Tartu Ülikool

Õigusteaduskond

Avaliku õiguse instituut

Katrin Kabel

EESTI KARISTUSSEADUSTIKU §-de 208 JA 216[1] VASTAVUSEST EUROOPA NÕUKOGU ARVUTIKURITEGEVUSEVASTASE KONVENTSIOONI ARTIKLILE 6.2 VÕITLUSES KÜBERKURITEGEVUSEGA

Bakalaureusetöö

Juhendaja: *Mag. iur* Lauri Aasmann

Tallinn

2013

Sisukord

SISSEJUHATUS

Viimase kümnekonna aastaga on küberkuritegevuse levik ja küberrünnete ohtlikkuse aste plahvatuslikult suurenenud[1] ning sellest tingituna suunavad riigid üha suuremaid ressursse küberturvalisuse tagamisse. Täna igapäevaseks kujunenud teated turvalisuse poolest maailmas esirinnas arvatud olevate asutuste ja organisatsioonide langemisest küberrünnete sihtmärgiks on nähtus, millega võitlemiseks enamusel riikidel puuduvad kogemused ning napib spetsialiste.

Üheks esimeseks riikide küberkuritegevuse ohjamise suunalisi püüdlusi koondavaks poliitilise tasandi kokkuleppeks tuleb pidada Euroopa Nõukogu 23.11.2001.a. vastu võetud Arvutikuritegevusevastast konventsiooni[2], millega alustati ühise kriminaalpoliitika väljatöötamist võitluses arvutikuritegevuse vastu. Eesti Vabariik ratifitseeris nimetatud konventsiooni 12.02.2003.a ning see jõustus 01.07.2004.a.

Põhinedes suuresti kõnealusele konventsioonile, on Eesti karistusseadustikku (edaspidi KarS)[3] lisatud arvutikuritegude süüteokoosseisud, mis käsitlevad arvutiandmetesse sekkumist (§ 206); arvutisüsteemi toimimise takistamist (§ 207); nuhkvara, pahavara ja arvutiviiruse levitamist (§ 208); arvutikelmust (§ 213); arvutikuriteo ettevalmistamist (§ 216[1]) ja arvutisüsteemi ebaseaduslikku kasutamist (§ 217).

Käesolev töö keskendub ühele eranditest, mille Eesti kriminaalseadus on otsustanud teha võrreldes konventsiooni originaaltekstiga. Nimelt välistab konventsiooni artikkel 6 teine lõige kriminaalkaristuse kohaldamise, kui konventsiooni mõttes kuriteo toimepanemise vahendiseks oleva seadme või programmi tootmise, müügi, kasutamiseks hankimise, impordi või turustamise või muul viisil kättesaadavaks tegemise või valdamise eesmärk on näiteks arvutisüsteemi lubatud katsetamine või arvutisüsteemi kaitse, mitte konventsiooni artiklites 2–5 nimetatud kuriteo toimepanemine. Eesti vastavat reeglit otsesõnu üle võtnud ei ole, vaid eristab üldjuhul karistusseadustiku arvutikuritegude koosseisudes lubatud ja lubamatut tegevust omadussõna „ebaseaduslik“ abil.

Käesoleva bakalaureusetöö hüpoteesiks on, et karistusseadustiku KarS § 208 toodud kuriteokoosseisu kriminaliseerimine ilma EN Arvutikuritegevusevastases konventsioonis toodud reservatsioonita, ei ole põhjendatud. Läbi sellekohase õigusanalüüsi püüab autor jõuda

[1] W. Gragido, J. Pirc. Cybercrime and Espionage. An Analysis of Subversive Multivector Threats. Syngress Publications 2011, lk 10

[2] Euroopa Nõukogu Arvutikuritegevusevastane konventsioon.- RT II 2003, 9, 32, arvutivõrgus kättesaadav: https://www.riigiteataja.ee/akt/550359 (21.03.2013)

[3] Karistusseadustik.- RT I 2001, 61, 364…RT I, 20.12.2012, 12, arvutivõrgus kättesaadav: https://www.riigiteataja.ee/akt/120122012012 (21.03.2013)

selgusele, kas töö kirjutamise ajal kehtiva KarS § 208 sõnastus on ülemäära piirav ning ei arvesta vajadusega läbi viia infosüsteemide turvatestimisi ega kasutada jälitustegevuse toiminguid näiteks infotehnoloogiavahenditest teabe salajaseks hankimiseks.

Nagu töö pealkiri viitab, on nuhkvara, pahavara ja arvutiviiruse levitamise ning töö uurimisküsimusega lahutamatult seotud ka karistusseadustiku § 216[1] koosseis, mis käsitleb arvutikuriteo, s.h KarS § 208 kirjeldatud levitamise, ettevalmistamist. Kriminaalkaristust vääriva arvutikuriteo ettevalmistamisena kirjeldab karistusseadustik tegevusi nagu näiteks nuhkvara valmistamine või isegi valdamine, mis tänaseks päevaks on kujunenud osaks küberturbeekspertide igapäevatööst.

Illustreerimaks probleemistiku aktuaalsust ja praktilist kaalu väljaspool tsiviil- või õiguskaitsesfääri, keskendub töö teisalt nuhkvara, pahavara või arvutiviiruse levitamisele riikliku julgeoleku strateegiliste eesmärkide saavutamiseks kübervõimekuse arendamisel ja küberoperatsioonide läbiviimisel. Näited niisugusest praktikast põhinevad USA avalikest allikatest kättesaadavatel andmetel küberväeosade kujundamise ja küberarsenali loomise kohta.[4]

Kuivõrd suur osa kurjategijatest, s.h rahvusvahelised terrorirühmitused kasutavad oma tegevuse hõlbustamiseks internetti ning infotehnoloogiavahendeid, samuti arvestades küberintsidente, mille tagamaad viitavad riikliku mandaadi olemasolule, on kübervõimekuse arendamine nii tsiviil- kui militaarvaldkonnas loogiline suund, mille riigid strateegilisel tasemel võtavad. Uue relvaliigi väljatöötamine toob kaasa omamoodi lumepalliefekti ning tänaseks on riikide mastaapset tegevust kübervõimekuse arendamisel hakatud võrdlema Teise Maailmasõja järgse võidurelvastumisega. Vastavatest püüdlustest ei tee saladust USA[5] ega muud arenenud riigid. Ametlikult ei loo Eesti küberrelvi[6], kuid kui selleks peaks tekkima vajadus või soov, siis käsitleks käesoleval ajal kehtiv karistusseadustik sellist tegevust kuritegelikuna eelkõige KarS § 208 valguses.

Eeltoodut arvestades püstitatakse uurimistöös küsimus, kas KarS § 208 väljatoodud tegevuse eranditu kriminaliseerimine ei pärsi riigi võimet end kaitsta, ehk kas isikud, kes näiteks loovad või soetavad pahavara, testimaks ühe või teise asutuse infosüsteemi turvalisust, rikuvad oma tegevusega seadust ning riskivad saada kriminaalkorras karistatud?

---

[4] J. L. Bayuk, J. Healy, P. Rohmeyer, M. H. Sachs, J. Schmidt, J. Weiss. Cyber Security Policy Guidebook. A John Wiley&Sons,Inc., Publications 2012, lk 233-235

[5] N. Burns & J. Price. Securing Cyberspace. A New Domain for National Security. The Aspen Institute 2012, lk 54

[6] Sarnaselt paljude muude küberkaitse valdkonnas ringlevate mõistetega, ei ole küberrelval ühtset kokkulepitud vastet. Reeglina mõistetakse selle all koodi või programmi, mida kasutatakse või mida saab kasutada objektidele, süsteemidele või elusolenditele füüsilise, funktsionaalse või moraalse kahju tekitamiseks või sellise kahju tekitamisega ähvardamiseks.

Töö kirjutamisel on kasutatud Tartu Ülikooli andmebaaside kaudu kättesaadavaid teadusartikleid, mis käsitlevad küberõigust ning sellega seotud küsimusi, samuti on kasutatud NATO Küberkaitsekeskuse publikatsioone. Suures osas toetub töö internetis avaldatud artiklitele, mis töö sisu arvestades on paratamatu, kuna alternatiivseid, s.h teadusallikaid ei ole olemas või on uuritav informatsioon piiratud käibega. Töös on kasutatud Eesti kohtupraktikat ning analüüsitud KarS § 208 rakendamist Riigikohtu kriminaalkolleegiumi ainsas selleteemalises lahendis 3-1-1-85-08 (25.02.2009).

Töö esimeses osas on toodud ära põhilised mõisted, mille määratlemine hõlbustab töö edasist lugemist. Uurimisobjektiks oleva KarS-i puudutava õigusliku küsimuse konteksti paigutamiseks on töös järgnevalt välja toodud Eesti Küberjulgeoleku strateegia 2008-2013, EL Küberkaitse strateegia, EN Arvutikuritegevusevastase konventsiooni ja EL 2005.a raamotsuse[7] põhilised küberkuritegevusele keskenduvad seisukohad. Autori hinnangul kinnitavad need dokumendid maailmas järjest suurenevat muret küberruumis leviva kuritegevuse pärast ning on tõestuseks siseriiklikust ja rahvusvahelisest püüdlusest antud nähtusega võidelda ning seda õiguslikult reguleerida. Ühtlasi tunnistavad nimetatud materjalid, et riigid on tegelemas strateegilisel tasandil kübervõimekuse arendamisega, mis sageli tähendab nii kaitse- kui ründemehhanismide väljatöötamist, olgugi, et viimast sageli kõva häälega välja ei öelda.

Töö teises osas on välja toodud põhjused, miks peaks teatud juhtudel olema lubatud küberrelvade kasutamine, antakse ülevaade erinevatest turvatestimise võimalustest ning tuuakse välja küberrelvastumise näiteid erinevate riikide põhjal.

Töö kolmas osa on karistusseadustiku § 208 ja § 216[1] koosseisuelementide analüüs, mis püüab leida vastust küsimusele, kas kehtiv õigus on piisavalt paindlik välistamaks IT-spetsialistide kriminaalvastutust olukorras, kus viimased käitlevad nuhkvara, pahavara või arvutiviiruseid oma igapäevatöö raames.

[7] Euroopa Liidu Nõukogu 24.02.2005 raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta, arvutivõrgus kättesaadav http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ET:PDF (18.05.2013)

1. KÜBERKURITEGEVUS- MÕISTED, STRATEEGIAD

1.1 Küberkuritegevusega seotud mõisted

Et paremini mõista töös läbivalt kasutatud termineid, on alljärgnevalt avatud kolme olulisema mõiste (küberjulgeolek, küberkuritegevus, küberrünne) sisu nii nagu need on defineeritud Eesti küberjulgeoleku strateegias 2008-2013[8].

Küberjulgeolek (riigi küberjulgeolek) – mõiste küberjulgeolek hõlmab kõiki elektroonilise teabe, teabekandjate ning -teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut. Riigi küberruumi julgeoleku tagamine koosneb mitmesugustest tegevustest eri tasanditel. Peamine eesmärk on vähendada küberruumi haavatavust, st ennetada küberrünnakuid ning taastada rünnakute korral võimalikult kiiresti infosüsteemide toimimine. Küberjulgeoleku tagamiseks on oluline hinnata riigi kriitilise infoinfrastruktuuri haavatavust, panna paika vastumeetmete süsteem küberrünnakute ärahoidmiseks, määratleda ametkondadevaheline koostöö riigis ning tööjaotus era- ja avaliku sektori vahel küberrünnakute tõrjumisel, arendada rahvusvahelist seadusandlust ja institutsionaalset koostööd, teavitada avalikkust ning töötada välja küberjulgeoleku alased koolitusprogrammid.[9]

Eesti tunnustatumaid kübervaldkonna õiguseksperte Eneken Tikk on oma doktoritöös väitnud, et küberjulgeoleku mõiste ja olemus on viimaste aastatega oluliselt muutunud. Infoühiskond on arenenud faasi, milles riik ja ühiskond tervikuna on muutunud infotehnoloogiliselt haavatavaks. Ühtlasi on ootuspäraselt sagenenud riikliku tähtsusega infosüsteemide ja elutähtsate infoühiskonna teenuste vastu suunatud poliitilise konteksti ja motivatsiooniga ründed. Seega ei piirdu küberohud enam üksnes arvutikuritegevusega, vaid hõlmavad ka ohte riigi julgeolekule ning võivad riikide sõjaliste võimete arendamise tulemusena eskaleeruda sõjapidamiseks küberruumis.[10]

Täna veel puuduvad andmed juhtumite kohta, kus küberründed üksi oleksid ohustanud riigi julgeolekut, küll aga on taolist eeldust arvesse võttes hetkel kehtiva karistusseadustiku reguleerimisala oluliselt laiem kui peamiselt rahalisele kasule suunatud arvutikuritegevus.

Küberkuritegevus - majandusliku kasu saamise eesmärgil toime pandud järgmised kuriteod:

---

[8] Küberjulgeoleku strateegia 2008-2013, lk 41, arvutivõrgus kättesaadav: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013(1).pdf (24.03.2013)

[9] *op. cit*., lk 40

[10] E. Tikk. Comprehensive legal approach to cyber security. Tartu Ülikooli Kirjastus 2011, lk 133

1) arvutisüsteemi vastu suunatud kuriteod (häkkimine, näotustamine);
2) arvutisüsteemi vahendusel toime pandud kuriteod (arvutikelmus, identiteedivargus, interneti vahendusel vaenu õhutamine jne);
3) autoriõiguste vastu suunatud kuriteod.[11]

Küberrünne – arvutisüsteemi (arvuti, arvutivõrk) vahendusel toime pandud rünne arvutisüsteemi või selles sisalduvate andmete vastu eesmärgiga häirida arvutisüsteemi tööd või muuta õigusliku aluseta andmetöötlusprotsessi (muutmine, kustutamine, sulustamine jne).[12]

1.2 Küberkuritegevusevastase võitluse alusdokumendid

1.2.1 Eesti küberjulgeoleku strateegia 2008-2013

Kaitsmaks Eesti küberruumi küberterrorismi eest ning ühtlustamaks valdkonnas tegutsevate kaitseorganite tööd, on Vabariigi Valitsus kinnitanud küberjulgeoleku strateegia aastateks 2008-2013. Küberjulgeoleku strateegia sõnastab küberjulgeoleku strateegilised eesmärgid ning abinõud Eesti küberruumi haavatavuse vähendamiseks. [13]

Kokkuvõtvalt on strateegia põhilisteks eesmärkideks aastateks 2008-2013 turvameetmete süsteemi arendamine ja laiaulatuslik rakendamine, küberjulgeoleku alase kompetentsuse tõstmine, küberjulgeoleku tagamiseks vajaliku õigusruumi täiendamine, rahvusvahelise koostöö arendamine ja teavitustegevus.

Küberjulgeolek Eesti jaoks on laia tähendusväljaga mõiste, mis hõlmab kõiki elektroonilise teabe, teabekandjate ning teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut. Riigi küberruumi julgeoleku tagamine koosneb mitmesugustest tegevustest eri tasanditel. Olulisemad neist on küberruumi haavatavuse vähendamine, küberrünnakute ennetamine ning infosüsteemide toimimise võimalikult kiire taastamine rünnakute korral. Küberjulgeoleku tagamiseks on vaja hinnata riigi kriitilise infrastruktuuri haavatavust, kavandada ennetavate meetmete süsteem küberrünnakute ärahoidmiseks ja määrata kindlaks riigisisene tööjaotus küberjulgeoleku korralduses. Tähtis on ka täiendada küberjulgeoleku

[11] E. Tikk. Comprehensive legal approach to cyber security. Tartu Ülikooli Kirjastus 2011, lk 41
[12] Küberjulgeoleku strateegia 2008-2013, lk 41, arvutivõrgus kättesaadav http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013(1).pdf (24.03.2013)
13 arvutivõrgus kättesaadav http://www.eata.ee/eesti-nato-s/kuberjulgeoleku-strateegia (24.03.2013)

tagamiseks vajalikku õigusruumi, arendada rahvusvahelist ja institutsionaalset koostööd, teavitada avalikkust ning töötada välja küberjulgeoleku alased koolitus- ja teadusprogrammid.[14]

Käesoleva töö seisukohast omavad eelnevast lõigust tähtsust eelkõige kaks asjaolu:

- vajadus kavandada ennetavate meetmete süsteem küberrünnakute ärahoidmiseks;
- vajadus täiendada küberjulgeoleku tagamiseks vajalikku õigusruumi.

Erialasest kirjandusest ning vestlustest küberkaitseekspertidega on töö autorile selgeks saanud, et tehnilisi võimalusi küberrünnakute ärahoidmiseks on rohkem kui üks ning nende seas on nii passiivse kui ka aktiivse kaitse meetodeid. Vajadus kavandada ennetavate meetmete süsteem küberrünnakute ärahoidmiseks hõlmab vähemalt ülesehituse faasis kokkupuudet KarS §-ga 208 ja/või 216[1], mistõttu on töös käsitletavad küsimused relevantsed küberjulgeoleku strateegia rakendusplaani seisukohast ning haakuvad otseselt strateegias viidatud vajadusega üle vaadata ning täiendada küberjulgeoleku tagamist toetav õigusruum.

Käeoleva aasta 21. märtsil kiitis Vabariigi Valitsus heaks „Küberjulgeoleku strateegia 2014-2017“ koostamise ettepaneku[15] ning määras uue strateegia koostamise eest vastutavaks ministeeriumiks Majandus- ja Kommunikatsiooniministeeriumi. Uuendatud strateegia koos selle rakendusplaaniga peab olema Vabariigi Valitsusele esitatud hiljemalt 2013.a detsembris.

1.2.2 **Euroopa Liidu Küberkaitse strateegia**

Töö valmimise seisuga kõige värskem Euroopa riikide küberruumi turvalisuse parandamisele suunatud ja riikide vastavaid püüdlusi kajastav dokument on Brüsselis 07.02.2013 koostatud Euroopa Liidu Küberkaitse strateegia (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*). Antud strateegia eesmärgiks on juhtida tähelepanu asjaolule, et kuivõrd küberkuritegevus on muutunud järjest suurenevaks julgeolekuohuks, on vajalik riikidevaheline kooskõlastatud ja ühtne tegutsemine, võitlemaks

[14] Küberjulgeoleku strateegia 2008-2013, lk 7-8, arvutivõrgus kättesaadav http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013(1).pdf (24.03.2013)

[15] „Küberjulgeoleku strateegia 2014-2017“ koostamise ettepaneku heakskiitmine.- RT III, 26.03.2013, 9. Arvutivõrgus kättesaadav https://www.riigiteataja.ee/akt/326032013009

internetist tulenevate ohtudega. Strateegias pannakse paika ELi ühine lähenemisviis digitaalvõrkude turbe, internetikuritegevuse tõkestamise ja tarbijakaitse küsimustes.[16]

Tegemist on raamdokumendiga, millest saavad tuge liikmesriigid oma siseriiklike küberjulgeoleku alaste strateegiate ja/või normatiivaktide kujundamisel. Olles Euroopas infotehnoloogia arengu ja ka vastavate turvalahenduste poolest esirinnas, on paljud EL Küberkaitse strateegias nimetatud tegevused juba kajastamist leidnud Eesti küberjulgeoleku strateegias 2008-2013. Sellele vaatamata annab EL vastvalminud strateegia tugeva pidepunkti korrakaitse- ja julgeolekuasutustele täna kasutatavate tehniliste lahenduste, tööprotsesside ning õigusaktide ülevaatamiseks ning vajadusel ettepanekute tegemiseks nende kaasajastamiseks.

Küberturvalisusega seotud pingutused Euroopa Liidus hõlmavad ka küberkaitse mõõdet. Et suurendada liikmesriikide kommunikatsiooni- ja informatsioonisüsteemide vastupanuvõimet, mis tagavad liikmeriigi kaitse ja rahvusliku julgeoleku huvisid, peab küberkaitse võimekuse areng olema keskendunud avastamisele, reageerimisele ja toibumisele keerulistest küberohtudest.[17]

Küberkuritegevuses kasutatavate tehnikate areng on järsult kiirenenud: korrakaitsjad ei saa küberkuritegevusega võidelda vananenud vahenditega. Praegusel hetkel ei ole kõikidel Euroopa Liidu liikmesriikidel operatiivseid vahendeid, mis on vajalikud küberkuritegevusele reageerimiseks. Kõik liikmesriigid vajavad efektiivset siseriiklikku küberkuritegudega tegelevat üksust.[18] Kahtlemata kuulub efektiivselt rakendatav õigusraamistik küberkuritgeevusevastase võitluse vahendite hulka.

1.2.3 Euroopa Nõukogu Arvutikuritegevusevastane konventsioon

Konventsiooni ettevalmistamine oli pikk protsess, võttes aega neli aastat ning kakskümmend seitse eelnõud enne kui viimane versioon, mis kuupäevastati 25. mail 2001

[16] Euroopa Liidu Küberkaitse strateegia (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace), a*rvutivõrgus kättesaadav http://ec.europa.eu/news/science/130212_et.htm (22.03.2013)
[17] o*p. cit.*, (24.03.2013)
[18] *op. cit.,* (24.03.2013)

aastal, oli esitatud Euroopa Kriminaalprobleemide Komiteele *(European Comittee on Crime Problems - CDPC)* selle 50ndal plenaaristungil 18.-22.juuni 2001.aastal.[19]

Arvutikuritegevusevastane konventsioon[20] võeti vastu 23.22.2001.a. See on ainus rahvusvaheliselt siduv leping antud teemal, mis on käesolevaks ajaks vastu võetud. Konventsioon on allkirjastamiseks avatud ka mitte-Euroopa riikidele ning käesolevaks hetkeks on allakirjutanuid 47, kellest 37 on konventsiooni ratifitseerinud. Konventsioon sisaldab juhiseid, sealhulgas seadusandlikke suuniseid kõigile valitsustele, kes soovivad ennast kaitsta küberkuritegevuse vastu. Konventsiooni eesmärk taotleb ühtset kriminaalpoliitikat eelkõige läbi asjakohase seadusandluse vastuvõtmise ning kiire ja efektiivse rahvusvahelise koostöö. Nimetatud eesmärgi täitmiseks on vajalik täiendada küberkuritegevuse vastast seadusandlust- ühtlustada siseriiklikku kriminaalseadusandlust (näiteks sisuliselt sarnased õigusrikkumiste elemendid); arendada uurimistehnikaid; anda siseriiklikule seadusandlusele õiguse menetleda ja esitada süüdistus nendes ning teistes arvutisüsteemidega seotud kuritegudes (või millega on seotud elektroonilised tõendid).[21]

Lõplik Arvutikuritegevusevastane konventsioon koosneb preambulast ja neljast peatükist- preambulas on selgitatud konventsiooni koostamise eesmärki ning eesmärke, mida soovitakse saavutada, esimeses peatükis on ära toodud mõisted, mida kasutatakse konventsioonis, teine peatükk määratleb riigi tasandil võetavad meetmed, kolmas peatükk käsitleb rahvusvahelist koostööd, neljas peatükk käsitleb täitevküsimusi, nagu näites konventsiooni allakirjutamise ja jõustumise aeg. [22]

1.2.3.1 Euroopa Liidu õigusruum

Asjakohaste rahvusvaheliste õigusinstrumentide nimetamisel tuleb lisaks EN ülakirjeldatud konventsioonile ära märkida ka Euroopa Liidu strateegiadokumendist üks aste allpool paiknev normatiivakt.

---

[19] M. D. Goodman and S. W. Brenner. The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, vol 10 No 2. Oxford University Press 2002, lk 171

[20] Arvutikuritegevusevastane konventsioon.- RT II 2003, 9, 32, arvutivõrgus kättesaadav: https://www.riigiteataja.ee/akt/550359 (21.03.2013)

[21] A. Klimburg (Ed.). National Cyber Security Framework Manual. NATO CCD COE Publication, Tallinn 2012, lk 160-161

[22] M. D. Goodman and S. W. Brenner. The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Informaation Technology, vol 10 No 2, Oxford University Press 2002, lk 171

ELi kontekstis reguleerib käesolevat teemat 2005. aastal vastu võetud Euroopa Liidu Nõukogu 24.02.2005 raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta[23]. Raamotsuse materiaalõiguse osa kordab põhimõtteliselt ENi konventsioonis reguleeritut. Raamotsuse puuduseks on selle kohaldatavus üksnes ELi liikmesriikide suhtes, kuid küberkuritegevuse puhul on tegemist märksa laiema piiriülese probleemiga. Nii konventsiooni kui ka raamotsuse puhul on puuduseks see, et need käsitlevad arvutisüsteemide vastaseid ründeid eeskätt varavastaste kuritegudena ning jätavad tagaplaanile riigi julgeolekumõõtme. Erinevaid arvutisüsteeme käsitletakse ühetaoliselt ning ei eristata suvalist arvutisüsteemi kriitilise infrastruktuuri arvutisüsteemist, samuti ei räägita neis eraldi massiliselt toime pandud rünnetest.[24]

2010.a septembrist alates on Euroopa Komisjonis menetluses küberkuritegevuse vastase võitluse „*Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK*“. Direktiivi eesmärk on näha ette EL tasandil miinimumnõuded st ühtlustada liikmesriikide õigust arvuti- ehk küberkuritegude osas. Direktiivi kohaselt on kõik liikmesriigid kohustatud direktiivis nimetatud tegevused kriminaliseerima ning nägema nende toimepanemise eest efektiivsed, proportsionaalsed ja hoiatavad karistused. Täiendavalt näeb direktiiv ette juriidiliste isikute vastutuse, raskendavad asjaolud nende kuritegude toimepanemisel ning reguleerib riikidevahelist koostööd küberkuritegevuse vastases võitluses.[25]

Kõiki punktis 1.2 nimetatud dokumente kritiseerides tuleb tõdeda, et läbivalt puuduvad nendes kasutatud mõistete definitsioonid või on need esitatud valikuliselt. Samas ei ole kindlasti tegemist kriitikaga ainult Eesti aadressil, vaid probleem on laiem ning küberjulgeoleku ning –turvalisuse maastikul puuduvadki täna laiapõhjalised kokkulepped võtmetähendusega mõistete osas.

[23] Euroopa Liidu Nõukogu 24.02.2005 raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta, arvutivõrgus kättesaadav http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ET:PDF (18.05.2013)

[24] Küberjulgeoleku strateegia 2008-2013, lk 18, arvutivõrgus kättesaadav http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013(1).pdf

[25] Justiitsministeeriumi kodulehekülg, arvutivõrgus kättesaadav http://www.just.ee/33098

2. VASTUTUSE VÄLISTAMISE PRAKTILINE VAJADUS

Käsitletud EL ja Eesti strateegiad kirjeldasid küberkuritegevuse järjest kasvavat ohtlikkust riikide majandustele ning tõdesid, et võitlust küberkuritegevusega tuleb tõhustada. Nimetatud dokumentides antud soovitused on tervitatavad suundanäitava iseloomuga juhistena, kuid jäävad konkreetsete organisatoorsete sammude võtmiseks või seaduse muudatusettepanekute põhjendamiseks liiga üldsõnaliseks. Selleks, et määratleda töö seisukohast olulise küsimuse – karistusõigusnormi sõnastusse sekkumise, tegelikku vajadust, tuleb arvestada muutustega küberkaitse kui doktriini arengus viimase 3-5 aasta jooksul.

Hiinast, Põhja- Koreast, Indiast, Iisraelist ja paljudest teistest riikidest pärit küberründed häirivad ründe objektideks olevate riikide või vähemalt nende äride igapäevast toimimist. Rünnakute rohkus ning nende tagajärjel häiritud tavaelu ning majanduse toimimine on tekitanud küsimuse, kas passiivses kaitseseisundis olemine ning tegelemine vaid tagajärgedega on põhjendatud. Üha enam otsivad riigid ja ettevõtted võimalusi asuda aktiivsele kaitsele ning üritavad leida seaduslikke viise taolise tegevuse läbiviimiseks.

Püüdes kaitsta oma arvutivõrke ja –süsteeme mahult ja ülesehituselt aina komplitseeritumate küberrünnete eest, on küberturbeeksperdid ammendamas vaid kaitsetaktikal põhinevate meetodite võimalusi. Ollakse uurimas seaduslikke võimalusi kasutada rünnete tõrjumiseks ja arvutikuritegude avastamiseks lahendusi, mis sisaldavad vasturünde, ennetava ründe või andmete kogumise eesmärgil võõrasse arvutisüsteemi loata sisenemise elemente. Kuna tegemist on valdkonnaga, mida ei ole kunagi varem õiguslikult reguleeritud, tekitab küsimus vastava tegevuse lubatavusest kahtlemata vastakaid arvamusi. Olenevalt sellest, kas räägitakse rahvusvaheliste organisatsioonide nimel või lahendatakse küsimust ühe riigi piires, võivad vaated olla kardinaalselt erinevad. Nii räägib näiteks NATO 2011.a vastu võetud küberkaitsepoliitika[26] küll küberrünnete ennetamise vajadusest, kuid sisustab selle kontseptsiooni siiski vaid kaitsemehhanismide rakendamisega, hoidudes kiivalt tegemast mistahes kujul viiteid ründavale või aktiivsele kaitsele. Seejuures näiteks USA (kuuludes samal ajal NATO-sse), peab avalikke debatte aktiivse kaitse vajalikkusest ning on lülitanud selle riiklikku arengukavva.[27]

[26] Arvutivõrgus kättesaadav http://www.nato.int/cps/en/natolive/topics_78170.htm

[27] I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security Policy Brief. February 2013, arvutivõrgus kättesaadav http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (18.05.2013)

2.1 Nihe klassikaliselt kaitsedoktriinilt aktiivse kaitse suunas

Alljärgnev peatükk kirjeldab passiivse ja aktiivse kaitse erinevust riigi vastumeetmena küberrünnaku ohvriks sattudes. Riigi tasemel vastumeetmeid analüüsides satume sõjaõiguse piirimaile, kuid kuna see ei ole käesoleva töö põhiteema, piirdub töö vaid doktriinide elementaarsete eristamise kriteeriumite nimetamisega.

Töö uurimisküsimusega seonduvalt on sõjaõiguses kasutatavate passiivse ja aktiivse kaitse meetodite põhimõtete ülevõtmine siiski relevantne, kuna küberintsidendi avastamise hetkel ei ole teada, kas see on motiveeritud rahalise või muu kasu (n: tööstusspionaaž) saamisest (st kas tegemist on küberkuriteoga) või soovitakse saavutada poliitilisi või toetada sõjalisi eesmärke (st kas küberintsidenti võib selle ulatuse tõttu võrdsustada relvastatud ründega). Olenevalt juhtumi asjaoludest võib toimunu uurimine seega jääda justiitsministeeriumi või kaitseministeeriumi valitsemisalasse - spetsialistide tasemel ei ole sellel aga rakendatavate töövõtete mõttes mingisugust erinevust.

Erialakirjandus defineerib *passiivset kaitset* kui meetmete võtmist vaenuliku tegevuse läbi tekkida võiva kahju tõenäosuse ja tekkinud kahju tagajärgede minimeerimiseks ilma kavatsuseta haarata ise initsiatiivi (või astuda aktiivseid samme).[28]

Passiivse kaitse põhimõtet järgides on riigil küberrünnete vastu end keeruline kaitsta, kuna see eeldaks kõigepealt rünnet ning seejärel alles kaitsetegevust. Kuivõrd aga küberrünnak võib halvata asutuse või ettevõtte tegevuse selliselt, et vastutegevus on kas võimatu või saadakse tegutseda peale ründe lõppu ja tagajärgede likvideerimist, on oluline, et asutused ja ettevõtted saaksid võimaluse end kaitsta ning oma turvasüsteeme testida ja parendada.

Küberohtude muutuv iseloom on teinud aktiivse küberkaitse üha tähtsamaks nii era- kui avalikus sektoris. Põhilised ohud ei tulene enam teismelistest häkkeritest või pisikurjategijatest, kuigi ka need on veel olemas. Vastupidi, kõrgetasemelised kurjategijad ja riigipoolt toetatud spioonid kujutavad suurimat ohtu ettevõtetele ja valitsustele. Need sissetungijad on eeskätt keskendunud intellektuaalse omandi vargustele ja inimeste ja äride petmisele.[29]

---

[28] USA Kaitseministeeriumi sõjaväeleksikoni termin, arvutivõrgus kättesaadav http://www.answers.com/topic/passive-defense (09.04.2013)

[29] I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security Policy Brief. February 2013, arvutivõrgus kättesaadav http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (18.05.2013)

Passiivse küberkaitse meetmed ei vasta taolistele ohtudele.[30] Passiivse küberkaitse meetmetest on küberkeskkonnas vaid mõningast kasu - tavaline küberpraktika nagu turvaaukude parandamine, võib aidata vähendada madalatasemeliste rünnakute hulka. Passiivse küberkaitse meetmed on vajalik osa heast küberkaitse programmist, kuid nad ei ole enam piisavad vastamaks järjest kasvavatele kõrgeltarenenud rünnakutele.[31] Passiivne küberkaitse, mis tugineb sissetungide ennetamisel välisanduritele *(perimeter sensors)*, ei paku küllaldast kaitset järjest keerulisemate küberrünnakute vastu.[32]

Ründav/aktiivne kaitse (*Offencive Defence* või A*ctive Defence*) on enim arutluse all olev vastumeede[33], mida võiks kasutada vastuseks küberrünnakule, kuid see on üksnes üks võimalus paljudest. Seadusega lubatud vastumeetme piir on see, et ta peab olema proportsionaalne kahjuga, mida rünnatav riik kannatas. [34]

Aktiivne küberkaitse kui väljend iseloomustab hulka ennetavaid tegevusi, mis tegelevad vastasega enne ja küberintsidendi ajal ning võivad suurendada püüdlusi keeruliste rünnakute avastamiseks ja neile vastamiseks.[35] Isegi kui aktiivne küberkaitse on järjest enam levinud, siis arutelu selle üle, millised meetmed on sobivad või isegi seaduslikud, alles algavad.[36] Paljud arutelud antud teemal on keskendunud aktiivse küberkaitse agressiivsetele külgedele, nagu näiteks karistatav „hack-back"[37] või ennetav häkkimine.[38]

---

[30] *op. ci*t., (18.05.2013)
[31] *op. cit.,* (18.05.2013)
32 *op. cit*., (18.05.2013)
[33] N. Burns & J. Price. Securing Cyberspace. A New Domain for National Security. The Aspen Institute 2012, lk 36
[34] O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel. The Law of Cyber-Attack. California Law Review 2012, lk 879

[35] I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security Policy Brief. February 2013, arvutivõrgus kättesaadav http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (18.05.2013)
[36] I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security Policy Brief. February 2013, arvutivõrgus kättesaadav http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (18.05.2013)
[37] vastavalt http://www.techopedia.com/definition/23172/back-hack toodud seletusele nimetatakse seda süsteemi vastu suunatud rünnete tuvastamise protsessiks ning kui võimalik, siis tuvastatakse ka rünnaku päritolu. Sellest võib mõelda kui vastupidist tehnikat häkkimisele, kus turvakonsultandid ja teised professionaalid püüavad ette näha rünnakuid ja neile adekvaatselt vastata.
[38] I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security Policy Brief. February 2013, arvutivõrgus kättesaadav http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (18.05.2013)

2.2 Küberrelvad tsiviilkäibes ja kriminaalmenetluse tööriistadena

Üheks kõige selgemaks näiteks küberrelvast peetakse 2010.a avastatud *Stuxnet* nimelist arvutiviirust[39], mille sattumine Iraani tuumaprogrammis kasutatavasse arvutisüsteemi takistas uraani rikastamise protsessis kasutatavate tsentrifuugide tööd, lükates sedasi edasi kogu tuumaprogrammi käivitamist.

Töö edasise lugemise hõlbustamiseks on asjakohane määratleda küberrelva mõiste: küberrelv on informatsioonitehnoloogial põhinev süsteem, mis on kavandatud mõne teise informatsioonitehnoloogial põhineva süsteemi ülesehituse või toimimise kahjustamiseks.[40]

Küberrelvadeks tuleb seega lugeda mistahes infotehnoloogilist laadi tööriista, mida kasutatakse võõrale arvutisüsteemile juurdepääsu takistamiseks, selle toimimise tõkestamiseks, funktsionaalsuse muutmiseks või arvutisüsteemi hävitamiseks. Eeltoodu kinnitab töös juba varasemalt püstitatud hüpoteesi, et KarS § 208 tähenduses nuhkvara, arvutiviirus või pahavara ei ole ükski arvutiprogramm *per se*, vaid vastav tiitel omistatakse mistahes arvutiprogrammile konkreetses kontekstis selle kasutamise läbi kuritegelikul eesmärgil.

2.2.1 Turvatestimine ehk *penetration testing*

Turvalisuse hindamise kategooriad hõlmavad turvaauditit (*Security Audit*), haavatavuse hindamist (*Vulnerability Assessment*), eetilist häkkimist (*Ethical Hacking*) ja turvatestimist (*Penetration Testing*).[41]

Allolevalt käsitletakse kahte põhilist võimalust, mille puhul on võimalik tuvastada turvaauke ning testide tulemustele vastavalt parandada kaitsesüsteeme ettevõtete arvutites.

Turvatestimine on protsess, tuvastamaks võrgustikus ilmnevaid nõrku kohti. Enamik, kui mitte kõik valitsusasutused üle maailma testivad järjepidevalt oma võrgustike kaitsemehhanisme, tagamaks turvalist küberkeskkonda. Küberrünnakud olid olemas juba

[39] L. Ferran. New version of Stuxnet-Related Cyber Weapon Discovered.- ABC News, arvutivõrgus kättesaadav http://usa.kaspersky.com/about-us/press-center/in-the-news/new-version-stuxnet-related-cyber-weapon-discovered (18.05.2013)
[40] P. Lorents, R. Ottis. Knowledge based Framework for Cyber Weapons and Conflict. Conference on Cyber Conflict. Proceedings 2010. CCD COE Publications 2010, lk 139
[41] Arvutivõrgus kättesaadav http://www.eccouncil.org/courses/licensed_penetration_tester.aspx (13.04.2013)

kümme aastat tagasi, kuid nad ei põhjustanud majanduslikku kaost ega ähvardanud rahvuslikku majandust nii nagu praegu. Tänapäeval, kui organisatsioonide toimimine sõltub üha enam interneti kättesaadavusest, toimub infovahetus elektrooniliselt ja silmapilkselt. Seega sõltub ettevõtete püsimajäämine võimekusest hinnata, varustada ja hoida informatsiooni ning mahajäämus info turvalisuse osas tähendab sageli negatiivseid tagajärgi ettevõtte kasumlikkusele.[42]

Penetration testing ehk turvatestimine ning eetiline häkkimine[43] on käesolevas töös välja toodud põhjusel, et nimetatud meetodite kasutamise tingimuseks on teise arvuti turvasüsteemi tungimine, mida saab teha, kasutades eelnevalt valmiskirjutatud pahavara või rünnates arvutisüsteemi viirustega, mis toovad välja ettevõtte arvutiturvalisuse nõrgad kohad. Nimetatud testimiste puhul on eelduseks pahavara kirjutamine ja kasutamine või turvasüsteemi tungimine, mis Eestis kehtiva karistusseadustiku §-de 208 ja 216[1] sõnastuse kohaselt on keelatud tegevused.

2.2.2 Eetiline häkkimine ehk *ethical hacking*

Eetiline häkkimine on laialt defineeritud kui metoodika, millega avastatakse olemasolevaid haavatavaid kohti infosüsteemidega tegelevates keskkondades. Eetilised häkkerid kasutavad tavaliselt samu tööriistu ja tehnikaid kui kuritegelikud ründajad, kuid nad ei kahjusta sihtsüsteemi ega varasta informatsiooni, säilitades seetõttu süsteemi terviklikkuse ja konfidentsiaalsuse[44]. Nende töö on hinnata sihtmärgi turvalisust, ajakohastada süsteemi vastavalt avastatud nõrkadele kohtadele ja soovitada sobivaid parendusmeetmeid.[45]

Valitsused, tööstusharud ja akadeemikud nõustuvad, et omaenda andmeturvalisuse proovilepanek läbi hindamise ja testimise on iga tõhusa andmeturvalisuse põhikomponent. Andmeturbe seisukohast on arvutisüsteemide turvalisuse tagamisest huvitatud kõik isiku- ja finantsandmete töötlemise eest vastutavad ettevõtted ja organisatsioonid, kes turvaintsidendi toimumise korral riskivad mainekahjuga. Sarnaselt sõltub paljude äriettevõtete jätkusuutlikkus olemasoleva ärisaladuse või intellektuaalse omandi säilimisest.[46]

---

[42] *op. cit.,*(13.04.2013)
[43] R. W. Taylor, T. J. Caeti, D. K. Loper, E. J. Fritsch, J. Liederbach. Digital Crime and Digital Terrorism. PearsonEducation Inc., Upper Saddle River, New Jersey 2006, lk 73-75
[44] R. I. Raether Jr. Data Security and Ethical Hacking. Points to Consider for Eliminatig Avoidable Explosure. Business Law Today. September/October 2008, lk 55
[45] Arvutivõrgus kättesaadav http://www.eccouncil.org/courses/licensed_penetration_tester.aspx (13.04.2013)
[46] R. I. Raether Jr. Data Security and Ethical Hacking. Points to Consider for Eliminatig Avoidable Explosure. Business Law Today. September/October 2008, lk 55

Turvatestimisi teostades kasutatakse pahavara või viiruseid, mis iseenesest võiksid kahju tekitada, kuid mille eesmärk on siiski üksnes osutada süsteemis esinevatele nõrkadele kohtadele. Arusaadavalt võiks olla karistatav üksnes selline pahavara ning viiruste levitamine ning võõrasse arvutivõrku tungimine, mille eesmärgiks on tekitada kahju. Lubatud peaks olema teatud juhtudel viiruste kirjutamine ning nende võimalik katsetamine ja mõjude ülesmärkimine näiteks kinnises arvutisüsteemis, võimalusega luua antiviiruseid juba olemasolevatele viirustele.

Antiviiruste uurimise edendamise puhul on enim räägitud viiruste loomisest ja uurimisest kontrollitud keskkonnas.[47] Probleem on selles, et terminit „viirus“ on õigustekstides tihti ebapiisavalt defineeritud. Adekvaatse definitsiooni puudumine viib sinnamaani, et mitmed healoomulised ja vajalikud programmid langevad arvutiviiruse definitsiooni alla. See ei tähenda ilmtingimata, et nende programmide loojad ja jagajad saavad karistada, küll aga tähendab see, et seaduses on ebamäärasust.[48]

2.3 Küberrelvade võimalik kasutamine Eesti õiguskaitseorganite tegevuses ning küberrelvade kasutamise näited erinevate riikide praktikate põhjal

2.3.1 FinFisher

FinFisheri on välja töötanud Briti ettevõte Gamma Group ning selle reklaami-materjalide järgi on toode mõeldud «*sihtsüsteemidele ligipääsemiseks, võimaldades koguda nii vajalikku krüpteeritud informatsiooni, kui ka üle võtta süsteemi enda erinevad funktsioonid.*»[49] Turvaanalüütikute väitel on FinFisher võimeline salvestama nakatunud arvutite ekraanipilte, Skype´i vestlusi, klahvivajutusi ning iseseisvalt sisse lülitama veebikaamera ja mikrofoni funktsioone.[50]

FinFisher on kommertskasutuses olev nuhkvaratoode, mida muuhulgas müüakse erinevate riikide võimudele, lihtsustamaks kurjategijate jälgimist.[51]

---

[47] M. Klang. A Critical Look at the Regulation of Computer Viruses. International Journal of Law and Information Technology. Vol. 11 No 2. Oxford University Press 2003, lk 180.
[48] *op. cit.,* lk 180
[49] Valitsuste kasutatava võimsa nuhkvara jälgi leiti ka Eestist.- Arvutivõrgus kättesaadav http://www.e24.ee/941062/valitsuste-kasutatava-voimsa-nuhkvara-jalgi-leiti-ka-eestist/ (14.04.2013)
[50] *op. cit.,* (14.04.2013)
[51] RIA: Meil ei ole FinFisheri nuhkvaraga kokkupuuteid olnud.- Arvutivõrgus kättesaadav http://www.e24.ee/1175412/ria-meil-ei-ole-finfisheri-nuhkvaraga-kokkupuuteid-olnud/ (14.04.2013)

Turbefirma Rapid7 spetsialistid tegid kindlaks nuhkvara struktuuri ja leidsid, et FinFisheril on olemas vähemalt 11 Indoneesias, Kataris, Etioopias, Tšehhis, Mongoolias, Lätis, Araabia Ühendemiraatides, USAs ja Eestis asuvat serverit.[52]

Peale seda, kui tuvastati, et üks nuhkvara kasutav server asub väidetavalt Eestis, ei ole Siseministeerium antud infot kinnitanud ega ka ümber lükanud. Selle asemel on antud mitmetitõlgendatav vastus- „*Eesti suhtub kindlasti tõsiselt kõikidesse taolistesse indikatsioonidesse nimetatud tarkvarade võimalikust kasutamisest Eestis. Kui tegemist on mistahes ebaseadusliku tegevusega, siis kavatseb Eesti riik sellist tegevust kindlasti takistada. Eesti riik ise kasutab inimeste turvalisuse tagamiseks neid vahendeid, mida on eesmärgi saavutamiseks vaja. Nende vahendite loetelu ei avaldata, kuna see annab ülevaate riigi võimekusest*“, vastas sisejulgeolekupoliitika asekantsler Erkki Koort E24 küsimusele, kas Eesti valitsusasutused kasutavad FinFisheri nuhkvara kriminaalide jälgimiseks.[53]

Lisaks võimatusele kinnitada nimetatud tarkvara kasutamist või mittekasutamist viitega võimalikule riigisaladusele, ei saaks riik sellele küsimusele vastata jaatavalt ka põhjusel, et juhul kui taolist nuhkvara kasutada, siis oleks see kasutamine karistatav KarS § 208 järgi. Seda enam ei saa uurimisasutused antud nuhkvara kasutamist jaatada, kuna see tähendaks, et riikliku julgeoleku tagamiseks ning kriminaalide jälgimiseks rikuks riik ise seadust, mille täitmist ta oma kodanikelt nõuab. Tsiteeritud ajaleheväljavõtete põhjal jääb siiski mõningane kahtlus, et riik kas siis FinFisher nuhkvara või mõnda muud sarnase toimega nuhkvara oma uurimisorganite kaudu kasutab.

2.3.2 Küberkaitseõppused

Vaadates tulevikku peavad sõja planeerijad olema võimelised jäljendama küberrünnakuid ja testima küberkaitset turvalises laboratooriumikeskkonnas, ohustamata operatsioonisüsteemide terviklikkust. [54]

Küberkaitseõppuse eesmärgiks on suurendada arusaama rahvusvahelisest küberkeskkonnast ja suurendada rahvusvahelist koostööd tehniliste intsidentidega toimetulemiseks.[55]

---

[52] *op. cit.*

[53] Siseministeerium ei kinnitanud ega lükanud ümber FinFisheri nuhkvara võimalikku kasutamist.- Arvutivõrgus kättesaadav http://www.e24.ee/941996/siseministeerium-ei-kinnitanud-ega-lukanud-umber-finfisheri-nuhkvara-voimalikku-kasutamist/ (14.04.2013)

[54] K. Geers. Strategic Cyber Security. CCD COE Publication 2011, lk 50-51

Üheks levinud viisiks teadlikkuse tõstmiseks ja koostöö harjutamiseks on läbi aegade olnud õppuste läbiviimine. Viimastel aastatel on hüppeliselt kasvanud justnimelt küberkaitse alaste õppuste korraldamine arenenud maades ja rahvusvahelistes organisatsioonides.

Küberõppuste vallas on olnud mitmes mõttes teenäitajaks Tallinnas tegutsev NATO Kooperatiivne Küberkaitse Kompetentsikeskus, mis korraldab alates 2010. aastast rahvusvahelist küberkaitseõppust algse nimega Baltic Cyber Shield (BCS) [56]. Alates 2012.a on ürituse nimetus LockedShields. Tegemist on samaaegselt umbkaudu kümnes Euroopa riigis spetsiaalselt harjutuse otstarbeks ehitatud arvutivõrgus peetava nö „*live-fire*" küberkaitse õppusega, mis tähendab, et ründed kaitstava infrastruktuuri pihta pannakse toime reaalajas ja tegelike arvutiprogrammide abil.

Õppusel osalevad erinevad meeskonnad, kelledest ühed panevad toime küberründe (*red team*), teised meeskonnad kaitsevad kokkulepitud IT-süsteemi antud ründe eest (*blue teams*). Küberkaitseõppuse eesmärgiks on reaalajas testida infosüsteemi valdajate võimekust seda rünnete eest kaitsta ning selle eelduseks on ründemeeskonna poolt rünnete toimepanemine. Ehk siis kasutab ründemeeskond muuhulgas pahavara levitamist.
Käesoleva töö eesmärki silmas pidades peab aga nentima, et ka taolise live-fire õppuse läbiviimine ei saa olla Eestis lubatud. Vaatamata antud õppuse eesmärgile, mis ei ole kuritegelik, vaid ilmselt siiski tulevikku suunatud ning mõeldud turvalisuse tagamiseks, puudub Eesti seadusandluses säte, mis võimaldaks antud õppuse läbiviimist. Eeldab ju antud õppus pahavara olemasolu ja levitamist ning teise arvutisüsteemi tungimist.

2.3.3 Küberrelvade kasutamine USA ja Iraani näite põhjal- Stuxnet, DuQu, Fame

Eestis praktiseeritav nulltolerants igasuguse nuhkvara, pahavara ja viiruse käitlemisel, olenemata taolise tegevuse eesmärgist, ei ole ettenägelik. On vähetõenäoline, et Eesti hakkaks välja töötama viiruslikku pahavara ehk küberrelva sarnaselt Ameerika Ühendriikidega, kuid teatud juhtudel riikliku julgeoleku vajadustest lähtuvalt ei peaks väga spetsiifilistel eesmärkidel loodud nuhkvara ja pahavara loomine ning levitamine olema karistatav.

[55] Arvutivõrgus kättesaadav http://www.ccdcoe.org/172.html (14.04.2013)
[56] Arvutivõrgus kättesaadav http://www.ccdcoe.org/publications/BCS2010AAR.pdf (14.04.2013)

Allpool toodud näidete põhjal saab teha järelduse, et riigid loovad ning kasutavad küberrelvi teiste riikide vastu, samuti täiustavad antud relvi pidevalt ning neid on üha raskem tuvastada.

2010.a juunis hakkasid Iraani tuumaprogrammi jaoks uraani puhastavad tsentrifuugid arusaamatutel põhjustel kontrolli kaotama ja purunema. Peagi sai selgeks, et kahju põhjustas arvutiviirus nimega Stuxnet, mida ühegi viirusetõrje programmiga ei avastatud. Selle avastamiseks oli vaja kahtlustele järgnenud põhjalikku ekspertanalüüsi. Kuna keegi end Stuxneti autoriks ei soovinud tunnistada ja see kahjustas maailmas laialt kasutusel olevaid Siemensi valmistatud tööstuslikke kontrollseadmeid, võeti viirus mureliku tähelepanu fookusesse. Uurimise tulemusel selgus, et kurja tegev programm kasutas Windows operatsioonisüsteemi praktiliselt tundmatut turvaauku.[57]

Aasta pärast Stuxneti avastamist jäi Budapesti Tehnoloogiaülikooli uurijatele silma seni tundmatu ja salaja andmeid koguv programm, mis sai nimeks DuQu. Koodi analüüsijad märkasid üllatavalt palju sarnasusi Stuxnetiga, kuigi DuQu ülesandeks polnud midagi lõhkuda. Arvatakse, et tegemist oli avastamise hetkeks vähemalt mõned aastad varjatult tegutsenud programmiga, mille loojad asuvad ühes kohas. Võimalik, et tegemist oli teineteise tegevust täiendama loodud paarikesega – Stuxnet pidi lõhkuma tööstuslikke seadmeid ja DuQu aitama kogutud andmete abil juhtida selle tegevust.[58]

2012.aastal kirjutab Briti ärileht Financial Times (FT) viitega IT-asjatundjatele, et kübersõja on tõstnud uuele tasandile Flame-nimeline viirus, mis jälgib ja kogub andmeid Iraani tuumauuringute kohta.[59] See tundub olevat kui spionaaži ja järelevalve tööriist, mis on suunatud Iraanile, ning mis oskab varastada andmeid ja pealt kuulata telefonikõnesid.[60]

---

[57] Viirustõrjeprogrammid mureliku tähelepanu fookuses.- ERR teadusuudised 06.06.2012. Arvutivõrgus kättesaadav http://forte.delfi.ee/news/digi/viirusetorjeprogrammid-mureliku-tahelepanu-fookuses.d?id=64497264 (13.04.2013)

[58] Viirustõrjeprogrammid mureliku tähelepanu fookuses. -ERR teadusuudised 06.06.2012. Arvutivõrgus kättesaadav http://forte.delfi.ee/news/digi/viirusetorjeprogrammid-mureliku-tahelepanu-fookuses.d?id=64497264 (13.04.2013)

[59] FT: Superviirus jälgib Iraani tuumaprogrammi. 29.05.2012. Arvutivõrgus kättesaadav http://www.delfi.ee/news/paevauudised/valismaa/ft-superviirus-jalgib-iraani-tuumaprogrammi.d?id=64465298 (13.04.2013)

[60] R. O´Harrow Jr. Understanding cyberspace is key to defending against digital attacks.- The Washington Post 03.06.2012. Arvutivõrgus kättesaadav http://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defending-against-digital-attacks/2012/06/02/gJQAsIr19U_story_1.html (14.04.2013)

Flame'i põhjustatud avalik tähelepanu ajendas USAd ja Israeli üles tunnistama, et nemad olid Stuxneti loomise taga. Väidetavalt kaotasid nad Iraani tuumaprogrammi jaoks loodud viiruse üle kontrolli ja see hakkas levima. President George W. Bushi ajal loodud ja Barack Obama poolt jätkatud viiruseid valmistav katteprogramm kannab koodnime „Olümpiamängud".[61]

Peagi pärast viiruste nagu Stuxnet ja selle järeltulija Flame, paljastamist, sattus USA üleriigiline meediaväljaanne The Washington Post loole, mis väidab, et ülisalajane *Defense Advanced Research Projects Agency (DARPA)* valmistub testima mehitamata küberrünnet, mis käivitab ennast ise, vajamata selleks inimese kontrolli.[62] Plan X-iks nimetatud ettevõtmine on Pentagoni üksuse *Defense Advanced Research Projects Agency* projekt, mis keskendub eksperimentaalsetele pingutustele ning millel on võtmeroll arvutivõimekuse rakendamisel, aitamaks sõjaväel efektiivsemalt sõdu pidada.[63] Plan X arhitektid loodavad arendada süsteeme, mis suudaksid anda ülemustele võime läbi viia välkkiireid rünnakuid ja vasturünnakuid, kasutades etteplaneeritud stsenaariume, mis ei hõlma inimoperaatorite poolt käsitsi koodide kirjutamist, kuivõrd viimast peetakse liialt aeglaseks.[64]

Ainuüksi ülaltoodud näide, kus Ameerika Ühendriigid ning Iraan möönsid küberrelva kasutamist teise riigi vastu, annab märku riikide tasemel praktikast pahavara loomisel ning lükkab ümber võimaluse nimetada nii pahavara kui ka viiruste loomist, kirjutamist ja levitamist alati kuritegelikuks.

---

[61] *vt viide 58,* (13.04.2013)

[62] J. Wolverton. The Pentagon is developing cyberweapons that launch without human intervention.- The New American 22.06.2012. Arvutivõrgus kättesaadav http://thenewamerican.com/usnews/item/11810-the-pentagon-is-developing-cyberweapons-that-launch-without-human-intervention (23.04.2013)

[63] E. Nakashima. With Plan-X, Pentagon seeks to spread U. S. Military might to cyberspace.- The Washington Post 30.05.2012. Arvutivõrgus kättesaadav http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html (23.04.2013)

[64] E. Nakashima. With Plan-X, Pentagon seeks to spread U. S. Military might to cyberspace. -The Washington Post 30.05.2012. Arvutivõrgus kättesaadav http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html (23.04.2013)

3. KARISTUSSEADUSTIKU KAASAJASTAMINE

3.1 Karistusseadustiku § 208 ja 216[1] kujunemine

Töö uurimisobjektiks oleva KarS-i § 208 koosseis sisaldus karistusseadustikus alates selle jõustumisest 01.09.2002.a. Seaduse algse sõnastuse kohaselt oli kriminaliseeritud vaid arvutiviiruse levitamine järgmises sõnastuses:

§ 208. Arvutiviiruse levitamine

(1) Arvutiviiruse levitamise eest - karistatakse rahalise karistuse või kuni üheaastase vangistusega.

(2) Sama teo eest, kui see on toime pandud:

1) vähemalt teist korda või

2) olulise kahju tekitamisega, -

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

21.02.2008. aastal vastu võetud karistusseadustiku muutmise seadusega[65] muudeti kõnealust koosseisu ning lisati karistatavate tegevuste hulka ka nuhkvara ja pahavara levitamine.

Karistuse osas karmistati ettenähtud vabadusekaotuslikku karistusmäära ühelt aastalt kolmele aastale (teises lõikes kvalifitseeritud koossisu puhul kolmelt aastalt viiele aastale). Veel lisati paragrahvile kolmas ja neljas lõige, mis vastavalt nägid ette vastutuse juriidilise isiku teo eest ning andsid kohtule võimaluse kohaldada süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimist.

2008.a Riigikogule esitatud karistusseadustiku muutmise seaduse eelnõu seletuskirja kohaselt oli muudatuste eesmärgiks täiendada KarS-i selliselt, et see oleks kooskõlas nõuetega, mis on sätestatud Euroopa Nõukogu arvutikuritegevusvastase konventsioonis (*Convention on Cybercrime*) ja EL nõukogu 24. veebruari 2005. a raamotsuses *infosüsteemide* vastu suunatud rünnete kohta 2005/222/JSK[66].[67]

[65] Karistusseadustiku muutmise seadus.- RT I 2008, 13, 87, arvutivõrgus kättesaadav https://www.riigiteataja.ee/akt/12937096 (17.05.2013)

[66] EL nõukogu 24. veebruari 2005. a raamotsuses *infosüsteemide* vastu suunatud rünnete kohta 2005/222/JSK. Arvutivõrgus kättesaadav http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ET:PDF

[67] Karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 seletuskiri, arvutivõrgus kättesaadav http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=197158&u=20130517132004 (17.05.2013)

3.1.1 Koosseisude analüüs

Sõnastuse poolest on KarS § 208 esimene lõige esmapilgul selge ja ühemõtteline. Edaspidises soovib töö autor tähelepanu pöörata, et niisugune esmamulje võib olla petlik ning grammatiliselt selge normi taga peitub hulgaliselt küsimusi, millele ammendavad vastused täna puuduvad.

3.1.1.1 Nuhkvara, pahavara ja arvutiviiruse levitamine

Nuhkvara, pahavara ja arvutiviiruse levitamise paragrahv paikneb karistusseadutiku varavastaste süütegude peatüki omandi vastu suunatud süütegude all (13.ptk I jagu). Seadus kirjeldab tegu järgmiselt.

§ 208. Nuhkvara, pahavara ja arvutiviiruse levitamine

(1) Nuhkvara, pahavara või arvutiviiruse levitamise eest –karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui see on toime pandud:

1) vähemalt teist korda või

2) kui sellega on tekitatud oluline kahju, –

karistatakse rahalise karistuse või kuni viieaastase vangistusega.

(3) Käesoleva paragrahvi lõikes 1 või 2 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –

karistatakse rahalise karistusega.

(4) Kohus võib kohaldada käesolevas paragrahvis sätestatud süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimist vastavalt käesoleva seadustiku §-s 83 sätestatule.

Paragrahviga kaitstav õigushüve on seaduslike arvutikasutajate õiguspärane ootus arvutite takistamatuks kasutamiseks.[68]

Koosseisutüübilt on esimese lõike näol tegemist formaalse ehk teodeliktiga, mis tähendab, et lõpuleviidud tegu ei eelda kahjuliku tagajärje tuvastamist.

Koosseisu objektiivne külg seisneb nuhkvara, pahavara või arvutiviiruse levitamises. Isiku suhtes süüdimõistva kohtuotsuse tegemiseks on seega vajalik tõendada, et tegemist on nuhkvara, pahavara või arvutiviirusega ja tuvastada levitamise fakt. Levitamise mõiste kohta

[68] J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. 3. trükk, Tallinn: Juura 2009, lk 559

on prof. J.Ginter kirjutanud, et see tähendab vastava programmi edastamist vähemalt ühte arvutisse, mille valdaja ei ole selleks nõusolekut andnud.[69]

Keerulisem on olukord arvutiprogrammide liigitamisega nuhkvaraks, pahavaraks või arvutiviiruseks.

Nuhkvara (*spyware*) all peetakse silmas kahjulikku arvutiprogrammi, mis kogub arvutikasutaja kohta informatsiooni ilma tema teadmata ning edastab seda nuhkvara paigaldajale või kolmandale isikule.[70]

Arvutiviirus (*computer virus*) tähendab KarS § 208 kontekstis mis tahes kahjulikku arvutiprogrammi, mis on võimeline end oma algsel või modifitseeritud kujul ise või teiste arvutiprogrammide abil arvutivõrgu kaudu edasi levitama ning häirima arvutite kasutamist. Häirimise all peetakse silmas mh arvutis olevate andmete või programmide muutmist või kustutamist, kasutades ära arvuti ressursse andmete säilitamiseks, edastamiseks või töötlemiseks.[71]

Pahavara (*malware*) puhul on tegemist programmiga, mis kasutaja teadmata muudab arvutisüsteemi tarkvaras seadistusi või muul viisil kahjustab andmetesse sekkumise teel arvutisüsteemi. Siia alla kuuluvad programmid, mis koguvad kasutaja arvutisüsteemist informatsiooni näiteks klaviatuuriklahvide vajutuste kohta (*keylogger*) ning edastab need andmed programmis määratud kolmandatele isikutele. Lisaks loetakse pahavaraks programmid, mille abil kolmas isik saab kontrolli arvutisüsteemi üle kasutaja teadmata. Omades kontrolli arvuti üle, saab seda kasutada näiteks rämpsposti saatmiseks või DDoS rünnete teostamiseks.[72]

Kui termin pahavara tavakasutuses hõlmab ka arvutiviiruseid ja nuhkvara, siis KarS § 208 kontekstis on „pahavara“ kasutusel kitsamas mõistes, tähistamaks kõiki muid kahjulikke õiguspärase arvutikasutaja teadmata arvuti kahjustamiseks või kuritarvitamiseks kasutatavaid programme, mis ei ole nuhkvara ega arvutiviirus. Pahavara näidetena võib nimetada nt programme, mis end levitavad, kasutamata selleks teiste programmide muutmist (uss, ingl k *worm*; bakter e laviinkiri, ingl k *bacterium, chain letter*); troojalasi (ingl k *Trojan horse*); käomune (ingl k *rootkit*).[73]

Subjektiivne külg eeldab põhikoosseisus tahtlust ja koosseis loetakse täidetuks, kui isik on toime pannud levitamisteo vähemalt kaudse tahtlusega.

[69] J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. 3. trükk, Tallinn: Juura 2009, lk 560
[70] *op. cit.*, lk 560
[71] *op. cit.*, lk 560
[72] *op. cit.*, 560
[73] J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. 3. trükk, Tallinn: Juura 2009, lk 560

3.1.1.2 Ettevalmistamistegu (KarS § 208 põhjal)

Käesoleval ajal sisaldab karistusseadustik kokku viite süüteokoosseisu[74], mille ühiskonnaohtlikkuse astet on seadusandja hinnanud piisavalt kõrgeks, et kriminaliseerida ka nende tegude ettevalmistamine. Arvutikuritegude ettevalmistamine muutus karistatavaks § 216^1 lülitamisega karistusseadustikku.

§ 216^1. Arvutikuriteo ettevalmistamine

(1) Käesoleva seadustiku §-s 206, 207, 208, 213 või 217 sätestatud kuritegude toimepanemise eesmärgil selleks vastavalt kavandatud või kohandatud seadme, programmi, ka salasõna, kaitsekoodi või muude arvutisüsteemile juurdepääsuks vajalike andmete valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, samuti muude käesolevas paragrahvis nimetatud kuritegude toimepanemiseks vajalike andmete kasutamise, levitamise või muul viisil kättesaadavaks tegemise eest –

karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –

karistatakse rahalise karistusega.

(3) Kohus võib kohaldada käesolevas paragrahvis sätestatud süüteo toimepanemise vahetuks objektiks olnud eseme konfiskeerimist vastavalt käesoleva seadustiku §-s 83 sätestatule.

Paragrahviga kaitstav õigushüve on arvutisüsteemi omaniku või õiguspärase kasutaja huvi arvuti või arvutisüsteemi takistamatuks kasutamiseks.[75]

Koosseisu objektiivne külg- karistatav ettevalmistamine, mis on seotud arvutiandmetesse sekkumise, arvutisüsteemi toimimise takistamise, arvutiviiruse levitamise, arvutikelmuse ja arvutisüsteemi ebaseadusliku kasutamisega. Kõnesoleva kuriteokoosseisu objektiivse külje moodustab niisuguste andmete, programmide, seadmete valmistamine, kasutamine, levitamine või muul viisil kättesaadavaks tegemine, mille eesmärgiks on või

[74] Peale arvutikuritegude ettevalmistamise on karistatavad veel:
- Narkootilise ja psühhotroopse aine levitamise ettevalmistamine (§ 189);
- Terrorikuriteo ettevalmistamine ja üleskutse selle toimepanemisele (§ 237^2);
- Massilise korratuse organiseerimine ja ettevalmistamine ning üleskutse selles osalemisele (§ 238);
- Raha, pangakaardi ja muu maksevahendi, väärtpaberi, maksumärgi, postimaksevahendi ja selle jäljendi ning proovijärelevalve märgise võltsimise ettevalmistamine (§ 340)

[75] J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. 3. trükk, Tallinn: Juura 2009, lk 589

mille tööpõhimõte on rünnete toimepanemine arvutisüsteemide vastu, sh ründed andmete ja arvutisüsteemi toimimise vastu. Siia alla kuuluvad kõikvõimalikud häkkimisriistad (*hacking tools*), aga ka arvutiviirused, nuhkvara ja pahavara, mida kasutatakse selleks, et toime panna või võimaldada ründeid arvutisüsteemi vastu, samuti arvutisüsteemis sisalduvate andmete vastu.[76]

Subjektiivne külg- antud koosseisu suhtes tervikuna kehtib subjektiivse külje pealt vähemalt kaudse tahtluse nõue ehk teo toimepanija peab tegutsema vähemalt kaudse tahtlusega kõigi koosseisu asjaolude suhtes. Paragrahvi esimese lõike subjektiivse külje elemendina on nimetatud tegutsemist teatud eesmärgiga, mis tähendab, et subjektiivsest küljest nõuab KarS § 216^1 lg 1 kõrgeimat tahtluse vormi ehk kavatsetust.

Samas teos nii KarS § 216^1 kui § 208 tunnuste esinemisel on § 208 erinormiks, st kui on tuvastatud nuhkvara, pahavara või arvutiviiruse levitamine, siis kvalifitseeritakse tegu § 208 järgi. Kui tarkvara ei ole veel jõutud levitada, kuid tegemist on tarkvara loomisega selle levitamise eesmärgil ning levitamise ettevalmistamisega, kuulub tegevus subsumeerimisele § 216^1 järgi.[77]

3.2 EN Arvutikuritegevusevastase konventsiooni artikkel 6.2

Antud konventsiooni artikkel 6 esimene lõige sätestab seadmete kuritarvitamise, mille kohaselt konventsiooniosaline võtab seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona tahtlikult ja ilma õigusliku aluseta toimepandud järgmised teod:

a) tootmine, müük, kasutamiseks hankimine, import, turustamine või muul viisil kättesaadavaks tegemine, kui nimetatud tegevuse objekt on:

i) seade või arvutiprogramm, mis on kavandatud või kohandatud eelkõige artiklites 2–5 nimetatud tegude toimepanemiseks;

ii) arvutiparool või juurdepääsukood või sama laadi andmed, mille abil võib juurde pääseda kogu arvutisüsteemile või selle osale, et kasutada seda artiklites 2–5 nimetatud tegude toimepanemiseks;

[76] *op. cit.*, lk 589-590
[77] *op.cit.*, lk 589-590

b) punkti a alapunktides i ja ii nimetatud toote valdamine kavatsusega kasutada seda artiklites 2–5 nimetatud teo toimepanemiseks. Konventsiooniosaline võib oma seaduse kohaselt taotleda, et kriminaalvastutusele võtmise kvalifitseeriva asjaoluna arvestataks mitme sellise toote valdamist.[78]

Artikkel 6 (2) sätestab, et käesoleva artikli alusel ei kohaldata kriminaalkaristust, kui lõikes 1 nimetatud tootmise, müügi, kasutamiseks hankimise, impordi või turustamise või muul viisil kättesaadavaks tegemise või valdamise eesmärk on näiteks arvutisüsteemi lubatud katsetamine või arvutisüsteemi kaitse, mitte konventsiooni artiklites 2–5 nimetatud teo toimepanemine.

Artiklil 6 on ka kolmas lõige, mis annab konventsiooniosalisele riigile õiguse jätta lõige 1 kohaldamata, kui reservatsioon ei hõlma lõike 1 punkti a alapunktis 2 nimetatud toodete müüki või turustamist või muul viisil kättesaadavaks tegemist. Kuna Eesti vastava reservatsiooni tegemise õigust kasutanud ei ole (art 6 lg 1 punkti a mõlemad alapunktid i ja ii sisalduvad KarS §-s 216[1]), siis artikli 6 kolmandal lõikel käesolev töö pikemalt ei peatu.

Tulles tagasi artikli 6 teise lõike juurde, näeme, et konventsioon ühemõtteliselt välistab selle sätte kohaldumise niisugustele seadmetele ja arvutiprogrammidele, mille eesmärgiks on arvutisüsteemi lubatud katsetamine või arvutisüsteemi kaitse. Vastavalt EN Arvutikuritegude vastase konventsiooni selgitavale raportile[79] põhineb kogu arvutikuritegude toimepanemiseks sobilike vahendite ja tööriistade käitlemise karistatavuse kontseptsioon lõikes 1 kasutataval mõistel „*ilma õigusliku aluseta*“. See tähendab, et näiteks arvutiprogrammi, mis on kavandatud arvutikuritegude toimepanemiseks on lubatud toota, müüa või kasutamiseks hankida, importida, turustada või teha muul viisil kättesaadavaks (st KarS-i mõistes *levitada*), kui selleks on õiguslik alus.

Autor nõustub, et probleemi olemuse seisukohast on oluline lahendada küsimus, kas konventsiooni artikli 6 lg 1 punkti a mõistes *„tootmine, müük, kasutamiseks hankimine, import, turustamine või muul viisil kättesaadavaks tegemine*“ on võrdsustatav karistusseadustikus kasutatava levitamise mõistega ehk tähendab *„vastava programmi edastamist teise arvutisse, mille valdaja ei ole selleks nõusolekut andnud*“. Autori arvates viitab termin *„muul viisil kättesaadavaks tegemine*“ võimalusele käsitleda seda

[78] Arvutikuritegevusevastane konventsioon.- RT II 2003, 9, 32, arvutivõrgus kättesaadav: https://www.riigiteataja.ee/akt/550359 (24.03.2013)
[79] Convention on Cybercrime Protocol on Xenophobia and Racism and Explanatory Report. Committee of Ministers of the Council of Europe at its 109th Session, 8 Nov 2001

samatähenduslikuna levitamisega. Seda seisukohta toetab ka KarS § 216[1] lg 1, mis räägib objektiivse koosseisu kirjeldamisel nii levitamisest kui muul viisil kättesaadavaks tegemisest, kasutades seejuures sidesõna „või“ (*... levitamise või muul viisil kättesaadavaks tegemise eest...*). Sellest tulenevalt on küsimus konventsiooni artikli 6 lõikes 2 ettenähtud testimise karistatavuse väljaarvamise puudumise kohta karistusseadustikust õiguslikult asjakohane.

Eesti on Euroopa Nõukogu Arvutikuritegevusevastase konventsiooni üle võtnud siseriiklikusse seadusandlusesse, täiendades karistusseadustikku konventsioonis toodud süüteokoosseisudega. Karistusseadustiku kohaselt on enamus arvutikuritegude põhikoosseise teodeliktid ehk karistatavad sõltumata tagajärje saabumisest. 2008.a Karistusseadustiku muutmise seaduse eelnõu seletuskirja[80] kohaselt oli seadusemuudatuse eesmärgiks täiendada KarS-i selliselt, et see oleks kooskõlas nõuetega, mis on sätestatud Euroopa Nõukogu arvutikuritegevusvastase konventsioonis. Autori hinnangul ei ole soovitud tulemust sajaprotsendiliselt saavutatud ja tänast karistusõigust, eelkõige KarS §- d 208 ja 216[1] silmas pidades puuduvad meie küberturbespetsialistidel võimalused kasutada konventsioonist tulenevat vabadust käidelda arvutisüsteemide kaitsmisel või testimisel pahavara. Samuti on ohus küberkaitsevaldkonna töötajad, kelle ülesandeks on tagada (aktiivse) kaitse võimekus küberrünnete puhuks ning kes sellel eesmärgil otsivad turvasüsteemides leiduvaid varjatud vigu mittekriminaalsel eesmärgil loodud pahavara abil, rikkudes tahtmatult seadust ja pannes potentsiaalselt toime KarS § 208 ja § 216[1] järgi kvalifitseeritava süüteo.

3.3 Õiguslikud küsimused

Käesoleva uurimuse käigus on autorile selgeks saanud, et KarS § 208 ja § 216[1] ebakõla EN Arvutikuritegevuse vastase konventsiooni artikli 6 teise lõikega ja sellest tekkida võivate praktiliste probleemide ring ei ole ainus, mis tänasel päeval kehtivat KarS §-i 208 ümbritseb. Küberturbespetsialistide hirm saada kriminaalkorras karistatud arvutisüsteemi lubatud katsetamise või kaitse eesmärgil toimepandud teo eest on töö läbiv teema, kuid sellega lahutamatult seotud on mõningad teised probleemid nagu näiteks jälitustegevuse lubatavus arvutisüsteemi kaudu või arvutiprogrammi määratlemine pahavarana. Neid ja mõningaid muid praktilisi probleeme analüüsib töö alljärgnevalt.

[80] Karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 seletuskiri, arvutivõrgus kättesaadav http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=197158&u=20130517132004 (17.05.2013)

3.3.1 KarS §-i 208 eristamine §-st 207 RK lahendi põhjal

Töö koostamise ajal ainsaks KarS §-i 208 koosseisu käsitlevaks Riigikohtu seisukohaks on Riigikohtu Kriminaalkolleegiumi 25.02.2009 lahend 3-1-1-85-08[81].

Kaasuse asjaoludest tuleneb, et J. K. anti kohtu alla süüdistatuna KarS § 217 lg 2 p 2 ja § 208 lg 2 p-de 1 ning 2 järgi.

Karistusseadustiku § 208 lg 2 p-de 1 ja 2 järgi süüdistati J. K.-d selles, et tema, omamata luba Rapla Maavalitsuse arvutivõrgu kasutamiseks, eesmärgiga sulustada maavalitsuse meiliserver, ajavahemikul 8.-14. novembrini 2005, sai oma koduarvutist interneti kaudu läbi tulemüüri ligipääsu Rapla Maavalitsuse arvutivõrku. Kasutades maavalitsuse serveri e-posti teenust ja e-posti kontosid ning programme Mozilla Thunderbird, Kmail ja Evolution, saatis J. K. Rapla Maavalitsuse e-posti aadressile 2-sekundilise intervalliga elektronkirju, mille tulemusena ummistusid maavalitsuse töötajate kirjakastid. Kokku saatis J. K. maavalitsuse e-posti aadressidele 1039 laviinkirja, millest 986 kirjale oli lisatud manus. J. K. tegevuse tagajärjel ei jõudnud töötajateni tööalaselt vajalik informatsioon ja puudus võimalus elektronkirjade saatmiseks, mis häiris tööd ja põhjustas olulise materiaalse kahju summas 31 633.52 krooni. Lisaks tekitas süüdistatav moraalset kahju summas 50 000 krooni, kuna vähenes maavalitsuse autoriteet riigiasutuste, omavalitsuste ja teiste asutuste ning kodanike ees.

Pärnu Maakohtu 23. aprilli 2008. a otsusega tunnistati J. K. süüdi KarS § 207 järgi ja talle mõisteti rahaline karistus 250 päevamäära (12 500 krooni). Maakohus nõustus kaitsjaga selles, et J. K. tegevus elektronkirjade saatmisel ei olnud käsitatav arvutiviiruse levitamisena. Süüdistatav ei loonud kahjulikku programmi ega muutnud arvutiprogramme Kmail, Evolution ja Mozilla Thunderbird muu programmi levitamise eesmärgil. Sel põhjusel puudub alus käsitada tema poolt massilist elektronkirjade saatmist arvutiviiruse levitamisena. Süüdistuses KarS § 217 lg 2 p 2 järgi mõisteti J. K. õigeks.

Prokuröri apellatsioonis taotleti maakohtu otsuse tühistamist ja J. K. süüditunnistamist KarS § 208 järgi.

Kolleegiumi seisukoht (lahendit on refereeritud eelkõige KarS §-ga 208 seonduvas osas):

[81] RKKK 3-1-1-85-08 25.02.2009, arvutivõrgus kättesaadav http://www.nc.ee/?id=11&indeks=0,1,69,14211,14619,14660,14661&tekst=RK/3-1-1-85-08 (18.05.2013)

Kuni 24. märtsini 2008 kehtinud redaktsioonis nägi KarS § 207 ette vastutuse arvutivõrgu või arvutisüsteemi ühenduse rikkumise või tõkestamise eest, KarS §-s 208 aga sätestati vastutus arvutiviiruse levitamise eest. Mõlema süüteokoosseisu puhul on kaitstavaks õigushüveks arvutivõrkude ja arvutisüsteemide kasutajate õiguspärane ootus nende võrkude ja süsteemide takistamatuks kasutamiseks. Karistusseadustiku §-s 207 sätestatud objektiivne koosseis seisneb andmesideühenduse võimaluse täielikus lubamatus katkestamises vähemalt kahe arvutivõrgus oleva arvuti vahel (ühenduse rikkumine) või andmesideühenduse kiiruse lubamatus vähendamises (ühenduse tõkestamine). Karistusseadustiku §-s 208 sisalduva objektiivse koosseisu kirjeldus aga seisneb sellise arvutiprogrammi levitamises, mis võib end algsel või modifitseeritud kujul ise või teiste programmide abil arvutivõrgu kaudu edasi levitada, häirides sellisel viisil arvutite kasutamist. Sisuliselt takistatakse või häiritakse mõlemal juhul objektiivses koosseisus kirjeldatud tegude toimepanemisega arvuti, arvutivõrgu või -süsteemi kasutamist ning toimimist. Maakohus subsumeeris süüdistusaktis kirjeldatud faktilised asjaolud KarS § 207 alla, asudes seisukohale, et elektronkirjade masspostitus ei ole vaadeldav arvutiviiruse levitamisena KarS § 208 mõttes. Lähtudes arvutiviiruse mõistest ei lugenud kohus tuvastatuks, nagu oleks süüdistatav loonud kahjuliku programmi või muutnud süüdistuses loetletud programme muu programmi levitamise eesmärgil. Ka süüdistuses toodud teokirjelduses heideti J. K.-le ette arvutisüsteemi tavapärase toimimise häirimist ja takistamist, mis toimus arvutivõrgu kaudu. Süüdistuse muutmise tingiski pelgalt küsimus selle kohta, kas elektronkirjade masspostitus on käsitatav arvutiviiruse levitamisena, millele maakohus on vastanud eitavalt.[82]

Kuni 24. märtsini 2008 kehtinud redaktsioonis sätestas KarS § 207 vastutuse arvutivõrgu või arvutisüsteemi ühenduse rikkumise või tõkestamise eest. Alates 24. märtsist 2008 seisneb KarS § 207 lg 1 objektiivses koosseisus kirjeldatud tegevus arvutisüsteemi toimimise ebaseaduslikus häirimises või takistamises andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel. Seega on võrreldes varasema redaktsiooniga 24. märtsist 2008 KarS § 207 täiendava objektiivse koosseisu tunnusena lisandunud termin "ebaseaduslik". Kriminaalkolleegium märgib, et vaadeldava süüteo koosseisupärasuse tuvastamisel ei ole vajalik eraldi tõendada, et süüdlase tegu on ebaseaduslik. Teo koosseisupärasus puudub, kui arvutisüsteemi toimimise häirimiseks või takistamiseks esines isikul õiguslik alus (nt töö- või ametiülesannetest tulenev volitus).[83]

[82] RKKK 3-1-1-85-08 25.02.2009, p. 10.2, arvutivõrgus kättesaadav http://www.nc.ee/?id=11&indeks=0,1,69,14211,14619,14660,14661&tekst=RK/3-1-1-85-08 (18.05.2013)
[83] *op. cit.*, p. 12.1 (18.05.2013)

Ülaltoodud lahendist nähtuvalt tuli kohtutel lahendada kaks peamist probleemi kohtualuse tegevusele hinnangu andmisel.

Esimene neist puudutas KarS § 208 ettenähtud viiruse funktsionaalset eristamist KarS § 207 objektiks oleva arvutisüsteemi toimimise takistamisest. Siin leidis maakohus, et Karistusseadustiku §-de 207 ja 208 koosseisulised tunnused erinevad oluliselt. Arvutiviiruse levitamine leiab aset ainult viiruse kui iseleviva ja isetoimiva kahjuliku arvutiprogrammi olemasolul. Seejuures ei ole ühendus arvutivõrguga vajalik, kuna viirust saab levitada ka andmekandja vahendusel (ka ei ole arvutivõrgu olemasolu KarS § 208 koosseisuliseks tunnuseks).

Teine oluline küsimus, millel Riigikohus peatus KarS § 207 seonduvalt, puudutab objektiivse koosseisu tunnust „ebaseaduslik“. Kohus rõhutas, et kui määratlus „ebaseaduslik“ on objektiivse koosseisu tunnus, ei ole süüteo koosseisupärasuse tuvastamisel vajalik teo ebaseaduslikkust eraldi tõendada. Teisisõnu, kui teo toimepanemiseks esineb isikul õiguslik alus - näiteks töö- või ametiülesannetest tulenev volitus – siis, koosseisupärasus automaatselt puudub.

3.3.2 Arvutiprogrammi käsitlemine nuhkvara, pahavara või arvutiviirusena

Üheks köitvamaks küsimuseks, mis autoril käesoleva töö koostamise käigus tekkis, on KarS § 208 kasutatav terminoloogia ehk see, milliste tunnuste abil tuleks tarkvara liigitada nuhkvaraks, pahavaraks või arvutiviiruseks. Kuigi terminoloogia ei ole töö peamiseks uurimisküsimuseks, ennustab autor, et see tekitab tulevikus seaduse rakendajatele ulatuslikke vaidlusi.

Ainsa olemasoleva Riigikohtu lahendi pinnalt terminoloogiat puudutavat debatti ei tekkinud, kuid teadaolevalt on vastavasisuline küsimus lahendamisel alates aprillist 2013 Harju Maakohtu menetluses olevas kriminaalasjas, kus Vladimir Tšaštšinit ja tema viit kaaslast kahtlustatakse selles, et nende kontrollitav pahavara DNS-Changer nakatas viie aasta jooksul üle maailma ligi neli miljonit arvutit. Pahavara suunas arvutikasutajad tavapärastelt veebilehtedelt nendele, kus olid Tšaštšinile tulu toovad reklaamid, või vahetas mõnel lehel reklaamid ära (näiteks guugeldab kasutaja sõna „iTunes”, mille esimene vaste oli Apple’i

koduleht, kuid nakatunud arvuti suunab sellele klõpsanud kasutaja hoopis Tšaštšinile kuuluvale veebilehele www.idownload-store-music.com).[84] [85]

Eesti õigusruumis ehk karistusseadustiku kontekstis on ainsaks tugepakkuvaks materjaliks mõistete nuhkvara, pahavara või arvutiviiruse sisustamisel juba viidatud karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 ja suuresti sellel põhinevad karistusseadustiku kommentaarid. EN arvutikuritegevusevastane konventsioon ega EL Nõukogu raamotsus 2005/222/JSK nimetatud mõisteid ei defineeri.

Olukorda püüavad lahendada, kuid kokkuvõttes ei muuda seda selgemaks ka EN arvutikuritegevusevastase konventsiooni kommentaarid[86] artiklile 6, kus mööndakse, et konventsiooni väljatöötamisel arutleti pikalt selle üle, kas artikliga peaksid olema hõlmatud seadmed ja programmid, mis on välja töötatud spetsiaalselt ja ainult arvutikuritegude toimepanemiseks, jättes artikli kohaldamisalast välja nö kahetoimelised (*dual-use*) seadmed ja programmid. EN Ministrite Komitee pidas sellist lähenemist siiski liialt kitsaks ja leidis, et vastava nõude rakendamine tähendaks ebamõistlikku tõendamiskoormist kriminaalsüüdistuste esitamisel ning kokkuvõttes muudaks kogu artikli 6 praktikas kohaldamatuks.

Tarkvara funktsionaalsuse mitmetahulisuse tõttu on autor kahtleval seisukohal, kas KarS § 208 mõttes karistatavuse põhistamise eesmärgil ühe või teise arvutiprogrammi sildistamine nuhkvaraks, pahavaraks või arvutiviiruseks, on pikas perspektiivis jätkusuutlik. Oskusliku kasutaja käes võib pealtnäha kahjutu ja heaukselt loodud programmi abil toime panna küberründe. Samamoodi on küberründeks spetsiaalselt kirjutatud tarkvara sageli võimalik kasutada seaduslikel eesmärkidel näiteks võrguliikluse analüüsitööriistana. Erialakirjanduses muutuvad arutelud nö heavara ja pahavara (*goodware vs badware*) eristamise kriteeriumitest järjest aktuaalsemaks. Tuntakse ka juhtumeid, kus muidu praktilisi omadusi eviva tarkvara sisse on peidetud funktsionaalsus, mis käivitub teatud tingimuste saabudes või kaugjuhtimise teel võimaldab süsteemi kahjustamist, andmete salajast edastamist vmt.[87] Unustada ei tohi, et lisaks nuhkvarale, pahavarale ja arvutiviirustele

[84] L. Tankler. Maailmakuulsa küberpätina vahi all: Vladimir Tšaštšini esimene sõnavõtt.- Eesti Päevaleht 28.03.2012, arvutivõrgus kättesaadav http://www.epl.ee/news/eesti/maailmakuulsa-kuberpatina-vahi-all-vladimir-tsastsini-esimene-sonavott.d?id=64127905 (18.05.2013)

[85] Küberkuritegudes süüdistatav Tšaštšin end kohtus süüdi ei tunnistanud.- www.delfi.ee uudised 01.04.2013, arvutivõrgus kättesaadav http://www.delfi.ee/news/paevauudised/110_112/kuberkuritegudes-suudistatav-tsastsin-end-kohtus-suudi-ei-tunnistanud.d?id=65906250, (18.05.2013)

[86] Convention on Cybercrime Protocol on Xenophobia and Racism and Explanatory Report. Committee of Ministers of the Council of Europe at its 109th Session, 8 Nov 2001, lk 80

[87] R. W. Taylor, T. J. Caeti, D. K. Loper, E. J. Fritsch, J. Liederbach. Digital Crime and Digital Terrorism. PearsonEducation Inc., Upper Saddle River, New Jersey 2006, lk 159-161

eristatakse veel hallvara (*grayware*), mida ei saa paigutada ühessegi KarS §-s 208 nimetatud pahavara kategooriasse.

Olukord, kus süüteokoosseisus kasutatavad definitsioonid ei ole lõpuni selged, muudab õigusvastase teo toimepanija süüdimõistmise kui mitte võimatuks, siis vähemalt äärmiselt keeruliseks. Süüdistatava seisukohalt on kahtlemata ahvatlev apelleerida *in dubio pro reo* põhimõttele ning paluda tõlgendada kõik kahtlused enda kasuks. Tõsiasi, et kübermaailmas teedrajavas Eestis ei ole tänaseni kohtupraktikat KarS § 208 rakendamisel, on kas õnnelik juhus või peitub siin taga prokuratuuri soovimatus testida selgelt piiritlemata koosseisu rakendatavust kohtus. Igal juhul oleks seadusandjal põhjust kaaluda KarS § 208 objektiivse koosseisu täiendamist teo eesmärgiga, läbi mille oleks võimalik hinnata toimepanija teadlikkust levitatava tarkvara kahjulikest omadustest.

3.3.3 Jälitustegevus

Punktis 3.3.1 käsitletud Riigikohtu lahendi pinnalt võib järeldada, et Riigikohus on sidunud mõiste „ebaseaduslik“ KarS § 207 kontekstis omaniku või valdaja nõusoleku puudumise või töö- või ametivolituste puudumise või siseriiklikest õigusaktidest tuleneva mandaadi puudumisega. Kuna ülejäänud arvutikuritegude paragrahvid (KarS §-d 206, 213, 217) kasutavad oma objektiivses koossisus sama määratlust, on autor seisukohal, et terminil „ebaseaduslik“ on arvutikuritegude koosseisudes läbivalt sama tähendus.
Sellest tulenevalt jääb arusaamatuks, miks ei sisalda Kars § 208 koosseis määratlust „ebaseaduslik“.

Tänaseks on olukord muutunud ning vajadus käidelda pahavara on omandamas üha kriitilisemat tähtsust. Tulenevalt karistusseadustiku § 208 sõnastusest võib õiguskaitseasutustel praktikas tekkida probleeme näiteks kriminaalasjade menetlemisel. Töös on varasemalt viidatud meedias levinud informatsioonile nuhkvara kasutamisest erinevate riikide õiguskaitseorganite poolt. Eelkõige ongi KarS § 208 tänane sõnastus potentsiaalses konfliktis jälitusasutuste võimaliku sooviga kasutada nuhkvara kurjategijate suhtluse jälgimisel arvutisüsteemis. Paratamatult tõstatub küsimus niisugusel viisil kogutud teabe seaduslikkusest ja hilisemast kasutamise võimalikkusest kohtumenetluses.

Julgeolekuasutuste seaduse § 2 kohaselt on julgeolekuasutuste tegevuse eesmärk tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning julgeolekupoliitika kujundamiseks ja riigikaitseks vajaliku teabe

kogumine ja töötlemine. Vastavalt sama seaduse §-le 25 lg 2 võib julgeolekuasutus oma pädevuse piires kuriteo tõkestamiseks piirata isiku õigust sõnumi saladusele, kui on olemas piisavad andmed ettevalmistatava või toimepandava kuriteo kohta. [88]

„Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise korra“ § 1 lg 1 p 2 kohaselt teostab Kaitsepolitseiamet isiku õiguse piiramisel sõnumi saladusele täiesti salajaste meetodite ja vahendite kasutamisega telegraafi, telefoni või muu tehnilise sidekanali kaudu edastatava sõnumi või muu teabe pealtkuulamist, -vaatamist või salvestamist, kasutades vastavaid tehnilisi vahendeid või vastavalt kohaldatud tehnoloogiaid ning § 1 lg 1 p 3 kohaselt muul viisil edastatava teabe pealtkuulamist, -vaatamist või salvestamist, paigaldades selleks vajalikke tehnilisi vahendeid.[89]

Nimetatud korra § 1 lõike 2 kohaselt hõlmab telegraafi, telefoni või muu tehnilise sidekanali kaudu edastatava sõnumi või muu teabe pealtkuulamine, -vaatamine või salvestamine kõiki audio-video, telekommunikatsioonivõrgu signaalide või kosmoseside edastamise liike.[90]

Eelnevalt oli teises peatükis toodud välja FinFisheri-nimelise nuhkvara kasutamise kahtlus muuhulgas ka Eesti uurimisorganite poolt. Nimetatud nuhkvara võimaldab silma peal hoida kurjategijate meilivahetusel, saades selliselt ka olulist informatsiooni toimepandavatest kuritegudest või nende ettevalmistamisest ning võimaldades sellisel juhul kuritegusid ennetada. Kuna vastavalt „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise korrale“ on teabe hankimise meetodid täiesti salajased, ei ole ka võimalik teha järeldust, millisel viisil uurimisasutus oma tegevust organiseerib ja milliseid vahendeid kasutades teavet saab. Küll aga kui tuvastada meilivestlust jälgides kuriteo toimepanemine või ettevalmistamine, eeldab see võõrasse arvutisüsteemi tungimist ning sinna nuhkvara paigaldamist. Nuhkvara levitamine on aga KarS § 208 järgi karistatav, vaatamata antud tegevuse eesmärgile.

Olukorda riigi seisukohast hinnates, tuleb kahtlemata arvesse võtta riigi kohustust tagada oma kodanike turvalisus ning sellest tulenevat õigust piirata proportsionaalsel määral

[88] Julgeolekuasutuste seadus.- RT I, 2001, 7, 17... RT I, 26.03.2013, 15, arvutivõrgus kättesaadav https://www.riigiteataja.ee/akt/126032013015 (26.04.2013)
[89] Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord.-RT I, 07.02.2013, 9, vastu võetud 06.06.2001 nr 76, arvutivõrgus kättesaadav https://www.riigiteataja.ee/akt/107022013009 (26.04.2013)
[90] *op. cit*., (26.04.2013)

isikute põhiõigusi. Euroopa Inimõiguste kohus oma 6. märtsi 2012 otsuses *Leas vs Eesti (59577/08)* on öelnud, et mis tahes kriminaalmenetluses võib esineda võistlevaid huvisid, nt riigi julgeolek või vajadus kaitsta tunnistajaid kättemaksu eest või hoida saladuses politsei meetodeid kuriteo uurimisel, mida tuleb arvestada süüdistatava õiguste vastukaaluna.[91]

Töö autori seisukohast ei ole siiski kriminaalmenetluse seadustikus ja muudes vastavates õigusaktides nimetamata meetodite rakendamine kooskõlas kriminaalmenetluse läbipaistvuse ega jälitustegevuse põhimõtetega ning riigipoolsed tegevused, mis tooksid tavakodanikule kaasa kriminaalvastutuse, peaksid olema keelatud või omama kindlasti vastavat volitusnormi seaduses.

3.4 Autori seisukoht KarS § 208 muutmisvajaduse osas

Hetkel kehtiva karistusseadustiku arvutikuritegude koosseisud ning nende tegude eest ettenähtud karistusmäärad on vastavuses Euroopa Nõukogu Arvutikuritegevusevastase konventsiooniga. Vähemalt taotles niisugust vastavust karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 seletuskiri[92], millega viidi sisse ulatuslikud muudatused arvutikuritegude paragrahvidesse. Kuivõrd peale 2008.aastat ei ole nimetatud koosseise muudetud, tuleb järeldada, et riik on veendunud KarS-i vastavuses konventsioonile.

Kuigi konventsiooni arvutikuritegude osa on üsna üheselt siseriiklikusse õigusesse üle võetud, leiame KarS-ist teatud erisusi. Üheks selliseks erisuseks on KarS § 208 koosmõjus KarS §-ga 216[1], mis ei arvesta konventsiooni võimaldatud erandit mitte kohaldada kriminaalkaristust nuhkvara, pahavara või arvutiviiruse levitamise eest juhul, kui selle eesmärgiks on arvutisüsteemi lubatud katsetamine või arvutisüsteemi kaitse (art 6.2).

Ülaltoodud kahe paragrahvi, KarS § 208 ja KarS § 216[1] eesmärgiks on karistada nuhkvara, pahavara ja arvutiviiruse levitamist ning selletoimeliste programmide ettevalmistamist. Kõikvõimalike statistikate kohaselt ei ole oht sattuda küberründe ohvriks

[91] EIKo 06.03.2012, 59577/08, Leas vs. Eesti, arvutivõrgus kättesaadav https://www.riigiteataja.ee/failid/KOHTUASI%20LEAS%20vs%20EESTI.pdf (27.04.2013)
[92] Karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 seletuskiri, arvutivõrgus kättesaadav http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=197158&u=20130517132004 (17.05.2013)

kunagi varem olnud nii käegakatsutav kui see on täna ning infotehnoloogiaseadmete levides ennustavad prognoosid ohutaseme jätkuvat tõusu.[93]

Küberrelvade omamine, loomine ning katsetamine (eelkõige USA, Lõuna-Korea, Iisrael, UK, India[94]) on muutumas järjest enamate riikide puhul normiks ja saamas elementaarseks riigi julgeoleku tagamise vahendiks. Ilmselt puudub vaidlus selles, et ühestki domeenist, sh küberruumist tulenevate potentsiaalsete ohtudega ei saa efektiivselt võidelda vahenditega, mille tõhusust ei ole varem katsetatud. Käesoleval hetkel puudub Eesti küberturvalisusega tegelevatel IT-spetsialistidel õigus luua programmide ja süsteemide turvalisuse kontrollimiseks ja katsetamiseks „laboratoorset" pahavara, kuna niisugusele tegevusele võib järgneda KarS § 208 ja KarS § 216[1] järgi.

Autor näeb kolme võimalust töös kirjeldatud olukorra parandamiseks:

a) Lubada teatud juhtudel käidelda nuhkvara, pahavara või arvutiviirusi ja täiendada karistusseadustikku vastava sättega. Normitehniliselt oleks üheks võimaluseks näha ette KarS § 208 koosseisust erand ja välistada levitamise karistatavus näiteks arvutisüsteemi turvalisuse testimise eesmärgil toimepandud teo või küberründe tõrjumise eesmärgil salajaste või delikaatsete andmete kaitsmiseks toimepandud teo korral.
b) Teine tee saavutamaks vastavust EN arvutikuritegevusevastase konventsiooniga on artikli 6 teise lõike otsesõnu ülevõtmine siseriiklikusse õigusesse. Vastavalt karistusseadustiku täiendamine muudaks oluliselt avaramaks arvutisüsteemide turvalisuse testimise ja riigi julgeoleku huvides info kogumise võimalused.
   Normitehniliselt tähendaks see KarS § 216[1] koosseisu täiendamist uue lõikega.
c) EN Arvutikuritegevusevastase konventsiooni artiklis 6.2 toodud testimise lubatavuse ülevõtmine välistaks konkreetsete tegevuste osas vastutuse vastavate seadmete või arvutiprogrammide käitlemise, sh levitamise eest ning oleks selliselt tervitatav. Autori hinnangul on aga võimalik saavutada mõjult samaväärne tulemus, täiendades KarS § 208 objektiivset koosseisu määratlusega „*ebaseaduslik*" (konventsiooni keelekasutuses „ilma õigusliku aluseta") nagu see on kirjas muudes arvutikuritegude koosseisudes.

[93] J. L. Bayuk, J. Healy, P. Rohmeyer, M. H. Sachs, J. Schmidt, J. Weiss. Cyber Security Policy Guidebook. A John Wiley&Sons,Inc., Publications 2012, lk 230-232
[94] Arvutivõrgus kättesaadav http://en.wikipedia.org/wiki/Cyber_Command

Nimetatud lahendus oleks kõige tõhusam, kuna sellega saavutataks kaks eesmärki samaaegselt: esiteks välistataks sellega vastutus levitamisteo eest arvutisüsteemide lubatud katsetamise või volitatud kaitse eesmärgil ning teiseks looks võimaluse siseriikliku õigusega anda korra- või riigikaitse ülesannete täitmiseks (eelkõige jälitustegevuse eesmärgil) mandaat pahavara tunnustele vastava tarkvara levitamiseks.

Autori soovitus KarS § 208 lg 1 uueks sõnastuseks:

(1) Nuhkvara, pahavara või arvutiviiruse ebaseadusliku levitamise eest- ... .

KOKKUVÕTE

Käesolev töö keskendus küsimusele, kas karistusseadustiku § 208 toodud kuriteokoosseisu kriminaliseerimine ilma EN Arvutikuritegevusevastase konventsioonis toodud reservatsioonita on põhjendatud ning töös vaadeldakse küberrelvade, sh pahavara loomist ning jõutakse järeldusele, et küberrelvade loomine on Eesti karistusseadustiku kohaselt keelatud. Eesti karistusseadustik on KarS § 208 sõnastuses jäik ning keelab igasuguse arvutiviiruse, nuhkvara ning pahavara levitamise, olenemata selle eesmärgist. Töös näidetena toodud küberõppused on selge näide vajaliku kogemuse omandamisest õppuse käigus, kuid antud tegevus iseenesest kvalifitseerub karistusseadustiku § 208 järgi ning on seetõttu keelatud, sama kehtib ka turvatestimise teenuse pakkumise suhtes. Samas ei ole töös toodud näidete põhjal küberrelvade omamine või loomine enam uudiseks või saladuseks.

Näiteks USAs luuakse relvi riigi julgeoleku huvides või sõjalisel eesmärgil. Seega on teatud juhtudel võimalik luua nii arvutiviiruseid, nuhk- ning pahavara ning kasutada neid küberrelvadena.

Töö hüpoteesiks oli, et kuni KarS § 208 sõnastus püsib 2008.a redaktsioonis muutumatuna, kujutab KarS §-s 216[1] kirjeldatud ettevalmistamistegu kõige reaalsemat ohtu IT-turvalisusega tegelevatele praktikutele sattuda kriminaaluurimise alla.

Antud juhul on tegemist kahetsusväärse olukorraga, kus karistusseadustik ei ole kaasa läinud infoühiskonna pideva arenguga. Suur osa kuritegudest ning kurjategijatest on liikunud küberruumi ning seeläbi suureneb ka vajadus ennast nende kurjategijate vastu kaitsta. Et seda teha, on vaja inimesi, kes looksid uutele viirustele vastupanu osutavaid antiviiruseid või viiruseid, mis hävitavad esialgse. Praegusel hetkel oleks antiviiruse looja tegevus ebaseaduslik, olenemata sellest, et tema tegevuse eesmärk ei ole kuritegelik.

Seega on kinnitust leidnud töös toodud väide, et Eesti karistusseadustik vajab täiendamist ning vajalik on Euroopa Nõukogu Arvutikuritegevusevastase konventsiooni artikli 6.2 ülevõtmine siseriiklikusse seadusandlusesse, tagamaks võimaluse teostada arvutite turvasüsteemide katsetusi, luua teatud juhtudel arvutiviiruseid ning pahavara ja tagada taoliste kaitstud keskkonnas katsetatavate arvutiviiruste loojate tegevuse seaduslikkus.

Autori hinnangul parimaks meetodiks selle tulemuse saavutamiseks oleks § 208 koosseisu täiendamine määratlusega „ebaseaduslik“.

THE COMPLIANCE OF THE §§ 208 AND 216[1] OF THE ESTONIAN CRIMINAL CODE WITH THE ARTICLE 6(2) OF THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME IN THE FIGHT AGAINST CYBERCRIME.

Summary

Main keywords in this thesis are: Estonian Criminal Code and it´s compliance with the Council of Europe Convention on Cybercrime´s Article 6.2, whether there is a possibility to create cyberweapons according to the Estonian Criminal Code and should the Criminal Code be complemented with the Article 6.2 of the Convention in order to allow the emission of malware, spyware or computerviruses when it is for the authorised testing or protection of a computer system.

The thesis have been divided into three chapters. and it has been written in Estonian.

Chapter one contains the main strategys to prevent cybercrime, main focus is on the Council of Europe Convention on Cybercrime, on the Cybersecurity Strategy of the European Union and on the Estonian Strategy of Cybersecurity 2008-2013.

Chapter two focuses on the ways of using cyberweapons and how the passive defence has turned into active defence, caused by the fast development of the information tehcnology.

Chapter three focuses on the need of implementing Convention´s Article 6.2 into internal law, so it would be allowed in some cases to create computer viruses and malware to protect the computersystems from the outside attackers.

Finally the author has come to the conclusion that it is necessary to supplement the Estonian Criminal Code with the Convention´s Article 6.2, so it would be legitimate to emission computer viruses and malware for the authorised testing or protection of a computer system.

Katrin Kabel

20.05.2013

Kasutatud kirjandus

1. A. Klimburg (Ed.). National Cyber Security Framework Manual. NATO CCD COE Publication: Tallinn 2012;
2. Convention on Cybercrime Protocol on Xenophobia and Racism and Explanatory Report. Committee of Ministers of the Council of Europe at its 109th Session, 8 Nov 2001;
3. E. Tikk. Comprehensive legal approach to cyber security. Tartu Ülikooli Kirjastus 2011;
4. Euroopa Liidu Küberkaitse strateegia- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, arvutivõrgus kättesaadav http://ec.europa.eu/news/science/130212_et.htm;
5. I. Lachow. Active Cyber Defence. A Framework for Policymakers. Center for a New American Security. Policy Brief, February 2013;
6. J. L. Bayuk, J. Healy, P. Rohmeyer, M. H. Sachs, J. Schmidt, J. Weiss. Cyber Security Policy Guidebook. A John Wiley&Sons,Inc., Publications 2012;
7. J. Sootak, P. Pikamäe. Karistusseadustik. Kommenteeritud väljaanne. 3. trükk, Tallinn: Juura 2009;
8. K. Geers. Strategic Cyber Security. NATO CCD COE Publication 2011;
9. Küberjulgeoleku strateegia 2008-2013, arvutivõrgus kättesaadav: http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013(1).pdf**;**
10. M. Klang. A Critical Look at the Regulation of Computer Viruses. International Journal of Law and Information Technology, Vol. 11 No. 2, Oxford University Press 2003;
11. M. D. Goodman, S. W. Brenner. The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology. Vol. 10 No 2. Oxford University Press 2002;
12. N. Burns & J. Price. Securing Cyberspace. A New Domain for National Security. The Aspen Institute 2012;
13. O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel. The Law of Cyber-Attack. California Law Review 2012;

14. P. Lorents, R. Ottis. Knowledge based Framework for Cyber Weapons and Conflict. Conference on Cyber Conflict. Proceedings 2010. CCD COE Publications 2010;
15. R. I. Raether Jr. Data Security and Ethical Hacking. Point to Consider for Eliminating Avoidable Explosure. Business Law Today. September/October 2008;
16. R. J. Kroczynski. Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited? Fordham Intellectual Property, Media&Entertainment Law Journal 2007-2008;
17. R. W. Taylor, T. J. Caeti, D. K. Loper, E. J. Fritsch, J. Liederbach. Digital Crime and Digital Terrorism. PearsonEducation Inc., Upper Saddle River, New Jersey 2006;
18. W. Gragido, J. Pirc. Cybercrime and Espionage. An Analysis of Subversive Multivector Threats. Syngress Publications 2011;

Kasutatud normatiivmaterjalid

19. Arvutikuritegevusevastane konventsioon 23.11.2001.- RT II 2003, 9, 32;
20. Euroopa Parlamendi ja Nõukogu diretiiv 2002/58/EÜ, Euroopa Liidu Teataja L 201, 31/07/2002 P.0037-0047;
21. Euroopa Liidu Nõukogu 24.02.2005 raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta;
22. Karistusseadustik. 06.06.2001.- RT I 2001, 61, 364…RT I, 20.12.2012, 12;
23. Julgeolekuasutuste seadus. 20.12.2000. - RT I, 2001, 7, 17... RT I, , 15;
24. Karistusseadustiku muutmise seadus.- RT I 2008, 13, 87;
25. Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord.- RT I, 07.02.2013, 9, vastu võetud 06.06.2001 nr 76;
26. „Küberjulgeoleku strateegia 2014-2017“ koostamise ettepaneku heakskiitmine. 21.03.2013.- RT III, 26.03.2013, 9;

Kasutatud kohtupraktika

27. EIKo 06.03.2012, 59577/08, *Leas vs. Eesti*, arvutivõrgus kättesaadav https://www.riigiteataja.ee/failid/KOHTUASI%20LEAS%20vs%20EESTI.pdf

28. RKKK 3-1-1-85-08 25.02.2009, arvutivõrgus kättesaadav http://www.nc.ee/?id=11&indeks=0,1,69,14211,14619,14660,14661&tekst=RK/3-1-1-85-08

Kasutatud elektroonilised materjalid

29. Euroopa Komisjoni netilehekülg http://ec.europa.eu/news/science/130212_et.htm
30. Välisministeeriumi kodulehekülg http://www.vm.ee/?q=node/8013
31. E. Nakashima. With Plan-X, Pentagon seeks to spread U. S. Military might to cyberspace. -The Washington Post 30.05.2012. Arvutivõrgus kättesaadav http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html
32. Euroopa Komisjoni netilehekülg http://ec.europa.eu/news/science/130212_et.htm
33. FT: Superviirus jälgib Iraani tuumaprogrammi. 29.05.2012. Arvutivõrgus kättesaadav http://www.delfi.ee/news/paevauudised/valismaa/ft-superviirus-jalgib-iraani-tuumaprogrammi.d?id=64465298
34. http://en.wikipedia.org/wiki/Cyber_Command
35. http://www.answers.com/topic/passive-defense
36. http://www.ccdcoe.org/172.html
37. http://www.ccdcoe.org/publications/BCS2010AAR.pdf
38. http://www.eata.ee/eesti-nato-s/kuberjulgeoleku-strateegia
39. http://www.eccouncil.org/courses/licensed_penetration_tester.aspx
40. http://www.infowar-monitor.net/
41. http://www.nato.int/cps/en/natolive/topics_78170.htm
42. http://www.techopedia.com/definition/23172/back-hack
43. J. Wolverton. The Pentagon is developing cyberweapons that launch without human intervention.- The New American 22.06.2012. Arvutivõrgus kättesaadav http://thenewamerican.com/usnews/item/11810-the-pentagon-is-developing-cyberweapons-that-launch-without-human-intervention
44. Justiitsministeeriumi kodulehekülg, arvutivõrgus kättesaadav http://www.just.ee/33098
45. Karistusseadustiku muutmise seaduse eelnõu nr 166 SE II-1 seletuskiri, arvutivõrgus kättesaadav

http://www.riigikogu.ee/?page=eelnou&op=ems2&emshelp=true&eid=197158&u=20130517132004

46. Küberkuritegudes süüdistatav Tšaštšin end kohtus süüdi ei tunnistanud.- www.delfi.ee uudised 01.04.2013, arvutivõrgus kättesaadav http://www.delfi.ee/news/paevauudised/110_112/kuberkuritegudes-suudistatav-tsastsin-end-kohtus-suudi-ei-tunnistanud.d?id=65906250
47. L. Ferran. New version of Stuxnet-Related Cyber Weapon Discovered.- ABC News, arvutivõrgus kättesaadav http://usa.kaspersky.com/about-us/press-center/in-the-news/new-version-stuxnet-related-cyber-weapon-discovered
48. L. Tankler. Maailmakuulsa küberpätina vahi all: Vladimir Tšaštšini esimene sõnavõtt.- Eesti Päevaleht 28.03.2012, arvutivõrgus kättesaadav http://www.epl.ee/news/eesti/maailmakuulsa-kuberpatina-vahi-all-vladimir-tsastsini-esimene-sonavott.d?id=64127905
49. R. O´Harrow Jr. Understanding cyberspace is key to defending against digital attacks.- The Washington Post 03.06.2012. Arvutivõrgus kättesaadav http://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defending-against-digital-attacks/2012/06/02/gJQAsIr19U_story_1.html
50. RIA kodulehekülg, arvutivõrgus kättesaadav https://ria.ee/cert/
51. RIA: Meil ei ole FinFisheri nuhkvaraga kokkupuuteid olnud.- Arvutivõrgus kättesaadav http://www.e24.ee/1175412/ria-meil-ei-ole-finfisheri-nuhkvaraga-kokkupuuteid-olnud/
52. Siseministeerium ei kinnitanud ega lükanud ümber FinFisheri nuhkvara võimalikku kasutamist.- Arvutivõrgus kättesaadav http://www.e24.ee/941996/siseministeerium-ei-kinnitanud-ega-lukanud-umber-finfisheri-nuhkvara-voimalikku-kasutamist/
53. Valitsuste kasutatava võimsa nuhkvara jälgi leiti ka Eestist.- Arvutivõrgus kättesaadav http://www.e24.ee/941062/valitsuste-kasutatava-voimsa-nuhkvara-jalgi-leiti-ka-eestist/
54. Viirustõrjeprogrammid mureliku tähelepanu fookuses. -ERR teadusuudised 06.06.2012. Arvutivõrgus kättesaadav http://forte.delfi.ee/news/digi/viirusetorjeprogrammid-mureliku-tahelepanu-fookuses.d?id=64497264
55. Välisministeeriumi kodulehekülg http://www.vm.ee/?q=node/8013

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Katrin Kabel (sünnikuupäev 31.03.1981)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Eesti Karistusseadustiku § 208 ja 216[1] vastavus Euroopa Nõukogu Arvutikuritegevusevastase konventsiooni artiklile 6.2 võitluses küberkuritegevusega,

mille juhendaja on Lauri Aasmann (Legal & Policy Branch Chief, NATO Cooperative Cyber Defence Centre of Excellence)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas_____(*kuupäev*)