PALVELUNESTOHYÖKKÄYKSEN KRIMINALISOINTI

Lapin yliopisto
Oikeustieteiden tiedekunta
Rikosoikeus
Maisteritutkielma
Jari Kuusela
Kevät 2014

TIIVISTELMÄ

Lapin yliopisto, oikeustieteiden tiedekunta
Työn nimi: Palvelunestohyökkäyksen kriminalisointi
Tekijä: Jari Kuusela
Oppiaine: Oikeustieteiden tiedekunta / Rikosoikeus
Työn laji: Maisteritutkielma_x_ Lisensiaatintutkimus__
Sivumäärä: XIII + 90
Vuosi: Kevät 2014

Tiivistelmä:
Tutkielmassani käsittelen tietoliikenteen häirinnän ja tietojärjestelmän häirinnän kriminalisointeja. Tietotekniikkarikoksia koskeva lainsäädäntö on vielä kehitysvaiheessa ja uusi Euroopan Unionin direktiivi on hyväksytty Euroopan parlamentissa.

Palvelunestohyökkäys voidaan suorittaa erilaisin keinoin sekä ohjelmallisesti, että teknisesti. Hyökkäys voi olla erittäin yksinkertainen toteutustavaltaan, että tahaton ja siten rikostunnusmerkistön edellytykset eivät täyty. Tietotekniikkarikoksen esitutkinta ja syyttäminen edellyttää viranomaisilta erityistä asiantuntemusta, jotta tekijä saadaan kiinni. Tietotekniikkarikokset ovat myös erittäin kansainvälisiä tekoja, joten tekijöiden kiinnisaaminen edellyttää useasti nopeita kansainvälisiä toimia. Tulevaisuudessa kansainvälistä yhteistyötä tulee helpottamaan Euroopan Unionin jäsenmaiden välillä, 24/7 toimiva yhteyspisteverkosto.

Tilastojen mukaan tietojärjestelmän häirintä ei ole tullut useasti sovellettavaksi. Se onkin toissijainen säädös suhteessa tietoliikenteen häirintään. Suhteessa tehtyihin rikosilmoituksiin tuomioita on tullut vähän, erityisesti tietojärjestelmän häirinnästä. Ovatko kysymyksessä tutkinnalliset ongelmat vai mahdolliset keinojen vähyys tutkinnassa, koska teot eivät ole edenneet syyteharkinnasta tuomioksi. Suomessa on tunnettua syytteiden erittäin korkea läpimenoprosentti, syyttäjät eivät syytä ellei syyte mene läpi erittäin korkealla todennäköisyydellä.

Avainsanat: atk-rikokset, verkkohyökkäykset
Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön x
Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi x

SISÄLLYS

LÄHTEET

Kirjallisuus

Andersen, Mads Bryde: IT-retten. Gjellerup. København 2005.

Andrews Mike & Whittaker James A.: How to Break Web Software. Pearson Education, Inc. Boston 2006.

Akkusastoori 3/2013. Valtakunnansyyttäjänvirasto.

Aronen Eeva & Sourander André: Lasten psykiatria. Teoksessa J. Lönnqvist & M. Heikkinen & M. Henriksson & M. Marttunen & T. Partonen(toim.) Psykiatria. 556–590. Jyväskylä: Gummerus Kirjapaino Oy, 2009.

Cisco Press: Ciscon verkkoakatemia – 1.vuosi. Suomentanut Jarmo Holttinen. Edita. Helsinki 2002. Englanninkielinen alkuteos 2001.

Ervasti Kaijus: Laki, konflikti, tuomio – Oikeus yhteiskunnallisena ilmiönä. Edita Publishing Oy. Helsinki 2012.

Frände Dan & Matikkala Jussi & Tapani Jussi & Tolvanen Matti & Viljanen Pekka & Wahlberg Markus: Keskeiset rikokset. Edita. Helsinki 2010.

Frände Dan: Yleinen rikosoikeus. Suomentanut ja seuraamusosan päivittänyt Markus Wahlberg. Edita. Helsinki 2012.

Husa Jaakko: Julkisoikeudellinen tutkimus. Tutkimus julkisoikeudessa harjoitettavan oikeusdogmatiikan metodologiasta. Jyväskylä 1995.

Husa Jaakko & Mutanen Anu & Pohjolainen Teuvo: Kirjoitetaan juridiikkaa. Talentum. Helsinki 2010.

Kaario Kimmo: TCP/IP-verkot. Docendo Finland Oy. Jyväskylä 2002.

Kaspersen Henrik W. K.: Jurisdiction in the Cybercrime Convention. Teoksessa Bert-Jaap Koops & Susan W. Brenner(edited). Cybercrime and Jurisdiction A Global Survey. T·M·C Asser Press. Hague. 2006.

Mcclure Stuart & Scambray Joel & Kurtz George: Hacking Exposed, Fifth Edition: Network Security Secrets & Solutions. McGraw-Hill/Osborne. Emeryville, California 2005.

McQuade III Samuel C.: Understanding and Managing Cybercrime. Pearson Education, Inc. Boston 2006.

Melander Sakari: EU-rikosoikeus. WS Bookwell Oy. Juva 2010.

Melander Sakari: EU-rikosoikeus – politiikkaa, oikeutta, tuomioistuinaktivismia? 55–75. Teoksessa Vapauden, turvallisuuden ja oikeuden Eurooppa. Yliopistopaino. Helsinki 2010.

International Guide to Combating Cybercrime. J. R. Westby(editor). American Bar Association. Chicago. 2003.

Pihlajamäki Antti: Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Datarikoksia koskeva sääntely Suomen rikoslaissa. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja No 258. Helsinki 2004.

Pihlajamäki Antti: Tietotekniikka, syyttäjä ja rikos. Teoksessa. J. Ohisalo & M. Tolvanen(toim.) Consilio manuque Yhtenäinen syyttäjälaitos 10 vuotta. Joensuu 2008.

Rathmell Andrew: Information Warfare and sub-state actors: an organizational approach. Teoksessa. D. Thomas & B. D. Loader(edited) Cybercrime law enforcement, security and surveillance in the information age. London. 2000.

Rosas Allan: Kansallinen tuomari EU-tuomarina. Teoksessa. K. Raulos, T. Esko & P. Välimäki(toim.) Da mihi factum, dabo tibi ius. Juva 2009.

Saarenpää Ahti: Verkkoyhteiskunnan oikeutta – johdatusta aiheeseen. 2000. Saatavilla osoitteesta: http://hdl.handle.net/10224/3699. Viitattu 23.3.2014.
Saarenpää Ahti: Teoskynnys, ymmärryskynnys, hyväksymiskynnys. Vähäisiä näkökohtia verkkoyhteiskunnan tekijänoikeudesta. Teoksessa Juhlajulkaisu Asianajotoimisto Borenius & Kemppinen 90 vuotta. 169-197. Gummerus Kirjapaino Oy, Jyväskylä. 2001.

Saarenpää Ahti: Oikeudellinen tieto verkkoyhteiskunnassa. 2008. Saatavilla osoitteesta: http://www.ulapland.fi/Suomeksi/Yksikot/Oikeustieteiden-tiedekunta/Tutkimus-ja-jatko-opinnot/Instituutit/Oikeusinformatiikan-instituutti/Elektronisia-artikkeleita-ja-muita-julkaisuja. Viitattu 23.3.2014.

Saarenpää Ahti: Oikeusinformatiikka sivut 411–545. Teoksessa Oikeusjärjestys Osa I. 7.täydennetty painos. Rovaniemi 2011.

Spang-Hanssen Henrik: Jurisdiction in the Cybercrime Convention. Teoksessa Bert-Jaap Koops & Susan W. Brenner(edited). Cybercrime and Jurisdiction A Global Survey. T·M·C Asser Press. Hague. 2006.

Valtakunnansyyttäjänvirasto: Esitutkintayhteistyötä koskeva ohje. Valtakunnansyyttäjänviraston julkaisusarja nro 7. Helsinki 2013.

Vuorenpää Mikko: Syyttäjän tehtävät. Erityisesti silmällä pitäen rikoslain yleisestävää vaikutusta. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja No 277. Helsinki 2007.

Walden Ian: Computer crime and information misuse. Teoksessa C. Reed(edited) Computer law. Oxford University Press Inc. New York 2011.

Xingan Li: Cybercrime and deterrence: Networking legal systems in the networked information society. Turku 2008.

Virallislähteet

2005/222/YOS. Euroopan unionin Neuvoston puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä. 24.2.2005.

2013/40/EU. Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta. 12.8.2013.

EUVL C 306. 17.12.2007. Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, allekirjoitettu Lissabonissa 13 päivänä joulukuuta 2007.

HE 94/1993 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 153/2006 vp. Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä sekä rikoslain, pakkokeinolain, esitutkintalain ja kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta.

KK 97/2007 vp. Kirjallinen kysymys. tietoverkkohyökkäykset.

KOM(2008) 448 lopullinen. Komission kertomus neuvostolle Tietojärjestelmiin kohdistuvista hyökkäyksistä 24 päivänä helmikuuta 2005 tehdyn neuvoston puitepäätöksen 12 artiklan perusteella.

KOM(2010) 517 lopullinen. Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta.

LaVM 17/1989 vp. Hallituksen esitys eduskunnalle rikosoikeudellisista toimenpiteistä luopumista koskevien säännösten uudistamiseksi.

LaVM 6/2000 vp – HE 184/1999 vp. Hallituksen esitys yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi.

Lausuntoja ja selvityksiä 2004:14. Tietoverkkorikostyöryhmän mietintö.

NOU 2003/27. Datakrimutvalgets betänkande, Lovtiltak mot datakriminalitet.

OM2011-00165/OM2011-00166: U-JATKOKIRJE. EU/OSA/Ehdotus direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta. 2.5.2011.

Ot.prp. nr. 40(2004-2005). Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet).

Poliisin tulostietojärjestelmä. tilastopalvelu@poliisi.fi. Viitattu 2.1.2013.

Regeringens proposition 2006/07:66. Angrepp mot informationssystem. http://www.regeringen.se/sb/d/7072/a/78673. Viitattu 13.3.2014.

Sisäasiainministeriö (2008): Järjestäytyneen rikollisuuden ja terrorismin torjunta.

SopS 60/2007. Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus.

Sou 2013:39. Betänkande av Utredningen om it-brottskonventionen. http://www.regeringen.se/content/1/c6/21/81/01/a83091f6.pdf. Viitattu 12.3.2014.

Tilastokeskus. http://tilastokeskus.fi/meta/til/syyttr.html. Viitattu 2.1.2013.

U 50/2010. Valtioneuvoston kirjelmä Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta.

Esitelmät

Rikoskomisario Timo Piiroisen esitys keskusrikospoliisissa Vantaalla 27.8.2013.

Rikosylikomisario Timo Virtasen esitys keskusrikospoliisissa Vantaalla 27.8.2013.

Oikeustapaukset

Helsingin kihlakunnan syyttäjänviraston syyttäjän 6.8.2003 tekemä syyttämättäjättämispäätös 03/1776 muun muassa tietoliikenteen häirintää koskevassa asiassa R 03/4111.

Helsingin kihlakunnan syyttäjänviraston syyttäjän 2.6.2004 tekemä syyttämättäjättämispäätös 04/1186 lievää tietoliikenteen häirintää koskevassa asiassa R 03/5297.

Helsingin kihlakunnan syyttäjänviraston syyttäjän 21.9.2005 tekemä syyttämättäjättämispäätös 05/2170 tietoliikenteen häirintää koskevassa asiassa R 05/1033.

Helsingin käräjäoikeuden 8.12.2006 antama tuomio 06/12059 muun muassa tietoliikenteen häirintää koskevassa asiassa R 06/8598.

Helsingin käräjäoikeuden 9.1.2003 antama tuomio 03/208 muun muassa tietoliikenteen häirintää koskevassa asiassa R 02/8258.

KKO 2008:86.

Varsinais-Suomen käräjäoikeuden 4.3.2011 antama tuomio 11/1235 muun muassa vaaran aiheuttamista tietojenkäsittelylle koskevassa asiassa R 10/3229.

Sähköiset lähteet

Chen Shay: Application Denial of Service. Is it Really That Easy? Hacktics. 2007. Saatavilla osoitteesta https://www.owasp.org/images/d/da/OWASP_IL_7_Application_DOS.pdf. Viitattu 18.12.2012.

Ehdotus EU:n direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä. Oikeusministeriö. 2012. Saatavilla osoitteesta http://www.om.fi/Etusivu/Valmisteilla/Lakihankkeet/Rikosoikeus/1290610003201. Viitattu 20.12.2012.

Huttunen Matti: Aspergerin oireyhtymä. 28.6.2013. Saatavilla osoitteesta http://www.terveyskirjasto.fi/terveyskirjasto/tk.koti?p_artikkeli=dlk00354. Viitattu 5.3.2014.

Palvelunestohyökkäyksiä on monta lajia. CERT-FI. 2007. Saatavilla osoitteesta http://www.cert.fi/tietoturvanyt/2007/05/P_12.html. Viitattu 15.12.2012.

Taylor Kimberly & Mesibov Gary & Debbaudt Dennis. Asperger Syndrome in the Criminal Justice System. 2009. Nomi Kaim(toim.). http://www.aane.org/asperger_resources/articles/miscellaneous/as_in_the_criminal_justice_system.html. Viitattu 5.3.2014.

Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin kansalliset täytäntöönpanotoimet. Oikeusministeriö. 2013. Saatavilla osoitteesta http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/rikosoikeus/tietojarjestelmiinkohdistuvathyokkaykset.html. Viitattu 16.10.2013.

Internet-linkkejä

https://lagen.nu/1962:700#K4P9c

http://www.regjeringen.no

http://lovdata.no

https://www.retsinformation.dk

http://www.dagensjuridik.se

http://www.iltalehti.fi

http://www.regeringen.se

http://www.digitoday.fi

http://www.tietoviikko.fi

http://www.taloussanomat.fi

http://us.practicallaw.com

LYHENTEET

brb	Brotssbalken
DADoS	distributed application denial of service
DDoS	distributed denial of service
DHCP	The Dynamic Host Configuration Protocol
DoS	denial of service
ETL	esitutkintalaki
EU	Euroopan Unioni
et al.	ynnä muut
HE	hallituksen esitys
ICMP	internet control message protocol
IP	Internet Protocol
KKO	korkein oikeus
LaVM	lakivaliokunnan mietintö
RL	rikoslaki
SEU	sopimus Euroopan unionista
SEUT	sopimus Euroopan unionin toiminnasta.
SYN	TCP-protokollan yhteydenmuodostamisviesti
TB	Teratavu
TCP	Transmission control protocol, tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille tietoverkossa
Ot.prp.	En odelstingsproposisjon
VKSV	Valtakunnansyyttäjänvirasto
vp	valtiopäivät

1. JOHDANTO

Tarkastelen tutkielmassani palvelunestohyökkäyksen kriminalisointia. Palvelunestohyökkäys eli denial of service -hyökkäys, myöhemmin DoS, on keino, jolla pyritään häiritsemään tai kokonaan estämään tietojärjestelmän normaali toiminta. Johtuen palvelunestohyökkäyksen moniulotteisuudesta, tämä tutkielma kohdistuu palvelunestohyökkäykseen sovellettavan, rikoslain 38 luvun 5 §, 38 luvun 6 § ja 38 luvun 7 § kriminalisointeihin eli tietoliikenteen häirinnän -tekomuotoihin sekä tietoliikenteen häirintää täydentäviin rikoslain 38 luvun 7 a § eli tietojärjestelmän häirinnän ja sen törkeän tekomuodon 38 luvun 7 b § kriminalisointeihin. Käsittelen myös aiheeseen osittain liittyvät kriminalisoinnit pinnallisesti, koska niitä esiintyy kaikissa aihepiiriin liittyvistä esimerkkioikeustapauksista, tutkielman tarkoitus ei ole kuitenkaan käsitellä rikoslain 38 luvun tietotekniikkarikos tunnusmerkistöjä tyhjentävästi.

Tutkimusongelmaan liittyy monia alakysymyksiä, kuten pykälien soveltaminen käytännössä, niiden käyttökelpoisuuden arviointi de lege ferenda ja niin edelleen. En tule niitä tässä tutkielmassa käsittelemään muutamaa esimerkin omaista tapausta lukuun ottamatta. Kyseessä on erittäin ajankohtainen aihe nykyaikaisen tietoverkkorikollisuuden muututtua yhä suuremmaksi uhkakuvaksi tietoverkkoympäristössä toimijoille, niin yrityksille, kuin yksityisille, että valtioille.[1] Bot-verkkoon kaapatun koneen haltija ei yleensä tiedä koneeseen kohdistuneesta teosta[2]. tällaisia kaapattuja tietokoneita on yllättävän suuri määrä, conficker-botnet:ssä on ollut jopa 9-15 miljoonaa kappaletta[3].

Lisäksi uudesta direktiiviehdotuksesta on päästy yhteisymmärrykseen Euroopan parlamentissa, joten lainsäädäntökin on muutosvaiheessa. Ongelmana tutkimuksen tekemisessä tulee olemaan aiheen uutuus oikeudellisessa kentässä, oikeuskäytäntöä on vähän sekä lainsäädäntö on uutta, että kehitysvaiheessa. Oikeuskäytännön osalta käsittelen

[1] http://www.digitoday.fi/yhteiskunta/2014/03/14/kreml-kaatui-verkossa-syyttaa-kyberhyokkaysta/20143713/66.
http://www.taloussanomat.fi/tietoliikenne/2014/03/04/lehti-venaja-aloitti-hakkerihyokkayksen-ukrainassa/20143131/12.
http://www.iltalehti.fi/ulkomaat/2014031618126970_ul.shtml.
http://www.digitoday.fi/tietoturva/2008/07/22/georgian-presidentti-joutui-palvelunestohyokkaykseen/200819029/66.
[2] Walden 2011, s.704.
[3] http://www.f-secure.com/en/web/labs_global/articles/about_botnets.

pääasiassa tietoliikenteen häirinnästä esimerkkitapauksia, koska tietojärjestelmän häirinnästä ei ole juurikaan oikeuskäytäntöä, kuten ilmenee tilastoista.[4]

Tutkielman tutkimusmenetelmänä on pääasiassa lainoppi eli oikeusdogmatiikka, jonka keskeisenä tavoitteena on selvittää tämänhetkinen oikeudentila ja kuinka aktuaalisessa tilanteessa tulisi voimassaolevan oikeuden mukaan toimia.[5] Keskeinen tutkimusmetodi on tekstianalyysi eli tulkintahermeneutiikka[6]. Tutkielmaa on sinänsä mahdotonta tehdä puhtaasti yhdellä menetelmällä, joten työssä on myös muun muassa oikeushistoriaa. Oikeusdogmatiikka rakentuu voimassaolevien oikeuslähteiden varaan, joita tulisi käyttää etusija ja käyttöjärjestyssääntöjen mukaisesti.[7] Tärkeimpiä tutkielman oikeuslähteitä ovat direktiivit, sopimusten esityöt, rikoslaki, rikoslain esityöt oikeuskäytäntö ja oikeuskirjallisuus.

Tutkielma rakentuu johdantoluvun lisäksi kahdeksasta pääluvusta. Ensin käsittelen toisessa luvussa yleisesti yhteiskunnan kehitystä tietotekniikkarikosten kriminalisointia. Miten rikosten sääntely on alkanut Suomessa ja miten yhteiskunta on kehittynyt sen rinnalla.

Kolmannessa pääluvussa kerron tilastotietoa tietoverkkorikollisuudesta Suomessa, neljännessä teknistä puolta palvelunestohyökkäyksestä. Viides pääluku sisältää tieto aiheesta oikeudelliselta kannalta (Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus, Euroopan unionin puitepäätös ja sen korvaava direktiivi, rikoslain tietojärjestelmän häirintä ja tietoliikenteen häirintä -pykälät).

Viides pääluku käsittelee käytännön tapauksia, jota seuraa kuudes oikeusvertaileva jakso ja seitsämäs jakso käsittelee internetin käyttöä terroristisiin tarkoituksiin ja lopuksi pohdintaa.

[4] Ks. Taulukko 2.
[5] Husa et al. 2008, s. 20.
[6] Husa et al. 2008, s. 25.
[7] Husa et al. 2008, s. 19.

2. YHTEISKUNNAN KEHITYKSESTÄ YLEENSÄ

2.1. Oikeudellistunut verkkoyhteiskunta

Saarenpään mukaan yhteiskunta on muuttunut palveluyhteiskunnasta informaatioyhteiskunnaksi ja nykyään elämme jo verkkoyhteiskunnassa, oikeudellistuneessa verkkoyhteiskunnassa.[8] 1950-luvulla tietokoneiden käytön lisääntyessä, tieto siirtyi tietopankkeihin. Nykyään elämme avoimessa tietoverkkoyhteiskunnassa, jossa tieto on pääasiassa saatavilla verkossa.[9] Tiedon käsittely on muuttunut yhteiskunnan muuttuessa palveluyhteiskunnasta verkkoyhteiskunnaksi, jolloin informaation merkitys, sen käsittely ja siihen liittyvien oikeuksien merkitys on kasvanut.[10]

Saarenpää on perustellut nimityksen muutosta tavalla, jolla verkot ovat muuttaneet yksilöiden, yritysten, yhteisöjen ja julkisen vallan toimintoja sekä toimintamahdollisuuksia eli vuorovaikutussuhteita. Tietoverkoista on tullut massojen väylä informaation vuorovaikutuksessa. Saarenpään mukaan on perusteltua sanoa verkkoyhteiskunnassa tietotekniikan ja sen käyttömahdollisuuksien kuuluvan kaikille. Ihmisoikeusajatteluun perustuvan oikeudenmukaisuusperiaatteen mukaisesti voidaan vaatia esteettömän verkkoyhteiskunnan toteuttamista.[11] Saarenpään mukaan kansalaisten verkkosidonnaisuuden on osoittanut korkein hallinto-oikeus ennakkoratkaisuissaan KHO:2006:18 ja taltio 876/2006. Molemmissa tapauksissa oli kysymys tietokoneen käytön mahdollistavien apuohjelmien hankinnasta. Kaupungit velvoitettiin järjestämään ohjelmat hakijoille, koska apuvälineissä ei ole kysymys harrastustoiminnan tukemisesta, vaan muun muassa päivittäisistä toiminnoista selviämisen edistämisestä.[12]

Kuten voimme nykypäivänä jo todeta, oikeudellinen viestintä on muuttunut elektroniseksi viestinnäksi. Hyvä esimerkki kehityksestä on yleisiin tuomioistuimiin ja

[8] Saarenpää 2000, s.3–5.
[9] Saarenpää 2008, s.1–3.
[10] Saarenpää 2008, s.24.
[11] Saarenpää 2011, s.436.
[12] Saarenpää 2011, s.437–438.

syyttäjänvirastoihin kehitteillä oleva AIPA, jonka välityksellä asiat tulevat siirtymään virastojen välillä sähköisesti, vireilletulosta, ratkaisuun ja arkistointiin. AIPA tulee viemään kehitystä pidemmälle, koska se on yhteensopiva poliisin VITJAN[13] kanssa ja lisäksi siitä löytyy tapaukseen liittyvät tiedot yhdestä paikasta.[14]

Saarenpään mukaan oikeudellisen verkkoyhteiskunnan tunnusmerkkejä ovat infrastruktuurien merkityksen muutokset, informaation ja sen käsittelyn oikeudellisesti muuttunut asema yhteiskunnassa, informaatiohallinto, tieto- ja tietoverkkorikokset ja niin edelleen. Lisäksi hän on todennut oikeudellisen verkkoyhteiskunnan sääntelyn lähtökohtana olevan ihmis- ja perusoikeudet. Uudessa oikeudellisessa verkkoyhteiskunnassa on oikeus vaatia tietoturvattua toimintaympäristöä, tietoturvallisuudesta on tullut yksilön eräänlainen metaperusoikeus. Verkkoyhteiskunnan myötä meillä on oikeus tietoturvalliseen informaatioinfrastruktuuriin.[15] EU:n direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä on myös tätä korostava:

> (3) Tietojärjestelmiä vastaan tehdyt hyökkäykset ja erityisesti järjestäytyneeseen rikollisuuteen liittyvät hyökkäykset ovat kasvava uhka unionissa ja maailmanlaajuisesti, ja samalla tietojärjestelmiin kohdistuvien terrorihyökkäysten tai poliittisista syistä tapahtuvien hyökkäysten mahdollisuus herättää lisääntyvää huolta, sillä tietojärjestelmät ovat osa jäsenvaltioiden ja unionin elintärkeää infrastruktuuria. Koska hyökkäykset uhkaavat turvallisemman tietoyhteiskunnan sekä vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen toteuttamista, niihin on varauduttava unionin tasolla ja ne edellyttävät tehokkaampaa kansainvälistä yhteistyötä ja yhteensovittamista.[16]

2.2. Käytännön kehitys

Pihlajamäen mukaan vuonna 1989 OECD:n toisen, edellistä kattavamman, järjestön jäsenmaille laaditun suosituksen atk-rikosten kriminalisoimisesta valmistuttua, Suomen oikeushallinnossa alettiin vähentää sähkökirjoituskoneita ja siirtyä Tekoplus-tekstinkäsittelyohjelman käyttöön. Toimistosihteerien pöydillä oli mustavalkoisilla

[13] http://www.tietoviikko.fi/kaikki_uutiset/poliisi+kaynnistaa+vitjan/a960782.
[14] Akkusastoori 3/2013, s.25.
[15] Saarenpää 2011, s.439 & 448.
[16] Euroopan parlamentin kanta, vahvistettu ensimmäisessä käsittelyssä 4. heinäkuuta 2013, Euroopan parlamentin ja neuvoston direktiivin 2013/.../EU antamiseksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta

näytöillä varustettuja koneita, mutta syyttäjien pöydillä ne olivat harvinaisia. ATK-rikoksien kriminalisoinnit olivat vähäisiä. Vanhat, luvatonta käyttöönottamista ja väärennystä koskevat säännökset eivät soveltuneet käytännössä, joten muutamissa jutuissa päädyttiin omituisiin lopputuloksiin.[17]

Toisin oli Yhdysvalloissa, jossa 1984 Richard Hollinger ensimmäistä kertaa määritteli rikoksen nimeltään computer crime, jossa tietokone oli 1) rikoksen kohde, 2) rikoksentekopaikka, 3) rikoksentekoväline. Siitä lähtien kehitettiin erilaisia tietokonerikos-käsitteitä, kuten computer-related crime. World Wide Web:n kehittämisen myötä, vuonna 1995, alkoi esiintyä rikollisuutta, joka ei sopinut olemassa oleviin käsitteisiin, joten muodostui käsite cybercrime eli tietoverkkorikos.[18]

Suomessa rikoslain kokonaisuudistus 1.1.1991 tarjosi uusia säännöksiä, kun luvatonta käyttöä, yritysvakoilua, väärennystä, vahingontekoa, petosta, maksuvälinepetosta, tekijänoikeusrikosta ja teollisoikeusrikosta koskevat kriminalisoinnit muokattiin tietoteknisiin ympäristöihin soveltuviksi. Pihlajamäen mukaan syyteharkintaan tällaisia rikoksia ei sanottavasti tullut. Atk-rikosten yleistymistä hidasti sähköpostin ja internetin vähäinen käyttö. Tekninen kehitys oli nopeaa ja 1990-luvun puolivälissä tilanne oli jo toinen.

1.9.1995 rikoslain kokonaisuudistuksessa, toisen vaiheen yhteydessä, lisättiin rikoslakiin uusi tieto- ja viestintärikoksia koskeva 38 luku. Tietoverkkojen käytön lisääntyminen toi tietotekniikkarikoksia syyteharkintaan. Keväällä 1998 poliisin tietoon tuli TCB-juttu. Nuori atk-ammattilainen oli tunkeutunut verkossa satoihin tietojärjestelmiin Suomessa ja ulkomailla. Rangaistusta vaatineita suomalaisia asianomistajia oli 137, ulkomaisia tekoja ei yritetty selvittää. Pihlajamäen mukaan jutussa tuli esille tyypillinen tietotekniikkarikosten ongelma eli asianosaisten suuri määrä. Sama ongelma konkretisoitui Vantaan hakkerijutussa, jossa oli liki 200.000 hakkeroinnin kohteeksi joutuneen järjestelmän IP-osoitteet. Vastaajat tuomittiin lyhyisiin ehdonalaisiin rangaistuksiin. Vahingonkorvauksia kertyi 20.000 euroa.[19]

[17] Pihlajamäki 2008, s.54.
[18] McQuade III 2006, s.12–15.
[19] Pihlajamäki 2008, s.54–56.

Pihlajamäen mukaan jokaisessa jutussa syyttäjä saattaa törmätä elektroniseen todistusaineistoon, joten tietoteknisen terminologien hallitseminen ja ymmärtäminen on jokaisen syyttäjän velvollisuus. Tyypillinen tietotekniikkarikos on myös muuttunut, tietoverkkorikoksilla on yhä useammin kytköksiä järjestäytyneeseen kansainväliseen rikollisuuteen.[20]

Tietoverkkorikollisuutta on tehty monien kymmenien eri organisaatioiden ja hallitusten välisten organisaatioiden puitteissa, mutta kaikista suurin merkitys on ollut Euroopan neuvostolla ja sen tietoverkkorikollisuutta koskevalla yleissopimuksella, huolimatta EU:n viimeaikaisesta aktiivisuudesta. Suuri merkitys sopimuksen kannalta oli se, että neljä Euroopan neuvoston ulkopuolista valtioita(Yhdysvallat, Japani, Etelä-Afrikka, Canada) otti osaa sopimuksen laatimiseen ja ne myös ratifioivat sopimuksen.[21] Tietokoneiden määrän nopea kasvu sekä liittyminen yhteiskunnan toimintaan, että taloudelliseen toimintaan on saanut aikaan tietokonerikollisuuden kasvun. Tietokone itsessään voi liittyä vahvasti tekoihin, mutta tietoverkkorikollisuus on päivän sana.[22]

[20] Pihlajamäki 2008, s.57.
[21] Walden 2011, s.706–708.
[22] Walden 2011, s.681.

3. TIETOVERKKORIKOLLISUUS SUOMESSA TILASTOJEN VALOSSA

Tässä kappaleessa on tilastotietoa tietoliikenteen häirinnästä ja tietojärjestelmän häirinnästä. Taulukosta 1 käy ilmi poliisille tehdyt ilmoitukset vuosittain. Liite 1:stä käy ilmi koko maassa tehdyt syyteharkintaratkaisut valittujen tekojen osalta. Tilastotiedot on hankittu kahdesta eri lähteestä, Poliisin tulostietojärjestelmästä ja syyttäjänlaitoksen tietojärjestelmästä. Suhteessa rikosilmoitusten määriin, syyteharkintaan edenneiden tapausten määrä on alhainen, toisaalta Suomessa syyttäjien syyteharkintakynnys on suhteellisen korkea.

Tietojärjestelmän häirinnästä ei ole annettu vuosien varrella montaa tuomiota, löysin yhden oikeustapauksen rikoslain 38 luvun 7 a § soveltamisesta käytäntöön. Törkeästä tietojärjestelmän häirinnästä ei ole tilastojen mukaan annettu yhtään tuomiota, katso Liite. Vaikka 38 luvun 7 a § ja 38 luvun 7 b § ei ole sovellettu kovin usein, on aihe kuitenkin erittäin ajankohtainen, yksittäisiin tietojärjestelmiin kohdistuu yhä enemmän hyökkäyksiä, käyttäjien itse sitä edes tietämättä.

Kuten useista viimeaikaisista uutisista voi päätellä, on palvelunestohyökkäyksen kriminalisointiin sekä rikostutkintaan, että kansainväliseen yhteistyöhön panostaminen erityisen tärkeä asia nykyaikana.[23] Xinganin mukaan tietotekniikkarikoksia ei alun perin katsottu omaksi rikosalakseen, vaan rikoksista tuomittiin normaaleina rikoksina tai jätettiin kokonaan rankaisematta.[24] Erityisesti tietotekniikkarikosten yhteydessä tulee esiin laillisuusperiaatteesta johtuva laventavan tulkinnan kielto. Rangaistavaa on vain rangaistavaksi säädetty, joten tietotekniikan ja käyttöön liittyviä tekoja ei ole ollut aina mahdollista katsoa rikoksiksi.[25] Joka tapauksessa valtiot ovat joutuneet vastaamaan

[23] Katso:
Yle palvelunestohyökkäyksen kohteena, 27.12.2012:
http://yle.fi/uutiset/yle_palvelunestohyokkayksen_kohteena/6429769.
Palvelunestohyökkäys sulki useita sivustoja, 25.12.2012:
http://www.iltalehti.fi/uutiset/201212251648744 6_uu.shtml.
Tietoturva nyt!, Suomalaisia murrettuja Joomla-palvelimia palvelunestohyökkäyksissä, 20.12.2012:
http://www.cert.fi/tietoturvanyt/2012/12/ttn201212201656.html.
Katsomo.fi palvelunestohyökkäyksen kohteena USA-Suomi -pelin aikana, 17.5.2012:
http://www.mtv3.fi/urheilu/mmjaakiekko2012/uutiset.shtml/2012/05/1550256/katsomofi-palvelunestohyokkayksen-kohteena-usa-suomi-pelin-aikana.
[24] Xingan 2008, s.113.
[25] Saarenpää 2011, s.537.

päivittämällä olemassa olevia rikoslain pykäliä tai luomalla uusia säännöksiä.[26] Kirjallisessa kysymyksessä eduskunnan puhemiehelle vuonna 2007, Oras Tynkkynen on kysynyt, miten hallitus aikoo suojata Suomea tietoverkkouhilta, minimoida niiden haittoja, varmistaa internet-palveluiden saatavuuden kriisiaikoina ja erityisesti palvelunestohyökkäyksiltä. Viestintäministeri Suvi Linden on vastannut, että liikenne- ja viestintäministeriö aikoo kiinnittää huomiota tietoturvaan ja käynnistetty valmistelutyö on kesken. Lisäksi hän on todennut, että EU on tärkeä tekijä, eikä kansallinen lainsäädäntö yksin ratkaise ongelmaa.[27] Euroopan unioni pitää hajautettua palvelunestohyökkäystä huomattavana uhkana Euroopalle.[28] EU on tietojärjestelmiin kohdistuvia hyökkäyksiä koskevassa direktiivissään muuttanut törkeiden tekomuotojen rangaistusasteikkoja ankarampaan suuntaan ja tiivistänyt yhteistyötä jäsenmaiden välillä.[29]

Tietoverkkorikollisuuden yksi syy on uhrien haavoittuvuus. Uhrit, toiminnanharjoittajat ja yritykset, eivät ilmoita rikoksista, koska niiden julkitulo toisi kohdeyritykselle huonoa mainetta, joka voisi vaikuttaa tuleviin liiketoimintamahdollisuuksiin.[30] Lisäksi poliisin on vaikea hankkia näyttöä ja virka-apua joudutaan pyytämään usein.[31] Myös tuomioiden määrä on tietoliikenteen häirintä ja tietojärjestelmän häirintä -rikoksissa alhainen, suhteessa poliisin tietoon tulleisiin rikosilmoitusten määriin. Viime vuosina tietoverkkorikosten määrä ja vakavuus on myös lisääntynyt, erityisesti tietoliikenteen häirintä -tapausten määrä on yli kolminkertaistunut vuodesta 2010 suhteessa vuoteen 2011, kuten taulukosta 1 voi päätellä. Taulukosta on myös helppo havaita määrien huomattava vaihtelu vuosittain, mutta tekojen määrät ovat selvästi nousussa pitkällä aikavälillä tarkastellen. Toisaalta käräjäoikeudessa annettujen tuomioiden määrä, katso Liite, on pysynyt vuosittain melko tasaisena suhteessa Taulukosta 1 ilmeneviin rikosilmoitusten määriin.

Tämän tutkielman kannalta on myös mielenkiintoista todeta, että tietojärjestelmän häirinnästä tehtyjä rikosilmoituksia on ilmennyt suhteellisen vähän, kuten Taulukosta 1 voi päätellä. Toisaalta kappalemäärät ovat selvässä kasvussa vuodesta 2011 eteenpäin. Valtakunnansyytäjänvirastosta saatujen tilastotietojen perusteella, katso Liite,

[26] Walden 2011, s.728.
[27] KK 97/2007 vp. s. 1 & 3.
[28] KOM(2010) 517 lopullinen, s.7.
[29] 2013/40/EU, s.5–6.
[30] KOM(2010) 517 lopullinen, s.3.
[31] Verkkorikoksista seuraa harvoin tuomio. Helsingin sanomat. http://www.hs.fi/kotimaa/Verkkorikoksesta+seuraa+harvoin+tuomio/a1356670497273.

tietojärjestelmän häirinnästä on annettu vain kolme tuomiota. Kyseessä onkin toissijainen pykälä, joka hallituksen esityksessä arveltiin tulevan harvoin sovellettavaksi.[32]

Taulukko 1. Poliisin tietoon tulleet tietojärjestelmän häirintä ja tietoliikenteen häirintä rikosepäilyt ja niiden törkeät tekomuodot vuosilta 2006–2013 (Lähde: Poliisin tulostietojärjestelmä).

Ilmoitettu Kpl	2006	2007	2008	2009	2010	2011	2012	2013
LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	8	5	4	1	8	3	5	9
TIETOLIIKENTEEN LIEVÄN HÄIRINNÄN YRITYS	0	0	0	0	0	1	0	0
TIETOLIIKENTEEN HÄIRINTÄ	36	37	36	33	25	79	50	93
TIETOLIIKENTEEN HÄIRINNÄN YRITYS	0	0	0	0	0	1	1	0
TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	1	2	4	6	2	4	7	13
TIETOJÄRJESTELMÄN HÄIRINTÄ	0	1	3	8	3	3	9	11
TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	0	0	0	0	0	0	0	0
Yhteensä	45	45	47	48	38	91	72	126

Annettujen tuomioiden määrä on alhaisella tasolla suhteessa poliisin tietoon tulleisiin rikosepäilyihin. Eli voitaneen todeta, että näiden kahden rikoslajin selvittäminen on haasteellista. Mikä on sen rikollisuuden määrä, joka ei tule poliisin tietoon?

Tieto- ja viestintärikoksissa tuomitaan usein lempeitä rangaistuksia, yleensä sakkoa, mutta vahingonkorvaukset voivat nousta suuriksi, kuten johdannossa on jo todettu.

[32] HE 153/2006 vp. s.70.

4. PALVELUNESTOHYÖKKÄYKSEN MÄÄRITELMÄ

Palvelunestohyökkäys on käsitteenä vaikea määritellä tyhjentävästi muutamalla lauseella tekniseltä kannalta, johtuen sen moniulotteisuudesta, joten esittelen mitä sillä yleensä tarkoitetaan.

Hallituksen esityksen mukaan palvelunestohyökkäyksellä tarkoitetaan tietojärjestelmän, esimerkiksi palvelinkoneen, tarkoituksellista estämistä taikka hidastamista. Hyökkäystekniikoita on monenlaisia, kuten järjestelmän ylikuormitus, teknisen haavoittuvuuden järjestelmällinen hyväksikäyttö, ohjelmallisen haavoittuvuuden hyväksikäyttö ja niin edelleen.[33] Hallituksen esityksessä ei eroteta tekniseltä kannalta eri palvelunestohyökkäysten muotoja, joita esittelen tässä luvussa.

Palvelunestohyökkäyksen eli DoS-hyökkäyksen kehittyneempi versio on DDoS-hyökkäys eli distributed denial of service -hyökkäys, joka on toteutustavaltaan samankaltainen kuin DoS, mutta hyökkäyksessä käytetään yhden tai muutaman tietokoneen sijasta useita tietokoneita, jotka sijaitsevat eri verkko-osoitteissa. Molemmilla hyökkäyksillä siis pyritään saamaan aikaan sama lopputulos, mutta keinot ovat erit. Hyökkäyksen lopputuloksena kohdejärjestelmä voi kokonaan estyä tarjoamasta palveluja, pystyy tarjoamaan ainoastaan rajoitetusti palveluja tai kykenee tarjoamaan palveluja ainoastaan joillekin käyttäjille.[34]

4.1. DoS

DoS-hyökkäys voidaan suorittaa monilla tavoin, kuten kaatamalla ohjelma, tuhoamalla dataa tai ylikuormittamalla järjestelmä. Sovelluksen kaataminen tarkoittaa aiheutettua seurausta, jonka johdosta ohjelma sammuu tai lopettaa normaalin toiminnan. Seuraus voidaan aiheuttaa esimerkiksi muistinvarausvirheellä tai muilla poikkeuksilla.[35]

Muistinvarausvirhe tapahtuu, kun on syötetty vääräntyyppistä dataa kohtaan, jossa sovellus ei odota sellaista olevan. Muita poikkeamia, jotka voivat saada aikaan sovelluksen

[33] HE 153/2006 vp. s.64.
[34] Application Denial of Service, Is it Really That Easy? Chen 2007, s.5–8.
[35] Poikkeus on ohjelman normaalin toiminnan keskeyttävä virhe.

kaatumisen, ovat esimerkiksi varatun muistin ylittäminen tai sovelluksen tietoturva-aukkojen hyväksikäyttäminen SQL-injektiolla. SQL-injektiolla sovelluksen tietokenttään syötetään koodia, jolla pyritään vaikuttamaan järjestelmän tietokantaan.[36] Sillä voidaan suorittaa esimerkiksi monimutkaisia verkottuneita hakuja, jolloin laskutoimitusten määrä kasvaa moneen potenssiin tai DELETE-käskyllä voidaan tuhota dataa.

Yksinkertainen tapa suorittaa DoS-hyökkäys on seuraava: hyökkääjä pyrkii lukitsemaan järjestelmän kaikki käyttäjätilit käyttämällä hyväkseen internet-sivun käyttäjätilien suojaksi luotuja turvamekanismeja. Hyökkääjä kokeilee jokaisen käyttäjänimen kohdalla useita salasanoja eli tekemällä sisäänkirjautumisyrityksiä. Lopputuloksena on DoS, koska kaikki käyttäjätilit ovat lukossa.[37]

Hyökkääjä voi myös yrittää saada aikaan kohdejärjestelmän resurssien ylikuormitustilanteen, mikäli hyökkääjällä on itsellään käytössä tarpeeksi suuret resurssit. Yksinkertaisimmilla DoS-hyökkäyksillä se ei ole enää nykypäivänä mahdollista. Ylikuormituksen kohteena voi olla kohdejärjestelmän prosessori, muisti tai sovellukselle allokoitu muisti. Prosessorin ylikuormitus onnistuu esimerkiksi suorittamalla keskustelufoorumin hakutoimintoa hyväksikäyttäen, laaja ja monimutkainen haku, skriptin avulla, yhä uudelleen.[38] Monilla keskustelufoorumeilla on rajoitettu käyttäjäkohtaisten hakujen määrää, edellä mainitun uhan vuoksi ja sivuston sujuvan toiminnan varmistamiseksi.

Muistin ylikuormitus voidaan suorittaa yksinkertaisimmillaan sähköpostisovelluksen avulla, hyökkääjä voi esimerkiksi luoda suuren määrän sähköposteja, joihin hän lataa liitetiedostoja, mutta jättää viestit lähettämättä. Liitteet tallentuvat automaattisesti sovelluksen muistiin, kunnes lähetä-nappia on painettu. Lopputuloksena on sovelluksen muistin täyttyminen.[39]

Ylikuormitustilanteen voi saada aikaan kohdejärjestelmässä myös siten, että hyökkääjä lähettää komennon, mutta hyväksyy hitaasti kohdejärjestelmältä palautuvaa dataa. Hyökkääjä ei halua kaikkea palautuvaa dataa hyväksyä, koska hänen pyrkimyksenään on

[36] Tietokantakäskyt mahdollistavat tiedonhankinnan, tietojärjestelmään tunkeutumisen ja sen kaatamisen.
[37] Application Denial of Service, Is it Really That Easy? Chen 2007, s.10–20.
[38] Skripti on yksinkertainen ohjelma, joka on luotu jonkin tehtävän suorittamiseksi, esimerkiksi taustalle valvomaan jonkin ehdon toteutumista.
[39] Application Denial of Service, Is it Really That Easy?, Chen 2007, s.10–20.

kohdejärjestelmän yhteysjonon täyttäminen. Palvelimeen eli kohdejärjestelmään on määritelty maksimiyhteyksien määrä, ja kun maksimimäärä yhteyksiä on jonossa, järjestelmä lopettaa vastaamisen yhteyspyyntöihin ja tuloksena on DoS.[40]

Laitepuolella hyökkääjä voi saada aikaan ylikuormitustilanteen käyttämällä hyväkseen jonkin internet-sovelluksen vikaviestejä, eli lokeja. Hyökkääjä tunnistaa omalle järjestelmälleen kevyen hyökkäystavan, mikä saa kohdejärjestelmän ohjelman luomaan virhelokin kiintolevylle. Hyökkääjä toistaa hyökkäyksen, kunnes kohdejärjestelmän kiintolevy on täynnä. Kohdejärjestelmä voi tämän seurauksena kaatua tai sovellus voi kaatua, joka tapauksessa seuraukset ovat arvaamattomat. Mikäli hyökkääjällä on käytettävissään niin sanotusti nopea internet-yhteys, hän voi tehdä useita pieniä kyselyjä kohdejärjestelmälle yhä uudelleen, mikä saa aikaan suuren määrän dataa, jolloin kohdejärjestelmä tukkii itse internet-yhteytensä ja tuloksena on DoS.[41]

4.2. Infrastruktuuritason DoS

Työkalu on merkityksetön ilman oikeanlaista käyttötapaa. Palvelunestohyökkäys voidaan toteuttaa monin tavoin, mutta yleinen tapa on väärinkäyttää verkkoprotokollia.[42] Yksi ensimmäisistä hyökkäystavoista oli infrastruktuuritason DoS-hyökkäys, eli hyökkäyksen tarkoitus oli ylikuormittaa kohdejärjestelmän resurssit, esimerkiksi sen tiedonkäsittelykapasiteetti.[43]

Tietoverkkohyökkäykset ovat moniulotteisia ja hyödyntävät mitä tahansa internet-protokollan neljästä eri kerroksesta: sovelluskerrosta, kuljetuskerrosta, internet-kerrosta tai verkkokerrosta.[44] TCP-protokolla kuuluu kuljetuskerrokseen ja sen kolmivaiheista kättelyä voidaan hyväksikäyttää hyökkäyksessä. Kolmivaiheisessa kättelyssä on tarkoituksena, että a) lähettäjä ottaa yhteyden, b) kohdekone vastaa, c) lähettäjä kuittaa yhteydenoton. SYN flood -hyökkäyksessä hyökkääjä lähettää suuren määrän TCP:n yhteydenmuodostamispaketteja (SYN, synchronize) ja jättää yhteydenottokuittaukset tekemättä, jolloin kohdekone jää odottamaan vastauksia lähettäjältä. Kohdejärjestelmän resursseja sitoutuu tällöin monella eri tasolla (palvelin, palomuuri, reititin ja niin

[40] Andrews et al. 2006, s.113.
[41] Application Denial of Service, Is it Really That Easy? Chen 2007, s.10–20.
[42] Palvelunestohyökkäyksiä on monta lajia, WWW.CERT.FI 2007, s.1.
[43] Mcclure et al. 2005, s.491.
[44] Cisco Press 2001, s.65.

edelleen).[45] Monet järjestelmät voivat kestää satoja samanaikaisia yhteyksiä tiettyyn porttiin, mutta yhteydenmuodostamiseen allokoitujen resurssien kuluttaminen loppuun voi vaatia ainoastaan kymmenen keskeneräistä yhteydenmuodostusta.[46]

SYN flood on pääasiallinen järjestelmän ylikuormituskeino laajoissa DoS- ja DDoS-hyökkäyksissä. Hyökkäys voidaan suorittaa seuraavasti: a) hyökkääjä ottaa yhteyden kohdejärjestelmään ja muuntaa lähettäjäksi järjestelmän, jota ei ole olemassa, b) kohdejärjestelmä yrittää vastata, mutta ei ikinä saa vastausta, jolloin yhteys jää jonoon. Mikäli lähettäjäksi olisi väärennetty jokin järjestelmä, joka ei ole yhteyspyyntöä tehnyt, kohdejärjestelmä saisi siltä vastauksen, eikä yhteys menisi jonoon. SYN-yhteysjonon ajastin voi olla 75 sekunnista 23 minuuttiin, minkä ajan järjestelmä odottaa yhteydenmuodostumista lähettäjään. Koska yhteysjono on yleensä melko lyhyt, voi hyökkääjä ylikuormittaa sen esimerkiksi 10 sekunnin välein lähetetyin yhteydenmuodostamisviestein, jolloin kohdejärjestelmä ei ehdi tyhjentämään yhteydenmuodostamisjonoaan.[47]

Hyökkäyksessä voidaan lisäksi käyttää hyväksi ICMP-kontrolliprotokollan ICMP ECHO REQUEST -paketteja eli ping:iä. Tässä hyökkäystavassa kuormitetaan kohdejärjestelmää lähettämällä verkkoon ping-yhteydenottopaketteja, joiden lähettäjäksi on muutettu oikean lähettäjän sijaan kohteena olevan koneen IP-osoite. Verkossa olevat koneet, jotka ovat vastaanottaneet yhteydenottopaketin, lähettävät vastauksensa kohdejärjestelmälle, jolloin kaikki paketit näyttävät kohdejärjestelmän näkökulmasta, tulevan eri osoitteista, eikä hyökkäyksen torjuminen tietenkään tällöin onnistu IP-osoitteen perusteella.[48] Smurf-hyökkäys on edellisen hyökkäyksen kehitysmuoto, jossa tehoa on kasvatettu käyttämällä hyväksi usean tietokoneen sisältävää, huonosti konfiguroitua verkkoa. Hyökkääjä lähettää tehosteverkon broadcast-osoitteeseen[49] ping:in, jonka lähettäjäksi on väärennetty hyökkäyksen kohdejärjestelmä. Seurauksena tehosteverkon kaikki koneet lähettävät vastauksensa kohdejärjestelmälle, jolloin hyökkääjän viestin teho nousee suhteessa tehosteverkon koneiden lukumäärään.[50] Variantteja edellä mainitusta hyökkäystavasta on myös olemassa, esimerkiksi Fraggle, mutta periaate on sama.

[45] Palvelunestohyökkäyksiä on monta lajia, WWW.CERT.FI 2007, s.1.
[46] Mcclure et al. 2005, s.492.
[47] Mcclure et al. 2005, s.492.
[48] Palvelunestohyökkäyksiä on monta lajia, CERT.FI 2007, s.1–2.
[49] Broadcast-osoite on osoite, jolla verkon kaikille koneille voidaan lähettää tiedotusluontoinen viesti tai suorittaa verkkodiagnostiikkaa. Lähde:https://wiki.helsinki.fi/display/verkko/Protokollat.
[50] Mcclure et al. 2005, s.493.

Monia hyökkäystapoja on hylätty, koska palveluntarjoajat ja verkkojen ylläpitäjät ovat estäneet suunnatut broadcast-lähetykset. Seuraava kehitysaskelma oli DDoS-hyökkäykset.[51] Nimipalvelimia eli DHCP-palvelimia on myös käytetty hyväksi.[52] Niille on lähetetty DNS-kyselyitä, joiden lähettäjäksi on väärennetty hyökkäyksen kohde, jolle DHCP-palvelimet puolestaan lähettävät vastauksensa. DNS-kyselyihin käytetään UDP-protokollaa, joka ICMP:n tapaan ei vaadi molemmilta yhteyden osapuolilta varmistusta yhteyttä muodostettaessa, kuten SYN-yhteydenotot edellyttävät.[53]

4.3. Sovellustason DoS

Sovellustason häirintä on yksi DoS:n suorittamistapa ja vaatii huomattavasti vähemmän resursseja hyökkääjältä. Ensin hyökkääjä etsii suositun internet-sivuston, jonka kuormittaminen vaatii vähän resursseja, mutta aiheuttaa kohdejärjestelmässä moninkertaisen resurssitarpeen.[54] Esimerkiksi vertaisverkon heikkoa tietoturvaa hyödyntämällä voidaan ohjata www-palvelimen käyttämään TCP-porttiin 80, normaalin HTTP-liikenteen sijasta, direct connect -liikennettä. Pelkistetyin palvelunestotilanne onkin palvelun rasittaminen raskaalla käytöllä. Tilanne voidaan saavuttaa ilmoittamalla www-osoite vilkkaalla keskustelufoorumilla, mikäli kohdepalvelin on alitehoinen. Ohjelmistohaavoittuvuus myös altistaa palvelunestohyökkäykselle. Yksinkertaisuudessaan palvelunestohyökkäys onnistuu verkkoyhteyden tukkimisella merkityksettömällä tietoliikenteellä. Yhteyksien määrän kasvaessa yli verkon sietokyvyn, se lamautuu.[55]

Työkaluina tietoverkkohyökkäyksissä voidaan käyttää internetistä saatavilla olevia valmiita työkaluja, esimerkiksi WinTrinoo, Trinoo, Agobot/Gaobot, Tribe Flood Network, Stacheldracht ja niin edelleen.[56]

Hallituksen esityksessä tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä mainitaan: ”Myös vahingoittamistarkoituksessa käytettävät välineet voivat olla

[51] Mcclure et al. 2005, s.493.
[52] Suomalaisia nimipalvelimia on käytetty palvelunestohyökkäyksessä. Maailmanlaajuisesti hyökkäyksessä on ollut noin 176 000 nimipalvelinta. http://www.digitoday.fi/tietoturva/2007/02/12/cert-fi-100-suomalaista-nimipalvelinta-dos-hyokkayksessa/20073742/66.
[53] Palvelunestohyökkäyksiä on monta lajia, CERT.FI 2007, s.1–2.
[54] Mcclure et al. 2005, s.497.
[55] Palvelunestohyökkäyksiä on monta lajia, CERT.FI 2007, s.1–2.
[56] Mcclure et al. 2005, s.495.

kaksikäyttöisiä."[57]. Palvelunestohyökkäykseen voidaan käyttää esimerkiksi ohjelmaa, jota normaalisti käytetään lailliseen käyttötarkoitukseen, esimerkiksi sähköpostin joukkolähetykseen, mutta väärinkäytettynä sitä voidaan käyttää lähettämään miljoona sähköpostia yhdelle palvelimelle. Täten täysin laillinen ohjelma voi olla laissa määritelty tietoverkkorikosväline, mutta kuten HE:ssä on mainittu: "yleensä vahingoittamistarkoituksessa käytettävät välineet eivät ole kaksikäyttöisiä" [58].

4.4. DoS:sta DDoS:iin

DDoS-hyökkäys oli DoS-hyökkäyksen looginen kehitysaskelma, kun tietokonejärjestelmät kyettiin suojaamaan palomuureilla DoS-hyökkäyksien varalta 1990-luvun lopussa.[59] DDoS-hyökkäyksen tarkoituksena on internet-verkon fyysisellä tai sovellustasolla rajallisen kaistan eli tiedonsiirtokyvyn ylikuormittamisnen, jolloin lopputuloksena on järjestelmän tukkeutuminen, järjestelmän tiedonsiirtokapasiteetin ylittäminen tai koko runkoverkon ylikuormitus.[60] Jokainen DDoS-hyökkäyksessä hyväksikäytetty tietokone tuottaa pieniä määriä tietoliikennettä, mikä ylikuormittaa kohdejärjestelmän.[61] 2000-luvun alussa ymmärrettiin uuden DoS-uhkan eli DDoS:n mahdollisuudet, kun useissa hyökkäyksissä käytettiin hyväksi TCP/IP-protokollan rajoituksia, erityisesti SYN-hyökkäystä.[62] SYN-hyökkäyksessä hyväksikäytetään TCP/IP:n kaksivaiheista kättelyä, siten että kohdejärjestelmän resursseja sitoutuu turhaan.

DoS-hyökkäyksessä hyökkääjän työkaluksi riittää yksittäinen tietokone, toisin kuin DDoS:ssa.[63] DoS-hyökkäyksissä käytettiin hyväksi järjestelmän haavoittuvuuksia, kuten ylisuuria paketteja(ping of death), pakettien fragmentoimista eli hajauttamista, päättymättömiä silmukoita, skriptejä, joilla kokeiltiin erilaisia tapoja haavoittuvuuksien löytämiseksi.[64] Moderneissa DoS-hyökkäyksissä käytetään hyväksi tiedonsiirtokapasiteettiin kohdistuvia hyökkäyksiä, toisin kuin aikaisemmissa, joissa hyökkäys kohdistettiin kohdejärjestelmän resurssien kuluttamiseen.[65]

---

[57] HE 153/2006 vp s.64.
[58] HE 153/2006 vp s.64.
[59] Mcclure et al. 2005, s.488.
[60] Tiedonsiirtokapasiteetti on riippuvainen palveluntarjoajalta ostetusta palvelusta eli yhteyden nopeudesta tai runkoverkon fyysisestä tiedonsiirtokapasiteetista eli käytetystä tiedonsiirtotekniikasta, valokuitu, kupari ja niin edelleen.
[61] Application Denial of Service, Is it Really That Easy? Chen 2007, s.8.
[62] Mcclure et al. 2005, s.488.
[63] Application Denial of Service, Is it Really That Easy? Chen 2007, s.41.
[64] Mcclure et al. 2005, s.490.
[65] Mcclure et al. 2005, s.491.

DDoS-hyökkäyksen työkaluna on mahdollista käyttää vertaisverkkoa, haltuunotettujen tietokoneiden verkostoa(botnet) tai verkkomatoa. Vertaisverkot, kuten DC++ eli direct connect -verkot, on rakennettu tiedostojenjakoon ja niissä olevia tietoturva-aukkoja hyödyntäen koneiden kaappaaminen on mahdollista. Niin sanotun botnetin, eli hallintaan otettujen koneiden verkoston käyttäminen perustuu tietoturva-aukkojen hyödyntämiseen. Koneet on otettu esimerkiksi viruksen avulla etähallintaan, jolloin niitä on mahdollista käyttää hyökkäyksissä. Kaapattuja koneita on kutsuttu aikaisemmin zombeiksi, mutta nykyään bot:eiksi, niiden hallitsemiseen käytetyn etähallintaohjelman alkuperäisen nimen perusteella. Ohjelma on ollut osa Internet Relay Chat eli IRC:n skriptejä, joita kutsuttiin boteiksi. Haltuunotettujen koneiden verkostoista on käytetty zombie-verkko tai bot-armeija nimityksiä.[66] Nykyään pääasiallinen kaikkein vaarallisimpien bot:ien ohjausmekanismi on IRC.[67] Bot-armeijaa voidaan käyttää muun muassa, DDoS-hyökkäyksiin, roskapostin lähettämiseen, omien jälkien peittämiseen, tiedon keräykseen ja tartuttamaan muita tietokoneita bot:eiksi. Verkkoa voidaan siten käyttää lailliseen ja laittomaan tarkoitukseen.

Verkkomato on tietokonevirus, joka leviää internetissä ohjelmistojen tietoturvahaavoittuvuuksia hyväksikäyttäen. Tietokoneeseen tartuttuaan mato ottaa yhteyksiä ennalta määritettyyn kohteeseen. Madon levitessä kasvaa myös kohdejärjestelmän kuormitus eli DDoS-hyökkäys voimistuu. Madon toiminta on ennalta ohjelmoitua, eikä sitä hallita etäyhteyden avulla.[68]

4.5. DADoS

DADoS -hyökkäys eli distributed application denial of service -hyökkäys oli seuraava kehitysaskel DDoS-hyökkäyksestä. DADoS:ssa käytetään kaapattuja koneita, mutta lukumäärällisesti vähemmän kuin DDoS-hyökkäyksessä, joten DADoS:n suorittaminen ei vaadi hyökkääjältä yhtä suuria resursseja. Sovelluspohjaiset hyökkäykset ovat vakava uhka organisaatioille, koska ne voidaan tehdä pienin resurssein ja ne keskittyvät sovelluslogiikkaan liittyviin virheisiin tietojärjestelmän tiedonsiirtokapasiteetin ylikuormittamisen sijaan.[69]

[66] Mcclure et al. 2005, s.494.
[67] Mcclure et al. 2005, s.640.
[68] Palvelunestohyökkäyksiä on monta lajia, CERT.FI 2007, s.1.
[69] Mcclure et al. 2005, s.488.

4.6. Yhteenveto

Kun tekijä suorittaa tietoverkkohyökkäyksen, liittyy tekoon yleensä rikosoikeudellisessa mielessä, useita eri rikoksia. Tekijä voi syyllistyä yhdessä teossa, rikoksen eri vaiheista riippuen, esimerkiksi tietoverkkorikosvälineen hallussapitoon, luvattomaan käyttöön, vaaran aiheuttamiseen tietojenkäsittelylle, tietoliikenteen häirintään tai tietojärjestelmän häirintään ja niin edelleen.

Kuten sovellustason DoS -hyökkäystä koskevassa kappaleessa on todettu, yksinkertaisimmillaan tietoverkkohyökkäys on mahdollista suorittaa keskittämällä raskasta verkkoliikennettä palvelimelle, mikä ei sitä ole suunniteltu kestämään. Kysymyksessä ei välttämättä ole rikos, esimerkiksi tietoliikenteen häirintä, jos tarkoituksena ei ole ollut saada aikaan palvelimen ylikuormitus, vaan esimerkiksi ainoastaan ottaa kantaa asioihin. Teon tahallisuus on yksi tunnusmerkistön täyttymisen edellytys.

5. PALVELUNESTOHYÖKKÄYKSEN KRIMINALISOINNIN TAUSTA

5.1. Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus tehtiin Budapestissä 23. päivänä marraskuuta 2001. Eduskunta hyväksyi sopimuksen ja sopimus astui voimaan. Suomi teki siihen muutamia varaumia. Yleissopimuksen voimaansaattamisen yhteydessä muutoksia tehtiin rikoslakiin, pakkokeinolakiin, esitutkintalakiin ja kansainvälisestä oikeusavusta rikosasioissa annettuun lakiin.[70] Tämän työn kannalta kiinnostavia ovat rikoslakiin lisätyt tietojärjestelmän häirintää sekä tietoverkkorikosvälineen hallussapitoa koskevat säännökset, että tiettyjen rikosten yrityksen säätäminen rangaistavaksi, joita olivat RL 35:1,2 tietovahingonteko, RL törkeä tietovahingonteko, RL 38:5 tietoliikenteen häirintä, RL 38:6 törkeä tietoliikenteen häirintä ja RL 38:7 lievä tietoliikenteen häirintä.[71] Euroopan neuvoston tietoverkkorikossopimus on ensimmäinen tietotekniikkarikoksia koskeva yleissopimus. Sen ovat allekirjoittaneet Euroopan neuvoston jäsenmaiden lisäksi Argentiina, Australia, Chile, Costa Rica, Dominikaaninen tasavalta, Etelä-Afrikka, Japani, Kanada, Meksiko, Panama, Filippiinit, Senegal ja Yhdysvallat. Ruotsi ei ole sitä ratifioinut, vaikka on Euroopan neuvoston jäsenvaltio.[72] Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen katsotaan olevan tähän mennessä täydellisin kansainvälinen standardi, joka tarjoaa kattavan kehyksen tietoverkkorikollisuuden eri muotoihin.[73] Sopimuksen 5 artiklassa on säädetty tietojärjestelmän häirinnästä:

> Tietojärjestelmän häirintä
>
> Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman tietojärjestelmän toiminnan vakavan estämisen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla.

[70] HE 153/2006 vp s.1.
[71] HE 153/2006 vp s.10.
[72] Reaaliaikainen sivusto sopimuksen ratifioinneista ja allekirjoittaneista valtioista. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. Viitattu 2.1.2013.
[73] KOM(2010) 517 lopullinen, s.2.

Sanktioista sopimuksessa säädettiin ainoastaan seuraavaa:

> Sanktiot ja muut seuraamukset
> 1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaakseen, että 2-11 artiklan mukaisesti rangaistaviksi säädettyihin tekoihin syyllistyneille voidaan määrätä tehokkaat, tekoon nähden oikeassa suhteessa olevat ja riittävät rangaistukset, mukaan luettuna vapausrangaistus
> 2. ..

5.2. Euroopan Unionin neuvoston puitepäätös

Rikosoikeus on perinteisesti ollut kansallista alkuperää. Jokainen valtio on päättänyt rangaistavien tekojen alasta, rangaistuksista ja oppirakenteista. Kansainvälistä rikosoikeusyhteistyötä on kuitenkin tehty jo 1900-luvun alusta lähtien, koska tietyt rikollisuuden lajit koettiin kansainvälisiksi.[74] Euroopan unionin rikosoikeus on alueellinen ilmiö, vaikka EU ei ole liittovaltio. Lissabonin sopimuksen myötä EU:n laajentunut ja tehostunut rikosoikeudellinen toimivalta voi Melanderin mukaan merkitä siirtymää lähemmäksi liittovaltiota, johtuen rikosoikeuden läheisestä yhteydestä kansalliseen suvereniteettiin.[75] Melanderin mukaan EU-rikosoikeus pitäisi olla tällä hetkellä rikosoikeuden arkipäivää ja rikosoikeuden eurooppalaistuminen on tärkeintä, mitä rikosoikeudessa on tapahtunut kymmeneen vuoteen. EU-rikosoikeus on osa suomen kansallista rikosoikeutta.[76]

Euroopan unionin rikosoikeuden historiassa on monia käänteitä, jotka ovat laajentaneet sen rikosoikeudellista toimivaltaa. EU:n piirissä on tehty rikosoikeudellista epävirallista, mutta tehokasta yhteistyötä jo ennen sopimuksien allekirjoittamista. Näin tapahtui jo 1962 epäonnistuneiden EY-petosten saralla, mutta myös myöhemmin muun muassa onnistuneiden TREVI-yhteistyön merkeissä 1975. Yhteistyö oli tuolloin ad hoc -luontoista ja EY-oikeudellisten puitteiden ulkopuolista. Rikosoikeudellinen yhteistyö sisällytettiin unionin tehtäviin Maastrichtin sopimuksella, joka allekirjoitettiin 7.2.1992 ja tuli voimaan 1.11.1993. Maastrichtin myötä luotiin Euroopan unionin kolmen pilarin-järjestelmä. Kolmas pilari, joka oli hallitusten välistä yhteistyötä sisältävä, käsitti oikeus- ja sisäasiat eli muun muassa oikeudellisen yhteistyön rikosoikeuden alalla.

[74] Melander 2010, s.1.
[75] Melander 2010, s.2.
[76] Melander 2010, s.2.

Lissabonin sopimus tuli voimaan 1.12.2009, joka sai aikaan muutoksia EU:n rikosoikeudellisessa yhteistyössä.[77] Sopimuksen myötä unionin pilarirakenteesta luovuttiin, joten rikosoikeudellinen yhteistyö kuuluu tällä hetkellä unionin jaetun toimivallan alaan. Yhteistyö ei tosin koske kaikkia jäsenvaltioita, koska muutama on jättäytynyt sen ulkopuolelle (Iso-Britannia, Irlanti ja Tanska). Lisäksi sopimuksen myötä EU-tuomioistuimen toimivalta rikosoikeudellisissa asioissa muuttui ennakkoratkaisutoimivallaksi.[78]

Rikosoikeudellisen yhteistyön instrumentteina käytetään nykyään puitepäätösten sijaan direktiivejä, SEUT[79] 82(2) ja SEUT 83(1) ja (2) artiklojen mukaisesti. Amsterdamin sopimuksen aikaiset puitepäätökset ovat kuitenkin vielä merkityksellisiä, koska ne ovat vielä voimassa. Lissabonin sopimukseen liitetyn siirtymämääräyksiä koskevan pöytäkirjan 19 artiklan 3 kappaleessa asetetaan vanhoille III-pilarin instrumenteille viiden vuoden enimmäisvoimassaoloaika Lissabonin sopimuksen voimaantulosta lukien. Komissio pyrkii korvaamaan voimassa olevat puitepäätökset direktiiveillä viiden vuoden sisällä eli vuosina 2010–2014.[80] Tämän työn kannalta tärkeä puitepäätös, 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä on vielä voimassa, mutta Euroopan parlamentti ja Euroopan unionin neuvosto hyväksyivät 12.8.2013 direktiivin 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.[81]

Puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä perustuu Euroopan neuvoston tietoverkkorikollisuutta koskevaan yleissopimukseen (CETS No. 185, SopS 60/2007) ja ne molemmat voimaansaatettiin samalla hallituksen esityksellä osaksi Suomen kansallista oikeutta. Yleissopimuksen artiklojen on katsottu toimeenpanoa koskevassa hallituksen esityksessä vastaavan puitepäätöksen kriminalisointivelvoitteita.[82] Melanderin mukaan yleissopimusta ja puitepäätöstä on aineellisen rikosoikeuden kriminalisointivelvoitteiden osalta, tulkintavaikutusta pohdittaessa, tulkittava kokonaisuutena.[83] Lisää EU-oikeudellisesta tulkintavaikutuksesta ja rikosoikeudellisen laillisuusperiaatteen siihen

[77] Melander 2010, s.14.
[78] Melander 2010, s.15–16.
[79] Sopimus Euroopan Unionin toiminnasta.
[80] EUVL C 306, 17.12.2007, s.164.
[81] Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin kansalliset täytäntöönpanotoimet. Oikeusministeriö. 2013.
[82] HE 153/2006, s.50–51.
[83] Melander 2010, s.317.

aiheuttamista rajoituksista jaksossa 3.6 Direktiiviehdotus tietojärjestelmiin kohdistuvista hyökkäyksistä.

Euroopan unionin puitepäätöksessä tietojärjestelmiin kohdistuvista hyökkäyksistä oleva tietojärjestelmän häirintää koskeva 3 artikla on sisällöltään yhtenevä aikaisemmin laaditun Euroopan neuvoston yleissopimuksen 5 artiklan kanssa. Melanderin mukaan puitepäätös vastaa Euroopan neuvoston tietoverkkorikollisuutta koskevaa yleissopimusta, mutta on suppeampi sisällöltään[84]. Puitepäätös sisältää ainoastaan 13 artiklaa(2005/222/YOS), kun yleissopimus sisältää 48 artiklaa(SopS 60/2007). Yleissopimuksessa on säädetty sopimusosapuolten velvollisuuksista laajemmin kuin puitepäätöksessä.

Puitepäätöksen 3 artiklassa on säädetty:

> Laiton järjestelmän häirintä
>
> Kunkin jäsenvaltion on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että oikeudeton tietojärjestelmän toiminnan tahallinen törkeä estäminen tai keskeyttäminen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla tai saattamalla datan käyttökelvottomaksi, on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

Lisäksi puitepäätöksen 7 artiklassa on säädetty raskauttavista olosuhteista, jotka edellyttivät tietojärjestelmän häirinnän törkeän tekomuodon kriminaalisointia, vastaavaa artiklaa ei ole Euroopan neuvoston yleissopimuksessa:

> Raskauttavat olosuhteet
>
> 1. Kunkin jäsenvaltion on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 2 artiklan 2 kohdassa sekä 3 ja 4 artiklassa tarkoitetusta teosta voidaan määrätä rikosoikeudellisia seuraamuksia, jotka enimmillään ovat vähintään kahdesta viiteen vuotta vankeutta, kun teko on tehty yhteisessä toiminnassa 98/733/YOS annetun määritelmän mukaisen rikollisjärjestön puitteissa riippumatta siitä, mikä on yhteisessä toiminnassa säädetty seuraamus
> 2. Jäsenvaltio voi toteuttaa 1 kohdassa tarkoitettuja toimenpiteitä myös silloin, kun teko on aiheuttanut vakavia vahinkoja tai vaikuttanut haitallisesti olennaisiin etuihin.

[84] Melander 2010, s.25.

Puitepäätöksen johdanto-osan 13 kohdassa on lausuttu, että kansallisissa implementoinneissa on keskityttävä vähäistä huomattavampiin tekoihin ja kriminalisoimatta tulee jättää muun muassa luvalliset tietojärjestelmien tietoturvatestaukset:

> (13) On vältettävä ylikriminalisointia, erityisesti vähämerkityksisten tapausten säätämistä rangaistaviksi, ja kriminalisoimasta toimintaa, jota harjoittavat oikeudenhaltijat tai toimintaan oikeutetut henkilöt.

5.3. Tietojärjestelmän häirintä

5.3.1. Tietojärjestelmän häirintä

Rikoslain 38 luvun 7 a §:ssa on säädetty tietojärjestelmän häirinnästä:

> Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava.

Lakitekstissä tietojärjestelmä tarkoittaa yksittäistä laitetta ja laitteiden kokonaisuutta, tietoverkko mukaan lukien. Data tarkoittaa sellaisia tietoja, jotka soveltuvat käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, jotka tietokone voi suorittaa.[85]

Tämän säännöksen yhteydessä oleva datan käsite poikkeaa esimerkiksi Pihlajamäen esittämästä määritelmästä, hänen mukaansa datan ei tarvitse olla tietokoneella käsiteltävässä muodossa, vaan data voi olla merkkejä, jotka ovat luettavassa, käsiteltävässä tai viestittävissä olevassa muodossa.[86]

Häirinnän tulee olla tahallista sekä oikeudetonta, että aiheuttaa haittaa tai vahinkoa. Teon oikeudettomuuden voi poistaa esimerkiksi suostumus.[87] Vakava häiriö voi olla järjestelmän toiminnan merkittävää hidastumista tai sen toimintavarmuuden merkittävää heikkenemistä

[85] HE 153/2006 vp. s.12.
[86] Pihlajamäki 2004, s. 26–27.
[87] HR 153/2006 vp. s.65.

siten, että tietojärjestelmää ei voida käyttää sen normaalilla käyttötarkoituksen edellyttävällä tavalla.[88]

Lakitekstistä käy ilmi että kyseessä on toissijainen säännös, joka säädettiin Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen ja Euroopan unionin puitepäätöksen tietojärjestelmään kohdistuvista hyökkäyksistä vuoksi. Tietojärjestelmän häirinnästä säädetään yleissopimuksen 5 artiklassa ja puitepäätöksen 3 artiklassa.[89]

RL 38 luvun 5 §:ssä on säädetty tietoliikenteen häirinnästä, jossa teon kohteena on viestintä. RL 38 luvun 7 a §:ssä kohteena on sitä vastoin tietojärjestelmä. Hallituksen esityksessä on arveltu 38 luvun 7 a §:n tulevan sovellettavaksi harvoin johtuen sen toissijaisuudesta, mutta se on kuitenkin katsottu tarpeelliseksi, koska yleissopimuksen ja puitepäätöksen artiklat kattavat kaikentyyppisen tietojärjestelmän häirinnän eli myös sellaisen, joka ei edes välillisesti liity viestien siirtoon.[90]

Datan syöttämisellä on tarkoitettu RL 38 luvun 7 a §:ssä sellaista hyökkäystä, joka aiheuttaa kohteessa toimintahäiriön. Toimintahäiriö voi johtua järjestelmän tarkoituksellisesta ylikuormituksesta tai syötettävän datan häiriötä aiheuttavista ominaisuuksista.[91] Datalla tarkoitetaan laissa ja hallituksen esityksessä sellaisessa muodossa olevia tietoja, jotka voidaan käsitellä tietojärjestelmässä ja ohjelmia, jotka voidaan suorittaa tietokoneessa jonkin toiminnon saavuttamiseksi.[92]

Jos tekotapana on datan vahingoittaminen, HE:ssä on huomautettu teon voivan täyttää samalla RL 35 luvun 1 § 2 momentissa tarkoitetun tietovahingon tunnusmerkistön. Edellä mainitussa tapauksessa tietojärjestelmän häirintää koskeva säännös ei kuitenkaan syrjäydy, koska HE:ssa mainittu RL 35 luvun 1 § 2 momentti jäi lievemmin rangaistavaksi kuin RL 39 luvun 7 a §. Tietovahingon soveltamisalaksi jää datan vahingoittaminen siten, että tietoliikenteen häirinnän tai tietojärjestelmän häirinnän tunnusmerkistöt eivät täyty. Jos teko täyttää sekä törkeän tietojärjestelmän häirinnän tunnusmerkistön RL 38 luvun 7 b §, että törkeän vahingonteon tunnusmerkistön, sovellettavaksi tulee RL 38 luvun 7 b §, koska

[88] HE 153/2006 vp. s.66.
[89] HE 153/2006 vp. s. 64–65.
[90] HE 153/2006 vp. s.65.
[91] HE 153/2006 vp. s.13.
[92] HE 153/2006 vp. s.65.

siinä ei ole toissijaisuuslauseketta. Molempien tekojen rangaistusmaksimi on neljä vuotta vankeutta.[93]

HE:ssä on todettu tietojärjestelmän häirinnän mahdollisesta rangaistavuudesta rikoslain 35 luvun 1 §:n 2 momentissa säädettynä vahingontekona. Vahingonteko ei kuitenkaan kata tekoa silloin kun tekotapana on jokin muu kuin suoranainen dataan kajoaminen. Myöskään rikoslain 28 luvun 7 §:n luvaton käyttö ei kata tekoa silloin, kun tekotapa ei sisällä suoranaista tietojärjestelmän käyttöä.[94]

Hallituksen esityksessä on todettu tietojärjestelmän häirintä -säännöksen eron suhteessa vahingontekoon olevan se, että tietojärjestelmän häirinnässä hyökkäys ei kohdistu järjestelmässä olevaan dataan, vaan järjestelmän toimintaan, josta esimerkki on palvelunestohyökkäys.[95]

5.3.2. Törkeä tietojärjestelmän häirintä

Rikoslain 38 luvun 7 b §:ssä on säädetty törkeästä tietojärjestelmän häirinnästä:

> *1)* Aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai
> *2)* Rikos tehdään erityisen suunnitelmallisesti
>
> ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.
>
> Yritys on rangaistava.

Pykälän erityisen tuntuvalla taloudellisella vahingolla tarkoitetaan rahassa mitattavia vahinkoja, jotka on aiheutettu tietojärjestelmän haltijalle. Vahinkoa voi aiheutua välittömien hankinta-, korjaus-, ja huoltokustannusten lisäksi siitä, että uhri joutuu käyttämään oman järjestelmänsä sijasta toista järjestelmää. Vahinkoa voi syntyä myös välillisesti, esimerkiksi menetettyinä tuloina. Erityisen tuntuvalla haitalla puolestaan tarkoitetaan aiheutetun seuraamuksen muita kuin taloudellisia vahinkoja. Tietojärjestelmän käyttömahdollisuuksien menettäminen tai heikkeneminen aiheuttaa uhrille haittaa. Erityinen suunnitelmallisuus voi ilmetä poikkeuksellisen laajoina ja monimutkaisina

[93] Frände et al. 2010, s.400.
[94] HE 153/2006 vp s.16–17.
[95] HE 153/2006 vp, s.16.

valmistelutoimenpiteinä. Myös monimutkaiset harhautustoimenpiteet kiinnijäämisen ehkäisemiseksi, rikoshyödyn piilottamiseksi ja todistusaineiston vääristelemiseksi voivat osoittaa erityistä suunnitelmallisuutta. Hallituksen esityksessä on esimerkkinä erityisestä suunnitelmallisuudesta palvelunestohyökkäys.[96]

Jos teko kohdistuu sähköiseen viestintään, törkeää tietoliikenteen häirintää koskeva säännös syrjäyttää törkeän tietojärjestelmän häirinnän.[97] Liite 1:stä voidaan päätellä, että törkeästä tietojärjestelmän häirinnästä ei ole oikeuskäytäntöä.

5.4. Tietoliikenteen häirintä

Tietoliikenteen häirintä on ns. pääsäännös ja tietojärjestelmän häirintä ainoastaan täydentää sitä, kuten on todettu hallituksen esityksessä:

> Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua tietojärjestelmän häirintää lähinnä vastaavasta rikoksesta sisältyvät rikoslain tietoliikenteen häirintää koskevaan 38 luvun 5 §:ään.

Lain esitöiden mukaan säännös koskee postiliikennettä sekä televiestintää, että radioviestintää kokonaisuudessaan. Lisäksi on todettu säännöksen tarkoituksena olevan kaikenlainen sähköinen viestintä, riippumatta teknisestä toteutustavasta. Televerkko voi olla yleinen tai sisäinen verkko ja johdollinen tai langaton. Tietoliikenteen häirinnän tulee olla tahallista. Se voi olla fyysisesti tapahtuvaa esimerkiksi laitteen toimintaan vaikuttamista tai muunlaista häirintää tai estämistä. Soveltamisala on laaja koskien esimerkiksi postilaatikkojen rikkomisen ja televisiolähetyksen häirinnän. Säännös kattaa ainoastaan tele- ja radioviestinnän häirinnän eli viestien siirtämisen paikasta toiseen toisin sanoen tämän työn kannalta palvelunestohyökkäyksen osalta, säännös kattaa sellaiset teot, jotka kohdistuvat viestintään.[98]

Kannattaa kuitenkin huomata, että tietoliikenteen häirintä -säännös kohdistuu viestinnän loukkaamattomuuteen. ”Rikoslain tieto- ja viestintärikoksia koskevan

[96] HE 153/2006 vp. s. 66.
[97] HE 153/2006 vp. s. 66.
[98] HE 153/2006, s. 16–17.

38 luvun 5-7 § suojaavat tietoliikennettä. Näiden pykälien tunnusmerkistöt edellyttävät teleliikenteen häiritsemistä tai estämistä. Pykälien tarkoituksena ei ole suojata häiriösoitoilta tai muulta kiusalliselta tai ei-toivotulta viestinnältä, kuten tekstiviesteiltä, sähköpostilta tai telekopioilta."[99] Korkein oikeus on viitannut tähän omassa ratkaisussaan KKO 2008:86, joka liittyi häiritsevään tekstiviestien lähettämiseen.

Rikoslain 38 luvun 5 §:ssä on säädetty tietoliikenteen häirinnästä:

> Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Tietoliikenteen häirintä on törkeää, mikäli jokin alla oleva koventamisperuste täyttyy ja teko on myös kokonaisesti arvostellen törkeä. Perusteita on kaksi, rikoslain 38 luvun 6 §:ssä on säädetty törkeästä tietoliikenteen häirinnästä:

> Jos tietoliikenteen häirinnässä
>
> 1) rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa teletoimintalaissa tarkoitetun yleistä teletoimintaa, kaapelilähetystoiminnasta annetun lain (307/87) mukaista kaapelilähetystoimintaa tai yleisradiotoimintaa harjoittavan laitoksen palveluksessa tai muuta erityistä luottamusasemaansa taikka
>
> 2) rikoksella estetään tai häiritään hätäkutsujen radioviestintää tai muuta sellaista tele- tai radioviestintää, jota harjoitetaan ihmishengen turvaamiseksi,
>
> ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietoliikenteen häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.
>
> Yritys on rangaistava.

Jos tietoliikenteen häirintä aiheuttaa vakavaa vaaraa yhteiskunnan kriittiselle infrastruktuurille, kuten energiahuollolle, yleiselle terveydenhuollolle, maanpuolustukselle, oikeudenhoidolle tai rinnastettavalle, voidaan myös soveltaa rikoslain 34 luvun 1 §:n 2 momentin säännöstä tuhotyöstä.[100]

[99] LaVM 6/2000 vp – HE 184/1999 vp. s.3.
[100] HE 94/1993 vp. s.153.

Jos tietoliikenteen häirintä on tilapäistä ja melko harmitonta voidaan teosta tuomita ainoastaan sakkorangaistus. Tietoliikenteen häirinnän vähäisyyden arvioinnissa tulee kiinnittää huomiota aiheutetun häiriön laatuun tai määrään taikka muihin tekoon liittyviin seikkoihin. Teon tulee olla myös kokonaisuutena arvostellen vähäinen.[101] Rikoslain 38 luvun 7 §:ssä on säädetty lievästä tietoliikenteen häirinnästä, josta siis voidaan tuomita vain sakkoa:

> Jos tietoliikenteen häirintä, huomioon ottaen aiheutetun häiriön laatu tai määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä tietoliikenteen häirinnästä sakkoon.
>
> Yritys on rangaistava.

5.5. Direktiiviehdotus tietojärjestelmiin kohdistuvista hyökkäyksistä

5.5.1. Direktiiviehdotuksen tausta

Komissio julkaisi 14.7.2008 kertomuksen Euroopan unionin neuvoston puitepäätöksen tietojärjestelmiin kohdistuvista hyökkäyksistä täytäntöönpanosta. Raportissa todettiin että puitepäätöksen laatimisen jälkeen on noussut uusia uhkakuvia, koska Euroopassa on tehty tietoverkkohyökkäyksiä. Erityisesti raportissa viitattiin Viron tietojärjestelmiä vastaan tehtyyn palvelunestohyökkäykseen toukokuussa 2007. Uhkia tietojärjestelmille ovat raportin mukaan laajamittaiset, bottiverkkojen avulla suoritetut palvelunestohyökkäykset eli hajautetut palvelunestohyökkäykset. Raportissa komissio kertoo pohtivansa toimenpiteitä uuden uhan torjumiseksi, koska puitepäätöksessä ei ole tällaisia hyökkäyksiä otettu huomioon.[102] Kuten edellä mainitusta käy ilmi, puitepäätös on havaittu vallinaiseksi jo muutama vuosi säätämisensä jälkeen ja direktiiviehdotuksesta käy selvästi ilmi, että siinä keskitytään erityisesti törkeistä tekomuodoista annettujen rangaistusten koventamiseen.

5.5.2. Direktiiviehdotuksen sisältö

Direktiiviehdotus on pääpiirteissään aikaisemman puitepäätöksen mukainen, mutta sisältää tiettyjä muutoksia sekä lisäyksiä suhteessa Euroopan neuvoston yleissopimukseen, että

[101] HE 94/1993 vp. s.155.
[102] KOM (2008) 448 lopullinen, s. 1–2.

Euroopan unionin puitepäätökseen. Direktiiviehdotuksessa ei ole samanlaisia mahdollisuuksia rajoittaa säännöksien soveltamisalaa tai tehdä niihin varaumia kuin oli aikaisemmassa puitepäätöksessä. Lisäksi ehdotuksessa on aikaisempaa velvoittavampia säännöksiä jäsenvaltion viranomaisten välisestä tietojen vaihdosta. Uutta direktiivissä on myös hyökkäysten laajamittaisuuden huomioonottaminen ja hyökkääjän suorittama oman henkilöllisyyden salaaminen siten, että aiheutetaan vahinkoa henkilöllisyyden oikealle haltijalle. Tällaisia tunnusmerkkejä sisältävien tekomuotojen rangaistukset tulevat direktiiviehdotuksen perusteella ankaroitumaan.[103]

Direktiiviehdotuksen 9 artiklan mukaan jäsenvaltioiden olisi säädettävä 3-7 artiklassa olevista teoista rikosoikeudellinen enimmäisseuraamus, mikä olisi vähintään kaksi vuotta vankeutta. Ehdotettu enimmäisseuraamus on ankarampi kuin puitepäätöksessä määritetty yksi vuosi vankeutta.[104] Yleissopimuksen 13 artiklan ensimmäisessä johdantokappaleessa säädetään rangaistuksesta siten, että rangaistuksen tulee olla tehokas, oikeasuhtainen ja riittävä vapausrangaistus.[105] Edellä mainitut muutokset eivät tule toteutuessaan aiheuttamaan muutoksia tietojärjestelmän häirinnän rangaistusasteikkoon.

Direktiiviehdotuksen 10 artiklassa määritellään raskauttavat olosuhteet, joiden täyttyessä artikloissa 3-7 määriteltyjen tekojen yhteydessä, tulisi rikoksista säädettävän enimmäisseuraamuksen olla vähintään viisi vuotta vankeutta. Tällaisia raskauttavia olosuhteita ovat ehdotuksen 3-7 artikloissa määriteltyjen rikosten tekeminen: a) rikollisjärjestön puitteissa, b) käyttämällä välinettä, jonka tarkoituksena on käynnistää hyökkäyksiä, jotka vaikuttavat suureen määrään tietojärjestelmiä; c) aiheuttavat huomattavaa vahinkoa joko palvelujen keskeytyksinä, taloudellisina menetyksinä tai henkilötietojen menetyksinä. Edellä mainittu 10 artikla siten koskee sekä tämän työn kannalta merkityksellistä törkeää tietojärjestelmän häirintää, että törkeää viestintäsalaisuuden loukkausta, törkeää tietoliikenteen häirintää, törkeää tietomurtoa ja törkeää vahingontekoa. Suomen rikoslain säännöksiä tulee muuttaa tulevaisuudessa, jotta ne vastaisivat direktiiviehdotuksen sisältöä, mikäli ehdotus hyväksytään[106]. Tällä hetkellä törkeän tietojärjestelmän häirinnän rangaistusasteikko on 4 kuukautta – 4 vuotta vankeutta.

[103] Ehdotus EU:n direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä. Oikeusministeriö. 2012, s.2–3.
[104] U 50/2010 vp. s.3–4.
[105] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus. SopS 60/2007.
[106] U 50/2010 vp. s.4.

Lisäksi direktiiviehdotuksen 14 artiklaan on lisätty velvoite, jonka mukaan jäsenvaltioilla on oltava yhteyspisteet, joiden avulla valtiot voivat kaikkina viikonpäivinä, ympärivuorokautisesti, kahdeksan tunnin sisällä, vastata kiireellisiin pyyntöihin. Vastauksesta olisi ilmettävä vastataanko avunpyyntöön ja missä muodossa ja milloin. Suomessa tämä säännös ei aiheuttaisi muutoksia, yhteyspisteenä toimii keskusrikospoliisi.[107] Ehdotuksen 14 artiklan säännös nopeuttaisi ja tehostaisi esitutkintaa jäsenvaltioiden alueella tapahtuvissa tietoverkkorikoksissa. Valtioneuvoston mukaan rangaistusarvon sekä rangaistusasteikkojen olisi oltava oikeassa suhteessa haluttuun tavoitteeseen, että rikoksen vakavuuteen. Lisäksi valtioneuvosto on sitä mieltä, että kansainvälisen viranomaisyhteistyön tehostaminen toimii rikosten ennaltaehkäisyssä paremmin kuin rangaistusasteikkojen koventaminen.[108]

Direktiiviehdotuksessa korostetaan erityisesti laajoja bottiverkkoja käyttämällä tehtyjen rikosten rangaistusasteikkojen korottamista. Rangaistusten korottamisen perusteluina oli tekojen suuri uhka vapaalle tietojenkäsittelylle koko Euroopan alueella.

Direktiiviehdotuksessa perustellaan jäsenvaltiotasoisten toimien olevan riittämättömiä, koska tietoverkkorikollisuudella on rajat ylittävä ulottuvuus erityisesti laajoissa hyökkäyksissä, jotka jakaantuvat usein eri paikkoihin ja eri maihin. Ehdotuksen tavoitteet saavutetaan parhaiten Euroopan unionin laajuisilla toimilla useasta syystä: 1. rikoksentekijöiden muuttaminen toisiin lievemmän tietoverkkohyökkäyksiä koskevan lainsäädännön maihin estyy, 2. yhteisten määritelmien pohjalta tietojen vaihto, keräys ja vertaaminen mahdollistuvat, 3. tekojen torjunta EU:ssa tehostuu ja kansainvälinen yhteistyö tiivistyy.[109] Puitepäätöksessä ei oteta riittävästi huomioon laajamittaisesta hyökkäyksestä aiheutuvaa uhkaa, rikosten vakavuutta ja niistä langetettavia rangaistuksia.[110]

5.5.3. Laillisuusperiaate

Direktiiviehdotuksen myötä mahdollisesti tulevat, tämän työn kannalta mielenkiintoisimmat asiat ovat näkemykseni mukaan lainsäädäntötekniset. Lissabonin sopimuksen myötä päätökset toteutetaan direktiivein. Direktiivin soveltamisen osa-alueena

[107] U 50/2010 vp. s.4–5.
[108] U 50/2010 vp. s.5–6.
[109] KOM(2010) 517 lopullinen, s.9.
[110] KOM(2010) 517 lopullinen, s. 5.

ovat sen välitön sovellettavuus ja välitön oikeusvaikutus, joihin liittyy läheisesti yhteisöoikeuden etusija eli yhteisöoikeudellinen etusijaperiaate. Etusijaperiaate ja sen syntyhistoria on näkemykseni mukaan erittäin tärkeä valitsemani aiheen kannalta, tätä tukee myös Rosas:

> Yhteisöoikeuden etusija kansalliseen oikeuteen nähden on tietenkin omiaan korostamaan suoran sovellettavuuden ja välittömän oikeusvaikutuksen merkitystä. Yhteisön oikeuden kannalta etusijaperiaate kattaa kaikki kansallisen oikeuden normit, kansallinen perustuslaki mukaan lukien.[111]

EU-säännösten suoraa sovellettavuutta kuitenkin rajaa rikosoikeudellinen laillisuusperiaate. Suomi sitoutui 1976 YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskevaan yleissopimukseen, jonka 15 artiklassa säännellään laillisuusperiaate. Vuonna 1990 Suomi liittyi Euroopan neuvoston yleissopimukseen ihmisoikeuksien ja perusvapauksien suojaamiseksi, jonka laillisuussäännöt sisältyvät 7 artiklaan. Lisäksi laillisuusperiaatteesta säädetään sekä perustuslain 8 §:ssä, että EU:n perusoikeuskirjan 49 artiklassa.[112] EY-tuomioistuin on täsmentänyt direktiivien välittömän oikeusvaikutuksen laajuutta nimenomaan laillisuusperiaatetta soveltamalla. Direktiiveistä ei voi kansallisesta oikeudesta riippumatta seurata rikosoikeudellista vastuuta tai rikosoikeudellista vastuuta ankaroittavaa vaikutusta. EY-tuomioistuimen mukaan laillisuusperiaatteen sisältöön kuuluu, että suoraan puitepäätöksen tai direktiivin perusteella, niiden määräyksiä rikkoneen henkilön rikosoikeudellista vastuuta ei voi ankaroittaa tai perustaa suoraan direktiiviin tai puitepäätökseen. Tulkintavaikutusta rajoittavat EY-tuomioistuimen mukaan erityisesti oikeusvarmuuden ja taannehtivuuskiellon periaatteet.[113]. Puitepäätöksen osalta välitön oikeusvaikutus on suljettu pois jo EU-sopimuksessa(EU 34 artiklan 2 kohta, siinä muodossa kuin sopimus on Amsterdamin sopimuksella muutettuna). Myös Melanderin mukaan laillisuusperiaate toimii tulkintavaikutuksen tärkeimpänä rajoituksena.[114]

Rangaistavaa on vain rangaistavaksi säädetty, joten tietotekniikan ja käyttöön liittyviä tekoja ei ole ollut aina mahdollista katsoa rikoksiksi.[115] Eli rikosoikeudellisissa asioissa EU tuomioistuimen mahdollisuus yhtenäistää kansallisien oikeuksien tulkintalinjoja tulee olemaan vähäinen, ilman EU:n jatkuvaa työtä lainsäädännön pitämiseksi ajantasaisena.

[111] Rosas 2009, s.547.
[112] Frände et al. 2012, s.28–29.
[113] C-105/03, Pupino, kohdat 44–45.
[114] Melander 2010, s.62.
[115] Saarenpää 2011, s.537.

Kansallinen tuomioistuin on mahdollista ottaa huomioon syytetyn eduksi puitepäätökseen liittyvä tulkintavaikutus tai tulevaisuudessa direktiivin välitön vaikutus. Erityisen tärkeä on huomata, että laillisuusperiaate pätee vain meneteltäessä epäillyn vahingoksi.[116]

5.6. Direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä

Euroopan parlamentti ja neuvosto ovat antaneet 12.8.2013 direktiivin 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä ja edellisen neuvoston puitepäätöksen 2005/222/YOS korvaamisesta. Direktiivin johdantokappaleen 1 kohdassa on todettu direktiivin tavoitteeksi lähentää jäsenvaltioiden tietojärjestelmiin kohdistuvia hyökkäyksiä koskevaa rikoslainsäädäntöä. Direktiivin johdantokappaleen kohdassa kolme on todettu tietoverkkohyökkäysten uhkaavan vapauteen, turvallisuuteen ja oikeuteen perustuvan tietoyhteiskunnan toteuttamista.

Kohdassa viisi on todettu, että on olemassa todisteita entistä vaarallisemmista laajamittaisista tietojärjestelmähyökkäyksistä jäsenvaltioiden ja yksityissektorin elintärkeisiin tietojärjestelmiin. Hyökkäyksiin liittyvät bottiverkkojen luominen, mikä sisältää eri vaiheita, joista jokainen yksin voi olla vakava riski yleiselle edulle.

Kohta 13 on tämän aiheen kannalta erittäin mielenkiintoinen ja rikosoikeuden kansainvälistymisen näkökulmasta myös erityisen ajankohtainen. Siinä on todettu olevan tarkoituksenmukaista säätää ankarammista seuraamuksista, kun tietojärjestelmään kohdistuvan hyökkäyksen on toteuttanut rikollisjärjestö[117] sekä verkkohyökkäys on laajamittainen, että vaikuttaa merkittävään määrään tietojärjestelmiä.[118] Kohdassa on myös todettu olevan tarkoituksenmukaista säätää ankarammista seuraamuksista silloin, kun hyökkäys on kohdistunut jäsenvaltioiden tai unionin tärkeään infrastruktuuriin. Direktiivin 9 artiklassa on säädetty. että törkeän tekomuodon rangaistuksen enimmäiskeston on oltava vähintään viisi vuotta, kun teko on tehty rikollisjärjestön puitteissa, aiheuttaa vakavaa vahinkoa tai kohdistuu elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään.

---

[116] Frände et al. 2010, s.46.

[117] Rikollisjärjestö on määritelty kohdan 13 mukaan puitepäätöksessä 2008/841/YOS. Puitepäätökseen liittyy valiokunnan lausunto EUVL L 300, s.42.

[118] Tietojärjestelmien määrä on merkittävä, kun a) hyökkäyksen tarkoituksena on luoda bottiverkko, b) verkkohyökkäys aiheuttaa vakavaa vahinkoa tai c) hyökkäys toteutetaan bottiverkon avulla.

Direktiivin kohdan 16 mukaan direktiivissä viitataan tietoverkkorikosvälineisiin, joita voivat olla erilaiset haittaohjelmat, kuten ohjelmat bottiverkkojen luomiseksi. Kuitenkin on mahdollista, että edellä mainittu väline on tarkoitettu laillisia tarkoituksia varten, joten mikäli väline on valmistettu laillista tarkoitusta varten, kuten tietotekniikkatuotteiden luotettavuuden ja tietojärjestelmien turvallisuuden testaamista varten, on kriminalisointia vältettävä ja yleisen tahallisuusedellytyksen lisäksi on edellytettävä myös välitöntä tahallisuutta direktiivissä mainitun rikoksen tekemisessä.

Kohdassa 17 on todettu, että direktiivissä ei määrätä rikosoikeudellisesta vastuusta objektiivisten kriteerien täyttyessä ilman tahallisuutta. Esimerkkeinä on todettu teko, jossa henkilöllä ei ole ollut lupaa tekoon, mutta hän ei ole ollut tietoinen luvan puuttumisesta tai kun on kysymys tietojärjestelmien luvallisesta testauksesta tai suojauksesta.

Kohdan 22 mukaan direktiivillä vahvistetaan ympärivuorokautisen ja kaikkina viikonpäivinä toimivan yhteyspisteverkoston merkitystä. Suomessa nämä yhteyspisteet ovat olleet toiminnassa jo pitkään.

Kohdassa 26 on todettu olevan jäsenvaltioiden velvollisuus vahvistaa elintärkeiden infrastruktuurien kestävyyttä verkkohyökkäyksiä vastaan ja se on kohdan mukaan myös tehokkaan tietoverkkorikollisuuden torjunnan edellytys.

Kohdan 27 mukaan puutteet ja eroavuudet jäsenvaltioiden lainsäädännöissä ja rikosoikeudellisissa menettelyissä tietojärjestelmiin kohdistuvien hyökkäysten osalta saattavat vaikeuttaa järjestäytyneen rikollisuuden ja terrorismin torjuntaa sekä tehokasta poliisi- ja oikeudellista yhteistyötä. Nykyaikaisilla tietojärjestelmillä on rajat ylittävä ulottuvuus, mikä korostaa tarvetta lähentää jäsenvaltioiden rikosoikeutta tällä alalla. Rikosoikeudenkäyntejä koskevien toimivaltaristiriitojen ehkäisemisestä ja ratkaisemisesta annetun neuvoston puitepäätöksen 2009/948/YOS asianmukaisen täytäntöönpanon ja soveltamisen pitäisi helpottaa syytetoimien yhteensovittamisessa.

Direktiivin 4 artiklassa on säädetty laittomasta järjestelmän häirinnästä:

> Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tietojärjestelmän toiminnan vakava estäminen tai keskeyttäminen tahallisesti ja oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla taikka saattamalla data

käyttökelvottomaksi on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

Direktiivin 9 artiklassa on todettu vankeusrangaistuksista seuraavaa:

> 3. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 4 ja 5 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään kolme vuotta, kun ne on tehty tahallisesti ja kun on vaikutettu merkittävään määrään tietojärjestelmiä käyttämällä 7 artiklassa tarkoitettua välinettä, joka on suunniteltu tai muutettu ensisijaisesti tätä tarkoitusta varten.

> 4. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 4 ja 5 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään viisi vuotta, kun
>
> a) ne on tehty rikollisjärjestön puitteissa, sellaisena kuin se on määritelty puitepäätöksessä 2008/841/YOS, riippumatta siitä, mikä on siinä säädetty seuraamus;
>
> b) ne aiheuttavat vakavaa vahinkoa; tai
>
> c) ne kohdistuvat elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään.

16 artiklan mukaan jäsenvaltioiden on saatettava kansalliset lainsäädännöt direktiivin mukaisesti viimeistään 4.9.2015.

6. SOVELTAMISKYSYMYKSET

Tässä kappaleessa on esitelty muutamia oikeustapauksia, joissa on annettu langettava tuomio joko tietoliikenteen häirinnästä tai tietojärjestelmän häirinnästä. Erityisesti tietojärjestelmän häirinnästä annettujen langettavien tuomioiden lukumäärä on vähäinen, johtuen tietotekniikan avulla tehtävien rikosten moniulotteisuudesta ja tietojärjestelmän häirinnän toissijaisuudesta suhteessa muihin tekomuotoihin. Johtuen tietotekniikkarikosten moniulotteisuudesta useimmissa oikeustapauksissa syytekohtia on ollut useampia kuin yksi tai kaksi. Tietoliikenteen häirintä ja tietojärjestelmän häirintä -tapauksissa on tekijä useasti syyllistynyt monet muutkin tunnusmerkistöt täyttäviin tekoihin, kuten tietomurtoon, kunnianloukkaukseen, luvattomaan käyttöön ja tietoverkkorikosvälineen hallussapitoon. Tapaukset esitellään ainoastaan tämän työn kannalta relevantin sisällön osalta, osapuolten henkilötiedot poistettuna.

Luvun lopussa on kaksi kappaletta koskien syyteoikeutta ja esitutkinnan rajoittamista. Käsittelen ne lyhyesti tässä yhteydessä, koska erityisesti tietotekniikkarikosten syyteharkinta on erityistä asiantuntemusta vaativaa.

6.1. Tapaus 1

Varsinais-Suomen käräjäoikeus antoi 4.3.2011 tuomion 11/1235 muun muassa vaaran aiheuttamista tietojenkäsittelylle koskevassa asiassa R 10/3229. Tässä tuomiossa on mielenkiintoista se, että tuomiossa on sovellettu aikaisemmin voimassa ollutta lakia ja/tai säännöksiä, koska teko on tehty aikaisemman lain voimassaoloaikana, eikä uusi laki ole lievempi. Lisäksi tapauksessa oli koventamisperusteen soveltuvuuden arviointia. Tämän tapauksen perustelut ovat yhä käytettävissä nykypäivän tuomioissa, koska tällä hetkellä voimassaolevan lain, hallituksen esityksen perusteluissa on käytetty viittauksia aikaisemman lain hallituksen esitykseen.

6.1.1. Teko ja syytekohdat

Syyttäjä vaati vastaajalle rangaistusta 1.vaaran aiheuttamisesta tietojenkäsittelylle rikoslain 34 luvun 9 a § 1 momentti(14.10.1999/951) ja 2.tietoliikenteen häirinnästä rikoslain 38 luvun 5 §. Syyttäjän muita vaatimuksia oli koventamisperuste rikoslain 6 luvun

5§:n(2003/515) perusteella, rikoksentekovälineiden menettäminen sekä oikeudenkäynnin kohteen olevan rikokseen läheisesti liittyvät esineet, jotka ovat yksinomaan tai pääasiallisesti tahallista rikosta varten hankittu tai valmistettu taikka ominaisuuksiltaan erityisen soveltuvia tahallisen rikoksen tekemiseen.

Syyttäjän 2. syytevaatimuskohdan mukaan vastaaja on 5.1.2005 – 24.2.2007 yhdessä tuntemattomaksi jääneiden henkilöiden kanssa lähettämällä ilkivaltaisessa tarkoituksessa televerkossa häiritseviä viestejä ja muulla tavalla oikeudettomasti estänyt tai häirinnyt lukuisien tuntemattomaksi jääneiden yritysten, yhteisöjen ja yksityisten henkilöiden palvelimien ja tietokoneiden televiestintää siten, että vastaaja on tunkeuduttuaan haittaohjelmien avulla saastutettuihin koneisiin, käyttänyt luvatta tuhansia tietokoneita ja palvelimia ympäri maailmaa muodostamalla niin sanottuja bot-verkkoja, joita on ohjattu vastaajan ja tuntemattomaksi jääneiden henkilöiden ylläpitämien kontrollikanavien kautta antamalla koneille erilaisia liittymis-, uudelleenohjaus, palvelunestohyökkäys ja skannaus- ja saastutuskomentoja, jotka ovat kohdistuneet useisiin yritysten, yhteisöjen tai henkilöiden palvelimiin tai tietokoneisiin. Palvelunestohyökkäyksillä ja skannaus- ja saastutuskomennoilla on estetty tai hidastettu kohteena olleiden tietokoneiden toimintaa.

Vastaajan toimesta on annettu ainakin 102 palvelunestohyökkäyskomentoa ja 2.553 skannaus- tai saastutuskomentoa. Lisäksi vastaajan ollessa seuraamassa bot-verkon hallintakanavien liikennettä on muiden tuntemattomien henkilöiden kautta annettu useita palvelunestohyökkäys ja skannaus- tai saastutuskomentoja.

6.1.2. Vastaajan vastaus

Vastaajan mukaan hänen toimintansa on alkanut ajattelemattomuudesta. Toiminta ei ole hänen mukaansa ollut millään lailla suunnitelmallista tai järjestäytynyttä, vaan melko lapsellista kilpailua. Toiminnan aiheuttama vaara ja uhka olivat hyvin rajattua. Toiminnan avulla ei luotu bot-verkkoja, joilla olisi voitu kaapata tietokoneita, urkkia tietoja, vahingoittaa tiedostoja tai ohjelmia tai aiheuttaa taloudellista vahinkoa ulkopuolisille.

Vastaaja on vastauksessaan myöntänyt kohdan 1 teon, mutta kiistänyt teonkuvauksen osittain. Vastaajan mukaan ohjelmien valmistaminen hänen koneellaan on tapahtunut pääosin muiden toimesta ja ohjein. Vastaajan mukaan toiminta vaaransi rajoitetusti tietojenkäsittelyä tai tietojärjestelmien toimintaa, eikä haittaohjelmien avulla voitu

vahingoittaa tietoja tai ohjelmistoja. Vastaajan mukaan syytteessä on esitetty toiminta lukujen valossa suurempana kuin se on ollut. Haittaohjelmat ovat olleet muutaman perusohjelman muunnoksia, joten haittaohjelmia ei ole teonkuvauksessa lueteltua määrää, 129 uutta haittaohjelmaa. Vastaajan mukaan teknisessä tutkinnassa ei ole voitu luotettavasti selvittää uniikkien IP-osoitteiden määrää ja lisäksi haittaohjelmia ei ole levitetty teonkuvauksessa lueteltua määrää, koska esitutkinnassa on päätelty access.log -kirjauksista, kuinka monta onnistunutta latausta on tapahtunut. Suurin osa onnistuneista latauspyynnöistä on olemassa olevien bottien latausilmoituksia. Vastaajan vastauksen mukaan erilaiset bottien ohjaustoimenpiteet edellyttivät uuden .exe -tiedoston lataamisen ja vanhan poistamisen. Lataukset epäonnistuivat useasti, joka aiheutti aina uuden merkinnän lokiin.

Vastaaja kiisti kohdan 2 teon kokonaan ja teonkuvauksen osittain. Rikoksentekohetken mukaisessa rikoslain 38 luvun 5 §:ssä teon tunnusmerkistön olennainen osa oli viestinnän häiritseminen joko fyysisesti puuttumalla tai itse lähettämällä häiritseviä viestejä. Vastaajan vastauksen mukaan palvelunestohyökkäykset ovat tapahtuneet dataa syöttämällä. Kohteena ovat olleet tietojärjestelmät, ei tietoliikenne, ja tekotapana datan syöttö, ei häiritsevä viestintä. Syytteessä ei ole esitetty näyttöä tietoliikenteen häirinnästä tai häiritsevästä viestinnästä, joten teko ei vastaajan mukaan täytä lainkohdan tunnusmerkistöä. Vastaajan mukaan hänen kantaansa tukee myöhempi tietojärjestelmän häirinnän kriminalisointi.

Vastaaja ei missään vaiheessa hallinnoinut tuhansista tietokoneista muodostunutta bot-verkkoa, vaan toimivia botteja oli enimmillään noin 300 kappaletta. Riittävästi tekemään DDoS -hyökkäys yhtä tai kahta kotitietokonetta vastaan. Saastutusohjelmien ominaisuuksista johtuen yksittäinen botti pystyi ottamaan vastaan ainoastaan DDoS -hyökkäyskäskyjä.

6.1.3. Tuomion perustelut tietoliikenteen häirinnän osalta

Vastaaja on kiistänyt syytteen tietoliikenteen häirinnästä lähinnä oikeudellisella perusteella, hänen mukaansa toiminta ei täytä tietojärjestelmän häirinnän tunnusmerkistöä. Teon aikana voimassaolevan lain esitöiden mukaan, HE 94/1993 s.153–154, rangaistava häirintä voi tapahtua puuttumalla tietoliikenteessä käytetyn laitteen toimintaan fyysisesti tai sanomien lähettämistä tai vastaanottamista muulla tavoin vaikeuttamalla. Tekijän tulee mieltää, että hän estää tai häiritsee viestintää.

Tutkijana toimineen todistajan mukaan DDoS -hyökkäyksessä dataa voi kulkea useiden operaattoreiden verkkojen läpi, syöden kaistatilaa muilta käyttäjiltä. Esitetyn selvityksen mukaan vastaajan hyökkäykset ovat kohdistuneet myös palvelimiin ja ovat siten ainakin välillisesti häirinneet tietoliikennettä. Vastaaja on siten myös syyllistynyt tietoliikenteen häirintään.

6.1.4. Muut syytekohdat lyhyesti

Tuomiossa on todettu, että rikoslain 3 luvun 2 §:n mukaan rikokseen sovelletaan lakia, joka oli voimassa rikosta tehtäessä. Jos voimassaoleva laki johtaa lievempään lopputulokseen, sovelletaan sitä. Tuomion mukaan sekä vanhassa, että uudessa laissa rangaistusasteikko on sakkoa tai vankeutta enintään kaksi vuotta, joten käräjäoikeus on katsonut ettei uusi laki johda lievempään lopputulokseen.

Perusteluiden mukaan rikoslain 34 luvun 9 a § (951/1999) kriminalisoi tietokoneviruksen valmistamisen, saataville asettamisen ja levittämisen. Rangaistavuus ei edellytä, että teosta tosiasiallisesti aiheutuisi konkreettista haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle tai että järjestelmän sisältämät tieto tai ohjelmistot vahingoittuisivat. Riittävää olisi, että ohjelma tai ohjelmakäskyjen sarja on suunniteltu aiheuttamaan vahinkoa(HE 4/1999 s.8).

Tuomioistuin on todennut, että vastaajan toiminta lähti liikkeelle siitä, kun häntä vastaan tehtiin DDoS -hyökkäyksiä. Hän oli osa peliporukkaa, joka antoi neuvoja, kyseessä ei kuitenkaan ollut mikään järjestäytynyt ryhmä. Hän ei tavoitellut taloudellista hyötyä. Poliisin päätutkija on todennut oikeudenkäynnissä todistajan asemassa seuraavaa: 1. bot-verkon koko vaihtelee yksittäisten koneiden pudotessa pois ja liittyessä uudelleen myöhemmin, 2. Jos hyökkäykseen osallistuu satoja botteja se kaataa pienen verkon, 3. ei ole näyttöä siitä, että epäilty olisi saanut toiminnastaan taloudellista hyötyä, 4. Albateam koostui muutamista henkilöistä, mutta ei voida puhua järjestäytyneestä toiminnasta, 5. Vastaaja on kiistänyt teonkuvauksen toiminnan laajuuden suhteen, mutta sen selvittämistä on vaikeuttanut se, että toimijat ovat luovuttaneet toisilleen käyttöoikeuksia, jolloin ei voida aina tietää kuka on ollut todellinen toimija, tällöin on kuitenkin kysymys yhdessä toimimisesta, kun toiselle on sallittu tällainen toiminta, vastaaja vastaa toiminnasta omalla palvelimellaan, 6. vastaaja on kiistänyt internetsivuston olevan hänen ylläpitämä, kuitenkin

eräs nimimerkki on voitu yhdistää vastaajaan tietoteknisessä tutkinnassa, 7. vastaaja on kiistänyt syyttäjän näkemyksen haittaohjelmien lukumäärästä, mutta haittaohjelmia muokataan juuri sen takia, että virustorjunta ei pysyisi perässä. Käräjäoikeuden mielestä ei ole väärin sanoa ohjelmaa uudeksi, vaikka siihen olisi tehty vain vähäisiä muutoksia. Eri asia on että kokonaan uuden ohjelman luominen on huomattavasti työläämpää, mikä voi jossain määrin vaikuttaa tekijän teon moitittavuuden arviointiin. Vastaaja on kiistänyt uniikkien IP-osoitteiden määrän, mutta todistajan mukaan uniikkien IP-osoitteiden määrä on ollut vähintään syytteessä ilmoitettu määrä, tältäkin osin on toimittu epäilty-ystävällisesti, nykyisin laajakaistaa käytettäessä IP-osoite ei juuri muutu vaan on kiinteä ja palvelintietokoneet lähes kaikki käyttävät kiinteää IP-osoitetta. Todistaja on todennut olevan vaikeaa selvittää uniikkien IP-osoitteiden tarkka määrä ja näin suuressa määrässä voi olla osoitteiden vaihtumisia, mutta haittaohjelmia on tosiasiallisesti levitetty useampaankin uniikkiin osoitteeseen, mutta mukaan on otettu vain ne haittaohjelmat joihin on kohdistunut yli 10 latauspyyntöä. Käräjäoikeus on todennut, että uniikkien IP-osoitteiden määrä ei ole ylimitoitettu.

Vastaaja on myös kiistänyt haittaohjelmien latausten lukumäärät, koska latauksia on toistettu epäonnistumisten vuoksi. Todistajan mukaan tutkinnassa on otettu huomioon vain lataukset, joihin on vastattu onnistuneesti ja ohjelma on lähtenyt koneesta. Latauspyyntöjä oli paljon enemmän sekä useampikertaiset IP-osoitteet on suodatettu pois, että laskelmissa eivät ole ne lataukset, joita on ollut vain 1-9 kappaletta. Todistajan mukaan asiassa on toimittu tältäkin osin hyvin epäilty-ystävällisesti. Käräjäoikeus katsoo, että vastaaja on menetellyt syytteessä kuvatulla tavalla ja syyllistynyt vaaran aiheuttamiseen tietojenkäsittelylle.

6.1.5. Muut syyttäjän vaatimukset

Syyttäjä on vaatinut koventamisperusteen soveltamista, koska toiminta on ollut suunnitelmallista ja rikos on kohdistunut kansalliset, rodulliseen, etniseen tai muuhun sellaiseen kansanryhmään kuuluvaan, tähän ryhmään kuulumisen johdosta.

Rikoslain 6 luvun 5 §:n mukaan koventamisperusteena on toiminnan suunnitelmallisuus. Lain esitöiden HE 44/2002 s. 191 tämän mittaamisperusteen kynnys riippuu rikostyypistä, jos tunnusmerkistö edellyttää jo itsessään jonkinasteista suunnittelua, suunnitelmallisuuden tulee olla voimaperäisempää kuin rikoslajiin säännönmukaisesti kuuluvan harkinnan.

Tuomioistuimen mukaan vastaaja on nähnyt paljon vaivaa, jotta on oppinut toimimaan syytteessä kuvatulla tavalla. Toiminta ei ole kuitenkaan ollut erityisen suunnitelmallista verrattuna siihen, mitä tällaisiin rikoksiin syyllistyminen normaalistikin vaatii. Toiminnalla ei ole ollut selkeää päämäärää, se ei ole perustunut selkeään suunnitelmaan, joten käräjäoikeus ei katsonut asiassa olevan perusteita soveltaa erityistä koventamisperustetta suunnitelmallisuuteen liittyen.

Vastaaja on tunnustanut palvelunestohyökkäyksensä kohdistuneen serbejä vastaan, mutta tuomioistuin on todennut lain esitöissä HE 44/2002 s.192 todetun, että säännöksen tarkoituksena on ennen kaikkea suojata kansallisia, rodullisia ja etnisiä vähemmistöjä rotuvihaan perustuvaa niin sanottua rasistista väkivaltaa vastaan, tarkoituksena on antaa suojaa niitä rikoksia vastaan, joiden alkusyy ja tekijän motiivi liittyy uhrin ominaisuuteen tietyn kansanryhmän jäsenenä, tämä koventamisperuste kattaa periaatteessa kaikki rikostyypit. Luontevin soveltamisala rajoittuu väkivaltarikoksiin sekä rikoksiin joilla vaarannetaan vähemmistöön kuuluvien ihmisten turvallisuutta tai toimeentulo- tai elinkeinomahdollisuuksia. Palvelunestohyökkäyksiä on tehty puolin ja toisin, kysymys on ollut tiettyjen ryhmien välisestä vihanpidosta tietoverkoissa. Tuomioistuimen mukaan toiminnan kansainvälisen ulottuvuuden vuoksi kohdehenkilö ei välttämättä ole asuinmaassaan vähemmistön asemassa. Edellä mainitun vuoksi ei ole perusteita soveltaa koventamisperustetta.

Käräjäoikeus on todennut lopuksi, että ottaen huomioon teon vahingollisuus ja vaarallisuus sakko ei ole riittävä rangaistus. Vastaajaa ei ole aikaisemmin tuomittu vankeuteen. Vankeusrangaistus tuomitaan ehdollisena. Ehdollinen rangaistus on yksinään riittämätön, joten ohessa tuomitaan sakkoa.

6.1.6. Tuomiolauselma

Vastaajan syyksi on luettu vaaran aiheuttaminen tietojenkäsittelylle ja tietoliikenteen häirintä. Rangaistusseuraamukseksi määrättiin 8 kuukautta ehdollista vankeutta, josta tehtiin rikoslain 6 luvun 13 §:n nojalla 2 päivää vähennystä. Ehdollisen vankeusrangaistuksen ohessa tuomittiin 50 päiväsakkoa. Lainkohtina oli edellisen lain 34 luvun 9 a § (951/1999) ja rikoslain 38 luvun 5 §.

Vastaajan rikoksentekovälineenä käyttämät tietokone, keskusyksikkö ja kolme levyasemaa on tuomittu valtiolle menetetyksi rikoslain 10 luvun 4 §:n 2 momentin perusteella.

6.2. Tapaus 2

Otin tämän tapauksen esimerkiksi tietoliikenteen häirinnän monimuotoisuudesta. Eli tietoliikenteen häirintä voi olla suoritettu tietokonetta hyväksikäyttäen tai jollain muilla keinoin, säännös ei ole riippuvainen tekotavasta, vaan aikaansaadusta seurauksesta ja tahallisuudesta. Helsingin käräjäoikeus on antanut 8.12.2006 tuomion 06/12059 muun muassa tietoliikenteen häirintää koskevassa asiassa R 06/8598.

6.2.1. Teko ja syytekohdat

Syyttäjä vaati vastaajalle rangaistusta 1. kotirauhan rikkomisesta, 2. kunnianloukkauksesta ja 3. tietoliikenteen häirinnästä. Asianomistaja yhtyi syyttäjän rangaistusvaatimukseen, vaati vahingonkorvausta henkisen kärsimyksen johdosta yhteensä 2600 euroa korkoineen sekä vastaajan määräämistä perusmuotoiseen lähestymiskieltoon että vastaajan velvoittamista korvaamaan oikeudenkäyntikulunsa viivästyskorkoineen.

Syyttäjän syytekohdan 3 mukaan vastaaja on oikeudettomasti tahallaan häirinnyt televiestintää 20.5.2004 – 23.7.2006, lähettelemällä asianomistajalle useita tekstiviestejä sekä soittelemalla useita häiritseviä puheluita ilkivaltaisessa tarkoituksessa päivä- ja yöaikaan aiheuttaen sen, ettei asianomistaja ole voinut käyttää liittymäänsä haluamallaan tavalla.

6.2.2. Vastaajan vastaus

Vastaaja on kiistänyt syyllistyneensä asiassa rikokseen. Syytekohdissa 1 ja 2 vastaaja on myöntänyt teonkuvaukset, mutta hänen tarkoituksenaan ei ole ollut häiritä asianomistajan kotirauhaa eikä halventaa asianomistajaa. Syytekohdan 3 osalta vastaaja on katsonut, ettei soittelu ja tekstiviestien lähettäminen ole häirinnyt asianomistajaa siten, että liittymän käyttö olisi estynyt.

Vastaaja on kiistänyt asianomistajan korvausvaatimuksen perusteeltaan, mutta myöntänyt määrällisesti oikeaksi korkeintaan 500 euroa. Vastaaja on katsonut, ettei ole perusteita lähestymiskiellon määräämiselle.

6.2.3. Tuomion perustelut tietoliikenteen häirinnän osalta

Käräjäoikeus on katsonut todistajien ja vastaajan oman kertomuksen perusteella näytetyksi, että vastaajan soittelu asianomistajalle on ollut ajoittain erittäin intensiivistä, jopa kymmeniä päivässä. Käräjäoikeus pitää uskottava, että soittelu on häirinnyt asianomistajan matkapuhelimen käyttöä, niin ettei hän ole voinut käyttää sitä haluamallaan tavalla. Soittelu ei ole ollut oikeutettua vaan tarkoituksellista häirintää.

Käräjäoikeus on katsonut vastaajan syyttäjän teonkuvauksessa kuvatulla tavalla oikeudettomasti häirinneen televiestintää soittelemalla useita häiritseviä puheluita ilkivaltaisessa tarkoituksessa päiväaikaan. Käräjäoikeuden mukaan näyttämättä on jäänyt, että soittelua olisi tapahtunut myös yöaikaan. Käräjäoikeuden mukaan tekstiviestien lähettäminen ei ole häirinnyt siinä määrin asianomistajan matkapuhelimen käyttöä, että menettelyn voisi tältä osin lukea syyksi tietoliikenteen häirintänä, johtuen siitä, että epätoivotut viestit voi puhelimen muistista helposti poistaa ennen muistin täyttymistä, eivätkä viestit ole siten häirinneet muiden viestien vastaanottamista.

6.2.4. Muut syytekohdat lyhyesti

Käräjäoikeus on katsonut, että todisteet tukevat käsitystä vastaajan asianomistajaan kohdistamasta pitkäaikaisesta yhteydenpidosta ja yhteydenpitoyrityksistä. Tuomioistuin on katsonut todistajan kertomusten perusteella yhteydenpidon ahdistavana ja häiritsevänä. Käräjäoikeus on katsonut vastaajan asianomistajaan kohdistaman soittelun ja tekstiviestien lähettelyn jatkuvuudeltaan, intensiivisyydeltään ja tyyliltään sellaiseksi, että kysymys ei ole enää normaalista yhteydenpidosta vaan puhelinhäirinnästä. Tuomioistuimen mukaan huolimatta siitä, että asianomistaja on pitänyt yhteyttä vastaajaan, yhteydenpito ei ole ollut vastavuoroista tai yhteismitallista ja yhteydenotot ovat usein olleet reaktioita vastaajan häirintään.

Tuomioistuimen mukaan kotirauhan rikkomisena on säädetty rangaistavaksi muun muassa oikeudettomasti kotirauhan rikkominen soittamalla puheluita tai muulla vastaavalla tavalla.

Vastaajan yhteydenpito on ollut oikeudetonta, koska se on tapahtunut häirintätarkoituksessa ja kielloista huolimatta. Häirintää on tapahtunut niin kotona kuin töissä. Koti on kotirauhan suojaamaa aluetta, töissä tai muussa paikassa, joka ei ole kotirauhan suojaama, menettely ei voi olla kotirauhan rikkomisena rangaistava. Käräjäoikeus on katsonut selvitetyksi vastaajan toimineen syytteessä kohdassa 1 kuvatulla tavalla, mutta katsoi näyttämättä jääneen, että kotirauhaa olisi rikottu myös yöllisellä yhteydenpidolla.

Käräjäoikeus on katsonut selvitetyn, että vastaaja on syytekohdan 2, teonkuvauksessa kuvatulla tavalla loukannut vastaajan kunniaa. Vastaajan asianomistajalle lähettämät tekstiviestien sisältö on ollut loukkaavaa ja halventavaa. Käytetyt ilmaisut ovat olleet käräjäoikeuden mukaan alatyylisiä, törkeitä ja asiattomia.

Tuomioistuin on katsonut sopivaksi sovitella yksityisoikeudellista korvausvelvollisuutta vahingonkorvauslain 6 luvun 1 §:n perusteella, koska asianomistaja on provosoinut ainakin osittain vastaajaa ja siten vaikuttanut puhelinhäirinnän määrään ja laatuun.

Tuomioistuin on ottanut rangaistusta mitatessaan lieventävinä seikkoina asianomistajan myötävaikutuksen rikoksiin sekä henkisen paineen, jonka alaisena vastaaja on rikosten tekoaikana toiminut.

Tuomioistuin on määrännyt perusmuotoisen lähestymiskiellon, koska häirintä on jatkunut yli kahden vuoden ajan. Lisäksi vastaaja on syytteen nostamisen jälkeen jatkanut viestien lähettämistä. Tuomioistuimen mukaan on perusteltua aihetta olettaa, että häirintä tulisi todennäköisesti jatkumaan ilman lähestymiskiellon määräämistä.

6.2.5. Tuomiolauselma

Käräjäoikeus on tuomiossa katsonut syytekohdat 1,2 ja 3 syyksi luetuiksi, joista oikeus antoi yhteisen sakkorangaistuksen 30 päiväsakkoa, RL 24 luvun 1 §:n, RL 24 luvun 9 §:n ja RL 38 luvun 5 §:n perusteella. Vastaaja velvoitettiin korvaamaan kotirauhan rikkomisen ja kunnianloukkauksen myötä aiheutetusta vahingosta 500 euroa korkoineen sekä oikeudenkäyntikulut 1043,10 euroa korkoineen.

6.3. Tapaus 3

Valitsin tämän tapauksen esimerkiksi tietoliikenteen häirinnän eräänlaisena tyyppitapauksena, nykyaikana. Nuori henkilö, joka on kiinnostunut tietokoneista. Helsingin käräjäoikeus antoi 9.1.2003 tuomion 03/208 muun muassa tietoliikenteen häirintää koskevassa asiassa R 02/8258.

6.3.1. Teko ja syytekohdat

Syyttäjä vaati vastaajalle rangaistusta nuorena henkilönä tehdyistä, tietoliikenteen häirinnästä ja kunnianloukkauksesta.

Asianomistaja 1 yhtyi syytteeseen ja ilmoittanut ettei hänellä ole asiassa vaatimuksia. Asianomistaja 2 yhtyi syytteeseen ja vaati vastaajaa korvaamaan asian selvittelykulut.

Syytekohdan 1. mukaan, vastaaja on lähettämällä ilkivaltaisessa tarkoituksessa häiritseviä viestejä asianomistaja 2:en ylläpitämälle keskustelupalstalle, oikeudettomasti häirinnyt televiestintää. Vastaaja on lähettänyt toistuvasti keskustelupalstalle pitkiä tekstiviestikopioita niin, että palstan asialliset viestit ovat hukkuneet niiden sekaan. Palstan ylläpitäjän estettyä pitkien viestien lähettäminen, on vastaaja ryhtynyt lähettämään lyhyitä viestejä peräkkäin. Kun vastaajan IP-osoitteelta on estetty pääsy keskustelupalstalle, vastaaja on ryhtynyt käyttämään eri lähettäjän osoitteita sekä eri välityspalvelinta ja onnistunut jatkamaan häirintää. Vastaaja on myös lähettänyt asianomistaja 2:en toimitusjohtajana toimivalle asianomistaja 1:lle useita asiattomia sähköpostiviestejä käyttämällä eri lähettäjien nimiä sekä lähettänyt asianomistaja 1:n nimissä sähköpostiviestejä eri vastaanottajille. Vastaaja on lisäksi häirinnyt televiestintää lähettämällä kymmenittäin saman asiattoman viestin kopioita asianomistaja 1:n matkapuhelimeen, tukkien matkapuhelimen muistin.

6.3.2. Vastaajan vastaus

Vastaaja on kiistänyt syytekohdan 1. Keskustelupalsta ei ole asianomistaja 2:n ylläpitämä, eikä sen toimialaan kuuluva, vaan asianomistaja 1:n harrastus. Vastaaja on häiriköinyt keskustelupalstalla, mutta tahallisesti ärsytettynä ja häiriköinti kyseisenlaisilla palstoilla on

niin yleistä, että vastaajaa ei yksittäistapauksena voida saattaa rangaistusvastuuseen, kun palstojen pitäjät joutuvat varautumaan häiriköintiin ja heillä on keinot estää pääsy palstalle.

6.3.3. Tuomion perustelut tietoliikenteen häirinnän osalta

Käräjäoikeuden mukaan vastaaja on syyllistynyt tekoihin, joista syyttäjä on vaatinut hänelle rangaistusta.

Käräjäoikeus on todennut ratkaisun perustuvan asianomistajan kertomukseen ja syyttäjän kirjallisiin todisteisiin. Vastaaja on myöntänyt menetelleensä syytteen teonkuvauksessa kerrotuin tavoin. Oikeuskirjallisuuden mukaan rangaistavuus edellyttää oikeudettomuutta. Tahallisuusvaatimus edellyttää tekijän mieltäneen, että hän toiminnallaan estää tai häiritsee televiestintää tai että hänen toiminnasta varsin todennäköisesti on tällainen seuraus.

Vastaaja on jatkanut sinnikkäästi häiritsemistä, vaikka asianomistaja on eri tavoin yrittänyt estää häiriköinnin. Käräjäoikeuden mukaan vastaajan on täytynyt erityisesti tekoa jatkaessaan ja keinoja kehitellessään tietää häiritsevänsä asianomistajan televiestintää.

6.3.4. Tuomiolauselma

Vastaajan syyksi tuomiolauselmassa on luettu nuorena henkilönä tehdyt: 1. tietoliikenteen häirintä ja 2. kunnianloukkaus, joista hänelle on langetettu yhteinen sakkorangaistus 10 päiväsakkoa. 1. kohta on perustunut rikoslain 38 luvun 5 §:ään ja 3 luvun 2 §:ään. 2. kohta on perustunut 24 luvun 9 §:ään ja 3 luvun 2 §:ään.

Vastaaja joutui korvaamaan valtiolle asianomistaja 1:lle maksetut päivärahat ym. Sekä asianomistaja 2:lle selvittelykulut yms. Vastaajan avustajalle maksetut palkkiot jäivät valtion vahingoksi.

6.4. Tapaus 4

Valitsin esimerkiksi yhden päätöksen syyttämättä jättämisestä, koska tahallisuusvaatimus on yksi perustavanlaatuinen edellytys teon rangaistavuudelle. Helsingin kihlakunnan syyttäjänviraston syyttäjä on antanut 21.9.2005 syyttämättäjättämispäätöksen 05/2170 tietoliikenteen häirintää koskevassa asiassa R 05/1033.

6.4.1. Teko ja tapahtumatiedot

Syyttämättäjättämispäätöksen tietojen mukaan epäilty on lähettänyt tietokoneellaan kaksiosaisen sähköpostiviestin eri lähteistä keräämiinsä noin 11800:een sähköpostiosoitteeseen. Viesti on sisältänyt erään kirjan esittelyä, kopion sen sisällöstä, vastaajan lähettäjätiedot. Kaksi asianomistajaa on katsonut olevan syytä epäillä vastaajan menettelyllään syyllistyneen rikokseen, koska viesti oli tukkinut tietokoneen.

6.4.2. Päätös ja sen perustelut

Syyttäjä on tehnyt asiassa päätöksensä, asiassa ei ole todennäköisiä syitä rikoksesta epäillyn syyllisyyden tueksi -perusteella.

Syyttämättäjättämispäätöksen perusteluiden mukaan tietoliikenteen häirintään voi syyllistyä se, joka lähettämällä ilkivaltaisessa tarkoituksessa häiritseviä viestejä oikeudettomasti estää tai häiritsee teleliikennettä. Päätöksessä on todettu, ettei asiassa ole käynyt ilmi, että motiivina olisi ollut tai olisi syytä epäillä olleen lain tunnusmerkistössä mainittu ilkivalta tai vastaava tarkoitus. Kysymys on ollut kertalähetyksestä.

6.5. Tapaus 5

Helsingin kihlakunnan syyttäjänviraston syyttäjä antoi 2.6.2004 syyttämättäjättämispäätöksen 04/1186 lievää tietoliikenteen häirintää koskevassa asiassa R 03/5297.

6.5.1. Teko ja tapahtumatiedot

Vastaaja oli ilmiannettu, syylliseksi epäiltynä lievästä tietoliikenteen häirinnästä siitä syystä, että vastaajan omistamasta gsm-liittymästä oli lähetetty noin kuukauden aikana yli 100 000 tekstiviestiä.

Asianomistaja on asiassa katsonut tekstiviestien määrän ja laadun poikenneen normaalista niin paljon, että on kysymys ilkivaltaisessa tarkoituksessa lähetetyistä asiattomista tekstiviesteistä ja siis tietoliikenteen häirinnästä.

6.5.2. Päätös ja sen perustelut

Syyttäjä on tehnyt päätöksen, ei näyttöä rikoksesta -perusteella. Vastaaja on esitutkinnassa kertonut lähettäneensä tekstiviestit neljään eri liittymäänsä käyttäen hyväkseen puhelimensa erikoisominaisuuksia. Viestien sisältönä oli sekalaisia kirjaimia. Vastaaja on kertonut lähettäneensä viestit testausmielessä saadakseen selville asioita liittymän toiminnasta.

Vastaaja on kertonut esitutkinnassa, että hänellä ei ole ollut tarkoitusta haitata tai vahingoittaa asianomistajan viestinvälitystoimintaa ja on toiminut asianomistajan liittymäehtojen mukaisesti.

Asianomistaja on todennut, etteivät vastaajan lähettämät viestit ole suoranaisesti keskeyttäneet tekstiviestien välittämistä verkossa, korkeintaan hidastaneet muiden käyttäjien tekstiviestien välittämistä.

Syyttäjän päätöksen mukaan asiassa on selvitetty asianomistajan oman kertomuksen perusteella, että vastaajan lähettämät tekstiviestit eivät ole tosiasiallisesti häirinneet tietoliikennettä, joten syyttäjä on katsonut, että asiassa ei ole esitetty todennäköisiä syitä vastaajan syyttämiseksi asiassa lievästä tietoliikenteen häirinnästä eikä muustakaan rikoksesta.

6.6. Tapaus 6

Helsingin kihlakunnan syyttäjänviraston syyttäjä antoi 6.8.2003 syyttämättäjättämispäätöksen 03/1776 muun muassa tietoliikenteen häirintää koskevassa asiassa R 03/4111.

6.6.1. Teko ja tapahtumatiedot

Tapauksessa epäiltyjä rikoksia oli kolme: 1. tietoliikenteen häirintä, 2. kunnianloukkaus, 3. tavaramerkkirikkomus. Tietoliikenteen häirintää koskevien tapahtumatietojen mukaan vastaaja oli asettanut asianomistajan boikottiin. Vastaajan kotisivuilla oli linkki, josta oli mahdollista lähettää palautetta asianomistajan toimitusjohtajalle. Palautteita oli tullut rikosilmoituksen mukaan useita kansioita.

6.6.2. Päätös ja sen perustelut

Päätöksen mukaan asia ei antanut aihetta syytetoimiin. Asiassa ei ollut näyttöä rikoksesta tai todennäköisiä syitä rikoksesta epäillyn syyllisyyden tueksi.

Syyttäjä on asiassa katsonut, että lähettämällä sähköpostilla lukuisia viestejä voitaisiin toteuttaa tietoliikenteen häirinnän tunnusmerkistö, sikäli kun viestien lähettämisen tarkoituksena on ilkivaltaisessa tarkoituksessa estää tai häiritä vastaanottajan tietoliikennettä. Tässä tapauksessa vastaajan ilmeisenä tarkoituksena on ollut vaikuttaa asianomistajan yrityspolitiikkaan, eikä asianomistajan tietoliikenteen häirintä. Asianomistajan selvityksen mukaan yrityksellä on ollut ongelmia sähköpostin kanssa, koska kuormitusaste on kasvanut suuremmaksi, kuin mihin oli varauduttu. Boikottikampanja ei ole ollut hyökkäys tietoverkossa, että se olisi tutkittuna ajanjaksona tullut mieltää tietoliikenteen häirinnäksi.

6.6.3. Huomioita tapauksesta, tahallisuus rangaistuksen edellytyksenä

Rikoslaissa säädettyjen tekojen rangaistavuuden edellytyksenä on tahallisuus, ellei toisin ole säädetty. Epäillyn tarkoituksena ei ole aina palvelunestohyökkäyksen aikaansaaminen, vaikka lopputulos voi sitä olla. Edellä mainittu tapaus on siitä hyvä esimerkki.

6.7. Tietojärjestelmän häirintä -tapaus

Tietoliikenteen häirintä ja tietojärjestelmän häirintä toissijaisena, täydentävänä säännöksenä ovat kokonaisuutena käsiteltäviä, toisiaan täydentäviä säännöksiä, kun asiaa pohtii Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen ja Euroopan unionin neuvoston puitepäätöksen kannalta, joissa kriminalisointi on toteutettu yhdellä säännöksellä. Kuten aikaisemmin tässä tutkielmassa on todettu, tietojärjestelmän häirintä on toissijainen tunnusmerkistö suhteessa moneen muuhun rikoslain säännökseen ja siten tulee harvoin sovellettavaksi. Se on yleensä syyttäjän toissijaisena rangaistusvaatimuksena siltä varalta, mikäli rangaistusvaatimus tietoliikenteen häirinnästä ei menesty. Käsittelen yhden esimerkkitapauksen tietojärjestelmän häirinnästä, joka yleensä aktualisoituu nuoren henkilön tekona.

6.7.1. Teko

Vantaan käräjäoikeus antoi 15.5.2012 tuomion 12/1763 muun muassa tietojärjestelmän häirintää koskevassa asiassa R 12/169. Esittelen tapauksesta ainoastaan tämän työn kannalta mielenkiintoisen tietojärjestelmän häirinnän teonkuvauksen.

Syyttäjä vaati kolmelle vastaajalle rangaistusta 1.tietojärjestelmän häirinnästä, 2.tietomurrosta, 3.luvattomasta käytöstä, 4.tietoverkkorikosvälineen hallussapidosta, 5.sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapidosta ja muina vaatimuksina rikoksentekovälineen menettämistä ja toissijaisesti, mikäli omaisuus määrätään palautettavaksi, kaikki data on poistettava. Syyttäjä ajoi lisäksi asianomistajan yksityisoikeudellista korvausvaatimusta syytekohtaan 1. liittyen. Vastaaja1:stä syytettiin teosta kohdissa 1-5 ja vastaajia 2 ja 3 syytettiin kohtien 2 ja 3 teoista.

Syyttäjän kohdan 1 syyte oli seuraava: Vastaaja on 29.1.2010 – 31.3.2010 Vantaalla, aiheuttaakseen toiselle haittaa, dataa syöttämällä taikka muuten siihen rinnastettavalla tavalla oikeudettomasti estänyt tietojärjestelmän toiminnan tai aiheuttanut sille vakavaa häiriötä siten, että on luonut lukion IT-luokan eräälle tietokoneelle, johon eräs oppilas oli ollut kirjautuneena ja unohtanut sen poistuessaan tunnuksillaan auki, .bat -tiedoston eli niin sanotun skriptin, joka on Vastaajan käynnistettyä sen, alkanut luoda satunnaisnimisiä alikansioita lukion oppilaiden yhteisenä tallennustilana toimineelle verkkolevylle täyttäen lopulta sen arvioilta miljoonilla alikansioilla seurauksin, että varmuuskopiointi on estynyt

ja tallennustilana toiminut verkkolevy sisältöineen, on jouduttu poistamaan. Teosta on aiheutunut kaupungille ylimääräisestä, ulkopuolisella teetetystä työstä koostuva 639,60 euron vahinko.

6.7.2. Vastaajien vastaukset

Vastaaja1 myönsi kohdan 1 teonkuvauksen, mutta kiisti teon tahallisuuden, teon ennakoimattomuuteen vedoten. Hän kiisti muut syytekohdat ja lisäksi menettämisseuraamuksen. Menettämisseuraamuksen osalta hän vetosi siihen, että pöytäkonetta on käytetty vain kokeilumielessä hash-tiedostojen aukaisuun ja kannettavaa konetta, ulkoista kovalevyä ja muistitikkua on käytetty vain tilapäisenä varmuuskopiona, eikä niitä ole hankittu rikolliseen tarkoitukseen. Vastaaja ilmoitti menettämisseuraamuksen osalta, että kaikki data voidaan hävittää levyiltä ja korvausvaatimuksen perusteen hän kiisti, koska lopputulos oli odottamaton ja korjauskustannusten määrän osalta tuntiveloitus oli kohtuuton ja yli alan keskihinnan.

Vastaaja 2 myönsi avanneensa kohdan 2 ja 3 kohdalla avanneensa tietokoneen kotelon ja olevansa siltä osin osallinen.

Vastaaja 3 kiisti syytteen kohdat 2 ja 3, koska oli vain paikalla, mutta ei koskenut koneeseen eikä murtautunut mihinkään.

6.7.3. Tuomion perustelut tietojärjestelmän häirinnän osalta

Tuomioistuin on todennut perusteluissaan vastaajan tarkoituksellisesti käyttäneen hyväkseen tilaisuutta, kun toinen käyttäjä on unohtanut tilinsä auki ja jättänyt skriptin toimintaan koko viikonlopuksi ajatelleen, että sitä ei voida kirjautumistiedoista yhdistää häneen. Tuomioistuimen mukaan Vastaaja1:n ilmeinen tarkoitus on ollut aiheuttaa haittaa toimellaan muille tietojärjestelmän käyttäjille. Käsitystä tukee muun muassa se, että hän on keskustelupalstalla kertonut sen pyörineen “viattoman ykkösen tai kakkosen auki unohtuneella käyttäjätilillä”. Tuomioistuin on katsonut syytteen toteen näytetyksi.

6.7.4. Muut syytekohdat lyhyesti

Tuomioistuimen mukaan syytekohdat 2 ja 3 koskevat samaa tapahtumaa ja vastaajien kertomuksia kokonaisuutena arvioiden näyttää olevan selvää, että he ovat tehneet koneelle tunkeutumisen yhdessä ja yksissä tuumin.

Tuomioistuimen mukaan teko täyttää tietomurron tunnusmerkistön jo pelkästään järjestelmään suojattuun osaan luvattomasti tunkeutumisella. Vastaajat ovat myös käyttäneet järjestelmää kopioimalla koneesta hash-arvoja, teko on hallituksen esityksessä 94/1993 kerrotuin perustein arvioitava kokonaisuudessaan luvattomaksi käytöksi. Tietojärjestelmän omistaja on ilmoittanut asian syytteeseen pantavaksi.

Kohdan neljä syyte hylättiin. Tuomioistuimen mukaan on kiistatonta, että syytteessä mainitut ohjelmat ovat soveltuneet 2 ja 3 kohdissa kerrotun teon toteuttamiseen, ovatko ne sitten nimenomaisesti suunniteltu sitä tarkoitusta varten, ei ole selvinnyt asian käsittelyssä, siitä ei ole esitetty selvitystä. Vastaajan mukaan ne ovat hänen jatko-opiskelujaan varten hankkimiaan vapaasti saatavissa olevia tietoturvallisuuden tutkintaan käytettyjä muuntamattomia ohjelmia, joista Cain & Abel on hänen mukaansa tarkoitettu kadonneiden salasanojen palauttamiseen, Ardamac Keylogger luvattoman käyttöyrityksen havaitsemiseen ja Backtrackin olevan yleisesti saatavissa oleva Linux-versio, jossa olevat ja kohdassa 2-3 käytetyt apuohjelmat ovat olleet vakiona siinä mukana. Syyttäjä ei ole kiistänyt ohjelmilla olevan myös laillisia käyttötarkoituksia. Pelkästään ohjelmien soveltuminen laillisten tarkoitusten ohella myös rikollisiin tarkoituksiin ei tee niistä RL 34 luvun 9 b §:ssä ja 9 a §:ssä tarkoitettuja ilman puuttuvaa selvitystä suunnittelutarkoituksesta tai muuntamisesta. Ei ole perusteita katsoa, että Vastaaja1 olisi ne hankkinut aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle tai tieto- ja viestintäjärjestelmän toiminnalle.

Tuomioistuin katsoi kohdan 5 syytteen toteen näytetyksi. Käräjäoikeus on todennut, ettei se pidä uskottavana väitettä, että kuvat olisivat olleet koneella hänen tietämättään.

Rangaistusseuraamuksesta tuomioistuin lausui seuraavaa: Sakkorangaistus on oikeudenmukainen seuraamus vastaajille syyksi luetusta rikoksesta, myös vastaajalle1, koska hänenkin tekonsa on katsottu johtuneen enemmän ajattelemattomuudesta kuin rikollisesta tarkoituksesta.

Menettämisseuraamuksesta tuomioistuin on todennut, että rikoslain 10 luvun 6 §:n perusteella laitteita ei voi tuomita rikoksentekovälineinä menetetyksi. Vastaaja on esittänyt todisteina ostolaskuja, joiden mukaan laitteiden maksaja on ollut vastaajan isä. Syyttäjä ei ole kiistänyt laskuja. Näyttämättä on siten jäänyt, että laitteet olisivat olleet lahjoja vastaaja1:lle.

Takavarikoilla laitteilla olevat lasta esittävät syytekohdan 5 kuvat sekä hash-arvot ja puretut salasanat tuomitaan rikoslain 10 luvun 5 §:n 1 ja 2 momentin nojalla menetetyksi ja määrätään poistettavaksi tarkoituksenmukaisella tavalla. Koska syyttäjän ilmoittaman mukaan näiden tietojen erottaminen ja poistaminen laitteilla olevasta muusta datasta ei ole hankaluuksitta mahdollista, tuomitaan rikoslain 10 luvun 5 §:n 3 momentin nojalla myös laitteilla oleva data menetetyksi siinä laajuudessa kuin se on välttämätöntä menetetyksi tuomittujen tietojen poistamiseksi.

6.7.5. Tuomiolauselma

Vastaaja1:en syyksi luettiin seuraavat rikokset: 1.tietojärjestelmän häirintä, 2.luvaton käyttö ja 3.sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito. Hän sai yhteisen sakkorangaistuksen 110 päiväsakkoa. Perusteena ovat lainkohdat: RL 38 luvun 7 a § 1 momentti, RL 28 luvun 7 § 1 momentti ja RL 17 luvun 19 §. Muuna rikosoikeudellisena seuraamuksena on tuomittu syytekohdan 5 kuvat sekä rikoksella aikaansaadut ja uusiin rikoksiin soveltuvat hash-arvot ja puretut salasanat rikoslain 10 luvun 5 §:n 1 ja 2 momentin nojalla menetetyksi ja määrättiin poistettavaksi tarkoituksenmukaisella tavalla. Rikoslain 10 luvun 5 § 3 momentin nojalla on tuomittu myös laitteilla oleva data menetetyksi siinä laajuudessa kuin se on välttämätöntä edellä mainittujen menetetyksi tuomittujen tietojen poistamiseksi. Takavarikko määrätään pidettäväksi voimassa, kunnes tuomio on tullut lainvoimaiseksi ja pantu täytäntöön poistamalla mainitut tiedot. Sen jälkeen takavarikoidut laitteet on palautettava omistajalleen.

Vastaaja2:en syyksi luettiin luvaton käyttö ja syyte tietomurrosta hylättiin. Hän sai rangaistusseuraamukseksi 25 päiväsakkoa.

Vastaaja3:en syyksi luettiin luvaton käyttö ja syyte tietomurrosta hylättiin. Hän sai rangaistusseuraamukseksi 25 päiväsakkoa.

Vastaaja1 tuomittiin lisäksi korvaamaan kaupungille tietojärjestelmän korjaamisesta aiheutuneesta ylimääräisestä työstä syntyneet kustannukset laillisine korkoineen 31.3.2010 lukien korkolain 4 §:n 1 momentin mukaisine viivästyskorkoineen tekopäivästä 31.3.2010 lukien.

6.8. Muita säännöksiä

Tietoverkkorikoksia ovat muun muassa: vaaran aiheuttaminen tietojenkäsittelylle, tietoverkkorikosvälineen hallussapito, vahingonteko, viestintäsalaisuuden loukkaus ja sen törkeä tekomuoto ja tietomurto. Säännöksien käsittelyä on vaikea rajoittaa suhteessa tämän työn aiheeseen, joten käsittelen näistä vaihtoehdoista kaksi, jotka voivat liittyä esimerkiksi tietoliikenteen häirintä -tapaukseen.

Tietomurron tyyppiesimerkkinä on pidetty tietokoneen kaappaamista bottiverkkoon[119], jossa laitetta käytetään haittaohjelmien levittämiseen, roskapostin lähettämiseen tai palvelunestohyökkäyksiin. Haittaohjelmien avulla voidaan esimerkiksi anastaa luottokorttitietoja, joita sitten voidaan käyttää rikosten tekemiseen. Toiminta voi olla varsin järjestäytynyttä; siihen voi liittyä rahanpesuverkostoja, joita käytetään anastettujen varojen siirtämiseen rikollisten haltuun.[120]

Datan vahingoittamisesta on säädetty Euroopan neuvoston tietotekniikkarikollisuutta koskevan yleissopimuksen 4 artiklassa. Artiklan 1 kappaleen mukaan tahallinen ja oikeudeton datan vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen tai poistaminen on säädettävä rangaistavaksi teoksi.

Tekotapaluettelossa on pyritty kattavuuteen, jonka vuoksi tekotavat ovat osittain päällekkäisiä. Esimerkiksi datan muuttaminen, turmeleminen ja vahingoittaminen on mainittu artiklassa erillisinä tekotapoina. Tekotavoille on yhteistä teon seuraus eli data ei

[119] Bottiverkko on tietoverkon kautta kaapatuista tietokoneista muodostuva verkko, jota sen haltija valtuutetun käyttäjän tietämättä käyttää haitallisiin tai laittomiin tarkoituksiin (*Sanastokeskus TSK ry* 2012, hakusanat *bottiverkko* ja *kaapattu tietokone*).
[120] Sisäasiainministeriö 2008, s. 20.

ole enää teon jälkeen samanlaista kuin ennen tekoa. Edellä mainitun vahingon voi aiheuttaa esimerkiksi tietokonevirus.

Suomessa voimassa oleva säännös vahingonteosta 35 luvun 1 §:ssä kattaa artiklassa tarkoitetun teon. Pykälän 2 momentin mukaan vahingonteosta on tuomittava se joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen. Lain esitöiden (HE 66/1988) mukaan tietovälineelle tallennetulla tiedolla tarkoitetaan tiedon asiasisältöä eli informaatioita ja asiasisältöä viestittäviä merkkejä eli dataa. Tietovälineellä tarkoitetaan esimerkiksi asiakirjaa, tai tietokonelevykettä. Säännös kattaa siten artiklassa tarkoitetun datan. Turmelemisella tarkoitetaan säännöksessä datan muuttamista sisällöltään toiseksi, epäymmärrettävään tai käyttökelvottomaan muotoon. Säännös kattaa siten kaiken datan muuttamisen, jonka seurauksena data joko muuttuu tai häviää.[121]

6.9. Syyteoikeus

Rikoslain 38 luvussa säädettyjen tekojen syyteoikeudesta on säädetty luvun 10 §:ssä, jossa on todettu tämän työn kannalta keskeisten tunnumerkistöjen osalta seuraavaa:

> ..Syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmärikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikoksentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista..

Toisin sanoen tähän tutkielmaan liittyvistä säännöksistä ainoastaan tietojärjestelmän häirintä on asianomistajarikos.

ETL 3 luvun 4 § mukaan asianomistajarikoksen esitutkinta on syyttäjän pyynnöstä toimitettava, jos syyttäjä saa lain mukaan erittäin tärkeän yleisen edun sitä vaatiessa nostaa syytteen asianomistajarikoksesta, vaikka asianomistaja ei ole vaatinut rangaistusta. Syyttäjä saa erittäin tärkeän yleisen edun niin vaatiessa nostaa syytteen ilman syyttämispyyntöä, mutta käytännössä tuomioistuin ratkaisee lopulta onko erittäin tärkeä syy ollut olemassa. Määrätessään esitutkinnan toimitettavaksi, syyttäjä ei voi olla varma

[121] HE 153/2006, s. 15–16.

syyn olemassa olosta.[122] Ottaen huomioon tietotekniikkarikosten vaatima ammattitaito ja esitutkinnasta aiheutuvat kustannukset, olisiko jokin toinen ratkaisu järkevämpi?

6.10. Toimivallan maantieteellinen ulottuvuus

Asia muuttuu mielenkiintoisesti kansainvälisesti asiaa tarkasteltaessa. Otan aiheen tutkielman rajauksesta huolimatta esille, sen mielenkiintoisuudesta johtuen suhteessa erityisesti kansainvälisiin juttuihin, joita tietoverkkorikokset yleensä ovat.

Tietoverkkorikosten kansainvälisyydestä johtuen ne voivat aiheuttaa monia oikeudellisia ongelmia. Ongelmat ratkaistaan joko nimenomaisen tuomioistuimen lain mukaan tai kansainvälisen oikeuden yleisten periaatteiden avulla. Yleinen periaate on, että maan rajojen sisällä tehty tekoon voidaan käsitellä maan tuomioistuimessa. Englannissa tuomioistuimella on toimivalta, mikäli teko tapahtui Englannissa tai merkittävä osa teosta tapahtui siellä.[123]

Hyvä esimerkki mahdollisista ongelmista on 1994 Citibank:iin kohdistunut tietomurto. Tekijä Levin väitti, että hän oli Venäjälle Pietarissa, kun suoritti tilinsiirrot, jonka vuoksi Venäjän lakia piti soveltaa. Tuomari tulkitsi asiaa niin, että teko tapahtui Citibank:in tietokoneella Yhdysvalloissa, Parsipenny:ssä, koska Levin:in tietokoneen ja Citibankin tietokoneen yhteys oli reaaliaikainen ja tekijän näppäimistön painallukset tapahtuivat reaaliaikaisesti Citibankin tietokoneella.[124]

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus jättää tekopaikka-käsitteen kansallisen lain määriteltäväksi. Sama koskee merkittävä yhteys -käsitettä, liittyen tekijän tai teon liittymiseen tiettyyn maahan.[125] Asiasta voisi kirjoittaa väitöskirjan tai kaksi, joten en käsittele aihetta sen enempää kuin huomioimalla, että on olemassa muitakin periaatteita, joihin tuomioistuin voi perustaa toimivaltansa, kuten universaaliperiaate, kansalaisuusperiaate ja niin edelleen.

[122] Vuorenpää 2007, s.140.
[123] Walden 2011, s.712.
[124] Walden 2011, s.714.
[125] Kaspersen 2006, s.11.

6.11. Esitutkinnasta ja sen rajoittamisesta

Esitutkinnan rajoittamisesta voisi kirjoittaa väitöskirjan ja se liittyy enemmän rikosprosessioikeuteen, joten käsittelen asian ainoastaan sivujuonteena. Esittelen esitutkinnan rajoittamisen yhdeksi ongelmaksi tietotekniikkarikosten kentässä, jotta lukija ymmärtää sen merkityksen ja sen aiheuttamat ongelmat tietotekniikkarikosten selvittämisen kannalta. Tietotekniikkarikosten esitutkinta on erityislaatuista siihen kohdistuvien ammatillisten vaatimusten ja kustannusten vuoksi. Useasti tietotekniset rikokset vaativat yhteistyötä sekä poliisin, että syyttäjän välillä ja kansainvälisesti eri maiden esitutkintaviranomaisten välillä.

Valtakunnansyyttäjänviraston esitutkintayhteistyötä koskevassa ohjeessa on määritelty tiettyjä ominaispiirteitä tietotekniikkarikosten esitutkintaan ja syyteharkintaan liittyen, ohjeen mukaan onnistumisen edellytyksenä on: 1. suunnitelmaan perustuva, pitkäkestoinen tutkinta, 2. asiantuntemus erityisistä tunnusmerkistöistä, vastuun kohdentamisesta ja lainsäädännöstä, 3. tutkinnan kohdentaminen ja rajaaminen esitutkintaa rajoittamalla ja käyttämällä muita keinoja. Tietotekniikkarikokset kuuluvat sellaisten rikosten joukkoon, joista esitutkintaviranomaisten on ohjeen mukaan, aina ilmoitettava syyttäjälle. Jokainen ilmoitus puolestaan edellyttää syyttäjän toimia ja ilmoitus katsotaan toimenpiteitä edellyttämättömäksi ainoastaan silloin, jos molemmat osapuolet, ilmoituksen jälkeen, keskustelun päätteeksi niin sopivat.[126]

Rikoksen tutkinnassa on pääsääntönä esitutkintapakko 1.1.2014 voimaantulleen esitutkintalain 3 luvun 3 § 1 momentin perusteella:

> Esitutkintaviranomaisen on toimitettava esitutkinta, kun sille tehdyn ilmoituksen perusteella tai muuten on syytä epäillä, että rikos on tehty..

Esitutkinnan rajoittaminen on poikkeus pääsääntöisestä esitutkintapakosta. Tutkinnanjohtaja voi tehdä päätöksen esitutkinnan toimittamatta jättämisestä ja lopettamisesta esitutkintalain 3 luvun 9 § perusteella:

> Esitutkinta saadaan jättää toimittamatta tai jo aloitettu esitutkinta lopettaa sellaisen rikoksen johdosta, josta ei ole odotettavissa ankarampaa rangaistusta kuin sakkoa ja

[126] Valtakunnansyyttäjänviraston julkaisusarja nro 7, s.39.

> jota on kokonaisuutena arvostellen pidettävä ilmeisen vähäisenä, jos asianomistajalla ei ole asiassa vaatimuksia..

Syyttäjä voi puolestaan rajoittaa esitutkintaa esitutkintalain 3 luvun 10 § perusteella:

> Syyttäjä voi tutkinnanjohtajan esityksestä päättää, ettei esitutkintaa toimiteta tai että se lopetetaan, jos syyttäjä oikeudenkäynnistä rikosasioissa annetun lain 1 luvun 7 tai 8 §:n taikka muun vastaavan lainkohdan nojalla tulisi jättämään syytteen nostamatta eikä tärkeä yleinen tai yksityinen etu vaadi syytteen nostamista.
> Syyttäjä voi tutkinnanjohtajan esityksestä myös päättää, että esitutkinta lopetetaan, jos tutkinnan jatkamisesta aiheutuvat kustannukset olisivat selvässä epäsuhteessa tutkittavana olevan asian laatuun ja siitä mahdollisesti odotettavaan seuraamukseen tai jos jo suoritettujen esitutkintatoimenpiteiden perusteella on varsin todennäköistä, että syyttäjä tulisi jättämään syytteen nostamatta muulla kuin 1 momentissa mainitulla perusteella..

Uuden esitutkintalain yllä mainitut säännökset vastaavat vanhan lain sisältöä, ainoastaan muutamaa sanaa on muotoiltu ja pykälämerkinnät ovat muuttuneet. Vanhassa ETL:ssä[127] on ollut sama sisältö 4 §:n 3 ja 4 momentissa. Uuden ETL:n asiasisällön vuoksi edellä mainittujen pykälien tulkinnan kannalta VETL:n lainvalmisteluaineisto on yhä ajankohtaista.

Lakivaliokunnan mietinnön mukaan VETL:n 4 §:n 3 momentissa (ETL:n 3 luvun 10 §:n 1 momentti, ks. yllä) on säädetty esitutkinnan rajoittamisesta, joka nojautuu odotettavissa olevaan seuraamusluonteiseen syyttämättäjättämispäätökseen.[128]

Valtakunnansyyttäjänviraston ohjeen 2007:2 mukaan VETL 4 §:n 4 momentilla(ETL:n 3 luvun 10 §:n 2 momentti, ks. yllä) laajennettiin syyttäjän mahdollisuus rajoittaa esitutkintaa ennakoitavissa olevan syyttämättäjättämisen tilanteisiin ja kustannusperusteisiin tilanteisiin.[129]

Joten rajoittamisperusteet voidaan jakaa kolmeen eri ryhmään: 1. seuraamusluonteiseen rajoittamiseen, 2. prosessuaaliseen rajoittamiseen ja 3. kustannusperusteiseen rajoittamiseen. Seuraamusluonteinen rajoittaminen jakaantuu edelleen: a. vähäisyysperusteiseen, b. nuoruus, c. kohtuus, d. konkurrenssi ja f.

[127] Tästä lähtien VETL.
[128] LaVM 17/1989 vp.
[129] VKS 2007:2. s.1.

erityissäännösperusteiseen. Prosessuaalinen rajoittaminen jakaantuu: a. ei rikosta, b. ei näyttöä, c. ei syyteoikeutta ja d. syyteoikeus vanhentunut -perusteeseen.[130]

Edellä mainituista rajoitusperusteista on tämän työn kannalta relevantein kustannusperusteinen rajoittaminen. Tietotekniikkarikoksissa odotettavissa olevat tuomiot ovat pieniä, mutta vahingonkorvaussummat voivat nousta korkeiksi. Teot on yleensä tehty nuoruuden innolla ajattelemattomuuttaan. Johtuen kuitenkin tekojen vahingoista suhteessa tutkinnasta aiheutuviin kustannuksiin, on esitutkinnan kustannusperusteinen rajoittaminen yleensä välttämätöntä.

VKS 2007:2 ohjeen mukaan esitutkinnan rajoittamisen yhteisenä taustaperiaatteena on prosessitaloudellisuus ja se säästää kaikkien rikosasian käsittelyyn osallistuvien resursseja: esitutkintaviranomainen, syyttäjä, tuomioistuin. Ohjeessa on todettu säästämisellä saatavilla olevan hyödyn olevan sitä suurempi, mitä aikaisemmassa rajoittamispäätös tehdään.[131]

Edellä mainittu asettaa haasteita esitutkintaviranomaisen ja syyttäjän ammattitaidoille. Heidän tulee pystyä jo tutkinnan alkuvaiheessa suunnittelemaan tutkinnan kulku ja arvioimaan sen kustannukset. Tähän tarvitaan mielestäni erityistä asiantuntemusta, erityisesti teknistä osaamista tietotekniikkarikosten esitutkinnasta ja siihen liittyvistä haasteista. Huolimatta esitutkinnan rajoittamisen mahdollisuudesta, tulee syyttäjän esitutkintapakkoon rakentuvassa järjestelmässä edellyttää esitutkintatoimenpiteiden suorittamista siinä laajuudessa, kuin se on mahdollista, suhteessa asian laatuun.

Esitutkintatoimenpiteitä ei tulisi rajoittaa vetoamalla tutkinnan hankaluuteen suhteessa tekoon, mikäli helposti suoritettavissa olevia, perustavanlaatuisia esitutkintatoimenpiteitä ei ole suoritettu. Esitutkinnan rajoittaminen ei pitäisi olla automaattista vakioperusteluihin vetoamista, ennen kuin asiaa on selvitetty riittävästi suhteessa selvittämisen kustannuksiin ja asian selvittämisintressiin.

VKS 2007:2 ohjeessa on todettu VETL 4 §:n 4 momentin eli ETL 3 luvun 10 §:n 2 momentista, että esitutkintaa ei voi rajoittaa jättämällä se kokonaan toimittamatta, vaan

[130] VKS 2007:2. s.2.
[131] VKS 2007:2. s.2.

kyse on aina aloitetun esitutkinnan lopettamisesta. Esitutkinta voi olla erilaisten tiedustelujen myötä jo aloitettu vaikka kuulusteluja ei ole toimitettukaan.[132]

VKS 2007:2 ohjeessa on todettu VETL 4 §:n 4 momentin 1. virkkeen alkuosan eli ETL 3 luvun 10 §:n 1 momentin alkuosasta sen olevan eräänlainen rikosprosessiekonominen suhteellisuusperiaate, poikkeuksena esitutkintapakolle. Ohjeen mukaan säännöksen tarkoituksena on yhteiskunnan voimavarojen käytön kustannustehokas kohdentaminen. Säännöksen perusteella ei kuitenkaan voida jättää vähäisiä rikoksia suoraan tutkimatta vaan säännös edellyttää vertailua vaadittuun lopputulokseen ja siinä olevaa epäsuhtaa. Epäsuhdan tulee olla lajissaan tavanomaista suuritöisempi [133]

> ..tutkinnan jatkamisesta aiheutuvat kustannukset suhteutetaan tutkittavana olevan asian laatuun ja siitä mahdollisesti odotettavissa olevaan seuraamukseen.[134]

Ohjeen mukaan kustannusperusteisen esitutkinnanrajoittamissäännöksen eli ELV 3 luvun 10 § loppukohta, on esitutkinnan rajoittamisen edellytyksenä se, ettei tapauksessa ole kysymys tärkeästä yleisestä edusta eikä tärkeästä yksityisestä edusta. Lyhyesti ohjeen mukaan tärkeä yleinen etu liittyy yleisprevention merkitykseen rikosoikeudellisen järjestelmän toimivuuden kannalta. Tärkeä yksityinen etu puolestaan etenkin asianomistajan vahingonkorvausintressiin ja ennen kaikkea siihen kuinka suuresta taloudellinen intressistä asiassa on kysymys asianomistajan kannalta.

Käytännössä esimerkiksi keskustelufoorumilla anonyymisti lähetetty ja julkaistu, asianomistajaa loukkaava lyhyt viesti, kuten loukkaava sana ei riittäne esitutkinnan jatkamiseen kovin pitkälle, ellei asianomistajalla ole epäilyä tekijästä. Mikäli asianomistajalla on epäily tekijästä, poliisi voinee jatkaa tutkintaa tiedusteluin. Nykyaikana yksi sana ei liene loukkaa ketään muutenkin anonyymissä ja melko heikosti kontrolloidussa internetissä. Esitutkinnan jatkaminen teknisin keinoin olisi yhteiskunnalle kallista suhteessa aiheutettuun vahinkoon, mutta esitutkintaa ei saa päättää tietynlaatuisten tapausten kohdalla kategorisesti, vaan asioita tulee aina tarkastella tapauksittain ja tehdä esitutkintatoimenpiteitä siinä määrin kuin asiassa voidaan järkevästi katsoen suorittaa, annettujen ohjeiden puitteissa.

---

[132] VKS 2007:2. s.4.
[133] VKS 2007:2. s.5.
[134] VKS 2007:2. s.5.

7. KANSAINVÄLINEN KATSAUS ERÄISIIN VALTIOIHIN

Tässä luvussa käydään läpi Ruotsissa, Norjassa, Tanskassa ja Yhdysvalloissa tällä hetkellä voimassa olevaa rikoslainsäädäntöä, mikä vastaa tietoliikenteen häirinnän ja tietojärjestelmän häirinnän säännöksiä eli käytännössä Euroopan neuvoston tietoverkkorikollisuutta koskevaa yleissopimusta. Katsantonäkökulman pääpaino on lähinnä palvelunestohyökkäyksen kriminalisoinnissa, kuten koko tämän tutkielman. Valtioista yleissopimukseen sitoutuneita ovat kaikki muut paitsi Ruotsi, joka on sopimuksen allerkirjoittanut, mutta ei ole sitä ratifioinut. Ruotsi on toisaalta täytäntöönpannut tietoverkkohyökkäyksiä koskevan puitepäätöksen vaatimukset.

Säätelytavat ovat pohjoismaiden välillä hieman erilaisia. Muutama maa on pitäytynyt perinteisessä tavassa säädellä asiasta, laajentamalla jo olemassa olevien säännösten ulottuvuutta, tietokoneiden välityksellä tehtyihin tekoihin. Toisissa maissa on puolestaan muokattu omat säännökset tietokonerikoksille.

7.1. Ruotsi

Ruotsin on katsottu olevan tietotekniikkaan liittyvän lainsäädännön kehittämisen edelläkävijä.[135] Mietinnössä on todettu ruotsin brottsbalkenin 4 luvun 9 c §:n dataintrång-säännöksen, olevan keskeisellä sijalla. Dataintrång-säännös otettiin brottsbalkeniin 1998 samalla kun datalagen korvattiin personuppgiftslagenilla. Datalagenin dataintrång -säännös siirrettiin ilman muutoksia brottsbalkeniin. Dataintrång-säännös sai lopullisen, voimassaolevan muotonsa vuonna 2007, samassa yhteydessä kun täytäntöönpantiin EU:n puitepäätös 2005/222/RIF.[136] Lakimuutoksen syynä ei ollut ainoastaan puitepäätöksessä asetetut vaatimukset, vaan tarkoituksena oli myös uudistaa säännöstä, jotta se olisi selkeämpi ja parempi kielellisesti.[137]

[135] Pihlajamäki 2004, s.105.
[136] Sou 2013/39, s.69.
[137] Sou 2013/39, s.70.

Brottsbalkenin 4 luvun 9 c §:ssä on säädetty:

> Den som i annat fall än som sägs i 8 och 9 § olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.[138]

Perustelujen mukaan säännös muotoiltiin tarkoituksella sellaiseksi. että se kattaa kaiken tiedon, datan, informaation, jota voidaan muokata tai lukea tietokoneella, sisältäen myös erilaiset ohjelmistot. Tarkoituksena oli, että säännöksen soveltaminen ei ole sidonnainen tiettyyn tallennusalustaan tai tiedon sijaintiin tietokoneessa. Tavoitteena on ollut siis säännöksen riippumattomuus käytettävästä teknisestä alustasta ja tekniikan kehittymisestä aiheutuvista muutoksista.[139] Säännös on huomattavan laaja käsittäen esimerkiksi salatun radioviestin purkamisen, muuttamisen tai tuhoamisen.[140] Kuten Suomessa, säännöksen soveltaminen edellyttää tahallisuutta.[141] Säännös kriminalisoi myös tietojärjestelmän oikeudettoman estämisen, joka voi olla myös hidastamista.

Hidastamisen voi aiheuttaa esimerkiksi palvelunestohyökkäys(DoS tai DDoS). Säännös voi kohdistua esimerkiksi ohjelmaan joka luo ja lähettää niin monta sähköpostia, että vastaanottajan järjestelmä kaatuu, toimii heikosti ja sitä kautta estää tai häiritsee järjestelmän tietojen käyttöä.[142] Rangaistusasteikko on sakkoa tai korkeintaan kaksi vuotta vankeutta. Tällä hetkellä hallitus on lähettänyt lagrådet:lle lakiehdotuksen lainsäädännön muuttamiseksi, jossa kovennettaisiin rangaistusmaksimi kuuteen vuotta vankeutta, jotta säännös täyttäisi uuden direktiivin vaatimukset.[143] Muutoksen jälkeen dataintrång-säännös ei tule enää olemaan toissijainen suhteessa brytande av post- eller telehemlighet -säännökseen, jossta on säädetty brb:n 4 luvun 8 §:ssä, eikä myöskään intrång i förvar -säännökseen, josta on säädetty brb:n 4 luvun 9 §:ssä.[144]

---

[138] https://lagen.nu/1962:700#K4P9c.
[139] Regeringens proposition 2006/07:66, s.40–41.
[140] Regeringens proposition 2006/07:66, s.49.
[141] Brottsbalken 1 luvun 2 §.
[142] Regeringens proposition 2006/07:66, s.50.
[143] http://www.dagensjuridik.se/2014/01/sex-ars-fangelse-det-nya-brottet-grovt-dataintrang-nytt-lagforslag-fran-regeringen-idag.
[144] SOU 2013/39, s.335.

Dataintrång-säännös on siis tällä hetkellä toissijainen suhteessa sekä posti- tai telekotirauhan rikkomiseen(brytande av post- eller telehemlighet), josta on säädetty brottsbalkenin 4 luvun 8 §:ssä, että vapaasti suomennettuna ns. murtoon(intrång i förvar), josta on säädetty 4 luvun 9 §:ssä. Yksinkertaistetusti ilmaistuna brytande av post- eller telehemlighet -säännös soveltuu tapaukseen, jossa tekijä mahdollistaa itselleen pääsyn viestin sisältöön. Puolestaan intrång i förvar -säännös soveltuu tekoon, jossa tekijä murtautuu kassakaappiin, avaa suljetun kirjeen tai avattu viesti on ollut muuten lukitussa paikassa. En käsittele edellä mainittuja säännöksiä sen syvällisemmin, koska ne eivät liity palvelunestohyökkäyksen kriminalisointiin.

Lähtökohtaisesti dataintrång-säännöksellä suojataan tietoa. Sama lähtökohta toistuu posti- tai telekotirauhan rikkomissäännöksessä brb:n 4 luvun 8 §:ssä, jossa suojeltavana oikeushyvänä on viesti. Toisin sanoen Ruotsin malli poikkeaa monien muiden maiden lainsäädäntötavasta. Ruotsissa lähtökohtana on tieto, muissa maissa itse toiminta. Euroopan neuvoston yleissopimuksenkin säännökset kohdistuvat pääasiassa menettelyyn.[145]

Mietinnössä on todettu Ruotsin lainsäädännön täyttävän sekä Euroopan neuvoston yleissopimuksen tietojärjestelmän häirintää koskevan 5 artiklan vaatimukset, että EU:n puitepäätöksen 3 artiklan vaatimukset. Lisäksi on todettu EU:n puitepäätöksen korvaavan, uuden direktiiviehdotuksen 4 artiklan eli tietojärjestelmän häirintä -artiklan olevan periaatteessa yhdenmukainen puitepäätöksen 3 artiklan ja yleissopimuksen 5 artiklan kanssa.[146] Myös oikeushenkilön rangaistusvastuu on toteutettu jo puitepäätöksen täytäntöönpanon yhteydessä.[147]

Mietinnössä on kuitenkin todettu, että maksimirangaistusta tulisi koventaa vähintään viiteen vuoteen, kun teko on tehty osana 1) järjestäytynyttä rikollisryhmää; 2) teossa on aiheutettu yleisvaarallista vahinkoa; 3) teko kohdistuu kriittiseen infrastruktuuriin, jotta dataintrång-säännös kattaisi uuden direktiivin vaatimukset.[148]

Mietinnön mukaan uudessa lakiehdotuksessa olisi täysin uusi 2 kappale, brb:n 4 luvun 9 c § tulisi olemaan seuraavanlainen:

[145] Sou 2013/39, s.72.
[146] Sou 2013/39, s.91 & 94.
[147] Regeringens proposition 2006/07:66, s.31.
[148] Sou 2013/39, s.309.

> Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.
>
> Om brottet är grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art. [149]

Tulevan muutoksen myötä myös teon yritys ja valmistelu olisi rangaistava teko.[150]

Dataintrång-säännös on huomattavan tärkeä Ruotsissa, johtuen sen laajasta soveltamisalasta verrattaessa posti- ja telekotirauhan rikkomiseen. Tämä käy ilmi mietinnössä olevista taulukoistakin, joiden mukaan dataintrång-teosta vuonna 2003 nostettiin 25 syytettä ja annettiin 10 tuomiota. Vuonna 2011 puolestaan nostettiin 64 syytettä ja 33 annettiin tuomiota. Eli tuomittujen tekojen määrä on kaksinkertaistunut. Samaan aikaan tele- ja kotirauhan rikkomisesta on annettu keskinmäärin yksi tuomio vuodessa.

Dataintrång-säännöksen ollessa päärikoksena, ketään ei ole tuomittu ehdottomaan vankeusrangaistukseen, vaan pääasiassa rangaistuksena on ollut sakkoa.[151] Poliisille tehtyjen dataintrång-säännökseen liittyvien rikosilmoitusten määrät ovat hurjasti nousseet, vuonna 2003 on tehty 731 ilmoitusta, vuonna 2013 on tehty jo 8646 ilmoitusta.[152] Mielenkiintoista asiassa on syytteiden ja tuomioiden alhainen määrä suhteessa tehtyihin rikosilmoituksiin.

7.2. Norja

Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen täytääntöönpanoa koskevassa mietinnössä on todettu Norjan lainsäädännön täyttävän sopimuksen vaatimukset vahingontekoa koskevalla säännöksellä.[153] Vahingontekoa koskeva säännös

[149] SOU 2013/39, s.335.
[150] Sou 2013/39, s. 307.
[151] SOU 2013/39, s.297.
[152] SOU 2013/39, s.294.
[153] Nou 2003/27, s.17–18.

soveltuu myös tekoihin joissa tietokoneella käsiteltävässä muodossa olevia tietoja esimerkiksi vahingoitetaan tai poistetaan.

Straffeloven 28 luvun 291 § mukaan:

> For skadeverk straffes den som rettstridig ødelegger, skader, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.
> For skadeverk straffes også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres data.
>
> Straffen for skadeverk er bøter eller fengsel inntil 1 år. Medvirkning straffes på samme måte.
>
> Offentlig påtale finner ikke sted uten fornærmedes begjæring, medmindre almene hensyn krever påtale.

Vahingonteon törkeän tekomuodon rangaistusmaksimi on kuusi vuotta vankeutta. Törkeysarvosteluun vaikuttava säännöksen mukaan: vahingonsuuruus, onko jonkun henki ollut vaarassa, teon rasistinen motiivi, onko yleinen tietoliikenne häiriintynyt ja niin edelleen. Straffeloven 292 § mukaan:

> Grovt skadeverk straffes med bøter eller med fengsel inntil 6 år. Medvirkning straffes på samme måte.
>
> Ved avgjørelsen av om skadeverket er grovt skal det særlig legges vekt på om skaden er betydelig, om den skyldige vitende har voldt velferdstap eller fare for noens liv eller helbred, om handlingen er rasistisk motivert, om det er voldt avbrekk i den offentlige samferdsel, om skaden er øvd på grenseskjel mot naborike eller mot offentlig minnesmerke, samlinger eller andre gjenstander som er bestemt til alminnelig nytte eller pryd eller som for almenheten eller en større krets har historisk, nasjonal eller religiøs verdi.

Norjassa on myös datainbrudd-säännös straffeloven 145 § 2 kappaleessa, josta tuomitaan se, joka murtamalla turvajärjestelyn tai muulla tavalla oikeudettomasti valmistelee pääsyn tietoihin tai ohjelmaan, jotka ovat tallennettuna tai jotka siirretään elektronisin tai teknisin keinoin.[154] Tekijä syyllistyy tekoon jo, kun hän saattaa tiedot saatavilleen. Dataintrång-säännös soveltuu myös salakuuntelun eri muotoihin.[155]

[154] Ot. prp. nr. 40 2004-2005, s.12.
[155] Nou 2003/27, s.16.

7.3. Tanska

Tanskan straffeloven 291 §:n vahingontekoa koskevaa säännöstä voidaan soveltaa tekoihin, joissa tietojärjestelmän laillinen haltija estyy käyttämästä tietojärjestelmää kokonaan tai osittain, esimerkiksi DoS -hyökkäyksen vuoksi. 291 §:n haervaerk-säännöksen lisäksi Tanskan lainsäädännössä on olemassa kaksi muutakin mahdollisesti soveltuvaa straffeloven säännöstä palvelunestohyökkäyksellä suoritettuun tekoon. Straffeloven 193 § suojaa hyökkäyksiltä, jotka kohdistuvat kriittiseen infrastuktuuriin, josta maksimirangaistus on kuusi vuotta vankeutta, mutta sitä ei ole koskaan sovellettu tietokoneen välityksellä aiheutettuihin tekoihin. Sen voidaan ajatella soveltuvan tekoihin, jossa henkilö levittää viruksia internetin välityksellä. Kolmas mahdollisesti soveltuva säännös on 293 §:n toinen kappale, jonka mukaan vapaasti suomennettuna rangaistaan sitä, joka oikeudettomasti estää toista hallitsemasta esinettään.[156]

Tanskassa tuomitaan straffeloven 291 §:n 1 kappaleen perusteella tietokoneella luettavassa olevassa muodossa käsiteltävien tietojen vahingoittamisesta ja poistamisesta. Vapaasti suomennettuna vahingonteosta(haervaerk) tuomitaan se, joka tuhoaa, vahingoittaa tai poistaa omaisuutta, joka kuuluu toiselle. Säännös on samankaltainen kuin Suomessa.

> § 291. Den, der ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde eller fængsel indtil 1 år og 6 måneder.
>
> Stk. 2. Øves der hærværk af betydeligt omfang eller af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyldig efter nærværende paragraf eller efter -§ 180, § 181, § 183, stk. 1 og 2, § 184, stk. 1, § 193 eller § 194, kan straffen stige til fængsel i 6 år.
>
> Stk. 3. Forvoldes skaden under de i stk. 2 nævnte omstændigheder af grov uagtsomhed, er straffen bøde eller fængsel indtil 6 måneder.

Tanskassa, säännöksen katsotaan soveltuvan myös tekoihin, joissa tietokoneen käyttö pyritään estämään tietokoneella luettavassa muodossa olevia tietoja vahingoittamalla, poistamalla, heikentämällä, muuttamalla tai estämällä tietojenkäsittely. Esimerkiksi DoS-hyökkäys voisi olla tällä säännöksellä rangaistavissa, riippuen teon luonteesta.[157]

[156] Andersen 2005, s.740.
[157] Lovforslag nr. L 55, Folketinget 2003-2004, s. 43.

291 §:n soveltamisala on laaja. Jos vahinko on huomattava ja on tehty tahallisesti, tuomio voi olla 291 §:n toisen kappaleen perusteella jopa kuusi vuotta vankeutta. Jos teko on johtunut törkeästä huolimattomuudesta, korkein rangaistus on 291 §:n kolmannen kappaleen mukaan kuusi kuukautta vankeutta. 291 § kattaa teot, joissa joku tarkoituksella esimerkiksi levittää virusta tietoverkossa, suorittaa DoS-hyökkäyksen, Ping of Death:n ja tilanteet, joissa käyttäjän pääsy dataan on estetty. Säännös sisältää myös datan ja ohjelmien tuhoamisen.[158]

Kun teko koskee tietojärjestelmän käytön estämistä, tietoa syöttämällä tai siirtämällä, katsotaan teon voivan täyttää, vapaasti suomennettuna, omavaltaisen menettelyn (rådighetshindring), josta on säädetty straffeloven 293 §:n 2 kappaleessa. Säännöksen aiempi sanavalinta ”lägger hinder i vägen” on muutettu, jotta on selvää, että esteen ei tarvitse olla fyysistä laatua, uusi muoto on ”oberättigat hindrar”. Sanamuoto ”helt eller delvis” valittiin, jotta säännös soveltuu myös silloin, kun esimerkiksi palvelunestohyökkäys estää ainoastaan osittain tietokoneen normaalin käyttämisen.[159] Vapaasti suomennettuna, säännöksen mukaan rangaistaan sitä, joka oikeudettomasti estää toista, kokonaan tai osittain vallitsemasta omaisuuttaan. 293 §:n rangaistusasteikko on sakkoa tai 1 vuosi vankeutta. Jos teko on tehty systemaattisesti tai organisoidusti, voidaan rangaistusta korottaa kahteen vuoteen:

> Stk. 2. Den, der uberettiget hindrer en anden i helt eller delvis at råde over ting, straffes med bøde eller fængsel indtil 1 år. Straffen kan stige til fængsel i 2 år, hvor der er tale om overtrædelser af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder.[160]

Jos dataan liittyvä teko aiheuttaa häiriötä yleiseen infrastuktuuriin, eli teleliikenteeseen, postitoimintaan, viesti- tai teleyhteyksiin, radioon tai televisioon, tietojärjestelmiin tai laitoksiin, kuten vesilaitos, kaasu, sähkö, lämmitys, 193 § voi soveltua. 193 §:n maksimirangaistus on kuusi vuotta vankeutta. Törkeästä huolimattomuudesta aiheutuneesta teosta maksimirangaistus on kuusi kuukautta vankeutta. Säännös kattaa tietojärjestelmät tai laitokset jotka ovat tärkeitä yleisölle, esimerkiksi hyökkäykset tietoverkkojen keskustietokoneisiin, palvelimiin ja pankkien tietojärjestelmiin.[161]

---

[158] Spang-Hanssen 2006, s.160.
[159] Lovforslag nr. L 55, Folketinget 2003-2004, s. 64.
[160] https://www.retsinformation.dk/Forms/R0710.aspx?id=113401.
[161] Spang-Hanssen 2006, s.161.

Tanskan lain mukaan, jos teko on tehty systemaattisesti ja organisoidusti, hakkeroinnin voidaan katsoa täyttävän koventamisperusteet. Euroopan unionin puitepäätöksessä koventamisperuteena on toiminta rikollisjärjestön osana, mutta Tanskan lain mukainen tulkinta on laajempi.[162]

7.4. Yhdysvallat

Johtuen Yhdysvaltojen kuulumisesta Common Law -oikeusperheeseen, sen lait ovat huomattavan erilaisia ja kasuistisia verrattaessa pohjoimaiden oikeusjärjestelmiin. Edellä mainitun vuoksi esittelen vain pinnallisesti sen tärkeimmän tietokonerikossäännöksen.

Yhdysvaltojen tärkein tietokonerikoslaki on Computer Fraud and Abuse Act(CFAA), joka säädettiin 11. syyskuuta 2001 tapahtuneen terroristi iskuun liittyen. CFAA suojaa tietokonetta, jota käytetään 1) taloudellisen instituution toimesta, 2) Yhdysvaltojen hallinnon toimesta, 3) tietoliikenteeseen tai Yhdysvaltojen osavaltioiden kanssakäyntiin tai ulkomaiseen kanssakäyntiin. CFAA määrittää rikokseksi vapaasti suomennettuna muun muassa 1) tietomurron, 2) tietomurtoon liittyvän petoksen, 3) tiedonsiirron ja sen yrityksen, ilman oikeutta, jos tarkoituksena on aiheuttaa vahinkoa jne.[163] Muun muassa CFAA voi soveltua DDoS -hyökkäykseen, mutta myös toiset lait voivat soveltua.[164]

Yksi mahdollinen laki Yhdysvalloissa on the Electronic Communications Privacy Act(ECPA) eli niin sanottu wire tap law, jonka mukaan rangaistaan sitä, joka 1)tarkoituksella pysäyttää esimerkiksi elektronisen tietoliikenteen, tai 2)tarkoituksella paljastaa tietoliikenteen sisällön toiselle, tai 3)tarkoituksella ja tietoisesti käyttää tietoa, joka on saatu laittomalla pysäytyksellä ja niin edelleen.[165]

[162] Spang-Hanssen 2006, s.162.
[163] International Guide to Combating Cybercrime 2003, s.16–18.
[164] http://us.practicallaw.com/7-516-9293.
[165] International Guide to Combating Cybercrime 2003, s.28.

8. INTERNETIN KÄYTTÖ TERRORISTISIIN TARKOITUKSIIN

Tässä kappaleessa käsittelen asiaa hieman eri kannalta. Internetiä voidaan käyttää monin eri keinoin esimerkiksi rikolliseen toimintaan, sotatoimissa kuin terrorismissa. Terrorismi internetin välityksellä ei ole päässyt otsikoihin ja siten lainsäädäntöäkään ei ole niin paljon kehitetty. Yhdistyneiden kansakuntien rikosten torjunnasta vastaava järjestö, UNODC, on luokitellut tavat käyttää tietoverkkoja terrorismin apuna, kuuteen osittain päällekkäiseen kategoriaan: propaganda, rahoitus, koulutus, suunnittelu, toimeenpano ja tietoverkkohyökkäykset. Käsite propaganda käsittää värväyksen, radikalisoinnin ja yllytyksen terrorismiin[166]. Otin tähän työhön terrorismia koskevan osion, koska internet on halpa keino terroristisen hyökkäysten tekemiseen ja tällä hetkellä ei ole olemassa yhtenäistettyä kansainvälistä lainsäädäntöä, joka sääntelisi erityisesti terroristisia tietoverkkohyökkäyksiä.

8.1. Terrorismi käsitteenä

Yhdistyneiden kansakuntien pääsihteeri Ban Ki-moon on todennut seuraavaa:

> The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.[167]

Terrorismi ei ole enää valtioiden sisällä tapahtuvaa, vaan siitä on tullut monikansallista. Erityisesti internet, mutta myös nykyaikaiset matkustustavat ovat pienentäneet välimatkoja ja yhdistäneet kansakuntia, mutta myös tuoneet kansalliset ongelmat kansainvälisiksi.

Terrorismin määrittely on vaikea kysymys, koska se sisältää paljon arvolataumia. Kansainvälisesti kattavaan yhteisymmärrykseen terrorismi-käsitteen sisällöstä ei ole päästy. Euroopan unionin terrorismin torjuntaa koskeva puitepäätös vuodelta 2002, sisältää yhdenlaisen määritelmän, koostuen subjektiivisesta ja objektiivisesta osasta:

> .. Puitepäätöksessä käytetty terrorismin käsite koostuu kahdesta osasta:

[166] UNODC 2012, s.3.
[167] UNODC 2012, ks. etusivu.

> objektiivisesta osasta, sillä siinä viitataan vakavien rikosten luetteloon (murha, ruumiinvamma, panttivangin ottaminen, kiristys, aseiden valmistus, terrori-iskujen tekeminen, edellä lueteltujen tekojen tekemisellä uhkaaminen jne.)
>
> subjektiivisesta osasta, sillä kyseisiä tekoja pidetään terrorismirikoksina, kun tekijän tarkoituksena on pelotella vakavasti väestöä, pakottaa aiheettomasti viranomaiset tai kansainvälinen järjestö johonkin tekoon tai pidättymään jostakin teosta tai horjuttaa vakavasti jonkin maan tai kansainvälisen järjestön poliittisia, perustuslaillisia, taloudellisia tai sosiaalisia perusrakenteita tai tuhota ne.[168]

Toinen määritelmä sisältyy terrorismin ennaltaehkäisyä koskevan Euroopan neuvoston yleissopimukseen, jonka voimaansaattamista koskevassa hallituksen esityksessä on todettu seuraavasti:

> ..Artiklan 1 kappaleessa määritetään ”terrorismirikokset,” joilla tarkoitetaan kaikkia liitteessä lueteltujen sopimusten soveltamisalaan kuuluvia ja niiden määritelmien mukaisia rikoksia. Yleissopimus ei sisällä näin määritettyjen terrorismirikosten yleistä kriminalisointivelvoitetta. Sopimuksen 5-7 ja 9 artiklasta johtuu kuitenkin velvoite säätää rangaistaviksi julkinen yllytys terrorismirikokseen, värväys terrorismiin, koulutus terrorismiin sekä eräät näihin tekoihin liittyvät rikokset..[169]

Yllä mainitussa liitteessä luetellaan yhteensä kymmenen YK:n piirissä laadittua yleissopimusta eli sopimuksen määritelmä ei sisällä tietoverkkohyökkäystä terroritekona, vaan ainoastaan aikaisemmin määritellyt sektorisopimukset.

Termiä terrorismi on käytetty lukuisissa yhteyksissä, mutta on olemassa kolme pääasiallista kontekstia, joissa termiä on käytetty kuvaamaan: 1. Totalitääristen kansallissosialistisen ja kommunistisen valtioiden käyttämän sortohallintoa, 2. Sokkitaktiikkaa liittyen epäsäännölliseen sodankäyntiin, 3. Äärimmäisenä protestin ja kiihotuksen muotona.[170]

Lehdon mukaan valtioiden on vaikea päästä terrorismi-käsitteestä yhteisymmärrykseen. Kirjallisuudessa terrorismi esitetään hänen mukaansa viestinnäksi väkivallan keinoin, siinä myös korostetaan terrorismin sotaan liittyviä ominaisuuksia ja terrorismin konteksti riippuvaisia näkökulmia. Hänen mukaan tulisi ymmärtää se, että vaikka YK:n yleiskokouksen päätöslauselmissa lausutaan terrorismista viitaten sen kaikkiin

[168] Europa.eu.
[169] HE 81/2007, s.6.
[170] European Commission’s Expert Group on Violent Radicalisation 2008, s.7.

olomuotoihin ja ilmentymiin sekä YK:n turvallisuusneuvosto on ottanut yhtä laajan näkökannan viitaten mihin tahansa ja kaikkiin terroritekoihin, että kaikki terrorismin ilmentymät eivät ole rikosoikeudellisesti relevantteja.[171]

8.2. Tietoverkkohyökkäys

Tietoverkkohyökkäys on laaja-alainen termi, sisältäen teot, joiden tarkoituksena on hyökätä, tietoverkkoa käyttäen, kohdetta vastaan. Hyökkäyksen tavoitteena voi olla kohteen tarkoituksenmukaisen toiminnan estäminen eri keinoja käyttäen, kuten hakkerointi, virukset, haittaohjelmat[172] ja floodaus[173]. Tietoverkkohyökkäys voi olla terroristiteko, eli teko, johon liittyy halu edistää poliittisia tai sosiaalisia tavoitteita aiheuttamalla pelkoa yhteiskunnassa.[174] Esimerkkinä tietoverkkohyökkäyksestä on Israelissa tapahtunut hyökkäys tammikuussa 2012. Hyökkäys kohdistui Tel Avivin pörssin web-sivuihin, kansalliseen lentoyhtiöön ja tuhansien Israelin kansalaisten luottokortti- ja tilitietoihin.[175]

On tärkeää muistaa, että tietoverkot ovat nykyaikana yhteydessä melkein kaikkiin yhteiskunnan eri toimintoihin. Ne ovat täten elintärkeitä yhteiskunnan toiminnalle, joten niitä tulee myös suojata riittävin keinoin, mutta suojaustoimenpiteiden ei tule ylittää laillisuusperiaatteen asettamia rajoja. Laillisuusperiaate on tärkeä ja suojaa monia perustavanlaatuisia ihmisoikeuksia.

Tehokkailla terrorismin vastaisilla toimilla ja ihmisoikeuksien suojelemisella on sama tavoite, joten molemmat täytyy ottaa vastatoimissa huomioon. Internet voi vaikuttaa lukuisiin eri ihmisoikeuksiin, kuten sananvapauteen, järjestäytymisvapauteen, yksityisyyteen ja oikeudenmukaiseen oikeudenkäyntiin. Tällä hetkellä velvollisuus terroritekojen tekijöiden rankaisemiseksi on kansallisten viranomaisten vastuulla, koska ei

[171] Lehto 2008, s. 62–63.
[172] Kansainvälisen televiestintäliiton dokumentin mukaan, Toolkit for Cybercrime Legislation, haittaohjelma tarkoittaa ohjelmaa, joka asennetaan tietokoneeseen yleensä salaa, tarkoituksena järjestelmän luottamuksellisuuden, eheyden tai ohjelman, datan tai järjestelmän saatavuuden estäminen.
[173] Flooding, tarkoittaa palvelimen tarkoituksellista kuormitusta useilla yhteydenotoilla, jotka jätetään vahvistamatta, kuten kuuluu, jolloin palvelimen yhteydenottojono lopulta täytty y.
[174] UNODC 2012, s.11–12.
[175] New York Times 2012, s. A7.

ole olemassa kansainvälistä tuomioistuinta, jolla olisi universaalitoimivalta terroritekojen suhteen.[176]

Tällä hetkellä kansainvälinen yhteistyö on hyvin aktiivista terrorismin vastaisten yleissopimusten solmimiseksi, jotka sisältävät lainsäädännöllisen perustan myös yhteistyölle tietoverkkorikostapauksissa. Sopimukset eivät kuitenkaan sisällä yksityiskohtaista tietoverkkorikoksia koskevaa lainsäädäntöä, joten tietoverkkorikosten ratkaiseminen nojaa olemassa oleviin kansainvälisiin tai alueellisiin sopimuksiin tai järjestelyihin, jotka on luotu helpottamaan kansainvälistä yhteistyötä terroritekojen tutkinnassa ja syyttämisessä tai järjestäytyneeseen rikollisuuteen liittyvissä teoissa.[177]
Tällä hetkellä Suomen rikoslaissa on säädetty terroristisessa tarkoituksessa tehdystä teosta, joka on kohdistunut esimerkiksi energiahuoltoon, 34 luvun 1 § tuhotyö.

Tietoverkkorikollisuutta ei oteta nykypäivänä riittävästi huomioon yhtenä terroriteon toteuttamisen tekomuotona. Tietoverkkohyökkäys ei suoraan aiheuta fyysisiä vaurioita kenellekään yksilölle, mutta sen aiheuttamat vauriot valtion infrastruktuurille voivat olla vakavat. Hyökkäyksen yhteydessä voidaan pyrkiä varastamaan tietoja, tekemään hyödyttömäksi viranomaisten tietokantoja, hyökätä kansalliseen pörssiin ja niin edelleen. Nykypäivän yhteiskunta toimii markkinatalouden ehdoilla ja toimiva vaihdanta on sen perustana. Sääntelyn tulisi olla yhtenäistä, jotta kansainvälinen yhteistyö onnistuisi parhaiten.

Informaatio ja sen puute on aina ollut osa politiikkaa ja sotatoimia. IW eli Information Warfare on tietoverkkohyökkäyksen yksi muoto ja on tärkeä osa nykyaikaista sodankäyntiä. Tietotekniikan keskeinen asema on luonut nykyaikaisesta yhteiskunnasta haavoittuvan. Sodankäynti perustuu nykypäivänä komentoon, kontrolliin, kommunikaatioon ja tiedustelutietoon, jotka mahdollistavat organisoidut ja koordinoidut sotatoimet. IW kohdistuu ITC:hen ja informaatioinfrastruktuuriin, tavoitteena on tietoliikenteen estäminen tai häirintä, tiedon kaappaus, tai järjestelmän tekeminen toimintakyvyttömäksi.[178] Persianlahden sota oli ensimmäinen sota, johon liittyi vahvasti IW.[179]

[176] UNODC 2012, s.13–15.
[177] UNODC 2012. s.74.
[178] Rathmell 2000, s.219.
[179] Rathmell 2000, s.221.

9. LOPUKSI

Tämä kappale sisältää erinäisiä näkemyksiä aiheeseen liittyen. Professori Wellfordin mukaan yleensä rikosoikeutta kuvatessa poikkitieteelliseksi, ajatellaan sosiaalitieteitä sekä käyttäytymistieteitä, että oikeustieteitä. Niiden avulla ymmärrämme rikollisuuden syitä, jotta voisimme kontrolloida rikollisuutta. Tietoverkkorikollisuuden ymmärtämiseksi tarvitaan kaikkia edellä mainittuja tieteenaloja ja lisäksi niin sanottuja kovia tieteitä, eli insinööri-tieteitä.[180]

Jaakko Husa on jakanut oikeusdogmatiikkaa kohtaan esitetyn kritiikin neljään ryhmään: 1) Oikeustieteen metodit eivät riitä selvittämään yhteiskunnallisesti merkittäviä ongelmia, 2) oikeustiede painottaa liikaa sisäistä näkökulmaa, 3) Oikeustieteen tutkimuskohteena pitäisi olla kaikki oikeudelliset ilmiöt, eivät vain oikeusnormit ja oikeudelliset päätökset, 4) Oikeustieteestä on tehtävä todellinen tiede.[181] Kaijus Ervastin mukaan oikeussosiologia voi auttaa ymmärtämään oikeudellisia ilmiöitä tavalla, jota perinteinen oikeustiede ei tee. Oikeussosiologia täydentää oikeusdogmatiikkaa oikeustieteen sisällä ja myös kilpailee oikeusdogmatiikan kanssa tulkinnoista. [182]

Johtuen kuitenkin aiheeseen liittyvien ongelmakenttien moniulotteisuudesta tässä tutkielmassa ei ole mahdollisuutta paneutua aiheeseen, sen vaatimalla syvyydellä, joten tässä kappaleessa käsittelen asiaa lähinnä pohdinnan kautta ja yleisesti käytännön näkökulmasta. Tekniseltä kannalta olen asiaa käsitellyt jo alkukappaleessa.

9.1. Esitelmät

Keskusrikospoliisin rikosylikomisario Timo Virtanen on todennut KRP:n vastuulla olevan rikosjutut liittyen järjestäytyneeseen rikollisuuteen, laajoihin kansainvälisiin tapauksiin, ennakkotapausjuttuihin ja yksittäisiin vakaviin rikoksiin. Ongelmana on erityisesti järjestäytyneen rikollisuuden määrittäminen eli vähintään 3 henkilön muodostama,

[180] McQuade III 2006, s.x.
[181] Husa 1995, s. 141–142.
[182] Ervasti 2012, s. 21–23.

organisoitunut, tiiviisti toimiva ryhmä. Verrattaessa EU:n määritelmään nousee kysymyksiä. Nykyään rikollisten eliitillä on käytössään huomattavat taloudelliset resurssit ja kansainvälistymisen lisäksi teknologian lisääntyvä käyttö on konkretisoitunut useissa KRP:n jutuissa. Tulevaisuuden haasteena ovat erityisesti tietoverkkorikokset. Ongelmana JR:n tutkimisessa on ns. vajaa työkalupakki, JR:n tutkinnassa olisi tarvetta omille ETL:n säännöksillä. Toisaalta on ongelmana JR:n tunnistaminen, eivät he mainosta itseään.[183]

Keskusrikospoliisin tutkintaosaston tietotekniikkarikosjaoksen esimies, rikoskomisario Timo Piiroinen on todennut vakavien tietotekniikkarikosten esitutkinnan jakautuvan kriittiseen infrastruktuuriin kohdistuvaan, JR:n epäillyksi tekemiin, tietoverkkopetoksiin. Tietoteknisissä jutuissa datan määrä on räjähtänyt, vuonna 2007 noin 7 TB[184], 2008 noin 116 TB. Dataa tulee tietokoneista, älypuhelimista ja muista lähteistä, esimerkiksi palveluntarjoajilta. JR tekee kohdennettuja hyökkäyksiä, esimerkiksi yritysvakoilua, valtiollista vakoilua, haittaohjelmia. Palvelunestohyökkäyksiä tekevät yksittäiset juniorit ajattelemattomuuttaan ja JR harhautustarkoituksessa, peittämään tekojaan. Asperger-oireyhtymää sairastavilla on alttius tietokonerikosten tekemiseen. DDoS -palkkausta ei ole ollut Suomessa, ehkä ulkomailla?[185]

Aspergerin oireyhtymä kuuluu autistisiin häiriöihin. Autistisille häiriöille on luonteenomaista laadulliset poikkeavuudet sosiaalisessa vuorovaikutuksessa ja yhteydenpitotavoissa sekä kaavamaiset harrastukset ja muut toiminnot. Aspergerin oireyhtymään ei liity kielen kehityksen viivästymää, kuten muihin autistisiin häiriöihin. Aspergerin oireyhtymää sairastavat lapset ovat usein motorisesti kömpelöitä, kielen rytmi, painotus, äänen käyttö sekä sointi ovat selvästi poikkeavia, että ilmeet, eleet ja liikkeet. He ovat yleensä älykkyydeltään normaaleja, mutta suorituskykyä leimaa kuitenkin usein epätasaisuus, osalla on jollain erityisalueella erityistä lahjakkuutta ja erityiskykyjä. Aspergerin oireyhtymää sairastavilla lapsilla on usein uitakin psyykkisiä häiriöitä, kuten ADHD:tä, masentuneisuutta, pakko-oireita ja Touretten oireyhtymää. [186]

[183] Rikosylikomisario Timo Virtasen esittely.
[184] TB tarkoittaa teratavua.
[185] Rikoskomisario Timo Piiroisen esittely.
[186] Aronen & Sourander 2009, s.584–585.

Aspergerin oireyhtymä on luonteeltaan pysyvä, ja siitä kärsivillä ilmenee myös aikuisena vaikeuksia ymmärtää toisten ihmisten tunteita, minkä tuloksena on vaikeuksia ihmissuhteissa[187]

Mitä kaikesta edellä mainitusta voidaan päätellä? Liittyykö sosiaalinen eristyneisyys alttiuteen tietotekniikkarikoksien tekemiseen? Asia on joka tapauksessa tiedostettu myös ulkomailla.[188] Joka tapauksessa ainoastaan Aspergerin oireyhtymää sairastavat eivät liene ole syyntakeettomia, rikosoikeuskomitean mietintö:

> Syyntakeeton on sellainen henkilö, jolta on siinä määrin puuttunut kyky tajuta tekonsa tosiasiallinen tai moraalinen luonne taikka puuttunut käyttäytymisen vapaus, että olisi kohtuutonta kohdistaa häneen moitetta. [189]

ja lisäksi mietinnössä on todettu:

> Ratkaisevaa olisi, missä määrin sairaus ilmenisi henkilön vähentyneenä kykynä käsittää ja ymmärtää asioiden tosiasiallinen ja moraalinen luonne sekä säädellä käyttäytymistään.[190]

Rikoslain 3 luvun 4 § mukaan:

> Tekijä on syyntakeeton, jos hän ei tekohetkellä kykene mielisairauden, syvän vajaamielisyyden taikka vakavan mielenterveyden tai tajunnan häiriön vuoksi ymmärtämään tekonsa tosiasiallista luonnetta tai oikeudenvastaisuutta taikka hänen kykynsä säädellä käyttäytymistään on sellaisesta syystä ratkaisevasti heikentynyt[191]

Asperger oireyhtymästä kärsivien älykkyysosamäärä on kuitenkin normaalin ja normaalia huomattavasti älykkäämmän välillä. He ovat ennemmin potentiaalisia uhreja kuin rikoksen tekijöitä.[192]

---

[187] Huttunen 2013.
[188] Gary Mckinnonia ei luovutettu Yhdysvaltoihin hakkeroituaan NASA:n ja Yhdysvaltain armeijan tietojärjestelmiä. Hänellä diagnosoitiin Aspergerin oireyhtymä ja masennus. Iso-Britanniassa häntä ei paikallisen lainsäädännön mukaan voitu myöskään syyttää. Hylkäävä luovutuspäätös on perusteltu ihmisoikeusperusteella. http://www.theguardian.com/world/2012/dec/14/gary-mckinnon-no-uk-charges http://articles.latimes.com/2012/oct/16/world/la-fg-britain-hacker-20121017.
[189] Rikoskomiteamietintö 1976:72.
[190] Rikoskomiteamietintö 1976:72.
[191] Rikoslaki 19.12.1889/39.
[192] http://www.aane.org/asperger_resources/articles/miscellaneous/as_in_the_criminal_justice_system.html.

9.2. Pohdinta

Tämän tutkielman aiheena on tietojärjestelmän häirintä, sen törkeä tekomuoto ja tietoliikenteen häirinnän tekomuodot lievästä törkeään. Tutkielman aihe oli helppo valinta koska päätöstä tehdessäni EU:n parlamentti käsitteli direktiiviehdotusta tietojärjestelmiin kohdistuvista hyökkäyksistä, jossa oli aikomus muuttaa tietoliikenteen häirinnän rangaistusasteikkoa.

Euroopan unioni tulee ankaroittamaan rangaistuksia ja panostamaan tulevaisuudessa huomattavan paljon tietoverkkorikollisuuden vähentämiseen sekä esitutkintaan, että kansainvälisen yhteistyön tehostamiseen. Suomessa 24/7 toimiva yhteyspiste on ollut jo pitkään keskusrikospoliisi, joka täyttää tulevan direktiiviehdotuksen vaatimukset, toisin kuin on laita monessa muussa jäsenmaassa. Direktiiviehdotuksen tullessa voimaan, voidaan olettaa tietoverkkorikosten selvittämisen ajan kuluessa helpottuvan ja myös RL 38 luvun 7 a § ja 38 luvun 7 b § tulevan useammin sovellettavaksi. Tietoverkkorikokset ovat luonteeltaan sellaisia, että ne ovat suhteellisen pienin resurssein suoritettavissa siten, että ilman nopeaa ja tehokasta yhteistyötä rikosten selvittäminen on erittäin vaikeaa. Tietotekniikka tarjoaa nykypäivänä monia työkaluja sekä DDoS -hyökkäysten suorittamiseksi, että jälkien peittämiseksi, joten rikosten selvittäminen on varsin haasteellista vähäisin resurssein.

Suomen rikoslain 38 luvun 7 a § ja 38 luvun 7 b § ovat unionin oikeutta ja täten kansallinen tuomari myös EU-tuomari ja EU-oikeuden soveltaja. Nykyään se unohtuu. Direktiiviehdotuksen tultua hyväksytyksi ja säädetyn täytäntöönpanoajan kuluttua, EU:n tietoverkkorikoslainsäädännöstä tulee osa Suomen rikoslakia, laillisuusperiaatteen mukaisin rajoituksin. Tällöin on kansallisen tuomarin otettava soveltamiskysymyksissä huomioon yhä enenevässä määrin tulkintakysymyksissä EU-oikeus ja sen etusija suhteessa kansalliseen oikeuteen. Tällä hetkellä EU-oikeus vaikuttaa ainoastaan puitepäätökseen liittyvän tulkintavaikutuksen kautta ja kuten edellä todettu, laillisuusperiaate vaikuttaa ainoastaan meneteltäessä syytetyn vahingoksi, joten tulkintavaikutus täytyy ottaa huomioon sovellettaessa Suomen rikosoikeutta.

Rangaistuksen yleisestävän vaikutuksen tehokkuuden edellytysten luokittelu on Vuorenpään mukaan jossain määrin vaihdellut esittäjästä riippuen, mutta hän on esittänyt seuraavien ehtojen olevan merkityksellisiä yleisprevention syntymiselle:

1)normituntemus;
2)sanktiovarmuus;
3)sanktioankaruus;
4)rangaistuksen tuomitsijan kokeminen auktoriteetiksi;
5)rikosoikeudellisen järjestelmän legitiimisyys;
6)rangaistusten mieltäminen moitteeksi; sekä
7)rangaistaviksi määrättyjen tekojen kokeminen paheksuttaviksi.[193]

Kuinka paheksuttavaksi tekijä katsoo, jossain kaukana rangaistavaksi määrätyn teon? Uuden tietoverkkohyökkäyksiä koskevan direktiivin myötä myös rangaistukset tulevat kovenemaan. Tietoverkkorikoksia pohtiessa, tulee myös mieleen sanktiovarmuuden merkitys. Mikä on tietotekniikkarikoksista kiinnijäämisen riski, kun melko suuri osa teoista jää ilmoittamatta ja suurin osa rikosilmoituksista ei etene syyttäjälle asti.[194]

Vuorenpään mukaan: ”rikosoikeudellisen järjestelmän hyväksyttävyyden ajatellaan olevan omiaan edistämään ihmisten omaehtoista lainnoudattamishalukkuutta.”[195] Kuinka hyväksyttävä voi olla rikosoikeudellinen järjestelmä, joka on luotu silmällä pitäen EU:n yhtenäistä politiikkaa?

Nykyinen arvojärjestelmä perustuu perus- ja ihmisoikeuksiin, jotka ilmaisevat yleisesti hyväksyttyjä arvoja ja käsityksiä.[196] Vuorenpään mukaan ihmisoikeusperiaatteilla katsotaan olevan keskeisin merkitys rikosoikeudellisen järjestelmän legitiimisyyteen kuuluvia tekijöitä määriteltäessä.[197]

[193] Vuorenpää 2007, s.26.
[194] Ks. tilastotietoa-kappale.
[195] Vuorenpää 2007, s.85.
[196] Vuorenpää 2007, s.86.
[197] Vuorenpää 2007, s.87.

LIITTEET

LIITE: Syyteratkaisut

Vuodesta 2006 vuoteen 2012 lievästä tietoliikenteen häirinnästä, tietoliikenteen häirinnästä, törkeästä tietoliikenteen häirinnästä, tietoliikenteen häirinnästä, törkeästä tietojärjestelmän häirinnästä tehdyt syyteratkaisut, käräjäoikeus-asiat, käräjäoikeudessa annetut hylkäävät tuomiot, syyttämättäjättämispäätökset, esitutkinnanrajoittamispäätökset ja muut päätökset. Taulukkoon on kirjattu tiedot ainoastaan, mikäli tapauksia on ollut. Lähde: Valtakunnansyyttäjänviraston tietojärjestelmä.

Vuosi	Rikosnimike	Ko-asiat	Ko-hylyt	SJP	ETR	Muu
2 006	TIETOLIIKENTEEN HÄIRINTÄ	6	0	7	1	1
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	1	0	0	0	0
2007	TIETOLIIKENTEEN HÄIRINTÄ	2	0	2	1	0
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	0	0	0	1	0
2008	TIETOLIIKENTEEN HÄIRINTÄ	2	0	2	3	2
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	0	0	0	1	0
2009	TIETOLIIKENTEEN HÄIRINTÄ	1	0	1	3	2
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	1	0	0	1	2
	LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	0	0	1	1	0
	TIETOJÄRJESTELMÄN HÄIRINTÄ	0	0	0	1	0
2010	TIETOLIIKENTEEN HÄIRINTÄ	5	2	1	3	0
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	2	0	0	0	0
	TIETOJÄRJESTELMÄN HÄIRINTÄ	2	1	0	1	0
2011	TIETOLIIKENTEEN HÄIRINTÄ	3	0	0	3	3
	LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	3	0	0	2	0
	TIETOJÄRJESTELMÄN HÄIRINTÄ	0	0	0	2	0
2012	TIETOLIIKENTEEN HÄIRINTÄ	7	0	1	5	1
	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	4	1	1	0	1
	LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	1	1	0	0	0
	TIETOJÄRJESTELMÄN HÄIRINTÄ	1	0	0	0	0