TARTU ÜLIKOOL

Euroopa Kolledž

Magistritöö

Kairi Listmann

EUROOPA LIIDU KÜBERJULGEOLEKU STRATEEGIA RAKENDAMINE KÜBERRÜNNAKUTE KORRAL EESTI KRIITILISE INFRASTRUKTUURI NÄITEL

Juhendaja: Piret Pernik, MA

Kaasjuhendaja: Jaan Masso, PhD

Tartu 2015

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite seisukohad, ning kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

/töö autori allkiri/

Kairi Listmann

Kaitsmine toimub 28.mail Lossi 36 auditooriumis 103.

Retsensent: Ramon Loik (MA)

LÜHIKOKKUVÕTE

Käesoleva töö eesmärgiks on Euroopa Liidu küberjulgeoleku strateegiast lähtuvalt võrrelda Eesti kriitilise infrastruktuuriga ettevõtete ja Eesti riigi küberjulgeoleku strateegiaid küberrünnakute eest kaitsmisel. Töö eesmärki aitavad saavutada neli uurimisküsimust, mis selgitavad küberjulgeoleku kujunemist, avaliku sektori ja erasektori koostööd, küberrünnakute liigitust ning kriitilise infrastruktuuri olemust ja kaitse vajalikkust. Teoreetilistest käsitlustest kasutatakse klassikalise julgeoleku kompleksi ning Kopenhaageni koolkonna teooriat.

Töö eesmärki aitavad saavutada kvalitatiivsetest uurimismeetoditest dokumentide analüüs ning poolstruktureeritud ekspertintervjuud. Dokumentide analüüsimisel võrreldi Euroopa Liidu ja Eesti küberjulgeoleku strateegiaid, mille tulemusena selgus strateegiate sarnasus ning rõhuasetus kriitilisele infrastruktuurile. Ekspertintervjuud viidi läbi seitsme energia ning telekommunikatsiooni ettevõtte eksperdi seas, mille tulemusel toodi peamiste kitsaskohtadena välja koostöö puudulikkus, avaliku sektori killustatus, investeeringute vähesus küberkaitsesse ning küberjulgeoleku teadlikkuse madal tase.

Peamiste ettepanekutena soovitati suurendada avaliku sektori ja erasektori koostööd läbi koolituste, infopäevade ning regulaarsete kohtumiste. Riigi Infosüsteemi Amet võiks edastada kriitilise infrastruktuuriga ettevõtetele kord poolaastas informatsiooni aktuaalsetest küberohtudest ning riik teavitada ettevõtteid Euroopa Liidus toimuvatest konverentsidest, parima praktika vahetamise võimalustest ja rahvusvahelistest koolitustest. Riik võiks lisaks omalt poolt küberjulgeoleku valdkonda rohkem politiseerida ning seeläbi tagada suurem investeeringute maht küberkaitsesse.

Märksõnad: küberjulgeolek, kriitiline infrastruktuur, avaliku sektori ja erasektori koostöö, küberrünnakud, strateegiad, Kopenhaageni koolkond.

SISUKORD

LÜHENDID, MÕISTED

CCD COE – NATO Koostöö Küberkaitse Kompetentsikeskus

ENISA – Euroopa Võrgu- ja Infoturbeamet

IKT – info- ja kommunikatsioonitehnoloogia

KII – kriitilise informatsiooni infrastruktuur

NIPP – siseriiklik infrastruktuuri kaitseplaan (USA-s)

PPP – (*public-private partnership*) avaliku ja erasektori koostöö

PwC - PricewaterhouseCoopers

RIA – Riigi Infosüsteemi Amet

CERT - viitab organisatsioonile, kes tegeleb turvaintsidentidega CERT tegevuse raamistikus, jagades informatsiooni infoturbeintsidentidest ja teavitades turvaohtudest.[1]

DDoS – (*Distributed Denial of Service*) hajutatud teenuse tõkestamise rünnak ühelt isikult või isikute rühmalt, kui mõne ettevõtte serverile, ruuterile või arvutivõrgule esitatakse massiliselt sisutühje päringuid robotvõrgu abil.[2]

DoS – (*Denial of Service*) teenuse tõkestamise rünnak, kus suur hulk üheaegseid päringuid viib serveri rivist välja.[3]

Infoturve - infovarade (andmed, riistvara, tarkvara, side, infrastruktuur, personal) turvalisuse tagamine.[4]

INSA – USA organisatsioon, mille eesmärgiks analüüsida ning uurida riigi julgeolekut puudutavaid valdkondi[5]

IP aadress - on arvutite ja muude arvutivõrgus toimivate seadmete omavaheliseks suhtlemiseks arvutivõrgus vajalik unikaalne aadress.[6]

ISKE - kolmeastmeline turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks

Pingimine – arvutivõrgu võrguühenduse programm, mille abil saab tuvastada, kas server või muu võrguseade on IP-aadressilt ligipääsetav

Võrguturve – võrgu turvalisuse tagamine

---

[1] CERT. [https://www.ria.ee/cert] 05.03.2015
[2] Mis on DDos küberrünnak. [https://arvutiturve.wordpress.com/2010/03/21/mis-on-ddos-kuberrunnak/] 05.03.2015
[3] DDoS. [http://www.arvutikaitse.ee/arvutikaitse-algtoed/ddos/] 05.03.2015
[4] EKSS. [http://www.eki.ee/dict/ekss/index.cgi?Q=infoturve&F=M] 05.03.2015
[5] INSA. [http://www.insaonline.org/i/a/i/a/index2.aspx?hkey=10d3ba7c-b95b-4298-9cdb-8cb4a343e161] 05.03.2015
[6] IP-aadress. [http://www.eava.ee/~anur/internet/misted.html] 05.03.2015

SISSEJUHATUS

Igapäevaselt on riigid, rahvusvahelised organisatsioonid ning ühiskonnaliikmed seotud interneti ja e-teenustega, mis võimaldavad kiiremini ja hõlpsamalt igapäevaelu organiseerida. Näidetena võib tuua mobiilse interneti nutiseadmetes või digitaalallkirja andmise võimaluse. Ühiskond on suuremal või vähemal määral kursis ohtudega, mida tehnoloogia kiire areng endaga kaasa toob. Samas ei pruugita tajuda ohte, mida küberrünnak võib põhjustada kriitilise tähtsusega infrastruktuurile nagu pangandus, telekommunikatsioon, elekter.

Töö aktuaalsust ja teemavalikut võib põhjendada asjaoluga, et internetipõhised teenused ning tehnoloogia arenevad, suurendades igaühe sõltuvust internetist. Samal ajal kui sõltuvus internetist kasvab, olenevad ka isikuvabadused, heaolu ja elukvaliteet üha enam info- ja võrguturbest.[7] Kui tehnoloogia areneb küberohtudele keskendumisest kiiremini, võivad tagajärjed olla ohuks inimeste tervisele, elule või kahjustada riiklikku julgeolekut.

Saksamaa küberjulgeoleku strateegiast lähtuvalt on küberruumi puudutavad küsimused muutunud 21. sajandil eluliselt tähtsateks.[8] Kui internetiühendus on katkenud ja hädaolukorras ei ole võimalik ligi pääseda elektroonilistele haiguslugudele, siis võib tekkida reaalselt oht inimese elule, sest arstidel puudub rünnakust tingituna patsiendi ravimiinfo.[9] Oktoobris 2011. aastal põhjustas küberrünnak Suurbritannia nutitelefonide ettevõtte andmekeskuses ulatusliku süsteemivea, mis takistas mitmel miljonil inimesel sõnumeid ning e-kirju üle maailma saata, tekitades finantssektorile suure kahjumi.[10] Seega kui esineb häireid telekommunikatsiooni või pangandusteenuseid pakkuvate

[7] Euroopa Majandus- ja Sotsiaalkomitee arvamus (2013) punkt 3.1
[8] Federal Ministry of Interior. Cyber Security Strategy for Germany (2011) p. 1
[9] Euroopa Majandus- ja Sotsiaalkomitee arvamus (2013) punkt 3.1
[10] Daskala, B., Dekker, M., Karsberg, C. Cyber Incident Reporting in the EU (2012) p. 3

ettevõtete teenustes, ei pruugita aimata, et probleemide nagu side- või kaardimaksehäirete taga, võivad olla küberrünnakud.

Käesoleva töö eesmärgiks on Euroopa Liidu (edaspidi: EL) küberjulgeoleku strateegiast lähtuvalt võrrelda Eesti kriitilise infrastruktuuriga (edaspidi: KII) ettevõtete ja Eesti riigi strateegiat küberrünnakute eest kaitsmisel. Töö eesmärki täpsustatakse konkreetsemalt väitega, et Eesti riigi ja KII ettevõtete strateegiad küberrünnakute eest kaitsmisel pole omavahel kooskõlas, mis omakorda suurendab süsteemide haavatavust ning millel võivad olla olulised tagajärjed ühiskonna toimimisele ja riigi julgeolekule. Ettevõtted lähtuvad äriloogikast, eesmärgiga teenida kasumit ning minimeerida kulusid. Samas riigile on teatud riskid elulise tähtsusega, mida kasumile orienteeritud ettevõtted ei tähtsusta ja mille vastu ei rakendata piisavaid turvameetmeid.

Eesti küberjulgeoleku strateegia 2008-2013 [11] ülevaatest selgub, et uurimused küberjulgeoleku valdkonnas on vajalikud, sest Eestist lähtuvalt on tarvis välja selgitada, kuidas saaks küberjulgeoleku alast regulatsiooni paremaks muuta, eeskätt erasektorit silmas pidades. Ettevõtteid avaliku sektori initsiatiivil julgustades, suudetakse tagada parem KII kaitse küberrünnakute eest[12]. Käesolevas töös keskendutakse Eestile, sest Eesti on nii NATO kui ka EL hinnangul üks eesrindlikumaid liikmesriike küberjulgeoleku valdkonnas ja Eestis on Riigi Infosüsteemi Ameti (edaspidi: RIA) sõnul infosüsteemid kõrge arengutasemega [13] . Lisaks on Eesti küberjulgeoleku strateegial põhirõhk KII kaitsmisel, olles heaks juhtumiuuringuks varasemates küberjulgeoleku alastes uurimustes. Tänu eelnevale on teistel riikidel ja EL liikmesriikidel võimalik Eesti kogemusest õppida. Varasemalt on Eestis magistritööde raames uuritud küberturvalisust ekspertide narratiivides [14] ning julgeolekustamist küberruumi juhtimise võtmes [15] , kuid need on vaid vähesed näited.

[11] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008)
[12] Pernik, P. Tuohy, E. Cyber Space in Estonia: Greater Security, Greater Challenges (2013) p. 1
[13] Riigi Infosüsteemi Amet (2013) lk. 1-2
[14] Kirch, K. Küberturvalisuse konstrueerimine ekspertide narratiivides. TÜ rahvusvaheliste ja sotsiaaluuringute instituut, 2013, 82 lk (magistritöö).
[15] Raud, H. Securitization and Governance of Cyberspace – Case study on cyber security policy and public administration capacity in Estonia. Tallinn University of Technology faculty of social sciences, 2012, 54 p. (master thesis)

Töös keskendutakse KII-le, sest tehnoloogiliselt arenenumad liikmesriigid[16] on töötanud välja tegevuskavad ja strateegiad küberjulgeoleku tagamiseks, rõhutades KII kaitsevajadust. Paljudes EL liikmesriikides ei ole riiklikku küberjulgeoleku strateegiat ega programme KII kaitseks küberünnakute eest. EL liikmesriikidest kuueteistkümnel (nt Slovakkia, Prantsusmaa, Saksamaa)[17] on välja töötatud riiklik küberjulgeoleku strateegia, kellest esimesena jõudis selleni Eesti 2008. aastal[18]. KII kaitse on oluline, sest tagades piisava kaitse, on tagatud majanduslik areng, ühiskonna elutähtsate funktsioonide toimimine ja riiklik julgeolek[19].

Kopenhaageni koolkonna sõnul on küberjulgeolek uus julgeoleku liik, mis pole konkreetset definitsiooni veel leidnud.[20] Kopenhaageni koolkonna peamiste autorite väitel on küberjulgeoleku referentobjektiks eksistentsiaalselt ohustatud objekt, kellel on õigus seaduslikule abile.[21] Käesoleva töö mõistes on referentobjektiks KII ning olenevalt reguleerimise tasandist riik või EL on julgeolekustaja, kes julgeolekustab küberohud referentobjekti ehk KII nimel. Töös uuritaksegi, kuidas riigile elutähtsates valdkondades regulatsiooni küberrünnaku korral rakendatakse ja kuivõrd KII ettevõtted suudavad end ise kaitsta või vajavad nad riigipoolset abi.

Eespool välja toodud töö eesmärgist lähtuvalt püstitati järgmised uurimisküsimused:

1) Mis on küberjulgeolek ja kuidas küberrünnakuid liigitatakse?
2) Mis on KII ja millised on küberohud sellele?
3) Millised on Eesti KII ettevõtete ja riigi strateegiad küberrünnakute eest kaitsmisel ning kuidas toimib koostöö riigiga?
4) Milliseid ettepanekuid annab käesoleva töö autor koostöö parandamiseks vähendamaks riigi haavatavust küberjulgeoleku valdkonnas?

[16] Euroopa Majandus- ja Sotsiaalkomitee arvamus (2013) punkt 3.4. Euroopa Majandus- ja Sotsiaalkomitee kümme kõrgelt arenenud võrgu- ja infoturbega liikmesriiki on moodustanud Euroopa valitsuste CERT rühma (EGC). Kümme kõrgemalt arenenud liikmesriiki leiab allolevalt aadressilt: [http://www.egc-group.org/contact.html]
[17] ENISA. National Cyber Security Strategies in the World. (2013)
[18] Raud, H.Küberjulgeolekust.[http://www.riso.ee/et/content/k%C3%BCberjulgeolekust#.VJ63-V4hQ] 27.12.2014
[19] Udeanu, G. (2012) p. 89
[20] Hansen, L., Nissenbaum, H. (2009) p. 2
[21] Buzan, B., Jaap, de W., Woever, O. (1998) p. 36

Töö sisuline pool koosneb kahest peatükist. Esimene peatükk koosneb neljast alapeatükist. Esimene alapeatükk keskendub rahvusvaheliste suhete allteooriatele - klassikalisele julgeoleku kompleksi teooriale ning Kopenhaageni koolkonna käsitlusele julgeolekust. Teises alapeatükis keskendutakse küberjulgeoleku kujunemisele ning tuuakse välja küberrünnakute liigitus ja nendega toime tulemise viisid. Kolmandas alapeatükis tuuakse välja küberjulgeoleku strateegiad ning avaliku ja erasektori koostöö toimimise mudelid. Viimases alapeatükis keskendutakse konkreetsemalt antud töö mõistes ühele olulisemale ehk KII definitsioonide erinevatele käsitlustele ja KII kaitse tagamisele küberjulgeolekus. Teine peatükk keskendub empiirikale, koosnedes kolmest alapeatükist. Esimene alapeatükk seisneb autoripoolses EL ja Eesti küberjulgeoleku strateegiate analüüsis, tuuakse välja peamised erinevused ja rõhuasetused KII seisukohast. Teises alapeatükis analüüsitakse KII ekspertidega läbi viidud poolstruktureeritud ekspertintervjuusid. Kolmandas alapeatükis esitatakse lisaks intervjuudest ning strateegiate analüüsist tehtud järeldustele, ettepanekud KII ettevõtete paremaks kaitseks ning sujuvamaks koostööks riigiga.

Käesoleva töö empiirilises osas kasutatakse kvalitatiivsetest uurimismeetoditest dokumentide analüüsi ning poolstruktureeritud ekspertintervjuusid. Dokumentide analüüsil võrreldakse EL ja Eesti küberjulgeoleku strateegiaid KII seisukohast lähtuvalt. Poolstruktureeritud ekspertintervjuud võimaldavad ettevõtete sisemisi probleemkohti tuvastada ning leida vastuseid küsimustele, mis muude uurimismeetoditega pole kättesaadavad ning vastuseid analüüsides, saab avastada valdkonna uusi ning seni võib-olla kättesaamatuks jäänud nurkasid [22]. Hädaolukorra seaduse [23] alusel on Eestis nelikümmend kaks elutähtsat teenust, millest kõikide KII ettevõtete teenustest peab autor energeetika ja telekommunikatsiooni teenuseid kõige tähtsamateks. Nimetatud teenused on vajalikud kõikide teiste elutähtsate teenuste toimimiseks. Empiirilise osa analüüsi käigus tekkinud tulemusi ning ettepanekuid võiks autori ettepanekul rakendada nii KII ettevõtetes kui ka avalikus sektoris küberjulgeoleku valdkonna reguleerimisel ning politiseerimisel.

[22] Balzacq, T. Securitization Theory. (2011) p.46
[23] Hädaolukorra seadus §34

1. TEOREETILISED LÄHENEMISED KRIITILISE INFRASTRUKTUURI KAITSELE KUI OSALE KÜBERJULGEOLEKU TAGAMISEL

1.1 Julgeolek Kopenhaageni koolkonnas

Globaalselt on kõik riigid omavahel julgeoleku-alaselt seotud ja riik on peamine üksus, kes suhtleb sama tasandi teiste sektorite või allüksustega. Niimoodi väidetakse klassikalise julgeoleku kompleksi teooria kohaselt (*classical security complex theory*), mis arenes välja 1991. aastaks. Teooria põhiautoriks on olnud Barry Buzan, kes on ühtlasi üheks Kopenhaageni koolkonna põhiautoriks. Klassikalise julgeoleku kompleksi teooria loogika seisneb selles, et rahvusvaheline julgeolek on suhteline. Rahvusvaheline julgeolek lähtub eelkõige regioonist ja regionaalsest tasandist ning antud teooria analüüsib, kuidas inimesed ja ühiskond on üksteisega turvaohtudest lähtuvalt seotud.[24]

Klassikalise julgeoleku kompleksi teooriast lähtuvalt, algab rahvusvaheline julgeolek regionaalsest tasandist ning riik peab olema peamine üksus, kes juhib suhtlust erasektoriga. Kui regioonis on julgeolek ja turvalisus tagatud, saab alles siis, hakata keskenduma järgmistele tasanditele ehk vaadata riigipiiridest väljapoole, seda ka küberjulgeolekus. Klassikalist julgeoleku kompleksi teooriat avades on võimalik teooria jagada kaheks - olenevalt sellest, kes on referentobjektid ja kelle vahel julgeolekualaseid debatte peetakse ning otsuseid vastu võetakse:

1) Homogeensed (*homogeneous complexes*) – põhineb lähenemisel, kus julgeolek keskendub spetsiifilistele sektoritele ja sarnaste üksuste omavahelisele suhtlusele;
2) Heterogeensed (*heterogeneous complexes*) – loobutud on ideest, kus julgeolek on kindlate sektorite vaheline aruteluteema. Põhineb olemusel, kus siseriikliku

[24] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 10-11

julgeoleku loogika lähtub erinevate sektorite vaheliste osalejate koostööst. (nt riik ja erasektor, riik ja rahvas).[25]

Kuna käesolevas töös analüüsitakse avaliku ja erasektori vahelist koostööd, siis lähtutakse edaspidi klassikalise julgeoleku kompleksi teooriat arvesse võttes julgeoleku heterogeensest olemusest. Ühesõnaga lähtutakse loogikast, kus regionaalsel tasandil julgeoleku-alaseid debatte peetakse erinevate sektorite vahel. Orienteerumaks julgeoleku erinevate analüüsitasandite ja sektorite vahel, tuuakse järgnevas loetelus välja rahvusvaheliste suhete uurimustes kasutuses olevate analüüsitasandite jaotus. Rahvusvaheliste suhete uurimustes kasutatakse peamiselt allolevat viit analüüsitasandit, millest lähtuvalt viiakse läbi uurimusi[26]. Kopenhaageni koolkonna teoreetiku Ole Wæver arvates suhtlevad erinevad ühiskonnad rahvusvahelises taustsüsteemis üksustena.[27] Kuna antud töös vaadeldakse heterogeenset ehk riigi ja erasektori vahelist suhtlust, siis analüüsitasanditest kasutatakse kolmandat ehk üksuse tasandi alljaotust:

1) rahvusvahelised süsteemid (konglomeraadid, kus enam suuremaid tasandeid pole, nt ÜRO);
2) rahvusvahelised allsüsteemid (nt EL);
3) üksused (osalejad erinevatest alagruppidest nt riigid, rahvad, rahvusvahelised ettevõtted);
4) allüksused (indiviidide organiseeritud grupid, nt lobistid, bürokraadid);
5) indiviidid.[28]

Mõistet „julgeolek“ on peamiselt uuritud ning defineeritud läbi rahvusvaheliste suhete teooriate. Julgeolek sisaldab rahvusvaheliste suhete teooriate kohaselt endas kõike, mis on seotud ellujäämisega ning julgeolekust saab rääkida siis, kui referentobjekti on tabanud eksistentsiaalne oht. Referentobjekti all peetakse tavaliselt silmas, kuid mitte ilmtingimata, riiki, valitsust, territooriumi, ühiskonda. Näiteks EL puhul võib pidada ohtudeks sellised eksistentsiaalseid sündmusi, mis katkestaksid EL toimiva integratsiooniprotsessi. Samas tuleks rõhutada, et erinevates sektorites nagu militaar-, poliitilises-, majanduslikus-, sotsiaalses-, keskkonnasektoris on referentobjektid

[25] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 16
[26] *Ibid.:* p. 5-6
[27] Collins, A. (2013) p. 179
[28] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 5-6

spetsiifilisemad ning valdkonnapõhisemad.[29] Julgeolekustamist on defineeritud ning tõlgendatud erinevate autorite poolt, kuid näiteks Johan Eriksson mõtestab julgeolekustamist kui käiku, mis klassifitseerib teatud teemat/probleemi eksistentsiaalse ohuna, nõudes omakorda erakordseid meetmeid.[30]

Julgeolekustamise analüüsimisel tuleb lähtuda kahest põhilisest ning omavahel seotud küsimusest: esmalt teha selgeks, mis on oht ning teisalt teha kindlaks, kuidas ohuga toime tulla.[31] Ehk kuidas selgitada välja, kas julgeoleku mõistes on tegemist julgeoleku-alase küsimusega ning kas ja kuidas tuleks ohtudega toime tulla. Julgeolekustamise puhul saab tegemist olla julgeoleku-alase küsimusega juhul kui tegemist on ühiskonda puudutava ja avalikku tähelepanu nõudva valdkonnaga või puudutab valdkond kriitiliselt poliitilist süsteemi[32].

Kopenhaageni koolkonda peetakse esimeseks, kes on küberjulgeoleku valdkonda laiemalt uurinud ning põhilisteks autoriteks on Barry Buzan, Ole Wæver, Lene Hansen, Helen Nissenbaum, kes kõik on avaldanud raamatuid ja artikleid regionaalse julgeoleku kompleksiteooria, Euroopa julgeoleku, regioonide ning globaalse julgeoleku vaheliste suhete teemadel. Peamiselt on keskendutud siiski ühiskondlikule turvalisuse ja julgeolekustamise uurimisteemadele.[33] Peale Kopenhaageni koolkonna on kriitilisi julgeolekuanalüüse läbi viinud veel kaks koolkonda: Frankfurdi ning Pariisi koolkond.

Frankfurdi koolkonna teoreetikud keskendusid traditsioonilise julgeolekumõiste riigi- ja sõjalise sektori kesksete eelduste lammutamisele, kus üheks eesmärgiks oli avada julgeoleku-uuringud laiemale ühiskonnale tervikuna . Tähelepanu keskpunkti tõsteti riigi asemel inimestega seotud õiguste piiramised. Pariisi koolkonna sotsioloogiline julgeolekukäsitlus keskendub seevastu julgeolekuväljal tegutsevate professionaalide sotsiaalse tegevuse ja tehnoloogia analüüsile. Teiste sõnadega mikropraktikatega seotud osaliste iseotsustusõiguse, tegevusrepertuaari ja tehnoloogiate mõju analüüsile, käsitledes julgeoleku haldamist kui erilist laadi valitsemistegevust.[34] Edaspidi

[29] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 21-22
[30] Eriksson, J. (1999) p. 315
[31] Balzacq, T. Securitization Theory (2011) p. 32
[32] *Ibid.:* p. 32
[33] Buzan, H. Hansen, L. (2010) p. 212
[34] Mälksoo, M. Akadeemilised julgeoleku-uuringud sõja ja rahu vahel. lk. 1773-1776

kasutatakse käesolevas töös Kopenhaageni koolkonda, sest koolkonda peetakse esimeseks, kes küberjulgeoleku-alaseid teemasid täpsemalt käsitlustes uurinud.

Kopenhaageni koolkonna autorid leivad, et julgeolek on kõneakt, mis julgeolekustab üht või mitut referentobjekti. Ajalooliselt on referentobjektiks rahvus või riik, kellel esineb oht rahvuse ellujäämisel või riigi püsima jäämisel ning ohu takistamiseks tuleks referentobjekte seadustega kaitsta.[35] Antud töö raames on referentobjektiks KII ning riik julgeolekustajaks, kes julgeolekustab küberohud referentobjekti ehk KII nimel. Nõustudes eelnevaga, siis KII püsima jäämine küberrünnaku korral on elutähtis, vajades riigipoolset kaitset. Vältimaks elutähtsate KII ettevõtete hävimist on avaliku sektori poolsed regulatsioonid vajalikud.

Kopenhaageni koolkonna teoreetikute arvates tuleb julgeolekut (sh küberjulgeolekut) analüüsides lähtuda neljast põhiküsimusest. Esimese küsimusena analüüsitakse, kas riiki tuleb eelistada referentobjektina või mitte. Julgeolek lähtub põhimõttest, et pidevalt on tarvis riiki, indiviide, etnilisi gruppe, keskkonda või kasvõi planeeti turvalisemaks muuta. Tagades turvalisuse riigis, on ka teiste ühiskonnaliikmete julgeolek tagatud.[36] Autor nõustub Kopenhaageni koolkonna teoreetikute väitega, et riigi tasandil peab olema turvalisus ja julgeolek tagatud, kuid nagu autor eespool mainis, on antud töös erasektor KII ettevõtete näol referentobjektiks ning riik julgeolekustajaks, kes tagab turvalisuse elutähtsate valdkondade ettevõtetes ehk KII-des.

Teine küsimus keskendub sisemistele ja välistele ohtudele. Kuna julgeolek on tihedalt seotud riigi suveräänsusega, siis tuleks ohud määratleda territoriaalsete piiridega.[37] Teiste sõnadega, tuleb defineerida, mis on riigile sisemised ning välised ohud. Julgeoleku laiemas mõistes on riigil ohte võimalik territoriaalselt määratleda, kuid küberrünnakuid on territoriaalselt üheselt piiritleda keerulisem. Küberrünnakud võivad tabada igalt poolt ja igast riigist, piiritledes neid siseriiklikeks või väljastpoolt riiki tabavateks rünnakuteks. Piirideta suhtlus toimub EL liikmesriikide vahel igapäevaselt ning EL teenuste, inimeste ning kapitali vaba liikumine peab olema küberintsidentide

[35] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 2
[36] Buzan, B., Hansen, L. (2010) p. 10-11
[37] *Ibid.:* p. 10-11

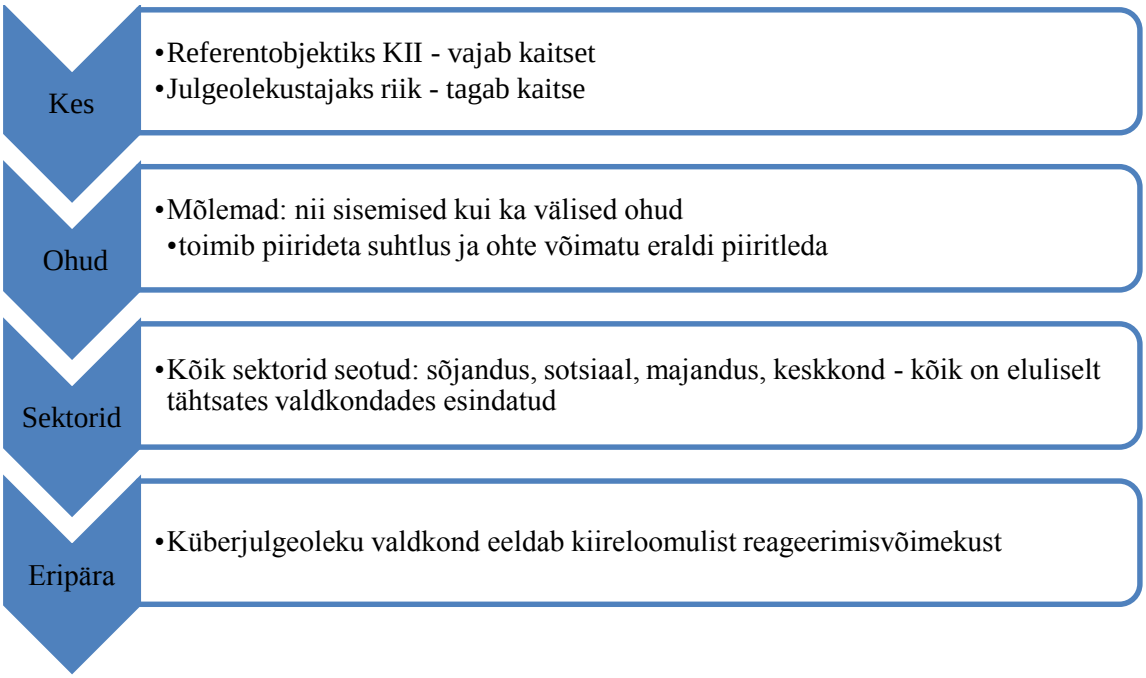
eest turvatud[38]. Kaitseuuringute keskuse RIA 2014. aastaraamatu kokkuvõttest selgub, et kasvavaks trendiks on küberruumi ühteseotus, mis tähendab, et välismaised probleemid võivad kiiresti muutuda riigisisesteks.[39]

Kolmas küsimus seisneb julgeoleku mõiste laiendamisel sõjandus-, sotsiaal-, majandus-, keskkonnasektorisse tuues sisse jõu kasutamise võimaluse.[40] Kolmanda küsimuse puhul autor nõustub, et küberjulgeolekut tuleks rakendada kõikides ülalnimetatud sektorites, sest kõik sektorid on ja jäävad tehnoloogiliselt küberjulgeoleku valdkonnaga seotuks. Samas, kas tasub küberintsidenti tagajärgi lahendada jõumeetoditega, selles küsimuses jääb autor erapooletuks. Neljas küsimus keskendub julgeoleku tihedale seotusele ohtude, rünnakute ja kiireloomulise tegutsemise põhimõtetega[41]. Autor leiab, et küberjulgeolek on tihedalt seotud ohtude, rünnakute ning kiire reageerimise vajadusega. Kui ei jõuta reageerida ja eeskätt ennetada küberrünnakuid, siis tuleks võimalusel kiiresti reageerida ja tagada võimalikult minimaalsete kahjudega tagajärjed. Eelpool kirjeldatu on kokku võetud alloleval joonisel 1, kus analüüsi ning küsimuste objektiks on võetud küberjulgeolek.

Julgeoleku-alaste otsuste vastu võtmiseks ning ohtudega tegelemiseks on teatud tasemel julgeolekustamist (*securitization*[42]) tarvis politiseerida. Kopenhaageni koolkonna sõnul peetakse julgeolekustamiseks tegevust, mis paneb poliitika oma tavaraamidest väljapoole liikuma, defineerides vastava teema (nt küberjulgeolek) poliitika tavavormiks või tavapoliitikat ületavaks. Seega saab julgeolekustamist vaadata kui ekstreemset politiseerimise versiooni.[43] Teoreetiliselt on iga avalikku teemat võimalik asetada skaalale, kus ühelpool on politiseeritud ja teisel mitte-politiseeritud teemad. Lühidalt öeldes reguleeritud või mittereguleeritud. Erinevus seisneb selles, et esimesel juhul riik sekkub ja reguleerib probleemi tekitanud valdkonda, teisel juhul debatti ei peeta ja otsuseid riigi tasandil vastu ei võeta. Küberjulgeolekus on tegemist nii

[38] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD) p.3
[39] Maldre, P. Eesti küberturbe olukord 2014. 02.04.2015. [http://www.icds.ee/et/blogi/artikkel/eesti-kuberturbe-olukord-2014/] 08.05.2015
[40] Buzan, B., Hansen, L. (2010) p. 10-11
[41] *Ibid.:* p. 12-13
[42] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 23
[43] Kallis, J. (2011) lk 15

ekstreemselt politiseeritud kui ka julgeolekustatud valdkonnaga.[44] Näiteks Eesti puhul on riik välja töötanud strateegia küberrünnakutega ja üldisemalt küberjulgeoleku reguleerimiseks ning Eesti riik on võtnud rolli vajadusel abi pakkuda.[45]

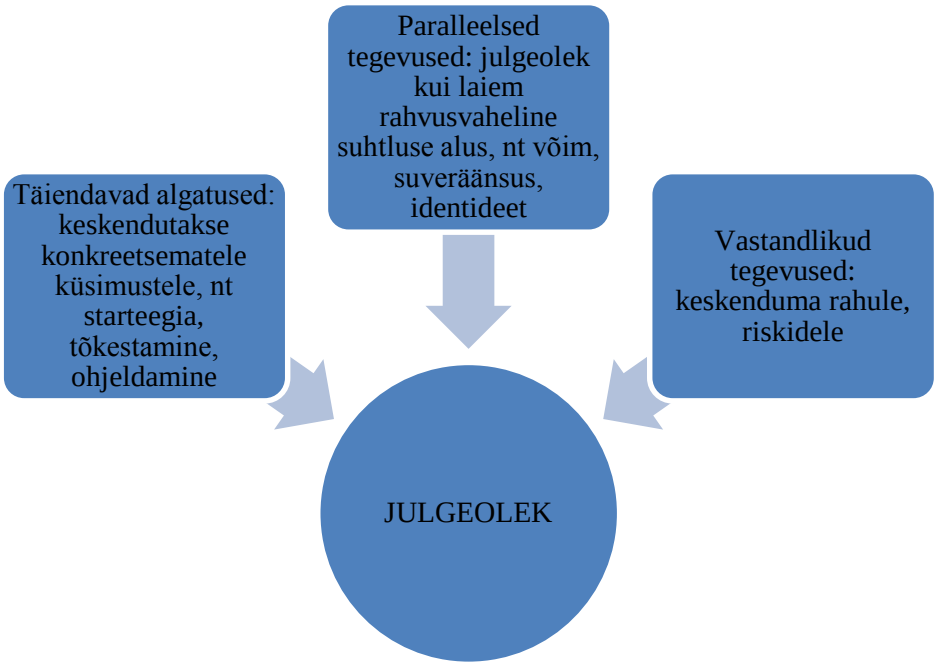


Joonis 1. Küberjulgeoleku kui julgeoleku liigi analüüsiskeem Kopenhaageni koolkonna põhiküsimustest lähtuvalt. Allikas: autori koostatud.

Sellest lähtuvalt tuleb rõhutada, et julgeolekustamine ei keskendu vaid seaduste loomisele ja eksistentsiaalsete ohtude elimineerimisele. Teatud juhtudel, kui esineb eluliselt tähtsaid rünnakuid, seadustatakse olukorrast tingituna eeskirjad, mis omakorda võivad tekitada probleeme ohu määratlemisel ja hindamisel. Kas oht on piisavalt tähtis või mitte seadusandluse elluviimiseks?[46] Vastus peitub ohtude adresseerimisel. Kui Pentagoni peaks ründama mõni kogenud häkker, siis ilmselt defineeritakse küberünnakut tõsise ohuna rahvuslikule julgeolekule, mitte vastupidi. Julgeolekustamine saab olla tõhus, kui on püstitatud võimalikult konkreetsed ohtude määratlused, tegevusjuhiseid hädaolukorraks ning mõju teistele seotud üksustele.[47] Allolevalt jooniselt 2 selgub, et julgeolek keskse mõistena on sõltuv paljudest tegevustest. Täiendavalt on välja toodud strateegia kui algatus, mis peaks keskenduma

[44] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 23-24
[45] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008)
[46] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 25-26
[47] Buzan, B., Wæver, O., Wilde, de J. (1998) p. 25-26

konkreetsematele küsimustele. Töös hinnataksegi strateegia mõju küberjulgeolekule ning täpsemalt, kuidas strateegia aitaks küberrünnakute korral olulisi üksuseid paremini kaitsta.



Joonis 2. Julgeolekuga seotud tegevused. Allikas: Buzan, H. Hansen, L. (2010) p. 14

Alapeatüki kokkuvõtteks võib öelda, et julgeolekut on defineeritud nii rahvusvaheliste suhete allteooriate raames kui ka Kopenhaageni koolkonna teoreetikute käsitlustes. Julgeolek on valdkond, mille defineerimisel tuleb arvestada, kes on julgeolekustamises osapoolteks ning kui suures ulatuses valdkonda on tarvis politiseerida. Kopenhaageni koolkonnast lähtuvalt esitati neli põhiküsimust, mille alusel saab julgeolekut analüüsida. Olulisena tasub välja tuua, et KII ettevõtteid tuleb käsitleda referentobjektidena ning riik julgeolekustajana peab vastutama selle eest, et vajadusel on KII kaitse tagatud.

1.2 Küberjulgeoleku kujunemine, küberrünnakute liigitus ning nendega toime tulemise viis

Tehnoloogia areneb igapäevaselt ning tahes-tahtmata arenevad erinevad ohud küberruumis. Küberruumiks peetakse taristust ja teenustest koosnevat keskkonda, kus toimuvad tavamaailmaga sarnased protsessid. Tavamaailma protsessidest eristab

küberruumiprotsesse infotehnoloogia.[48] Siinkohal leiab autor, et tänapäeval on keeruline eristada tavamaailma ja küberruumi protsesse, sest suuremal või vähemal määral on tegemist pigem kombineeritud protsessidega, kus igasse protsessi on kaasatud tehnoloogia. Teiste sõnadega, küberruum ei ole seotud ainult internetiga, vaid küberruumi mõiste sisaldab endas lisaks võrguühendusele füüsilisi objekte nagu arvuti, serverid ning võrgukaablid[49].

1990-ndatel, vastusena tehnoloogilisele innovatsioonile ja muutuvale geopoliitilise olukorrale, leidis täpsema käsitluse küberjulgeoleku kontseptsiooni kujunemine. Esmakordselt võeti küberjulgeoleku mõiste kasutusele arvutiteadlastelt, defineerides ridu ebakindlusi, mis olid seotud võrku ühendatud arvutitega.[50] Lisaks tunnistas USA endise presidendi Clintoni administratsioon 1990-ndatel aastatel, et küberjulgeolek on oluline valdkond ning sellele tuleb hakata rohkem tähelepanu pöörama. Peale Clintoni väljaütlemist analüüsiti esmakordselt, kuidas tehnoloogia võib referentobjekte kahjustada.[51]

1970-80-ndatel olid referentobjektideks erasektori ettevõtted, kes olid äsja üle läinud digitaalsetele lahendustele ning avalikust sektorist valitsusasutused, kel tuli kaitsta salajast infot laiema avalikkuse eest. 1990.-ndatest, kui toimus suurem tehnoloogiline areng, laienes referentobjekti mõiste kõikidele KII ettevõtetele, sest mõisteti, et ohustatud on kõik KII ettevõtted, kui nad tehnoloogiliselt küberruumis eksisteerivad.[52] Järgmised suuremad arengud küberjulgeolekus toimusid pärast 11. septembri terrorirünnakut, kus USA eestjuhtimisel hakati täiendavat tähelepanu pöörama kõigele, mis oli seotud arvutite, infotehnoloogia ning julgeolekuga. Vähetähtsamad polnud digitaalse infrastruktuuri kaitse, elektrooniline valve ja internet kui võrgustik, mis on platvormiks riikide omavahelisele suhtlusele.[53] Kuigi meedias ja poliitikas pööratakse palju tähelepanu küberjulgeoleku puudujääkidele, siis puudub julgeolekut uurivates ringkondades ühtne küberjulgeoleku alaste mõistete käsitlus.[54]

[48] Riigi Infosüsteemi Amet. (2013) lk 1
[49] Collins, A. (2013) p. 363-364
[50] Hansen, L, Nissenbaum, H. (2009) p. 1
[51] Buzan, H. Hansen, L. (2010) p. 248
[52] Collins, A. (2013) p. 365
[53] Buzan, B., Hansen, L. (2010) p. 1-2
[54] Hansen, L. Nissenbaum, H. (2009) p. 2

Tänapäeva küberruumi hetkeseisu ilmestavad järgmised 2013. aasta alguses Euroopa Komisjonilt esitatud faktid: hinnanguliselt tuvastatakse igapäevaselt üle 150 000 arvutiviiruse; Maailma Majandusfoorumi arvates tabab järgneva aastakümne jooksul 10% tõenäosusega laiaulatuslikum KII küberrünnak, mille kahjud jäävad 250 mld dollari ulatusse; 2012. aasta eurobaromeeter näitab, et vaid 26% EL ettevõtetest on süsteemidesse integreerinud IKT julgeolekustrateegia.[55] Eelnimetatud statistika on vaid mõned näited sellest, kuivõrd tuleb küberjulgeolekule veelgi enam tähelepanu pöörata.

Üha enam pidevalt internetiga seotud maailmas võivad ohud riigi- ja küberjulgeolekule tulla ootamatutest allikatest. Küberjulgeoleku ekspluateerimine ja pahatahtlik tegevus on muutunud üha keerukamaks, tõsisemaks ja kindlatele sihtmärkidele suunatumaks.[56] Sihtmärkideks võivad olla KII ettevõtted, sest meenutades Eesti 2007. aasta sündmusi,[57] siis lisaks muudele e-teenustele olid enamik Eesti pankade e-teenused häiritud ning internetipangatehinguid polnud võimalik teatud aja jooksul häirete tõttu sooritada. Küberrünnaku objektideks võivad olla erinevate sektorite infosüsteemid, näiteks avalikus sektoris riigi infosüsteemid, täpsemalt kaitse-, tsiviil- ja luureasutuste infosüsteemid[58].

2007. aasta sündmusi Eestis on rahvusvahelistes debattides peetud esimeseks kübersõja momendiks, sest seoses Teise maailmasõja mälestusmärgi teisaldamisega rünnati suuremahuliselt Eesti veebilehtesid. [59] Tihti puudub nägemus ning teadmine, et maksekaardi häiretel võib tegelikuks põhjuseks olla väiksem või laiaulatuslikum küberrünnak. Seega pidevalt arenev tehnoloogia võimaldab terroristidel ja teistel pahatahtlikel osalejatel rünnata digitaalselt infrastruktuure, katkestades elutähtsate valdkondade teenuseid, hävitades KII töö või häirides globaalsel tasandil sidevõrkude tööd. Tänapäeval on paljud suutelised kergesti kättesaadavate vahenditega suuri kahjusid tekitada.[60]

[55] European Commission. EU Cybersecurity plan to protect open internet and online freedom and opportunity. (2013)
[56] Choo, R. (2011) p. 719-720
[57] Ilves, T. H. Järgmine väljakutse: küberkaitse. (2012)
[58] Leis, P. (2013) Cybersecurity Risk Management. p.15
[59]Hansen, L. Nissenbaum, H. (2009) p. 2
[60] Buzan, H. Hansen, L. (2010) p. 269-270

Seega on küberjulgeoleku valdkonnas küberrünnakute näol tegemist valdkonnaga, mida pole lihtne hallata ning KII ettevõtteid üheselt kaitsta, sest tehnoloogia on pidevas arengus. Kui tehnoloogia muutub igapäevaselt, siis koos positiivsete arengutega nagu e-kool, e-riik, digitaalallkirja andmise võimalus, toimuvad paralleelselt ka negatiivsed edasiminekud - näiteks küberrünnakud kriitilisele taristule. Orienteerumaks küberrünnakute ja -ohtude maastikul tuuakse järgnevalt välja mõned küberrünnakute klassifikatsioonid, sest toimiva küberjulgeoleku strateegia loomiseks on tarvis teada ohte ning küberrünnakute võimalikult täpset liigitust[61]. Lisaks tuleb erasektoril ja avalikul sektoril seada küberohtudest ja -rünnakutest tulenev oht esikohale,[62] sest kui ollakse kursis ohtudega ja võimalike küberrünnakute sihtmärkidega, siis osatakse end strateegiliselt paremini kaitsta.

Küberohte on võimalik liigitada mitmel viisil, vastavalt rünnaku iseloomule ja küberrünnakute eesmärkidele. Enamik küberohte tekivad olukordades, kus interneti turvalisus on nõrgalt tagatud ning serveritele/võrkudele pääsevad ligi isikud, kes suudavad kiiresti oma identiteeti muuta[63]. Esmased tõsiseltvõetavad ja laialdasemalt kasutusele võetud küberrünnakute definitsioonid pärinevad USA sõjaväe uuringute tulemustest,[64] kuid kuna USA sõjaväes keskendutakse küberrünnakutele kübersõja mõistes, siis käesolevas töös seda klassifikatsiooni välja ei tooda, sest kübersõjad on eraldi uurimisvaldkond, mida antud töös ei käsitleta. Choo arvates jagunevad küberrünnakud vastavalt rünnaku eesmärkidele ja sihtgruppidele järgmiselt:

1) Pahavara (*malicious software/malware*):
   a) Üldiselt ühiskonnale – (nt rämpsposti levitamine)
   b) Kohandatud teabevargusele orienteerunud pahavara, mis suunatud konkreetsele institutsioonile (nt *keylogger* tüüpi pahavara, kus pahavara allalaadimiseks saadetakse emailile manuseid, linke, mille avades laaditakse asutuse serverisse, sisevõrku klahvivajutusi jälgiv pahavara, laadimaks alla paroole jms)[65]
2) Kaubanduslikud *off-the-shelf* tooted:

[61] Choo, R. (2011) p 720
[62] Regioonide Komitee arvamus. C 280/19 (2013) lk 2
[63] Klimburg, A. Tiirmaa-Klaar, H. (2011) p. 12
[64] *Ibid.:* p. 14
[65] Choo, R. (2011) p. 721

a) tooted, mis originaalis sisaldavad endas turvaauke, üheks võimalikuks küberohuks kriitilise infrastruktuuri infosüsteemidele[66]

3) *Phishing* rünnakud:
   a) süntaktilised (riist- ja tarkvara turvaaukudele keskenduv rünnak)
   b) semantilised (sotsiaalsele haavatavusele keskenduv saamaks isikuandmeid)
   c) kahe eelmise kombinatsioon (tehniliste vahendite abil läbi sotsiaalsete kanalite siseteabe hankimine.[67]

Euroopa Komisjoni eestvedamisel on küberohud jagatud ründamise eesmärkidest lähtuvalt järgmistesse kategooriatesse:

1) **kasusaamise** eesmärgil - „püsivad edasiarenenud ohud"[68], majandusliku ja poliitilise spionaaži eesmärkidel (nt GhostNet), identiteedivargus, hiljutised rünnakud kasvuhoonegaaside heitkoguste kauplemise süsteemile või valitsusasutuste IT-süsteemidele;
2) **häirimise** eesmärgil - DDos, DoS või robotvõrkudest tekitatud rämpspost, Stuxnet ja sidekanalite sulgemine;
3) **hävitamise** eesmärgil – antud stsenaarium ei ole veel realiseerunud, kuid võttes arvesse IKT üha laiaulatuslikumat kasutust elutähtsate infrastruktuuride raames (nt targad energiavõrgud ja veesüsteemid), ei saa rünnaku tõenäosust tulevikus välistada.[69]

Kindlasti on mitmeid erinevaid liigitusi ning tüpoloogiaid küberrünnakute ja –ohtude klassifitseerimisel, kuid antud töös toodi välja ülalnimetatud. KII puudutavad ülemaailmsed küberrünnakud on välja toodud allolevas tabelis 1. Selleks, et saada ülevaadet, millised on küberrünnaku tagajärjed, on järgnevas tabelis 2 välja toodud küberrünnakute ja süsteemide haavatuse seosetabel. Tabelist 1 selgub, et välja toodud üksikud näited KII-le suunatud küberrünnakutest maailmas on tehtud rünnaku iseloomust lähtuvalt kasusaamise või häirimise eesmärgil. Töös lähtutaksegi edaspidi Euroopa Komisjoni poolt välja toodud eesmärkidest lähtuvast liigitusest. Kuna töö keskendub KII ettevõtetele, siis võib eeldada, et siiani on ühiskonnal reaalselt

[66] Choo, R. (2011) p. 723
[67] *Ibid.:* p. 724
[68] Antud mõiste tähendab pidevaid koordineeritud rünnakud valitsusasutuste ja avaliku sektori vastu. Nimetatud ohud on muutumas päevakajaliseks ka erasektoris
[69] Euroopa Komisjoni teatis KOM/2011/163 lk 4

kokkupuuteid olnud telekommunikatsiooni ja panganduse valdkonna rünnakutega (telefoniside või internetipangamaksed, kaardimaksed häiritud).

Tabel 1. Näiteid KII´le suunatud küberrünnakutest maailmas

Rünnaku nimi	Aasta	Kirjeldus	Teostajad
GhostNet	2009	Küberluure operatsioon, koguti 30 riigi kohta kõrge väärtusega poliitilist, majanduslikku informatsiooni	Hiinast
Aurora	2009	Rünnakud Google ja teistele ettevõtetele eesmärgiga pääseda ligi ning muuta kõrge väärtusega informatsiooni, mis pärit julgeolekut ja kaitset pakutavatest ettevõtetest	Hiinast
Stuxnet	2010	Arvuti pahavara eesmärgiga aeglustada Iraani tuumaprogrammi	USA valitsus (+Iisrael)
CO2 emissiooni paberite vargus	2011	6,9-9,3 mln dollari väärtuses emissiooni paberite vargus	Organiseeritud küberkuritegu

Allikas: Collins, A. Contemporary security studies. 2013. p 369

Tabel 2. Küberrünnakute seos süsteemi haavatavusega

Tekitaja	Objekt	Tulemus
Viirus	Viirusetõrjetarkvara puudumine	Viirusinfektsioon
Häkker	Serveril töötavad suuremahulised teenused	Volitamata juurdepääs konfidentsiaalsele infole
Kasutajad	Valesti konfigureeritud parameetrid operatsioonisüsteemis	Süsteemihäired
Töötajad	1)Kutsestandardite, koolituste puudumine. 2) Auditi puudumine	1) Asutusesisese kriitilise info jagamine 2) Muudetud andmete sisendid/väljundid andmetöötlus rakendustes
Töövõtja	Kerge juurdepääs kontrollimehhanismidele	Ärisaladuse vargus
Ründaja	Rangete tulemüüri seadete puudumine	DoS-rünnak

Allikas: Leis, P. Cybersecurity Risk Management (2013) p. 31

Vältimaks halvimat, tuleb tagada erasektori ja avaliku sektori koostöös strateegiate ühildamine ning ühistel eesmärkidel tegutsemise siht. Lisaks tugevale strateegiale ja koostööle, aitab KII ettevõtetel küberjulgeoleku ja –rünnakute alal toime tulla läbimõeldud riskianalüüs ning -juhtimine. Küberjulgeolekus on digitaalse majandusega kokkupuutuvatel ettevõtetel peamiseks mureks riskijuhtimine [70] . Ettevõtete riskijuhtimiseks peetakse strateegilist äridistsipliini, mis toetab organisatsiooni eesmärkide täitmist läbi kõikide ettevõtte riskide kaardistamise. Lisaks kaardistamisele tuleks hinnata kõiki riske tervikuna. [71] Järgnevalt tuuakse välja näide, kuidas KII ettevõtted võiksid küberturvalisuse tagamise protsessi juhtida.

Toetudes riskipõhise küberturvalisuse tagamise protsessile, tuleks KII ettevõtetel riskijuhtimisel lähtuda viiest etapist:

1) esimeses etapis defineerida probleem ning välja selgitada, mille eest ettevõtte süsteeme kaitstakse;
2) teises etapis kaardistada ettevõtte tegevusalast lähtuvalt võimalikud küberrünnakud, ning hinnata süsteemi läbi ründaja pilgu;
3) kolmandas etapis tuleks eelnevas etapis kaardistatud rünnakud järjestada nende kulu, keerulisuse ja toimumise tõenäosuse alusel;
4) neljandas etapis analüüsida alternatiive ehk teha kindlaks, kas rünnakuid on võimalik elimineerida või muuta nad ründaja silmis vähem atraktiivsemaks;
5) viiendas etapis võrrelda kompromisse ehk kogu ettevõtte tegevus ei ole ja ei saa olema ainult küberjulgeolekust lähtuv. Turvalisuse tagamise protsessi koostamisel tuleb hinnata võimalikke kaasnevaid kulutusi ning tehnilist teostatavust.[72]

Võideldes 21. sajandi küberohtude ning -rünnakutega, siis nende allutamiseks on tarvis lähtuda 21. sajandi strateegiatest, taktikatest, koolitustest ja tehnoloogiatest. [73] Küberkeskkonna kaitsmisel on tarvis mõista riske, tunda ära ohud ning olla valmis nende eest end kaitsma või tagajärgedega toime tulema. Häid teadmisi, praktikat,

[70] Leis, P. Cybersecurity Risk Management. (2013) p. 12
[71] Leis, P. Enterprise Risk Management.(2013) p. 6
[72] Leis, P. Cybersecurity Risk Management (2013) p. 3
[73] *Ibid.:* p. 13-14

kogemust on tarvis nii ettevõtete juhtidele kui ka ülejäänutele.[74] Seega võib alapeatüki kokkuvõtteks öelda, et 1990-ndate algusest hakati nii USA valitsuse kui ka arvutiteadlaste eestvedamisel rohkem keskenduma küberjulgeoleku spetsiifikale. Pärast 11.septembri terrorirünnakut toimus suurem areng, mille käigus peale tehnoloogia arengust tulenevatele ohtudele, hakati tähelepanu pöörama riistvarade, tarkvarade ehk üldisemalt infoturbest tingitud ohtudele ning küberjulgeoleku tagamisele. Küberjulgeolekus on olulisel kohal riskide juhtimine, riskianalüüs, koostöö ja kvaliteetsete strateegiate koostamine. Strateegilise tugevuse saavutamiseks, tuleb nii ettevõtetel kui avalikul sektoril hoida end kursis küberjulgeoleku valdkonnas toimuvaga ning uute rünnakute allikatega. Võttes arvesse riske ja ohte, mis on kõige tõenäolisemad, kuid samas hinnata reaalselt olukorda ja võimalusi, et võidelda küberrünnakutega. Senised peamised küberrünnakud on toimunud Euroopa Komisjoni hinnangul häirimise eesmärgil, kus sihtmärkideks võivad olla kõik sektorid sealhulgas KII.

1.3 Küberjulgeoleku strateegiad avaliku ja erasektori koostöös

Antud alapeatükis keskendutakse avaliku ja erasektori koostööle ning kirjeldatakse erinevaid koostööetappe küberjulgeoleku valdkonnas. Tuuakse välja CCD COE välja töötatud juhised, mis peaks aitama koostada EL-st tulenevatele soovitustele vastavat küberjulgeoleku strateegiat. Võrreldes 2010. aastaga suurenes küberrünnakute hulk 2011. aastal 36% võrra nii Euroopas kui ka mujal maailmas[75]. 2013. aastal tuvastati Euroopas 41% võrra rohkem küberrünnakuid.[76] Suurenenud küberrünnakute maht on andnud põhjuse välja töötada strateegiaid ning koostööplaane küberruumi kaitsmiseks. Samas pole välja kujunenud rahvusvahelist õigust ja konkreetsemalt küberrünnakuid käsitlevat õiguslikku raamistiku, mida EL liikmesriigid saaksid ühtselt järgida. Võtmerolli õigusliku raamistiku välja töötamiseks ja küberjulgeoleku tagamiseks on võtnud enda kanda EL.[77]

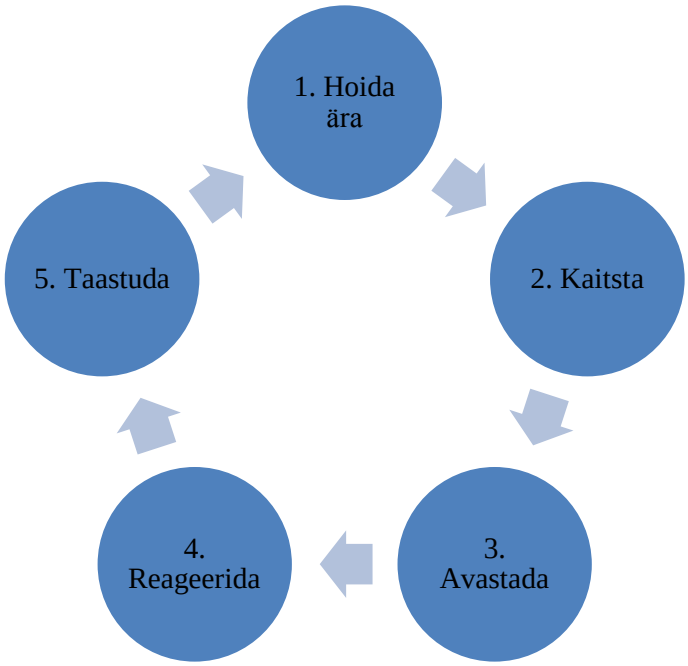
[74] Riigi Infosüsteemi Amet. (2013) lk 1
[75] European Commission. About trust and security. (2013)
[76] PricewaterhouseCoopers. The Global State of Information Security® Survey 2015. Managing cyber risks in an interconnected world. p. 9
[77] Hansen, L. Nissenbaum, H. (2009) p. 4

EL küberjulgeoleku kujunemine sai alguse 1995. aastal, kui kinnitati andmekaitse direktiiv.[78] EL küberjulgeoleku strateegia töötati välja Stockholmi programmi raames[79] koostöös Euroopa Komisjoni ning Euroopa Välisteenistusega, kus strateegia märksõnadeks on avatud, ohutu ja turvaline internet.[80] EL strateegias on kaks läbivat poliitikavaldkonda, millest esiteks keskendutakse meetmetele võitlemaks küberrünnakutega ja teiseks meetmetele, mis aitaks kaitsta KII.[81] EL strateegia rõhutab, et küberjulgeolekus tuleks saavutada üleeuroopaline vastupanuvõime, kaitstes eeskätt KII süsteeme ja soodustades koostöövalmidust avaliku ja erasektori vahel.[82] Euroopa Komisjoni tegi pikalt eeltööd teiste globaalsete küberjulgeoleku poliitikate osas, enne kui alustas EL-sisest küberjulgeoleku strateegiat looma.[83] EL on volitatud vastu võtma meetmeid[84], mis aitaksid kaasa siseturu toimimise tagamisele, seega on küberjulgeolek üheks oluliseks osaks siseturu toimimisel.[85]

Küberjulgeoleku valdkonna reguleerimisel ning regulatsioonide loomisel tuleb tähelepanu pöörata valdkonna keerulisusele ning asjaolule, et riskide määratlemine on mitmetasandiline ning arvestada tuleb rahvusvaheliste, rahvusüleste ning siseriiklike autoriteetide osalusega.[86] Ühesõnaga küberjulgeoleku valdkond oma uudsuses ning pidevalt arenevate riskidega vajab strateegiate, regulatsioonide, direktiivide loomisel kõikide osapoolte tähelepanu ning kaasamist, sest valdkond puudutab kõiki osalejaid igapäevaselt. EL endise välisasjade ja julgeolekupoliitika kõrge esindaja Catherine Ashtoni arvates peaksid liikmesriigid küberjulgeoleku kontekstis keskenduma varases faasis küberünnakute ennetamisele. Kui küberrünnak KII-le on aga toimunud, siis tuleb rünnaku allikad esimesel võimalusel tõkestada ning tagada kiire küberrünnakust

[78] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ
[79] Fahey, E. The EU-s cybercrime and Cybersecurity rule-making: mapping the internal and external dimensions of EU security. European Journal of Risk Regulation. Vol 1/2014. p.4
[80] European Commission. Cyber Security Strategy of the European Union.
[81] Klimburg, A. Tiirmaa-Klaar, H. (2011) p. 36
[82] Final Report by the High Representative (2013) p. 8-9
[83] Fahey, E. The EU-s cybercrime and Cybersecurity rule-making: mapping the internal and external dimensions of EU security. European Journal of Risk Regulation. Vol 1/2014. p. 22
[84] Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid. ELTL artikkel 26 ja artikkel 114
[85] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD), p. 8
[86] Fahey, E. The EU-s cybercrime and Cybersecurity rule-making: mapping the internal and external dimensions of EU security. European Journal of Risk Regulation. Vol 1/2014. p. 4

taastumine.[87] Lähtudes endise kõrge esindaja Ashtoni kõnest on avaliku ja erasektori koostööks (*public-private partnership* - edaspidi: PPP) võimalikud erinevad staadiumid. Alloleval joonisel 3 tuuakse välja olulised sammud küberrünnakute eest kaitsmisel.[88]



Joonis 3. PPP üldised etapid küberrünnakutega toime tulemises. Allikas: ENISA. Cooperative Models for Effective Public Private Partnerships. (2011) p 19

Jooniselt 3 nähtub esimese etapi eesmärgina küberrünnakute ära hoidmise suutlikkus, mida saab tagada turvameetmete rakendamisega või avalikkuse teavitamisega rünnaku tagajärgedest ning õiguskaitsemeetmetest. Juhul kui ei suudeta avalikkuses tekitada huvi küberrünnakute tagajärgede kohta, siis õiguskaitsemeetmete tutvustamine võimalike karistuste valguses võib mõjuvam olla.[89] Esimese ja teise etapi vahel peab ettevõtetel enne rünnakut eksisteerima täielik ülevaade sellest, millest ettevõtte võrgustik koosneb: seadmed, operatsioonisüsteemid, teenused, rakendused, kasutajad. Lisaks tuleb rakendada juurdepääsukontrolle, tagada turvalisuspoliitika eeskirjade järgne täitmine ning blokeerida juurdepääs rakendustele, mis võivad olla ohtlikud kriitilistele valdkondadele.[90]

[87] Final Report by the High Representative (2013) p. 8-9
[88] ENISA. (2011) p. 19
[89] ENISA. (2011) p. 19
[90] Cisco 2014. Annual Security Report. p. 65

Teises etapis tuleb keskenduda uute ohtude välja selgitamisse läbi uuringute, kaitsemehhanismide tugevdamise ning infojagamise. Kasutades teiste ettevõtete kogemusi ja praktikat, tuleks kohandada ettevõtte strateegiat küberrünnakute eest kaitsmisel. Kolmandas etapis tuleb kaardistada uued võimalikud küberohud, kasutades uute küberohtude välja selgitamiseks infojagamise ja varase hoiatamise süsteeme. Neljandas etapis tuleb arendada hädaolukorras küberrünnakutega toime tulemise võimekust ning viimases etapis võimalikult kiiret küberrünnakust taastumist.[91] Kahe viimase etapi lisaks võib öelda, et kui rünnak on toimunud, siis tähendab, et rünnak oli edukas. Ettevõtetel peab seega olema ametlik tegevusjuhis või strateegia, mis võimaldab neil määrata kahju suuruse, teha võimalusel olukorrapõhine riskianalüüs ning selgitada välja rünnaku teoks saamise põhjused ning võimalikult kiiresti tagada operatsioonisüsteemide normaalne töö.[92]

Avaliku sektori ja erasektori koostöö vajalikkust võib põhjendada asjaoluga, et toimiva koostöö korral on strateegiate rakendamise tõenäosus suurem, [93] sest poliitika kujundamisel ja loomisel peaksid osalema kõik sidusrühmad[94]. Autor nõustub, et tõhus ning rakendatav strateegia on võimalik siis, kui asjasse puutuvad osapooled on saanud otsustusprotsessides kaasa rääkida ning tunda, et ettevõtteid on kaasatud. Selleks, et strateegia rakendamine ja elluviimine toimiksid, tuleb avaliku ja erasektori koostöös jagada informatsiooni, vahetada parimaid praktikaid ja kogemusi kriisisituatsioonidest, läbides erinevaid koolitusi ning osaledes EL poolt välja töötatud küberjulgeoleku alastes harjutustes[95]. Samas tuleb rõhutada, et küberjulgeoleku valdkonnas avaliku ja erasektori koostöömudel erineb tavalistest, traditsioonilistest koostöömudelitest, milleni jõuti esmalt USA-s erinevate traditsiooniliste avaliku ja erasektori koostöömudelite analüüsimisel. USA koostöömudelite lõpptulemus on esitatud käesoleva töö lisas 1. Koostöömudelite analüüsi tulemusel leiti kolm olulist punkti, mis eristavad küberjulgeolekule keskendunud avaliku ja erasektori koostöövorme traditsioonilistest.

Esiteks omandi mõiste küberjulgeolekus ei oma otseseid paralleele olemaolevate kontseptsioonidega senistes PPP mudelites, seda nii intellektuaalse kui ka füüsilise

[91] ENISA. (2011) p. 19
[92]Cisco 2014. Annual Security Report. p. 65
[93] ENISA. (2012) p. 12
[94] Regioonide Komitee arvamus. C 280/19 (2013) lk. 2
[95] ENISA. (2012) p. 12

omandi mõistes. Teiseks küberjulgeoleku valdkonnas puuduvad samaväärsed seadused, mis teistes PPP koostöövormides. Kolmandaks tuleb küberrünnaku toimimise hetkest alates oluliselt lühema aja jooksul reageerida, kui mõnes muus valdkonnas.[96] Autor nõustub kõigi ülal nimetatud punktidega. Küberjulgeolekus on omandi mõiste spetsiifilisem kui traditsioonilises mõttes. Küberjulgeolekus ei ole ühtset seadusandlust, mida tõlgendataks siseriiklikul tasandil ühtselt, rääkimata EL tasandist. Samas liigub EL selles suunas, et ühtlustada ning defineerida küberjulgeoleku alaseid mõisteid üheselt. Kolmanda punktiga seoses on mõistetav, et küberrünnakute korral on reageerimise aeg lühike ning piiratud. Küberrünnakud ei ole üldiselt etteaimatavad ja -oodatavad, neid teostatakse ootamatult ning kõik KII ettevõtted pole võrdsetel tehnoloogilistel ja teadmiste tasemel kaitsmaks KII ettevõtet vajalikus mahus. Küberrünnaku takistamiseks, peab ettevõte olema teadlik erinevatest küberrünnakute liigitustest, et olla õigel hetkel suuteline end küberrünnakute eest kaitsma ning hoidmaks ära suurema kahju tekkimise võimaluse.

Seni on jäänud meedia vahendusel arusaam, et küberrünnakutega on tegutsetud pigem reaktiivelt kui proaktiivselt ehk reageeritakse, kui rünnak on toimunud, mitte ei keskenduta ennetustööle. Samas ei saa kelleltki eeldada, et suudetakse 100% kõiki küberrünnakuid ennetada. Rünnakuid ja haavatavusi pidevalt tehnoloogiliselt arenevas ühiskonnas ei ole võimalik täielikult ennetada, vaid tuleb õppida tagama arvutivõrkude toimepidevus pidevate rünnakute all. Teiste sõnadega, täna aktuaalne küberoht on homseks juba minetatud ja pigem tuleb investeerida toimepidevusse ning infoturbesse laiemalt. Seega kui EL tahab jõuda ja areneda liikmesriigiti paremini integreeritud KII kaitse suunas, siis siseriiklikul tasandil on väljakutse lähtuda EL strateegiast, mis kehtiks korraga kõigile 28 liikmesriigile. Iga liikmesriigi KII jaotub ja on defineeritud siseriiklikul tasandil erinevalt ning eesmärgid võivad siseriiklikes strateegiates olla erinevad[97]. Samas EL liigub parema KII kaitse suunas, kus EL küberjulgeoleku strateegia alusel on 13.03.2014 seisuga esitatud Euroopa Nõukogule Euroopa Parlamendi muudatustega ettepanek direktiiviks, mis tagaks liikmesriikides üldiselt

[96] INSA. (2009) p. 4-5
[97] Pursiainen, C. (2007) p. 11

kõrge taseme võrgu ning infoturbes.[98] KII kaitse seisukohalt kehtib hetkel kuni direktiivi jõustumiseni Euroopa Nõukogu raamotsus 2005/222/JSK[99]

Direktiivi vajalikkust põhjendas Euroopa Komisjoni endine[100] asepresident Neelie Kroes läbi kolme samba süsteemi. Esiteks tuleb liikmesriikidel olla valmis tagama direktiivist tulenevaid nõudeid nii tehniliselt kui ka organisatoorselt. On liikmesriike, kelle tehnoloogiline areng jääb alla eesrindlikumatele liikmesriikidele ning siseriiklikult peavad direktiivi vastuvõtmise hetkeks kõik liikmesriigid valmis olema. Teiseks tuleb liikmesriikidel teha koostööd, sest infovahetuse käigus saab ennetada suuremaid küberrünnakuid. Kui hetkel puudub liikmesriikidel otsene kohustus infovahetuseks, siis direktiivi vastuvõtmisel see kohustus tekib. Kolmandaks tuleb tagada valmisolek nii avalikus kui ka erasektoris.[101] Lisaks soovitab EL liikmesriikidel ellu rakendada järgmised tegevused, mis aitaksid tagada EL liimesriikides parema küberjulgeoleku-alase võimekuse: toetada EL küberjulgeoleku alast valmisolekut; viia läbi liikmesriikides kübervaldkonna simulatsioone; seada liikmesriikides üles siseriiklikud hoiatussüsteemid.[102]

Siseriiklike küberjulgeoleku strateegiate koostamiseks ning parema lõpptulemuse saavutamiseks on CCD COE välja töötanud juhised, mis aitavad siseriiklikult küberjulgeoleku-alaseid strateegiaid koostada. Juhiste välja töötamise üheks eesmärgiks on strateegiate võrreldavuse parandamine. Võrreldavus on oluline, sest siseriiklike strateegiate üheks suurimaks probleemiks on definitsioonide erinev käsitlemine, kus ühe mõiste all - käsitletakse erinevaid lähenemisi.[103] Autor leiab, et CCD COE poolsete juhiste väljatöötamine aitab liikmesriikidel tulevikus koostada strateegiaid, mis on võrreldavad, aidates vähendada ebaühtlaste meetmete kasutamist küberjulgeolekus ning tõstes üleüldist kübervõimekuse taset.

---

[98] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD). 13.03.2014

[99] Euroopa Nõukogu raamotsus 2005/222/JSK ELT [http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32005F0222&from=EN] 05.03.2015

[100] Kabineti aeg lõppes novembris 2014. [http://ec.europa.eu/commission_2010-2014/kroes/]

[101] Kroes, N. 15. High common level of network and information security (debate) [http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140312&secondRef=ITEM-015&language=EN&ring=A7-2014-0103] 16.12.2014

[102] European Commission. EU Cybersecurity plan to protect open internet and online freedom and opportunity. (2013)

[103] CCD COE. (2013) p. 12-13

Üldises plaanis ei ole reaalne oodata, et riiklikust küberjulgeoleku strateegiast lähtuvalt suudaks riik tagada kõikidele KII ettevõtetele ekspertiisi küberrünnakutel. Pigem on suurenemas erasektori roll riigi küberjulgeoleku võimekuse tugevdamises.[104] Eesti küberjulgeoleku strateegia oli EL-is esimene taoline koostatud strateegia.[105] Autor nõustub, et erasektori roll on suurenemas, kuid ei nõustu, et erasektor peaks võtma juhtiva rolli küberjulgeoleku valdkonna kitsaskohtade väljatoomisel. Peamised suunised siseriikliku strateegia näol peaksid tulema siiski riigilt ning erasektor peaks riiki suunama vajaduspõhiselt ehk lähtuvalt sellest, mis KII ettevõtetele valmistab enim probleeme küberjulgeoleku tagamisel. Täpsemat toimeloogikat on lähemalt analüüsitud käesoleva töö teises peatükis.

Küberjulgeolekut peetakse üha rohkem pigem horisontaalseks ehk eri poliitikavaldkondi läbivaks julgeolekuharuks. Küberjulgeoleku olulisus väljendub strateegiliselt siseriiklikes teemavaldkondades, kuna puudutab kõiki ühiskonnaliikmeid. Samas siseriiklikud strateegiaid (nt Eesti puhul) rõhutavad rahvusvahelise koostöö suurendamise hädavajalikkust, sest küberohud ületavad riigipiire. Seega on riiklik küberjulgeoleku strateegia vahend, mis annab võimaluse parandada esmalt riiklikke infrastruktuuride ja teenustele julgeolekut ning paindlikkust ning seejärel keskenduda rahvusvahelisele koostööle.[106] Kuna EL soovitab avalikul ja erasektoril garanteerida parem koostöö, siis järgnevalt tuuakse välja võimalikud ettepanekud, kuidas saaks tagada sujuvama koostöö era- ja avalikus sektoris. Esiteks peab koostööle keskendunud rühm esindajaid nii avalikust kui ka erasektorist olema piisavalt suur, katmaks kõiki valdkondasid, kuid samas piisavalt väike, et tegutseda vajadusel kiiresti. Teiseks avalikul sektoril peab olema piiritletud roll kindlate ülesannetega ning erasektor peab EL arvates võtma juhtrolli. Kolmandaks tuleb leida esindajad, kel on motivatsioon ja ühised huvid küberjulgeoleku alaste probleemidega tegelemiseks[107].

Alapeatüki kokkuvõtteks võib öelda, et küberjulgeoleku strateegiad pole küll kohustuslikud täitmiseks[108], kuid annavad kindlad juhised ja seavad eesmärgistatud

[104] Choo, R. (2011) p. 727
[105] ENISA (2012) p. 5
[106] *Ibid.:* p. 4
[107] INSA (2009) p. 3
[108] Eesti küberjulgeoleku strateegia on kohustuslik riigiasutustele, samuti on EL direktiiv kohustuslik, kui see EL tasandil vastu võetakse

tegevused olukorras, kus küberrünnak on aset leidnud. Küberjulgeoleku valdkonna ühtlustatud taseme tagamiseks ning olemasolevate puuduste vähendamiseks nii EL kui ka liikmesriikide tasandil, tuleb soodustada koostööd avalikus ja erasektoris. Sidusrühmasid on oluline kaasata ja KII ekspertidele, tuleb anda võimalus poliitika kujundamisprotsessides kaasa rääkida. Edusamme on tehtud strateegiate tõhusamaks muutmise suunas CCD COE juhiste välja töötamisega. Senisteks küberjulgeoleku strateegiate puudusteks[109] on siseriiklikult erinevate definitsioonide käsitlemine, mida CCD COE juhistega proovitaksegi edaspidi välistada.

1.4 Kriitilise infrastruktuuri kaitse

Käesolev alapeatükk keskendub KII kontseptsioonile ning tuuakse välja, kuidas erinevad käsitlused KII defineerivad. KII kaitse osas selgitatakse, miks kaitse on vajalik ning kuidas on võimalik KII paremini kaitsta. KII on süsteemid, mis hoiavad koos eluliselt oluliste teenuste toimimise, tagades sealjuures inimestele tarneahela, tervishoiu, turvalisuse, majandusliku ning sotsiaalse heaolu. Kuigi nimetatud taristud ja teenused on eksisteerinud läbi aastate, siis KII käsitlus on võrdlemisi uus[110]. KII laiem kontseptsioon sai alguse 1990. aastate keskel USA-s, kus erinevates programmides, tegevuskavades ning üldisemas seadusandluses defineeriti KII kui elutähtsat valdkonda. Mõningase viivitusega muutus kontseptsioon oluliseks ka Euroopas.[111] USA ja NATO dokumentatsioonis on KII mõiste EL-i omast erinev. USA esmane ning konkreetsem definitsioon pärineb 1997. aastast, kus KII oli erasektorile kuuluv ja ühiskonna põhivajadusi täitev oluline ressurss. Võrreldes EL-iga on USA lähenemine pigem laiem ning ühendatud olulise ressursi mõistega[112].

Pärast 11. septembri sündmusi, kui Euroopas muutus üleüldiselt küberjulgeolek sh KII kaitse olulisemaks, siis paljud USA KII põhielemendid võeti NATO dokumentatsiooni üle. NATO defineeris seega KII kui rajatist, teenust ja infosüsteemi, mis on riikidele

[109] Puudused, sest erinevad küberjulgeoleku alased definitsioonid liikmesriikides ei anna alust andmete võrdlemiseks või kasvõi olukordade hindamiseks, sest mõistete erineval käsitlemisel võidakse rääkida erinevatest asjadest.
[110] Pursiainen, C. (2007) p. 17
[111] *Ibid.:* p. 17
[112] NIPP (2006) p. 17

eluliselt niivõrd tähtsad, et nende töövõimetus või hävimine oleks riigi julgeolekule nõrgestava mõjuga.[113] Euroopa Nõukogu direktiivi järgi käsitletakse KII kui elutähtsat infrastruktuuri, mis on EL-i liikmesriikides asuv vara, süsteem või nende osa, mis on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks ning mille kahjustada saamine või hävimine mõjutaks nimetatud toimingute toimimishäire tulemusena oluliselt liikmesriiki.[114] Eestis on hädaolukorra seaduse §34[115] järgi nelikümmend kaks elutähtsat teenust ehk KII valdkonda, mis kõik vajavad küberjulgeoleku mõistes kaitset küberünnakute eest. Nimetatud nelikümmend kaks elutähtsat teenust on jagunenud seitsme ministeeriumi valitsemisala vahel ning lisaks on elutähtsaid teenuseid Eesti Panga haldusalas. KII Eesti liigitus on ära toodud lisas 2.

EL-i õigusaktides on lisaks KII-le kasutusel mõiste „Euroopa elutähtsad infrastruktuurid“, milleks on liikmesriikides asuvad elutähtsad infrastruktuurid ja mille kahjustada saamisel või hävimisel oleks oluline mõju vähemalt kahele liikmesriigile.[116] Antud töös on oluline vahet teha, et keskendutakse liikmesriikides olevatele elutähtsatele ehk KII-le, mitte „Euroopa elutähtsatele infrastruktuuridele“. Võrreldes nii USA, EL kui ka NATO KII mõisteid, siis väga suuri erinevusi definitsioonides pole. USA mõiste puhul vaadeldakse KII laiemas mõistes ja teises kontekstis, kuid üldjoontes on KII mõiste maailmas üheselt defineeritud, mida võib pidada huvitavaks, sest kõik muud küberjulgeolekuga seotud mõisted nagu küberruum, küberrünnak, küberohud jt on pigem erinevalt kui sarnaselt defineeritud, olles küberjulgeoleku üheks suurimaks probleemiks.

Liikudes KII küberrünnakute eest kaitsmise suunas, siis EL-is muutus KII kaitse olulisemaks pärast terrorirünnakuid Jaapanis (1995)[117], Hispaanias Madridis (2004)[118], Suurbritannias Londonis (2005)[119] ja Venemaal Vologradis (2013[120]).[121] Viidates

[113] Pursiainen, C. (2007) p. 54-55
[114] Euroopa Nõukogu direktiiv 2008/114/EÜ, art 2
[115] Hädaolukorra seadus. §34
[116] Euroopa Nõukogu direktiiv 2008/114/EÜ, art 2
[117] Japan railroad station attack.
[http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199504190006] 07.02.2015
[118]Spain bombing.
[http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200403110004] 07.02.2015
[119] London underground bombing.
[http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200507070002] 07.02.2015

eelnenud sündmustele, taibati, et terrorism ning küberjulgeolek on tihedalt omavahel seotud ning tuleb liikuda tõhusama KII kaitse suunas. EL esmased õigusaktid KII kaitsmiseks võeti vastu 2004. aastal,[122] millele järgnesid mitmed uuendused ning täpsemad programmid KII kaitseks.[123] Europoli direktor on öelnud 2012. aastal, et on „mures levinud, kuid eksliku arvamuse pärast, et internet on haavamatu". Ta lisas, et sageli on kuulda, kuidas kurjategijad, terroristid või välisriikide valitsused on taas korraldanud uue küberrünnaku mõne elutähtsa taristu vastu. Ohvreid enamiku rünnakute kohta ei avalikusta, sest kardetakse maine kahjustumist. Samas on ilmnenud rünnakuid Euroopa internetitaristu ja pangandussüsteemide vastu, mis olid liiga hävitavad, et neid saaks varjata.[124] Autor nõustub Europoli direktori väidetega, et ettevõtted ei pruugi mõista, mis on küberrünnakute tegelik mõju ja haardeulatus ning konkurentsi tingimustes pigem hoitakse rünnakute-alane info enda teada. Samas on liigutud aastast-aastasse selles suunas, et ettevõtted on kohustatud esitama toimunud rünnakute kohta infot pädevale asutusele, kelleks Eestis on RIA[125].

Eesti president Toomas Hendrik Ilves on väitnud, et traditsiooniline arusaam sellest, et riigi rivist välja löömiseks piisab riigi territooriumi vallutamisest või sõjaväe purustamisest, enam alati paika ei pea. Tänapäeval on võimalik vaenlasel sõjaväest mööda vaadata - keerukate küberrünnetega saab riigi majanduse ja kriitilise taristu vähemalt ajutiselt põlvili suruda.[126] Euroopa Komisjoni dokumentatsioonist võib leida näiteid, milline on võimalik kahju, kui KII tabab küberrünnak. Sageli arvatakse, et rünnaku mõju on minimaalne ning kahjud väikesed, aga näiteid võib tuua mõlemast äärmusest. Kui esineb nn edukas küberrünnak avalikele telefoniliinidele, siis tarbijate telefoniside on mõni hetk häiritud, kuniks tehnikud olukorra lahendatavad. Kui rünnaku objektiks on keemia- või loodusliku gaasi kontrollsüsteemid, siis olukord võib viia massiliste inimohvriteni või märkimisväärsete füüsikaliste kahjustusteni.[127]

---

[120] Suicide bomber in Volgograd train station. [http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201312290007] 07.02.2015
[121] Udeanu, G. (2012) p. 86
[122] Euroopa Komisjoni teatis KOM/2004/0702
[123] Udeanu, G. (2012) p. 86-87
[124] Euroopa Majandus- ja Sotsiaalkomitee arvamus. (2013) lk 3
[125] Riigi Infosüsteemi Amet. Turvaintsidentide käsitlemine CERT Eesti. [https://www.ria.ee/cert/] 07.02.2015
[126] Ilves, T. H. Ilves: küberrünnakud võivad riigi vähemalt ajutiselt põlvili suruda. 30.08.2013
[127] Euroopa Komisjoni teatis KOM/2004/0702 lk 3

Iga liikmesriigi KII valdkonnad saab jagada vastavalt kriitilisuse tasemele, mis erineb igal riigil vastavalt geograafilisest asukohast, loodusvaradest, rahvuslikest huvidest, sotsiaalmajanduslikust arengust ja infovajaduse kaitse taseme liigitusest. Tavaliselt sisaldab KII järgmisi valdkondi: tarne, transport, infotehnoloogia ja side, vesi, toit, rahvatervis, tööstusharud, riigikaitse süsteemid ning keemilised ja tuumaalased asutused.[128] Liikmesriigiti on liigitus erinev, vastavalt liikmesriigi enda nägemusele, seega pole ülalolev loetelu ammendav. Siinkohal tuleb rõhutada, et paljud valdkonnad on üksteisest sõltuvad, mis tähendab, et kui küberrünnak tabab energeetika valdkonda, siis on rünnaku mõju palju suurem, kui transpordi valdkonda tabanud küberrünnak. Leitakse, et telekommunikatsiooni ja elektrienergia protsessid on kõige kriitilisemad valdkonnad, mis mõjutavad kõiki teisi valdkondi[129].

KII kaitse olulisus ettevõtjate seisukohast väljendub selles, et kui elektrivõrgu rünnaku puhul on paljudel ettevõtetel võimalik edasi toimida lokaalsete akude või generaatoritega, siis vähestel puudub võime seda lõputult ja iseseisvalt oma vahenditest lähtuvalt teostada. Seega vältimaks elutähtsa infrastruktuuri mitte toimimist, peaks iga liikmesriigi huvides olema KII kaitse.[130] Samas tasub olla realistilik, sest pole olemas riiki, kes 100% suudaks tagada igakülgse KII kaitse.[131] Küberrünnakud ja -ohud on kiiresti muutuvad ning ületavad riigipiire. Riikidel on lisaks muudele seadusest tulenevatele kohustustele keeruline keskenduda vaid küberjulgeoleku valdkonna reguleerimisele ning pidevalt uuenevate sündmustega kursis olla.

Tagamaks vajaliku KII kaitse, tuleb eelnevalt määratleda KII kaitsest tulenevalt olulised punktid. Ettevõtte tegevusvaldkonnast lähtuvalt tuleb kaardistada tõenäolisemad küberriskid ning sellest tulenevalt määratleda tegevused ja valdkonnad, mis vajaksid rohkem tähelepanu. Eeskätt tuleb rõhuda paindlikkusele, sest lähtudes rangetest ja kindlatest piiridest, võidakse küberrünnakutest tingitud olukordi valesti hinnata ning kahjud võivad olla kordades suuremad[132]. KII kaitse defineerimisel tuleb jätta ruumi paindlikule lähenemisele ning võimalusel läheneda spontaanselt, sest küberruumi ohud on muutumises. Samas üldreeglid ning tegevusjuhised KII küberrünnakute eest

[128] Udeanu, G. (2012) p. 88
[129] Lukasik et al. (2003) p. 7
[130] Purser, S. (2011) p. 238
[131] Lukas, L., Necesal, L. (2010) p. 1323
[132] Holmström, P., Landstedt, J. (2007) p. 74

kaitsmisel tuleb määratleda arusaadavalt. Probleemne on pigem see, et üldised süsteemid töötavad üle kõikide infrastruktuuride, seega KII kaitse vastutus lasub suuremal või vähemal määral riigil[133]. Kõik KII valdkonnad on omavahel seotud ning üldsuunised paremaks kaitseks tuleks kehtestada riigil. Riigid eeskätt valitsustega on peamiselt õiguslikult vastutavad KII kaitse eest, sest enamus KII ettevõtteid kuulub erasektorile[134].

Probleem seisnebki autori arvates selles, et ühest küljest oodatakse, et riik garanteeriks üldtasemel suunised paremaks kaitseks nagu tagab EL liikmesriikidele nn miinimumstandardid. Teisest küljest EL miinimumstandardid tähendavad seejuures seda, et EL strateegias tuuakse välja üldisemad punktid ja kitsaskohad, millele liikmesriigid peaksid tähelepanu pöörama. Erasektor peaks nii palju vastu tulema, et riigil oleks infot, millisel tasemel ja määral riik panustama peaks. Kui ettevõtted hoiavad infot endale ja ei jaga ärisaladusest tulenevalt informatsiooni, siis riigil on keeruline neid abistada ja küberkaitsesse investeerida. Kuigi avalik sektor vastutab poliitika kujundamise eest, siis lasub lõppkokkuvõttes erasektoril spetsiifilisem vastutus[135]. Seega on riigil vaja põhjendada erasektorile avalikust sektorist lähtuvalt, miks on pikaajalises perspektiivis tarvis investeerida KII kaitsesse.[136] Teisalt tuleks mõista KII ettevõtteid, sest sageli valitsustel on eraettevõtete omanike suhtes ootused, et nad panustaksid, arvestaksid avaliku huviga ja investeeriksid küberkaitse tugevdamisesse. Ettevõtete seisukohast tuleb mõista, et ettevõtted lähtuvad eeskätt majandustegevuse jätkusuutlikkusest. Kui enamus vahenditest kulub küberkaitse tugevdamisele, siis ettevõte võib seeläbi ohustada ärimudeli üldist suutlikkust ja püsima jäämist.[137]

Autori arvates võib siinkohal tekkida ka usalduse küsimus. Eraettevõtted pigem ei jaga detailset infot äritegevuse kohta, kaitstes ärisaladust ning teavet konkurentide eest. Koostöö toimimise eesmärgil, tuleb pingutada mõlemal osapoolel. Kopenhaageni koolkonna põhiargumendiks küberjulgeoleku tagamiseks seisneski selles, et riik referentobjektina peab vajadusel kaitsma neid, kellel julgeoleku aspektist on tarvis

[133] Lukas, L., Necesal, L. (2010) p. 1323
[134] Abele-Wigert, I. (2006) p. 57-58
[135] Lukas, L., Necesal, L. (2010) p. 1323
[136] Purser, S. (2011) p. 238
[137] De Bruijne, M., Van Eeten , M. (2007) p. 24

õiguslikku abi ning kes vajavad kaitset. Lisaks rõhutab EL Regioonide komitee, et kuigi erasektori operaatorid muutuvad järjest enam vastutavaks kriitilise tähtsusega taristute ja internetiteenuste eest, ning hoolimata vajadusest tunnistada erasektori otsustavat tähtsust, peab riik võtma lõpliku vastutuse nii kodanike vabaduse säilitamise kui ka nende turvalisuse eest internetikeskkonnas[138]. Näitena võib tuua Suurbritannia, kes lisaks Eestile panustab, et erasektori ja riigi vaheline koostöö sujuks ja andmete jagamine KII ettevõtetega küberrünnakutest toimiks. Kui suurettevõtted jagavad oma kogemusi, siis läbi selle suudavad väikeettevõtted end halvimaks ette valmistada ja küberrünnakute ennetamiseks valmis olla.[139] Autor nõustub, et kui väikeettevõtetel on niigi võimalused ja ressursid piiratud, siis suurettevõtete kogemuse ning hea praktika jagamise teel suudetaks kulusid kokku hoida ning kasvõi minimaalne tase küberjulgeolekus tagada.

[138] Regioonide Komitee arvamus. (2013) lk 5
[139] Ashford, W. 31.10.2013

2. KÜBERJULGEOLEKU STRATEEGIATE VÕRDLUS EUROOPA LIIDUS EESTI KRIITILISE INFRASTRUKTUURI NÄITEL

2.1 Euroopa Liidu ja Eesti küberjulgeoleku strateegiate analüüs

Antud alapeatükis võrreldakse EL ja Eesti küberjulgeoleku strateegiaid, kus esmalt tuuakse välja KII ettevõtetega seotud strateegiate peamised eesmärgid ning tegevused. Analüüsitakse, kas EL strateegias välja toodud ettepanekud liikmesriikidele on Eesti siseriiklikus strateegias rakendatud või mitte. Autor rõhutab, et strateegiaid analüüsitakse KII-st lähtuvalt, sest käesolev töö keskendub KII-le. Samuti tasub välja tuua, et EL küberjulgeoleku strateegia on vaid üks osa EL küberjulgeoleku nn paketist, lisaks kujundavad küberjulgeoleku valdkonda ettepanek direktiiviks [140], erinevate komiteede hinnangud ning teatised.

EL küberjulgeoleku strateegia[141] üheks märksõnaks on küberuum, mis oleks avatud, ohutu ning turvaline, rõhutades mitmel korral, et küberjulgeoleku tagamisel on eraldi roll nii avalikul kui ka erasektoril. Laiemas plaanis on avaliku sektori ülesandeks tagada juurdepääs avatud internetile ning erasektoril tuleks võtta initsiatiiv läbipaistvama, vastutust võtva ja turvalisema küberjulgeoleku suunas.[142] Direktiivi artiklis 5[143] on välja toodud, mida siseriiklik strateegia peab sisaldama: peale strateegiliste eesmärkide tuleb keskenduda infovahetusele ning koostööplaani koostamisele.

[140] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD)
[141] Avaldatud 07.02.2013 seisuga
[142] European Commission. Cyber Security Strategy of the European Union. p. 2-4
[143] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD)

Ajavahemikku 2008-2013[144] katnud Eesti küberjulgeoleku strateegia, tugines eeskätt küberruumi haavatavuse vähendamisele, eeldades vastavate riigisiseste tegevuskavade elluviimist ja aktiivse rahvusvahelise koostöö olemasolu[145]. Seega võrreldes EL ja Eesti strateegiate märksõnasid või rõhuasetusi, võib öelda, et EL keskendub pigem üldisematele põhimõtetele ning Eesti siseriiklik strateegia keskendub konkreetsemalt küberruumi haavatavuse vähendamisele. Autori arvates on loogiline, et EL väljendab strateegiates üldisemaid kitsaskohti ja iga liikmesriik vastavalt siseriiklikule olukorrale keskendub spetsiifilisematele probleemidele. EL annab üldised suunitlused, sest igas liikmesriigis on info ja kommunikatsioonitehnoloogia (edaspidi: IKT) arengutase ning küberjulgeoleku-alased probleemid erinevad. Nii EL kui ka Eesti küberjulgeoleku strateegiate eesmärgid või eesmärkidest lähtuvad tegevused on välja toodud tabelis 3, kus on hinnatud, kas strateegiate eesmärkidel ja tegevustel on otsene seos KII-ga.

Tabel 3. Küberjulgeoleku strateegiate eesmärkide seotus kriitilise infrastruktuuriga.

EL küberjulgeoleku strateegia eesmärgid, tegevused	**Seotus kriitilise infrastruktuuri ettevõttega**	**Eesti küberjulgeoleku strateegia eesmärgid, tegevused**	**Seotus kriitilise infrastruktuuri ettevõttega**
Küberjulgeoleku toimepidavuse tagamine	**JAH**	Turvameetmete süsteemi arendamine ja rakendamine	**JAH**
Küberkuritegevuse drastiline vähendamine	EI	Küberjulgeoleku alase kompetentsuse tõstmine	EI
Ühise julgeoleku- ja kaitsepoliitika raames küberkaitsepoliitika arendamine	EI	Õigusruumi täiendamine	**JAH**
Tööstuslikke, tehnoloogiliste ressursside arendamine	**JAH**	Rahvusvahelise koostöö arendamine	**JAH**
EL-is ühtse rahvusvahelise küberruumi poliitika loomine	**JAH**	Teavitustegevusest tulenevad eesmärgid	EI

Allikas: Autori koondatud EL ja Eesti küberjulgeoleku strateegiate alusel.

[144] Uus küberjulgeoleku strateegia ajavahemikuks 2014-2017 on vastu võetud, kuid kuna strateegia võib veel muutmisele minna, siis hinnati käesolevas töös eelmise perioodi strateegiat
[145] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 4-6

Tabeli 3 andmetest nähtub, et nii EL kui ka Eesti tasandil ühtivad eesmärgid ja tegevused KII-ga kolmel juhul. Järgnevalt analüüsitakse esmalt EL-i ning seejärel Eesti strateegilisi eesmärke, mis on otseselt KII-ga seotud. EL esimene eesmärk, küberjulgeoleku toimepidavuse tagamine, keskendub eeskätt avaliku ja erasektori koostöö suurendamisele, õigusalaste miinimumstandardite kehtestamisele, ennetus-avastamismehhanismide välja töötamisele, infovahetuse tõhustamisele ja teadlikkuse tõstmisele. [146] Seega liikmesriigi KII ettevõtetele tähendaks näiteks miinimumstandardite kehtestamine, et iga KII ettevõte peab koostama miinimumstandarditest lähtuvad tegevuskavad või ettevõttesisesed küberjulgeoleku strateegiad. Antud EL strateegiline eesmärk on sisse viidud ka Euroopa Parlamendi ja Nõukogu direktiivi ettepanekusse konkreetsete meetmetena kaitsmaks EL siseturgu, KII ettevõtteid ning teisi asjassepuutuvaid osapooli[147].

Lisaks rõhutatakse esimese eesmärgis erasektori valmisolekut koostööks, sest KII ettevõtetena on neil oluline roll küberjulgeoleku tagamisel. [148] Ettevõtted peaksid sektorite üleselt jagama parimaid praktikaid ning olema valmis koostööks. Avalik sektor peaks EL sõnul regulaarselt avaldama infot uute võimalike ohtude/riskide kohta, mida on KII ettevõtetel oluline teada. Direktiivi ettepanekus rõhutatakse rollide jaotust, kus koostöömehhanism ja juhised peavad tulema EL tasandilt ning siseriiklikult tuleb kehtestada miinimum turvanõuded, mida kõik KII ettevõtted järgiksid[149]. Direktiivi ettepanekust tuleneb ENISA roll, kes EL tasandil peab tagama, et kõik osapooled oleksid teavitatud uutest trendidest ning parimast praktikast rünnakute ennetamisel ja nendega toimetulemisel[150].

Teine EL strateegiline eesmärk on seotud tööstuslike ja tehnoloogiliste ressursside arendamisega küberjulgeolekus. Lühidalt öeldes, küberjulgeoleku tagamine ei lähtu vaid tehnoloogiast, vaid on seotud füüsiliste tarkvara komponentidega. [151] Tagamaks internetis küberjulgeolek, siis on oluline, et ollakse kindlad kolmandatest riikidest

[146] European Commission. Cyber Security Strategy of the European Union. p. 4-9
[147] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD), p 4
[148] European Commission. Cyber Security Strategy of the European Union. p. 2-3
[149]European Commission. Texts adopted – proposal for a directive. (2014) Amendment 4
[150] *Ibid.:* Amendment 14
[151] European Commission. Cyber Security Strategy of the European Union. p. 12

pärinevate tarkvarakomponentide usaldusväärsuses. Seoses teise eesmärgiga toetab EL IKT valdkonna toodete usaldusväärsuse, turvalisuse tõstmist ning turvastandardite arendamist, kus tähelepanu keskpunktis on KII ettevõtted. Liikmesriikide KII ettevõtetele tähendaks see tõenäoliselt kulude suurenemist. Samas rõhutatakse direktiivi ettepanekus, et liikmesriikide tehnoloogiline valmisolek on liikmesriigiti väga erinev. Selleks, et KII ettevõtted saaksid siseriiklikult tagada valmisoleku direktiivist tulenevate miinimumnõuete täitmiseks rõhutab EL direktiivi ettepanekus, et ülikoolidel ning teistel uuringusasutustel on täita kandev roll teadus-arendustegevuses.[152] Kolmas eesmärk keskendub ühisele rahvusvahelise küberruumi poliitika loomisele, puudutades KII ettevõtteid seeläbi, et ettevõtteid ergutatakse lisaks siseriiklikule ka rahvusvahelisele koostööle.[153] Näiteks EL tasandil töögruppide tasandil kohtumised või rahvusvaheliste organisatsioonide (NATO, ÜRO, EL) seminaridel, koolitustel osalemine. Seega rahvusvahelise koostöö mõistes mitte ainult avaliku sektori koostöö, vaid ka ettevõtete omavahelist koostööd tuleks arendada.

EL strateegia analüüsi kokkuvõtteks võib öelda, et EL tasandil KII ettevõtetega seotud eesmärgid on keskendunud peamiselt koostöö suurendamisele ja koostöövalmiduse tõstmisele. Konkreetsemalt puudutab ettevõtteid kindlasti erinevate standardite kehtestamine EL tasandil ning siseriiklikul tasandil nende rakendamine. Autor leiab, et KII ettevõtted on suuremal või vähemal määral teadlikud ettevõtte olulisusest riigi julgeoleku mõttes ning teatud tasemel KII turvalisuse ja kaitse tagamise on KII ettevõtted saavutanud. Seega kui tulevikus kehtestatakse standardid, mis siseriiklikult rakendamist vajaksid, siis Eesti kui kõrgelt arenenud infoturbega[154] riik tõenäoliselt suuri muudatusi KII kaitse tagamiseks tegema ei pea.

Eesti siseriikliku küberjulgeolekustrateegia viiest eesmärgist neli on seotud KII ettevõtetega. Esimene eesmärk, mis keskendub turvameetmete arendamisele ja rakendamisele[155], puudutab KII-d niisamuti kui EL tasandi tööstusliku ja tehnoloogilise arengu tõstmise eesmärk. Kui EL tasandil keskenduti pigem füüsiliste komponentide turvalisuse tõstmisele, siis Eesti tasandil tähendab see KII ettevõttele pigem

[152] European Commission. Texts adopted – proposal for a directive. (2014) Amendment 7
[153] European Commission. Cyber Security Strategy of the European Union. p. 14-16
[154] Eesti on maailmas 5.kohal. ITU. Global 2014 results. ABI Research. (2014) [http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Global_2014_results.pdf]
[155] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 14-16

vastupanuvõime suurendamist küberrünnakute eest, kindlustades infosüsteemide vastupidavuse ja turvameetmed. Allolevas tabelis 4 on näitena välja toodud, milliseid kaitsemeetmeid asjassepuutuvad osapooled küberjulgeolekus kasutada võiksid. Teiste sõnadega, kes on tehnilise poole peamised vastutajad, mis on referentobjektid ning kuidas tagada kaitse erinevate referentobjektide korral nii siseriiklikul kui ka rahvusvahelisel tasandil.

Tabel 4. Küberjulgeoleku osapooled ning kaitsemeetmed

	Tehniline pool	**Küberjulgeoleku õiguslik pool**	**Sõjaline, tsiviilkaitse**
Peamised vastutajad	*arvuti eksperdid *viirusetõrje ettevõtted	*õiguskaitse *luure institutsioonid	*turvaspetsialistid, sõjavägi, tsiviilkaitse loomine
Peamised referentobjektid	*arvutid *arvutivõrgud	*erasektor *salastatud informatsioon	*sõjalised võrgustikud *kriitiline infrastruktuur
Kaitsekontseptsioon	**Teabekindlustamine**		
Siseriiklikul tasandil	*CERT	*arvutiõigus	*kriitilise infrastruktuuri kaitse *paindlikkus *küberkaitse
Rahvusvahelisel tasandil	*rahvusvahelised CERT-d *rahvusvahelised informatsiooni standardid	*seaduste harmoniseerimine *vastastikune õigusalane abistamine	*relvastuskontroll *rahvusvahelised käitumisnormid

Allikas: Collins, A. Contemporary Security Studies. 2013. p.374

Teine Eesti küberjulgeoleku strateegia eesmärk on seotud kompetentsuse tõstmisega[156], mis EL tasandi strateegias vastas küberjulgeoleku vastupidavuse suurendamise eesmärgile. Mõlema tasandi strateegia eesmärgid lähtuvad sellest, et nii avalikus kui ka erasektoris tuleb suurendada infoturbe alaste teadmiste kvaliteeti. Laiemas plaanis on haavatavuse vähendamise ning toimepidavuse parandamise eesmärgiks mitmesugused tegevused nagu erinevate turvameetmete kehtestamine, riskianalüüside teostamine ning asjakohane väljaõpe.

[156] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 16-17

Kolmas eesmärk keskendub õigusruumi ning -loome täiendamisele, kus Eesti näitel soovitatakse ette valmistada KII küberkaitset tagavad õigusaktid.[157] Autor rõhutab siinkohal, et Kopenhaageni koolkonna autorid leidsidki, et riik peab tagama kaitse ja õigusliku abi neile, kes seda vajavad[158]. Eesti strateegiast tuleb välja, et riik kaitseb KII ettevõtteid läbi küberkaitse regulatsiooni ette valmistamise ning rakendamisega. Neljas eesmärk Eesti strateegias keskendub rahvusvahelise koostöö arendamisele. Eesti soodustab strateegias rahvusvahelist koostööd ning on olnud üks juhtivamaid liikmesriike küberjulgeoleku valdkonnas.[159] KII ettevõtteid puudutab rahvusvaheline koostöö nii EL kui ka Eesti tasandi strateegiates. EL tasandil puudutab see läbi koolituste, töögruppides osalemise ning parima praktika vahetamise. Mõlemas strateegias rõhutatakse kogemuse ja info jagamist ning selle vajalikkust.

Peale konkreetsete strateegiliste eesmärkide, toob EL strateegia välja rollide jaotuse, kus väidetakse, et kõik osalejad on seotud küberjulgeolekuga ning valdkonna tugevdamiseks tuleb võtta vastutus nii siseriiklikul kui ka EL tasandil. EL rõhutab, et liikmesriikide valitsused (avalik sektor) on võrreldes erasektoriga tõhusamad küberintsidentide ennetamises ja nende suhtes reageerimises. Seega avaliku sektori roll on luua ja hoida kontakte erasektoriga.[160] Liikmesriikide tasandil soovitab EL, et liikmesriikides eksisteeriksid siseriiklikud küberjulgeoleku strateegiad koos kindlaks määratud tegevuskavadega küberjulgeoleku toimepidavuse suurendamiseks ja võimekus küberrünnakutega toimetulemiseks. Vastutus peaks EL sõnul olema optimaalne ning pigem valitsuse tasandil.[161] Eesti strateegia vastab EL soovitustele, sest siseriiklikul tasandil küberjulgeoleku strateegia eksisteerib. Lisaks sedastab Eesti strateegia rollide osas, et nii indiviidid, ettevõtted kui ka avalik sektor vastutavad ise oma vahendite turvalisuse eest.

Alapeatüki kokkuvõtteks võib seega öelda, et mõlemad strateegiad on olemuselt sarnased, mida võis ka eeldada, sest Eesti on üks juhtivamaid liikmesriike küberjulgeoleku valdkonnas ning on jaganud teadmisi ja parimat praktikat rahvusvahelisel tasandil. Mõlemad strateegiad rõhutasid mitmel korral koostöövajadust

[157] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 17-21
[158] Buzan, B., Jaap, de W., Woever, O. (1998) p. 36
[159] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 32-35
[160] European Commission. Cyber Security Strategy of the European Union. p. 17
[161] *Ibid*

ja seda eeskätt avaliku sektori ja KII ettevõtete vahel. Lisaks keskendusid mõlemad strateegiad üldisele teadlikkuse tõstmisele ühiskonnas. Oluline on, et kõik sektorid oleksid piisavalt teadlikud küberjulgeoleku valdkonna riskidest ja ohtudest. Erinevuseks strateegiate vahel võibki pidada seda, et EL annab liikmesriikidele kätte üldisemad suunad ja liikmesriigid vastavalt vajadusele koostavad siseriiklikud strateegiad.

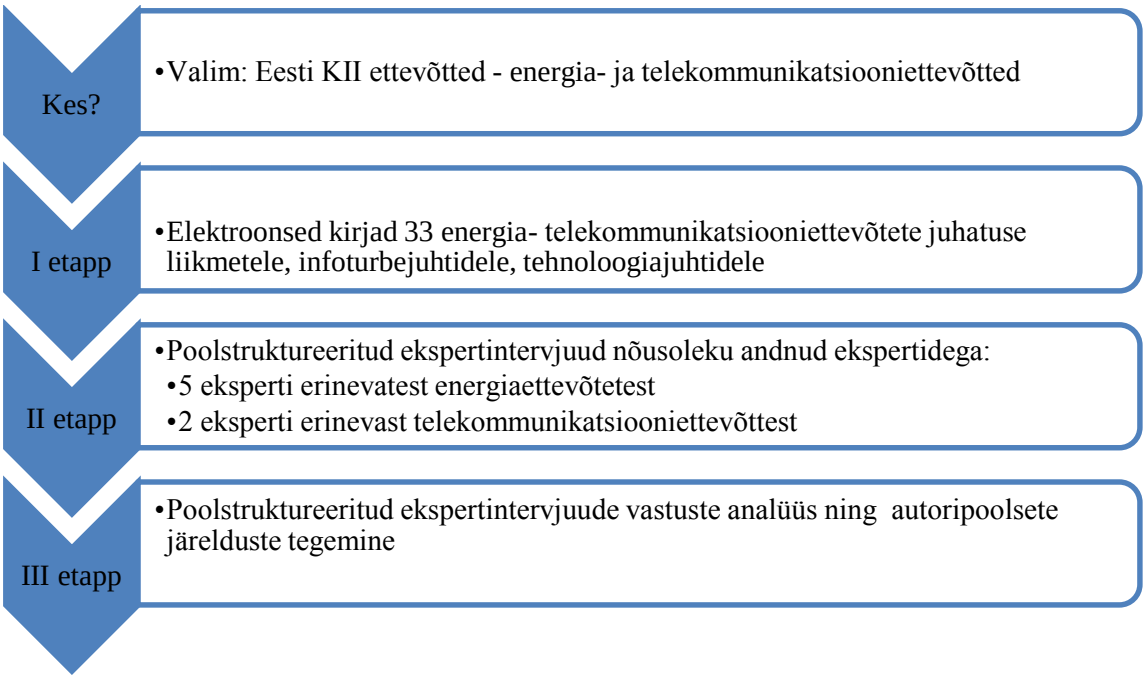
2.2 Eesti kriitilise infrastruktuuri ettevõtete eksperthinnangute analüüs

Antud alapeatükis analüüsitakse Eesti KII ettevõtete ekspertide arvamust küberjulgeoleku valdkonnas, hinnates reaalset hetkeseisu erasektorites seoses küberjulgeolekuga. Autor viis läbi poolstruktureeritud ekspertintervjuud ning valimisse kaasati Eesti telekommunikatsiooni ja energiaettevõtete eksperdid, sest nimetatud teenused on vajalikud kõikide teiste elutähtsate teenuste toimimiseks, olles hädaolukorraseaduse §34 alusel neljakümne kahe[162] teenuse hulgast kõige olulisemad. Lisaks leiab autor, et telekommunikatsiooni ja energia valdkonna häirete või küberrünnakutega puututakse eraisiku tasandil tõenäoliselt kõige rohkem kokku ja tajutakse nimetatud valdkondades toimuvat paremini.

Esmalt saadeti telekommunikatsiooni ning energiaettevõtete juhatuse liikmetele, infoturbejuhtidele ja tehnoloogiajuhtidele[163] kokku 33 elektroonset kirja, kus kirjeldati uurimustöö olulisemaid punkte ning töö eesmärki. Elektroonsed kirjad saadeti seepärast, et selgitada välja kõikide Eesti KII ettevõtetest, kui paljud on uurimuses nõus osalema ja ettevõtte kogemust jagama. Võimaliku probleemina nägi autor, et ettevõtted ei pruugi nõustuda uurimuses osalema ärisaladusest tingituna. Vastupidiselt oldi pigem abivalmid ettevõtte kogemust jagama, kuid anonüümselt, seepärast pole ka antud töös välja toodud ekspertide ametipositsioonid või valdkondlikud töökogemused. Peale selle prooviti mitmel korral uurimusse kaasata RIA ekspertarvamust, võtmaks arvesse ka avaliku sektori esindaja seisukohti, kuid RIA ei avaldanud soovi ega vastanud korduvatele päringutele.

[162] Hädaolukorra seadus §34
[163] Ekspertide ametinimetused ettevõtete lõikes olid erinevad

Eksperdid, kes nõustusid uurimuses osalema, põhjendasid nõustumist asjaoluga, et küberjulgeoleku-alased uuringud on aktuaalsed ning soovitakse ettevõtte parimat praktikat ning kogemust jagada. Nõustunud ettevõtete ekspertidega viidi läbi ekspertintervjuud ning kui kõik intervjuud olid läbi viidud, analüüsis ning võrdles autor iga intervjuud eraldi lisas 3 välja toodud küsimuste alusel. Kuna intervjuude maht polnud väga suur, ei kasutatud vastuste analüüsimisel eraldi analüüsiprogramme. Autor otsustas kasutada ekspertintervjuusid, sest intervjuu vorm on ainuvõimalik delikaatsete uuringuteemade korral ning teatud privaatsust nõudvates sihtrühmades[164], milleks KII ettevõtted küberjulgeoleku-alases valdkonnas on. Allolevalt jooniselt 4 on võimalik näha metodoloogiline protsessiskeem, kuidas ja mille alusel ekspertintervjuude analüüs läbi viidi.



Joonis 4. Poolstruktureeritud ekspertintervjuude analüüsi protsessiskeem. Allikas: autori koostatud.

Energiaettevõtetest nõustusid uuringus osalema viie erineva ettevõtte eksperdid, kes on küberjulgeoleku valdkonnaga seotud ning oluliste küsimustega igapäevaselt kursis. Vastust ei saadud korduval pöördumisel kahest ettevõttest. Eitavalt vastati kokku viiel korral. Põhjendused uuringus mitte osalemiseks lähtusid pigem sellest, et küberjulgeoleku valdkond on nende ettevõttele võõras või ei puututa nende arvates

[164] TNS Emor. Kvalitatiivsed uuringutehnikad http://www.emor.ee/kvalitatiivuuringud/] 06.05.2015

küberjulgeolekuga igapäevaselt kokku. Telekommunikatsiooni ettevõtetest nõustus uuringus osalema kahest erinevast ettevõttest kaks eksperti, kes igapäevaselt suuremal või vähemal määral seotud küberjulgeoleku valdkonnaga. Vastust ei saadud korduval pöördumisel kuuelt eksperdilt. Kahel juhul vastati eitavalt, kus põhjenduseks toodi, et enam ei tegutseta telekommunikatsiooni valdkonnas või napib uurimuses osalemiseks aega ja muud kohustused koos põhitööga vajavad tegemist.

Eraldi tasub välja tuua põhjenduse uuringus mitte osalemise kohta, kus vastati, et ettevõte ei ole KII ettevõte. Siinkohal tekkis küsimus, kuidas ettevõte, kes küberjulgeoleku strateegia ja hädaolukorra seaduse alusel liigitub KII ettevõtteks, seda ettevõtte eksperdi väidete kohaselt siiski pole. Autori arvates näitab see, et küberjulgeolekusse ei suhtuta piisava tõsidusega ning ei tunnetata või ei taheta võtta vastutust KII ettevõttena lisakohustuste täitmise osas. Samas tuleb rõhutada, et kuigi loobuti erinevatel põhjustel uuringus osalemast, siis soovitati uurimusse kaasamiseks teiste konkureerivate ettevõtete kontakte, kellelt võib vajalikku informatsiooni saada ning kelle poole küsimustega pöörduda. Autori arvates näitab see, et ettevõtted tunnevad teiste samas sektoris tegutsevate ettevõtete kontakte, kellelt vajadusel ettevõtted omavahelises suhtluses küberjulgeoleku-alast informatsiooni vahetada saaks.

Mõlema valdkonna peale kokku viidi läbi seega seitse poolstruktureeritud ekspertintervjuud. Intervjuu küsimuste koostamisel võeti osaliselt aluseks Suurbritannia valitsuse läbi viidud uurimuse küsimusi[165], kus uuriti ettevõtete teadmisi ja valmisolekut küberrünnakute eest kaitsmisel. Poolstruktureeritud intervjuu küsimused, millele ettevõtete eksperdid vastasid on ära toodud lisas 3. Küsimused olid esitatud kolmes osas, kus esimeses osas keskenduti juhatuse tegevustele ning strateegiale, teises osas uuriti koostöövõimalusi nii avaliku ja erasektori vahel (kui ka erasektori ettevõtete vahel) ning kolmandas osas pöörati tähelepanu küberohtudele ja –riskidele.

Intervjuu esimeses osas küsiti üldisemaid küsimusi juhatuse strateegiate ning tegevuste kohta küberjulgeoleku valdkonnas. Kõigi intervjueeritud ettevõtete eksperdid väitsid, et puutuvad igapäevaselt küberjulgeolekuga kokku ning küberjulgeolekul on oluline ja strateegiline roll ettevõtetes. Rõhutati, et küberjulgeoleku tähtsus väljendub selles, et

[165] HM Government. FTSE 350 Cyber Governance Health Check

kõik ettevõtte põhitegevused on seotud IT-süsteemidega ja teatud ettevõtetes on valdkond allutatud otsese juhi pädevusalasse.

Antud töö raames üheks olulisemaks küsimuseks oli, kas ettevõtetel eksisteerib ettevõttesisene tegevuskava või strateegia kübervaldkonna reguleerimiseks. Kahe energiaettevõtte puhul täheldati, et lähtutakse igapäevaselt seadusest tulenevast regulatsioonist, mis keskendub elutähtsa teenuse infosüsteemidele ja infovarade turvameetmetele[166]. Üks energiaettevõte lähtub infosüsteemide kasutamise korrast, kus on hõlmatud küberturvalisuse poliitikad ja töötajatele küberkäitumise juhised. Konkreetset strateegiat pole üheski intervjueeritud energiaettevõttes, kuid on tegevuskavad ja -juhised, mis katavad erinevate süsteemide IT struktuure, kirjeldusi. Lisaks selgus ühe energiaettevõtte intervjuust, et neil on kübervaldkonna reguleerimiseks koostööpartner ning ühes energiaettevõttes toodi välja, et luuakse turvaspetsialisti ametikoht, kes otseselt ja terviklikult tegeleks küber-füüsiliste turvariskide haldamisega. Telekommunikatsiooni ettevõtete intervjuudest selgus, et juhindutakse ISKE[167] nõuetest ja kübervaldkonda eraldiseisvana ei vaadelda. Kui peaks toimuma küberrünnak või esinema muudest asjaoludest tingitud oht KII ettevõttele, lähtutakse välja töötatud tegevusjuhistest. Jälgitakse nii proaktiivselt kui ka operatiivselt IT-turvalisusnõuete täitmist. Intsidentide puhuks on välja töötatud stsenaariumid, mis hõlmavad kogu intsidendi haldusprotsessi, alustades küberrünnaku registreerimisest, lokaliseerimisest, vastutusaladest ning lõpetades kriisikomisjoni tegevustega.

Autori arvates näitavad need vastused teatud ettevõtete puhul, et osatakse näha küberjulgeoleku riske ning tahab panustada KII kaitsesse. Ollakse teadlikud ning töötatakse selles suunas, et KII oleks paremini kaitstud. Suuremal või vähemal määral on ettevõtted vähemalt tegevusjuhiste kaudu kübervaldkonda ettevõttes reguleerinud. PricewaterhouseCoopers (edaspidi: PwC) uuringust selgus, et 1/3 maailma ettevõtetest puudub selge ning läbimõeldud strateegia küberrünnakutega toimetulemiseks[168]. Samas nagu ka käesoleva töö esimesest osast selgus, siis selleks, et olla kaitstud

[166] Peetakse silmas Vabariigi Valitsuse määrust nr 43: Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed.
[167] ISKE on kolmeastmeline turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks. [https://www.ria.ee/iske-kkk/#Mis_on_iske] 21.03.2015
[168] PricewaterhouseCoopers. The Global State of Information Security® Survey 2015. 30.09.2014 Managing cyber risks in an interconnected world. p.28

küberrünnakute eest, tuleb ettevõtetel läbi mõelda riskijuhtimine ning –analüüs ja panustada küberjulgeoleku strateegia välja töötamisse, milleks on CCD COE välja töötatud juhised heaks aluseks.

Küsimusele, kui tihti arutatakse ettevõttes strateegilisi riske ning kas küberohud kuuluvad ettevõtte strateegiliste riskide hulka, vastati erinevalt. Neljast energiaettevõttest kolmes arutatakse strateegilise riske kord aastas ning küberohte hinnatakse põhjalikumalt vastavalt vajadusele. Sama võib väita telekommunikatsiooni ettevõtete kohta. Ühe energiaettevõtte puhul selgus, et küberohud on kas igapäevaselt või vähemalt kord nädalas aruteluteemaks. Ühe energiaettevõtte puhul ei käsitleta küberohtusid laiemas tähenduses, vähemalt mitte strateegiliste riskide hindamisel. Autori arvates selgub ülaloleva küsimuse põhjalt, et küberohtudega kokkupuude ning tegelemine on KII ettevõtete lõikes väga erinev ning kübervaldkonda tähtsustatakse erinevalt, mis seab riigi keerulisse seisu, kui tahetakse liikuda KII ettevõtete küberjulgeoleku alase taseme ühtlustamise suunas. Riik on KII ettevõtete teadmatusest tingituna haavatavam. Siinkohal soovitaks autor riigil välja selgitada ettevõtted, kes vajaksid rohkem küberteadlikkuse tõstmist ning aitaks neil kogenumatele ettevõtetele järele jõuda.

Võrreldes teiste strateegiliste riskidega väideti, et küberriskid on uued ja raske on teha järeldusi nende olulisuse kohta. Laiemas plaanis peeti nii energia kui ka telekommunikatsiooni ettevõtetes küberriske siiski väga olulisteks ning rõhutati, et küberohtudega tuleb tegeleda esmatasandil. Küberrünnaku ohvriks oli langenud viiest energiaettevõttest kaks, kus rünnaku sisuks oli e-posti spämmimine, IP-aadresside *pingimine*, rünnakud tulemüürile ning oli proovitud siseneda ettevõtte andmebaasidesse. Autori arvates näitab see, et rünnakud on Eestis levinud, kuid antud väidet tuleks edaspidiste uuringutega täpsemalt kontrollida, kaasates valimisse rohkem erinevate valdkondade KII ettevõtteid. Kui autor küsis intervjueeritavatelt täpsemalt ettevõtte küberohtude ning võimalike tagajärgede kohta, siis peamisteks ohtudeks energiaettevõtetes peetakse järgnevaid ohte ning neist tulenevaid tagajärgi:

1) elektrivõrgu juhtimissüsteem või kaitsesüsteem ei tööta või on pahatahtliku mõju all;
2) DDoS rünnak infosüsteemi iseteenindusele;

3) rünnak iseteenindust haldava teenusepakkuja pihta, halvates iseteeninduse töö;
4) infosüsteemi häkkimise käigus andmete kahjustamine või vargus;
5) teenusepakkuja süsteemidesse häkkimise käigus *backup*-i vargus;
6) *social engineering* võtete abil isikuandmete vargus;
7) ettevõte kaotab rünnaku korral andmebaasi;
8) infosüsteemide häirimise korral rahaline kahju;
9) kaugjuhtimise teel meelevaldselt alajaama lülituste korraldamine/ elektriarvestite töö halvamine.

Telekommunikatsiooni ettevõtetes peetakse peamisteks küberohtudeks sidekatkestusi, elektrikatkestusi ning pahavara levikut. Ühe telekommunikatsiooni ettevõtte ekspert väitis, et suuremaid küberrünnakuid toimunud pole, sest tegeletakse järjepidevalt küberturvalisuse tagamisega ning on suudetud rakendada piisaval määral ennetavaid meetmeid küberrünnakute vältimiseks. Teise telekommunikatsiooni ettevõtte ekspert tõdes siiski, et DDoS rünnakuid on paar tükki aasta jooksul siiski esinenud. Kui ettevõtet oli varem tabanud või on tõenäosus, et tabab tulevikus küberrünnak, siis esmaste tegevustena toodi välja vajalike osapoolte teavitamine, serverite blokeerimine, ajutiselt töö katkestamine, tulemüüri vastupidavust uurida, selgitada välja rünnaku päritolu. Olenevalt rünnaku liigist käivitub intsidendi lahendamise protsess, kus teatud juhtudel tuleks infosüsteem ajutiselt internetist lahti ühendada ning infosüsteemide töö peatada.

Võrreldes energia ja telekommunikatsiooni ettevõtete vastuseid, siis küberohud KII ettevõtetele ühtivad. Lähtudes töö esimeses osas Euroopa Komisjoni poolt välja toodud küberrünnakute liigitusest, siis olgu rünnakust tingitud ajutine süsteemi katkestus või igapäevase töö häirimine, kahju on ettevõttele tekitatud. Autori hinnangul on ettevõtted küberohtudest teadlikud ning esmased tegevused küberrünnakutega toime tulemiseks tegevusjuhiste põhjal reguleeritud. Võrdluseks Eesti KII ettevõtetega, viis maailma suurima täiustatud turvalahenduste eraarendajana on Kaspersky Lab 2013. aastal läbi ülemaailmse uuringu kaardistamaks globaalsete korporatsioonide IT-riskid. Uuringus osalenud suurkorporatsioonide ja keskmiste/väikeettevõtete omanikud, kes igapäevaselt puutuvad kokku küberrünnakutega, vastasid milliste peamiste küberohtudega silmitsi seistakse. Uuringu tulemusel liigitatakse välised küberohud järgmiselt: viirused, ussid,

nuhkvara ja muud pahavara programmid (66%); rämpspost (61%); *phishing* rünnakud (36%); võrku sissetungimine/häkkerlus (24%); teenusetõkestusrünnakud DoS (*Denial of Service*) ja robotvõrkudega hajutatud teenuse tõkestuse rünnakud DDoS (*Distributed Denial of Service*) (19%); konkreetsele ettevõttele suunatud rünnakud (9%)[169]. Tuues näiteid EL-st, siis PwC uuringust[170] selgus, et Suurbritannia ettevõtetest 69% sattusid 2013. aastal küberrünnaku alla, kogu maailmas jääb rünnakute protsent 59% juurde[171]näidates, et Suurbritannias on võrreldes maailmaga rünnakute arv suurenenud. EL-is tuvastati 2013. aasta suhtes 41% küberrünnakute arvu kasv. Olukorra tõsidust aitab hinnata ka 2014. aasta märtsis CCD COE tabanud küberrünnak[172], mis näitab, kuivõrd sellisel tasemel asutus pole küberrünnaku eest kaitstud.

Järgnevalt küsiti kui suur osa ettevõtte investeeringutest suunatakse küberjulgeoleku valdkonda, eesmärgiga selgitada välja, kui palju ettevõtted investeerivad KII kaitse tagamisse. Kaks energiaettevõtet väitsid, et eraldi küberkaitsesse ei investeerita, aga olles elutähtsa teenuse osutajad, siis investeeringuid tehnoloogia arendamisse või IT valdkonda saab kaudselt lugeda investeeringuteks küberjulgeolekusse. Kolme energiaettevõtte puhul toodi eraldi välja, et investeeritakse vastavalt 1-2%, 5% või 0,1% ettevõtte eelarvest. Telekommunikatsiooni ettevõtete eksperdid väitsid, et eraldi eelarvet küberjulgeoleku valdkonnas pole, kuid investeeringuid tehakse IT-turvalisusse, mis on otseselt seotud kübervaldkonnaga. Kui protsendid tunduvad esmapilgul väikesed, siis suurte infrastruktuuri investeeringutega ettevõtete silmis on absoluutsumma siiski oluline. Autori arvates pole investeeringud IT-valdkonna arendamisesse otseselt seotud küberkaitse suurendamisega, sest see, kui ostetakse juurde uus terminal või nutitelefon, siis võivad küberriskid KII ettevõttele hoopis suureneda. Peale selle tasub rõhutada, et suurendades investeeringuid küberjulgeolekkuse, võidakse ära hoida suuremad kahjud, mis kaasnevad küberrünnaku kahjude likvideerimise käigus. Näiteks kulus ühel Itaalia

[169] Kaspersky Lab (2013) p. 8
[170] PricewaterhouseCoopers. The Global State of Information Security® Survey 2015. [http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml] 27.11.2014
[171] Ashford, W. UK falling behind in cyber intrusion detection, study shows. (2014)
[172] Postimees. NATO võrguleheküljed langesid küberrünnaku alla. 16.03.2014 [http://www.postimees.ee/2729272/nato-vorgulehekuljed-langesid-kuberrunnaku-alla] 05.05.2015

ettevõttel häkkimisest tulenevalt tekitatud küberrünnaku tagajärjel kahjusummaks 875 mln $, kahjude likvideerimise kulud ulatusid aga 8,5 mld $ suuruseks[173].

Esimese ploki viimase küsimusena küsiti, kas ettevõttes on olnud viimase aasta jooksul küberjulgeoleku-alaseid koolitusi töötajatele ning kas koolituste järgi on ekspertide hinnangul vajadust. Kõikide ettevõtete arvates küberjulgeoleku alased koolitused on vajalikud, sest tehnoloogia arenguga kasvavad järjest küberturbe alased riskid. Energiaettevõtetest kolmes on viimase aasta jooksul koolitusi toimunud. Vastavalt koolitustena või kübervaldkonnast ülevaate andmise vormis. Kahe energia ettevõtte puhul koolitusi toimunud pole. Siinkohal märgiks autor ära, et EL tasandil poldud koolitustel, töögruppides osaletud. Vaid üks energiaettevõtetest on spetsialistide tasemel olnud kaasatud EL tasandil küberõppuste stsenaariumite koostamisel ja osalenud Hollandis parima praktika vahetamise projektis. Telekommunikatsiooni ettevõtetest ühes on osaletud viimase aasta jooksul CERT üritustel ning kaasatud poliitika kujundamisse. Autori arvates tuleks KII ettevõtetele võimaldada rohkem koolitusi, sest kübervaldkond on pidevas muutumises ja elutähtsa teenuse eest vastutaja võiks kursis olla viimaste arengutega küberjulgeoleku valdkonnas.

Intervjuu teises osas keskenduti erinevatele koostöövormidele. Seoses avaliku sektoriga küsiti, kas riik peaks rohkem valdkonda sekkuma või aitama erasektorit küberjulgeoleku valdkonnas. Ehk lähtudes Kopenhaageni koolkonna põhiväidetest, kas riik peaks KII ettevõtteid referentobjektina rohkem erinevate seaduste alusel reguleerima ning küberjulgeoleku valdkonda rohkem politiseerima. Viiest energiaettevõttest kolm leidsid, et riik peaks rohkem erasektorit aitama. Leiti, et riik peaks pakkuma omapoolset kompetentsi, tuge ja juurdepääsu küberturbega tegelevate isikute võrgustikule. Lisati, et riik võiks võtta rolli teadlikkuse tõstmisel, teavitades ettevõtteid võimalikest küberriskidest läbi koolituste või infopäevade. Seega saab vastustest järeldada, et riik peaks kaasama koolitustele rohkem asjassepuutuvaid ettevõtteid. Täiendati, et küberjulgeolek on üksikutes ettevõtetes tihti kitsas teema, kus riigi tugi aitab ettevõttel paremini oma majasiseste ressurssidega reaalseid tulemusi saavutada. Üks energiaettevõte tõi eraldi välja, et riik peaks sekkuma riigi tasandil ehk hoiatama ettevõtteid teiste riikide küberrünnakute eest ning jagama ettevõtetega ohuhinnanguid.

[173] Rimo, T. Walsh, M. McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies. 09.06.2014 [http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx] 27.11.2014

Telekommunikatsiooni ettevõtete ekspertide arvamused olid vastandlikud. Ühe ettevõtte ekspert leidis, et puudub otsene vajadus riigi sekkumiseks. Samas rõhutas teine ekspert vastupidiselt, et RIA ja CERT võiksid lisaks erasektorile nõuete koostamisele, panustada ka küberturbesse tehnoloogiliselt. Antud vastustega seoses jäi autorile ekspertide vastustest mulje, et seni riik ettevõtteid väga kaasanud pole ning teavitustöö ettevõtete seas on olnud kas valikuline või puudulik. Samas ühe energiaettevõtte ekspert tõi välja, et RIA on korraldanud infoturbe alaseid koolitusi, andes juhtnööre küberturvalisuse parandamiseks.

Avaliku sektori puudusena toodi välja, et takistuseks on vahel avaliku sektori killustatus. Telekommunikatsiooni ekspert rõhutas, et riik võiks rohkem vaadata suuremat pilti ja arvestada KII ettevõtete eripäradega. Näitena toodi välja, et määrates elektrienergia müügiga tegelevatele ettevõtetele nende infrastruktuuri taasteajaks suurema ajaperioodi kui näiteks telekommunikatsiooni ettevõtetele, kelle teenuse üheks peamiseks komponendiks on elektrienergia, siis seda ei saa pidada riigipoolseks terviklikuks lähenemiseks. Vastusest jäi kõlama, et riik reguleerib KII valdkonda ühtselt, kuigi tuleks arvestada ettevõtete tegevusvaldkonnast tulenevate eripäradega. Koostööst teiste sama valdkonna või erasektori ettevõtetega vastati nii energia kui ka telekomi ettevõtetest, et juhatus motiveerib töötajaid vahetama parimat praktikat teiste erinevate ettevõtetega, kas siis oma ala professionaalidega või tarkvara arendajatega.

Järgnevalt küsiti, kas ollakse kursis EL ja Eesti küberjulgeoleku strateegiatega. Viiest energiaettevõttest kolm polnud kursis kummagi küberjulgeoleku strateegiaga. Autori arvates näitab see, et ettevõtjad pole teadlikud riigis toimuvast (rääkimata EL tasandist), kuigi ollakse KII ettevõtted. Vastustest selgus, et riik pole ettevõtete sõnul küberjulgeoleku strateegia olemasolust KII ettevõtteid teavitanud. Autori arvates pole riigi kohustus kõiki KII ettevõtteid uutest regulatsioonidest eraldi teavitada. Kaks energiaettevõtet siiski olid teadlikud Eesti küberjulgeoleku strateegiast ning üks neist on kaasatud uue küberjulgeoleku strateegia väljatöötamise protsessi. Lisaks oldi EL tasandil läbi ENISA koolituste ja töögrupis osalemiste EL küberjulgeoleku strateegiaga kokku puututud. Telekommunikatsiooni ettevõtetest mõlemad olid kursis nii Eesti kui ka EL küberjulgeoleku strateegiaga.

Alapeatüki kokkuvõtteks võib öelda, et eksperdid olid vastutulelikud ja jagasid meelsasti ettevõtte kogemusi ja praktikat siiski delikaatsel teemal. Autor leiab, et energiaettevõtete vastuste põhjal annab energeetika valdkonna kohta järeldusi teha, kuid telekommunikatsiooni ettevõtete vastuste vähesuse tõttu antud töö raames tehtavaid järeldusi kogu telekommunikatsiooni sektorile laiendada ei saa. Telekommunikatsiooni ettevõtete osas teeb autor ettepaneku järgnevates uurimustöödes uurida ankeetküsitluse põhjal (saamaks representatiivsema tulemuse), kas järeldused vastavad tõele või mitte. Järgmises alapeatükis koondatakse aga ekspertintervjuude ning dokumentide analüüsist ilmnenud olulisemad punktid ning tehakse autoripoolsed järeldused ja ettepanekud.

2.3 Järeldused ning ettepanekud

Eelmise alapeatüki põhjal saab väita, et ettepanekuid ja soovitusi kvaliteetsema ja siduvama küberjulgeoleku tagamiseks on mitmeid, sest küberjulgeoleku valdkond on Kopenhaageni koolkonna teoreetikute sõnul üks julgeoleku liikidest, mis puudutab otseselt ühiskonda ning kriitiliselt poliitilist süsteemi, vajades riigipoolset sekkumist. KII ekspertide intervjuudest selgusid mitmed kitsaskohad, mida antud alapeatükis koondatakse ning eelnevalt välja toodud puudustele, pakutakse käesoleva töö autorilt välja võimalikud lahendused. Peale selle tuuakse välja järeldused nii EL kui ka Eesti küberjulgeoleku strateegiate analüüsi osas ning üldisemad ettepanekud avaliku sektori ning erasektori koostöö paremaks toimimiseks.

Poolstruktureeritud ekspertintervjuudest selgus, et küberohtudega tegelemine, neile tähelepanu pööramine ning arvestamine, on KII ettevõtete lõikes väga erinev ning kübervaldkonda tähtsustatakse erinevalt. On ettevõtteid, kus kaardistatakse küberohte igapäevaselt või kord nädalas. Teisalt valitses trend, kus riske hinnati kord aastas, mis küberjulgeoleku mõistes ei ole autori arvates piisav. Riskid on pidevas muutumises ning aastatagused küberohud ei pruugi enam teatud ajaperioodi möödudes aktuaalsed olla. Suured ettevõtete vahelised erinevused võivad tuleneda sellest, et ettevõtete suurus ja tegutsemise aeg on erinev. Suuremad ja pikaajalisema ettevõtlusajalooga ettevõtted orienteeruvad erinevates teemavaldkondades paremini, kui alles alustavad või väikeettevõtted, kellel pole nii palju kogemusi erinevate valdkondadega toime tulemiseks.

Esimese ettepanekuna soovitaks autor KII ettevõtete siseselt kübervaldkonnaga kokkupuutuvatel isikutel (tehnoloogiajuhid, infoturbejuhid jt) vähemalt kord poolaastas kokku saada ning arutleda küberjulgeoleku viimaste trendide temaatikal. Tõenäoliselt peaks siinkohal abiks olema RIA, kes avaliku sektori esindajana võiks KII ettevõtetele saata uudiskirjana poolaasta kokkuvõtte aktuaalsematest küberrünnakutest. Seeläbi on ettevõtetel kergem küberjulgeoleku valdkonnas orienteeruda ning vajadusel saavad KII ettevõtted riske ümber hinnata või ettevõttesiseseid tegevusplaane muuta, misläbi paraneks KII ettevõtete kaitse ja valmisolek uuteks võimalikeks küberrünnakuteks.

Teiseks ilmnes, et küberrünnakute ohvriks langes 2013. aastal energiaettevõtetest kaks ning telekommunikatsiooni ettevõtetest üks ettevõtte, mis tähendab, et seitsmest ettevõttest ligi pooled puutusid 2013. aastal kokku otseselt KII-le suunatud küberrünnakutega. Kuigi valimisse kaasatud ekspertide arv antud töö puhul oli väike saab siiski järeldada, et küberünnakud KII ettevõtetes on levinud. Siinkohal soovitaks autor edasistes uurimustes kontrollida järelduse autentsust, kaasates rohkem erinevate valdkondade KII ettevõtteid ning eksperte, et saavutada ülevaatlikumat pilti erinevatest sektoritest ning KII ettevõtetes toimunud küberrünnakutest, selgitades välja, kui haavatav Eesti riik on.

Kolmandaks selgus, et KII ettevõtted ei investeeri eraldi küberkaitsesse, vaid investeeritakse tehnoloogia arendamisse või IT-valdkonda, mida kaudselt saab KII ettevõtete arvates pidada investeeringuteks küberkaitsesse. Siinkohal tuleb autori arvates väga kindlalt teha vahet, küberkaitse ja IT-valdkonna arendamisel. Küberkaitse korral kaitstakse näiteks konkreetselt servereid tulemüüridega, piiratakse kasutajaõiguseid (blokeeritakse tavakasutajate ligipääse nt sotsiaalvõrgustikele), tarkvaradele paigaldatakse antiviirused, korraldatakse küberjulgeoleku-alaseid koolitusi töötajatele. IT-valdkonna arendamine võib puudutada vaid üht eelpool nimetatut instrumenti. Seega on autori arvates otseste küberkaitsealaste investeeringute puudumine kitsaskohaks KII ettevõtete kaitse tagamisel ning mõjutab otseselt riigi haavatavust olles reaalseks riskiks sisejulgeolekule. Autor leiab, et KII ettevõtted peaksid endale kitsamas perspektiivis lahti mõtestama ettevõtte rolli küberjulgeolekus ning laiemalt riigi julgeolekus. Seeläbi jõudma teadmiseni, et tänased investeeringud küberkaitsesse, hoiavad ära homsed küberrünnakute taastumisest tingitud lisakulud.

Neljandaks ilmnes, et üks ekspert seitsmest on osalenud EL tasandil küberõppuste stsenaariumite koostamisel ning Hollandis parima praktika vahetamise projektis. Kuna EL ja Eesti küberjulgeoleku strateegiate analüüsist selgus, et nähakse ette ja soositakse rahvusvahelisel tasandil koostöö toimimist, siis antud töö raames selgus ekspertintervjuudest, et rahvusvaheline koostöö energeetika ning telekommunikatsiooni valdkonnas pole piisav ning teadlikkus EL tasandil toimuvatest õppustest ning koolitustest on vähene. Kuigi teatud KII ettevõtetel esineb piiriülene suhtlus (nt emaettevõttega teises liikmesriigis), soovitaks autor avalikul sektoril, kellel tõenäoliselt on tihedam suhtlus EL-iga, teavitada KII ettevõtteid võimalikest õppustest, konverentsidest ja parima praktika vahetamise projektidest. Intervjuudest selgus, et seni pole info teatud osale KII ettevõtetest jõudnud, kuigi huvi EL tasandil toimuva kohta eksisteerib.

Viienda järeldusena selgus, et esineb vajadus siseriiklike koolituste järgi ning küberjulgeoleku alase teadlikkuse tase on ettevõtete lõikes väga erinev. Teatud ettevõtted on küberjulgeolekuga seotud teemadest teadlikud kuni EL tasandini välja, samas kui teised KII ettevõtted pole teadlikud Eestis kehtivast küberjulgeoleku strateegiast. Seega soovitab autor avalikul sektoril koolitada KII ettevõtete lõikes eksperte ning asjapuutuvaid isikuid, kes omakorda saavad vajadusel ettevõttesiseselt töötajaid koolitada. Viimase järeldusena tuuakse välja KII ettevõtete mure avaliku sektori killustatuse osas ning selles, et riik võiks rohkem arvestada KII ettevõtete eripäradega. Avaliku sektori killustatus on tekitanud KII ettevõtetes olukordi, kus ei teata, kelle poole peaks küberjulgeoleku alastes küsimustes pöörduma. KII ettevõtetel puudub arusaam sellest, kes ja millise valdkonna eest avalikus sektoris vastutab. Rõhutati, et riik ei näe terviklikku pilti ning ei arvesta KII ettevõtete eripäradega. Osadel KII ettevõtetel on küberrünnakust taastumise periood pikem kui teistel nt energeetika vs telekommunikatsiooni ettevõtted. Riik pole arvestanud, et telekommunikatsiooni ettevõtetel kulub selle võrra rohkem aega, kui elektrienergia on ajutiselt häiritud. KII ettevõtete ekspertide sõnul pole riik sellega arvestanud ning küberrünnakutest taastumisajad ei vasta tegelikule olukorrale.

Autor soovitab erasektori ning avaliku sektori koostöös välja selgitada kõigi KII ettevõtete eripärad ning juhtiva rolli soovitaks autor võtta KII ettevõtetel. Erasektori

esindajad tõid välja avaliku sektori puudused ning võimalikud kitsaskohad, seega edaspidi võiks erasektor puudustele rohkem tähelepanu pöörata. KII ettevõtted võiksid riigile edastada omapoolsed nägemused sellest, kuidas antud juhul küberrünnakutest taastumisaegasid arvestama peaks, tuues välja ettevõtte põhise stsenaariumi küberrünnakutest toibumisel ja tooma välja ajakulu, siis saab avalik sektor edaspidi ettevõtete välja toodud näitajatega arvestada. Laiemas plaanis tuleks avaliku sektori ja erasektori koostöös panna paika rollide jaotus ning jagada ära vastutusvaldkonnad, kes, millal ja kuidas küberjulgeoleku-alastes küsimustes vastutab. Allolevas tabelis 5 on koondatud peamised küberjulgeoleku-alased probleemid ning võimalikud autori poolt pakutavad lahendused.

Tabel 5. Peamised küberjulgeoleku-alased probleemid autoripoolsete lahendustega

Probleem	Lahendus
Küberohtudega tegelemise tase ettevõtete lõikes väga erinev – riigi haavatavus küberjulgeolekus suur	Ettevõtete siseselt teatud ajaperioodi tagant koguneda ning viimaseid trende küberjulgeolekus arutada. Koostöös RIA-ga.
Küberkaitsesse suunatud investeeringute puudumine	KII ettevõtted rohkem teadvustama oma olulisust riigi julgeolekus ning suunama otseselt investeeringuid küberkaitsesse
Küberjulgeoleku kui valdkonna teadlikkuse madal tase	Selgitada välja, kas suur vs väikeettevõtted on võrdselt teadvustatud ning suunata neile ettevõtetele, kes infopuuduses, riigipoolsed küberjulgeoleku-alased programmid
EL tasandil koolituste, parima praktika vahetamise võimaluste mitte-teadlikkus KII ettevõtetes	Riik teavitada ja suunata KII ettevõtteid küberjulgeoleku alastest võimalustest EL tasandil
Rollide jaotus KII ettevõtetele arusaamatu, avaliku sektori killustatus	Avaliku sektori ja erasektori koostöös panna paika küberjulgeoleku alane rollide jaotus ning vastutusvaldkonnad

Allikas: autori koostatud.

Üldisemas plaanis jäi nii teoreetilistes käsitlustes, strateegiate analüüsis kui ekspertintervjuude läbi viimisel tähtsaima märksõnana kõlama koostöö. Tagamaks küberjulgeolekus KII ettevõtete kvaliteetne kaitse, tuleb avalikul sektoril ja erasektoril tihedalt koostööd teha. Teatud perioodi tagant planeerida kokkusaamisi ja vahetada infot probleemide, kitsaskohtade kohta. Lisaks peaks toimuma erasektori ja avaliku sektori esindajate kohtumistel ajurünnakud teemal, kuidas saaks koostööd küberjulgeoleku-alastes teemades paremini tööle rakendada. Ei avalik sektor ega

erasektor ei suuda üksi end küberrünnakute eest kaitsta, selleks on tarvis teha koostööd. Esialgu siseriiklikul tasandil ja seejärel liikmesriikide tasandil EL-is.

Autor soovitab siinkohal avalikul sektoril korraldada KII ettevõtetele erinevate küberjulgeoleku teemade lõikes koolitusi ning infopäevi. Näiteks infopäevi levinumatest KII küberrünnakutest Eestis võrreldes EL-iga ning infopäevadele tuleks kaasata kõik KII ettevõtted sh suured ja väikesed. Koostööd saaks tõhustada tihedama suhtluse abil. Näiteks võiks RIA, kes on autori arvates võtnud Eestis hetkel juhtiva rolli küberturbe teemades, edastada kord kuus KII ettevõtetele uudiskirja näol infot viimase aja trendidest küberrünnakutes ja küberohtudes. Miks autor niivõrd pöörab tähelepanu just küberrünnakute alastele koolitustele ja teadlikkuse tõstmisele seisneb selles, et ettevõtted võiks ja peaks olemas kursis viimaste aktuaalsete arengutega. Sellisel juhul saavad ettevõtted muuta oma tegevusi või pöörata tähelepanu IT-valdkonnas sinna, kus seda hetkel kõige rohkem teha oleks vaja. Rahvusvahelise koostöös, mida soosivad nii Eesti küberjulgeoleku strateegia kui ka EL strateegia, soovitaks KII ettevõtetele edastada informatsiooni, kuidas ja kes on oodatud töögruppides või küberõppustel osalema ja selgitataks, miks nendes osalemine oluline on. Kindlasti annaks EL tasandil õppustel osalemine siseriiklikul tasandil teadlikkust juurde ning ettevõttes osatakse pöörata tähelepanu valdkondadele, mis esialgu ei tundu tähtsad. Lisaks aitab parima praktika vahetus vähendada riski riigi sisejulgeolekule.

Töö eesmärgist lähtuvalt aitasid mitmed juba eelpool nimetatud järeldused tõestada väidet, et KII ettevõtete strateegiad pole kooskõlas riigi strateegiaga. Ekspertintervjuude tulemusena puudub ettevõtetel kõikehõlmav lähenemine või strateegia küberohtude eest kaitsmisel. Kõikides KII ettevõtetes pole piisavaid või ajakohastatud tegevusjuhiseid küberrünnakutega toime tulemiseks ehk KII kaitseks. Juhtkonnad, kas ei käsitle regulaarselt küberjulgeoleku küsimusi, misläbi ei teadvustata reaalselt ohte süsteemidele. Seega lähtudes Kopenhaageni koolkonna väitest, selleks, et valdkonnas paraneks teadlikkus ning küberjulgeolekut võetaks KII tõsisemalt, tuleb teemavaldkonda politiseerida ning rohkem avalikkuse tähelepanu kätte tuua. Kui riik võtab juhtiva rolli ning aitab välja tuua küberohtude tõsiduse ning nende mõju riigi julgeolekule ning suveräänsusele, siis suudavad KII ettevõtted ehk ka paremini enda kaitse tagada.

KOKKUVÕTE

Tragöödia olemus on see, et maailm pole meeldiv väike pesa, mis on tehtud meie kaitsmiseks, vaid tohutu ja suuresti vaenulik keskkond, kus võime saavutada suuri asju ainult jumalaid trotsides ja see trots toob vältimatult kaasa karistuse.[174] Küberjulgeolek Kopenhaageni koolkonna teoreetikute väitel on uus valdkond, mille reguleerimisega ning julgeolekustamisega seotud otsuseid tuleb vastu võtta riigil, sest julgeolek lähtub põhimõttest, kus pidevalt tuleb tähelepanu pöörata osapoolte turvalisuse tagamisele.[175] KII, kui referentobjektide ja eluliselt tähtsate teenuste eest vastutavate ettevõtete kaitsmine küberrünnakute eest, peab olema riigi üks olulisematest prioriteetidest, kuna see määrab ära riigi haavatavuse. 2013. aastast on küberrünnakute maht suurenenud ning meedia vahendusel on ühiskonnaliikmeteni jõudmas teadmine küberrünnakute tihedast seotusest igapäevaeluga. 2014. aasta märtsis tabas CCD COE küberrünnak näidates kuivõrd sellisel tasemel asutus pole küberrünnakute eest kaitstud, peaksid kõik seaduse alusel elutähtsaks valdkonnaks liigitatud KII ettevõtted tõsiselt mõtlema küberkaitse võimekuse suurendamisele.

Käesoleva töö eesmärgiks oli EL küberjulgeoleku strateegiast lähtuvalt võrrelda KII ettevõtete ja Eesti riigi küberjulgeoleku strateegiat küberrünnakute eest kaitsmisel. Konkreetsemalt rõhutas autor, et Eesti riigi ja KII ettevõtete strateegia küberrünnakute eest kaitsmisel pole omavahel kooskõlas. KII ettevõtetele keskenduti antud töös seepärast, et tegemist on elutähtsat teenust pakkuvate ettevõtetega ning KII kaitse on nii EL küberjulgeoleku kui ka Eesti küberjulgeoleku strateegiast lähtuvalt oluline. Töö eesmärgist lähtuvalt püstitati neli uurimisküsimust, kus esmalt selgitati klassikalise julgeoleku kompleksi teooriast ning Kopenhaageni koolkonna autorite põhiteesidest lähtuvalt, kuidas on arenenud julgeoleku kontseptsioon ning millal sai alguse küberjulgeoleku kui julgeoleku valdkonna kujunemine. Julgeolekut on defineeritud nii

[174] Wiesner, N. The Human Use of Human Beings: Cybernetics and Society. 1950. p.184
[175] Buzan, B., Hansen, L. (2010) p. 10-11

rahvusvaheliste suhete allteooriate raames kui ka Kopenhaageni koolkonna teoreetikute käsitlustes, olles valdkonnaks, mille defineerimisel tuleb arvestada, kes on julgeolekustamise osapoolteks ning kui suures ulatuses valdkonda on tarvis politiseerida. Mõistmaks küberrünnakute tõsidust ning võimalikke ohte, tuleb küberjulgeoleku valdkonda Kopenhaageni teoreetikute väitel rohkem politiseerida ning valdkonda läbi erinevate debattide või kõneaktide tähtsustada, rõhutades kui oluline antud valdkonna haavatavus on riigi sisejulgeoleku tagamisel.

Riigi rolli ning olulisust aitavad tõestada siseriiklikud regulatsioonid küberjulgeoleku valdkonnas. Nii Eesti kui ka EL tasandil on välja töötatud küberjulgeoleku strateegiad. Lisaks on Euroopa Nõukogu menetlusse saadetud Euroopa Parlamendis heaks kiidetud direktiivi ettepanek, mille eesmärgiks on tagada kõikides liikmesriikides ühtselt kõrge info- ning võrguturbe tase. Strateegiad pole olemuselt otsekohaldatavad, kuid direktiivi jõustumisel, saab mõju liikmesriikidele suurem olema, sest direktiivist tulenevate eesmärkide täitmiseks on siseriiklikke õigusakte vastavalt siseriiklikule valmisolekule tarvis vastavalt muuta. Seega Kopenhaageni põhiteesist lähtuvalt on riigi tasandil tagatud seadusandlik abi, et tagada omakorda KII ettevõtete kaitse.

Tagamaks KII ettevõtete kaitse, tuleb kursis olla peamiste ohuallikate ehk küberrünnakute võimaliku liigitusega. Peamiselt jagatakse küberrünnakuid rünnaku eesmärgist või sihtgrupist lähtuvalt ning on seni teostatud häirimise eesmärgil. Küberrünnakud on ajas ja ruumis pidevalt muutumises ning olles kursis hetkel aktuaalsete küberrünnakutega, suudetakse end tulevaste küberrünnakute eest paremini kaitsta ning vajadusel ettevõttesiseid tegevusplaane või riskijuhtimist ajakohastada.

Töö empiirilises osas kasutati kvalitatiivsetest uurimismeetoditest dokumentide analüüsi ning poolstruktureeritud ekspertintervjuusid. Dokumentide analüüsis võrreldi EL ja Eesti küberjulgeoleku strateegiaid KII ettevõtte võtmes. Võrreldi, kas EL ja Eesti strateegiad pööravad eraldi tähelepanu KII-le. Dokumentide analüüsist selgus, et suurem osa mõlema strateegia eesmärkidest on otseselt või kaudselt KII ettevõtetega seotud. Nii Eesti kui ka EL strateegiates rõhutatakse erasektori ja avaliku sektori koostöö vajalikkust ning rahvusvahelisel tasandil KII ettevõtete parimate praktikate vahetamist. Lisaks keskenduvad strateegiad üldisemas plaanis ühiskonna teadlikkuse tõstmisele läbi koolituste, meediakampaaniate või infopäevade. Samuti tasub välja tuua,

et EL toimeloogikast ning otsustusprotsessist lähtuvalt on antud töö puhul läbivalt näha, kuidas toimib EL otsustusprotsess. Kuidas esialgu reguleeritakse valdkonda õiguslikult mittesiduvate strateegiatega ning kui valdkonna eripärast tingituna on teemat tarvis politiseerida ning esile tõsta, liigutakse õiguslikult siduvate direktiivide välja andmise suunas.

Poolstruktureeritud ekspertintervjuudele vastas energia ja telekommunikatsiooni ettevõtetest kokku seitse eksperti. Intervjuude tulemused polnud ootuspärased ning peamise järeldusena sai lahendatud sissejuhatuses püstitatud töö eesmärk: KII ettevõtete ning Eesti riigi küberjulgeoleku strateegiad pole omavahel kooskõlas. Üheski intervjueeritud ettevõttes polnud küberjulgeoleku valdkonnaga seotud strateegiat ning valdkonda reguleeritakse pigem tegevusjuhiste või kord aastas toimuva strateegiliste riskide hindamisega. Selleks, et ettevõtted saaksid konkreetse KII ettevõttele küberjulgeoleku strateegia koostada, peaksid ettevõtted olema paremini informeeritud küberjulgeoleku riskidest ja võimalikest küberrünnakute ohtudest.

Peamise ettepanekuna soovitab autor riigi küberjulgeoleku haavatavuse vähendamiseks nii era kui ka avalikul sektoril pöörata rohkem tähelepanu koostöö suurendamisele. Peale selle tuleb erasektori KII ettevõtetel koostada ettevõttepõhised strateegiad, mis arvestaks ettevõtete eripäradega ning kaardistaks KII ettevõtetele olulised küberohud ja võimalikud kaitsemeetmed. Täiendava ettepanekuna soovitab autor RIA-l kui avaliku sektori ühel esindajal kord poolaastas edastada KII ettevõtetele uudiskirju, mis sisaldaks endas hetkel kõige aktuaalsemaid küberriske.

Teiseks suurimaks riskiks riigi küberjulgeoleku haavatavuse aspektist on KII ettevõtetes küberkaitsesse suunatud investeeringute puudumine. Autori ettepanekul tuleb KII ettevõtetel väga konkreetselt teha vahet investeeringutel, mida tehakse IT-vahenditesse või küberkaitsesse. IT-vahendid ja küberkaitse ei ole võrdsed mõisted ning üks võib hoopis KII ettevõtte haavatavust suurendada, mitte ootuspäraselt vähendada. KII ettevõtted peaksid teadvustama, mis roll neil siseriiklikult on kanda ning kuidas mõjutavad nende tegemata jätmised riigi julgeolekut laiemas plaanis. Selleks, et tagada suuremad investeeringud küberkaitsesse, tuleks riigil omalt poolt küberjulgeoleku valdkonda rohkem politiseerida ning debattides ja kõneaktides küberjulgeolekut esile tooma.

Kolmanda ettepanekuna soovitab autor riigil võtta juhtiv roll küberjulgeoleku teadlikkuse tõstmisel ehk koolituste ja infopäevade läbiviimisel ning KII ettevõtetele vajaduspõhiselt suunatud riiklike programmide läbi viimisel. Intervjuude käigus selgus, et suurem osa ettevõtetest pole 2013. aastal koolitustel osalenud, kuigi vajadus nende järele eksisteerib. Neljas ettepanek haakub eelmisega, kuid rõhuasetus on EL tasandil – avalikul sektoril võtta juhtiv roll erinevate EL tasandil toimuvate koolituste, õppuste ja parima praktika vahetamise teavitamisest.

Edaspidi soovitab autor küberjulgeoleku valdkonnas uurida erinevaid KII ettevõtteid veelgi rohkem süvitsi minnes ning olenevalt ettevõtte suurusest kindlaks määrata, kuidas ettevõtte suurusest olenevalt küberjulgeoleku valdkonnas orienteerutakse. Kuna vastu võtmisel on küberjulgeoleku valdkonda reguleeriv direktiiv, siis heaks uurimisprobleemi püstituseks saab võtta direktiivi ülevõtmisega seotud KII ettevõtete kohustused ning võimalikud probleemvaldkonnad. Kas KII ettevõtetele tuleb direktiivist lähtuvalt uusi täiendavaid kohustusi ja kuidas Eesti ettevõtted ning avalik sektori direktiivi ülevõtmisega toime tulevad. Autori hinnangul on magistritöö saavutanud oma eesmärgi, võrreldes EL ja Eesti küberjulgeoleku strateegiat KII ettevõtete võtmes ning pakkudes ettepanekuid KII parema kaitse tagamiseks ja riigi küberjulgeoleku haavatavuse vähendamiseks. Magistritöö autor loodab, et antud töö leiab rakendust nii KII ettevõtetes kui ka avalikus sektoris ning seda eeskätt koostöö suurendamise eesmärgil ja siseriikliku küberjulgeoleku haavatavuse vähendamise nimel.

KASUTATUD ALLIKATE LOETELU

Artiklid, raamatud

1. **Balzacq, T.** Securitization Theory. How security problems emerge and dissolve. London and New York: Routledge, 2011, 258 p.

2. **Buzan, B., Hansen, L.** The Evolution of International Security Studies. New York: Cambridge University Press, 2010, 384 p.

3. **Buzan, B., Jaap, de W., Woever, O.** Security: a New Framework for Analysis. Boulder, Colo: Lynne Rienner Publishers, 1998, 239 p.

4. CCD COE. National Cyber Security Strategy Guidelines. Tallinn: NATO CCD COE Publications, 2013, 40 p.

5. **Choo, R.** The cyber threat landscape: Challenges and future research directions. - Computers & Security, 2011, Volume 30, Issue 8, p. 719-731

6. **Collins, A.** Contemporary Security Studies. Third edition. 2013. Oxford University Press. 479 p.

7. **De Bruijne, M., Van Eeten, M.** Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. - Journal of Contingencies and Crisis Management, 2007, Vol. 15, No.1, p. 18-29

8. **Lukasik, S. J., Goodman, S. E., Longhurst D.W.** Protecting Critical Infrastructure against Cyber Attack. Adelphi Paper 359, New York: Oxford University Press. p.7

9. **Mälksoo, M.** Akadeemilised julgeoleku-uuringud sõja ja rahu vahel. Akadeemia, 2009, nr. 9, lk. 1768-1781.

10. NIPP 2006. National Infrastructure Protection Plan. U.S. Department of Homeland Security. 2006. 17 p.

11. **Purser, S.** The European cooperative approach to securing critical information infrastructure. - Journal of Business Continuity & Emergency Planning Revised: 28.10.2011, Volume 5, Number 3, 10 p.

12. **Udeanu, G.** Critical infrastructure protection – imperative of the European Union's harmonious development - Buletin Stiintific, June 2012, Vol. 17 Issue 1, 86-92 p.

13. **Wiener, N.** The Human Use of Human Beings: Cybernetics and Society. London: Free Association Books. 1989. 199 p.

Internetiallikad

14. **Abele-Wigert, I.** Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives. International CIIP Handbook 2006. Vol. II. [http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-04.pdf] 21.02.2014

15. **Ashford, W.** Threat info sharing tough, says RSA conference committee. [http://www.computerweekly.com/news/2240208237/Cyber-threat-info-sharing-a-huge-challenge-says-RSA-conference-committee] 02.11.2013

16. CERT. Turvaintsidentide käsitlemine CERT Eesti. [https://www.ria.ee/cert] 05.03.2015

17. Cisco 2014. Annual Security Report. [https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf] 21.03.2015

18. **Daskala, B., Dekker, M., Karsberg, C.** Cyber Incident Reporting in the EU. An overview of security articles in EU legislation. 27.08.2012 [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu] 15.03.2014

19. DDoS. [http://www.arvutikaitse.ee/arvutikaitse-algtoed/ddos/] 05.03.2015

20. **Dekker, M., Karsberg, C., Lakka, M**. Annual Incident Reports 2012. Analysis of Article 13a annual incident reports. 20. August 2013. [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012] 15.03.2014

21. EKSS. [http://www.eki.ee/dict/ekss/index.cgi?Q=infoturve&F=M] 05.03.2015

22. ENISA. Cooperative Models for Effective Public Private Partnerships. Good Practice Guide. 01.10.2011. [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps] 15.03.2014

23. ENISA. National Cyber Security Strategies in the World. 07.02.2013. [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world] 17.02.2014

24. ENISA. National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace. May 2012. [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper] 17.02.2014

25. **Eriksson, J**. Symposium. Observers or Advocates? On the Political Role of Security Analysts. Cooperation and Conflict, SAGE Publications, 1999. [http://cac.sagepub.com/content/34/3/311.full.pdf+html] 07.02.2015

26. European Commission. About trust and security. [http://ec.europa.eu/digital-agenda/en/about-trust-and-security] 24.10.2013

27. European Commission. EU Cybersecurity plan to protect open internet and online freedom and opportunity. 07.02.2013 [http://europa.eu/rapid/press-release_IP-13-94_en.htm] 26.11.2014

28. **Fahey**, E. The EU-s cybercrime and Cybersecurity rule-making: mapping the internal and external dimensions of EU security. European Journal of Risk Regulation. Vol 1/2014. p.4 [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2384491] 27.11.2014

29. Federal Ministry of Interior. Cyber Security for Germany. 10.03.2011 [http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=47906D07946774A41B703CAB3B10B4FD.2_cid297?__blob=publicationFile] 18.02.2014

30. **Hansen, L, Nissenbaum, H.** Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 2009, 20 p. [http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf] 24.10.2013

31. **Holström, P., Landstedt, J.** Electric Power Systems Blackouts and the Rescue Services: the Case of Finland. Civil Protection Network. 2007:1. [http://www.helsinki.fi/aleksanteri/civpro/publications/WP1.pdf] 21.02.2014

32. HM Governance. FTSE 350 Cyber Governance Health Check. Tracker Report. November 2013. 64 p. [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf] 15.03.2014

33. **Ilves, T. H.** Järgmine väljakutse: küberkaitse. – Diplomaatia, 2012, nr 105. [http://www.diplomaatia.ee/artikkel/jargmine-valjakutse-kuberkaitse/] 15.03.2014

34. **Ilves, T. H.** Ilves: küberrünnakud võivad riigi vähemalt ajutiselt põlvili suruda. ERR. 30.08.2013 [http://uudised.err.ee/v/eesti/60268791-5d89-4095-8f3c-430ed22456dd] 18.02.2014

35. INSA.[http://www.insaonline.org/i/a/i/a/index2.aspx?hkey=10d3ba7c-b95b-4298-9cdb-8cb4a343e161] 05.03.2015

36. INSA. Addressing Cyber Security through Public-Private Partnership: An Analysis of Existing Models. November 2009. [https://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx] 15.03.2014

37. IP-aadress. [http://www.eava.ee/~anur/internet/misted.html] 05.03.2015

38. Riigi Infosüsteemi Amet. ISKE korduma kippuvad küsimused. [https://www.ria.ee/iske-kkk/#Mis_on_iske] 21.03.2015

39. ITU. Global 2014 results. ABI Research. [http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Global_2014_results.pdf] 21.03.2015

40. Japan railroad station attack.[http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199504190006] 07.02.2015

41. Kaspersky Lab. Global Corporate IT Security Risks: 2013. May 2013. 26 p. [http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf] 02.11.2013

42. **Klimburg, A., Tiirmaa-Klaar, H.** Cyber security and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. 2011. [http://www.europarl.europa.eu/committees/de/sede/studiesdownload.html?languageDocument=EN&file=41648] 15.03.2014

43. **Kroes**, N. 15. High common level of network and information security (debate). [http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140312&secondRef=ITEM-015&language=EN&ring=A7-2014-0103] 16.12.2014

44. London underground bombing. [http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200507070002] 07.02.2015

45. **Lukas, L., Necesal, L.** Critical infrastructure protection and role of infrastructure owners/operators. Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1. [http://www.daaam.info/Downloads/Pdfs/proceedings/proceedings_2010/24622_Young_1_head.pdf] 24.10.2013

46. **Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., Ignatuschtschenko, E.** Comprehensive Study on Cybercrime. New York, 2013.

[http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf] 24.10.2013

47. **Maldre, P.** Eesti küberturbe olukord 2014. 02.04.2015. [http://www.icds.ee/et/blogi/artikkel/eesti-kuberturbe-olukord-2014/] 08.05.2015

48. Mis on DDoS küberrünnak. [https://arvutiturve.wordpress.com/2010/03/21/mis-on-ddos-kuberrunnak/] 05.03.2015

49. **Pawlak, P.** Cyber world: site under construction. European Union Institute for Security Studies, 2013, 4 p. [http://www.iss.europa.eu/uploads/media/Brief_32.pdf] 24.10.2013

50. **Pernik, P., Tuohy, E.** Cyber Space in Estonia: Greater Security, Greater Challenges. ICDS, August 2013. [http://www.icds.ee/index.php?id=73&L=1&tx_ttnews%5Btt_news%5D=13621&cHash=65d6d041ac] 18.02.2014

51. Postimees. NATO võrguleheküljed langesid küberrünnaku alla. 16.03.2014 [http://www.postimees.ee/2729272/nato-vorgulehekuljed-langesid-kuberrunnaku-alla] 05.05.2015

52. PricewaterhouseCoopers. The Global State of Information Security® Survey 2015. 30.09.2014 Managing cyber risks in an interconnected world. [http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml] 27.11.2014

53. **Pursiainen, C.** Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection. Nordregio report. 2007. Sweden. [https://www.siseministeerium.ee/public/Elut_htsate_valdkondade_korraldus_teistes_riikides.pdf] 21.02.2014

54. **Raud**, H. Küberjulgeolekust. [http://www.riso.ee/et/content/k%C3%BCberjulgeolekust#.VJ63-V4hQ]. 27.12.2014

55. Riigi Infosüsteemi Amet. Riigi Infosüsteemi Ameti kokkuvõte küberturvalisuse tagamisest 2012. 2013. [https://www.ria.ee/public/KIIK/RIA_kyberturbe_ylevaade_2012.pdf] 24.10.2013

56. Riigi Infosüsteemi Amet. Turvaintsidentide käsitlemine CERT Eestis. [https://www.ria.ee/cert/] 09.04.2014

57. **Rimo, T**. **Walsh, M**. McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies. 09.06.2014 [http://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx] 27.11.2014

58. **Robinson, N., Gribbon, L., Horvath, V., Robertson, K.** Cyber-security threat characterization. Published: RAND Corporation, Stockholm, 2013 [http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf] 24.10.2013

59. RSA. The current state of cybercrime 2013. [http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf] 24.10.2013

60. Spain bombing. [http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200403110004] 07.02.2015

61. Suicide bomber in Volgograd train station. [http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=201312290007] 07.02.2015

62. TNS Emor. Kvalitatiivsed uuringutehnikad. [http://www.emor.ee/kvalitatiivuuringud/] 06.05.2015

Ametlik dokumentatsioon, õigusaktid

63. Council of the European Union. Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Luxembourg. 25.06.2013.

[http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137602.pdf] 24.10.2013

64. Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmete määrus. Vastu võetud 14. märtsil 2013. a nr 43. – RT I, 20.03.2013, 7. [https://www.riigiteataja.ee/akt/120032013007] 21.03.2015

65. Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid. [https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026et.pdf] 21.03.2015

66. European Commission. Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels. 07.02.2013. [http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf] 24.10.2013

67. European Commission. Texts adopted – proposal for a directive. 13.03.2014 [http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=EN&ring=A7-2014-0103] 21.03.2015

68. Euroopa Komisjon. Komisjoni teatis - Euroopa esmatähtsate infrastruktuuride kaitse programmi kohta. Euroopa Liidu Teataja. KOM/2006/0786 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:ET:PDF] 08.04.2014

69. Euroopa Komisjon. Komisjoni teatis Nõukogule ja Euroopa Parlamendile - Kriitilise infrastruktuuri kaitse terrorismivastases võitluses. Euroopa Liidu Teataja. KOM/2004/0702 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:ET:PDF] 08.04.2014

70. Euroopa Komisjon. Euroopa Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele elutähtsate infrastruktuuride kaitse kohta. Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas. Euroopa Liidu Teataja. KOM/2011/163. [http://eur-

lex.europa.eu/legalcontent/ET/TXT/?qid=1396985161151&uri=CELEX:52011DC0163] 08.04.2014

71. Euroopa Liidu leping ja Euroopa Liidu Toimimise Leping. [https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026et.pdf] 07.02.2015

72. Euroopa Majandus- ja Sotsiaalkomitee arvamus. Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus. Euroopa Liidu Teataja. C271. 19.09.2013 [http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:271:0133:01:ET:HTML]

73. Euroopa Nõukogu direktiiv 2008/114/EÜ. Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta. Euroopa Liidu Teataja. L345/75. 23.12.2008 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ET:PDF] 24.10.2013

74. Euroopa Nõukogu raamotsus 2005/222/JSK. Euroopa Liidu Teataja. L69/67. 16.03.2005 [http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32005F0222&from=EN] 05.03.2015

75. Euroopa Parlamendi ja Euroopa Nõukogu direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK. Euroopa Liidu Teataja. L218/8, 12.08.2013 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:ET:PDF]24.10.2013

76. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Euroopa Liidu Teataja, L281/31. 23.11.1995 [http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:ET:PDF] 24.10.2013

77. European Parliament. Legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD) [http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&format=XML&language=EN] 05.04.2014

78. Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy. Preparing the December 2013 European Council on Security and Defence. Brussels, 15.10.2013. [http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf] 02.11.2013

79. Hädaolukorra seadus. Vastu võetud Riigikogus 15. juunil 2009. aastal- Riigi Teataja I osa, 2009, nr. 39, art. 262. [https://www.riigiteataja.ee/akt/13247564?leiaKehtiv] 24.10.2013

80. Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. 2008. Kaitseministeerium. Tallinn. Lk 43 [http://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf] 08.04.2014

81. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM/2013/048 final - 2013/0027 (COD).[http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013PC0048&from=EN] 07.02.2015

82. Regioonide Komitee arvamus „Küberjulgeoleku strateegia." Euroopa Liidu Teataja. C280/19. 27.09.2013 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:280:0019:0026:ET:PDF] 24.10.2013

Muud allikad

83. **Kallis, J.** Eesti rahvusvähemuste julgeolekustamine Pihkva oblasti näitel. TÜ riigiteaduste instituut, 2011, 70 lk. (magistritöö)

84. **Kirch, K**. Küberturvalisuse konstrueerimine ekspertide narratiivides. TÜ rahvusvaheliste ja sotsiaaluuringute instituut, 2013, 82 lk (magistritöö).

85. **Leis, P.** Cybersecurity Risk Management. Küberturvalisuse juhtimine. TTÜ Küberkaitse õppekava loeng. 2013. 99 p.

86. **Leis, P.** Enterprise Risk Management. Küberturvalisuse juhtimine. TTÜ Küberkaitse õppekava loeng. 2013. 64 p.

LISAD

Lisa 1. Avaliku ja erasektori koostöömudel küberjulgeolekus[176]

	Huvid	Võimalused	Piirangud
Telekommuni-katsiooni ettevõtted, riist- ja tarkvara pakkujad, internetiteenuse pakkujad	✓ Tahavad pakkuda teenust ning kaitsta klientide privaatsust ✓ Olla usaldusväärsed tarnijad: optimaalne töö ja kättesaadavus oluline ✓ Tuleb kinnitada, et seadused ei piira arengut ning ei tekitaks puudusi majanduslikus konkurentsis	✓ Spetsialiseerunud tehnikud, kes anomaaliate korral tegutsevad kiiresti ✓ Blokeeritakse *downstream* rünnakuid ✓ Levitavad turvalahendusi tarbijatele, standardid tellijatega	✓ Ei soovita liigselt julgeolekule pühenduda, ärisaladuse problemaatika ✓ Ei soovita tõenäoliselt suurendada kulutusi turvalisusele
Valitsus regulaatorina	✓ Usaldusväärsus, kaitsevõime kaitsmaks kriitilist infrastruktuuri ✓ Sõltub internetitehingute terviklikkusest, kaitsmaks kodanike privaatsust ja majanduslikku heaolu riigis	✓ Saavad võimaldada õigusaktide täitmise küberjulgeolekus ✓ Võivad pakkuda platvormi rahvusvahelisel tasandil ning korraldada teavitustööd ✓ Näidata initsiatiivi, julgustada paremaks koostööks küberjulgeolekus	✓ Keeruline koordineerida vastutust suurte asutuste vahel ✓ Valitsusel on killustatud, hajutatud autoriteet ✓ On võimetud jagama kogu informatsiooni ✓ Julgeoleku tagamine võib mõnel juhul olla seotud eraelu puutumatuse probleemidega
Indiviidid	✓ Tahavad juurdepääsu vastavalt nõudlusele ✓ Vajavad suuremat kaitset isikuandmetele ja isiklikele arvutitele ✓ Umbusaldavad	✓ Suur hulk seadmeid, mille abil vabatahtlikult koguda ja jagada teavet võimalike rünnakute kohta	✓ Tihtipeale pole teadlikud küberjulgeoleku riskidest ✓ Puuduvad piisavad teadmised kaitsmaks end küberrünnaku eest

[176] INSA. Addressing Cyber Security Through Public-Private Partnership. (2009) p. 6

	valitsuse rolli internetis, mis nõuaks karmimaid seadusi ja järelvalvet		
Valitsus	✓ Sõltub interneti kättesaadavusest, pakkumaks internetiteenuseid, suhelda ja toetada riikliku julgeoleku tegevusi	✓ Omavad teavet toimunud rünnakute kohta, mis heaks analüüsi aluseks	✓ Uusi, kindlaid tehnoloogiaid adopteeritakse aeglaselt ✓ Ei suudeta reageerimist koordineerida piisavalt heal tasemel
Ettevõtted	✓ Tahavad juurdepääsu vastavalt nõudlusele ✓ Suur huvi interneti ohutuks muutmise vastu, eesmärgiga edendada e-ettevõtlust, turvata suhtlust ja kaitsta konkurentsi puudutavaid andmeid	✓ Tihtipeale omavad lepingut turvalisuse pakkujatega ✓ Jagavad informatsiooni läbi erinevate liitude, olemas standardid, valitsuse sidemed ✓ Osalevad standardite arendamises	✓ Ettevõtte suurenedes ei suudeta väga kiirelt uusi tehnoloogiaid ja praktikaid uuendada ✓ Infovahetuses ja jagamisel piiratud osalejad, privaatsuse ja usalduse tõttu

Lisa 2. Eesti kriitilise infrastruktuuri liigitus[177]

- Energiarajatised ja -võrgud: elektrienergia, nafta ja gaasi hoidmine, ladustamisrajatised ja töötlemistehased, edastamis- ja jaotussüsteem.
- Side ja infotehnoloogia: telekommunikatsioon, edastus- ja teavitussüsteemid, tarkvara, riistvara ja võrgud, kaasa arvatud Interneti infrastruktuur
- Rahandus: pangandus, väärtpaberid ja investeeringud.
- Tervishoid: haiglad, tervishoiurajatised, laborid ja ravimid, otsingu-, päästе- ja kiirabiteenistused.
- Toit: ohutus, tootmisvahendid, hulgimüük ja toiduainetööstus.
- Vesi: veehoidlad, puhastusjaamad ja veevõrgud.
- Transport: lennujaamad, sadamad, ühendveorajatised, raudtee- ja massitransiidivõrgud, liikluse juhtimissüsteemid.
- Ohtlike kaupade tootmine, ladustamine ja transport: keemilised, bioloogilised, radioloogilised ja teised ohtlikud materjalid.
- Riigiasutused: kriitilised teenistused, rajatised, infovõrgud, riiklikku julgeolekut ja kaitsevõimet tagavad infosüsteemid, ressursid, andmekogud ja õiguslikku tähendust omavad kohturegistrid ning rahvuslikud kultuuriobjektid.

[177] Küberjulgeoleku strateegia komisjon. Küberjulgeoleku strateegia 2008-2013. (2008) lk 38

Lisa 3. Poolstruktureeritud ekspertintervjuude küsimused

1. Juhatuse strateegia/tegevused

1.1 Selgitage, kuivõrd Te puutute ettevõttes kübervaldkonnaga kokku?

1.2 Kas ettevõttel on olemas strateegia/tegevuskava/tegevusjuhised kübervaldkonna reguleerimiseks? Mida strateegia endas hõlmab?

1.3 Kui tihti arutatakse juhatuses strateegiliste riskide üle? Kas küberohud kuuluvad nende riskide alla?

1.4 Kui tähtsaks peetakse küberohte teiste strateegiliste riskide kõrval? On nad olulised või vähemtähtsad?

1.5 Kui palju on ettevõte investeerinud küberkaitsesse võrreldes kogu investeeringutega? (nt % kogu investeeringutest, ei ole tarvis konkreetset summat välja tuua)

1.6 Kas viimase aasta jooksul on toimunud koolitusi küberjulgeoleku alaselt? Kui ei, kas selle järgi oleks vajadust?

2. Koostöö - erasektor vs avaliku sektor ja era vs erasektor

2.1 Kas riik peaks rohkem sekkuma ja aitama erasektorit küberjulgeoleku valdkonnas? Millisel kujul "sekkumine" välja võiks näha?

2.2 Mis on peamised puudused, mis esinevad erasektori arvates avalikus sektoris?

2.3 Kas ettevõte on kursis Eesti küberjulgeoleku strateegiaga? Kas oskate tuua välja puudusi?

2.4 Kas ettevõte on kursis Euroopa Liidu tasandil küberjulgeoleku strateegiaga?

2.5 Kas ettevõte on osalenud Euroopa Liidu tasandil töögruppides, parima praktika vahetamise projektides?

2.6 Kas juhatus julgustab ja motiveerib ettevõtte töötajaid vahetama informatsiooni ja parimat praktikat sama sektori teiste ettevõtetega, tehakse koostööd?

3. Küberohud- ja riskid

3.1 Millised on peamised küberohud Teie ettevõttele ja mis võiksid olla halvimad tagajärjed küberrünnaku korral?

3.2 Milliseid küberrünnakuid on ettevõttes esinenud? Kui jah, tuua näiteid.

3.3 Mis on esmased tegevused kui ettevõtet on tabanud küberrünnak?

Soovi korral lisada alloleva punkti alla ettepanekuid, soovitusi, murekohti seoses küberjulgeoleku/rünnakute valdkonnaga.

IMPLEMENTING EUROPEAN UNION CYBER SECURITY STRATEGY IN CASE OF CYBER ATTACKS IN EXAMPLE OF ESTONIAN CRITICAL INFRASTRUCTURE

Kairi Listmann

Summary

Every day states, international organizations and members of society are connected with internet and different e-services, which help to organize everyday life faster and more easily. Internet-based services and technology are developing constantly, increasing reliance on the Internet. If the technology develops faster than focusing on the cyber threats, then it can be a threat to human health and life or damage the national security. Society is familiar to a greater or lesser extent with the threats that rapid technological development entails. At the same time, it cannot be expected from everyone to know and realize, what could happen, when the critical infrastructure comes under the cyber attack.

The aim of this thesis is to compare European Union cybersecurity strategy with Estonian cybersecurity strategy, focusing on the critical infrastructure. To be more specific, in Estonia the cybersecurity strategies in public and private sector are not compatible and they don´t serve fully the same purposes. If the private sector doesn´t have strong strategy in cybersecurity then public sector and state both are more vulnerable and it threatens national security. Private sector follows the logic of business, with the purpose to earn profits and to keep the costs as low as possible. At the same time for the public sector some threats are more prior and what profit earning companies don´t consider and to what companies don´t implement adequate security measures.

To achieve the research aim there are four research questions, which are as following:

1) What is cybersecurity and how the cyber threats are classified?
2) What is critical infrastructure and what are the main threats to it?
3) What are the state's and critical infrastructure companies' strategies in defending against cyber attacks and how works the co-operation with the state?
4) What kind of suggestions gives the author of this thesis to improve collaboration between public and private sector and in order to reduce the country´s vulnerability in the field of cyber security?

For answering the mentioned research questions author used classical security complex theory and Copenhagen School theory about security in theoretical part of this thesis. In the empirical part analysis of two strategic documents was used: European Union cybersecurity and Estonian cybersecurity strategy – focusing on the critical infrastructure. In addition to the analysis of strategies seven interviews with the experts from telecommunication and energy sector critical infrastructure companies were made by the author.

Answering the first two research questions, different theories brought out, that cybersecurity is a new security sector in theoretical security approaches. The main argument of the Copenhagen School is that if the referent object is in existential threat, the state/government should act and help the ones, who are threatened. Cyber attacks are classified in different approaches differently. Mainly they can be categorized by the aim of the attack – to disturb, to benefit or to destruct, but the fact is, that cyber threats are constantly changing.

The main results from the remaining two research questions came from document analysis and expert interviews and were as following. Strategies in European Union and in Estonia are both mostly focusing on the critical infrastructure and emphasize the importance of protecting the critical infrastructure from the cyber attacks. Results from the expert interviews were partly unexpected. Experts from the telecommunication and energy critical infrastructure companies answered that they don´t have concrete strategy in cybersecurity area, which approved the aim of the thesis, that strategies in public and private sector are not serving the same purposes.

Interviews revealed that critical infrastructure owners don´t invest enough resources into cybersecurity. Author proposed that companies should be more aware of their importance in national security and devote their direct investments into cybersecurity. It also occurred that awareness of cybersecurity and its threats differs in critical infrastructure companies. As a solution the state could find out, whether different sized companies are equally conscious in cybersecurity area and if cybersecurity-programmes run by the state would help to raise the awareness.

The comparison of European Union's and Estonia's cybersecurity strategies in focus of critical infrastructure and main conclusions of the thesis helped to achieve the aim of this thesis. Author hopes that this thesis would find its use in both sectors, because it could increase the cooperation between public and private sector and reduce the vulnerability in national cybersecurity. In further researches the authors could find out, how the different critical infrastructure companies protect themselves against cyber attacks or how the new directive impacts both public and private sector.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kairi Listmann, (isikukood: 48708055220)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose Euroopa Liidu küberjulgeoleku strateegia rakendamine küberrünnakute korral Eesti kriitilise infrastruktuuri näitel, mille juhendaja on MA Piret Pernik ning kaasjuhendaja PhD Jaan Masso,

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 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.

Tartus, **11.05.2015**

_____

(allkiri)