TALLINNA TEHNIKAÜLIKOOL

INSENERITEADUSKOND

Elektroenergeetika ja mehhatroonika instituut

ELEKTRIVÕRGU DIGITALISEERIMISEST TULENEVATE KÜBERRISKIDE JA NENDE VÕIMALIKE MÕJUDE ANALÜÜS

CYBER THREATS CAUSED BY DIGITALIZATION OF POWER GRIDS AND ANALYSIS OF THEIR POTENTIAL IMPACTS

MAGISTRITÖÖ

Üliõpilane: Erik Tamsalu

Üliõpilaskood: 163406AAVM

Juhendaja: Karl Kull, Doktorant-nooremteadur

Tallinn 2019

(Tiitellehe pöördel)

AUTORIDEKLARATSIOON

Olen koostanud lõputöö iseseisvalt.
Lõputöö alusel ei ole varem kutse- või teaduskraadi või inseneridiplomit taotletud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

"....." ..... 201.....

Autor: .....
/ allkiri /

Töö vastab bakalaureusetöö/magistritööle esitatud nõuetele

"....." ..... 201.....

Juhendaja: .....
/ allkiri /

Kaitsmisele lubatud

"....."..... 201... .

Kaitsmiskomisjoni esimees .....
/ nimi ja allkiri /

LÕPUTÖÖ LÜHIKOKKUVÕTE

Autor: Erik Tamsalu *Lõputöö liik:* Magistritöö

Töö pealkiri: Elektrivõrgu digitaliseerimisest tulenevate küberriskide ja nende võimalike mõjude analüüsimine

Kuupäev: 24.05.2019 76 *lk (lõputöö lehekülgede arv koos lisadega)*

Ülikool: Tallinna Tehnikaülikool

Teaduskond: Inseneriteaduskond

Instituut: Elektroenergeetika ja mehhatroonika instituut

Töö juhendaja(d): Doktorant-nooremteadur Karl Kull

Töö konsultant (konsultandid):

Sisu kirjeldus:

Tänapäeva digitaliseeritud maailmas leiab aset üha enam juhtumeid, kus küberrünnakute sihiks on elektrivõrgud ning energiasüsteemid tervikuna. Käesoleva magistritöö eesmärk on analüüsida elektrivõrkude digitaliseerimisega kaasnevaid küberturvalisuse riske elektrisüsteemidele. Lähtudes võrkudesse integreeritavatest kaugjuhitavatest nutistu seadmetest ja inverteritest.

Magistritöö esimeses osas antakse ülevaade Eesti elektrisüsteemist ja elektrivõrkude digitaliseerimise põhjustest. Lisaks tuuakse välja Eesti elektrivõrkudesse lisanduvad kaugjuhitavuse funktsionaalusega seadmed. Täiendavalt uuritakse tarkvõrku tervikuna, selle arengusuundasid, karakteristikuid, tarkvõrgu integreerimist nutistuga ja tutvustatakse nutistu võimalusi targas võrgus.

Töös analüüsitakse Tallinna tihe- ja hajapiirkonnas paiknevatele kaugjuhitavatele nutistu seadmetele ja inverteritele suunatud küberrünnaku stsenaariumeid. Täiendavalt uuritakse küberturvalisuse suurendamise võimalusi läbi elektrivõrke reguleeriva seadusandluse.

Märksõnad: tarkvõrk, küberturvalisus, nutistu, elektrivõrk, digitaliseerimine, seadusandlus, elektrisüsteem

ABSTRACT

Author: Erik Tamsalu *Type of the work:* Master Thesis

Title: Title Cyber threats caused by digitalization of power grids and analysis of their potential impacts

Date: 24.05.2019 76 *pages (the number of thesis pages including appendices)*

University: Tallinn University of Technology

School: School of Engineering

Department: Department of Electrical Power Engineering and Mechatronics

Supervisor(s) of the thesis: Early Stage Researcher Karl Kull

Consultant(s):

Abstract:

The main purpose of this Masters thesis is to analyse cyber security of Estonian power grids and potential cyber threats caused by digitalization of energy system. Mainly focusing on grid integrated remote controlled internet of things devices and solar inverters.

The first part of the thesis gives an overview of Estonian electricity system and discusses reasons for digitalization. Additionally main characteristics of smart grid and its possibilities are defined. Including the review of the main groups of grid integrated remote controlled smart devices such as solar inverters, based on Estonian electricity system.

In the second part of the work a cyber attack on Tallinn's distribution grid is simulated. The simulated attack is carried out by grid integrated smart remote controlled devices such as solar inverters and home appliances. In addition legislation of Estonian energy sector is analysed based on cyber security.

Finally impacts of the simulated cyber attack are analszed and opportunities of improving Estonian energy sector legislation are given.

Keywords: smart grid, cyber security, internet of things, power grid, digitalization, electricity system.

LÕPUTÖÖ ÜLESANNE

Lõputöö teema:	**Elektrivõrgu digitaliseerimisest tulenevate küberriskide ja nende võimalike mõjude analüüs**
Lõputöö teema inglise keeles:	**Cyber threats caused by digitalization of power grids and analysis of their potential impacts**
Üliõpilane:	**Erik Tamsalu, 163406AAVM**
Eriala:	**Elektroenergeetika**
Lõputöö liik:	**Magistritöö**
Lõputöö juhendaja:	**Doktorant-nooremteadur Karl Kull**
Lõputöö ülesande kehtivusaeg:	**kehtivusaja annab juhendaja**
Lõputöö esitamise tähtaeg:	**24.05.2019**

_____	_____	_____
Üliõpilane (allkiri)	Juhendaja (allkiri)	Õppekava juht (allkiri)

1. Teema põhjendus

Tänapäeva digitaliseeritud maailmas leiab aset üha enam juhtumeid, kus küberrünnakute sihiks on elektrivõrgud ning energiasüsteemid tervikuna. Elektrivõrkudesse integreeritakse järjest rohkem nutistu seadmeid, invertereid ja kaugloetavad arvesteid. Seetõttu lisandub elektrisüsteemi ühes erinevate sideprotokollidega ka väliste sidevõrkudega ühenduses olevaid seadmeid, mis paiknevad võrguettevõtete füüsilise kontrolli alt väljaspool. Uued seadmed ja targad lahendused võimaldavad elektrisüsteemi üha optimaalsemalt juhtida, kuid toovad kaasa ka uusi probleeme küberturvalisuse seisukohast. Selle tulemusena lähtutakse elektrivõrkude arendamisel üha enam küberturvalisusest, mis vähendab potentsiaalselt ulatuslike katkestuste ja elektrisüsteemi ebastabiilsuse esinemise tõenäosust. Kirjutaja uurib antud magistritöös kliendi seadmetest tulenevaid riske ning võimalikku majanduslikku kahju, mis kaasneb potentsiaalse küberrünnaku korral. Antud töö analüüsib võrku integreeritavate seadmete parameetreid ning teeb Ühendkuningriigi ja Ameerika Ühendriikide seadusandlusele tuginedes ettepanekuid Eesti elektrivõrkude küberturvalisuse suurendamiseks.

2. Töö eesmärk

Käesoleva magistritöö eesmärk on analüüsida elektrivõrgu digitaliseerimisega kaasnevaid küberturvalisuse riske elektrisüsteemile. Töös käsitletakse riske lähtudes Võrgueeskirjast,

Elektrituruseadusest, energiajulegeolekust ja majanduslikest aspektidest. Töö peamine rõhuasetus on seatud võrguga ühendatavatele nutistu seadmetele, inverteritele ning nendega kaasnevatele riskidele.

3. Lahendamisele kuuluvate küsimuste loetelu:

1) Tarkvõrgu mõiste ja vajalikkus.

2) Nutistu ja elektrivõrgu integreerimisega kaasnevad küberriskid.

3) Kulu edastamata jäänud elektrienergiast.

4) Võrgueeskirja, Seadmeohutuse seaduse, Elektrituruseaduse analüüs lähtudes elektrivõrkude küberturvalisusest energeetikasektoris.

5) Küberturvalisuse seadus ja küberturvalisuse strateegia 2019-2022 mõju energeetikasektorile.

4. Lähteandmed

Esitatud küsimustele vastuste leidmisel tugineb autor allikakriitilisusele. Siinkirjutaja on konsulteerinud erinevate võrguettevõtjatega ning tutvunud Euroopa Liidu, Ühenkuningriigi ja Ameerika Ühendriikide võrgueeskirjade ning direktiividega. Lisaks kasutab autor inverterite tootjate materjale ja kasutusjuhendeid. Aluseks on maailmas aastatel 2007-2018 toimunud küberrünnakute pretsedendid, energeetikaasektorit reguleerivad seadused, sarnased uurimustööd ja erialane teaduskirjandus. Eelnevalt välja toodud lähteandmetele võimaldavad ligipääsu näiteks Sciencedirect ja IEEEXplore digitaalraamatukogud.

5. Uurimismeetodid

Uurimisküsimustele leiab autor vastused tuginedes toimunud pretsedentide andmete analüüsile ja võrdlusele. Siinkirjutaja kasutab töö käigus loodavaid mudeleid ja uurimusraamistikku. Antud töö metoodika põhineb prognoosimisel, autori poolt kirjeldatud hüpoteetilistel stsenaariumitel ja kirjanduse analüüsil. Analüüsi tarkvarana kasutatakse Excelit.

6. Graafiline osa

Joonis 5.2 Neli stsenaariumit juhitava võimsuse kooslustele Tallinna tihepiirkonnas

Joonis 5.3 Neli stsenaariumit juhitava võimsuse kooslustele Tallinna hajapiirkonnas

Joonis 5.4 Küberrünnaku tõttu andmata jäänud elektrienergia hind EUR/kWh, tihepiirkonnas Tallinnas, 200x 200m alal.

Joonis 5.5 Küberrünnaku tõttu andmata jäänud elektrienergia hind EUR/kWh, hajapiirkonnas Tallinnas, 200x 200m alal.

Tabel 5.3 Elektrilevi OÜ poolt võrku lubatavate inverterite nimekiri

7. Töö struktuur

1. EESTI ELEKTRISÜSTEEMI ÜLEVAADE

2. TARKVÕRK

3. KÜBERRÜNNAKUD JA SEADUSANDLUS

4. ELEKTRIVÕRGULE SUUNATUD KÜBERRÜNNAKU MAJANDUSLIKU KAHJU HINDAMINE

5. KÜBERTURVALISUSE VAJALIKKUS NING SELLEGA KAASNEVAD OHUD JA VÕIMALUSED EESTI ELEKTRIVÕRGUS

8. Kasutatud kirjanduse allikad

Käesoleva magistritöö koostamisel on kasutatud IEEExplore ja Sciencedirect digitaalraamatukogusid. Eesti elektrivõrgu analüüsimiseks kasutab autor Eleringi ja Elektrilevi varustuskindluse aruandeid. Lisaks tugineb siinkirjutaja katkestuskahjude hinna määramisel Kristen Sokki magistritööle. Käesolevas töös analüüsitud ja mudelites kasutatud seadmete andmed on saadud tootjate kodulehtedelt. Seadusandluse analüüsiks on kogutud andmeid põhiliselt Riigiteatajast ja Euroopa Liidu andmebaasidest. [1] [2] [3] [4] [5]

SISUKORD

EESSÕNA

Küberrünnakut elektrivõrgule vaadatakse sageli kui ulatuslikku koordineeritud kallaletungi, millel on tervet energiasüsteemi halvavad tagajärjed. Simuleeritakse *blackout*-i stsenaariumeid ning näiteks saarestumise võimalust. Päikeseelektrijaamade inverterite paigaldamisel saadud kogemused andsid autorile teadmise, et küberrünnakut elektrivõrgule on oletatavasti märgatavalt lihtsam läbi viia väiksemal skaalal. Näiteks soodustab turvariski paljude inverterite tootjate läbi veebibrauseri või mobiilirakenduse pakutav kaughalduse fuktsionaalsus. Seeläbi ühendatakse avalikesse internetivõrkudesse rohkelt küberkurjategijatele lihtsasti ligipääsetavaid seadmeid. Arvukate kaugjuhitavate suure võimsusega seadmete korduv lülimine võimaldab küberkurjategijal tekitada kahju nii kliendile kui võrguettevõtetele. Magistritöö „Elektrivõrgu digitaliseerimisest tulenevate küberriskide ja nende võimalike mõjude analüüsimine“ tugineb siinkirjutaja kogemustele ja elektrivõrkude küberturvalisuse päevakohasusele.

Käesolevas töös koostatud hüpoteetilised mudelid ja nende analüüs tõestavad kaugjuhitavast võimsusest ja koormusest tulenevaid küberriske. Eesti elektrivõrgu tööd reguleeriva seadusandluse kujundamisel on käesolev magistritöö sobilik referatiivne allikas avaliku sektori ametnikkonnale.

SISSEJUHATUS

Elektrienergia tootmise ja tarbimise viisid on kogu maailmas teisenemas. Seoses kliimasoojenemise ja ressursside ammendumisega liigutakse eemale pikalt kasutuses olnud traditsionaalsetest fossiilkütustest ning tsentraalsest elektritootmisest. Järjest enam panustatakse uute tehnoloogiate ja materjalide arendamisesse ning üha enam integreeritakse elektrisüsteemidesse stohhastilise toodanguga taastuvenergiaallikaid. Muudatused elektritootmises ja –tarbimises nõuavad elektrisüsteemi alustala ehk elektrivõrkude pidevat optimeerimist ning kiiret, strateegilist ja ühiskonna huvidest lähtuvat arendamist. Praeguste elektrisüsteemide optimeerimine ja areng on jõudnud punkti, kus investeeringute ning elektrisüsteemi efektiivsuse praktiline limiit on saavutatud. Luues omakorda nõudluse uute lahenduste ja elektrivõrgu digitaliseerimise järele. [6]

Käesolevas magistritöös uurib autor elektrivõrkude arengut ja digitaliseerimise põhjuseid. Töö annab ülevaate tarkvõrgu olemusest, eripäradest, võimalustest ja ohtudest, keskendudes eelkõige küberturvalisusele ning sellega kaasnevatele riskidele. Analüüsitakse küberrünnakute osapooli, pretsedente ja elektrivõrkude talitlust reguleerivat seadusandlust Eestis, Ameerika Ühendriikides ja Ühendkuningriigis. Magistritöö keskendub nutistu seadmete ja inverterite võrku lisandumisega kaasnevatele potentsiaalsetele küberriskidele. Valitud seadmete elektrivõrguga sidumisel puuduvad levinud standardid ja seadusandlik regulatsioon, mis tekitab elektrivõrku rohkelt küberrünnakuks sobivaid punkte. Hoolimata seadmete väikesest nimivõimsusest, on piisavalt kontsentreeritud piirkonnas suurel hulgal nutistu seadmeid ja invertereid kontrollides võimalik juhtida arvestatavat võimsust. Tekitades pahatahtlikel lülimistel elektrikatkestusi ning kahjustades seadmeid. Antud töö annab hinnangu eelnevalt välja toodud stsenaariumi majanduslikule mõjule ning pakub parendusettepanekuid vastava valdkonna seadusandlusele.

Magistritöö esimeses osas antakse ülevaade Eesti elektrisüsteemi praegusest olukorrast ja Eesti elektrivõrku lisatavatest potentsiaalsetest kaugjuhitavatest seadmetest. Järgnevalt analüüsitakse elektrivõrgu digitaliseerimist ja selle põhjuseid. Uuritakse tarka võrku tervikuna, selle arengusuundasid, karakteristikuid, tarkvõrgu integreerimist nutistuga ja tutvustatakse nutistu võimalusi targas võrgus. Samuti antakse ülevaade sektoris tegutsevatest ettevõtetest.

Elektrivõrk on kriitilise tähtsusega taristu ning selle küberturvalisuse tagamine peab olema prioriteet. Lisades elektrivõrku rohkelt vastava sektori seadusandluse poolt vähesel määral või täielikult reguleerimata kaugjuhitavaid seadmeid, lisandub elektrivõrku arvukalt küberrünnakuteks sobivaid objekte. Küberturvalisuse tagamise elektrivõrkudes muudab raskemaks seadmete eeldatav pikk eluiga, mille vältel seadme küberturvalisuse funktsioonide efektiivsus väheneb märgatavalt. Nutistu seadmete sidumine elektrivõrguga on eriti kriitiline puuduvate standardite

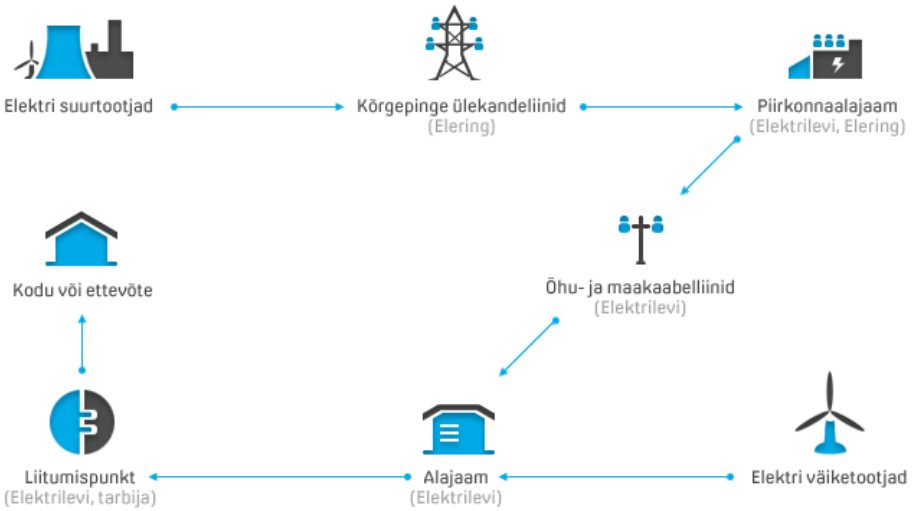
ning puuduliku valdkonna küberturvalisust reguleeriva seadusandluse tõttu. Seeläbi tekib mitmeid turvalisuse kitsaskohti, mida on võimalik küberkurjategijatel elektrivõrkude töö härimiseks kasutada.

Eesti elektrivõrgu tööd reguleerivas seadusandluses ei ole tänasel päeval seadmete küberturvalisuse tagamisele tähelepanu pööratud. Vastavad muutused toimuvad juba näiteks Ameerika Ühendriikides, Ühendkuningriigis ja Euroopa Liidu tasandil. Maailmas, kaasaarvatud Eestis, tekib üha enam küberrünnakute pretsedente elektrivõrkude vastu, mis rünnaku tüüpide ja kuritegelike osapoolte tõttu erinevad nii iseloomult kui eesmärgilt. Näiteks registreeriti Eestis 2018. aastal kokku 3390 küberintsidenti. Küberturvalisus energeetikavaldkonnas saab üha rohkem tähelepanu, kuid suure hulga muutujate, andmete ja erinevate osapoolte tõttu on rünnakute majandusliku mõju hindamise universaalsed mudelid siiani vähe levinud.

Antud magistritöö teises osas luuakse stsenaariumid, millele tuginedes analüüsitakse Tallinna linna 200x 200m tihe- ja hajapiirkonnas potentsiaalselt küberrünnakutele avatud klientide valduses paiknevat juhitavat võimsust. Vaadeldava piirkonna kontsentreeritus põhjustab ohu, et lülimistel tekkiv voolu, pinge ja võimsuse kõikumine võib mõjutada üksnes kindlat jaotusalajaama, liini või maakaablit. Luues seeläbi suuremad eeldused võrguettevõtte vara kahjustamiseks ning pikema kestusega katkestuste tekkeks. Läbi edastamata energia hinna meetodi antakse küberrünnakutest põhjustatud katkestustele hind. Praktilises osas analüüsitakse põhjalikult Eesti elektrivõrku lubatavaid invertereid kui üht suurimat võrguettevõtete füüsilise kontrolli alt väljas paiknevat juhitava võimsuse kooslust. Tuues välja nende võimalikud riskid ning arengusuunad. Lisaks tuuakse välja tänase õigusruumi tugevused, nõrkused, võimalused ja ohud küberturvalisuse seisukohast. Võrreldakse sektori seadusandluse trende Ameerika Ühendriikides ja Ühendkuningriikides rakendatavate tavadega. Tuues seeläbi välja elektrivõrkude tööd reguleeriva seadusandluse nõrkkohad ning lihtsasti elluviidavad parendusettepanekud.

1. EESTI ELEKTRISÜSTEEMI ÜLEVAADE

Antud peatükis käsitletakse Eesti elektrivõrgu hetkeolukorda ja arengusuundasid. Lähtudes elektrivõrgu arendamise põhjustest ning analüüsides võrku lisatavaid seadmeid. Eesti tänase elektrisüsteemi struktuur on kirjeldatud joonisel 1.1.



Joonis 1.1. Eesti elektrisüsteem [7]

Eleringi 2018. aasta varustuskindluse aruandes välja toodud Eesti elektrisüsteemi talitusparameetrid on kuvatud tabelis tabelis 1.1. Võimaldades võrrelda elektrivõrgu digitaliseerimisega võrku lisanduvaid tootmisvõimsuseid hetkeolukorraga. 2018. aasta lõpu seisuga oli Eestisse paigaldatud päikeseelektrijaamade võimsus 27% minimaalsest suvisest netotootmisest. Minimaalsest suvisest tarbimisest oleks võimalik täisvõimsusel töötavate päikeseelektrijaamadega katta ligi 23% – moodustades juba arvestatava osa Eesti elektrivõrgus. Kõik päikeseelektrijaamad on ühendatud elektrivõrku läbi inverterite, millest suur osa on ühendatavad avalikesse internetivõrkudesse ning omavad kaughalduse funktsionaalsust. Sellest tulenevaid küberriske käsitletakse täiendatavalt antud töö käigus.

Tabel 1.1 Eesti elektrisüsteemi talitusparameetrid 2017/2018 talve- ja suveperioodil**.** [8]

Eesti elektrisüsteemi talitusparameetrid	**Väärtus, MW Talvine**	**Aeg**	**Väärtus, MW Suvine**	**Aeg**
Maksimaalne netotarbimine	1553	28.01.2018	1153	16.08.2017
Minimaalne netotarbimine	703,09	05.11.2017	483	12.08.2017

Eesti elektrisüsteemi talitusparameetrid	Väärtus, MW Talvine	Aeg	Väärtus, MW Suvine	Aeg
Keskmine netotarbimine	1053		814	1.05-1.10.2017
Maksimaalne netogenereerimine	2031	15.11.2017	1932	30.06.2017
Minimaalne netogenereerimine	662	01.11.2017	413	22.07.2017
Keskmine netogenereerimine	1296		1185	1.05-1.10.2017

1.1 Eesti Põhivõrk

Eesti elektrivõrk jaguneb kaheks suuremaks üksuseks. Põhivõrk ehk ülekandevõrk ja jaotusvõrk. Põhivõrgu eesmärk on kanda suurematest tootmisüksustest elektrienergiat lõpptarbijate lähedusse ning võimaldada riikide vahelisi ühendusi. Elektrienergia üle kandmiseks põhivõrgus kasutatakse kõrgepinget. Eestis kuuluvad põhivõrku järgnevad pingedastmed: 35, 110, 220 ja 330 kV. Kogu põhivõrk kuulub Eestis AS Eleringile, mis hooldab ja arendab ligi 5500 km pikkuses kõrgepinge liine ning 150 alajaama. Aktsiaseltsi tegevust finantseeritakse suuresti läbi võrgutasude. Pideva ennetava hoolduse ja arendustegevuse eesmärgiks on tagada võimalikult kõrge talitluskindlus [9] [10]. Eestis on põhivõrguga liitunud klientide arv 28. [11]

1.2 Eesti Jaotusvõrk

Jaotusvõrgu eesmärk on tarnida elektrienergia põhivõrgu liitumispunktidest lõpptarbijateni. Lõppklientidele elektrienergia tarneks kasutatakse enamasti madalamaid pingeastmeid – vahemikus 0,4–35 kV, üksikutel juhtudel ka 110 kV. Eesti jaotusvõrgu elektriliinide pikkus on üle 60 000 km, lisaks on jaotusvõrgus üle 22 000 alajaama. Jaotusvõrgu hooldust ning investeeringuid finantseeritakse võrgutasudega. [10] [7]

Jaotusvõrgu ettevõtteid on täna 27. Neist suurim on OÜ Elektrilevi, kelle turuosa moodustab 87,5%. Elektrilevile järgnevad VKG Elektrivõrgud OÜ ja Imatra Elekter AS [12]. Kokku on Eestis jaotusvõrkudega liitunud kliente hinnanguliselt 720 000. Statistikaameti andmete kohaselt moodustab Elektrilevi turuosa 87,5% ning Elektrilevi andmete kohaselt on paigaldatud 630 000 kaugloetavat arvestit. [12] [13]

1.3 Eesti elektrisüsteemi areng

Traditsionaalselt on Eesti nagu ka teiste Euroopa riikide elektrienergia tootmine põhinenud konventsionaalsetel soojuselektrijaamadel, moodustades üle 90% elektrienergia kogutoodangust. [14]

Seoses Energiamajanduse arengukavaga aastani 2030 (ENMAK 2030) ja erinevate Euroopa Liidu (EL) direktiividega, kasvab elektrisüsteemi lisatavate stohhastiliste hajatoomisüksuste koguvõimsus iga aastaga. Taastuvatest energiaallikatest elektrienergiatootmist soodustavad näiteks EL-i Energia ja kliimapakett 2020, EL-i energia teekaart 2050 ja Euroopa puhta õhu programm. [15]

Eleringi 2018. aasta varustuskindluse aruande kohaselt on installeeritud netotootmisvõimsus 2828 MW, millest hüdro-, tuule-, ja päikeseelektrijaamad moodustavad üle 17%. Plaaniliselt suletakse aastaks 2026 ligi 620 MW elektrienergia tootmisvõimsust. [8]

Eelnevalt välja toodud muutused elektrienergia tootmises loovad eeltingimused ning ka vajaduse elektrivõrgu pidevaks uuendamiseks ja automatiseerimiseks. Arvestades muutliku toodangu kasvu, on tarkvõrgu tulemuslik arendamine Eesti elektrisüsteemile oluline.

1.4 Kaugloetavad arvestid Eesti elektrivõrgus

Kokku on Elektrilevi võrgus ligi 630 000 kaugloetavat arvestit ning Eestis kokku hinnanguliselt üle 700 000. Eesmärk on suurendada tarbimisprognooside täpsust, elektrienergia ülekande efektiivsust ning vähendada katkestuste kestvust [13]. Esimene suuremahulisem elektrivõrgu digitaliseerimise projekt, kus elektrivõrgu taristu kriitiliste punktide ümbert eemaldatakse füüsilised tõkked.

Seega saab eeldada, et elektrisüsteemi lisandus sadu tuhandeid küberrünnakutele haavatavaid punkte, mis on küll võrguettevõtete kontrolli all, aga füüsiliselt ligipääestavad ka teistele osapooltele. Lisaks on arvestid läbi sidevõrkude kaugjuhitavad. Tekitades seeläbi teoreetilise ohu andmete kuritarvitamiseks ja mõõtmisandmetega manipuleerimiseks. [16]

1.5 Eesti elektrivõrku integreeritavad inverterid

2018. aasta jooksul lisati Eesti elektrivõrku ligi 100 MW uusi päikeseelektrijaamasid. Kõikide elektrivõrguga ühendatud päikeseelektrijaamade koguvõimsus ulatus 2019. aasta alguseks ligi 110 MW-ni [17]. Tuues seega kaasa tuhandete tarkade, IP (*internet protocol*) sidet kasutavate inverterite võrku lisandumise. Võrku integreeritavad inverterid paiknevad füüsiliselt võrguettevõtete kontrolli alt väljas. Võimaldades seeläbi seadmetele kergemat ligipääsu

rohkematel osapooltel. Suureneb ka tõenäosus, et tootmisseadet kasutatakse ebasihipäraselt teadmatusest või näiteks pahatahtlikul eesmärgil. Tulemusena on võimalik negatiivselt mõjutada elektrivõrgu talitlust.

Eestis teostavad inverterite liitumist võrguettevõtted ning uute inverterite võrku lisamist reguleerib seadusandluses põhiliselt Võrgueeskiri. Seadus ei sisalda kuni 1 MW nimiaktiivvõimsusega elektrivõrku lisatavatele inverterile ühtegi küberturvalisusega seotud punkti. Tänases võrgueeskirjas keskendutakse peamiselt releekaitse funktsionaalsusele [18]. Põhiliselt integreeritakse elektrivõrku invertereid seoses päikeseelektrijaamadega [19], aga lisaks leiavad inverterid rakendust ka elektriautode laadimisel [20] ja akupankades [21].

Imatra Elekter AS ja VKG Elektrivõrgud OÜ jaotusvõrkudes lähtutakse inverterite elektrivõrku lisamisel standardist EVS-EN 50438-2013. Erandiks on üle 200 kW nimivõimsusega tootmisüksused, mida reguleerivad Elektrilevi OÜ või Elering AS [22] [23]. Lisaks aksepteerivad nii VKG Elektrivõrgud kui ka Imatra Elekter Elektrilevi sobivate seadmete nimekirjas välja toodud seadmeid, mis on põhjalikumalt välja toodud tabelis 1.2.

1.5.1 Elektrilevi OÜ poolt aksepteeritavate inverterite põhjalik ülevaade

Elektrilevi OÜ poolt lubatavad seadmed väiketootjatete elektrivõrguga liitumiseks on välja toodud Elektrilevi liitumistingimustes [24]. Seadmed peavad vastama Euroopa Parlamendi ja nõukogu kahele järgnevale direktiivile. Esiteks 2014/35/EU, mis reguleerib teatavas pingevahemikes kasutatavate elektriseadmete kättesaadavust, eesmärgiga tagada eelkõige seadmete kasutajate füüsiline turvalisus [25]. Teiseks 2014/30/EU, mis reguleerib elektromagnetilist ühilduvst [26]. Lisaks peavad seadmed omama vastavusmärgist lähtudes määruses (EC) No. 765/2008 [27].Direktiividest puuduvalt täielikult küberturvalisust reguleerivad punktid, misläbi võib eeldada, et tegemist pole hetkel prioriteediga.

Elektrilevi nimekiri võrguga liitumiseks sobivatest inverteritest väiketootjatele koosneb paljude tootjate erinevatest mudelitest.Tabelis 1.2 vaadeldakse invertereid ainult tootja järgi, kuna kasutusel olevad kaugjuhtimise platvormid on ühe tootja erinevatel seadmetel ühilduvad. Kaugjuhtimise ja loetavuse funktsionaalsus tähendab tabelis 1.2, et tootjal on tootevalikus inverter, mis toetab kaughaldust või võimaldavad kaughaldust inverteriga ühilduvad lisaseadmed. Inverterite tootja DVE Technologies ApS on suletud, seadmeid ei toodeta ega hooldata enam, sellega seoses puudub ka informatsioon antud tootja omaduste kohta [28]. Samuti puudub info INVOLAR Corporation Ltd. inverteri kohta.

Tabel 1.2 Elektrilevi OÜ poolt võrku lubatavate inverterite nimekiri. [24]

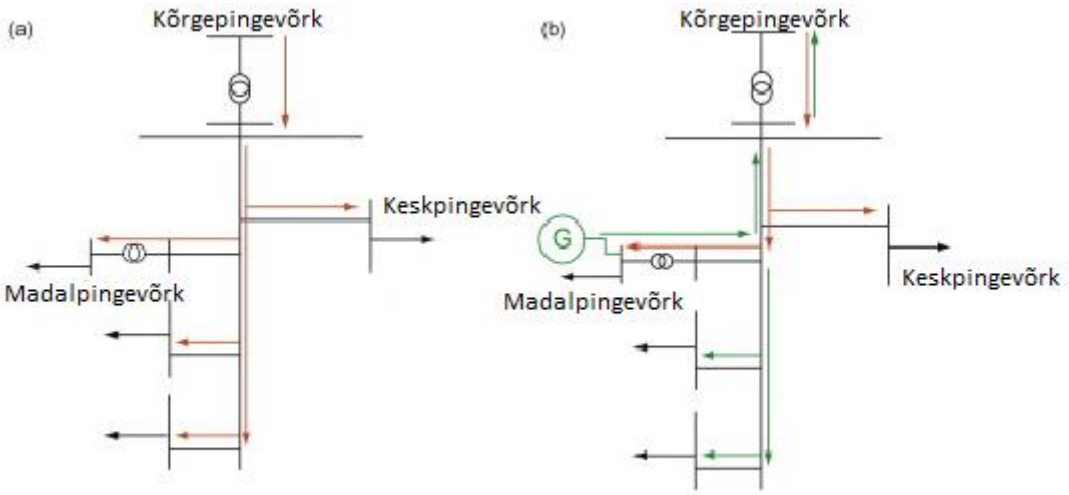
Tootja	**Sobivate inverterite võimsused (kW)**	**Kaugjuhtimise ja –loetavuse funktsionaalsus**	**IP side**
ABB	3 - 100	Jah [29]	Jah
Altenergy Power System Inc.	0,5 - 0,9	Jah [30]	Jah
Delta Energy Systems GmbH	3-50	Jah [31]	Jah
DVE Technologies ApS	10	-	-
Eaton	4,6	Jah [32]	Jah
EC POWER A/S	20	-	-
Envertech Corporation Ltd.	0,25-0,5	Jah [33]	Jah
Fronius International GmbH	3-27	Jah [34]	Jah
GoodWe Power Supply Technology Co. Ltd.	0,9-75	Jah [35]	Jah
Growatt New Energy Technology Co. Ltd.	1-48	Jah [36]	Jah
Hoymiles Converter Technology Co. Ltd.	0,25-1,2	Jah [37]	Jah
Huawei Technologies Co. Ltd.	2-60	Jah [38]	Jah
INVOLAR Corporation Ltd.	0,235	-	-
Indop d.o.o.	130	-	-
KACO new energy GmbH	5-50	Jah [39]	Jah
Kostal Solar Electric	3-36	Jah [40]	Jah

Tootja	Sobivate inverterite võimsused (kW)	Kaugjuhtimise ja –loetavuse funktsionaalsus	IP side
LG Electronics Inc.	5	-	-
Ningbo Ginlong Technologies Co. Ltd.	3-3,6	Jah [41]	Jah
Orbital A/S	250	-	-
REFU Elektronik GmbH	13-20	Jah [42]	Jah
Renesola	0,22	Jah [43]	Jah
Shenzhen JingFuYuan Tech	10	Jah [44]	Jah
SMA Solar Technology AG	1,6-60	Jah [45]	Jah
Solaredge Technologies Inc.	2,2-27,6	Jah [46]	Jah
Solutronic AG	2,85-10	Jah [47]	Jah
SoMa Solar Holding GmbH	2-10	Jah [48]	Jah
Tuge Energia	50	-	-
Twerd	5,5	Ei [49]	Ei
Volter Oy	45	-	-
Zeversolar New Energy Co.	2-33	Jah [50]	Jah
Zucchetti Centro Sistemi Spa	3,68-20	Jah [51]	Jah
XZERES Wind	2,4	-	-

1.6 Elektrivõrgu digitaliseerimise põhjused

Järjest enam tekib elektrivõrku kahesuunalist elektrienergia liikumist. Traditsiooniline ülevalt alla integreeritud elektrivõrgu mudel on asendumas aina enam kasvava prosumerite osakaaluga

elektrivõrguks. Praegune elektrivõrgu infrastruktuur on ajalooliselt planeeritud ja ehitatud elektrienergia ühesuunaliseks liikumiseks. [6]



Joonis 1.2 (a)Traditsonaalne elektrienergia liikumine elektrisüsteemis (b) Kahesuunaline elektrienergia liikumine, mis kaasneb hajatootmise kasvuga [6]

Praeguste elektrisüsteemide optimeerimisega on jõutud punkti, kus nii investeeringute kui ka süsteemi üldine efektiivsus on praktilise limiidi lähedal. Ehk täiendav parendamine ei pruugi tuua majanduslikku kasu. Tuginedes allikatele [6] [52] [53] [54], on põhilised põhjused elektrivõrgu üha suuremaks digitaliseerimiseks ning tarkvõrkude arendamiseks järgnevad:

- Suurendada elektrivõrku tehtavate investeeringute efektiivsust.
- Realiseerida uute tehnoloogiate potentsiaali. Näiteks uued materjalid, sidetehnoloogiad, autonoomsed seadmed, informatsiooni kogumine ja salvestamine ning elektriautode osakaalu kasv.
- Parem võimekus ning efektiivsus taastuvenergial põhinevate stohhastiliste energiatootmistehnoloogiate võrku integreerimiseks.
- Vähendada emissioone ja kasvuhoonegaase nagu näiteks: SF6 ja C02.
- Suurendada energiatootmise ja tarbijale tarnimise kvaliteeti ning efektiivsust.
- Tagada elektrivõrgu töökindlus ja turvalisus.
- Suurendada nii põhi- kui ülekandevõrgu efektiivsust, tagades seeläbi tarbijatele soodsam elektrienergia hind.

2. TARKVÕRK

Tarkvõrku käsitletakse kirjanduses kui traditsionaalse ühesuunalise tarbimisega elektrivõrgu edasiarendust. Termini paremaks mõistmiseks on järgnevalt välja toodud mõned definitsioonid tarkvõrgule:

Tarkvõrku saab defineerida kui integreeritud elektrivõrgu tehnoloogiate, seadmete ja juhtimissüsteemide gruppi, mille eesmärk on koguda ja utiliseerida digitaalset informatsiooni optimeerimaks elektrivõrgu efektiivsust, töökindlust ja tarnekindlust. Tarkvõrgu tähtsamateks karakteristikuteks saab pidada automaatset süsteemi balansseerimist, autonoomset võrguparameetrite kogumist ja rikete tuvastamist, erinevate energiaressursside utiliseerimise võimekust, elektritootmisest ja ülekandest tulenevate kasvuhoonegaaside minimeerimist, elektrienergia ülekande kitsaskohtade parendamist ja süsteemi tõrkekindluste suurendamist ning tarbimise ja tootmise vahelist realajas infovahetust. [55]

Kokkuvõttes saab modernset tarkvõrku vaadelda kui küber-füüsilist inimiteguriga süsteemi. Milles elektri ülekande, mõõtmiste, süsteemi juhtimise ja otsuste tegemise eest vastutavad võrdselt nii inimene, füüsilised seadmed küberliidesed. Iga liige on omavahel ühendatud ning elektrivõrgu turvaliseks normaaltalituse tagamiseks peavad kõik osapooled toimima laitmatult. Eksimus mistahes süsteemi osaliselt toob kaasa negatiivse mõju elektrivõrgule. [56]

Lähtudes Euroopa Komisjoni Innovaatilise liidu 2020 strateegiast on tarkvõrk uuendatud elektrivõrgustik, mille on lisatud intelligentsed mõõtmisvõimalused ning tootjate ja tarbijate vaheline kahesuunaline digitaalne andmevahetus. Ülesanne on efektiivse ja jätkusuutliku elektrisüsteemi tagamine, integreerides tootjad, tarbijad ning prosumerid, pakkudes seeläbi tarbijale kvaliteetset ja turvalist teenust. [57]

Ameerika Ühendriikide Riikliku Standardite ja Tehnoloogia instituudi definitsioonist tulenevalt on tarkvõrk eelmise sajandi elektrivõrgu ning käesoleva sajandi informatsiooni- ja kommunikatsioonitehnoloogiate integratsioon. [16]

2.1 Asjade internet

Tarkvõrk seob omavahel traditsionaalse elektrivõrgu ning informatsiooni- ja kommunikatsioonitehnoloogiad, lisades elektrivõrku hulgaliselt intelligentseid seadmeid. Nutistut mainiti tõenäoliselt esimest korda 1999. aastal, viidates raadiosagedustuvastuse ühendamisele internetiga. [58]

Nutistu jaguneb kolmeks suuremaks kategooriaks – Tööstuslik asjade internet (*Industrial Internet of Things – IIoT*), kõige internet (*Internet of Everything – IoE*) ja sotsiaalne asjade internet (*Social Internet of Things*). [3]

Asjade internet on arvutuslik kontseptsioon, mis kirjeldab tavaliste füüsiliste seadmete ühendamist internetti, omades seejuures võimekust ennast võrgule identifitseerida ning teisi seadmeid tuvastada. Seega tekib olukord, kus füüsilistest seadmetest ja infrastruktuurist moodustub ühtne suur informatsioonisüsteem, mis võimaldab jälgida seadmete seisukorda ja rikkeid, teostada ennetavat hooldust ning suurendada süsteemide kulupõhist efektiivsust. [59]

Omavahel ühendatud seadmete ehk nutistu suurus on koos arvutusvõimekuse kiire tõusuga pidevalt kasvamas. Prognoositavalt koondavad tark elektrivõrk, sõidukid, targa linna lahendused, targad kodud, tark tervishoid ja igapäevaselt kasutatavad tavaseadmed 2020. aastaks ligi 30 miljardit ühendatud seadet. Mängides üha suuremat rolli inimeste igapäevaelu järjest kriitilisema tähtsusega funktsioonide juures, vajades protsessides minimaalselt inimese sekkumist. [3]

Joonis 2.1. IoT seadme tunnused [60]

2.1.1 Pilvandmetöötlus ja pilveteenus

Saab vaadelda kui eraldi valdkonda, kuid antud töös vaadeldakse pilveteenuseid ja pilvandmetöötlust kui nutistu ja inverterite tugifunktsiooni.

Pilv andmetöötlus võimaldab kasutajal salvestada või andmeid töödelda serverites, millele on seadmetel või kasutajal läbi interneti ligipääs. Pakkudes seeläbi suuremat arvutusvõimsust nutistu seadmetele, inverteritele ja teistele elektrivõrku lisatavatele seadmetele, mis on mõeldud suhtlema läbi interneti protokolli. [61]

2.2 Asjade internet targas elektrivõrgus

Tarkvõrku nähakse ühe suurema potentsiaaliga infrastrukuuri, kus on võimalik realiseerida nutistu potentsiaali. Nutistu omab fundamentaalset rolli tarkvõrgu arengus, aidates reguleerida

suuremahulist infovahetust üle interneti ning tagades probleemideta kommunikatsiooni sensorite, lülitite, kaugloetavate arvestite ja võrguettevõtete serverite vahel. [16]

Prognoositakse, et aastaks 2030 elab ligi 80% maailma elanikkonnast linnapiirkondades. Elektrienergia utiliseerimine ja kättesaadavus dikteerib, kuidas inimesed töötavad, elavad ja kogukonnana arenevad. Loobumine elektritootmisel kasutatavatest konventsionaalsetest kütustest võib tuua kaasa muutusi inimeste elektrienergia tarbimises. Tänapäeva elektrisüsteemis toimub tootmine keskustest eemal asutavates suure võimsusega elektrijaamades, mis töötavad fossiilkütustel. Elektrijaotus tugineb sarnasel ehita–ja–ühenda põhimõttel, arvestades ühenduspunkti koormusega konkreetsel hetkel ning tulevikus. Motiveerituna kliimasoojenemisest on paljud riigid, ettevõtted ja võrguoperaatorid asunud pikalt toiminud töökindlat süsteemi reformima tarkvõrgu suunal. Lootes infrastruktuuri, elektrienergia hinnastamise, tootmise ja tarbimise järjest põhjalikumal integreerimisel vähendada kadusid ning suurendada elektrisüsteemi efektiivsust. Erinevalt traditsionaalsest elektrisüsteemist suudab tarkvõrk jälgida elektrienergia liikumist nii seadmete kui süsteemisiseselt, seadmete ja süsteemiväliselt. Sealjuures dünaamiliselt kohanduda reaalajas ümbritsevate tingimuste ja vajadustega, luues eeldused eneseteadlikumale elektrisüsteemile, mis on võimeline paremini juhtima nii tarbimist, jaotamist kui tootmist. Elektrisüsteemi üha suurem automatiseerimine ja avalikes võrkudes paiknevate seadmete arvukuse kasvuga kaasneb ka ohte. Kaasates rohkem eratarbijaid elektrivõrgu protsessidesse ja kujundades vajaduse pideva mitmesuunalise informatsiooni järgi, tekib elektrivõrku järjest rohkem küberturvalisusest tulenevaid ohte. [3]

Nutistut peetakse üheks potentsiaalseimaks tehnoloogiaks tarkvõrkude arengus. Asjade interneti integreerimisel elektrivõrku, tekib lisaks traditsionaalsetele, kriitilise tähtsusega ja võrdlemisi hästi seaduste ja võrguettevõtete poolt reguleeritud seadmetele võrku üha enam avalikes võrkudes olevaid seadmeid. Võrreldes elektrivõrgu tööd kontrollivate seadmetega nagu näiteks ja kaugjuhtimisterminali on asjade internetiga nii tarkvõrgu kui ka välise elektrivõrgu osaks saamas ka riisikeetjad, külmkapid, televiisorid, elektriboilerid ja pesumasinad. Antud muutusega kaasneb plahvatuslik elektrivõrguga suhtlevate seadmete kasv, misläbi suureneb ka süsteemi haavatavust. [16]

2.2.1 Nutistu rakendused elektrivõrkudes

Alljärgnevalt on välja toodud mõned nutistu rakendused elektrivõrkudes ja elektrisüsteemides, mida maailmas kasutatakse:

- General Electric Grid Solutions – Energiasüsteemide juhtimine, laiseire- ja juhtimissüsteemid, reaalajas elektrisüsteemi jälgimine, hajatootmise juhtimine ja optimeerimine, tarkvaralahendused. [62]

- Locus Energy – Aitab planeerida ja optimeerida päikeseelektrijaamade rajamist. Haldavad üle 80 miljoni mõõtmispunkti, mis aitavad tagada päikeseelektrijaamade parima väljundvõimsuse. [63]

- GridIO – Osaleb koduseadmeid integreerides võimsusturul. Omab võimekust lülitada sisse- ja välja näiteks veeboilereid ning muid seadmeid. [64]

- Clebox – Juhib elektritarbijate seadmete tööd, et elektritarbimine toimuks võimalikult soodsal hetkel. Jälgides tarbija vajadusi ning elektrituru hinda. [65]

- Sympower – Pakub turule reservvõimsust. Juhtides klientide seadmete tarbimist. Eesmärgiga vähendada fossiilkütustel põhinevaid reservvõimsust pakkuvaid elektrijaamasid. [66]

- Smart Load Solutions – Platvorm võimaldab kliendil kütte- ja ventilatsiooniseadmete tarbimist juhtida vastavalt soodsale elektrienergia börsihinnale. [67]

2.3 Küberturvalisuse väljakutsed tarkvõrgus ja nutistuga integreeritud tarkvõrgus

Elektrivõrk liigitub kriitilise tähtsusega taristu alla, seetõttu on tarkvõrgu küberturvalisus olulise tähtsusega ning elektrivõrgu digitaliseerimisel ning nutistu integreerimisel üks suuremaid väljakutseid. Lisades elektrivõrkudesse arvukalt nutistu seadmeid kujuneb välja suur hulk võrgu küberrünnakutes haavatavaid punkte.

Energeetikasektor on traditsiooniliselt keskendunud ohtudele nagu näiteks füüsilised kahjustused, õnnetused, looduskatastroofid ja seadmete rikked. Tänaseks on maailmas olnud mitmeid küberrünnakute pretsedente, mis illustreerivad küberrünnakute hävitavaid tagajärgi. Teisalt on küberrünnakute uudsuse ning esinemise tiheduse tõttu ohu teadvustamine sageli võrkude seisukohast tertsiaarne probleem. [68]

Erinevalt traditsionaalselt elektrivõrku ühendatud kontrollseadmetest nagu arvutid ja *IED*-d, pole enamus nutistu seadmed uuendatavad ning on seetõttu hiljem avastatud turvaaukudele avatumad. Lisaks on suur enamus nutistu seadmeid võrguga ühenduses läbi ebaturvaliste interneti

protokollide ja paiknevad avalikes võrkudes [16]. Probleemi süvendavad ka nutistu seadmetele omased parameetrid nagu näiteks madal võimsus, vähendatud võimekusega tulemüürid ja protsessorid, mis raskendavad krüptogtraafia ning turvaprotokollide rakendamist. Siinkohal tuleb mäkrida, et võrguettevõtted ja tootjad planeerivad intelligentsete seadmete elueaks hinnanguliselt 10 või rohkem aastat. [69] [68]

2.3.1 Tarkvõrgu sidelahenduste iseärasused

Seadmete valik on enamasti homogeenne ning erineb põhiliselt funktsionaalsuse poolest. Paigaldatavate sensorite ja võrguseadmete elueaks eeldatakse kuni 10 või rohkem aastat, mis on tehnoloogia arengut silmas pidades pikk periood. Tarkvõrgu tööd juhtivatele seadmetele on iseloomulik ka vajadus kaugjuhitavuse ja –uuendamise tarbeks. Tuues kaasa erinevate osapoolte ligipääsu seadmetele [68]. Tarkvõrgus rakendatavad side- ja kommunikatsioonitehnoloogiad põhinevad suuresti autonoomsel masin-masin andmevahetusel. [70]

2.3.2 Küberturvalisusega seotud ohud tarkvõrgus

2017 aastal oli internetiga ühendatud hinnanguliselt 8,4 miljardit nutistu seadet. Samal aastal läbi viidud uuringus skanneerisid 310 000 nutistu kasutajat oma võrguga ühendatud seadmeid ning tuvastasid 4,5% seadmetel turvariske. Kõik tuvastatud riskid kuulusid kategooriasse kergesti ligipääsetavad või lahti murtavad süsteemid. Varasemalt välja toodud prognooside kohaselt võib 2020. aastaks internetivõrguga seotud olla kuni 30 miljardit nutistu seadet [71]. Sarnase statistika põhjal muudaks see kergelt ligipääsetavaks hinnanguliselt 1,35 miljardit nutistu seadet.

Küberohtude seisukohast on probleemiks ka võrguettevõtete tava kasutada ühe tootja toodangut terves piirkonnas, suurtes alajaamades või kogu võrgus, luues seeläbi homogeense seadmete keskkonna, mis on ideealne pinnas pahavara levikule ning terve piirkonna, üksuse või süsteemi küberrünnakuga kahjustamiseks. [68]

Kuritegelikel osapooltel või organisatsioonidel on ligipääs suurele hulgale inverteritele ja seeläbi näiteks päikeseelektrijaamadele on võimalik valede parameetrite sisestamisega inverterisse mõjutada reaktiiv- ja aktiivvõimsust. [19]

Stsenaariumis, kus kuritegelikul isikul või organisatsioonil on ligipääs suurele hulgale nutistu seadmetele, võib õigeaegsetel seadmete kommuteerimistel kaasneda sageduse ebastabiilsus. Näiteks USA lääne ühendvõrgus eeldatakse, et 30% äkiline koormuse kasv kindlas piirkonnas suudab põhjustada generaatorite kaitsereleede rakendumise [4]. USA lääne ühendvõrgu suvine tipukoormus suvel oli 150 700 MW ja talvel 126 200 MW. Terve süsteemi sageduse häirimiseks

oleks vaja suvel ligi 45 000 MW koormuse kasvu ning talvel ligi 38 000 MW koormuse kasvu. Selle eelduseks on näiteks 9 miljoni soojaveeboileri ootamatu sisselülitamine suvel ja 7,6 miljoni soojaveeboileri sisselülitamine talvel. Vaadeldavas piirkonnas elab 2015. aasta seisuga 80 miljonit elanikku ning lääne süsteemis installeeritud tootmisüksuste nimivõimsus on kokku 265 000 MW, millest 15% moodustavad tuule-, päikese- ja muud taastuvenergial põhinevad stohhastilise toodanguga elektrijaamad. [72]

Suure võimsusega nutistu seadmete sisselülitamise tulemusel tekib liinide ülekoormamine ja väljalülitumine. Varasemalt uuritud Poola elektrivõrgu näitel piisab suvise tipukoormuse ajal vaid 1% koormuse suurenemisest. [4]

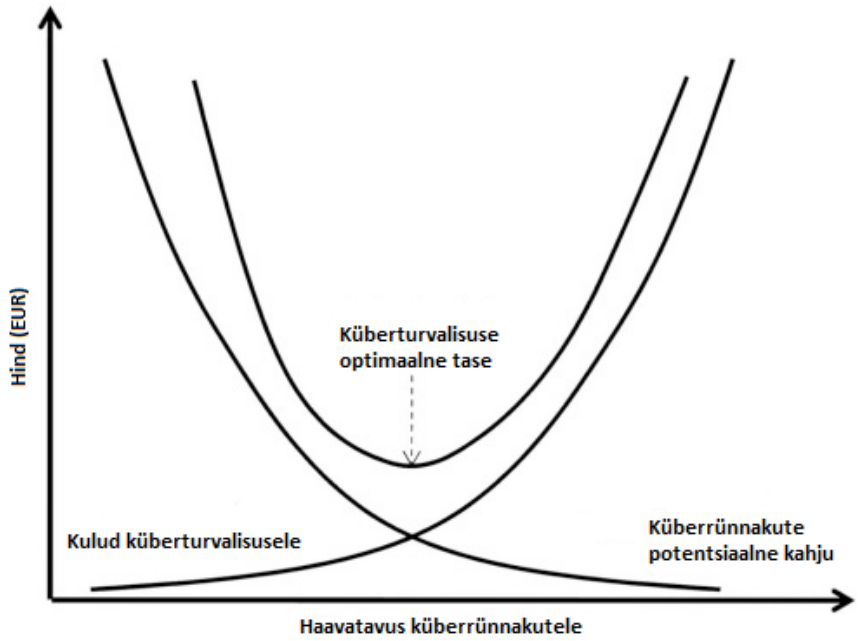
Inverteri parameetritega manipuleerides on võimalik imiteerida elektrivõrgu veaolukorraga sarnane karateristik, mille tulemusena võib rakenduda kaitserelee, tekitades ajutisi põhjuseta katkestusi. Lisaks on küberkurjategijatel võimalik lülitada välja läbi inverterite võrku ühendatud tootmisvõimsusi, tuues kaasa näiteks päikeseelektrijaama omanikule kahju müümata jäänud elektrienergia eest. [19]

Bilansituru ebastabiilsusest tulenevad kulud, mis on seotud päevasisese ootamatu tarbimise kasvamisega. Juhul kui lülitatakse sisse prognoosimata koormust, peab elektrimüüja süsteemioperaatori kulud tasuma. [4]

2.3.3 Küberturvalisusega seotud võimalused tarkvõrgus ning küberrünnakute ennetamine

Tarkvõrkudes ja elektrivõrkudes üldisemalt toimub põhiline infovahetus masinalt-masinale (Machine-to-Machine) põhimõttega. Olles seega tunduvalt etteaimatavam ja prognoositavam võrreldes tüüpilise inimeselt-inimesele (Human-to-Human) või inimeselt masinale suhtlusega (Human-to-Machine). Võimaldades anomaaliate või väärtalituse korral ennetavalt tegutseda, vähendades ka seeläbi küberrünnakute õnnestumsie võimalust. [68]

Võimalus on anda võrguettevõtetele suurem kontroll elektrivõrku lisatavate inverterite ja nutistu seadmete üle. Suurendades läbi seadusandluse võrguettevõtete volitusi ja kohandades regulatsioone vastavalt tarkvõrgu arengule – selle tulemusel rakendada näiteks põhjalikke autentimismeetmeid ja reguleerida seadmete valikut. [73]



Joonis 2.2 Küberrünnakutete ennetamiseks tehtavate rahaliste kulutuste optimaalsuse kõver. [5]

Sõltumata valdkonnast on küberrünnakute ennetamiseks olemas erinevaid kaitsemeetodeid, ennetamisvõimalusi ning vastupanu meetmeid. Globaalselt on prognoositav küberturvalisuse suurendamiseks mõeldud kulu 2019. aastal 124 000 MUSD [74]. Seevastu küberkuritegevusest tulenevad kulud on hinnanguliselt 600 000 MUSD [75]. Ennetavate turvameetmete majanduslikult optimaalset rakendamist iseloomustab joonis 2.2.

Ettevõtete näitel kulutab Microsoft küberturvalisusele hinnanguliselt üle 1000 MUSD aastas, mis moodustab 0,9% ettevõtte käibest 2018 aasta seisuga [76] [77]. JPMorgan Chase & Co kulutab küberturvalisusele hinnanguliselt 600 MUSD aastas, mis moodustab antud ettevõtte käibest 0,05% [78]. Vaadeldud ettevõtete näitel võib eeldada, et Elektrilevi eelarve küberturvalisusele võiks olla üle 2 MEUR [79]. Teistel jaotusvõrgu ettevõtetel VKG Elektrivõrkud ja Imatra Elektril võiks küberturvalisuse eelarve olla hinnanguliselt vahemikus 100 000 - 160 000 EUR [80] [81]. Eesti põhivõrku haldaval Eleringil üle 1 MEUR-i [82]. Kõiki Eesti võrguettevõtteid on võrreldud 2017. aasta käibele tuginedes ning küberturvalisuse osakaaluks käibeks on Microsfoti näitel 0,9%.

3. KÜBERRÜNNAKUD JA SEADUSANDLUS

3.1 Elektrivõrgu tööd/turvalisust reguleeriv seadusandlus Eestis

Eestis suunavad võrguettevõtjate tegevust õigusruumis põhiliselt võrgueeskiri, elektrituruseadus, küberturvalisuse seadus, küberturvalisuse strateegia 2019-2022 ja seadme ohutuse seadus.

Võrgueeskiri [83], mille reguleerimisala lähtuvalt paragrahvist 1 on järgnev:

1) Elektrisüsteemi varustuskindlusest tulenevad tehnilised nõuded tootmisseadmetele;

2) Lihtsustatud tingimused alla 15 kW võimsusega taastuvat energiaallikat tootmiseks kasutavate tootmisseadmete ühendamiseks võrguga.

Elektrituruseadus [84], mille reguleerimisala lähtuvalt paragrahvist 1 on järgnev:

1) Käesolev seadus reguleerib elektrienergia tootmist, edastamist, müüki, eksporti, importi ja transiiti ning elektrisüsteemi majanduslikku ja tehnilist juhtimist. Seadus näeb ette elektrituru toimimise põhimõtted, lähtudes vajadusest tagada põhjendatud hinnaga, keskkonnanõuete ja tarbija vajaduste kohane tõhus elektrivarustus ning energiaallikate tasakaalustatud, keskkonnahoidlik ja pikaajaline kasutamine.

Küberturvalisuse seadus [85], mille reguleerimisala lähtuvalt paragrahvist 1 on järgnev:

1) Käesolev seadus sätestab ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused.

Antud seadusega kehtestatakse ka paragrahv 3 punkti 1 alusel, tuginedes Hädaolukorra seadusele, et elektriga varustamine liigitub elutähtsa teenuse alla. Sellest tulenevalt on teenuse osutaja kohustatud rakendama meetmeid küberintsidentide ennetamiseks ja lahendamiseks. Teenuse osutajal on õigus piirata küberintsidendi mõju vähendamiseks ka süsteemi kasutamist või juurdepääsu süsteemile. [85] [86]

Seadme ohutuse seadus [87], mille reguleerimisala ja eesmärk lähtuvalt paragrahvist 1 on järgnev:

1) Käesoleva seaduse eesmärk on tagada seadmete ja nendega seotud protsesside ohutus.

2) Käesoleva seadusega reguleeritakse seadme kasutusele võtmist ja kasutamist ning seadmetööd.

Küberturvalisuse strateegia 2019-2022, mille eesmärgiks on määratleda küberturvalisuse valdkonna pikeajalisem strateegia, eesmärkide saavutamiseks vajalikud tegevused ning on aluseks ressursside planeerimisel. Strateegia koostamisel on arvestatud EL-i ja NATO sarnaste arengusuundadega. Võimaldades Eestil seeläbi teha paremat koostööd partnerriikidega. Strateegia üheks põhiliseks eesmärgiks on tõsta Eesti ühiskonna küberteadlikust tervikuna. Eesti üheks suurimaks küberriskiks on riigi tähtsate funktsioonide suur digisõltuvus. Võrdlusena on näiteks kõik Eesti kaugloetavad arvestid kaugjuhitavad, mis muudab küberriski aktuaalseks ka energeetikasektoris. Võimaldades küberrünnaku korral võrgust lülitada enamus kliendid. Tähtsal kohal on ka uute tehnoloogiatega kaasnevate riskide hindamine ja haldamine. Tulevikuriskide ennetamiseks on vaja panustada ühiskondliku diskussiooni loomisesse ja lahenduste väljatöötamisel tugineda teaduskompetentsidele. [88]

Euroopa Liidu direktiivid

- Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/1148. Direktiiv meetmete kohta, millega tagada võrgu- ja informatsioonisüsteemide turvalisuse ühtalselt kõrge tase kogu EL-is. Direktiiv muudab liikmesriikidele kohustuslikuks turvalisuse strateegia ning loob liikmesriikide vahelise valdkonna sisese koostöö edendamiseks koostöörühma. Eestis on vastav töörühm CERT-EE, mis edastab infot küberintsidentidest Riigi Infosüsteemi Ametile. Antud direktiiviga kehtestatakse oluliste teenuste operaatoritele ja teenuse osutajatele turvanõuded, sealhulgas ka elektriettevõtetele. Tulenevalt sellest tekib liikmesriigil kohustus tagada, et riigis vastava teenuse osutajad võtavad asjakohased meetmed ja turvanõuded kasutusel. [89]

3.2 Tarkvõrgu tööd reguleeriv seadusandlus teistes riikides

California informatsiooniturvalisuse 2020. aastal kehtima hakkavas seadusepunktis määratletakse võrguga ühendatud seadmete turvalisus. Vastavalt sellele on tootja või tootja esindaja kohustatud tagama optimaalse küberturvalisuse taseme kõikidele California osariigis müüdavatele ja toodetavate seadmetele. Seadmele implementeeritud turvalisus peab vastama seadme omadustele, funktsionaalsusele ning seadme disain peab kaitsma infovarguse või autoriseerimata ligipääsu eest. Igal toodetud seadmel peab olema unikaalne parool ning esmakasutusel peab seadme funktsionaalsus kasutajale uue parooli genereerima. [90]

Ühendkuningriikides on kasutusel nutistu seadmete kasutust reguleeriv hea tava koodeks (CoP-Code of Practice). CoP sätestab 13 põhipunktis järgneva: nutistu seadmetel ei tohi olla universaalset parooli ja kasutajatunnust ega tehase seadete lähtestamise võimekust, nutistu seadmete tootjatel

peab olema avalikult kättesaadav keskkond turvariskide raporteerimiseks, seadmed peavad olema uuendatavad, seadmed peavad võimaldama andmete turvalist salvestamist ning kustutamist, tundliku informatsiooni kommunikatsioon, kaasaarvatud kaugjuhtimine ja -haldus, peavad olema krüpteeritud, seadmete paigaldus peab olema võimalikult lihtne ning turvaline. [91] [92]

3.3 Küberrünnakute liigid

Küberrünnakud ja küberjulgeolek ei erine olenemata valdkonnast oma sisult. Sarnast tehnikat, mida kasutatakse kellegi pangakonto tühjendamiseks, võib pahatahtlik häkker, grupeering või riik kasutada ettevõtetelt oskusteabe varastamiseks. Kuigi energeetikasektor on strateegiline valdkond ja selle toimimine on kriitilise tähtsusega, võib energiasüsteemi rünnata sarnaste meetoditega nagu eraisikut. Lisaks pidevalt ohule tuleb arvestada, et ründajad leiavad pidevalt uusi meetodeid süsteemitungimiseks. Võrdluseks on näiteks lennundussektori opereerimine tunduvalt lihtsam kui interneti liikluse haldamine, kui hoolimata sellest oluliselt rohkem reguleeritud. [93]

- Kinnisründeoht (Advanced Persistent Threat). Olemuselt peamiselt mingi välisriigi majanduslikest, poliitilistest, või näiteks sõjalistest huvidest lähtuv, enamasti pikemat aega kestev rünnak [94]. Eesmärgiks on tungida süsteemi, kus võimalikult pikka aega märkamatult andmeid koguda ning jätta maha minimaalselt jälgi. Omadustelt on kinnisründeoht enamasti suunatud spionaažiks nii riiklikul- kui korporatiivtasandil. [95]

- Hajus ummistusrünne (Ddos, distributed denial-of-service attack) sooritamiseks kasutatakse sihtvõrgu liikluse kiireks suurendamiseks või ülekoormamiseks suurt arvu ründavaid süsteeme, näiteks *bottnete* [94]. Võrreldes näiteks kinnisründeohuga, pole hajus ummistusründe eesmärgiks infovargus, vaid süsteemide ja sihtmärkide töö häirimine.

- Teenusetõkestus (DoS, denial of service) on mõeldud ligipääsu tõkestamiseks erinevatele ressurssidele või toimingute viivitamiseks, mille tulemusena kaotab kasutaja süsteemi käitlemise võimekuse. [96]

- Meta- ja polümorfne kahjuvara (Metamorphic, polymorphic Malware) näol on tegemist kahjuvaraga, mille algkood avastamise takistamiseks igal iteratsioonil muutub. Polümorfne kahjuvara on avastamise vältimiseks pidevas muutuses sarnaselt metamorfsele, kuid ei muuda algkoodi [94].

- Õngitsemisrünnak (Phishing) on petturlik protsess, millega elektroonilises suhtluses usaldatavat olemit teeseldes püütakse saada privaatset või konfidentsiaalset teavet,

kasutades selleks suhtlusosavust või tehnilist pettust. Põhiliselt on rünnaku edukaks sooritamiseks vaja inimeksimust. Eriliik harpuunimine (*Spearphishing*), sihtmärgiks kindel organisatsioon. Eelduseks on teavae organisatsiooni struktuuri kohta. [94]

- Uss (Worm) on iseseisev programm, mis võib end levitada andmetöötlussüsteemide või arvutivõrkude kaudu. Uss sageli ehitatud täielikult ära kasutama vabu ressursse, näiteks mäluruumi või töötlusaega, ei vaja paljunemiseks ja kahju põhjustamiseks peremeesprogrammi ega inimabi. [94]

- Troojalane (Trojan) on andmete volitamatut kogumist, võltsimist või hävitamist võimaldavat ründeloogikat sisaldav näiliselt kahjutu programm. Kasulikku rakendust teesklev kahjurprogramm. [94]

- Bottnett (Botnet) on pahatahtlike seadmete kogum koos kaugjuhitava tarkvaraga, mis töötab autonoomselt, õõnestatud arvutites. Kasutusvaldkond näiteks ebaseaduslik spämmimine ja teenusetõkestus. [97]

3.4 Küberrünnakute osapooled/ründajate iseloomustus/grupid

- *Script kiddies* – Väheste arvutialaste oskustega isik, kes kasutab teiste poolt loodud tööriistu küberrünnakute läbiviimiseks. Eesmärgiks on tihti lihtsalt uute asjade proovime. [3]

- *Hacktivists* – Edasijõudnud programmeerimis- ja arvutialaste teadmistega. Suudavad läbiviia keerulisemaid rünnakuid. Motiveeritud poliitilistest või isiklikest põhimõtetest. [3]

- Organiseeritud küberkurjategijad – Võimelised läbi viima suureulatuslikke ja raskesti tuvastatavaid küberrünnakuid. Teenivad küberkuritegudega raha. [3]

- Riiklikult toetatud küberrünnak – Riigi poolt toetatud küberkurjategijad. Kasutuses on suured ressursid, et viia läbi ulatuslikke rünnakuid kriitiliste teenuste ja infrastruktuuride pihta. [3]

3.5 Küberrünnakud Eestis

Eestis tagab ja jälgib kübersüsteemide turvalisust Riigi Infosüsteemi Amet. Joonisel 3.1 on välja toodud RIA arvuline võrdlus Eestis 2016., 2017. ja 2018. aastal toimunud küberrünnakutest.

Joonis 3.1. Kolme viimase aasta küberohtude raporteerimine RIA-le. [98]

2019. aasta küberturvalisuse raportis on andmed esitatud erineval kujul võrreldes 2018. aastaga. Võrreldakse aastate jooksul tehtud pöördumisi RIA poole. Seoses 2018. aastal jõustunud küberturvalisuse ja andmekaitse regulatsioonidega tõusis RIA poole pöördumine märgatavalt. Lisaks registreeriti 2018. aasta jooksul kokku 3390 intsidenti, mis on ligi 7,7% suurune kasv võrreldes eelneva aastaga ning ligi 34% suurune kasv võrreldes 2016. aastaga. 2018. aasta üheks trendiks oli seadmete, näiteks ruuterite ründamine. Ruuterid muudeti osaks robotovõrgustikust, mis võimaldab koguda andmeid või sooritada erinevaid tüüpi rünnakuid. [98]

Eesti näitel on konkreetsemalt just energeetikasektoris rünnaku alla sattunud Viru Keemia Grupp. Rünnakud toimusid 2016. aasta vältel ning küberrünnakute taga olid tõenäoliselt Venemaa küberkurjategijate rühmitused. Lisaks pääsesid ründajad ligi ka kriitilistele SCADA süsteemidele. [99] [100]

Pronksiöö on riikide vaheliste küberrünnakute üks rahvusvahelisi pretsedente. Esimesed rünnakud toimusid 27. aprilli õhtul pärast pronkssõduri teisaldamist. Küberrünnakud olid koordineeritud ning etteplaneeritud. Teenusetõkestusmeetodil (*DoS*) rünnati esimese lainena valitsusega seotud veebilehti ning teenuseid ja meediaväljaandeid. Teise laine robotvõrgustikuga rünnati panga- ja majandusteenuseid. [101]

3.6 Küberrünnakud mujal maailmas

2016. aasta uuringu tulemusena selgus, et ligi 54% Ameerika Ühendriikide kriitilise infrastruktuuri vastu tehtud küberrünnakutest olid suunatud energeetika infrastruktuurile, olles seeläbi küberrühmituste eelistatuimaks sihtmärgiks. [102]

RIA küberturvalisuse 2018. aasta aruandes on eraldi välja toodud 2017. aastal toimunud küberrünnakud Energiasektorile, tuues pretsedentidena välja sissetungimised energeetikaettevõtete ärivõrkudesse Ameerika Ühendriikides. Lisaks on sarnaseid juhtumeid täheldatud Ühendkuningriigis ja Türgis. [103]

Puerto Rico kaugloetavate arvestite 2009. aastal toimunud rünnaku eesmärgiks oli vähendada elektriarveid. Tänu füüsilisele seadmetele ligipääsule installeeriti seadmetesse muudetud tarkvara, mis vähendas mõõdetud elektrienergia kogust. [104] [105]

2013. aastal toimus rünnak kaupluste ketile Target, mille käigus õnnestus küberkurjategijatel varastada 40 miljoni inimese krediitkaardi andmed. Süsteemile pääseti ligi tänu nutistuga ühendatud küttele, ventilatsioonile ja jahtusseadmetele. [105]

2015. aastal Ukraina jaotusvõrgu ettevõttele Kyivolblenergo suunatud küberrünnaku tulemusel võtsid küberkurjategijad SCADA süsteemi üle kontrolli ning lülitasid välja 7 110 kV alajaama ning 23 35 kV alajaama. Väiksemamahulised rünnakud toimusid samaaegselt veel kolmele jaotusvõrgu ettevõttele. Rünnakute tagajärjel kaotasid hinnanguliselt 225 000 klienti kolmeks tunniks elektriühenduse. [106]

Mirai *botnet*-i esimene pretsedent leidis aset 2016. aastal, kui nutistuga ühendatud põhiliselt turvakaameratest ja videosalvestitest koosneva *botnet*-iga rünnati Prantsusmaa ettevõtte OVH teenuseid. *DdoS* rünnak koosnes hinnanguliselt miljonist ühendatud seadmest, mille tulemusena koormati OVH süsteeme tipphetkel 1 Tbps mahuga. [105]

2017. aastal toimus küberrünnak Ühendkuningriigi ja Iirimaa võrguettevõttele, kus *phishing* rünnakuga varastati kriitilise tähtsusega paroole ning üritati saada kontrolli antud võrguettevõtte hallatava taristu üle. Küberrünnak ei olnud edukas. [16] [107] [108]

4. ELEKTRIVÕRGULE SUUNATUD KÜBERRÜNNAKU MAJANDUSLIKU KAHJU LEIDMINE

Küberrünnakute ja -riskide majanduslik hindamine on raskendatud rohkete varieeruvate tegurite, andmete kättesaadavuse, andmete hulkade ning inimfaktori tõttu. Puudub kindel, laialt levinud mudel kõikide küberriskide ning nende tagajärgede hindamiseks. Sellest tulenevalt pole näiteks levinud ka küberturvalisusega seotud kõiki riske katvad kindlustused. [109] [71]

Kirjanduses on mitmeid teoreetilisi ettepanekuid küberrünnakutest tulenevate majanduslike kahjude täpsemaks hindamiseks. Kasutades riskide hindamiseks inimestele näiteks *MicroMort*-i [110] ja finantsriskide hindamiseks riskiväärtuse meetodit (VaR) [111] [112], [5].

4.1 Andmata energia hind

Andmata energia hind (*CENS/ cost of energy not supplied*) – Võimaldab leida andmata jäänud keskmise elektrienergia hinna keskmise katkestuse pikkuse korral. Sobiv meetod kui puudub täpne informatsioon katkestuste ajaliste kestuste tõenäosuste kohta. Andmata energia hinda arvutatakse valemiga 4.1. [113]

$$CENS = \frac{1}{n}\sum_{i=1}^{n}\frac{Cl(ri)}{LF * ri} \tag{4.1}$$

Kus ri - erikahjufunktsiooni i-ndale punktile vastava katkestuse kestus, h,

Cl(ri) – eriakahjufunktsiooni i-ndale punkti ordinaat (€/kWh),

n – erikahjufunktsiooni punktide arv,

LF – vaadeldava kliendikogumi koormustegur. [113]

Ekvivalentne meetod, mis võimaldab leida edastamata jäänud energia hinna majandussektorite kaupa. Edastamata energia hind moodustub majandussektori kogutoodangu jagamisel vastavas majandussektoris tarbitud elektrienergiaga. Majandussektori põhise andmata jäänud energia hinna leidmiseks kasutatakse valemit 4.2.

$$CENS = \frac{GVAi}{ECi} \tag{4.2}$$

Kus GVAi – Aastas loodav i −sektoris loodav kogulisandväärtus, MEUR,

ECi – Aastas i – sektoris tarbitav elektrienergia, GWh. [114]

4.2 Elektrienergia tarbimine erinevates Eesti elektrivõrgu varustuspiirkondades

Eesti jaotusvõrk jaotatakse varustuskindluse piirkondadeks vastavalt klientide tihedusele [klienti/km^2], tarbimistihedusele GWh/km2 ja eelnevate parameetrite korrutisele [klienti*GWh/km2]. Sellest tulenevalt on jaotus: ülitihe-, tihe-, hajatihe- ja hajapiirkond. [1]

Tabel 4.1. Elektrienergia tarbijate osakaalud vastavalt varustuskindluse piirkonnale [1]

Tarbija/Varustuspiirkond	**Ülitihepiirkond**	**Tihepiirkond**	**Hajatihepiirkond**	**Hajapiirkond**
Kodutarbijad	70,2%	71,7%	78,4%	89,8%
Põllumajandus	0%	0,01%	1,0%	3,1%
Tööstustarbijad	0,1%	0,5%	2,3%	1,7%
Teenindustarbijad	29,7%	27,8%	18,3%	5,4%
Kokku (tk)	**58545**	**303386**	**209966**	**83262**

Tabel 4.2. Elektrienergia tarbimine vastavalt varustuskindluse piirkonnale [1]

Tarbija/Varustus- piirkond	**Ülitihepiirkond**	**Tihepiirkond**	**Hajatihepiirkond**	**Hajapiirkond**
Kodutarbijad	47%	33%	35%	72%
Põllumajandus	0%	0%	4%	9%
Tööstustarbijad	1%	6%	12%	7%
Teenindustarbijad	52%	61%	45%	11%
Kokku (GWh)	440	3539	2504	305

4.3 Andmata energia hind Eesti elektrivõrgus

Lähtudes elektrienergia tarbimisest erinevates varustuspiirkondades ja tuginedes kirjanduses avaldatud andmetele on töös kasutusel järgnevad andmata energia hinnad.

Tabel 4.3. CENS, EUR/kWh Eestis majandussektorite kaupa. 2016. aasta seisuga [2]

Tarbijasektor	**CENS, EUR/kWh**
Põllumajandussektor	2,16 €
Tööstussektor	2,42 €
Äri ja avalik teenindus	4,32 €
Majapidamised	4,79 €

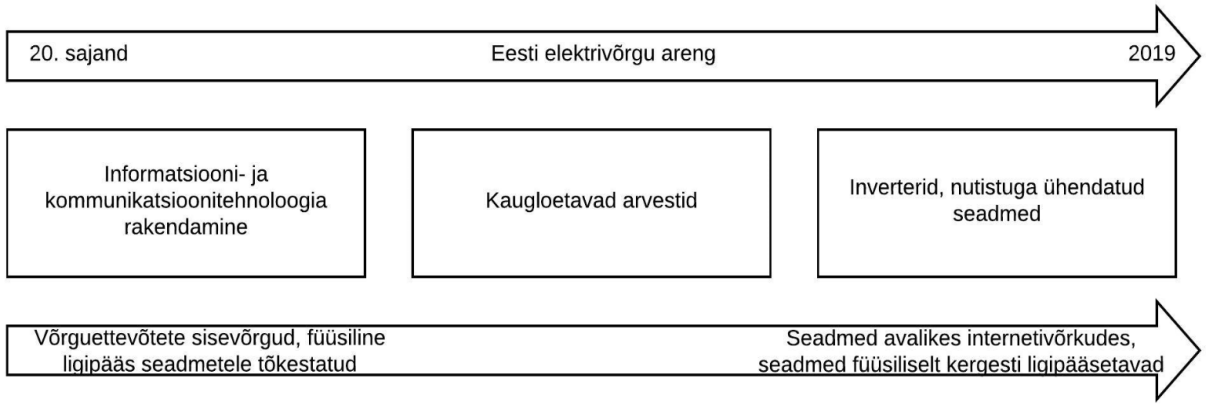
Hinnad on leitud analüütilistel meetoditel, jagades majandussektori loodava väärtuse sektori tarbimisega ning korrigeerides saadud tulemust CEPA (Cambridge Economic Policy Associates Ltd) leitud asendamatu energia koefitsendiga. [2] Vastavalt sektorile on kogu elektrienergia tarbimisest asendamatu tööstussektoris 80,9%, äri- ja avalikussektoris 68,2% elektrienergiast. Viimast osakaalu saab rakendada ka põllumajandusele, mis kuulub CEPA uuringus teeninduse sektorisse. Majapidamissektoris oli CEPA uuringus elektrist sõltuvate tegevuste osakaal 63,1%. [115]

5. KÜBERTURVALISUSE VAJALIKKUS NING SELLEGA KAASNEVAD OHUD JA VÕIMALUSED EESTI ELEKTRIVÕRGUS

Antud töös püstitatud ülesannetest lähtuvalt luuakse hüpoteetilised stsenaariumid, mille analüüsimisel antakse hind küberrünnakutele Eesti elektrivõrgus. Küberohtude analüüs tugineb eeldusele, et elektrivõrkudesse integreeritakse üha enam avalike internetivõrkudega ühenduses olevaid seadmeid. Näiteks inverterid ja nutistuga ühendatud kodumajapidamisseadmed, mis paiknevad füüsiliselt võrguettevõtete otsese kontrolli alt väljaspool. Vastavat arengut elektrivõrgus iseloomustab ka joonis 5.1.

Selle tulemusel on võimalik küberkurjategijatel saada kontroll arvukate kaugjuhitavate seadmete üle. Koondnimivõimsusega 100 - 3000 kW kaugjuhitavate seadmete kogumiku pahatahtliku lülimise mõju on kogu elektrisüsteemi mastaabis marginaalne. Antud võimsuse korduva lülimise mõju on kordades suurem väiksemas võrgupiirkonnas, kus pahalaste kontrollitav võimsus moodustab arvestatava osakaalu kogu piirkonna koormusest. Selleks vaadeldakse antud magistritöö küberrünnakute stsenaariumites kahte Tallinna linna 200x200m suurusega piirkonda, kus kliendid on liitunud põhiliselt pingel 0,4 kV.

Vaadeldavate stsenaariumite käigus tuvastatud küberriskide minimeermise peamise võimalusena nähakse elektrivõrkude valdkonda ja selle arengut reguleerivat seadusandlust. Küberturvalisusest tulenevad ohud ja võimalused leitakse läbi Eesti elektrivõrke reguleeriva seadusandluse analüüsi. Võimalustena vaadeldakse ka Ameerika Ühendriikides ja Ühendkuningriigis levinud seadusandluse praktikaid ning EL-i direktiive.



Joonis 5.1 Elektrivõrku lisanduv kaugjuhitav koormus ja võimsus on järjest kergemini ligipääsetav.

5.1 Mudelite kitsendused

Juhitavate võimsuste koosluste koostamisel on lähtutud Eestis kõige tõenäolisemalt kasutatavaid kaughallatavaid suure võimsusega koduseadmeid ehk alates nimivõimsusega 1 kW. Inverterite juhitav võimsus on arvestatud sarnaselt koduseadmetele ning summeeritud, kuigi tavaolukorras on võimsuse liikumine inverterites vastassuunaline. Arvestades põhimõttega, et inverterid on multifunktsionaalsed ning leiavad rakendust ka elektriautode laadimispunktides ja akupankades, kus karakteristikud on koduseadmetele sarnased. Mudelis kasutatava inverteri nimivõimsus 15 kW põhineb Eesti Võrgueeskirja paragrahv 1 punktis 2 sätestatul ehk alla 15 kW võimsusega tootmisseadmete võrku ühendamisel kehtivad lihtsustatud tingimused.

Klienti käsitletakse antud töös kui ühte tarbimiskohta. Juhitava võimsusega klientide osakaalude arvestamisel on lähtutud varustuskindluse piirkondade liigitamisel piirmääradest. Seega on tihepiirkonna klientide arv 200x200m piirkonnas suurem kui 400. Samuti on aasta keskmine tarbimine 10 000 kWh/h piirväärtus ning reaalsuses on mõne 200x200m Tallinna südalinna tihepiirkonna aasta keskmine tarbimine üle 20 000 kWh/h. Vastupidiselt tihepiirkonnale on leitud tihepiirkonna väärtused konservatiivsed. Hajapiirkondades on klientide arv vaadeldud 200x200m piirkonnas 25 või vähem ja aasta keskmine tarbimine 1000 kWh/h või vähem.Vaadeldavate varustuspiirkondade karakteristikud on välja toodud Lisas 1. Tulemustes võivad selle tõttu olla hajapiirkonna majanduslikud kahjud ning juhitava võimsuse osakaalud üledimensioneeritud. Koormused võivad varieeruda ka seoses aastaaegadega, kuna kütteperioodil on Eesti elektritarbimine suurem.

Majandusliku kahju hindamisel on kasutatud kirjanduses avaldatud kõige hilisemaid andmeid, kuid hoolimata sellest kasutatud CENS €/kWh tugineb 2016. aasta andmetele. Lisaks pole arvestatud tööstus-, põllumajandus- ja teenindussektoris katkestuse tagajärjel saamata jäänud rahavoogudega, riknenud kaupadega või kaotatud töötundidega. Võib eeldada, et küberrünnakutest tulenevate katkestuste tegelik majanduslik negatiivne mõju on suurem.

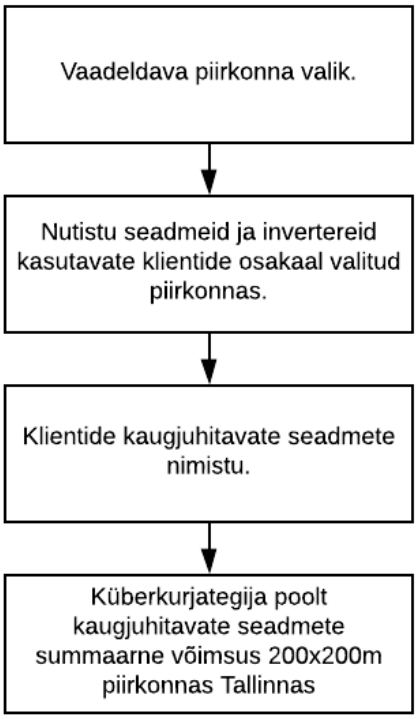
5.2 Küberrünnaku tõttu tekkiv potentsiaalne majanduslik kahju

Puuduvate universaalsete majanduslike mudelite tõttu kasutatakse antud töös küberrünnakutest tuleneva kahju rahaliseks hindamiseks andmata jäänud energia rahalist väärtust. Käsitledes täiendavalt erinevatele majandussektoritele põhjustatavat kahju. Meetod on tänu andmete kättesaadavusele keskmiste arvutamiseks ja ülevaatlike mudelite loomiseks sobiv. Lisaks leiab andmata energia hinna arvutamine kasutamist laialdaselt ka kirjanduses ning on kasutuses ka Eesti elektrivõrgu varustuskindluse hindamisel. [1] [2]

5.3 Küberrünnakuteks sobivate kaugjuhitavate seadmete summaarse võimsuse kujunemine

Antud töös analüüsitavates stsenaariumites koostatakse küberkurjategijate poolt kaugjuhitavate seadmete võimsuste kooslused. Stsenaariumite koostamisel alustatakse piirkonna valikust, milleks on Tallinna linna 200x200m suurusega hajapiirkond ning Tallinna linna 200x200m tihepiirkond. Seejärel määratakse, mitu protsenti vaadeldavas piirkonnas asuvatest klientidest omab kaugjuhitavuse funktsionaalsusega nutistu seadmeid või invertereid. Võrreldakse stsenaariumeid, kus küberrünnaku läbiviimiseks sobivad seadmeid kasutavad 10-75% vaadeldavas priikonnas asuvatest klientidest. Realistliku olukorra loomiseks on kaugjuhitavad võimsused jagatud nelja seadmetegruppi ning on välja toodud tabelis 5.1. Lisaks on joonisel 5.3 jagatud kasutatav seadmete nimistu kolme gruppi osakaalude järgi. Kaugjuhitavate seadmete osakaalud kõikidest vaadeldavas piirkonnas asuvatest kaugjuhitavatest seadmetest varieeruvad vahemikus 10 - 50%.

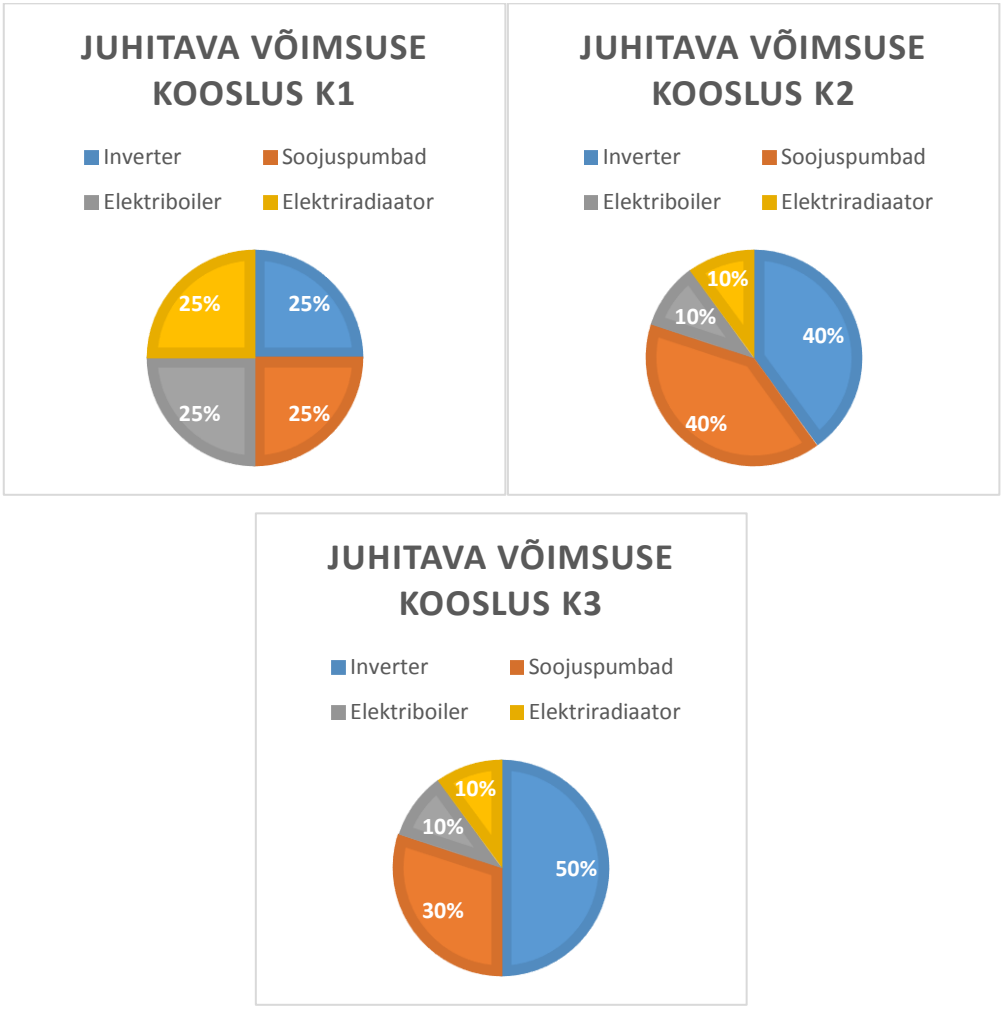
Küberrünnakuks sobiv summaarne kaugjuhitav võimsus saadakse piirkonnas asuvate klientide arvu, kaugjuhitavat võimsust omavate klientide osakaalu, kaugjuhitavate seadmete võimsuse ning kaugjuhitavate seadmete osakaalu korrutise tulemusel.



Joonis 5.2. Küberrünnakuks sobivate kaugjuhitavate seadmete summaarse võimsuse leidmise plokkskeem

5.4 Kolm kaugjuhitava võimsuse kooslust

Töös koostatakse 3 hüpoteetilist kaugjuhitava võimsuse kooslust, mis on sobilikud Eesti elektrivõrku. Kooslused iseloomustavad tabelis 5.1 väljatoodud seadmegruppide osakaalu kõikidest piirkonna kaugjuhitavatest seadmetest. Seejärel implenteeritakse joonisel 5.3 näidatud kooslused Tallinna tihepiirkonda ning Tallinna hajapiirkonda. Eesmärgiga simuleerida tarkvõrgu klientide mitmekesine seadmete nimistu, millel on kaughalduse liides või nutistuga liitmise võimekus. Arvestades iga seadmegrupi osakaalu ning nimivõimsust, leitakse vaadeldavates 200x200m piirkondades asuvate kaugjuhitavate seadmete summaarsed võimsused (kW).



Joonis 5.3 Juhitava võimsuse kooslused 1-3

Juhitava võimsuse koosluses kasutatavad seadmed põhinevad osaliselt varasemates sarnastes uurimustöödes kasutatud seadmetele, näiteks elektriboiler. Analüüsis kasutatakse võimsamaid kodumajapidamises kasutatavaid seadmeid [4]. Lisaks on kooslusesse lisatud

päikeseelektrijaamades, akupankades ja elektriautolaadijates kasutusel olevad alalisvoolu inverterid, mille nimivõimsuseks on valitud 15 kW. Teiste seadmete valik on kohaldatud vastavalt Eesti elektritarbimise iseloomule, kus tähtsal kohal on kütteseadmed. Vaadeldavate seadmete kaughaldus on muutumas populaarsemaks ja klientidele majanduslikult atraktiivsemaks. Seda kinnitab ka punktis 2.2.1 välja toodud elektrivõrkudes kasutatavate nutistu rakenduste ülevaade.

Kõik kaugjuhitavate võimsuste kooslustes kasutatavad seadmed on Eesti turul müüdavad ning hinnanguliselt mediaanvõimsusega ehk välditud on miinimum ja maksimum väärtuseid. Seadmete nimistu ning võimsused paiknevad tabelis 5.1.

Tabel 5.1 Antud töös vaadeldavate kaugjuhitavate seadmete nimivõimsused

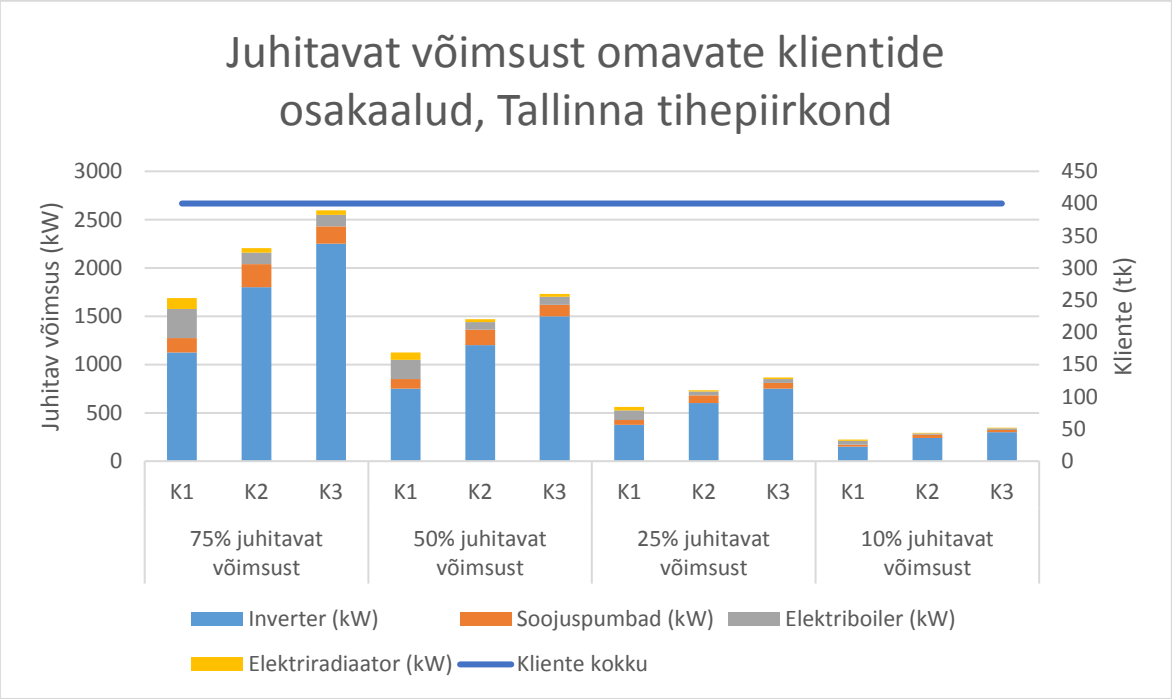
Kaugjuhitav seade	**Nimivõimsus**
Inverter	15 kW
Soojuspumbad [116]	2 kW
Elektriboiler [117]	4 kW
Elektriradiaator [118]	1,5 kW

5.5 Elektrivõrgus toimuva küberrünnaku parameetrid ja potentsiaalsed tagajärjed Tallinna tihe- ja hajapiirkonnas

Antud peatükis koostati kaugjuhitava võimsuse kooslusi kasutades neli stsenaariumit nii Tallinna haja- kui tihepiirkonna kohta. Kahes vaadeldavas 200x200m suurusega Tallinna piirkonnas on kaugjuhitavat võimsust omavate klientide osakaal kõikidest piirkonna klientidest vahemikus 10 - 75%. Eeldusel, et igal kliendil on üks vastav seade. Sellest tulenevalt on joonistel 5.4 ja 5.5 kujutatud igale stsenaariumile kolm vastavat kaugjuhitava koosluse summaarset võimsust. Suurimad summaarsed kaugjuhitavad võimsused tekivad kõrgema inverterite osakaaluga koosluste puhul, mis on põhjustatud inverterite suurimast ühikvõimsusest. Saadud tulemused võimaldavad piirkonna keskmist koormust võrrelda küberkurjategijate poolt ülevõetavate kaugjuhitavate seadmete summaarse võimsusega.

Küberrünnakutest tuleneva luhtunud vara ja katkestuste esinemine on tõenäolisem suuremate summarse kaugjuhitava võimsusega stsenaariumites. Moodustades vaadeldava Tallinna 200x200m piirkonna aasta keskmisest koormusest suurima protsentuaalse osakaalu.

Joonistel 5.4 ja 5.5 selgub, et küberkurjategijatel on teoreetiliselt võimalik kontroll saada 2595 kW summaarse võimsusega kaugjuhitavate seadmete koosluse üle. Seda Tallinna tihepiirkonnas, kus 75% klientidest kasutavad nutistu seadmeid ja invertereid. Hajapiirkonnas on sama stsenaariumi korral summaarne kaugjuhitav võimsus 162 kW. Moodustades vastavalt 26% ja 16,2% piirkondade aasta keskmisest koormusest.



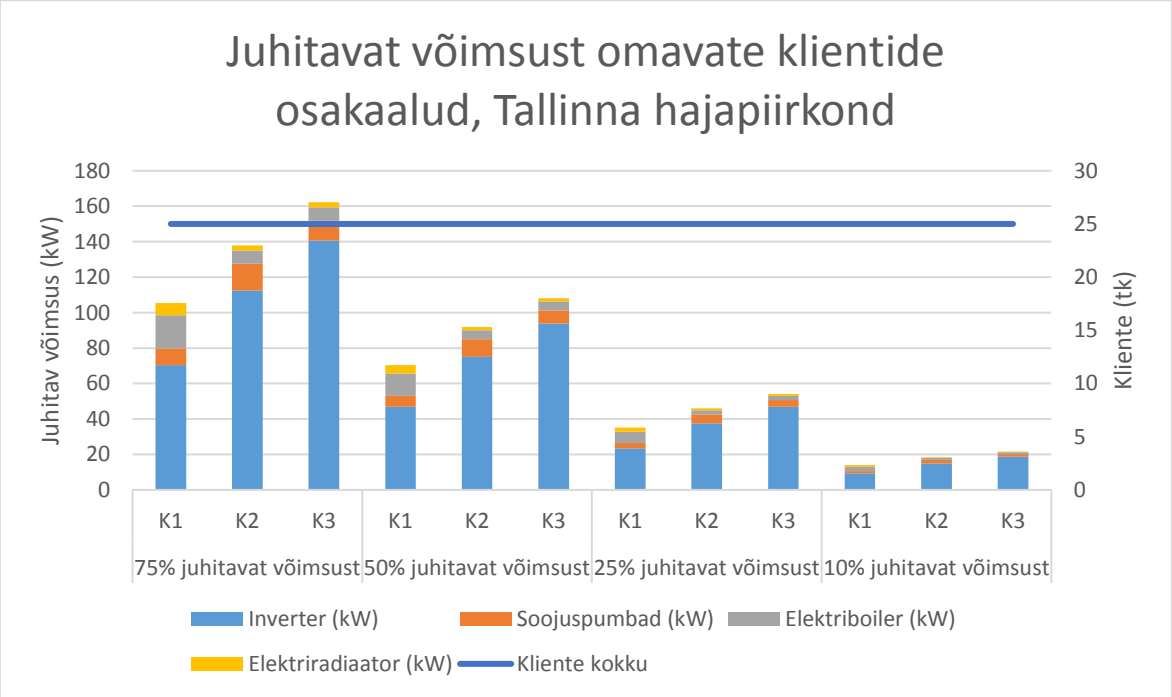
Joonis 5.4 Neli Stsenaariumit kaugjuhitava võimsuse kooslustele Tallinna tihepiirkonnas

Tabel 5.2 Neli Stsenaariumit kaugjuhitava võimsuse kooslustele Tallinna tihepiirkonnas

Kaugjuhitavaid seadmeid kasutavate klientide osakaal piirkonnas %	**Kliente (tk)**	**Summaarsed kaugjuhitavad võimsused (kW)**		
		K1	**K2**	**K3**
75%	300	1688	2205	2595
50%	200	1125	1470	1730
25%	100	563	735	865
10%	40	225	294	346

Joonisel 5.4 ja tabelis 5.2 selgub, et kõige suurem summaarne kaugjuhitav võimsus tekib stsenaariumi korral, kus kaugjuhitavaid seadmeid on 75% klientidest. Vaadeldavas Tallinna

tihepiirkonnas on võimalik 300 kliendi kaugjuhitavaid seadmeid pahatahtlikult lülides tekitada potentsiaalselt 2595 kW suurune võimsuse kõikumine. Moodustades 26% vaadeldava piirkonna keskmisest koormusest. Juhitava võimsuse osakaal koormusest võib suureneda või väheneda sõltuvalt aasta- ning kellaajast. Seadmete korduval lülimisel tekivad sõltuvalt seadme omadustest kuni 15 kordsed tõukevoolud võrreldes tavatalitusega [119] [120] [121] [122]. Reeglina on nii suurte tõukevoolude tekke välistamiseks kasutusel sagedusmuundurid. Välja toodud võimsuse ja voolu kõikumine on piisav, et põhjustada releekaitse tööd või kahjustusi seadmetele.



Joonis 5.5 Neli Stsenaariumit kaugjuhitava võimsuse kooslustele Tallinna hajapiirkonnas.

Tabel 5.3 Neli Stsenaariumit kaugjuhitava võimsuse kooslustele Tallinna hajapiirkonnas

Kaugjuhitavaid seadmeid kasutavate klientide osakaal piirkonnas %	**Kliente (tk)**	**Summaarsed kaugjuhitavad võimsused (kW)**		
		K1	**K2**	**K3**
75%	19	105	138	162
50%	13	70	92	108
25%	6	35	46	54
10%	3	14	18	22

Joonisel 5.5 ja tabelis 5.3 on tulemused Tallinna hajapiirkonna kaugjuhitava võimsuse osakaalude kohta. Kõige suurema osakaaluga ehk 19 kliendiga stsenaariumi puhul on kaugjuhitava võimsuse

osakaal aasta keskmisest koormusest 16,2% ning kõige konservatiivsema kooslusega 1,4%. Seega on kaugjuhitava võimsuse pahatahtliku lülimise tõttu tekkinud katkestuste või luhtunud vara esinemise tõenäosus väiksem kui tihepiirkonnas. Hajapiirkondade puhul võivad suuremat rolli mängida ka aastaajad.

5.5.1 Juhitava koormuse ohud Tallinna näitel

Töös vaadeldavas 400 kliendiga Tallinna tihepiirkonnas, mille suurus on 200x200m piisab küberkurjategijal katkestuste või kahjude tekitamiseks tõenäoliselt kahest analüüsitud stsenaariumist. Esimesel juhul, kui tihepiirkonna 400 kliendist 200 ehk 50% kasutab kaugjuhitavaid nutistu seadmeid ja invertereid ning teisel juhul, kui sarnaste klientide osakaal on 75%. Taolise küberrünnaku eesmärgiks on kaaperdatud seadmete korduv õigeaegne lülimine, põhjustades seeläbi klientidele majanduslikku kahju nii potentsiaalselt luhtunud vara kui andmata jäänud energia kujul. Vaadeldav 200x200m piirkonna kontsentreeritus põhjustab ohu, et lülimistel tekkiv voolu, pinge ja võimsuse kõikumine võib mõjutada üksnes kindlat jaotusalajaama, liini või maakaablit. Luues seeläbi suuremad eeldused võrguettevõtte vara kahjustamiseks ning pikema kestusega katkestuste tekkeks.

Koormuse kiirel ja korduval muutumisel põhjustavad voolukaitsed rakendudes katkestusi ning erandjuhtudel pingest lähtuvad mõõteahelate rikked ja sageduskaitseautomaatika. Rakenduda võivad järgnevad releekaitse funktsioonid:

- Liigvoolukaitse
- Suunatud voolukaitse
- Lühisvoolukaitse
- Pinge muutustest tingitud mõõteahelate rikked
- Sagedusautomaatika

Juhul kui teostada tihedaid juhitavate koormuste lülitamisi on võimalik kahjustada ka klientide ja võrguettevõtete seadmeid. Põhjustades seeläbi ajutisi või pikemaid elektrikatkestusi ning häiringuid elektrivõrgu töös. Põhilised riskigruppi kuuluvad seadmed on järgnevad:

- Maakaablid, kaablimuhvid
- Trafod

- Jaotusvõrgu klientide seadmed ja inverterid

Kahjustused võrguettevõtete seadmetele on tõenäolisemad suveperioodil, mil välitemperatuurid on kõrgemad. Lisaks otsestele seadmete riketele põhjustavad nominaalväärtusest kõrgemad voolud ja võimsused seadmete isolatsiooni kahjustusi. Tuues seeläbi kaasa seadmete eluea lühenemise. Korduva kaugjuhitavate seadmete lülimisega on võimalik ründajatel vältida ka taaslülitusautomaatika (TLA) korrektset tööd, kui taaslülitamist teostatakse 1-2 korda.

5.6 Küberrünnakust põhjustatud majanduslik kahju Tallinna tihe- ja hajapiirkonnas

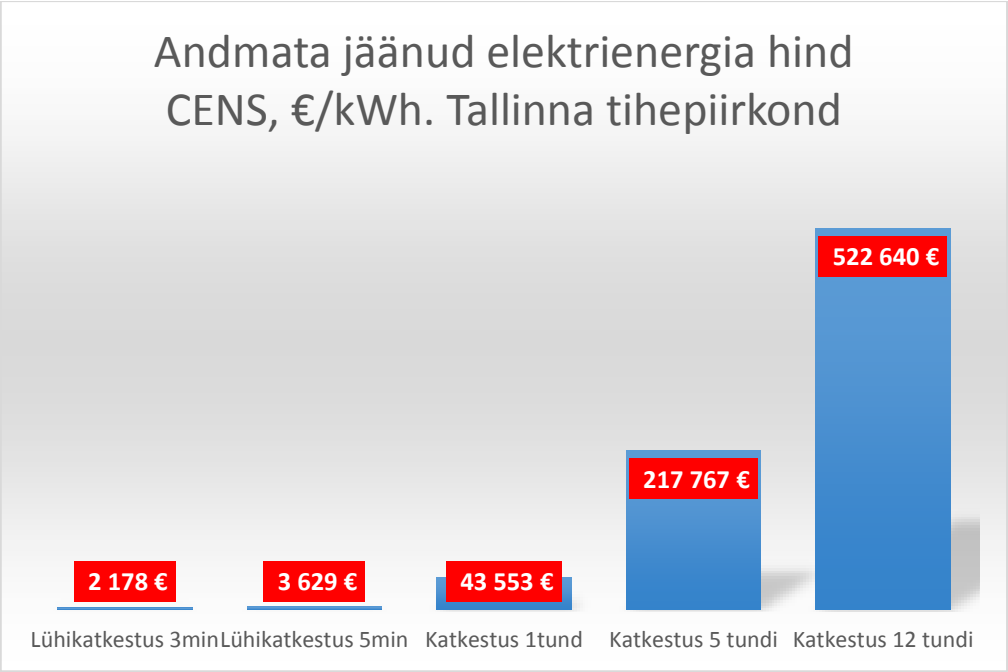
Tabelis 5.4 välja toodud varustuskindluse piirkondade andmata jäänud energia hinna abil saab leida küberrünnakutest põhjustatud katkestuste kahju. Eeldades, et kaugjuhitav võimsusus on küberkurjategijate kontrolli all ning kuritahtlike lülimistega põhjustatakse elektrikatkestusi tervele piirkonnale või üksikutele klientidele. Tulemusena on varustuskindluse piirkonna järgi arvutatud katkestustest tulenevad keskmised majanduslikud kahjud, mida illustreerivad joonised 5.6 ja 5.7.

Tabel 5.4 Varustuskindluse piirkondade järgi CENS, EUR/kWh

Piirkond	**CENS, €/kWh**
Ülitihepiirkond	4,50 €
Tihepiirkond	4,36 €
Hajatihepiirkond	4,00 €
Hajapiirkond	4,33 €

Matemaatilises mudelis on lähtutud varustuskindluse piirkonnas paiknevate tarbijasektorite elektrienergia tarbimise osakaaludest. Võttes arvesse ka tarbijasektori põhist andmata jäänud energia hinda. Näiteks on arvutatud ülitihe piirkond:

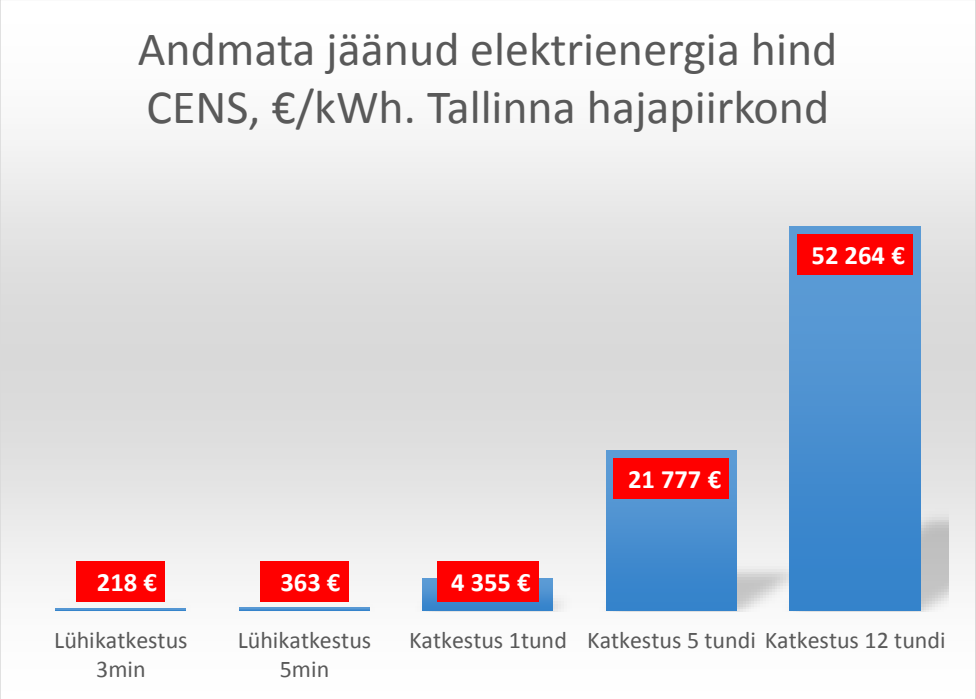
$$\text{Ü}litihepiirkond\ (\frac{EUR}{kWh}) = 4{,}79 * 0{,}47 + 4{,}32 * 0{,}52 + 2{,}42 * 0{,}01 = 4{,}50€$$



Joonis 5.6 Küberrünnaku tõttu andmata jäänud elektrienergia hind EUR/kWh, tihepiirkonnas Tallinnas, 200x200m alal.

Joonisel 5.6 vaadeldavas 200x200m Tallinna tihedas varustuskindluse piirkonnas on keskmiseks tunnitarbimiseks arvestatud 10 000 kWh. Lühikatkestuste puhul saab eeldada, et jaotusvõrgu või muudele elektrifitseerimisseadmetele püsivat kahju ei põhjustatud ning elektriühenduse saab kiirelt manuaalselt või TLA-ga taastada. Kõige lühema katkestuse puhul jääb 400-le tihepiirkonna kliendile edastama 500 kWh ulatuses elektrienergiat, tekitades kolme minutiga kahju 5,45 EUR/klient.

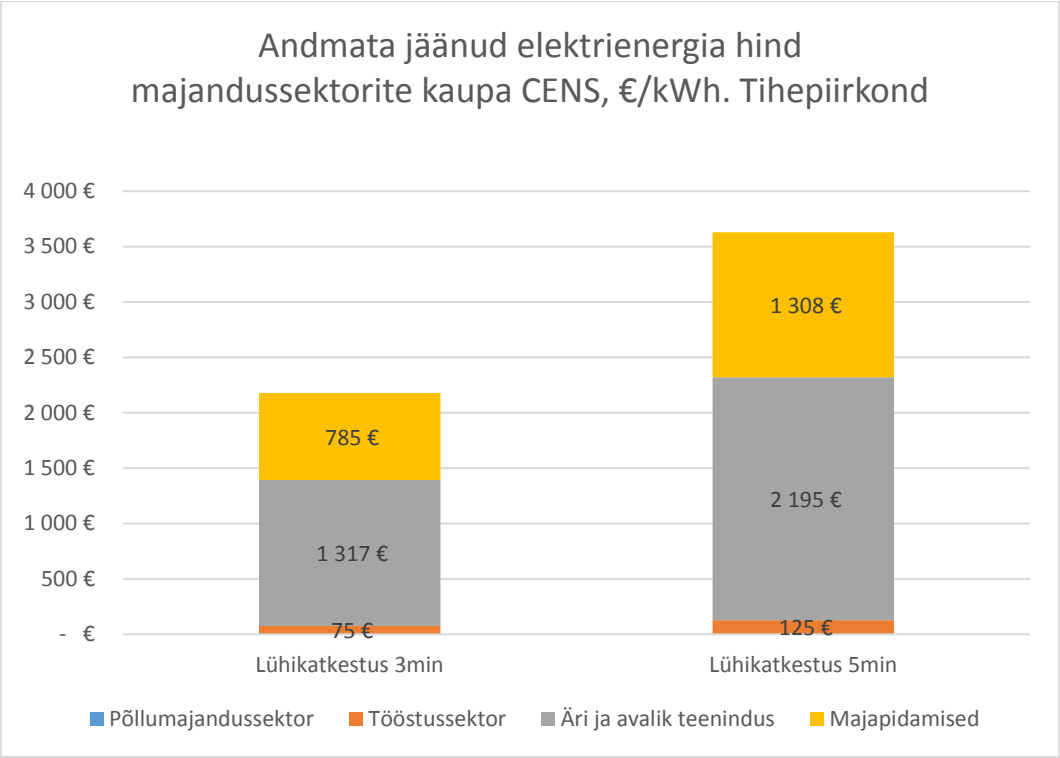
Tallinna 200x200m hajapiirkonnas joonisel 5.7 on arvestatud keskmise tunnitarbimisega 1000 kWh. Kõige lühema katkestuse stsenaariumi korral jääb edastamata 50 kWh elektrienergiat 25-le kliendile. Seeläbi kujuneb ühe kliendi 3minutilise katkestuse hinnaks keskmiselt 9 EUR/klient, mis on 40% suurem võrreldes tihepiirkonna kliendi kuluga. Varustuskindluse piirkondade vahe tuleneb põhiliselt asjaolust, et kasutatav andmata energia meetod hindab kodutarbijatele edastama jäänud elektrienergiat kõige kallimaks. Teisalt on vaadeldavas hajapiirkonnas katkestuste põhjustatud summaarsed kulud tunduvalt odavamad, kuna piirkonna elektritarbimine moodustab tihepiirkonna elektritarbimisest kümendiku.



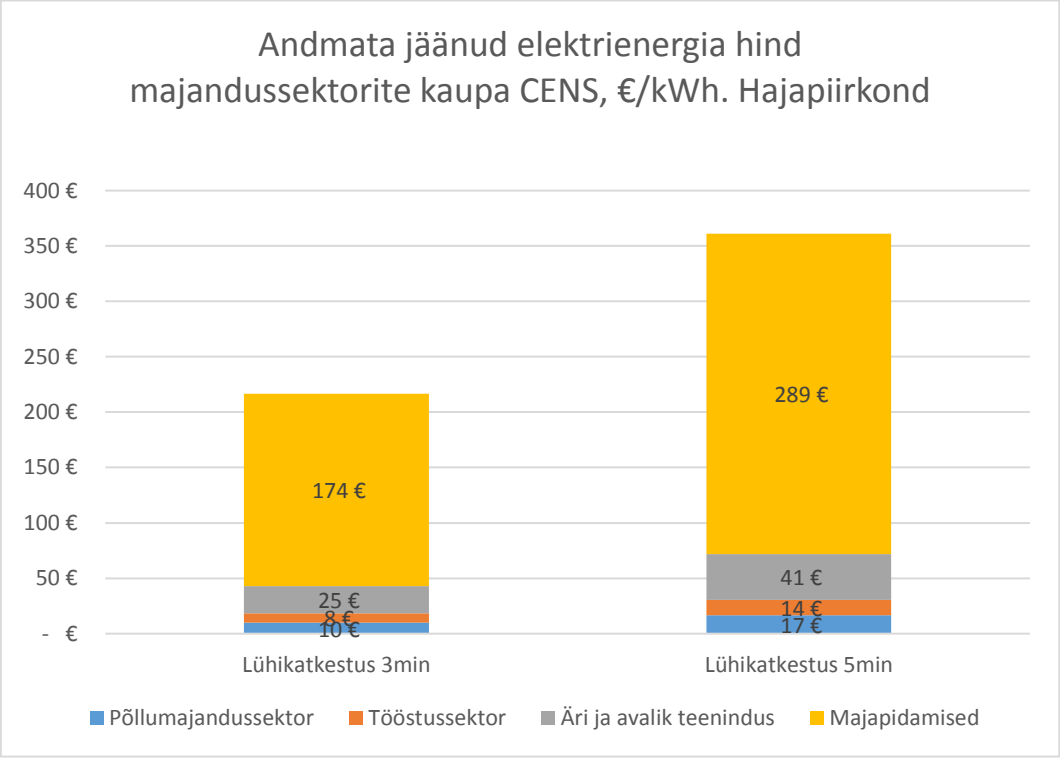
Joonis 5.7 Küberrünnaku tõttu andmata jäänud elektrienergia hind EUR/kWh, hajapiirkonnas Tallinnas, 200x200m alal.

Tabelites 4.2 ja 4.3 on välja toodud tarbijasektori energiatarbimine vastavalt varustuskindluse piirkonnale ning andmata jäänud energia hind vastavalt majandussektorile. Seeläbi on arvutatud küberrünnakust põhjustatud elektrikatkestuse hind Eesti majandussektorite põhiselt. Katkestustest tulenevad kulud majandussektorite kaupa on välja toodud joonistel 5.8-5.11.

Põllumajanduse osakaal on joonisel 5.8 vaadeldavas Tallinna 200x200m tihepiirkonnas 0,03%. Seetõttu pole sektori rahalist kaotust kuvatud. Eesti tihepiirkonda iseloomustab suur kodutarbijate ja teenindussektori osakaal. Seega põhjustatakse 3 minutiga piirkonna teenindussektori 111 kliendile kahju ulatuses 12 EUR/klient ning 5 minutiga 20 EUR/klient. Kodutarbijatele 3 minutiga 2,7 EUR/klient ning 5 minutiga 4,5 EUR/klient. Suure elektritarbimise ja väikese tööstusklientide osakaalu tõttu tekitab küberrünnakuga tekitatud katkestus tööstustarbijatele kahju 3 minutiga 37,5 EUR/klient ning 5 minutiga 62,5 EUR/klient.

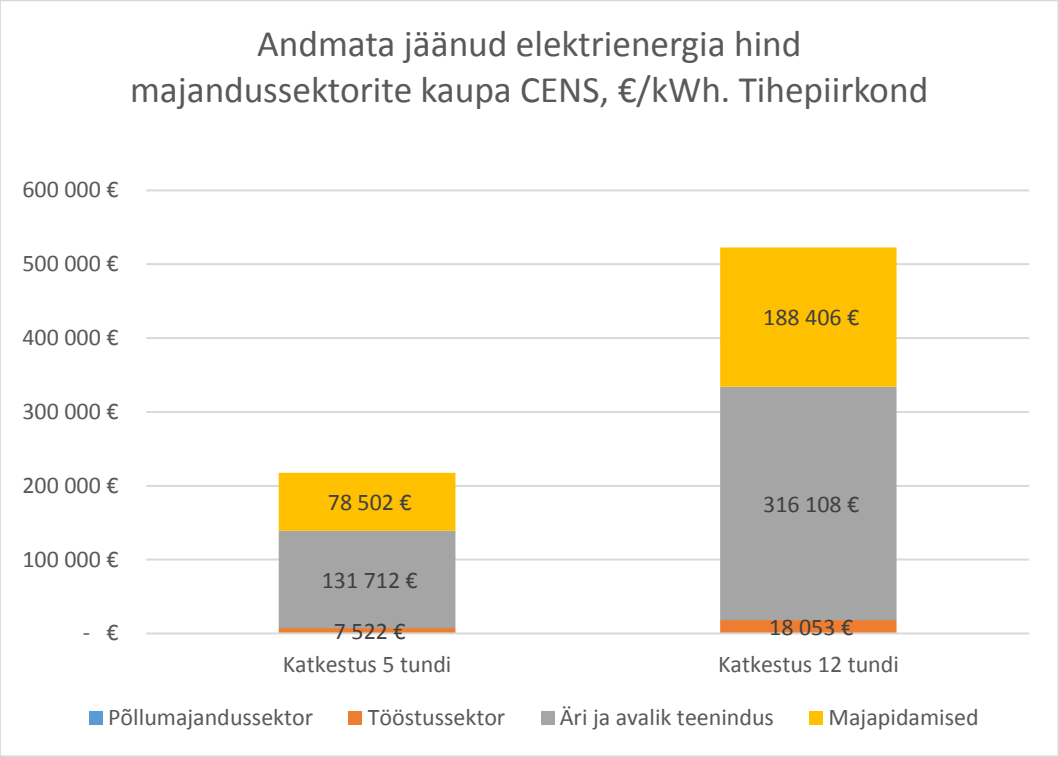


Joonis 5.8 Küberrünnaku majandussektoritele põhjustatud kahju Tallinna tihedas varustuspiirkonnas CENS, EUR/kWh



Joonis 5.9 Küberrünnaku majandussektoritele põhjustatud kahju Tallinna haja varustuspiirkonnas CENS, EUR/kWh

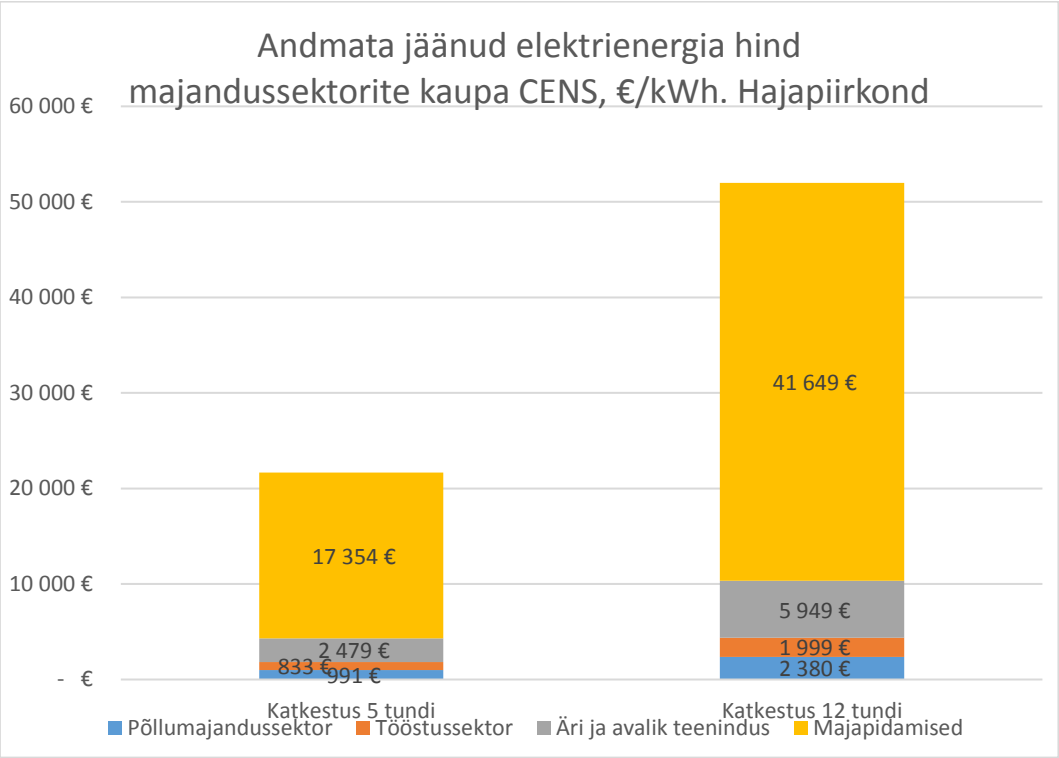
Joonisel 5.9 kuvatud hajapiirkonnas on 90% klientidest kodutarbijaid. Seega 3 minutilise katkestusega põhjustatakse 23-le kodutarbijale kahju 7,5 EUR/klient ning 5 minutilise katkestusega 12,6 EUR/klient. Arvestades, et teenindustarbijaid on hajaastuses ainult 5%, siis tekib kahju 3 minutiga 25 EUR/klient ning 5 minutiga 41 EUR/klient. Vastavalt 48% rohkem kui tihepiirkonnas. Erinevalt tihepiirkonnast on hajapiirkonnas arvestatav elektritarbise osakaal ka põllumajandussektoril. Põhjustades sektorile kahju 3 minutiga vähemalt 10 EUR/klient ning 5 minutiga vastavalt 17 EUR/klient. Kuna töös vaadeldav hajapiirkond asub Tallinnas, siis reaalne põllumajanduse osakaal kogu piirkonna elektritarbimist võib olla väiksem.



Joonis 5.10 Küberrünnaku majandussektoritele põhjustatud kahju Tallinna tihedas varustuspiirkonnas CENS, EUR/kWh.

Eelnevalt välja toodud joonisel 5.10 pikkade katkestuse 5 ja 12 tundi stsenaariumi korral peab rünnaku järel olema takistatud võrguühenduse taastamine. See võib näiteks olla põhjustatud jaotusvõrgu või kliendi elektriseadmete püsivast kahjustusest. Antud stsenaarium on ekstreemne näide ning esinemise tõenäosus väike. Teenindustarbijatele 5 tunniga ja 12 tunniga põhjustatud kahjud on vastavalt 1187 EUR/klient ja 2849 EUR/klient. Tööstustarbijatele 5 tunniga ja 12 tunniga põhjustatud kahjud on vastavalt 3671 EUR/klient ja 9026 EUR/klient. Pikaajaliste katkestuste puhul võivad kaasneda lisaks elektrivarustuse tõttu tegemata jäänud äriprotsesside kahjudele ka riknenud

kaubad, kadunud dokumendid, purunenud seadmed ning muud ressursid, mis suurendavad majanduslikku kahju veelgi.



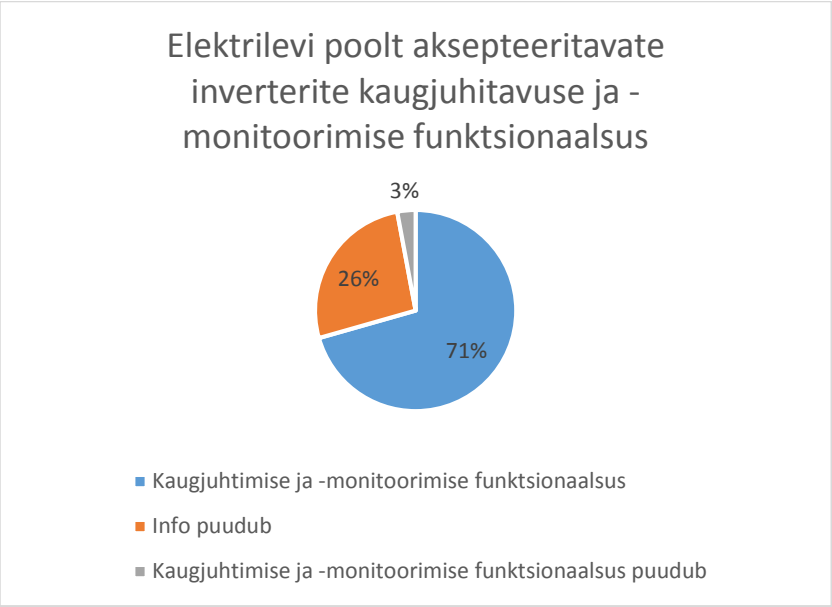
Joonis 5.11 Küberrünnaku majandussektoritele põhjustatud kahju Tallinna haja varustuspiirkonnas CENS, EUR/kWh.

Joonis 5.11 toob välja 5 tunni ja 12 tunni kodutarbijate kulud, mis on vastavalt 694 EUR/klient ja 1810 EUR/klient. Tõenäoliselt ei saa nii pika katkestuse puhul CENS meetodit rakendada, kuna majanduslik kulu kodutarbjale muutub ebaproportsionaalselt suureks. Teenindussektori puhul on 5 tunni ja 12 tunni majanduslik kahju vastavalt 833 EUR/klient ja 1999 EUR/klient ning põllumajanduses vastavalt 991 EUR/klient ja 2380 EUR/klient. Sõltuvalt hooajast võib kahjusid põllumajandussektorile suurendada näiteks viljakuivatite seiskumine.

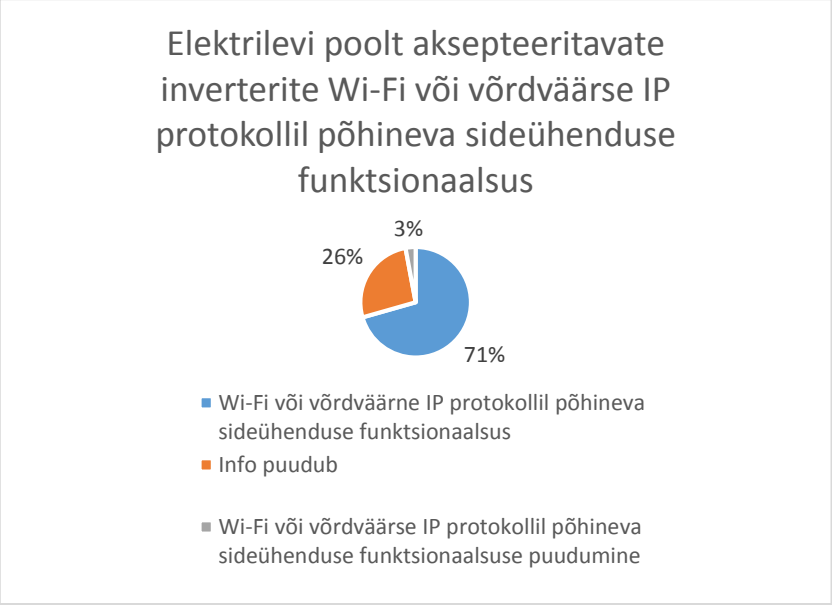
5.7 Elektrilevi OÜ lubatud inverterid väiketootjatele

Joonisel 5.12 selgub, et 34-st Elektrilevi poolt aksepteeritavast inverterist või seadmest on kaugjuhtimise ja kaughalduse funktsionaalsus 71%. Arvestades, et 26% seadmete kohta puudub avalik info või on tootmine erinevatel põhjustel lõpetatud, võib kaughaldusega seadmete osakaal olla suurem kui 71%. Analüüsitud nimekirjas on vaid üks inverter, millel puudub kaugjuhtimise ja kaugmonitooringu funktsionaalsus. Paljud inverterite tootjad võimaldavad internetiga ühendatud inverterites kaugjuhtimist teostada ka seadmete paigaldajal või tootjal. Kasutades selleks peamiselt

pilveteenuseid. Suurendades seeläbi seadmetele mitte sihipärase ligipääsu saamise võimalust kolmandatel osapooltel. Enamusel kaughalduse funktsionaalsusega inverteritel on vaikeparoolid, mis on kõigile vabalt kättesaadavad tootjate kodulehtedel.



Joonis 5.12 Elektrilevi poolt aksepteeritavate inverterite kaugjuhtimise ja –monitooringu funktsionaalsus



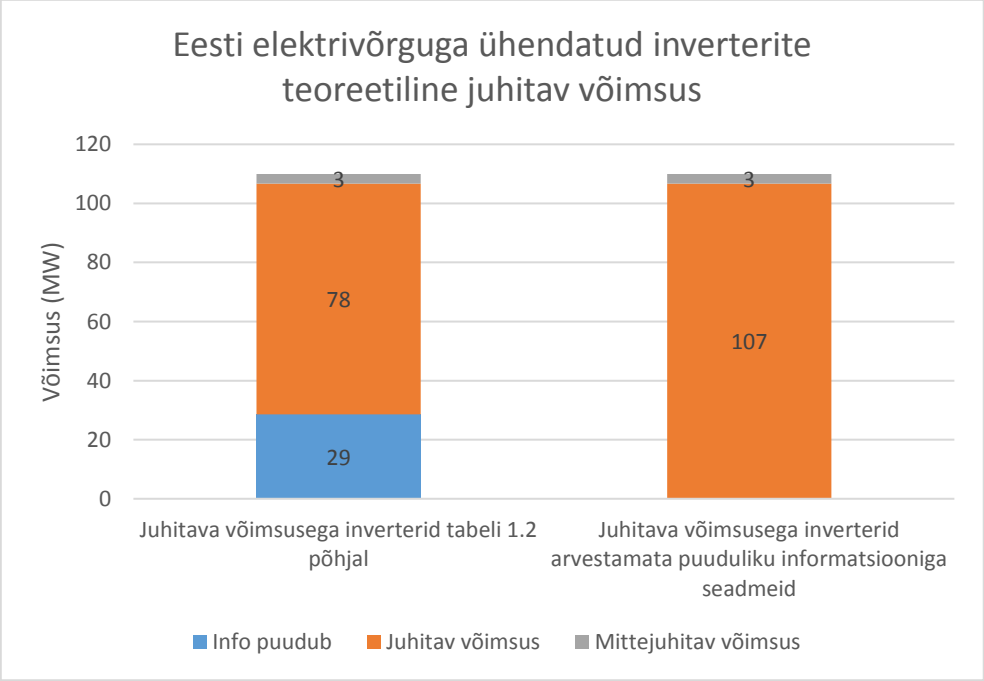
Joonis 5.13 Elektrilevi poolt aksepteeritavate inverterite WiFi või võrdväärse IP protokollil põhineva sideühenduse funktsionaalsus

Joonisel 5.13 on näha, et Wi-Fi funktsionaalsus inverterite puhul kattub kaugjuhitavusega. Wi-Fi võrkude küberturvalisuse puudusi on korduvalt tõestatud näiteks Starbucks-i, American Airlinesi ja TalkTalki võrkudesse ligipääsu saades [123]. Samuti on WiFi võrgud ligipääsetavad hoolimata kasutatavatele krüpteeringutele nagu näiteks WEP, WPA, WPA2. [124]

5.7.1 Inverteritega võimalik kaasnev kahju

Päikeseelektrijaamade osakaalu kasvuga kogu tootmisvõimsusest suureneb alalisvoolu inverterite osatähtsus elektrisüsteemis tervikuna. Kitsendusena saab eeldada, et põhivõrguga liidetud ning alates 200 kW nimivõimsusega päikeseelektrijaamade puhul kontrollivad ja reguleerivad seadmete funktsionaalsust põhi- ja jaotusvõrgu operaatorid. Vähendades lihtsamaid turvariske, kuigi jaotusvõrgus on kasutusel samad seadmed, mis mikrotootjatel alla 200 kW. Joonistel 5.14 ja 5.15 on välja toodud inverteritega seotud andmed ja suhtarvud.

Jaotusvõrku lubatavate inverterite analüüsist joonisel 5.13 tulenevalt on keelatud osapooltelt võimalik üle 70% päikeseenergia tootmisüksustele ligipääseda ja tööd kontrollida. Omades seeläbi võimekust tekitada jaotusvõrgus kui ka põhivõrgus häire- või rikketalitlus. Kurjategijal on võimalus manipuleerida inverteris reaktiivvõimsuse ja seeläbi pingega. Seadmete korduv lülimine põhjustab võimsuse kõikumisi, tuues kaasa potentsiaalseid probleeme elektrisüsteemi sagedusele. Samuti saab küberrünnaku tagajärjel majanduslikku kahju päikeseelektrijaama omanik, kas edastamata jäänud elektrienergia või rikutud seadmete kujul.

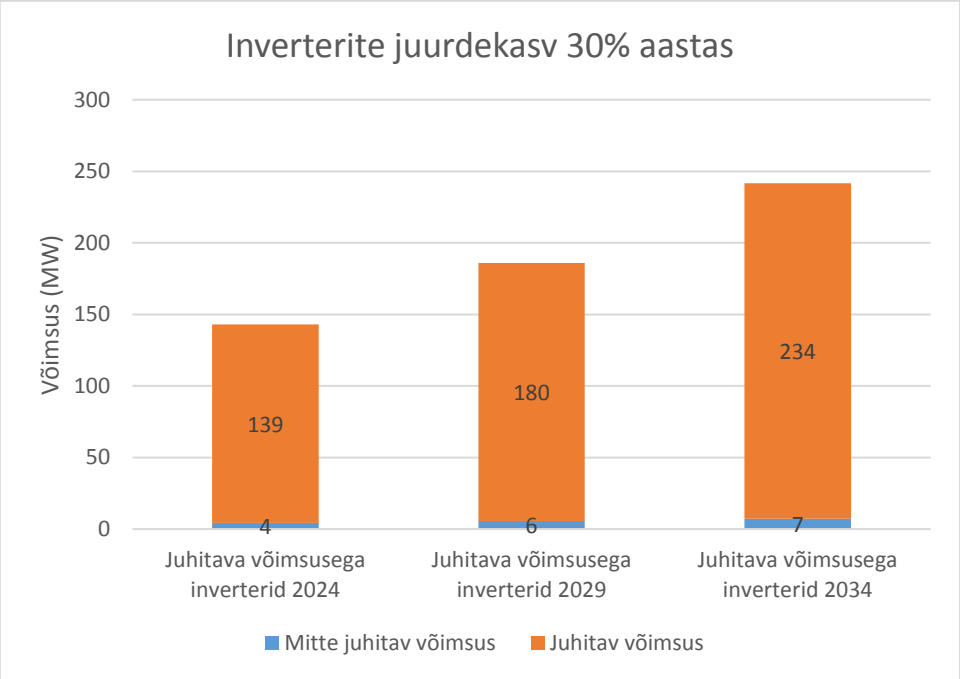


Joonis 5.14 Teoreetiline kaughaldusega inverterite võimsus Eesti elektrivõrgus

Joonisel 5.14 välja toodud kaughalduse funktsionaalsusega inverterite nimivõimsus on 78 MW ning eeldades, et puuduliku informatsiooniga vähetuntud seadmete osakaal on minimaalne võib kaugjuhitavate inverterite nimivõimsus ulatuda 107 MW-ni.

Aastatel 2015–2018 oli keskmine päikeseelektrijaamade ning seeläbi ka inverterite juurdekasv 476%, mis oli suuresti tingitud 2018. aasta detsembris lõppenud taastuvenergia toetustest ning 100 MW tootmisvõimsuse lisandumisest 2018. aasta jooksul. Päikeseelektrijaamade võimsus kasvas üle 1000%-i [125] [126] [8]. Sellele lisanduvad täiendavalt teised seadmed nagu näiteks akupangad ja elektriautode laadijad, mis kasutavad samuti sarnaseid invertereid.

Antud suuruses tootmisvõimsuse kasvu tõenäoliselt enam oodata ei ole. Seetõttu lähtutakse antud töös Eesti tuleviku päikeseenergia tootmisvõimsusi prognoosides EL-i päikeseenergia juurdekasvu prognoosidest. Päikesenergia keskmine aastane juurde kasv on EL-is olinud viimastel aastatel ligi 40% [127].



Joonis 5.15 Teoreetiline kaughaldusega inverterite juurdekasv.

Päikeseenergia osakaalu kasv tootmisüksustes on olnud EL-is keskmiselt 40%, kuid toetuste kadumise ja pika vaadeldava perioodi tõttu ning Eesti geograafilist asukohta arvesse võttes, on valitud aastaseks juurdekasvuks konservatiivselt 30% viie aasta jooksul. Joonisel 5.15 on välja toodud teoreetilise juhtava võimsuse osakaalu lisandumine Eesti elektrivõrku. Arvestades, et 2017. aasta suveperioodi keskmine netogenereerimine oli 1185 MW, moodustavad tuleviku prognoosid

vastavalt 12%, 15% ja 20% kogutootmisvõimsusest. Minimaalsest suvisest netogenereerimisest moodustab 2034. aasta prognoos 56%. Sellise osakaaluga võimsuse pahatahtlik lülimine võib põhjustada tõsiseid häiringuid Eesti elektrisüsteemis.

5.8 Küberturvalisusest lähtuv Eesti elektrivõrku reguleeriva seadusandluse analüüs

Suure tähtsusega tarkade elektrivõrkude küberturbe arengus on seadusandlus. Seadusandlus loob turuosalistele regulatsioonid, välistab ebausaldusväärsete tootjate seadmed ning suunab sektori arengut ühiskonna ja riigi huvidest lähtuvalt. Õigusruum erineb riigiti, kuid sarnastel põhimõtetel toimiva energeetikasektori kitsendatud tarkvõrkude seadusandlust on tänu riikide sarnasele funktsionaalsusele võimalik võrrelda. Teiste riikide pretsedentidest ja vigadest on võimalus õppida. Samuti kuulub Eesti EL-i, mille direktiivid ja seadusandlus kohaliku energeetikasektori õigusruumi kujundab.

Analüüs Eesti elektrivõrku reguleeriva seadusandluse tugevuste, nõrkuste, võimaluste ja ohtude kohta võrreldes teiste riikidega viiaks läbi *SWOT* (Tugevused, nõrkused, võimalused, ohud) meetodil.

Tugevused:

Eestis on elektrivõrku ühendatavate seadmete funktsionaalsuse ja omaduste reguleerimiseks kasutusel mitmeid seaduseid, näiteks võrgueeskiri, seadme ohutuse seadus ja elektrituruseadus. Tänu sellele tekib hästi reguleeritud ning lihtsasti täiendatav keskkond küberturvalisust arvestavate aspektide lisamiseks.

Euroopa Liidu direktiiv (EL) 2016/1148, mis kohustab liikmesriike koostama küberturvalisuse arengukava. Selle tulemusel koostab Eesti regulaarselt küberturvalisuse strateegiat.

Euroopa Liidu arengukavad ja riikidevahelise koostöö soodustamine tagab elektrivõrkude ühtlasema ning ajakohasema arengu kogu EL-is. Stimuleerides liikmesriike tegema koostööd nii tarkvõrgu, küberturvalisuse kui elektrivõrgu strateegilisel arendamisel.

Küberturvalisuse seadusega kehtestatakse, et elektriga varustamine liigitub elutähtsa teenuse alla. Sellest tulenevalt on teenuse pakkuja kohustatud rakendama meetmeid küberintsidentide ennetamiseks ja lahendamiseks.

Nõrkused:

Ükski täna kehtiv seadus ei reguleeri elektrivõrku lisatavate seadmete küberturvalisuse aspekte. Seadme ohutuse seaduses sätestatakse seadmetöö ja seadmete kasutamisel vajalik ohutus keskkonnale, inimese tervisele ning elule. Võrgueeskiri sätestab, millised releekaitsefunktsioonid ning elektrotehnilised parameetrid on nõutavad.

Elektrivõrgu talitlust reguleeriv seadusandlus ei arvesta, et seade võib olla ohtlik keskkonnale, tervisele või elektrivõrgule ka puuduliku küberturvalisuse tõttu.

Eesti küberturvalisust tervikuna reguleeriv küberturvalisuse seadus laieneb üksnes digitaalse ja elutähtsa teenuse osutajale, mis välistab suurema osa päikeseelektrijaamasid paigaldavatest ja haldavatest ettevõttevõtetest. Samuti ei laiene seadus väikestele ettevõtetele, milles aastane käive või bilansimaht on alla 10 MEUR ning pakub tööd vähem kui 50 inimesele.

Võimalused:

2019–2022 küberturvalisuse strateegias on eraldi tegevussuunana välja toodud, et ühiskonnale kriitilise tähtsusega sektoris, sealhulgas energeetikasektoris tegutsevad spetsialistid, peavad erialased küberoskused kätte saama tasemeõppe alusel. Võimaldades vertikaalset küberturvalisuse integreerimist haridusasutusest kuni ettevõteteni.

Eestis on päikeseelektrijaamade osakaal kogu tootmisvõimsusest alla 5% ning nutistu integreerimine elektrivõrku algfaasis. Elektrivõrkude tulevikuarenguid silmaspidava seadusandluse loomiseks on tegemist ideaalse keskkonnaga, mis areneks ja täieneks koos sektoriga ning väldiks hilinenud reguleerimisest tulenevaid ebatäpsusi.

Võimalus on rakendada California ja Ühendkuningriigi näitel hea tava või nutistu seadmetele laienevaid seaduseid, millega vähendada küberriske elektrivõrgus tervikuna. Esialgu piisab regulatsioonidest, et antud seadmeid paigaldavad ettevõtted on kohustatud muutma tehases sätestatud paroole ja kasutajatunnuseid. California näitel on võimalus tulevikus rangemaid regulatsioone võtta kasutusele.

Euroopa Liidu liikmesriigid võtavad kasutusele ühised standardid nutistu ja teiste elektrivõrku integreeritavate seadmete reguleermiseks. Luues seeläbi paremini reguleeritud ja turvalisema turukeskkonna.

Ohud:

Euroopa Liidu direktiivid, mis ei pruugi arvestada täielikult Eesti elektrivõrgu iseärasustega. Näiteks ei kohaldata Euroopa Komisjoni soovitusel küberturvalisuse seadust väike- ega mikroettevõtetele. Raskendades ühtlase küberohutustest lähtuva sektori kujunemist.

Suurde BRELL-i elektrisüsteemi kuulumine tekitab mugavustunnet ning väikesemad potentsiaalsed riskid elektrivõrgu seisukohast ei saa piisavalt tähelepanu.

Võrgueeskirja viimane redaktsioon 27.04.2019 ei arvesta endiselt ühtegi küberturvalisusest tulenevat aspekti. Seega võib vastava sisuga muudatuste elektrivõrku reguleerivasse seadusandlusesse sisse viimine võtta veel aastaid.

Esimeste küberturvalisust arvestavate seadusmuudatusteni elektrivõrgu õigusruumis viib küberrünnaku tagajärg, mitte soov ennetada.

5.9 Ohud kaughalduse ja –juhtimise funktsionaalsusega seadmete Eesti elektrivõrku lisamisel

Joonisel 5.2 ja 5.3 välja toodud mudeli progressiivsemate stsenaariumite korral on kontsentreeritud piirkonnas avalike võrkudega ühendatud juhitavate seadmete koondvõimsuse osakaal 26% piirkonna keskmisest koormusest. Seeläbi tekib küberrünnakut läbiviival osapoolel näiteks, *hacktivistil*, organiseeritud küberkurjategijal või mõne riigi poolt toetatud organisatsioonil potentsiaalne võimalus tekitada häiringuid piirkonna elektrivarustusele. Tuues seeläbi endaga kaasa edastamata jäänud energia kulu ning täiendava majandusliku kahju luhtunud vara näol.

Üksikut või väikest gruppi kliente puudutavat elektrikatkestust või päikeseelektrijaama tootmise seisakut on lihtsam tekitada ning majanduslikud kahjud on enamasti minimaalsed. Võrguettevõtete varade kahjustamine ning suuremate katkestuste põhjustamine läbi nutistu seadmetele ja inverteritele suunatud küberrünnaku on tõenäolisem suveperioodil. Sõltudes kõrgemast välistemperatuurist. Olukorras, kus piirkonna koormus on aasta keskmisest väiksem võib kaugelt juhitava koormuse osakaal olla üle 26%, tekitades ajutisi voolutõukeid ja pingelange. Ebakorrektselt toimiva trafo temperatuurikaitse korral põhjustaks situatsioon isolatsiooni kahjustusi, trafo rikke, maakaabli muhvi purunemise või releekaitseautomaatika rakendumise. Tuues klientidele kaasa potentsiaalselt mitmetunnilisi elektrikatkestusi.

Inverterite analüüsi tulemusel selgub, et elektrivõrku lubatavate inverterite nimekirjast puudub erinevatel põhjustel info 26% seadmete kohta. Põhjusteks näiteks ettevõtte tegevuse lõpetamine, seadmete tootmise lõpetamine või avaliku info puudumine. Olukorras, kus installeeritud võimsus

peaks jagunema lubatavate inverterite vahel võrdselt, on Eesti elektrivõrgus ligi 24 MW tootmisvõimsust, millel puudub igasugune tootjatugi. Tänase seadusandluse kohaselt võib 15 aasta pärast olla Eesti elektrivõrgus üle 200 MW kaugelt juhitavat võimsust, mille kasutajatunnused ja paroolid on internetis vabalt kättesaadavad. 3% kaugjuhtimise funktsionaalsuseta inverteritest moodustab Poola väiketootja Twerd, mille seadmed on turul pigem vähem levinud.

Nutistu seadmete küberründamine ning kuritegelik kasutamine on maailmas laialt levinud. 2016 aasta Mirai *botnet*-i rünnakud koosnesid rohkem kui miljonist seadmest. Sealhulgas rohkelt erinevaid nutistu seadmeid. Prognooside kohaselt on aastaks 2020 internetivõrku ühendatud nutistu seadmeid üle 30 miljardi, millest 1,35 miljardit on küberkurjategijatele kergesti ligipääsetavad, muutes sarnased *botnet*-i rünnakud veelgi ohtlikumaks, tõenäolisemaks ja laiaulatuslikumaks.

5.10 Võimalused kaughalduse ja –juhtimise funktsionaalsusega seadmete elektrivõrku lisamisel

Üks võimalus vähendada potentsiaalsete küberrünnakutest põhjustatud võimsuse ja koormuse kõikumist väikestes jaotusvõrgu piirkondades on lisada jaotusalajaamade protsessorreleedele täiendavaid kaitsefunktsioone.

Küberturvalisuse suurendamiseks on soovituslik rakendada seadmetele ja sektoris tegutsevatele ettevõtetele kohustuslikke standardeid. Seadmetele kehtivad standardid pevad olema sätestatud eelkõige EL-i tasandil. Sektoris tegutsevatele ettevõtetele on võimalik kohustuslikke koolitusi ja standardeid implementeerida seadusandluse teel.

Seadusandluse kaudu tuleb nutistu seadmetele, inverteritele ja teistele elektrivõrguga seotavatele seadmetele sätestada kohustuslikud küberturvalisust arvestavad miinimumnõuded. Sarnaselt Ameerika Ühendriikide ja Ühendkuningriigiga, kus pööratakse eelkõige tähelepanu seadmete paroolihaldusele. Motiveerides kasutama tootjaid, kelle seadmetel on olemas nõuetele vastav funktsionaalsus, näiteks ABB pakutav keskne kasutaja haldussüsteem (Central Account Management).

Eesti tarkvõrguga integreeritud nutistu seadmete osakaal on väike. Päikeseelektrijaamade osakaal kogu tootmisvõimsusest on alla 5%. Seega on parim aeg põhjaliku ja siduva seadusandluse väljatöötamiseks. Luues seeläbi ideaalne keskkond sektori jätkusuutlikuks arenguks ning võimaldades kasutada nutistu ning tarkvõrgu maksimaalset funktsionaalsust.

KOKKUVÕTE

Magistritöö eesmärgiks oli uurida elektrivõrgu digitaliseerimisega kaasnevaid küberturvalisuse riske elektrisüsteemile. Lähtudes eelkõige võrguettevõtete füüsilise kontrolli alt väljas paiknevatest kaugjuhitavatest seadmetest ning seadusandlusest. Praeguste elektrisüsteemide optimeerimine ja areng on jõudnud punkti, kus saavutatud on investeeringute ja efektiivsuse praktiline limiit, mis omakorda loob nõudluse elektrisüsteemi järjepideva digitaliseerimise järele. Uued tarkvõrgu lahendused ja internetivõrguga ühenduses olevad seadmed võimaldavad elektrisüsteemi üha optimaalsemalt juhtida, kuid toovad kaasa ka uudseid probleeme, sealhulgas küberturvalisuse seisukohast.

Tarkvõrk on traditsionaalse tsentraliseeritud elektrivõrgu kombineerimine informatsioonitehnoloogia pakutavate võimalustega. Selle eesmärk on optimeerida elektrivõrgu efektiivsust, integreerida elektrisüsteemi suuremas mahus stohhastilise toodanguga taastuvenergiaallikaid ja minimeerida elektrivõrgust ja –tootmisest tulenevaid kasvuhoonegaase, tagades seejuures võrdväärse või parendatud varustuskindluse. Tarkvõrgul on kriitiline roll detsentraliseeritud elektritoomises, tarbimisjuhtimises ja uute tehnoloogiate edukas rakendamises. Elektrivõrgu optimeerimisülesandele lisandub seetõttu ka tarkvõrgu küberturvalisuse optimeerimisülesanne..

Tarkvõrgu ja nutistu integreerimisel ühendatakse lähiaastatel Eesti elektrivõrku tuhandeid ja üleilmses mastaabis miljardeid seadmeid, mille parameetritest, funktsioonidest ja turvalisusest puudub võrguettevõtetel täielik ülevaade. Integreerimise peaeesmärk on juhtida tarbmist, päikeseelektrijaamade efektiivsust ja pakkuda klientidele võimalust osaleda võimsus– või reservvõimsusturul. Nutistu lahendused on osaliselt keskenunud ka klientidele raha säästmisele, muutes tehnoloogia ja seadmete kasutusele võtmise atraktiivseks. Teisalt kaasneb suure hulga nutistu, inverterite ja teiste võrguettevõtete poolt reguleerimata seadmete elektrivõrku lisamisega küberriske. Põhjustadades väikesele grupile klientidele potentsiaalselt majanduslikku kahju saamata jäänud energia ja luhtunud vara tõttu. Piisavalt suures koguses kaughaldus ja –juhtimise võimekusega seadmete korral on võimalik elektrisüsteemile suureulatuslikke häiringuid põhjustada – sageduse ja pinge ebastabiilsus, suuremahulised katkestused ja ulatuslik majanduslik kahju klientidele ning võrguettevõtetele.

Eesti elektrivõrgu näitel on Tallinna tihepiirkondades suurel hulgal inverterite ja nutistu seadmete pahatahtlikul kaugjuhtmisel võimalik klientidele ja võrguettevõtetele majanduslikku kahju põhjustada. Küberrünnakute otsene rahaline kahju leiti andmata energia meetodil, CENS EUR/kWh. Stsenaariumis, kus Tallinna vaadeldud 200x200m tihepiirkonnas paiknevatest

klientidest 75% omavad vähemalt 1 kW nimivõimsusega kaughaldus ja –juhtimis funktsionaalsusega seadmeid, võib juhitavate seadmete koormuse ja võimsuse suhe ulatuda tavaolukorras 26%-ni kogu koormusest. Tulemusena on 10 000 kWh keskmise tunnitarbimisega piirkonnas võimalik küberkurjategijatel saada kontroll progressiivses stsenaariumis ligi 2600 kW nimivõimsusega seadmetele. Põhjustades korduvate lülitustega väikeses võrgu piirkonnas pingelange, tõukevoole ja seadmete eluea vähenemist. Koormuse osakaal võib olla suurem suveperioodil, kui keskmine elektritarbimine on väiksem. Lisaks on kõrgema välistemperatuuri tõttu haavatavamad võrguseadmed nagu näiteks trafod, liinid ja maakaablid.

Arvestamata luhtunud vara, põhjustab modelleeritud küberrünnak tihepiirkonnas 3 minutilise katkestusega majandusliku kahju: kodutarbijale 2,7 EUR/klient, teenindustarbijale 12 EUR/klient ja tööstustarbijale 37,5 EUR/klient. Tööstustarbijate suurem rahaline kahju võib-olla põhjustatud tööstussektori väikesest osakaalust tihepiirkonnas.

Eesti elektrivõrku ühendatavate võrguettevõtete füüsilise kontrolli alt väljas paiknevatest seadmetest moodustavad suurima juhitava võimsuse osakaalu päikeseelektrijaamades kasutatavad inverterid. Ühtlasi on tegemist kõige suurema kasvupotentsiaaliga juhitava seadmegrupiga, mille osakaalu kasv Eesti elektrivõrgus oli vahemikus 2017–2018 ligi 1000%. Eesti jaotusvõrgu ettevõtete poolt aktsepteeritavatest inverteritest puudub 26% seadmete kohta info või on seadmete tootmine lõpetatud. Ülejäänud 74% inverteritest on 71% seadmetest kaughalduse ja –juhitavuse funktsionaalsus. Antud seadmete võrguga integreerimist reguleeritakse ainult releeekaitseautomaatikast ja tehnilistest parameetritest lähtuvalt, rakendamata ühtegi küberturvalisuse seadust või kindlat direktiivi. Prognooside kohaselt on tänase seadusandluse järgi jätkates 15 aasta pärast Eesti elektrisüsteemis üle 10% tootmisvõimsusest kaugjuhitavad ning küberkurjategijatele lihtsasti ligipääsetavad. Sellele lisanduvad nutistuga ühendatud seadmed, mis võimaldavad piiramatute ressurssidega riikliku toetusega küberkurjategijate organisatsioonidel tekitada häiringuid kogu Eesti elektrisüsteemile.

Magistritöö uurimisküsimustele vastuste leidmiseks koostati hüpoteetiline mudel. Autor analüüsis elektrivõrgule läbi nutistu seadmete ja inverterite suunatud küberrünnakut Tallinna haja– ja tihepiirkonnas. Küberrünnaku põhjustatud kahjudele määrati rahaline väärtus läbi andmata energia meetodi. Täpsemate tulemuste saamiseks on vajalik koostada vastavate elektrivõrgu piirkondadele sobilikud mudelid ning simuleerida koormuse ja võimsuste sagedast kõikumist. Täiendav simulatsioon annaks põhjalikuma ülevaate rünnaku mõjust vaadeldava piirkonna jaotusvõrgu osale ja seadmetele. Võimaldades määrata seeläbi täpsemaid katkestuste kestusi ja põhjuseid.

Inverterite analüüs vajaks täiendamist täpsemate andmetega järgnevates punktides: mikrotootjate osakaal installeeritud võimsusest, põhi ja –jaotusvõrku lisatavate inverterite osakaal ning millisel osal on täiendav kaughaldus ja –juhtmise funktsionaalsus aktiveeritud. Samuti võib eeldada, et 26% inverteritest, mille kohta puuduvad avalikud andmed, on Eesti elektrivõrgus vähelevinud.

Eesti elektrivõrkude tööd reguleerivas seadusandluses kehitvad küberturvalisuse nõuded alates keskmise suurusega ettevõtetest, kes osutavad elutähtsat teenust. Lisaks puuduvad täielikult küberturvalisusest lähtuvad regulatsioonid nutistu seadmete ja inverterite võrku lisamisele. Muuhulgas ei ole sektoris tegutsevad mikro- ja väikeettevõtted kohustatud teenuse pakkumisel küberturvalisusest lähtuma, raskendades seeläbi küberturvalisuse ühtlast integreerimist energeetikasektoris. Olukorra parandamiseks on võimalik California ja Ühendkuningriigi näitel viia sisse regulatsioonid autentimismeetoditele. Samuti võimaldavad turvalist kasutajatunnuste haldamist erinevad ettevõtted, ka magistritöös näitena kasutatud ABB. Valitud seadmete eelistamine kriitilise tähtsusega rakendustes on lihtsasti teostatav.

SUMMARY

The purpose of this master's thesis was to research potential cyber threats caused by digitalization of power grids. Mainly focusing threats caused by smart remote controlled devices. The optimization of power grids in terms of cost effectiveness have reached to theoretical limits. Therefore creating a demand for new solutions such as smart grid. Heavy information and communication technology usage allows to optimize power grids even further. Reducing emissions, the cost of electricity and allows to integrate more renewable energy sources into electricity system. On the other hand major digitalization makes power grids more vulnerable to cyber attacks.

Smart grid combines traditional centralized power grids with new information technology solutions. In order to optimize power grids, integrate even more renewables and minimize emissions. Smart grid is a critical platform for new technologies, load control and stochastic electricity generation. Therefore creating a demand for cyber security optimization in power grids.

Due to integration of smart grid and internet of things thousands of smart devices in Estonia and billions of smart devices globally are being integrated into power grids. Majority of these devices have no cyber security measures and grid operators have little information about parameters of these types of devices. Smart solutions and devices make services such as demand response, load control and participating in reserve markets possible. On the other hand integration of many low security devices causes cyber threats. Especially when the cyber criminal or organisation gains access to switch those devices on or off. Causing power, current and voltage fluctuations. Potentially causing false tripping of relays and short outages for a few clients in concentrated area. Control of huge number of such devices could cause instability of system frequency or long outages. Which results in major financial damages to both clients and grid operators.

Cyber attack on Tallinn 200x200m two different areas with smart remote controlled devices was simulated and financial costs calculated. Economic impacts for outages caused by such attack were found using compensation for energy not supplied(CENS). According to results cyber criminals could control 2600 kW of power in the most progressive scenario, which is 26% of the areas average load. Vulnerable load consists of solar inverters, water heaters and electrical heating devices. Intentionally switching such load in the 200x200m area in Tallinn is potentially enough to cause relay automation tripping. Due to voltage, current and power fluctuation and inrush current. Therefore causing short outages and in worst case scenario damaging grip devices such as transformers, cables and overhead lines. Impacts of such cyber attack are potentially more harmful during the summer. Because of the higher outside temperatures and smaller load.

Using CENS the author found costs of 3 and 5 minute outages and 5 and 12 hour outages. In more populated area cost for 3 minute outage is following: domestic sector 2,7 EUR/client, public and business sector 12 EUR/client and industry sector 37,5 EUR/client.

The majority of smart remote controlled loads in Estonian electricity system consists of solar inverters. Additionally inverters have the biggest growth potential among such devices. For an example between 2017 and 2018 the solar power growth in Estonia was 1000% with over 110 MW totally installed. About 26% of all inverters which are allowed to Estonian power grid, have no public information or are out of production and 71% of the inverters have remote control or management possibility. Therefore forming a huge amount of power potentially vulnerable to cyber criminals. One of the main concerns is that there is currently no legislation in Estonia which could regulate cyber security of such devices. In the future easily accessible power for cyber criminals could form over 10% of total power generation capacity in Estonia.

As a result of this work a hypothetical model was created. Through which cyber attack impacts to distribution grid in Tallinn 200x200m areas were analysed. Potential attack was based on grid integrated smart remote controllable devices such as solar inverters and internet of things devices. Based on analysis an economic impacts of such attack were calculated. In order to get more accurate results additional simulations on impacts of such power fluctuations should be considered. Additionally more data about currently grid integrated data is required.

There are too few legislative regulations based on cyber security in Estonian energy sector. In addition they only regulate medium sized or large companies which are a minority in Estonia. Currently there are no legislation in Estonia which would regulate new smart devices grid integration based on cyber security. Improvements on devices authentication measures should be established based on examples in California and United Kingdom.

KASUTATUD KIRJANDUS

[1] J. V. Heiki Tammoja, „Elektrilevi,“ [Võrgumaterjal]. Available: https://www.elektrilevi.ee/-/doc/6305157/ettevottest/uuringud/Elektrilevi_varustuskindluse_naitajad_muutuste_mojurid_yleminekul_kaablivorgule.pdf. [Kasutatud 22 04 2019].

[2] K. Sokk, „ETIS,“ [Võrgumaterjal]. Available: https://www.etis.ee/Portal/Mentorships/Display/7e9f36c6-c326-43cd-904a-66ecb8eb2432. [Kasutatud 22 04 2019].

[3] A. Gupta, „Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey,“ *Journal of Network and Computer Applications,* pp. 118-148, 2019.

[4] S. Soltan, „BlackIoT: IoT Botnet of High Wattage Devices,“ %1 *27th USENIX Security Symposium*, Baltimore, 2018.

[5] K. Ruan, „Introducing cybernomics: A unifying economic framework for measuring cyber risk,“ *Computers & Security,* pp. 77-89, 2017.

[6] D. C. Bayliss ja B. Hardy, Transmission and distribution Electrical Engineering, Newnes, 2011, pp. 1059-1074.

[7] „Elektrilevi,“ 16 03 2019. [Võrgumaterjal]. Available: https://www.elektrilevi.ee/elektrisysteem.

[8] Elering AS, „Elering,“ [Võrgumaterjal]. Available: https://elering.ee/sites/default/files/public/Infokeskus/elering_vka_2018_web.pdf. [Kasutatud 31 03 2019].

[9] „Elering,“ [Võrgumaterjal]. Available: https://elering.ee/elektri-pohivorgu-kaart. [Kasutatud 16 03 2019].

[10] „Energiatalgud,“ [Võrgumaterjal]. Available: https://energiatalgud.ee/index.php/Elektriv%C3%B5rk. [Kasutatud 16 03 2019].

[11] „Elering,“ [Võrgumaterjal]. Available: https://elering.ee/elekter/teenused#tab0. [Kasutatud 21 05 2019].

[12] „Majandus- ja kommunikatsiooniministeerium,“ 16 03 2019. [Võrgumaterjal]. Available: https://www.mkm.ee/et/tegevused-eesmargid/energeetika/elektriturg.

[13] Elektrilevi OÜ, „Elektrilevi,“ [Võrgumaterjal]. Available: https://www.elektrilevi.ee/et/kauglugemine-paigaldamine. [Kasutatud 31 03 2019].

[14] „Energiatalgud,“ 31 03 2019. [Võrgumaterjal]. Available: https://energiatalgud.ee/index.php/Elektri_tootmine?menu-81.

[15] Majandus- ja Kommunikatsiooniministeerium, „Majandus- ja Kommunikatsiooniministeerium,“ 31 03 2019. [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/enmak_2030_koos_elamumajanduse_lisaga.pdf.

[16] K. Kimani, „Cyber security challenges for IoT-based smart grid networks,“ *International Journal of Critical Infrastructure Protection,* pp. 36-49, 2019.

[17] Elering, „Elering,“ 23 04 2019. [Võrgumaterjal]. Available: https://elering.ee/eesti-vabariigi-juubeliaasta-toi-juurde-100-megavatti-paikeseelektrijaamu.

[18] „Riigiteataja,“ 31 03 2019. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/12831412.

[19] J. Qi, „Cybersecurity for distributed energy resources and smart inverters,“ *The institution of Engineering and Technology Journals,* pp. 28-39, 2016.

[20] Solaredge, „Solaredge,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.solaredge.com/us/products/ev-charger#/.

[21] K. Field, „Cleantechnica,“ 23 04 2019. [Võrgumaterjal]. Available: https://cleantechnica.com/2019/01/19/everything-you-need-to-know-about-the-powerwall-2-2019-edition/.

[22] „Imatra Elekter AS,“ 23 04 2019. [Võrgumaterjal]. Available: https://imatraelekter.ee/vormid-ja-tingimused/.

[23] „VKG Elektrivõrgud OÜ,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.vkgev.ee/est/kliendile/elektrivorguga-liitumine/liitumisprotsess/mikrotootjad.

[24] „Elektrilevi,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.elektrilevi.ee/-/doc/6305157/kliendile/kodulehe_nimekiri_2018.pdf.

[25] „Euroopa Liidu Teataja,“ 26 02 2014. [Võrgumaterjal]. Available: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014L0035&from=EN. [Kasutatud 21 05 2019].

[26] „Euroopa Liidu Teataja,“ 26 02 2014. [Võrgumaterjal]. Available: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014L0030&from=EN. [Kasutatud 21 05 2019].

[27] „Elektrilevi,“ [Võrgumaterjal]. Available: https://www.elektrilevi.ee/-/doc/6305157/kliendile/inverterite_lisamine_elektrilevi_nimekirja_est.pdf. [Kasutatud 16 05 2019].

[28] „Orbital,“ 23 04 2019. [Võrgumaterjal]. Available: https://orbital.dk/dve-closed/.

[29] „ABB,“ 23 04 2019. [Võrgumaterjal]. Available: https://new.abb.com/power-converters-inverters/solar/monitoring-and-communication/aurora-vision-plant-management-platform/plant-viewer-for-mobile.

[30] „APsystems,“ 23 04 2019. [Võrgumaterjal]. Available: https://global.apsystems.com/wp-content/uploads/2018/04/4271801031_APsystems-Energy-Communication-Unit-ECU-C-User-manual_Rev1.5_2018-1-16.pdf.

[31] „Delta Energy Systems,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.delta-americas.com/Products/CategoryListT1.aspx?CID=0505&PID=3694&hl=en-US&Name=R3%20Controller.

[32] „Eaton,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.eaton.com/Eaton/ProductsServices/Electrical/ProductsandServices/Residential/EnergyMonitoringSystem/index.htm.

[33] „Envertech,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.envertec.com/Software/Software4.htm.

[34] „Fronius,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.fronius.com/en/photovoltaics/products/home/system-monitoring/hardware/fronius-datamanager-2-0/fronius-datamanager-2-0.

[35] „goodwe,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.goodwe.com/Products/index_sems.html.

[36] „Growatt,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.ginverter.com/en/Products/Monitoring-system/Monitoring-Platform/Growatt-ShineServer.

[37] „Hoymiles,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.hoymiles.com/Monitoring.html.

[38] „Huawei,“ 23 04 2019. [Võrgumaterjal]. Available: http://solar.huawei.com/ar-AE/download?p=%2F~%2Fmedia%2FSolar%2Fattachment%2Fpdf%2Fmea%2Fdatasheet%2FSmartlogger1000.pdf.

[39] „KACO,“ 23 04 2019. [Võrgumaterjal]. Available: https://kaco-newenergy.com/news-and-events/detail/new-monitoring-portal-for-solar-pv-systems/.

[40] „Kostal,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.kostal-solar-electric.com/en-gb/products/tools-and-software/monitoring.

[41] „ginlong,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.ginlong.com/epm_en/2501.html.

[42] „REFU,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.refu.com/en/solar-solutions/refusol-products/software/.

[43] „Renesola,“ 23 04 2019. [Võrgumaterjal]. Available: http://www.renesola.com/file/Global/product/pdf/Inverter%20and%20Accessory.pdf.

[44] „Shenzhen,“ 23 04 2019. [Võrgumaterjal]. Available: http://jfy-tech.net/on-grid-inverter/monitoring/wifi-plug/wifi-plug.html.

[45] „SMA,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.sma.de/en/products/monitoring-control.html.

[46] „Solaredge,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.solaredge.com/us/products/pv-monitoring#/.

[47] „Solutronic,“ 23 04 2019. [Võrgumaterjal]. Available: http://solutronic-energy-cyprus.de/Solar%20Log.

[48] „Solarmax,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.solarmax.com/Downloads/DK_IM_XPN_EN.pdf.

[49] „Twerd,“ 24 04 2019. [Võrgumaterjal]. Available: http://www.twerd.pl/eng/solar_produkty.html.

[50] „Zeversolar,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.zeversolar.com/products/productline-detail/productline/detail/en-zevercom/.

[51] „Zucchetti Centro,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.zcsazzurro.com/en/products/monitoring-systems.

[52] R. Bucher, „Smart grid functionality for the high-voltage transmission grid: On the market readiness of Digital Substation 2.0 technology,“ %1 *Saudi Arabia Smart Grid (SASG)*, Jeddah, 2017.

[53] O. Hafez, „The impact of smart PEV loads in the smart grid considering demand response provisions,“ %1 *IEEE*, Jeddah, 2016.

[54] M. Masera, „Smart (Electricity) Grids for Smart Cities: Assessing Roles and Societal Impacts,“ *Proceedings of the IEEE,* kd. 106, nr 4, pp. 613-625, 2018.

[55] D. W. D'Andrade, The Power Grid Smart, Secure, Green and Reliable, Academic Press, 2017.

[56] Y. Xiang, „Coordinated attacks on electric power systems in a cyber-physical environment,“ *Electric Power Systems Research,* pp. 156-168, 2017.

[57] European Comission, „EUROPEAN COMMISSION,“ [Võrgumaterjal]. Available: https://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf. [Kasutatud 24 03 2019].

[58] K. Ashton, „RFID Journal,“ 23 03 2019. [Võrgumaterjal]. Available: https://www.rfidjournal.com/articles/view?4986.

[59] „Techopedia,“ 23 03 2019. [Võrgumaterjal]. Available: https://www.techopedia.com/definition/28247/internet-of-things-iot.

[60] P. I. R. Grammatikis, „Securing the Internet of Things: Challenges, threats and solutions,“ *Internet of Things: Engineering Cyber Physical Human Systems,* pp. 41-70, 2019.

[61] Andmekaitse Inspektsioon, „Andmekaitse Inspektsioon,“ 31 03 2019. [Võrgumaterjal]. Available: https://www.aki.ee/et/pilvandmetootlus.

[62] General Electric, „General Electric,“ 31 03 2019. [Võrgumaterjal]. Available: http://www.gegridsolutions.com/software_solutions.htm.

[63] Locus Energy, „Locus Energy,“ 31 03 2019. [Võrgumaterjal]. Available: https://www.locusenergy.com/about-locus.

[64] GridIO, „GridIO,“ 31 03 2019. [Võrgumaterjal]. Available: https://gridio.io/en#about.

[65] CEER, „Council of European Energy Regulators,“ 31 03 2019. [Võrgumaterjal]. Available: https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124.

[66] „Sympower,“ 13 04 2019. [Võrgumaterjal]. Available: https://www.sympower.net/about/our-story.

[67] „Smart Load Solutions,“ [Võrgumaterjal]. Available: http://www.smartloadsolutions.ee/. [Kasutatud 19 05 2019].

[68] P. Eder-Neuhauser, „Cyber attack models for smart grid environments,“ *Sustainable Energy, Grids and Networks,* pp. 10-29, 2017.

[69] F. Rahman, „Hardware-Assisted Cybersecurity for IoT Devices,“ %1 *2017 18th International Workshop on Microprocessor and SOC Test and Verification*, Austin, 2017.

[70] R. H.Khan, „A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network,“ *Computer Networks,* pp. 825-845, 2013.

[71] P. Radanliev, „Future developments in cyber risk assessment for the internet of things,“ *Computers in Industry,* pp. 14-22, 2018.

[72] Western Electricity Coordinating Council, „WECC,“ 18 04 2019. [Võrgumaterjal]. Available: https://web.archive.org/web/20160809221758/https://www.wecc.biz/Reliability/2016%20SOTI%20Final.pdf.

[73] V. Namboodiri, „Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids,“ *IEEE Systems Journal ,* kd. 8, nr 2, pp. 509-520, 2013.

[74] „Gartner,“ [Võrgumaterjal]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. [Kasutatud 19 05 2019].

[75] „McAfee,“ [Võrgumaterjal]. Available: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf. [Kasutatud 21 05 2019].

[76] T. Cohen, „Reuters,“ 26 01 2017. [Võrgumaterjal]. Available: https://www.reuters.com/article/us-tech-cyber-microsoft-idUSKBN15A1GA. [Kasutatud 21 05 2019].

[77] „Microsoft,“ [Võrgumaterjal]. Available: https://www.microsoft.com/en-us/Investor/earnings/FY-2018-Q4/press-release-webcast. [Kasutatud 21 05 2019].

[78] K. Townsend, „Securityweek,“ [Võrgumaterjal]. Available: https://www.securityweek.com/600-million-cybersecurity-budget-jpmorgan-chief-endorses-ai-and-cloud. [Kasutatud 21 05 2019].

[79] „Inforegister,“ [Võrgumaterjal]. Available: https://www.inforegister.ee/11050857-ELEKTRILEVI-OU. [Kasutatud 21 05 2019].

[80] „Inforegister,“ [Võrgumaterjal]. Available: https://www.inforegister.ee/10224137-FORTUM-ELEKTER-AS. [Kasutatud 21 05 2019].

[81] „Inforegister,“ [Võrgumaterjal]. Available: https://www.inforegister.ee/10855041-VKG-ELEKTRIVORGUD-OU. [Kasutatud 21 05 2019].

[82] „Inforegister,“ [Võrgumaterjal]. Available: https://www.inforegister.ee/11022625-ELERING-AS. [Kasutatud 21 05 2019].

[83] „Riigiteataja,“ 15 04 2019. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/12831412.

[84] „Riigiteataja,“ 15 04 2019. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/113032019044.

[85] „Riigiteataja,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/K%C3%BCTS. [Kasutatud 15 04 2019].

[86] „Riigiteataja,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/HOS. [Kasutatud 21 05 2019].

[87] „Riigiteataja,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/123032015004. [Kasutatud 14 05 2019].

[88] „Küberturvalisuse Strateegia,“ 15 04 2019. [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

[89] Euroopa Parlament ja Nõukogu, „Euroopa Liidu Teataja,“ [Võrgumaterjal]. Available: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L1148&from=EN. [Kasutatud 15 04 2019].

[90] „California Lgeislative Infromation,“ [Võrgumaterjal]. Available: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. [Kasutatud 14 05 2019].

[91] „Mapping Security & Privacy in the Internet of Things,“ Copper Horse Solutions Limited, [Võrgumaterjal]. Available: https://iotsecuritymapping.uk/code-of-practice-guideline-no-12/. [Kasutatud 14 05 2019].

[92] „Government Digital Service,“ [Võrgumaterjal]. Available: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice#make-better-use-of-data. [Kasutatud 14 05 2019].

[93] E. Lucas, Küberfoobia, Tallinn: Kirjandus Varrak, 2016.

[94] Cybernetica AS, „Andmekaitse ja infoturbe leksikon,“ 24 03 2019. [Võrgumaterjal]. Available: http://akit.cyber.ee/.

[95] „Recorded Future,“ 24 03 2019. [Võrgumaterjal]. Available: https://www.recordedfuture.com/cyber-threat-landscape-basics/.

[96] „Cybernetica,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/684. [Kasutatud 13 05 2019].

[97] „Cybernetica,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/118-botnet-2. [Kasutatud 13 05 2019].

[98] Riigi Infosüsteemi Amet, „Küberturvalisus 2019,“ 2019.

[99] K. Paas, „Ärileht,“ 31 03 2019. [Võrgumaterjal]. Available: https://arileht.delfi.ee/news/uudised/mis-voi-kes-rundas-it-sodurid-tulistasid-vkg-d-toopaeviti-kella-8st-18ni?id=77740298.

[100] M. Tammet, „Ärileht,“ 31 03 2019. [Võrgumaterjal]. Available: https://arileht.delfi.ee/news/uudised/gru-mollas-eesti-uhes-rikkamas-ettevottes-sojavaeluure-ekspluateeris-viru-keemia-gruppi?id=77713762.

[101] SteveMansfield-Devine, „Estonia: what doesn't kill you makes you stronger,“ *Network Security,* kd. 2012, nr 7, pp. 12-20, 2012.

[102] K. Thakur, „Impact of Cyber-Attacks on Critical Infrastructure,“ %1 *2016 IEEE 2nd International Conference*, New York, 2016.

[103] Riigi Infosüsteemi Amet, „Riigi Infosüsteemi Amet,“ 2018.

[104] „Krebsonsecurity,“ [Võrgumaterjal]. Available: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/. [Kasutatud 14 05 2019].

[105] European Union Agency For Network And Information Security, „Baseline Security,“ European Union Agency For Network And Information Security, Hague, 2017.

[106] E. i. s. a. a. center, „Analysis of the Cyber Attack on the Ukrainian Power Grid,“ Electricity information sharing and analysis center, Washington, 2016.

[107] L. Dearden, „Independent,“ [Võrgumaterjal]. Available: https://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html. [Kasutatud 14 05 2019].

[108] A. Hern, „The Guardian,“ [Võrgumaterjal]. Available: https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre. [Kasutatud 14 05 2019].

[109] M. Eling, „What are the actual costs of cyber risk events?,“ *European Journal of Operational Research,* pp. 1109-1119, 2019.

[110] „US National Library of Medicine,“ 12 05 2019. [Võrgumaterjal]. Available: https://www.ncbi.nlm.nih.gov/pubmed/26747014.

[111] „Eesti Pank,“ 12 05 2019. [Võrgumaterjal]. Available: https://www.eestipank.ee/rahapoliitika/riskid-varade-paigutamisel-riskijuhtimine.

[112] C. C. Fung, „A proposed study on economic impacts due to cyber attacks in Smart Grid: A risk based assessment,“ %1 *2013 IEEE Power & Energy Society General Meeting*, Vancouver, 2013.

[113] P. Raesaar, „Energiatalgud,“ 22 04 2019. [Võrgumaterjal]. Available: https://energiatalgud.ee/img_auth.php/a/a8/Raesaar%2C_P._Elektriv%C3%B5rkude_t%C3%B6%C3%B6kindlus._Tallinn_2010.pdf.

[114] London Economics, „The Value of Lost Load (VoLL) for Electricity in Great,“ 26 04 2019. [Võrgumaterjal]. Available: https://www.ofgem.gov.uk/ofgem-publications/82293/london-economics-value-lost-load-electricity-gbpdf.

[115] Cambridge Economic Policy Associates Ltd, „acer.europa.eu,“ 22 04 2019. [Võrgumaterjal]. Available: https://www.acer.europa.eu/en/Electricity/Infrastructure_and_network%20development/Infrastructure/Documents/CEPA%20study%20on%20the%20Value%20of%20Lost%20Load%20in%20the%20electricity%20supply.pdf.

[116] „Soojuspumbad,“ 12 05 2019. [Võrgumaterjal]. Available: https://www.soojuspumbad.ee/maasoojuspump-thermia-diplomat-optimum-g3/.

[117] „Cerbos,“ 12 05 2019. [Võrgumaterjal]. Available: https://www.cerbos.ee/et/59-kuttekehad-elektritennid.

[118] „Atlantic-eesti,“ 12 05 2019. [Võrgumaterjal]. Available: https://www.atlantic-eesti.com/product/elektriradiaatorid/elektriradiaator/.

[119] K. Darcovich, „Propagation of Electrical Disturbances to Automotive,“ %1 *IEEE Electrical Power and Energy Conference*, Ottawa, 2016.

[120] Y. T. Quek, „DC appliance classification and identification using k-Nearest Neighbours technique on features extracted within the 1st second of current waveforms,“ %1 *EEEIC*, Rome, 2015.

[121] A. Reinhardt, „Electric appliance classification based on distributed high resolution current sensing,“ %1 *37th Annual IEEE Conference on Local Computer Networks - Workshops*, Clearwater, 2012.

[122] Z. J. Ahmed, „Power Management of Domestic Air Condition Units,“ %1 *11th International Conference on Developments in eSystems Engineering*, Cambridge, 2018.

[123] G. Schofield, „Has your wifi left you wide open to cybercrime?,“ *Network Security,* pp. 13-14, 2019.

[124] J. S. Atkinson, „Your WiFi is leaking: What do your mobile apps gossip about you?,“ *Future Generation Computer Systems,* pp. 546-557, 2018.

[125] „Elering,“ [Võrgumaterjal]. Available: https://elering.ee/sites/default/files/public/Elering_VKA_2016.pdf. [Kasutatud 13 05 2019].

[126] „Elering,“ [Võrgumaterjal]. Available: https://elering.ee/sites/default/files/public/Elering_VKA_2017.pdf. [Kasutatud 13 05 2019].

[127] A. Jäger-Waldau, „PV Status Report 2018,“ Publications Office of the European Union, Luxembourg, 2018.

[128] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[129] A. Claudio Marchetti, „ABBs Digital Substation,“ 2018.

[130] Kaitseministeerium, „Küberjulgeoleku strateegia 2008–2013,“ Tallinn, 2008.

[131] „Letrikasol,“ 23 04 2019. [Võrgumaterjal]. Available: https://letrikasol.com/downloads/en/commercial-catalogues/Solar_sistems_letrika_1.pdf.

[132] „Steca,“ 23 04 2019. [Võrgumaterjal]. Available: https://www.steca.com/index.php?Professional_system_monitoring_for_reliable_yields.

LISAD

1. Lisa 1. Tallinna 200x200m varustuspiirkondade kaart.

Lisa 1 Töös kasutatud Tallinna 200x200m varustuspiirkondade kaart. [1]