusikaltimais[99]. Pagrindinis to argumentas, tai jog naujos sutarties nereikia, anot G.Masters, buvo tai, kad egzistuoja 2001 metų Konvencija dėl elektroninių nusikaltimų[100].

Apibendrinant Jungtinių Tautų kuriamas teisines kovos su elektroniniais nusikaltimais priemones, galime daryti išvadą jog dauguma šios organizacijos kuriamų priemonių, tokių kaip ITU teisės aktų rinkinys, yra girtinos nepaisant jomis sukuriamo rezultato. O 2010 metų balandį Jungtinių Tautų atmestas naujos tarptautinės sutarties dėl elektroninių nusikaltimų siūlymas, argumentuojant tai kaip pasikartojantį 2001 metų Konvencijos dėl elektroninių nusikaltimų variantą, įrodo, kad tarptautinės organizacijos ne tik abejoja savo kūrimo galiomis ir įtaka, bet ir tai kad teisės harmonizavimo elektroninių nusikaltimų srityje dar teks palaukti.

### 2. 3. 2. Didžiojo aštuoneto šalys

Didysis aštuonetas arba kitaip G-8 susiformavo ekonomikos viršūnių susitikime Prancūzijoje 1975 metais. Didysis aštuonetas susideda iš didžiausių pasaulio pramonės šalių: Didžiosios Britanijos, Prancūzijos, Vokietijos, Italijos, Kanados, JAV, Japonijos ir Rusijos.

1996 metais metiniame viršūnių susitikime valstybių vadovai priėmė rekomendaciją skirtą kovoti su tarptautiniu nusikalstamumu. Sekančiai metais buvo sukurta didžiojo aštuoneto grupė, skirta kovoti su modernių technologijų nusikaltimais.[101] Nuo susikūrimo jis sukūrė šias teisines priemones:

- Įkurtas 24/7 tarptautinių ryšių tinklas tarp didžiojo aštuoneto ir kitų suinteresuotų valstybių, dėl elektroninių nusikaltimų.
- Peržvelgta organizacijos teisinė sistema, susijusi su elektroniniais nusikaltimais, sumažintos sistemoje esančios spragos.
- Sustiprino organizacinius sugebėjimus greičiau surasti ir nustatyti nusikaltimą padariusį asmenį, kuris naudojasi ryšių tinklais teikiamomis paslaugomis.

Tais pačiais metais didžiojo aštuoneto valstybių teisingumo ir vidaus reikalų ministrai susitiko ir priėmė dešimt principų, skirtų kovai su elektroniniais nusikaltimais, kuriuos taip pat galima priskirti prie deklaruojamų kovos priemonių:

---

[98] International Telecommunications Union. ITU Toolkit for Cybercrime Legislation. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf [žiūrėta 2014-01-15]
[99] Masters G. Global Cybercrime Treaty Rejected at U.N. 2010. http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/ [žiūrėta 2014-01-15]
[100] Ten pat.
[101] The role of the G-8. http://www.g8.co.uk/ [žiūrėta 2014-01-14]

- Negali likti nenubaustų, kurie piktnaudžiauja nusikalstamomis elektroninėmis veikomis;
- Nusikalstamos veikos tyrimas ir baudžiamasis persekiojimas turi būti koordinuojamas tarp visų nusikalstama veika suinteresuotų valstybių, nepriklausomai nuo žalos atsiradimo vietos;
- Tyrimus vykdantys darbuotojai turi būti tinkamai pamokyti ir turėti tinkamą išsilavinimą;
- Valstybių teisinės sistemos privalo saugoti konfidencialumą, vientisumą ir duomenų prieinamumą;
- Valstybių teisinė sistema turėtų sudaryti reikiamas sąlygas išsaugoti ir prieiti prie duomenų elektronine forma, kurie yra reikalingi atliekant nusikalstamos veikos tyrimą;
- Pagalbos teikimas, duomenų rinkimas ir keitimasis bylose turi būti užtikrintas valstybių iniciatyva;
- Duomenys turi būti laisvai prieinami užsienio valstybės teisėsaugos institucijoms;
- Reikiama įstatyminė bazė, garantuojanti laisvą elektroninių duomenų naudojimą nusikaltimo tyrimui privalo būti užtikrinta valstybės;
- Kiek įmanoma informacinėmis ir telekomunikacijų sistemomis užkirsti kelią vykdomoms nusikalstamoms elektroninėms veikoms;
- Darbas šioje srityje privalo būti suderintas su kita atitinkama veikla tarptautiniuose forumuose, siekiant užtikrinti dubliavimosi galybę;[102]

Tuo pačiu metu valstybių narių teisingumo ir vidaus reikalų ministrai priėmė veiksmų planą, kurio tikslas buvo peržiūrėti nacionalines teisės sistemas, siekiant užtikrinti, ar jie tinkamai kriminalizavo piktnaudžiavimą telekomunikacijomis ir kompiuterinėmis sistemomis.[103]

2000 metais didžiojo aštuoneto iniciatyva įvyko konferencija, su tikslu aptarti, kaip kartu pažaboti elektroninius nusikaltimus.[104] Tuo metu G-8 paskelbė komunikatą, kuris reikalavo priimti suderintą požiūrį į elektroninius nusikaltimus. Todėl dar karta buvo sustiprinta 24/7 tarptautinio ryšio tinklo veikla, kuri leidžia ne tik G-8 narėms, bet ir kitoms valstybėms užmegzti ryšį su patyrusiais elektroninių nusikaltimų tyrėjais įvairiose valstybėse. Nors G-8 teisinės kovos priemonės yra iš tiesų girtinos, jų nauda yra pasiekiama tik mažoje dalyje pasaulio valstybių.

Įvertinant tai, kad šią organizaciją sudaro aštuonios stipriausios pasaulio valstybės, šios organizacijos viduje negalima tikėtis vienos ar kitos valstybės aiškaus dominavimo ar intereso

[102] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Communique_en.pdf [žiūrėta 2014-01-16]
[103] Ten pat.
[104] Group of Eight Meets to Discuss Internationals Cooperation on Cybercrime. http://en.wikipedia.org/wiki/International_cybercrime [žiūrėta 2014-01-16]

priimant vienokias ir kitokias tarptautines teisinės kovos priemones. Nes toks elgesys galėtų išprovokuoti tam tikrą kitų organizacijos narių nepasitikėjimą ar įtarumą. Tačiau tokių inicijuotų veiksmų, kaip nacionalinių baudžiamųjų įstatymų peržiūrėjimas, tam tikrų nusikalstamų veikų kriminalizavimas nacionaliniuose įstatymuose ir 24/7 ryšio tinklo sukūrimas rodo tam tikrą pavyzdį ekonomiškai silpnesnėms pasaulio valstybėms.

### 2. 3. 3. EBPO

EBPO - Ekonominio bendradarbiavimo ir plėtros organizaciją sudaro daugiau kaip trisdešimt valstybių narių. Valstybės narės drauge aptaria esamą padėtį, plėtoja ir tobulina ekonominę ir socialinę politiką. Remdamosi savo patirtimi ieško atsakymų į iškilusias bendras problemas, bei koordinuoja vidaus ir užsienio tarptautinę politiką.

EBPO buvo pirmoji organizacija pradėjusi išsamų tyrimą dėl baudžiamosios teisės problemų, taikant elektroniniams nusikaltimams tarptautiniu mastu. 1983 metais ekspertų grupė rekomendavo EBPO imtis iniciatyvos suderinant Europos valstybių teisės aktus, susijusius su kompiuteriniais nusikaltimais.[105] Problema buvo tirta iki 1985 metų, kol 1986 metais buvo paskelbta ataskaita, pavadinta „Su kompiuteriais susiję nusikaltimai: teisinės politikos analizė". Ataskaitoje išanalizuoti galiojantys įstatymai ir jų reformų siūlymai, palygintos materialinės teisės normos visame pasaulyje, bei pateiktos rekomendacijos.[106] Ši EBPO ataskaita yra reikšminga dviem aspektais. Pirma, ji nurodė minimalų rinkinį kompiuterių ir kompiuterinio tinklo pažeidimų, kurie gali potencialiai sukelti žalą visiems subjektams, nepriklausomai nuo jų pobūdžio. Antra, EBPO ataskaitoje pateiktos rekomendacijos yra neprivalomų priemonių rinkinys, kuris suteikia valstybei laiko apmąstyti ir priimti tinkamus sprendimus savo nuožiūra, nes mėginimai nustatyti griežtas taisykles iki šiol bet kurioje srityje būdavo priimti su priešinga reakcija ir pasipiktinimu. Tačiau praėjus daugiau nei dešimtmečiui, 2002 metais, EBPO priėmė naujas organizacines gaires dėl informacinių sistemų ir tinklų saugumo: link kultūros saugumo[107]. Toks požiūris į ypatingos svarbos informacinės infrastruktūros apsaugą yra pagirtinas, tačiau dėl savo juridinės galios nėra privalomas valstybėms narėms.

Ekonominio bendradarbiavimo ir plėtros organizacija buvo pirmoji tarptautinė organizacija inicijavusi elektroninių nusikaltimų gaires, tačiau šiandiena tiesiogiai su elektroniniais nusikaltimais nebedirba. Ši organizacija kaip praėjusį dešimtmetį, taip ir iki šiol daugiausia dėmesio skiria

[105] Sieber U. Legal aspects of computer-related crime in the information society.// 1998, p. 20-21.
[106] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime http://www.uncjin.org/Documents/EighthCongress.html [žiūrėta 2014-01-16]
[107] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.html [žiūrėta 2014-01-16]

elektroniniam saugumui ir skatina pasaulinę politiką, grindžiamą tarpusavio pasitikėjimu. O EBPO darbo grupės dėl privatumo ir informacijos (angl. Working Party on Information and Privacy) rengia tarptautines gaires šioje srityje[108].

### 2. 3. 4. ASEAN

Pietryčių Azijos valstybių asociacija, dar kitaip žinoma, kaip ASEAN susideda iš dešimties valstybių narių: Brunėjaus, Kambodžos, Indonezijos, Laoso, Malaizijos, Filipinų, Singapūro, Tailando, Mianmaro, bei Vietnamo.[109] Per savo organizacinę gyvavimo istoriją ASEAN tam tikru periodu vykdė ministrų susitikimus, siekiant išspręsti tarpvalstybinio nusikalstamumo problemas.

1997 metais ASEAN narių vidaus reikalų ministrai susirinko į pirmąją ASEAN konferenciją dėl kovos su tarptautiniu organizuotu nusikalstamumu ir paskelbė deklaraciją, kurioje buvo paskelbta nemažai priemonių, kuriomis buvo siekiama stiprinti regioninį bendradarbiavimą ir veiksmų koordinavimą visose baudžiamosiose bylose.[110] S. Schjolberg manymu, jei priemonės būtų sulaukusios tinkamo finansavimo ir pilno įgyvendinimo, tai būtų buvęs didelis žingsnis teisėsaugos bendradarbiavimo srityje[111]. Kas šiuo metu būtų turėję didelės įtakos kylančiam dabartiniam nusikalstamumui rytuose.

2003 metais spalio 8 dieną Indonezijoje buvo pasirašyta ASEAN ir Kinijos Liaudies Respublikos partnerystės deklaraciją, siekiant tinkamai reaguoti į galimas elektronines grėsmes. Valstybės sutarė bendradarbiavimo ir kritinio reagavimo atveju išlaikyti ir pagerinti elektroninį saugumą, prevencinius veiksmus ir kovą su elektroniniais nusikaltimais. Tačiau jokie nacionaliniai teisės aktai nebuvo pakeisti.

Per 2004 metų valstybių narių susitikimą Bankoke buvo priimtas sprendimas, kad ASEAN valstybės narės siekdamos kovoti su elektroniniais nusikaltimais, privalo veiksmingai tarpusavyje bendradarbiauti, taip kartu sustiprindamos kovą su tarpvalstybiniu nusikalstamumu. O galiausiai 2008 metais ASEAN bendrame komunikate su Kinijos Liaudies Respublika, Japonija ir Korėja buvo priimtas pareiškimas, kad šios valstybės stiprina bendradarbiavimą kovojant su gerai organizuotu tarptautiniu nusikalstamumu, skiriant dėmesį naujai kylantiems iššūkiams, tokiems kaip elektroniniai nusikaltimais, terorizmas ar prekyba žmonėmis. Tačiau grėsmė ir reikalingumas ASEAN šalims bendradarbiauti tarpusavyje, siekiant stiprinti apsaugą nuo įsilaužėlių, kurie kelia grėsmę šios organizacijos valstybėms narėms ir jų piliečiams, išlieka kiekvieną dieną. Tokios

[108] Information security and privacy www.oecd.org/sti/security-privacy [žiūrėta 2014-01-14]
[109] ASEAN Members States http://www.asean.org/asean/asean-member-states [žiūrėta 2014-01-14]
[110] ASEAN and the securitization of transnational crime in Southeast Asia http://www.tandfonline.com/doi/abs/10.1080/09512740320000856 53#preview [žiūrėta 2014-01-14]
[111] Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. December 2008, p. 2.

nuomonės buvo ir Singapūro ministras pirmininkas Lee Hsien Loong po 2013 metų pabaigoje įvykusių hakerių įsilaužimų keliose ASEAN valstybėse narėse[112].

Apibendrinant, ASEAN tai organizacija siekianti įgyvendinti vieną iš pagrindinių Konvencijoje dėl elektroninių nusikaltimų įtvirtintą teisinės kovos priemonę, tai yra tarptautinį bendradarbiavimą. Bendras ASEAN ir kitų trijų stiprių Azijos valstybių komunikatas parodo šios organizacijos geranoriškumą ir racionalumą siekiant pažaboti nenuvaldomai plintantį organizuotą tarptautinį nusikalstamumą.

### 2. 3. 5. OAS

OAS - Amerikos Valstybių Organizacija dar 1999 metais pradėjo aktyviai spręsti problemas, kylančias dėl elektroninių nusikaltimų.[113] Šiuo metu ši organizacija turi 35 valstybes nares.[114] Amerikos Valstybių Organizacija yra surengusi ne vieną įgaliojimų neviršijantį valstybių narių teisingumo ministrų ir advokatų sutikimą - REMJA.[115]

REMJA susitikimo metu buvo prieita bendro sprendimo, dėl tarpvyriausybinės ekspertų grupės dėl elektroninių nusikaltimų sukūrimo. Ekspertų grupei buvo paskirta:

- baigti nusikalstamos veikos susijusios su elektroniniais nusikaltimai analizę, kuria siekiama aprėpti kompiuterius ir informaciją, arba kurios naudoja kompiuterius kaip nusikalstamos veikos atliko priemonę;
- užbaigti nacionalinių teisės aktų, politikos ir praktikos, susijusios su elektroniniais nusikaltimai analizę;
- nustatyti nacionalinius ir tarptautinius subjektus, susijusius su elektroniniais nusikaltimais;
- nustatyti kovos mechanizmus su elektroniniais nusikaltimais, pasitelkiant bendradarbiavimą tarp JAV ir kitų valstybių;

Trečiojo REMJA susitikimo metu, jo dalyviai priėmė bendrą sprendimą dėl rekomendacijų.[116] Šios rekomendacijos buvo pirmasis ekspertų grupės indėlis į JAV kovą su elektroniniais nusikaltimai ir kompiuterinio saugumo plėtrai. Susitikimo metu, valstybėms buvo

[112] Asean countries must work together against cyber crimes: Hsien Loong http://www.asianewsnet.net/Asean-countries-must-work-together-against-cyber-c-53945.html [žiūrėta 2014-01-20]
[113] Inter-American Cooperation Portal on Cyber-Crime http://www.oas.org/juridico/english/cyber.htm [žiūrėta 2014-01-20]
[114] OAS Member States http://www.oas.org/en/member_states/default.asp?utm_source=LifeSiteNews.com+Daily+Newsletter&utm_campaign=b88fabf545-LifeSiteNews_com_Intl_Full_Text_06_06_2013&utm_medium=email&utm_term=0_0caba610ac-b88fabf545-326192614 [žiūrėta 2014-01-20]
[115] Final Report of the Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas. http://www.oas.org/juridico/english/ministry_of_justice_v.htm [žiūrėta 2014-01-20]
[116] Final Report of the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas. http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber [žiūrėta 2014-01-20]

rekomenduota, peržiūrėti priemones, kurios palengvintų tarpusavio bendradarbiavimą kovojant su elektroniniais nusikaltimai, taip pat išanalizuoti prisijungimo prie 24/7 tinklo, įsteigtą G-8 kaip priemonę kovojant su elektroniniais nusikaltimais, galimybę. Taip pat valstybėms narėms buvo pavesta įvertinti Europos Tarybos Konvencijos dėl elektroninių nusikaltimų ir apsvarstyti galimybę prisijungti prie minėto konvencijos.

Šeštojo REMJA susitikimo metu ir toliau didelis dėmesys buvo skiriamos bendradarbiavimui su Europos Taryba.[117] OAS narėms buvo siūloma dar kartą apsvarstyti galimybę prisijungti prie elektroninių nusikaltimų Konvencijos arba laikantis šios Konvencijos normų priimti atitinkamas nacionalines teisės normas ir priemones, reikalingas jos įgyvendinimui. Be to, susitikime buvo rekomenduojama stiprinti bendradarbiavimą su tarptautinėmis organizacijomis ir įstaigomis, tokiomis kaip APEC, G-8, INTERPOLAS, elektroninių nusikaltimų srityje. Susitikimo metu valstybės narės buvo paragintos įsteigti specializuotus padalinius, kurie tirtų elektroninius nusikaltimus.[118] Dar vėliau, OAS pradėjo bendradarbiauti su Amerikos komitetu prieš terorizmą ir Amerikos telekomunikacijų komisija. Kaip bendradarbiavimo vaisius buvo priimti OAS Generalinės Asamblėjos rezoliucija AG/RES 2004 (XXXIV-O/04). [119]

Paskutinio REMJA susitikimo metu, 2012 metais, sąlyginai buvo pakartotos anksčiau paminėtos priemonės ir dar kartą valstybės narės, kurios dar neturi persikėlusios Konvencijos dėl elektroninių nusikaltimų priemonių, paragintos tai padaryti, atsižvelgiant į pirmojo REMJA metu sukurtos darbo grupės dėl elektroninių nusikaltimų rekomendacijas. Taip pat buvo išreikštas kvalifikacijos tobulinimo reikalingumas teisėjams, prokurorams ir kitiems atsakingose institucijose dirbantiems asmenims.[120]

### 2. 3. 6. Interpolas

Nuo 1990, Tarptautinė kriminalinės policijos organizacija – Interpolas buvo labai aktyvus elektroninių nusikaltimų srityje. Interpolas tarnauja valstybių teisėsaugos institucijoms. Jis atlieka žvalgybos funkcijas ir teikia paramą valstybių vykdomiems tyrimams dėl įvykdytų ar vykdomų tęstinio pobūdžio nusikalstamų veikų, nepriklausomai nuo valstybių sienų[121]. Pagal savo misiją, organizacija ,,egzistuoja, kad padėtų sukurti saugesnį pasaulį... teikti unikalias paslaugas

[117] OAS Technical Workshops Following the Sixth Meeting http://www.oas.org/juridico/english/cyber_tech_wrkshpVI.htm [žiūrėta 2014-01-25]
[118] Ministers of Justice or Attorneys General of the Americas (REMJA) VI Final Report http://2001-2009.state.gov/p/wha/rls/rpt/77518.htm [žiūrėta 2014-01-21]
[119] Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity http://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf [žiūrėta 2014-01-21]
[120] Ninth Meeting om Ministers of Justice or Other Ministers or Attorneys General of the Americas http://www.oas.org/en/sla/dlc/remja/pdf/recomm_IX.pdf [žiūrėta 2014-01-20]
[121] INTERPOL: Cybercrime http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [žiūrėta 2014-01-21]

teisėsaugos institucijoms, optimizuoti tarptautines pastangas kovojant su nusikalstamumu."[122] Šiuo metu Interpolo centrinė būstinė yra įsikūrusi Lione, Prancūzijoje. Prie jo yra prisijungę 190 valstybių narių.[123]

Taip pat 1990 metais Interpolas sukūrė pirmąją darbo grupę elektroninių nusikaltimų klausimais, pavadintą Europos darbo grupė su informacinių technologijų nusikaltimais. O prabėgus keletui metų, 1995 metais, įvyko pirmoji Interpolo organizuojama tarptautinė konferencija dėl elektroninių nusikaltimų.[124] Po šios konferencijos Interpolas patvirtino, kad valstybių teisėsaugos institucijos dalyvavusios konferencijoje yra susirūpinusios dėl elektroninių nusikaltimų daromos žalos, nenuvaldomo plitimo ir latentiškumo. Būtent nuo tada Interpolas turi žemynines darbo grupes, susijusias su informacinių technologijų nusikalstamu. Šiuo metu šios darbo grupės turi sukaupusios neįkainojamą regioninę patirtį ir yra įsikūrusios Azijoje, Šiaurės ir Pietų Amerikoje, Afrikoje ir Europoje.[125]

Kiekvienas Interpolo regionuose įsikūręs centrinis biuras yra atsakingas už jiems pateiktus pagalbos prašymus, suteikti reikiamą pagalbą dėl vienokios ar kitokios elektroninės nusikalstamos veikos. Jungtinių Amerikos Valstijų centrinis biuras buvo įsikūręs Vašingtone, bet yra koordinuojamas JAV Teisingumo departamento. Todėl visi JAV teisėsaugos darbuotojai į centrinę būstinę Lione galėjo kreiptis tik pateikę prašymą per savo nacionalinį centrinį Interpolo biurą Vašingtone.[126] S. Ghosh ir kiti mokslininkai kritikavo tokią savitarpio pagalbos sistemą, dėl itin lėto ir sudėtingo proceso[127]. Atsižvelgiant į viso pasaulio dėmesį skiriamą šiai organizacijai, biudžeto apribojimus ir beveik kasdieną kintančias technologijas Interpolas buvo priverstas žengti koja kojon su visais elektroniniais nusikaltimais, nepriklausomai nuo jų sudėtingumo masto ar geografinės vietos.[128]

Būtent dėl šių priežasčių Interpolas dabar turi saugią sistemą, pritaikytą rinkti, saugoti, analizuoti, keistis prašoma ir pateikiama informacija.[129] Valstybės narės gali gauti visus reikiamus duomenis susijusius su nusikalstama elektronine veikla.[130] Naujoji sistema palaikoma 24 valandas per parą, 7 dienas per savaitę[131].

Negana to Interpolas atliko bendrą projektą su privačių verslo sektoriumi, siekiant pažaboti elektroninių nusikaltimų plitimą. Interpolas kartu su programinės įrangos kūrimo gigante *Microsoft* organizavo BotNet darbo grupę (angl. BotNet Task Force), kuri vėliau padėjo spręsti didėjančią

[122] About Interpol. http://www.interpol.int/About-INTERPOL/Overview [žiūrėta 2014-01-21]
[123] Ten pat.
[124] Ten pat.
[125] S. Ghosh, E. Turrini. Cybercrimes: A Multidisciplinary Analysis. Springer. 2010. p. 330-332.
[126] Ten pat.
[127] Ten pat.
[128] Ten pat.
[129] Interpol: An overview. www.interpol.int/Public/ICPO/FactSheets/GI01.pdf [žiūrėta 2014-01-21]
[130] Ten pat.
[131] Interpol. Cyber-crime. www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf [žiūrėta 2014-01-21]

kompiuterinių zombių grėsmę.[132] Tokia konkreti, rūšinė, kovos priemonė susilaukė gausaus palaikymo tiek iš užsienio valstybių, tiek ir iš kitų verslo subjektų. Autoriaus nuomone, tokio ar labai panašaus pobūdžio darbo grupių kūrimas turėtų būti skatinamas pirmiausia nacionaline iniciatyva, o vėliau per jas į verslo subjektus.

Apibendrinant Interpolo ir kitų autoriaus išanalizuotų tarptautinių organizacijų veiklą ir efektyvumą gali daryti išvadą, kad visos tarptautinių organizacijų kuriamos priemonės yra iš esmės panašios, tačiau gaila, kad neprivalomo, o daugiau rekomendacinio pobūdžio. Priemonių įgyvendinimas paliekamos pačioms valstybėms, o raginimai prisijungti jau prie esamos Konvencijos atspindi tarptautinių organizacijų nekūrybiškumą ir menką pačių sukuriamą iniciatyvos teisę. Tačiau tokių procesinių priemonių kaip 24/7 ryšio tinklo steigimas ir tarpvalstybinis bendradarbiavimas parodo didelį norą kaip įmanoma efektyviau per trumpesnį laiką kovoti su kintančiais elektroniais nusikaltimais.

[132] Interpol. Annual report 2006. http://interpol.int/Public/ICPO/InterpolAtWork/iaw2006.pdf [žiūrėta 2014-01-21]

## III. JURISDIKCIJOS PROBLEMA

Diferenciacija tarp įvairių nusikalstamų veikų yra žinoma nuo XVI a., kuomet imperatoriaus Karolio V baudžiamajame teisyne, kitaip žinomame, kaip Karolina, nusikalstamos veikos buvo skirstomos remiantis skirtingais požymiais ir skirtingomis baudžiamosiomis normomis. Šiuolaikiniai nacionaliniai baudžiamieji kodeksai nebeapsiriboja valstybių ribomis, priešingai nei tada, kuomet teisė buvo tik vidaus funkcinė dalis. Šiuolaikinė technologijų revoliucija greitu metu taip pakeis visuomenę, kad pačių žmonių sukurta dirbtinio intelekto programinė įranga bus sunkiai atskiriama nuo žmogaus. Elektroninės erdvės atsiradimas pakeitė nusistovėjusį ir ilgai nesikeitusį baudžiamosios teisės modelį. Nusikaltimai interneto pagalba vyksta neapsiribojant vienos valstybės teritorija, nusikalstami veiksmai elektroninėje erdvėje gali atkeliauti iš kitos valstybės, tokiu būdu išskaidant nusikaltimo vietas per kelias valstybes, kartais net per kelis skirtingus žemynus.[133] Tokią problemą dera spręsti tarptautinės teisės priemonių pagalba. Konvencija dėl elektroninių nusikaltimų, kuri įsigaliojo 2004 metais[134] buvo siekiama – gerbti žmogaus teises šiuolaikinėje informacinėje visuomenėje. Tačiau, nors jurisdikcijos klausimai ir buvo apibrėžti minėtoje Konvencijoje, trūkumų išvengti nepavyko, todėl kai kuriais atvejais kovojant su nusikalstamomis veikomis, įvykdytomis kompiuterinių technologijų pagalba, efektyviausia priemone laikytinas tiesioginis tarptautinis bendradarbiavimas.

Pagrindiniai šio skyriaus uždaviniai atskirti visas galimas jurisdikcijos teorijas, atlikti Konvencijoje dėl elektroninių nusikaltimų įtvirtintų jurisdikcijos normų analizę, nepaliekant nuošalyje tarptautinio tarpvalstybinio bendradarbiavimo. Taip pat išnagrinėti keletą atvejų ir problemų susijusių su jurisdikcija ir tarptautiniu bendradarbiavimu, atskleisti jurisdikcijos problemą debesų kompiuterijoje.

### 3. 1. Jurisdikcijos teorijos

Pats žodis jurisdikcija turi keletą skirtingų reikšmių. Viena iš reikšmių yra siejama su jurisdikcija nustatyti, kita su jurisdikcija priimti sprendimą ir trečia su jurisdikcija vykdyti. Teisinėje literatūroje yra paminėtos net penkios skirtingos jurisdikcijos teorijos, kurios buvo taikomos skirtingų valstybių teismuose ar paminėtos valstybių nacionaliniuose teisės aktuose. Taigi, analizuojant teisinės kovos su elektroniniais nusikaltimai priemones, svarbiausia yra jurisdikcijos priskyrimas tam tikram teismui.

[133] Brenner S.W., Scherha J.J., Cybercrime Havens: Challenges and Solutions.// Business Law Today, vol.17, December, 2007, p. 49.
[134] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2013-12-27]

*Teritorinė jurisdikcija* yra tuomet, kai jurisdikcija yra nustatoma pagal vietą, kur nusikalstama veika buvo visiškai ar iš dalies atlikta. Turint omenyje, kad valstybė turi teritorinį suverenitetą, tai be abejo ji turi ir jurisdikciją bet kokiam nusižengimui, kuris vyksta tos valstybės teritorijoje ir padaro žalą vienam ar keliems tos pačios valstybės piliečių. Kaip sudėtingą teritorinės jurisdikcijos atvejį galima paminėti situaciją susiklosčiusią byloje *Bavarija v Somm*, kurioje vienos Vokietijos įmonės generalinis direktorius, kuris turėjo Šveicarijos pilietybę, buvo atsakingas už prieigas Vokietijoje į smurtinius, vaikų pornografijos interneto tinklapius, kurių serverio paslaugas atliko Vokietijos kompanija, tačiau patys serveriai buvo JAV[135]. Teismas nusprendė, kad ginčą turi nagrinėti Vokietijos teismas nes generalinis direktorius faktiškai gyvena Vokietijoje ir nusikalstama veika padaryta šios valstybės teritorijoje, nepaisant to kad jis yra Šveicarijos pilietis.

*Pilietybės principu grindžiama jurisdikcija* yra susijusi su asmens, kuris padarė tam tikrą nusikalstamą veiką pilietybe[136]. Ypač plačiai pripažįstama, kad valstybė turi beveik neribotą savo piliečių kontrolę[137]. Manoma, kad valstybė turi jurisdikciją savo piliečių atžvilgiu, nepaisant to kur jie ir ką jie veikia. Tai jokiu būdu negali būti suvokiama kaip diktatoriška kontrolė, kai valstybė kontroliuoja visą savo piliečių gyvenimą. Tiesiog valstybė turi pareigą apsaugoti savo visuomenę nuo nusikaltimų. Be to, padaryta veika gali būti laikoma teisėta padarytos valstybės teritorijoje, tačiau veiką atlikusio asmens tėvynėje tai laikoma nusikaltimu. Tokios normos įtvirtintos daugelyje Europos Sąjungos valstybių baudžiamuosiuose kodeksuose, ne išimtis yra Vokietijos bausmių knygos 5 skyrius, kuriame yra numatyta, jog Vokietijos pilietis padaręs nusikaltimą kitoje šalyje, kurioje piliečio veiksmas nėra laikomas nusikaltimu, bausmę turi atlikti savo tėvynėje. Geriausias pilietybės jurisdikcijos pavyzdys yra byla *JAV v. Galaxy Sports*[138]. Tai buvo pirmasis JAV federalinis ieškinys prieš ofšorinių kompanijų operatorius, kurie naudojo internetinius tinklapius nelegalių lošimų tikslams. Lošimų bendrovės orientavosi į klientus Jungtinėse Amerikos Valstijose, reklamavo savo verslą per visas tuo metu įmanomas žiniasklaidos priemones. Reklamose buvo raginama statymus atlikti tiesiogiai per kompaniją, nei per internetą. Kadangi ofšorinės kompanijos buvo registruotos Antigvoje, JAV teismas buvo netinkamas nagrinėti bylą. Tačiau ofšorinių kompanijų prezidentas, kuris buvo pagrindinis teisiamasis byloje buvo JAV pilietis. Todėl 2000 m. rugpjūčio 10 d. po prisiekusiųjų sprendimo buvo nuteistas laisvės atėmimo bausme.

*Nukentėjusiojo buvimo vietos jurisdikcija* yra tiesiogiai susijusi su nukentėjusio asmens pilietybe[139]. Tokia teorija yra visiškai nepalanki nusikaltimą įvykdžiusiam asmeniui, jei jis yra kitos

[135] People v. Somm, Case 8340 Ds 465 Js 173158/95 (Amstsgericht, Munchen, Bavaria)
[136] Blakesley C.L. Jurisdictional Issues and Conflicts of Jurisdiction.// p. 139.
[137] August R. International Cyber-Jurisdiction: A Comparative Analysis.// American Business Law Journal, vol. 39 Summer, 2002, p 539.
[138] The United States Department of Justice. http://www.justice.gov/criminal/cybercrime/bentleySent.pdf [žiūrėta 2013-12-27]
[139] Blakesley C.L. Jurisdictional Issues and Conflicts of Jurisdiction.// p. 139.

valstybės pilietis, nei nukentėjusysis. Idealus šios teorijos pavyzdys yra byla *USA v. Ivanov ,* kurioje kaltinamasis Rusijos pilietis Aleksėjus Ivanovas, gyvenantis Čeliabinske, įsilaužė į kompiuterius esančius Jungtinėse Valstijose.[140] Po ilgai trukusio baudžiamojo persekiojimo jis vis tiek buvo sučiuptas JAV slaptųjų agentų.

*Apsauginė jurisdikcija*, kitaip vadinama saugumo principu leidžia jurisdikciją priskirti valstybei, kuri turi savo interesą baudžiamojoje byloje[141]. Baudžiamųjų bylų praktikoje ši teorija egzistuoja visuomet, išskyrus išimtis, kuomet bylos yra susijusios su pinigų ar vertybinių popierių klastojimu.

Paskutinė *universalios jurisdikcijos teorija* grindžiama tarptautinio pobūdžio nusikaltimu ir priešingai nei kitos jurisdikcijos teorijos leidžia kiekvienos valstybės kompetentingą teismą kreiptis dėl bylos nagrinėjimo priskyrimo, net jei nusikalstamos veikos neturi tiesioginio poveikio valstybei ar jos saugomoms vertybėms, todėl yra reikalaujamas priežastinis ryšys tarp jurisdikciją turinčio teismo ir paties nusikaltimo[142]. Pirmasis universaliai jurisdikcijai priskiriamas nusikaltimas buvo piratavimas. Vėliau po Antrojo pasaulinio karo, karo nusikaltimai, nusikaltimai žmoniškumui, teroristiniai aktai, lėktuvų užgrobimas, kankinimai ir kiti žmogaus teisių pažeidimai taip pat buvo priskiriami universaliajai jurisdikcijai.[143]

Trumpai aptarus teisėje egzistuojančias jurisdikcijos rūšis, toliau yra tikslinga išanalizuoti Konvencijoje dėl elektroninių nusikaltimų įtvirtintas jurisdikcijos nuostatas.

### 3. 2. Jurisdikcijos taikymas remiantis 2001m. Konvencija dėl elektroninių nusikaltimų.

2001 metų Budapešte priimtos Konvencijos dėl elektroninių nusikaltimų 22 straipsnio 1 dalis nustato, kad Konvencija remiasi tik teritorijos ir pilietybės jurisdikcijų teorijomis. Tačiau nepaisant to, yra paliekama visiška teisėkūros laisvė pačiai valstybei. Svarbu tai, kad valstybės teisės aktai turi nustatyti jurisdikciją Konvencijos 2-11 straipsniuose nurodytiems nusikaltimams, tai yra neteisėta prieiga ir perimtis, kompiuterinis sukčiavimas ir kiti, kuomet nusikalstama veika atlikta pačios valstybės teritorijoje, laive ar orlaivyje plaukiančiame su tos valstybės vėliava, ar įregistruotame pagal tos valstybės teisės aktus. Tai reiškia kad asmenys įvykdę nusikalstamą veiklą savo valstybės teritorijoje ir yra patraukiami baudžiamojon atsakomybėn pagal savo valstybės teisės aktus. Konvencijos 22 straipsnio 1 dalies *b* ir *c* punktuose nustatytos prielaidos yra naudingos, kai laivas arba orlaivis yra ne tos pačios valstybės teritorijos, kurioje yra padaromas nusikaltimas.

[140] The United States Department of Justice. http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm [žiūrėta 2013-12-27]
[141] Blakesley C.L. Jurisdictional Issues and Conflicts of Jurisdiction.// p. 139-141.
[142] Ten pat.
[143] Fry J.D. Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction.// UCLA Journal of International Law and Foreign Affairs, vol. 7, 2002, p. 176.

Tuomet atsižvelgiant į minėto straipsnio 1 dalies *d* punktą, kuomet pilietis iš vienos valstybės padaro vieną iš Konvencijoje numatytų nusikalstamų veikų už bet kurios kitos valstybės teritorinės jurisdikcijos ribos, yra priskiriamas savo valstybės jurisdikcijai. Konvencija jokiu būdu nepašalina nei vienos baudžiamosios jurisdikcijos, kuri vykdoma pagal vidaus teisės aktus.

Konvencijos 22 straipsnio 2 dalis leidžia valstybėms pasilikti teisę netaikyti arba tam tikrais atvejais arba esant tam tikroms aplinkybėms taikyti jurisdikcijos taisykles, nustatytas anksčiau minėtuose 22 straipsnio 1 dalies b-d punktuose, arba taikyti tik dalį šių taisyklių. Taip valstybėms suteikiama daug laisvės sprendžiant jurisdikcijos klausimą, net jei valstybė negali išvengti įsipareigojimo pagal Konvenciją pradėti baudžiamąjį persekiojimą, kai nusikaltimas padarytas valstybės teritorijoje. Kadangi praktikoje kai kurie nusikaltimai teisines pasekmes sukelia keliose valstybėse tuo pačiu metu, tai tokiu atveju gali nekelti jurisdikcijos įpareigojimo nei vienai iš tų valstybių, manant, kad kita valstybė patyrė daugiau žalos ir todėl turi pirmenybę į baudžiamąjį persekiojimą[144]. Todėl ši dalis turėtų apimti įpareigojimą visoms žalą dėl nusikalstamos veikos patyrusioms valstybėms konsultuotis viena su kita, nes kol to nėra dalis įvykdytų nusikaltimų lieka be bausmės. Taip pat šio straipsnio 2 dalis prieštarauja to paties straipsnio pirmai daliai, kuri tvirtina, kad valstybės turi nustatyti jurisdikciją remiantis savo nacionaliniais teisės aktais.

Konvencijos 24 straipsnio 3 dalyje nustatyta tarptautinės paprotinės teisės norma[145], ekstradicijos ir baudžiamojo persekiojimo principai - *aut dedere aut judicare*[146]. Ekstradicija vykdoma pagal prašančios šalies teisėje arba taikytinose ekstradicijos sutartyse nustatytas sąlygas, įskaitant pagrindus, kuriems esant prašomoji valstybė gali atsisakyti. Prašomoji valstybė turi pareigą vykdyti baudžiamąjį persekiojimą, kaip teisinę galimybę atlikti tyrimus ir procesinius veiksmus, taip kaip ir savo valstybėje. Realus situacijos pavyzdys buvo kai 36 metų kinų kilmės hakeris Fang Yong ekstradicijos sutartimi Kanados buvo išduotas Kinijai ir ten nubaustas mirties bausme, už tai, kad laikotarpyje tarp 1990 metų gegužės ir rugpjūčio pavogė pinigų iš trečiųjų asmenų bankų sąskaitų Kinijoje, kurių vertė buvo virš vieno milijono juanių[147]. Pagrindinė ekstradicijos taisyklė, kuri visuomet privalo būti palaikoma, yra tai, jog nusikaltėliai negali likti nenubausti už padarytas nusikalstamas veikas. Tačiau praktikoje pasitaiko atvejų, kuomet Konvencijoje numatytą nusikaltimą padariusį asmenį atsisakoma išduoti vien dėl jo pilietybės arba dėl to, kad prašomoji valstybė mano, kad įvykdytas nusikaltimas priklauso jos jurisdikcijai. Tuomet

[144] Brenner S.W., Koops B.J.Approaches to Cybercrime Jurisdiction.// Journal of High Technology Law, vol. 4, 2004, p. 3.
[145] Paust J.J. Above the Law: Unlawful Executive Authorization Regarding Detainee Treatment, Secret Renditions, Domestic Spying, and Claims to Unchecked Executive Power.// Utah Law Review, vol. 2007, issue 2, p. 367.
[146] Galicki Z. The Obligation to extradite or Prosecute in International Law.// Report of the nternational Law Commission, Fifthysix session (2 May- 4 June and 5 July- 6 August 2004), p. 312.
[147] Chinese Hacker Sentenced to Death for Embezzlement. http://english.people.com.cn/english/200006/13/eng20000613_42866.html [žiūrėta 2013-12-27]

prašomoji valstybė prašančiosios valstybės prašymu perduoda bylą savo kompetentingoms institucijoms, kad jos vykdytų baudžiamąjį persekiojimą ir reikiamu metu praneštų prašančiai valstybei apie galutinį rezultatą. Institucijos priima sprendimą ir atlieka tyrimą tokiu būdu, kaip ir kitose panašiose baudžiamosiose bylose, sprendžiamose pagal tos valstybės teisę.

Išnagrinėtų situacijų yra aiškiai matyti, kad Konvencijos dėl elektroninių nusikaltimų normos, ne visais atvejais yra pajėgios užtikrinti, kad asmuo būtų nubaustas už padarytą nusikaltimą.

### 3. 2. 1. Neigiamo pobūdžio jurisdikcijų kolizijos

Nors elektroninių nusikaltimų jurisdikcijos nuostatos yra plačios, tačiau atsižvelgiant į valstybių skaičių visuomet gali atsirasti neigiamos jurisdikcijų kolizijos. Tai situacija kai kelios valstybės teigia turinčios jurisdikciją, susijusią su atitinkamais elektroniniais nusikaltimais. Dauguma valstybių turi jurisdikciją visoms Konvencijoje minimoms nusikalstamoms veikoms. Didžioji dalis elektroninių nusikaltimų, tai yra įsilaužimai arba išpuoliai siekiant apriboti tam tikras technologines funkcijas, yra nukreipti į konkrečius kompiuterius, todėl valstybės turi jurisdikciją remiantis keliomis skirtingomis jurisdikcijos teorijomis. Tačiau S.W.Brenner ir B.J. Koops manymu, kurios valstybės jurisdikcijai pateks nusikalstama veika gali lemti tik žalos dydis arba tiesioginis ryšys su valstybe.[148] Tokiai nuomonei pritaria ir autorius, nes vargu ar kaip kitaip galima ginti savo pažeistą interesą, jei nesi nukentėjęs ir tarp veikos ir kilusių padarinių nėra tiesioginio priežastinio ryšio.

Tačiau, autoriaus nuomone, dar sunkesnė tyrimo situacija yra nusikalstamose veikose susijusiose su kompiuteriniais virusais ir duomenų turinio pakitimais. Šio tipo nusikaltimų esmė yra ta, kad žalos atsiradimo vieta dažniausiai nėra iš anksto numatyta ar sietina su tam tikru asmeniu ar kompiuteriu, tačiau dažniausiai tai būna kelios dešimtys skirtingų vietų tuo pačiu metu. Tokiais atvejais, kai nusikaltimo vykdytojas veikia iš tėvynės, kuri savo baudžiamuosiuose įstatymuose nėra kriminalizavusi veikų, susijusių su elektroniniais nusikaltimas, dažniausiai kyla neigiama jurisdikcijų kolizija. Be visa to, anot B.J. Koops, visuomet išlieka esminis klausimas, ar valstybė visada turi pakankamą suinteresuotumą grįsti savo jurisdikciją, nes kompiuteriniai virusai ir internetinės svetainės, skleidžiančios propagandą, dažniai valstybėms atrodo menkavertis nusikaltimas lyginant jį su jurisdikcijos įrodinėjimo procesu.[149]

Apibendrinant galima daryti išvadą, jog neigiama jurisdikcijų kolizija praktikoje pasitaiko gana dažnai. Todėl valstybėms pajutus net ir menkavertę elektroninių nusikaltimų žalą reikėtų

[148] Brenner S.W., Koops B.J.Approaches to Cybercrime Jurisdiction.// Journal of High Technology Law, vol. 4, 2004, p. 40-41
[149] Ten pat.

nenuleisti rankų, o tarpvalstybinio bendradarbiavimo pagrindu tirti ir analizuoti tokius atvejus, net jei ir iškyla jurisdikcijų kolizija.

### 3. 2. 2. Teigiamos jurisdikcijos kolizijos.

Svarbesni už neigiamas jurisdikcijų kolizijas yra teigiami jurisdikcijų konfliktai, kai daugiau nei viena valstybė tvirtina savo jurisdikciją dėl tos pačios nusikalstamos veikos. Šiuo metu tai reali situacija, nes elektroniniai nusikaltimai paprastai apima ne vienos valstybės teritoriją, todėl turint galvoje plačias jurisdikcijos nuostatas daugelyje valstybių, dažnai net keletas valstybių turi jurisdikciją pradėti baudžiamąjį persekiojimą ir patraukti asmenį baudžiamojon atsakomybėn remiantis nacionaliniais baudžiamosios teisės aktais. Pavyzdžiui, Lietuvos pilietis naudodamasis kompiuteriu Latvijoje įsilaužia į kompiuterius esančius Estijoje. Tokiu atveju Lietuva, Latvija ir Estija turi teisę programišių patraukti baudžiamojon atsakomybėn. S.W Brenner ir Todėl tokio pobūdžio daugiašaliai jurisdikcijos reikalavimai turi būti švelninami grindžiant protingumo principu.[150] Minėtu atveju, valstybės jurisdikcija bus silpninama, jei ji patyrė mažesnę žalą lyginant su kitomis valstybėmis arba jei duomenys pereidami per valstybės teritoriją nesukėlė jokios žalos. Reziumuojant, protingumo principas yra labai lankstus, todėl valstybių nacionaliniai teismai gali interpretuoti, kaip jiems atrodo tinkama, taip išsirenkant tos valstybės nacionalinį teismą, kuri patyrė daugiau žalos. Tačiau tokiu atveju, teisinės kovos su elektroniniais nusikaltimais priemonės pasiektų savo tikslą, nes nusikaltimą padaręs asmuo neišvengtų atsakomybės.

Elektroninių nusikaltimų Konvencija taip pat nesukuria tinkamų gairių atsiradus jurisdikcijų kolizijai. Konvencijoje pasakyta tik tai, kad esant atvejui, kuomet daugiau nei viena valstybė teigia turinti jurisdikciją dėl tariamo nusikaltimo, suinteresuotos valstybės konsultuojasi tarpusavyje, siekiant nustatyti tinkamiausią baudžiamojo persekiojimo jurisdikciją.[151] Remiantis Konvencijos aiškinamuoju raštu, Konvencijoje minimos konsultacijos nėra privalomo pobūdžio, todėl valstybė gali ignoruoti kitos šalies kreipimąsi dėl tos pačios nusikalstamos veikos. Akivaizdu tai, kad visuotinai priimtos veiksmų hierarchijos nėra, todėl labai svarbu plėtoti teigiamą jurisdikcijų konfliktų sprendimą pagrįsta tarpvalstybiniu bendradarbiavimu.

[150] Brenner S.W., Koops B.J.Approaches to Cybercrime Jurisdiction.// Journal of High Technology Law, vol. 4, 2004, p. 15.
[151] 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [žiūrėta 2013-12-28]

### 3. 3. Jurisdikcija kibernetinėje erdvėje.

Tai, jog Elektroninių nusikaltimų konvencijos 22 straipsnyje yra nustatyta kad jurisdikcija remiasi teritoriniu ar pilietybės principu, autorius manymu, sukuria daugiau teisinių problemų, nei jų išsprendžia. Taip yra todėl, nes Konvencija apibrėžia tik tam tikros rūšies nusikalstamas veikas: asmuo gali siųsti arba įkelti failus, kurių turinys yra nusikalstamo pobūdžio, iš konkretaus kompiuterio iš vienos valstybės į kitos valstybės kitą kompiuterį ar serverį ir minėti failai gali būti parsisiųsti visame pasaulyje. Taigi, kur minėtu atveju yra įvykdytas nusikaltimas? Toje šalyje, kurioje asmuo gyvena, ir/arba failai yra įkeliami, toje šalyje kurioje faktiškai yra serveris ar tose šalyse, kuriose failą su nusikalstamo pobūdžio turiniu faktiškai matė? Ir ką daryti jei failą mačiusių asmenų šalyje, turinys nėra laikomas nusikalstamo pobūdžio ir tai nėra laikoma nusikaltimu?

Puikus pavyzdys jurisdikcijos kazusui kibernetinėje erdvėje yra vadinamoji *Yahoo.com* byla.[152] Byloje kaltinimą palaikė LICRA – tarptautinė lyga prieš rasizmą ir antisemitizmą, jie skundėsi kad internetiniame *www.yahoo.com* aukcione buvo pardavinėjamos nacistinio pobūdžio relikvijos. LICRA rėmėsi Prancūzijos baudžiamojo kodekso R 645-1 straipsniu, kurio normos šiuo atveju draudžia nacistinių simbolių eksponavimą ar kitokį jų panaudojimą. *Yahoo.com* kompanija teigė, kad nėra techninių priemonių užkirsti kelią Prancūzijos gyventojams dalyvauti jų aukcionuose, nesukuriant papildomų finansinių sunkumų. Taip pat jie pažymėjo, kad jų serveriai buvo įsikūrę JAV teritorijoje, jų paslaugos pirmiausia buvo skiriamos JAV gyventojams ir, kad ginčas turi būti priskiriamas JAV jurisdikcijai.[153] Prancūzijos aukščiausiasis teismas nusprendė, jog buvo pakankamas ryšys su Prancūzija suteikti jai visišką jurisdikciją nagrinėti skundą. Nacių relikvijų aukcionai buvo atviri dalyviams iš bet kurios šalies, įskaitant Prancūziją. *Yahoo.com* žinojo, kad Prancūzijos gyventojai naudojosi aukciono svetaine, nes atveriant svetainę iš Prancūzijos ji buvo rodoma prancūzų kalba. Tačiau byla šioje vietoje nesibaigė. Nepatenkinti Prancūzijos teismo sprendimu *Yahoo.com* nusprendė paduoti ieškinį JAV apygardos teismui San Franciske, tikėdamiesi gauti nutartį, kad Prancūzijos teismo nutartis negali būti vykdoma prieš *Yahoo.com* Jungtinėse Amerikos Valstijose. JAV apygardos teisėjas Jeremy Fogel nustatė, kad Prancūzijos teismo sprendimas yra nesuderinamas su pirmąja pataisa į JAV Konstituciją, kuri garantuoja žodžio ir saviraiškos laivę, ir kad bet koks mėginimas priversti vykdyti teismo sprendimą JAV prieštarauja JAV Konstitucijai.[154] Tuomet LICRA nepatenkinta JAV teismo sprendimu kreipėsi i JAV apeliacinį teismą už devintos apygardos.[155] Praėjus kiek laiko, galų gale

[152] Byla LICRA prieš Yahoo. http://en.wikipedia.org/wiki/LICRA_v._Yahoo [žiūrėta 2013-12-29]
[153] Yahoo! v. LICRA Amicus Brief http://www.law.berkeley.edu/4647.htm [žiūrėta 2013-12-29]
[154] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme http://cyber.law.harvard.edu/is02/readings/yahoo-order.html [žiūrėta 2013-12-29]
[155] United States Court of Appeals for the Ninth Circuit http://en.wikipedia.org/wiki/United_States_Court_of_Appeals_for_the_Ninth_Circuit [žiūrėta 2013-12-29]

vienuolikos teisėjų kolegija priėmė sprendimą, kad JAV apygardos teismas turėjo atsakovo – LICRA jurisdikciją, tačiau apygardos teismo nuosprendis buvo panaikintas.[156]

Taigi, nusikaltimai elektroninėje erdvėje yra labai plataus pobūdžio veikla, kuri dėl savo sudėtingumo tampa sunkiai atskleidžiama. Jurisdikcijos ribų neaiškumas kompiuterijoje taipogi prisideda prie techninio tyrimo sudėtingumo. Tai pasidaro akivaizdu, kai pradedame kalbėti apie tarptautines jurisdikcijas. Doktrinoje nurodoma, kad jurisdikciją nustato trijų pakopų institucijos. Pirma institucija nustato galimybę parengti ir numatyti baudžiamąsias ir reguliuojamąsias sankcijas – vyriausybės prerogatyva. Antra, institucija spręsti, t.y. kompetencija nagrinėti ginčus – prerogatyva teismams. Trečia, institucija vykdyti – prerogatyva vyriausybei.[157] O elektroninio nusikaltimo, kaip tarptautinio nusikaltimo tyrimas visada turi priklausyti nuo šalių geros valios. Net jei Kovencijos veiksmingumas yra tiesiogiai priklausomas nuo tarptautinio bendradarbiavimo, tai yra pagrindas kovoti su šiais naujos rūšies nusikaltimais.

### 3. 3. 1. Tarptautinis bendradarbiavimas baudžiamosiose bylose dėl el. nusikaltimų.

Iškart po jurisdikcijos principų Konvencijoje yra detalizuojamas tarptautinis bendradarbiavimas. Konvencijos 23 straipsnis pavadintas „Bendrieji principai, susiję su tarptautiniu bendradarbiavimu", sukuria valstybių įsipareigojimą bendradarbiauti tarpusavyje ekstradicijos, savitarpio pagalbos ir savaiminio informavimo klausimais. Geri tarptautinio bendradarbiavimo pavyzdžiai yra *Rome Labs* ir *Tore Tvedt* bylos. 1994 metais Roma oro plėtros centre, Griffiss oro pajėgų bazėje (angl. Rome Air Development Center, Griffiss Air Force Base), Niujorke kompiuterinių sistemų administratoriai rado, kad į jų kompiuterinę sistemą buvo neteisėtai įsilaužta programos „Sniffer" pagalba.[158] Minėta programa buvo įdiegta nelegaliai įsilaužus, siekiant surinkti registruotų vartotojų prie kompiuterinės sistemos prisijungimo duomenis. Šnipinėjanti programa buvo įdiegta į vieną iš sistemų, sujungtą su karinės laboratorijos tinklu. Tyrimo metu nustatyta, kad įsilaužėliai save vadino „Datastream Cowboy" ir „Kuji", tačiau jų tapatybės nežinomos. „Datastream Cowboy"- šešiolikmetis hakeris, kuriam patiko įsilaužimai į karinius tinklus, buvo įsikūręs Didžiojoje Britanijoje. Todėl JAV karinių oro pajėgų atstovai kreipėsi į Skotland Jardo agentus ir suėmė minėtą hakerį. Šešiolikamečiui hakeriui baudžiamosios bylos procesas vyko Didžiojoje Britanijoje, ir po trejus metus trukusio proceso, jam buvo paskirta 1200 svarų bauda už

[156] Yahoo Inc V. La Ligue Contre Le Racisme et Antisemitisme http://caselaw.findlaw.com/us-9th-circuit/1144098.html#sthash.jhpZB1Bv.dpf [žiūrėta 2013-12-29]
[157] Brenner S.W., Koops B.J.Approaches to Cybercrime Jurisdiction.// Journal of High Technology Law, vol. 4, 2004, p. 4.
[158] The Case Study: Rome Laboratory, Griffiss Air Force Base, NY Intrusion. http://www.fas.org/irp/congress/1996_hr/s960605b.htm [žiūrėta 2013-12-29]

įsibrovimą[159]. Kitas įsilaužėlis slapyvardžiu ,,Kuji'' taip pat buvo suimtas, bet po pusantrų metų buvo išteisintas, nes nebeliko viešo intereso tęsti bylą.[160]

*Tore Tvedt* byla kilo dėl rasistinių ir antisemitinių propagandų skelbimo internetinėje erdvėje. Toras buvo Norvegijos kraštutinių dešiniųjų organizacijos narys. Organizacija skleidė rasinę neapykantą, tikėjimą senovės skandinavų dievais, pasisakė prieš kraujomaišą. Jis taip pat buvo atsakingas už šios organizacijos internetinio tinklapio turinį, tačiau internetinis tinklapis buvo saugomas Šiaurės Amerikos serveryje. Atsižvelgiant į tai, iš kur buvo talpinama informacija, Norvegijos teismas skyrė septyniasdešimt penkias dienas kalėjimo ir du metus lygtiniai[161]. Tai buvo du atvejai, kai nusikalstamas veikas pavyko išaiškinti nepaisant egzistuojančio jurisdikcijos kazuso.

Tačiau ne visas nusikalstamas veikas pavyksta užkardyti remiantis tarptautiniu bendradarbiavimu. 2001 metais spalio 10 dieną JAV Teisingumo Departamentas paskelbė, kad Rusijos pilietis Vasilijus Gorshkovas buvo pripažintas kaltu dėl sąmokslo, įvairių kompiuterinių nusikaltimų ir sukčiavimo. [162] Po to kai buvo nustatyta, kad į kai kurias įmones patenka įsilaužėliai, FTB sukūrė fiktyvią įmonę pavadinimu ,,Invita".[163] Taip su hakeriais buvo užmegztas ryšys ir pradėta juos vilioti į JAV su darbo pasiūlymais. Po ilgų derybų internetu, Vasilijus Gorshkovas ir Aleksėjus Ivanovas sutiko susitikti gyvai. Susitikimo metu jie slaptiems FTB agentams papasakojo apie įvairiausius įsilaužimus ir kitas nusikalstamas veikas elektroninėje erdvėje. Pabaigoje ,,Invita'' susitikimo abu hakeriai buvo suimti. Pasak JAV Teisingumo Departamento JAV teismas keletą kartų nesėkmingai bandė susisiekti su Rusijos valdžios institucijomis dėl bendradarbiavimo tiriant minėtų hakerių nusikalstamas veikas.[164] Tai buvo vienas iš atvejų, kuomet tarptautinis bendradarbiavimas neveikė dėl vienos iš valstybių abejingumo.

Tačiau buvo ir kita byla, kurioje valstybės bendradarbiavo, nepaisant reikiamų teisės normų nebuvimo, bet bausmės vis tiek pavyko išvengti. 2000 metais kompiuterinis virusas ,,Love Bug'' padarė žalą dešimtims milijonų kompiuterių visame pasaulyje. JAV agentai greitai atsekė į Filipinus, vietą iš kurios kilo virusas. Tačiau Filipinai savo baudžiamajame įstatyme neturėjo kriminalizavę tokios nusikalstamos veikos kaip įsilaužimas į kompiuterį.[165] Todėl niekas nebuvo nubaustas už šį nusikaltimą, spraga įstatyme padarė ekstradiciją neįmanomą.[166]

---

[159] More Naked Gun than Top Gun http://cryptome.org/jya/naked-gun.htm [žiūrėta 2013-12-29]
[160] History repeats for former hacker http://news.bbc.co.uk/2/hi/technology/4761985.stm [žiūrėta 2013-12-29]
[161] Norwegian jailed for Web racism http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/ [žiūrėta 2013-12-29]
[162] Russian Computer Hacker Convicted by Jury http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm [žiūrėta 2014-01-03]
[163] High-tech net helped FBI snag alleged hackers http://usatoday30.usatoday.com/tech/news/2001-05-09-fbi-tech-sting.htm [žiūrėta 2014-01-03]
[164] FBI "hack" raises global security concerns http://news.cnet.com/2100-1001-256811.html [žiūrėta 2014-01-03]
[165] Philippine investigators detaion man in seach for 'Love Bug' creator Clinton to attend funeral of cardinal John O'Connor http://www.mail-archive.com/htmlquicknews@cnnimail4.cnn.com/msg00036.html [žiūrėta 2014-01-03]
[166] Philippine Prosecutors Release 'Love Bug' Suspect http://partners.nytimes.com/library/tech/00/05/biztech/articles/10virus.html [žiūrėta 2014-01-03]

### 3. 3. 2. Jurisdikcijos nežinomybė debesų kompiuterijoje.

Naujausia debesų kompiuterija (angl.- iCloud Computing) ir multi-jurisdikciniai nusikaltimai gali priversti suabejoti, ar tradicinis nusikalstamų veikų tyrimas ir baudžiamasis persekiojimas yra tinkamos priemonės kovoti su elektroniniais nusikaltimais. Duomenys debesyje (angl. *Cloud*) yra perkeliami iš vieno serverio į kitą, taip judant ir sukuriant prieigą įvairiose šalyse bet kuriuo metu. Be to duomenys debesyse gali būti tik atspindėti (angl. mirrored) siekiant užtikrinti duomenų saugumą ir prieinamumą. To pasėkoje duomenys yra pasiekiami daugelyje vietų, vienoje ar keliose valstybėse. Todėl Interpolo teigimu, net ir debesų kompiuterijos paslaugas teikiantis subjektas negali tiksliai žinoti, kur yra konkreti duomenų lokacinė vieta.[167]Saugumo ir privatumo užtikrinimo klausimai yra labai svarbūs debesų kompiuterijoje. Daugumą saugumo ir privatumo problemų šioje srityje sukelia patys vartotojai, nes jiems nėra galimybės fiziškai kontroliuoti šią infrastruktūrą. Todėl būtent šioje vietoje iškyla teisinis klausimas, susijęs su debesų fizine vieta, kuria remiantis galima nustatyti jurisdikciją. Iš ko vėliau gali atsirasti problema tiriant įvykdytą nusikalstamą veiką.

DDoS atakos buvo problema ir kriminalizuota nusikalstama veika dar prieš atsirandant debesų kompiuterijai. N. Jasper gana nesenai rašė, kad DDoS atakos buvo nukreiptos ir prieš *Amazon.com* kompanijos debesis, tačiau niekur nebuvo paminėta, kad siekiant išvengti ar apsisaugoti nuo ateityje kilsiančių išpuolių kompaniją *Amazon.com*, iš debesų vartotojų bus imamas papildomas užmokestis, galimai interpretuojamas kaip saugumo mokestis[168]. Tokie ir kiti panašūs išpuoliai įtakojo Debesų saugumo aljanso (angl. Cloud Security Alliance) įsikūrimą. Tai daugiau pramonės grupė, kurios nariai yra visame pasaulyje gerai žinomos kompiuterinių technologijų kompanijos, tokios kaip *HP* ar *Microsoft*[169]. Ši pramonės grupė yra paskelbusi geriausios buvusios praktikos ir tolimesnių gairių rinkinį organizacijoms savo veiklą orientuojančioms į debesų kompiuteriją[170]. ENISA – Europos tinklų ir informacinės apsaugos agentūra paskelbė ataskaitą saugumo klausimais debesų kompiuterijoje[171]. Jie įvardino trisdešimt penkis galimus pavojus naudojantis debesų kompiuterija ir juos išdalino į šias kategorijas[172]:

- Politika ir organizaciniai pavojai;
- Techniniai pavojai;

---

[167] INTERPOL European Working Party on Informtaion Technology Crime (EWPITC) – Project on cloud computing, 2011.
[168] Jasper N. On our extended downtime, Amazon and what is coming.// October 4, 2009. http://blog.bitbucket.org/2009/10/04/on-our-extended-downtime-amazon-and-whats-coming/ [žiūrėta 2014-01-08]
[169] Cloud Security Alliance. https://cloudsecurityalliance.org/ [žiūrėta 2014-01-08]
[170] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.// 2009.
[171] Catteddu D., Hogben G. Cloud Computing: benefits, risks and recommendations for information security.// Technical Report of European Network and Information Security Agency, 2009.
[172] Ten pat.

- Teisiniai pavojai;
- Debesų kompiuterijai nebūdingi pavojai;

Taip pat savo pranešime ENISA pabrėžė, kad saugumas pigiau įgyvendinamas platesniu mastu, todėl debesų teikėjai galėtų potencialiai pateikti daugiau saugumo priemonių[173]. Jurisdikcijos problema paminėta dviejose kategorijose, t.y teisinių pavojų ir debesų kompiuterijai nebūdingų pavojų kategorijose, tačiau problemos sprendimas nebuvo įvardintas.

Aktyvus mokslininkas L. M. Kaufmanas taip pat niekuomet nebandė spręsti jurisdikcijos problemos tiriant nusikalstamas veikas šioje srityje, tik aptarė saugumo atsakomybę ir iškėlė idėją, ar debesų populiarumą lemia debesų teikėjams krentanti atsakomybė dėl bet kurios nusikalstamos veikos prieš duomenis saugomus debesyje atveju[174]. Pasitvirtinus tokiai šio mokslininko idėjai jurisdikcijos problema vartotojų atžvilgiu taptų visiškai nebeaktuali, visa našta ir įrodinėjimo reikalingumas būtų subjekto teikiančio debesijos paslaugas prievolė. Dėl kurios vėliau galėtų atsirasti probleminis klausimas dėl jurisdikcijos priskyrimo vienai ar kitai valstybei. Sekantis veiksnys sukeliantis jurisdikcijos problemą yra debesų kompiuterijos duomenų centrų geografinė vieta. Galiojantys teisės aktai konkrečioje jurisdikcijoje gali turėti reikšmingą poveikį tiek debesų teikėjui, tiek debesų vartotojui, nepaisant ar jis nukentėjo nuo elektroninės nusikalstamos veikas ar ne, o gal net jei ir pats tapo nusikalstamą veiką darančiu asmeniu[175].

Apibendrinant galime daryti išvadą, kad jurisdikcijos problema tiriant nusikalstamas veikas įvykdytas debesų kompiuterijoje šiuo metu dar nėra aktuli, plačiai išanalizuota tema teisės mokslininkų tarpe. O valstybė per teisės aktus, politiką ir reguliavimą gali arba slopinti, arba skatinti debesų kompiuteriją savo teritorijoje[176]. Tokiu atveju autorius daro išvadą, kad teisės normos šioje srityje slopina tokio pobūdžio verslą, o menkavertis teisinis reguliavimas skatina naujo tipo nusikalstamas veikas, taip paruošiant dirvą naujam elektroninių nusikaltimų rojui.

[173] Catteddu D., Hogben G. Cloud Computing: benefits, risks and recommendations for information security.// Technical Report of European Network and Information Security Agency, 2009.
[174] Kaufman L.M. Data Security in the World of Cloud Computing.// Security & Privacy, IEEE, 2009, p. 61-64.
[175] Jaeger P., Lin J., Grimes J., Simmons S. Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing.// First Monday peer-reviewed Journal in the internet, Vol. 14, 2009.
[176] Ten pat.

## IV. TEISMŲ VAIDMUO KOVOJANT SU EL. NUSIKALTIMAIS TARPTAUTINIU MASTU

Tik maža dalis asmenų, kurie per pastaruosius metus įvykdė elektroninius nusikaltimus buvo patraukti baudžiamojon atsakomybėn, o tuo labiau nuteisti. Elektroninei erdvei, kaip penktai bendrai erdvei po žemės, jūrų, oro ir kosmoso yra reikalingas koordinavimas ir bendradarbiavimas teisiniu lygmeniu tarp viso pasaulio valstybių. Labai svarbu, kad tarptautinė bendruomenė suprastų neatidėliotiną ir didėjančią elektroninio pavojaus svarbą.[177] Tarptautinis baudžiamasis teismas iki šiol yra trūkstama grandis tarptautinėje teisės sistemoje. Remiantis Jungtinių Tautų Organizacija taika ir teisingumas elektroninėje erdvėje turi būti apsaugotas, pagal visus egzistuojančius tarptautinės teisės principus, t.y. per sutartis ar sutarčių rinkinius.

Atsižvelgiant į 2013 metų Jungtinių Tautų narkotikų ir nusikalstamumo biuro – UNODC, 69 skirtingų valstybių pateiktą apklausos ataskaitą[178], teisminio proceso tobulinimas nėra būtinas. Apklausoje dalyvavusios valstybės nurodė, kad tik tarp 30% ir 70% įvykdytų elektroninių nusikaltimų apima tarptautinį lygmenį. Iš to kyla klausimas - kur slypi viso šito *modus operandi*? Atsakymas aiškus tik išanalizavus visų valstybių apklausoje pateiktus duomenis. Dauguma Europos valstybių mano, kad nacionalinių įstatymų susijusių su baudžiamuoju persekiojimu išplėtimas arba papildymas taptų tinkama priemone kovojant su kompiuteriniais nusikaltimais tarptautiniu mastu. Tačiau kituose regionuose 50% apklausoje dalyvavusių valstybių ataskaitose teigiama, jog trūksta pačios teisinės sistemos, pradedant nuo įstatymų bazės ir baigiant kompetentingais teismais, sugebančias adekvačiai įvertinti kiekvieną elektroninio pobūdžio nusikalstamą veiką. UNODC pateiktoje apklausos ataskaitoje pažymėjo, kad tarpvalstybinis teismų bendradarbiavimas visuomet vyko siekiant gauti įrodymus elektroninių nusikaltimų atvejais, iš jų 70% naudojant oficialius tarpvalstybinius teisinės pagalbos prašymus. Beveik 60% prašymų buvo skirti dvišalėms priemonėms, o tik 20% atvejų daugiašalėms priemonės užtikrinti. Taip pat UNODC pažymi, kad susitarimai tarp valstybių užtrukdavo mėnesiais, o tai sudaro kliūtis lakiųjų elektroninių įrodymų rinkime. UNODC, sulaukus kritikos iš kompiuterinių technologijų teisės srities mokslininkų - šie atsakė, kad jų apklausos ataskaitoje pateikti duomenys gali neatspindėti esamos tarptautinės situacijos ir todėl to nereikėtų vertinti, kaip realios situacijos valstybių teismų sistemose.

Iš pateiktos apklausos duomenų galima daryti išvadą, jog siekiant kovoti su elektroniniais nusikaltimais tarptautiniu mastu yra būtinas tarpvalstybinis teismų bendradarbiavimas. Remiantis Jungtinių Tautų narkotikų ir nusikalstamumo biuro apklausos duomenimis matyti, kad

[177] Schjolberg S. A presentation at the Europol-INTERPOL Cybercrime Conference.// The Hague, Netherlands, September 24-25, 2013.
[178] Expert Group to Conduct a Comprehensive Study on Cybercrime – Executive Summary, January 23, 2013 (UNODC/CCPCJ/EG. 4/2013/2) https://www.unodc.org [žiūrėta 2014-03-01]

nusikalstamos veikos turi aiškų tarptautiškumo požymį ir, kad nusikalstama veika dažniausiai apima ne vienos valstybės jurisdikciją, todėl toliau darbe autorius išanalizuos Tarptautinio Teismo kompiuteriniams nusikaltimams idėją ir Tarptautinio elektroninių nusikaltimų Tribunolo įkūrimo galimybę.

### 4. 1. Tarptautinio teismo kompiuteriniams nusikaltimams idėja.

Tarptautinio teismo kompiuteriniams nusikaltimams įkūrimo idėją pasiūlė Norvegijos teisėjas Steinas Schjolbergas, po to, kai ši idėja buvo apsvarstyta Rytų-Vakarų Instituto, Elektroninių nusikaltimų teisinės darbo grupės.[179] Šią darbo grupę sudarė visiškai nepriklausomi, nevyriausybiniai specialistai, besispecializuojantys internetinės apsaugos ir kompiuterinio nusikalstamumo srityse. Minėtos darbo grupės užduotis buvo paruošti rekomendacijas naujoms teisinėms priemonėms, kovosiančioms su kompiuteriniais nusikaltimais ir kibernetinėmis atakomis. Steinas Scholbergas siūlo Tarptautinį teismą kompiuteriniams nusikaltimams prijungti, kaip atskirą teismo skyrių prie jau egzistuojančio Tarptautinio Baudžiamojo teismo.[180] Tokią savo idėją teisėjas grindžia Romos statutu, kuris numato visų teismams reikalingų institucijų sukūrimą, vardan nusikalstamų veiksmų sustabdymo.[181] Tačiau tuo galėtų būti remiamasi tik iš dalies, nes pagal Jungtinių Tautų Chartijos septintą skyrių[182] bet kokio naujo tarptautinio teismo įsteigimas galimas tik priėmus naują Jungtinių Tautų Saugumo Tarybos rezoliuciją.[183]

Steino Schjolbergo nuomone, elektroninių nusikaltimų bylose, prokuroras yra privaloma organizacinė grandis.[184] Jam būtų suteikta išimtinė teisė tam tikrais apibrėžtais atvejais inicijuoti nusikalstamos veikos tyrimą, todėl asmenys pretenduojantys užimti tokias atsakingas pareigas privalėtų turėti atitinkamą išsilavinimą. Šioje vietoje Schjolbergas taip pat siūlo glaudų prokurorų ir Tarptautinės Kriminalinės Policijos Organizacijos, kitaip INTERPOLO bendradarbiavimą.[185] Tokiam siūlymui autorius pritaria, nes Tarptautinė Kriminalinės Policijos Organizacija nuo 1980 metų yra pagrindinė institucija tirianti tarptautinius elektroninius nusikaltimus. O nuo 1990 metų Europos, Afrikos, Šiaurės ir Pietų Amerikos ir kitų regioninių INTERPOLO darbo grupių vadovai ir nariai yra patyrę specialistai kovojant su tarptautiniais kompiuteriniais nusikaltimais. Be to kompiuterinių nusikaltimų tyrime galėtų padėti The INTERPOL Digital Crime Centre (IDCC) –

[179] EastWest Institute (EWI) was founded in 1980 in order to enable individuals, institutions and nations to communicate through a network across the borders.
[180] Schjolberg S. Peace and Justice in Cyberspace.// Norway, 2012, p. 3.
[181] Jungtinių Tautų Chartija, Valstybės žinios, 2002-03-13, Nr. 15-557. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=211305&p_query=&p_tr2 [žiūrėta 2014-03-01]
[182] Ten pat.
[183] Kraft W., Streit C. Ideas on the Establishment of an Inernational Court for Cyber Crime.// Germany, WCLF, 2011, p. 7.
[184] Schjolberg S. Peace and Justice in Cyberspace.// Norway, 2012, p. 3-4.
[185] Ten pat.

Skaitmeninis Interpolo Nusikaltimų Centras, kuriame nuo 2014 metų vidurio dirbs per tris šimtus darbuotojų, o pati centro veikla bus sistemingai suskirstyta į paramą elektroninių nusikaltimų tyrimui, moksliniams tyrimams ir inovacijoms, bei kibernetiniam saugumui užtikrinti.[186]

Kita S. Schjolbergo siūloma pagalbos grandis, yra siūlymas sukurti pasaulinę virtualią specialistų grupę (angl. Global Virtual Taskforce Group) susidedančią iš suinteresuotų valstybių pasaulinės informacijos ir ryšių technologijų pramonės, finansinių paslaugų pramonės, privataus sektoriaus, ne vyrausybinių organizacijų, teisėsaugos institucijų ir akademinės bendruomenės specialistų.[187] Tokiu atveju, autoriaus nuomone, tai galėtų būti specialistai iš „Yahoo", „Google", „Youtube", „Apple", „Facebook" - tačiau kyla klausimas ar tai leistų pačios kompanijos, kad jų darbuotojai atliktų kitas, su darbo santykiais nesusijusias funkcijas darbo metu. Savaime suprantama, kad toks virtualių grupės specialistų išsidėstymas įvairiose geografinėse vietose būtų veiksminga priemonė kovojant su pasaulinio masto elektroniniais nusikaltimais, ypač bandant pažaboti realaus laiko kompiuterines atakas. Taip pat, tokia specialistų darbo grupė gebėtų ne tik užkardyti daromas nusikalstamas veikas realiu laiku, bet ir ženkliai pagerintų prokurorų darbą veiksmingai tiriant ir traukiant baudžiamojon atsakomybėn kompiuterinių nusikaltimų organizatorius.

Sekanti, ne tik Tarptautinio Teismo kompiuteriniams nusikaltimams sukūrimo, bet ir sėkmingo egzistavimo problema yra elektroninių nusikalstamų veikų diversiškas pobūdis. Visų elektroninių nusikaltimų pagrindas yra netradicinė technologinė aplinka, kurioje yra įvykdomi nusikaltimai. Tokia aplinka leidžia nusikaltimą vykdantiems asmenims likti nepastebimiems ir nebijoti būti sugautiems nusikaltimo darymo metu, jau nekalbant apie suėmimą ir patraukimą baudžiamojon atsakomybėn.[188] Todėl atrodo, kad kompiuteriniai nusikaltėliai kuria naujus nusikalstamų veikų įgyvendinimo metodus tokiu tempu, kad net pačios moderniausios technologijos negali apsaugoti.[189] Dėl šios priežasties didžioji dalis elektroninėje erdvėje padarytų nusikaltimų yra latentinio pobūdžio, nusikalstama veika lieka nepastebėta.[190] Akivaizdu tai, kad kuo ilgiau nusikaltimas kuriamas ir organizuojamas, tuo jis sunkiau išaiškinamas ir už jį nubaudžiama.

Saugumo tyrinėtojas Sandro Gaycken iš Vokietijos išskyrė keturis pagrindinius veiksnius, kurie, jo nuomone, apsunkina nusikaltimo tyrimą ir todėl nubausti už elektroninį nusikaltimą tampa

[186] The INTERPOL Global complex for Innovation. http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI [žiūrėta 2014-03-05]
[187] Schjolberg S. Peace and Justice in Cyberspace.// Norway, 2012, p. 5.
[188] Deloitte Center for Security and Privacy Solutions. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat. Deloitte. 2010, p. 4.
[189] Deloitte Center for Security and Privacy Solutions. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat. Deloitte. 2010, p. 5.
[190] Deloitte Center for Security and Privacy Solutions. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat. Deloitte. 2010, p. 6.

beveik nebeįmanoma.[191] Tuo pačiu tai yra veiksniai paneigiantys kompiuterinės baudžiamosios teisės naudingumą ir Tarptautinio Teismo kompiuteriniams nusikaltimams efektyvumą. Taigi Sandro Gayckeno išskirti veiksniai:

- *Fizinių įkalčių lakumas.* Tai reiškia, kad beveik jokie fiziniai nusikaltėlio pėdsakai nusikaltimo vykdymo metu nepaliekami.
- *Neratyvus priešiškos programos požymis* – kompiuterinės atakos kodas yra kažkieno sąmoningai sukurta kalba siekiant suklaidinti kompiuterinės nusikalstamos veikos tyrėjus.
- *Žmogaus ir kompiuterinės įrangos skirtumas*. Atsekus kompiuterį arba kompiuterius, kuriais pasinaudojant buvo atlikta kompiuterinė nusikalstama veika, jie niekada nesakys kas naudojosi tuo kompiuteriu ir kokie buvo atliktų veiksmų motyvai. Tai reiškia, kad kompiuterinė įranga negali atlikti liudytojų vaidmens baudžiamuosiuose teismuose.
- *Ginklų naudojamų kibernetiniame kare universalumas*. Kompiuteriai, USB atmintinės ir bendro naudojimo programos gali būti panaudojamos blogiems tikslams turint programavimo žinių pagrindus. Tačiau tiesioginis ginklas žmogžudystėms negali būti sukurtas.

Kita problema apsunkinanti kompiuterinių nusikaltimų tyrimą yra tai, kad konkuruojančių kompiuterinių programų autoriai-kūrėjai savo sugebėjimus ,,išnuomoja" kompiuterinių technologijų srityje besispecializuojantiems nusikaltėliams.[192] Tokia veiklos rūšis, autoriaus nuomone, gali būti prilyginama samdomiems žudikams, nes jie taip pat neturi asmeninio motyvo ir ji visiškai paneigia anksčiau paminėtą Norvegijos teisėjo Steino Schjolbergo nuomonę, jog prokurorams Tarptautiniame Teisme kompiuteriniams nusikaltimams talkinti galėtų pasaulinė virtualių specialistų grupė (angl. - Global Virtual Taskforce Group) susidedanti iš suinteresuotų valstybių pasaulinės informacijos ir ryšių technologijų pramonės, finansinių paslaugų pramonės, privataus sektoriaus, nevyriausybinių organizacijų, teisėsaugos institucijų ir akademinės bendruomenės specialistų. Elementaru, kad būtų labai sunku sukontroliuoti ar šios siūlomos darbo grupės specialistai nedirba nusikaltėliams. Tokios veikos kylančios iš prieš tai minėtų veiksmų nekriminalizavimas šiuo metu yra plačiai diskutuojamas tarp teisės ekspertų.[193] Taip pat jau egzistuojanti ties yra tai, kad informacinių technologijų ekspertai dirbantys teismuose jau dabar patiria didžiulį spaudimą šiuo klausimu[194].

[191] Gaycken S. Krieg der Rechner in: Internationale Politik.// April, 2011, p. 88-95.
[192] Deloitte Center for Security and Privacy Solutions. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat. Deloitte, 2010, p. 5.
[193] Sylvia M. Kierkegaard in cooperation with FU Berlin and UNIDIR. The conference on ,,Challenges in Cybersecurity". December, 2011.
[194] Ten pat.

Apibendrinant galima teigti, kad Steino Schjolbergo iškelta Tarptautinio Teismo kompiuteriniams nusikaltimams idėja yra sveikintina, tačiau nėra taip paprastai įgyvendinama, kaip gali atrodyti iš pirmo karo. Tačiau, autoriaus manymu, norint įgyvendinti tokią ryžtingą idėją, kovoje su elektroniniais nusikaltimais reikėtų pasiekti kritinį bejėgiškumo tašką viso pasaulio mastu.

### 4. 2. Tarptautinio Tribunolo tinkamumas teisti už elektroninius nusikaltimus

Prieš dvidešimt metų pasaulis pamatė pirmąjį komercinio pobūdžio internetinį puslapį.[195] Maždaug tuo pat metu, pasaulis pamatė pirmąjį Jungtinių Tautų įgaliotą baudžiamąjį teismą. Tokio pobūdžio teismas buvo visiškai naujo tipo, įsteigtas remiantis statutu ir įgaliotas Jungtinių Tautų Saugumo Tarybos.[196] 1993 metų gegužę ir 1994 metų lapkritį buvo įsteigti Tarptautiniai Baudžiamieji Tribunolai buvusiai Jugoslavijai[197] ir Ruandai.[198] Visais kaip ir šiais autoriaus paminėtais atvejais Tribunolai organizuojami siekiant patraukti asmenis baudžiamojon atsakomybėn už tokius nusikaltimus, kaip neteisėtas karas ir kitus sunkius, žiaurius ir labai didelę grėsmę žmonijos saugumui keliančius nusikaltimus. Tarptautinio Tribunolo veikimo pagrindas yra tarptautinės teisės normos.[199] Todėl tarptautinei bendruomenei iki šiol egzistuoja galimybė drauge kurti elgesį internete reglamentuojančias tarptautines teisės normas.[200] Šios normos nustatytų kas yra leidžiama, o kas ne, kokių kompiuterinių atakų atveju būtų panaudojama jėga ir kokios būtų sankcijos už šiuos normų nusižengimus.

Prieš kompiuterines atakas, kaip ir prieš tikro ginklo panaudojimą gali būti nukreiptas teisėtas jėgos panaudojamas siekiant apsaugoti saugomas nacionalines vertybes. S.R. Stevens teigimu, kai kurios kompiuterinės atakos galima būtų prilyginti kinetiniams kariniams išpuoliams.[201] Skirtumai yra tik tai, kad kompiuterinės atakos gerokai sumažina grėsmę gyvybei ir nuosavybei. Todėl labiau humaniška yra išjungti elektrinę kompiuterinės atakos būdu, nei bombarduoti ją kartu su joje esančiais žmonėmis. Kitas privalumas, kurį turėtų įžvelgti tarptautinių normų rengėjai yra galimybė iš naujo įvertinti standartus dėl karinių veiksmų. Remiantis dabartine tarptautine teise, kariniai veiksmai negali būti nukreipti į civilius asmenis įskaitant ir jų asmeninį

---

[195] Global Network Navigator. http://oreilly.com/gnn/. GNN was the first commercial website, launched August 1993.
[196] Brooks R. The Politics of the Geneva Conventions: Avoiding Formalis Traps.// J. INT. L., 2005, p. 197.
[197] United Nations, International Criminal Tribunal for the Former Yugoslavia. http://www.icty.org [žiūrėta 2014-01-20]
[198] United Nations, International Criminal Tribunal for Rwanda. http://69.94.11.53/ [žiūrėta 2014-01-20]
[199] The Secretary-General, Report on Aspects of Establishing an International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yougoslavia. U.N Doc. S/25704 (May 3, 1993).
[200] Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 293.
[201] Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18., Issue 1,2008.

turtą. Toks elgesys yra laikomas amoraliu ir neteisėtu. Tačiau jei karinė kompiuterinė ataka sukėlė nepatogumą, ekonominę žalą valstybei ir tai palietė civilius gyventojus, kaip kad nutiko 2007 metais Estijoje, ar tai galime prilyginti įprastiems kariniams veiksmams?

### 4. 2. 1. Kompiuterinių atakų prieš Estiją prilyginimas įprastiems kariniams veiksmams.

2007 metų balandžio mėnesio pabaigoje - gegužės mėnesio pradžioje Estijoje buvo įvykdytos masinės kompiuterinės atakos, kuriuos Duncan B. Hollis paprasčiausiai prilygino kariniams veiksmams[202]. Atakų metu atlikti veiksmai buvo labai paprasti. Pradedant Estijos vyriausybės internetiniu puslapiu ir baigiant valstybinių laikraščių, ligoninių, bankų, universitetų internetiniais puslapiais, kurie buvo atakuojami duomenų užklausomis.[203] Internetiniai puslapiai pasitelkus vadinamuosius kompiuterinius zombius buvo perkrauti iš jų siunčiamomis įvairiomis užklausomis, ir taip paprasčiausiai sutriko jų veikimas.[204] Daugiau nei milijonas kompiuterinių zombių dalyvavo šių kompiuterinių atakų metu.[205] Tačiau ne visi tikslai kompiuterinių išpuolių metu buvo įgyvendinti. Jie taip pat turėjo paralyžiuoti medicinos įstaigų, ugniagesių ir interneto paslaugų teikėjų darbą.[206] Skirtingai nuo prieš tai pasaulyje įvykdytų kompiuterinių atakų, Estijoje atakos vyko net kelias savaites.[207]

Kompiuterinės atakos sukėlė rimtus ekonominius nuostolius ir politines pasekmės. Didžiausias Estijos bankas buvo priverstas nutraukti savo internetinių paslaugų teikimą daugiau nei valandai, kol galiausiai išvis uždraudė vartotojams iš užsienio prisijungti prie savo serverio.[208] Vėliau ir kitų įstaigų administruojamos internetinės svetainės pasekė jų pavyzdžiu.[209] Tokia sąlyginė Estijos izoliacija nuo likusio pasaulio sukėlė didžiulį Estijos vyriausybės pasipiktinimą. Kompiuterinių atakų padariniai, C. Wilson nuomone, be didesnių klausimų gali būti prilyginami tiesioginiam Estijos pasiuntimui į krizę.[210] To pasėkoje Estija iškeldino visus sovietinio karo memorialus stovėjusius lankomose vietose. Tokiems veiksmams Rusijos vyriausybė aktyviai

---

[202] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1024.
[203] Ten pat.
[204] Steven L.M.'E-stonia' Accuses Russia of Computer Attacks. N.Y. TIMES, May 18, 2007. http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h. [žiūrėta 2014-01-20]
[205] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1026.
[206] Ten pat.
[207] Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 3. January 29, 2008. https://www.fas.org/sgp/crs/terror/RL32114.pdf [žiūrėta 2014-01-21]
[208] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1026.
[209] Ten pat.
[210] Melnick J. The Cyber War Against The United States.// Boston Globe. August 19, 2007.

prieštaravo, iki to momento, kai Estija pajuto poreikį kovoti su Rusijos skleidžiama propaganda.[211] Tačiau kompiuterinių atakų pasekmės buvo apribojusios Estijos galimybes paaiškinti susiklosčiusią situaciją su Rusija visam likusiam pasauliui.

Estija apkaltino Rusiją dėl kompiuterinių išpuolių, tačiau Rusija tai kategoriškai neigė.[212] Pasak Estijos gynybos ministro, tokie dvi savaites trukę išpuoliai turi būti interpretuojami ne kaip chuliganizmas, o kaip karinė ataka prieš valstybę.[213] Tačiau su tokia nuomone nesutiko ir Šiaurės Atlanto Sutarties Organizacija, kitaip žinoma kaip NATO, nes anot jų, tokie veiksmai negali būti prilyginami jokiems kariniams veiksmams.[214]Apžvalgininkai, analizavę situaciją Estijoje, veiksmus įvertino kaip paprastą nusikalstamą veiką, bet jokiu būdų jos neprilygino terorui, kiti kilusius padarinius prilygino ginkluotų veiksmų sukeltiems padariniams.[215]

Be to Estijai buvo sunku nustatyti kas iš tiesų įvykdė kompiuterines atakas ir kas privalo atsakyti už kilusius padarinius.[216] Kai kurie ekspertai mano, kad įvykdytos atakos prieš Estiją nebuvo remiamos valstybės:

*,,Po ilgo tyrimo, tinklo specialistai nustatė, kad kompiuterinės atakos prieš Estiją nebuvo viena suderinta tęstinė ataka, bet nepaisant to, tai buvo spontaniškas pykčio iššauktas veiksmas, kurį atliko keli skirtingose lokacinėse vietose buvę asmenys. Techniniai duomenys parodė, kad kompiuterinių atakų šaltiniai buvo išsiskirstę po visą pasaulį, o ne susitelkę keliose vietose. Kompiuterinis kodas, kuris sukėlė DDoS atakas buvo paviešintas ir platinamas daugelyje rusiškų pokalbių kambariuose, kur sovietinių memorialų perkėlimo tema buvo labai aktyviai diskutuojama. Analitikai taip pat teigia, kad nepaisant prieigos prie Estijos vyriausybinių įstaigų užblokavimo pasitelkus kenksmingą kodą, nebuvo aišku, ar atakų tikslas tikrai nebuvo tik interneto prieigos sutrikdymas...''*[217]

Tam tikra prasme, tikroji kompiuterinių atakų kaltininkų tapatybė yra mažiau svarbi lyginant su patirtimi, kurią Estija perdavė visam pasauliui. Estija dvi savaites trukusias kompiuterines atakas įvertino kaip priešo karinius veiksmus.[218] Estijos pakantumas šiam išpuoliui priskiriamas daugiau politinėms realijoms, nei jų pačių polinkiams. Tačiau teisės srities ir karybos

---

[211] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1027.
[212] Ten pat.
[213] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1026.
[214] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1028.
[215] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1026.
[216] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1025-1027.
[217] Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 3. January 29, 2008. https://www.fas.org/sgp/crs/terror/RL32114.pdf [žiūrėta 2014-01-21]
[218] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1025-1027.

specialisto B. Davis nuomone, jei atakos nukreiptos prieš Estiją būtų vykdomas įprastiniu būdu, pasitelkiant įprastus ginklus, tarptautinei teisei būtų pravartu turėti normas, kurios atsakytų į klausimą ar atakos yra teisėtos, t.y. ar kariniai veiksmai yra pateisinami.[219] Estijos atvejis nėra vienintelis istorijoje, 2008 metų rugpjūtį Gruzijoje buvo įvykdytos panašaus tipo išpuolis[220], todėl tarptautinė bendruomenė turėtų susirūpinti siekiant apsaugoti panašaus išpuolio aukas nuo karinių veiksmų pateisinimo.

Reziumuojant galima teigti, kad kompiuterinės atakos, pasitelkus kompiuterinius tinklus, prieš Estiją buvo visiškai neteisėti veiksmai, bet tikriausiai ne tokie amoralūs, kaip įprasto karinio išpuolio metu. Autorius visiškai pritaria S. R. Stevens nuomonei, kad ir civiliai gyventojai tiesiogiai jaučia tokių išpuolių poveikį.[221] O šiuolaikinės jėgos panaudojimo kontekste tai gali būti priimtina, jei tai sumažina galimybę kinetiniam armijos įsikišimui ir tolimesniems gyvybių praradimams.[222]

### 4. 2. 2. Kibernetinė ataka tolygu jėgos panaudojimui

Teisės mokslininkas D.Hollis išskiria tris metodus taikant JT Chartijos 2 straipsnyje numatytą jėgos panaudojimo doktriną, kompiuterinėms atakoms. Pirmasis – žinybinis metodas.[223] Remiantis tradicine Chartijos 2 straipsnio 4 dalies analize, kompiuterinės atakos negali būti laikomos ginkluotu užpuolimu, nes jos neturi fizinės savybės – tradicinio karinio užpuolimo.[224] Norint tai pagrįsti, vertėtų atkreipti dėmesį į Jungtinių Tautų Chartijos 41 straipsnį, kuris leidžia visišką ar dalinį tam tikrų, tai yra oro, pašto, radijo ir kitų santykių nutraukimą, neįtraukiant ginkluotos jėgos panaudojimo.[225] Kadangi dauguma kompiuterinių atakų tikslų ir yra nutraukti tam tikrus ryšius, kitų formų agresiniai išpuoliai privalo būti įrodyti, norint juos pripažinti ginkluotu užpuolimu remiantis Jungtinių Tautų Chartija.

Antrasis metodas yra vadinamas tiksliniu metodu, kuris yra orientuotas į tikslo pobūdį.[226] Kuomet kompiuterinėmis atakomis siekiama kritinės nacionalinės infrastruktūros, visiškai

---

[219] Davis B. A Proposal for an Internatonal Convention to Regulate the Use of Informations Systems in Armend Conflicts. Vol. 47, No. 1, 2006. http://www.harvardilj.org/attach.php?id=59 [žiūrėta 2014-01-23]
[220] Markoff J. Before the Gunfire, Cyberattacks. N.Y. Times. August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 [žiūrėta 2014-01-23]
[221] Stevens S. R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 658-714.
[222] Ten pat.
[223] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1041.
[224] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1042.
[225] Jungtinių Tautų Chartija, Valstybės žinios, 2002-03-13, Nr. 15-557. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=211305&p_query=&p_tr2 [žiūrėta 2014-03-01]
[226] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1042.

nepriklausomai nuo žalos masto, tai jau ir yra ginkluotas išpuolis.[227]Taip pat Hollis pažymi, kad tikslinis metodas pasireiškia per įtraukimą: Kompiuterinė ataka gali sukelti plataus masto žalą, nuo informacinės (propaganda) iki laikinų nepatogumų (sutrikdyti sistemų darbą), potencialiai pavojingų (implantuoti loginę bombą, kuri neturi tiesioginės žalos, tačiau turi galimybę tokią žalą sukelti ateityje) arba iš karto destruktyvų (nuolatos išjunginėti sistemą pasitelkiant į pagalbą virusus).[228] Idėjos apie proporcingumą ir teisingumą sukelia grėsmę sulaukti susidorojimo atakų, panaudojant įprastas priemones arba kibernetinę erdvę. Kadangi į tikslą orientuotas požiūris leistų naudoti karines arba kompiuterines atsakomąsias priemones, bet kokiai atakai prieš kritinius subjektus atremti, toks būdas laikomas per daug drastišku. Tokia reakcija prieštarauja Jungtinių Tautų Chartijoje nurodytam pagrindiniam tikslui – palaikyti tarptautinę taiką ir saugumą.[229]

Paskutinis metodas – pasekmės metodas, akcentuoja atakos padarinius.[230] Jei kompiuterinės atakos sukelia tokius pačius padarinius – mirtis ir turto sunaikinimas, kaip ir kinetinė ataka, tuomet yra leidžiama naudoti savigyną, remiantis Jungtinių Tautų Chartijos 51 straipsniu.[231] Kompiuterinė ataka, kuri išjungia valstybės ypatingos svarbos infrastruktūros dalį galimai sukelia daugiau žalos nei tradiciniai kariniai išpuoliai. Žinoma valstybė dėl kompiuterinių atakų patirtos žalos gali turėti pretenzijų dėl restitucijos tose srityse, kuriose patyrė žalą. Kadangi pasekmės metodas sutelkia dėmesį į tos pačios rūšies fizinę žalą, kaip ir įprasta karinė ataka, tai nesudaro pagrindo kitaip apsaugoti ypatingos svarbos infrastruktūros objektus.

Barkham Jonson nustato ir kitų trūkumų kompiuterinėms atakoms taikant Jungtinių Tautų Chartijos jėgos panaudojimo doktriną. Chartija yra grindžiama visų jos narių suverenios lygybės principu.[232] Teroristinės ir nevalstybinės grupės nėra įtrauktos.[233] Jungtinių Tautų Chartijos sistema turėjo reikšmę dar prieš atsirandant internetui ar kovojant su terorizmu. Tuo metu naudoti karinę jėgą prieš civilius gyventojus buvo netinkama ir neteisėta.[234] Tačiau dabar, nevalstybiniai subjektai gali padaryti tokią žalą, kurią anksčiau buvo galima prilyginti tik valstybės remiamiems kariniams išpuoliams.

---

[227] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1041.
[228] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1042.
[229] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1040.
[230] Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007, p. 1041.
[231] Jungtinių Tautų Chartija, Valstybės žinios, 2002-03-13, Nr. 15-557. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=211305&p_query=&p_tr2 [žiūrėta 2014-02-27]
[232] Barkham J. Information Warfare and International Law on the Use of Force.// New York University, N.Y.U. Journal of International Law and Politics. Fall 2001. http://www1.law.nyu.edu/journals/jilp/issues/34/pdf/34_1_b.pdf [žiūrėta 2014-02-27]
[233] Ten pat.
[234] Ten pat.

Pabaigai, atsimenant prieš tai autoriaus išanalizuotą Estijos atvejį, galima teigti, kad civiliai agresoriai įgiję pirminius kompiuterinius įgūdžius gali sukelti tiek pat žalos, kiek sukelia karinė ataka. Humanitarinės tarptautinės teisės sritis neatitinka šiuolaikinės tarptautinės bendruomenės poreikių, kuomet humanitarinė teisė bent kiek kertasi su kompiuterinėmis technologijomis. Tarptautine teisė turėtų padėti užkirsti kelią kompiuterinėms atakoms ir padėti įgyvendinti teisingumą šalyje, patyrusioje kompiuterinių atakų išpuolius. O tarptautinė bendruomenė turėtų stengtis sukurti naujus humanitarinės teisės ir kompiuterinių technologijų standartus, kurie konkrečiai būtų taikomi tik kompiuterinėms atakoms, siekiant suformuoti tinkamą pamatą kovojant ir užkardant tolimesnius tokio pobūdžio išpuolius.

### 4. 2. 3. Tarptautinio tribunolo reikalingumas.

Hagos taisyklių ir Ženevos Konvencijos kūrimo metu, dauguma karo kovotojų buvo kombatantai.[235] Valstybės praradusios ištisus kaimus, brolius, tėvus ir vyrus pajuto tikrą karo kainą. Tačiau, dėka šiuolaikinių technologijų gyvybių kare prarandama vis mažiau. Galbūt tokią situaciją įtakoja, samdomų kareivių skaičiaus didėjimas.

Irako kare, JAV karinių pajėgų pusėje dirba 160000 samdomų kareivių.[236] Laisvai samdomų karių įtraukimas į karines operacijas palengvina politinę įtampą, tačiau kaina kurią mes šiandien mokame už karą ateina iš mūsų pačių kišenių. Didelę ekonominę žalą valstybei yra siekiama padaryti būtent per kompiuterines atakas. M. Romero teigimu, kompiuterinės grėsmės internetinio tinklo būdu turi naudą[237]. Jo nuomone, internetas, kaip biologinis organizmas sustiprėja, kuomet jis atakuojamas iš išorės, o nauji gynybos ir saugos būdai sukuriami tik susidūrus su naujais pavojais.[238] Puolimo metu patirtas stresas sąlygoja geresnę bendrą sistemą, nes technologijos privalo keistis, norit apsisaugoti nuo naujai kylančių grėsmių.[239] Remiantis šiuo mokslininko pateiktu imunologiniu požiūriu, paprasti civiliai žmonės jaučia kompiuterinės atakos pasekmes, todėl inovacijos ieškant naujų būdų, kaip išspręsti karinius konfliktus yra grindžiamos mažesniu agresijos, nukreiptos prieš civilius asmenis, pasirinkimu. Todėl, visas pasaulis turėtų iš naujo įvertinti Hagos ir Ženevos Konvencijas, siekiant tinkamai atsižvelgti į kompiuterinių atakų pavojingumą ir į teisėtos jėgos panaudojimą, kaip atsakomuosius veiksmus į kompiuterinius išpuolius internetinio tinklo pagalba.

---

[235] McCormich Tribune Foundation. Understanding the Privatization of National Security. 2006. p. 33-34
[236] The Dark Truth about Blackwater. http://www.brookings.edu/research/articles/2007/10/02militarycontractors [žiūrėta 2014-03-01]
[237] Romero M.P. An Immunological Appeoach to Counter-Terrorism and Infrastructure Defense Law in Electronic Domains.// International Journal of Law & Information Technology, 14(1), 2006, p. 101-136.
[238] Ten pat.
[239] Ten pat.

Tarptautinei bendruomenei būtų naudinga leisti tam tikrų rūšių kompiuterinių atakų panaudojimą kaip teisėtas jėgos priemones, tačiau lieka ir kita dalis kompiuterinių atakų rūšių, kurios turėtų būti pripažintos savaime neteisėtomis. R. Stevans nuomone, draudžiamos atakos turėtų būti tos, kuriomis yra siekiama niokojimo ir civilių žmonių žūties, kaip kad yra numatyta Ženevos Konvencijoje.[240] Kompiuterinė ataka, kuri priverčia atsidaryti užtvankas ir užtvindo civilių žmonių gyvenamas zonas, to pasėkoje žudydama žmones ir niokodama jų turtą privalo būti laikoma karo nusikaltimu arba nusikaltimu žmonijai ir už tai privalo bausti tarptautinis Tribunolas.[241] Kadangi internetiniai tinklai sukuria skirtingą jėgos panaudojimo supratimą, specialios taisyklės pasauliniam tinklui yra būtinos ir S. Schjolbergo nuomone.[242] Nes iki šiol tarptautinėje teisėje nėra jokio aiškaus atsakymo dėl valstybės remiamų kompiuterinių išpuolių teisėtumo. Kai kurių teisės mokslininkų nuomone, kompiuterinės atakos nepatenka į jėgos panaudojimo apibrėžimą, nes tai nėra ginkluotas užpuolimas pagal 2(4) ir 41 straipsnius iš Jungtinių Tautų Chartijos.[243] Tačiau T. Jensen nuomonė yra priešinga prieš tai išreikštai nuomonei, nes jis teigiama, kad būtent kompiuterinės atakos sukelti padariniai nulemia tokio pobūdžio išpuolių teisėtumą.[244]

Vis dėlto reziumuojant galima teigti, kad dabartinės teisės normų ribos įtvirtintos Jungtinių Tautų Chartijoje privalo būti keičiamos, nes neatitinka šiuolaikinių karinės jėgos panaudojimo sąvokos suvokimo tendencijų. Teisės normos šiuo aptariamu klausimu privalo būti aiškios, nes dabar kompiuterinės atakos yra galingas ginklas neturintis aiškių teisėtumo ribų. Tokiomis atakomis galima nepastebimai manipuliuoti labai ilgą laiko tarpą. Paslėptomis kompiuterinėmis atakomis, interneto pagalba, galima kariauti nematomą karą, kuris laikui bėgant gali sukelti rimtą žalą valstybinių organizacinių sistemų naudingumui.[245] Nes valstybei įvykus panašiam kaip Estijos atvejui, būtų pravartu turėti aiškias tarptautines taisykles, kuriomis remiantis galėtų būti pradėtas tarptautinis baudžiamasis persekiojimas prieš asmenis, kompiuterinėmis atakomis sukėlusius tokią žalą. Be to tarptautinė teisė turėtų plačiau išaiškinti nevalstybinių subjektų apibrėžimą, integruojant į jį kompiuterinėmis technologijomis pažeidžiamus subjektus.[246] Kuomet kompiuterinės atakos yra valstybinio pobūdžio su jomis turi būti kovojama remiantis nacionalinėmis baudžiamosios teisės normomis ir 2001 m. priimta Konvencija dėl elektroninių nusikaltimų. Tačiau, kuomet

[240] Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 703.
[241] Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 704.
[242] S. Schjolberg. A Presentation at the Europol-INTERPOL Cybercrime Conference.The Hague, The Netherlands, September 24-25, 2013, p. 1-15.
[243] Vida M., Jenkins A. Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?.// Naval Law Review, Vol. 51, 2005, p. 132-139.
[244] Jensen E.T. Computer Attacks on Critical Natinal Infrastructure: A Use of Force Invoking the Right of Self-Defense.// Stanford Journal of International Law, Vol. 38, 2002, p. 223-226.
[245] Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 704.
[246] Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 705.

kompiuterinės atakos kelią grėsmę tarptautinei taikai ir saugumui, per negailestingą ir siaubingą padarinių sukėlimą, tai turėtų būti laikoma karo nusikaltimu, nepaisant ar ataką sukėlusią tokius padarinius įvykdė valstybės pareigūnas ar paprastas asmuo. O už tokius veiksmus tiek autoriaus tiek ir S.R Stevens nuomonės[247] sutampa, bausti turėtų , kaip ir iki šiol – karo nusikaltimų Tribunolas.

[247]Stevens S.R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008, p. 706.

## IŠVADOS

1. Egzistuojančias teisines kovos priemonės su elektroniniais nusikaltimais galima skirstyti į: tarptautinių organizacijų kuriamas priemones, pavienių valstybių arba valstybių grupių kuriamas priemones, regionines (geografines) teisines priemones. Tarptautinių ir regioninių organizacijų kuriamos priemonės yra iš esmės panašios, tačiau neprivalomo, o rekomendacinio pobūdžio. Priemonių įgyvendinimas paliekamos pačioms valstybėms, o raginimai prisijungti jau prie esamos Konvencijos atspindi tarptautinių organizacijų nekūrybiškumą ir menką pačių iniciatyvos norą. Pavienių valstybių arba valstybių grupių kuriamos priemonės yra greičiau įgyvendinamos, tačiau veikimo ribos apsiriboja labai siauriai, dažniausiai tik valstybių teritorijomis. Atsižvelgiant į esamą padėtį elektroninių nusikaltimų srityje su šia problema reikia kovoti nedelsiant. Reikia skatinti tiek tarptautinių organizacijų, tiek ir nacionaliniu interesu kuriamas naujas kovos priemones su elektroniniais nusikaltimais. Jokių būdu nepaliekant reikiamų sprendimų ateičiai.
2. 2001 metų Konvencija dėl elektroninių nusikaltimų nepasiekė savo juridinės populiarumo viršūnės, nesukūrė tokių teisinės kovos priemonių su elektroniniais nusikaltimais, kokių iš jos buvo tikėtasi. Pagrindinės to priežastys yra santykinai mažas sutartį pasirašiusių ir ratifikavusių valstybių skaičius, sunkiai nacionaliniame lygmenyje įgyvendinamos technologinės ir procesinės priemonės. Tačiau Konvencijos efektyvumas santykinai proporcingas valstybės pasirašymo ir ratifikavimo laikui, bei įtakai šios srities tarptautinėje teisėkūroje. Naujos tarptautinės sutarties ar tarptautinio teisės akto reikalingumas negali būti grindžiamas nepasiteisinusia Konvencija dėl elektroninių nusikaltimų, nes jokia teisėta teisės forma negali būti grindžiama prievarta, šiuo atveju priverstiniu prisijungimu o vėliau ir priverstine teisės normų harmonizacija. Todėl efektyviausia yra palikti galiojančią 2001 metų Konvencija dėl elektroninių nusikaltimų, o teisines spragas papildyti leidžiamais naujais papildomais protokolais.
3. 2001 metų Budapešte priimtos Konvencijos dėl elektroninių nusikaltimų 22 straipsnio normos remiasi tik teritorijos ir pilietybės jurisdikcijų teorijomis, todėl ne visais atvejais jos yra pajėgios užtikrinti, kad asmuo būtų nubaustas už padarytą nusikaltimą. Didžioji dalis sėkmės kovojant su tarptautiniais elektroniniais nusikaltimais priklauso nuo valstybių geros valios, t.y. tarpvalstybinio bendradarbiavimo, kuris baudžiamojoje teisėje yra neatskiriamas nuo jurisdikcijos. Be to kovą su šios rūšies nusikaltimais apsunkina jurisdikcijos ribų neaiškumas ne tik debesų kompiuterijoje, bet ir apskritai visoje elektroninėje erdvėje.
4. Siekiant kovoti su elektroniniais nusikaltimais tarptautiniu mastu yra būtinas tarpvalstybinis teismų bendradarbiavimas. Tačiau Steino Schjolbergo iškelta Tarptautinio Teismo

kompiuteriniams nusikaltimams sukūrimo idėja galėtų būti įgyvendinta tik pasiekus kritinį bejėgiškumą kovojant su elektroniniais nusikaltimais tašką pasauliniu mastu. Be to Jungtinių Tautų Chartijoje įtvirtintos teisės normos neatitinka šiuolaikinių karinės jėgos panaudojimo sąvokos tendencijų. Šiuo metu kompiuterinės atakos yra galingas ginklas neturintis aiškių teisėtumo ribų. Ir jei jomis keliama grėsmė tarptautiniai taikai ir saugumui, tai turėtų būti laikoma karo nusikaltimu, nepaisant ar ataką įvykdė valstybės pareigūnas ar paprastas pilietis. O už tokius veiksmus turėtų bausti karo nusikaltimų tribunolas.

## LITERATŪROS SĄRAŠAS

**Knygos ir vadovėliai:**


1. Britz T.M. Computer Forensics and Cyber Crime: An Introduction.// Person Education, 2009.
2. Brooks R. The Politics of the Geneva Conventions: Avoiding Formalis Traps.// J. INT. L., 2005.
3. Civilka M., Lamanauskas T., Osinaitė G., Sauliūnas D. ir kt. Informacinių technologijų teisė.// Vilnius, NVO Teisės Institutas, 2004.
4. Clough J. Principles of Cybercrime.// New York, USA, Cambridge University Pres, 2010.
5. Fooner, M. Interpol: Issues in World Crime and International Criminal Justice.// New York and London, Springer, 1989
6. Gaycken S. Krieg der Rechner in: Internationale Politik.// Berlin, April, 2011.
7. Gercke M. National, Regional and International Legal Approacges in the Fight against Cybercrime.// 2008.
8. Gercke M. Understanding Cybercrime: A Guide for Developing Coutries.// ITU Telecommunication Development Sector Second Edition. 2011.
9. Ghosh S, Turrini E. Cybercrimes: A Multidisciplinary Analysis.// Springer, 2010.
10. Higgins G.E. Cybercrime:An introduction to an Emerging Phenomen.// Library of Congress Cataloging, 2010.
11. Kaufman L.M. Data Security in the World of Cloud Computing.// Security & Privacy, IEEE, 2009.
12. Kiškis M., Petrauskas R., Rotomskis I., Štitilis D. Teisės informatika ir informatikos Teisė.// Vilnius, Mykolo Romerio Universitetas, 2006.
13. Kostopoulos G.K. Cybercpace and Cybersecurity.// CRC Press, Taylor & Francis Group, 2013.
14. Kraft W., Streit C. Ideas on the Establishment of an Inernational Court for Cyber Crime.// Germany, WCLF, 2011.
15. S. Ghosh, E. Turrini. Cybercrimes: A Multidisciplinary Analysis. Springer. 2010.
16. Schjolberg S. Crossing jurisdictional boundaries.// The Hague, The Netherlands, 2013.
17. Schjolberg S. Peace and Justice in Cyberspace.// Norway, 2012.
18. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva.// December 2008.
19. Sieber U. Legal aspects of computer-related crime in the information society.// 1998.

20. Štitilis D. Elektroniniai nusikaltimai.// Vilnius, Mykolo Romerio Universitetas, 2011.
21. Summit G., Elliot T. Cybercrimes: a multidisciplinary analysis.// Germany, Springer, 2010.

**Straipsniai periodiniuose leidiniuose:**

1. August R. International Cyber-Jurisdiction: A Comparative Analysis.// American Business Law Journal, vol. 39 Summer, 2002.
2. Barkham J. Information Warfare and International Law on the Use of Force.// New York University, N.Y.U. Journal of International Law and Politics. Fall 2001.
3. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace.// Library of Congress Cataloging, 2010.
4. Brenner S.W., Koops B.J.Approaches to Cybercrime Jurisdiction.// Journal of High Technology Law, vol. 4, 2004.
5. Brenner S.W., Scherha J.J., Cybercrime Havens: Challenges and Solutions.// Business Law Today, vol.17, December, 2007.
6. Davis B. A Proposal for an Internatonal Convention to Regulate the Use of Informations Systems in Armend Conflicts. Vol. 47, No. 1, 2006.
7. Duncan B.H. Why States Need an International Law for Information Operations.// 11 Lewis & Clark Law Review. 2007.
8. Fry J.D. Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction.// UCLA Journal of International Law and Foreign Affairs, vol. 7, 2002.
9. Jaeger P., Lin J., Grimes J., Simmons S. Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing.// First Monday peer-reviewed Journal in the internet, Vol. 14, 2009.
10. Jensen E.T. Computer Attacks on Critical Natinal Infrastructure: A Use of Force Invoking the Right of Self-Defense.// Stanford Journal of International Law, Vol. 38, 2002.
11. Paust J.J. Above the Law: Unlawful Executive Authorization Regarding Detainee Treatment, Secret Renditions, Domestic Spying, and Claims to Unchecked Executive Power.// Utah Law Review, vol. 2007, issue 2.
12. Pryce J. Convention on Cybercrime.// Privacy & Security Law Report. Vol 5, No. 1, BNA, Inc., 2006 October 16.
13. Romero M.P. An Immunological Appeoach to Counter-Terrorism and Infrastructure Defense Law in Electronic Domains.// International Journal of Law & Information Technology, 14(1), 2006.

14. Stevens S. R. Internet War Crimes Tribunals and Security in an Interconnected World.// Transnational Law & Contemporary Problems, Vol. 18, Issue 1, 2008.
15. Vida M., Jenkins A. Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?.// Naval Law Review, Vol. 51, 2005.
16. Xingan L. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology, Vol. 4, No 3, September 2007.

**Kiti straipsniai ir leidiniai:**

1. Blakesley C.L. Jurisdictional Issues and Conflicts of Jurisdiction.// 2006.
2. Broderic T. R. Regulation of the Information Technology in the European Union.// London, Kluver Law International, 2000.
3. Catteddu D., Hogben G. Cloud Computing: benefits, risks and recommendations for information security.// Technical Report of European Network and Information Security Agency, 2009.
4. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.// 2009.
5. Computer-Related Criminality: Analysis of Legal Policy in the OECD Area. Report DSTI-ICCP 84.22, 18 April 1986.
6. Contribution on the Secretary general of the council of Europe. To the Twelfth United Nations Congress on Crime prevention and Criminal Justice. Salvador, Brazil, 12-19 April 2010 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf
7. Deloitte Center for Security and Privacy Solutions. Cyber crime: a clear and present danger Combating the fastest growing cyber security threat. Deloitte, 2010.
8. Eight U.N. Congress on the Prevention of Crime and the Treatment of Offenders. 1990 September 4. http://www.asc41.com/UN_congress/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/026%20ACONF.144.28.Rev.1%20Eighth%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf
9. Expert Group to Conduct a Comprehensive Study on Cybercrime – Executive Summary, January 23, 2013 (UNODC/CCPCJ/EG. 4/2013/2) https://www.unodc.org
10. Final Report of the Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas. http://www.oas.org/juridico/english/ministry_of_justice_v.html

11. Final Report of the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas. http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber
12. Galicki Z. The Obligation to extradite or Prosecute in International Law.// Report of the international Law Commission, Fifthysix session (2 May- 4 June and 5 July- 6 August 2004).
13. Greek D. Change to Computer Misuse Act Worries Researchers. 2006. http://www.computeractive.co.uk/computeractive/news/2169530/changes-computer-misuse-act
14. ICT Regulation Toolkit http://www.itu.int/itudoc/gs/promo/bdt/flyer/87876.pdf
15. International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime http://www.uncjin.org/Documents/EighthCongress.html
16. International Telecommunications Union. ITU Toolkit for Cybercrime Legislation. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf
17. Interpol. Annual report 2006. http://interpol.int/Public/ICPO/InterpolAtWork/iaw2006.pdf
18. Interpol. Cyber-crime. www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf
19. Jasper N. On our extended downtime, Amazon and what is coming.// October 4, 2009. http://blog.bitbucket.org/2009/10/04/on-our-extended-downtime-amazon-and-whats-coming/
20. Magnin C. J. The 2001 Council of Europe: Convention on Cybercrime: an efficient tool to fight crime in cyberspace. 2001.
21. McConnell International.Cyber Crime…and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December 2000.
22. McCormich Tribune Foundation. Understanding the Privatization of National Security. 2006.
23. Melnick J. The Cyber War Against The United States.// Boston Globe. August 19, 2007.
24. Ministers of Justice or Attorneys General of the Americas (REMJA) VI Final Report http://2001-2009.state.gov/p/wha/rls/rpt/77518.htm
25. Ninth Meeting om Ministers of Justice or Other Ministers or Attorneys General of the Americas http://www.oas.org/en/sla/dlc/remja/pdf/recomm_IX.pdf
26. OAS Technical Workshops Following the Sixth Meeting http://www.oas.org/juridico/english/cyber_tech_wrkshpVI.htm
27. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.html

28. Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyberterrorism and Use of Internet for Terrorist Purpose http://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf
29. Police Commissioners Conference Electronis Crime Working Party, 2000, p. 64. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.4966
30. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf
31. S. Schjolberg. A Presentation at the Europol-INTERPOL Cybercrime Conference.The Hague, The Netherlands, September 24-25, 2013.
32. Sofaer A.D., Goodman S.E. Cyber Crime and Security The Transnational Dimension. http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf
33. Sylvia M. Kierkegaard in cooperation with FU Berlin and UNIDIR. The conference on „Challenges in Cybersecurity". December, 2011.
34. The Dark Truth about Blackwater. http://www.brookings.edu/research/articles/2007/10/02militarycontractors
35. The INTERPOL Global complex for Innovation. http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI
36. Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG
37. Urbas G. Cybercrime legislation in the Asia - Pacific Region. Regional conference of piracy and cyber crime. The university of Hong Kong, April 25-26, 2001.
38. Vogel J. First World Conference of Penal Law// Mexico, November 2007.
39. Wahlert G. Crime in Cyberspace: trendsin Computer Crime in Australia. Paper presented at the conference, held in Melbourne, 16-17 February, 1998, by the Australian institute of Criminology.
40. Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 3. January 29, 2008. https://www.fas.org/sgp/crs/terror/RL32114.pdf
41. WSIS Thematic Meeting on Cybersecurity. Geneva, June 28 - July 1, 2005. http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf

**Teisės norminiai aktai:**


1. 18 U.S. Code § 1030 - Fraud and related activity in connection with computers http://www.law.cornell.edu/uscode/text/18/1030
2. 2001 m. Konvencija dėl elektroninių nusikaltimų. Valstybės žinios. 2004-03-07, Nr. 36-1188. Angliškas Konvencijos tekstas: Convention on Cybercrime, prieiga internetu: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
3. Additional Protocol to the Convention on Cybercrime, cornening the criminalisitaion of acts of a racist and xenophobic nature committes through computer systems. Strasbourg, 28.I.2003 http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
4. Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity http://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf
5. Cominication from the Commission to the Council, the Europien Parliament, the Economic and the Social Committee and Committee of the regions. Creating a Safer Information Infrastructures and Combating Computer-related Crime. Brussels, COM (2000) 890 final. https://www.conventions.coe.int
6. Commission of the European Communities COM (2000) 890 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF
7. Computer Misuse Act 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents
8. Council of Europe Recommendation No. R(95) 13 http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp
9. Europos Komisijos komunikas KOM (2007) 267 galutinis http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF
10. Europos Komisijos komunikas KOM (2009) 149 galutinis http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:LT:NOT
11. Europos Parlamento ir Tarybos direktyva 2013/40/ES http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32013L0040&from=LT
12. Jungtinių Tautų Chartija, Valstybės žinios, 2002-03-13, Nr. 15-557. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=211305&p_query=&p_tr2
13. Jungtinių Tautų konvencija prieš tarptautinį organizuotą nusikalstamumą. Valstybės žinios. 2002-05-22, Nr. 51-1933. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=166679

14. United Arab Emirates, The Federal Law No. (2) on 2006 on The prevention of information Technology Crimes. http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf

**Teismų sprendimai:**

1. People v. Somm, Case 8340 Ds 465 Js 173158/95 (Amstsgericht, Munchen, Bavaria)
2. The Case Study: Rome Laboratory, Griffiss Air Force Base, NY Intrusion. http://www.fas.org/irp/congress/1996_hr/s960605b.htm
3. The Secretary-General, Report on Aspects of Establishing an International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yougoslavia. U.N Doc. S/25704 (May 3, 1993).
4. United Nations, International Criminal Tribunal for Rwanda. http://69.94.11.53/
5. United Nations, International Criminal Tribunal for the Former Yugoslavia. http://www.icty.org
6. Yahoo Inc V. La Ligue Contre Le Racisme et Antisemitisme http://caselaw.findlaw.com/us-9th-circuit/1144098.html#sthash.jhpZB1Bv.dpf
7. Yahoo! v. LICRA Amicus Brief http://www.law.berkeley.edu/4647.htm
8. Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme http://cyber.law.harvard.edu/is02/readings/yahoo-order.html

**Interneto šaltiniai:**

1. 2013–The Impact of Cybercrime. http://resources.infosecinstitute.com/2013-impact-cybercrime/
2. About Interpol. http://www.interpol.int/About-INTERPOL/Overview
3. ASEAN and the securitization of transnational crime in Southeast Asia http://www.tandfonline.com/doi/abs/10.1080/09512740320000856 53#preview
4. Asean countries must work together against cyber crimes: Hsien Loong http://www.asianewsnet.net/Asean-countries-must-work-together-against-cyber-c-53945.html
5. ASEAN Members States http://www.asean.org/asean/asean-member-states
6. Biograpfhy of Stein Schjolberg. http://www.cybercrimelaw.net/biography.html
7. Byla LICRA prieš Yahoo. http://en.wikipedia.org/wiki/LICRA_v._Yahoo

8. Chinese Hacker Sentenced to Death for Embezzlement. http://english.people.com.cn/english/200006/13/eng20000613_42866.html
9. Cloud Security Alliance. https://cloudsecurityalliance.org/
10. Cyber Crime Statistics and Trends. http://www.go-gulf.com/blog/cyber-crime/
11. FBI "hack" raises global security concerns http://news.cnet.com/2100-1001-256811.html
12. Global Network Navigator. http://oreilly.com/gnn/.
13. Group of Eight Meets to Discuss Internationals Cooperation on Cybercrime. http://en.wikipedia.org/wiki/International_cybercrime
14. High-tech net helped FBI snag alleged hackers http://usatoday30.usatoday.com/tech/news/2001-05-09-fbi-tech-sting.htm
15. History repeats for former hacker http://news.bbc.co.uk/2/hi/technology/4761985.stm
16. Information security and privacy www.oecd.org/sti/security-privacy
17. Inter-American Cooperation Portal on Cyber-Crime http://www.oas.org/juridico/english/cyber.htm
18. International Cybercrime Treaty https://www.aclu.org/technology-and-liberty/international-cybercrime-treaty
19. International Cyberspace Strategies http://www.nsci-va.org/WhitePapers/2010-06-28-InternationalCyberspaceStrategies-Stephens-McKee.pdf
20. International Telecommunication Union. http://www.itu.int/net/about/
21. Internet Usage Statistics http://www.internetworldstats.com/stats.htm
22. Interpol: An overview. www.interpol.int/Public/ICPO/FactSheets/GI01.pdf
23. INTERPOL: Cybercrime http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
24. ITU will IP-Adressen verwalten http://www.heise.de/netze/meldung/ITU-will-IP-Adressen-verwalten-835928.html
25. Markoff J. Before the Gunfire, Cyberattacks. N.Y. Times. August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0
26. Markoff J., Kramer A. In Shift, U.S Talks to Russia on Internet Security.http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0
27. Masters G. Global Cybercrime Treaty Rejected at U.N. 2010. http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/
28. More Naked Gun than Top Gun http://cryptome.org/jya/naked-gun.htm
29. Norwegian jailed for Web racism http://edition.cnn.com/2002/WORLD/europe/04/23/norway.web/
30. OAS Member States http://www.oas.org/en/member_states/default.asp?utm_source=LifeSiteNews.com+Daily+N

ewsletter&utm_campaign=b88fabf545-LifeSiteNews_com_Intl_Full_Text_06_06_2013&utm_medium=email&utm_term=0_0caba610ac-b88fabf545-326192614

31. Philippine investigators detaion man in seach for 'Love Bug' creator Clinton to attend funeral of cardinal John O'Connor http://www.mail-archive.com/htmlquicknews@cnnimail4.cnn.com/msg00036.html
32. Philippine Prosecutors Release 'Love Bug' Suspect http://partners.nytimes.com/library/tech/00/05/biztech/articles/10virus.html
33. Protecting Youyou're your Rights in Cyberspace: Minimising the Risks, Maximising the Freedom http://en.collaboratory.de/w/Protecting_You_and_Your_Rights_in_Cyberspace:_Minimising_the_Risks,_Maximising_the_Freedom
34. Russian Computer Hacker Convicted by Jury http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm
35. Steven L.M.'E-stonia' Accuses Russia of Computer Attacks. N.Y. TIMES, May 18, 2007. http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h.
36. The role of the G-8. http://www.g8.co.uk/
37. The United States Department of Justice. http://www.justice.gov/criminal/cybercrime/bentleySent.pdf
38. U.N and Cybercrime http://www.ictparliament.org/node/2128
39. United States Court of Appeals for the Ninth Circuit http://en.wikipedia.org/wiki/United_States_Court_of_Appeals_for_the_Ninth_Circuit

# SANTRAUKA

Šiuo metu kompiuterinės technologijos ir internetas yra neatsiejama kiekvieno iš mūsų gyvenimo dalis. Tačiau tiek kompiuteris, tiek ir internetas gali būti naudojamas ne tik pramogoms ir kasdieninėms gyvenimiškoms funkcijoms atlikti, bet taip pat ir vykdant nusikalstamas veikas. Siekiant kovoti su tarptautinio masto elektroniniais nusikaltimais, 2001 metais Budapešte buvo pasirašyta Konvencija dėl elektroninių nusikaltimų. Todėl siekiant atvaizduoti esamą situaciją, elektroninių nusikaltimų mastus, pirmame skyriuje pateikiama ir atskleidžiama elektroninio nusikaltimo sąvoka, elektroninių nusikalstamų veikų rūšys, įtvirtintos Konvencijos dėl elektroninių nusikaltimų 2 – 10 straipsniuose. Skyriaus pabaigoje pateikiama praėjusių metų elektroninių nusikaltimų statistika, kuria remiantis yra matomi aiškūs šių nusikalstamų veikų mastai.

Antrame skyriuje pateikiamas egzistuojančios teisinės kovos priemonės su elektroniniais nusikaltimais tarptautiniu mastu. Išanalizavus Didžiosios Britanijos, Jungtinių Arabų Emyratų ir Jungtinių Amerikos Valstijų egzistuojančius teisės aktus ir teisės aktų kaitą po Konvencijos priėmimo, nustatomas Europos Tarybos Konvencijos dėl elektroninių nusikaltimų efektyvumas. Analizuojamos valstybės pasirinktos remiantis skirtingu prisijungimo prie Konvencijos ir ratifikavimo laikotarpiu, o siekiant akivaizdaus skirtumo pasirenkama valstybė, kuri nėra nei prisijungusi, nei ratifikavusi šios tarptautinės sutarties dėl elektroninių nusikaltimų. Toliau darbe atskleidžiamos mums aktualiausios Europos Sąjungos regioninės teisinės priemonės ir tarptautinių organizacijų, tokių kaip EBPO, ASEAN, G-8 ir Interpolas, kuriamos priemonės.

Tolesniame skyriuje pateikiamos visos teisėje egzistuojančios jurisdikcijos teorijos bei atskleidžiama egzistuojanti jurisdikcijos problema tiriant ir kovojant su elektroniniais nusikaltimais tarptautiniu mastu. Pateikiama oficiali teismų praktikos pavyzdžiai skirtingose valstybėse. Analizuojant 2001 metų Konvencijoje dėl elektroninių nusikaltimų pateiktas jurisdikciją reglamentuojančias teisės normas, įvardinamas aiškus tarptautinio bendradarbiavimo būtinumas. Greta to išskiriamos neigiamo ir teigiamo pobūdžio susidarančios jurisdikcijos kolizijos bei įvardinama jurisdikcijos nežinomybė debesų kompiuterijoje.

Paskutiniame skyriuje analizuojama Steino Schjolbergo pateikta tarptautinio teismo ir tribunolo idėja kovojant su elektroniniais nusikaltimais. Gana smulkiai išanalizuojami 2007 metais Estijoje įvykdyti kibernetiniai išpuoliai, pateikiamas skirtingas mokslininkų ir ekspertų požiūris į šiuos išpuolius. Taip pat vertinama, ar kibernetinę ataką galima prilyginti kariniam jėgos panaudojimui.

SUMMARY

Currently computer technologies and the Internet are an integral part of each of our lives. However, both the computer and the Internet can be used not only for entertainment and everyday real life functions, but also for criminal offenses. In order to combat international cyber-crimes, Budapest Convention on Cybercrime was signed in 2001. In order to reflect the current situation, the extent of cybercrimes, the first section of this master work discloses the concept of an 'e-crime' and the variety of electronic crimes contained in articles 2-10 of the Convention on Cybercrime. The end section includes cyber-crime statistics of the recent year, which clearly shows the scale of the criminal offences.

The second section of the work reviews the existing legal measures against cyber-crimes internationally. After analysing existing laws and regulations in the United Kingdom, the United Arab Emirates and the United States of America and their changes after the adoption of the Convention, the efficiency of The Council of Europe's Cyber Crime Treaty is evaluated. The countries chosen for the evaluation have been selected because of the different period of entering the treaty and one country which is neither a party, nor ratified this international treaty on cyber-crime is chosen to show the obvious differences. Further in this work the most prominent legal means of the regional European Union are named and also means created by international organizations such as ESBO, ESAN, INTERPOL or G-8.

The further section contains all jurisdiction theories that exist in the legal system and the problem of jurisdiction while investigating international legal crimes. Official case law in different countries is presented. The necesity of international cooperation is underlined while analyzing the convention's legal instruments on jurisdiction. In addition negative and positive colisions of jurisdiction are extracted and also the uncertainty of jurisdiction in cloud computing is named.

The final section examines Stein Schjølberg's named idea of the international court and tribunal of combating cyber-crimes. The cyber-attacks that took place in Estonia in 2007 are broadly analyzed, the different scientific approach to such attacks is named. The work also assesses whether the cyber-attack can be compared to a military force.