Tartu Ülikool

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Ajakirjanduse ja kommunikatsiooni õppekava

Eesti ja NATO küberkaitse võimekuse narratiivne konstrueerimine Eesti ajakirjandusväljaannetes

magistritöö

Maia Klaassen

Juhendaja: Mari-Liis Madisson, PhD

Tartu 2021

Sisukord

SISSEJUHATUS

On tähelepanuväärne, et veel kümnend tagasi kirjutatud teadustöödes räägitakse infooperatsioonidest käsikäes konventsionaalse sõjaga, ning et diskursiivne pööre on toimunud kõigest viie aasta jooksul. Brexit, USA 2016. aasta ning Prantsusmaa 2017. aasta presidendivalimised on võimaldanud kvantitatiivselt tõestada varem teoretiseeritut: kommunikatsioonioperatsioonidega, mille relvaks on informatsioon ja eesmärgiks muuta sihtmärgi olukorrataju ning käitumist mõjutaja huvides (Murphy, 2008: 13-14), on võimalik demokraatiat ja valitsevat riigikorda õõnestada. Sotsiaalmeedias võimendavad info levikut ka pahaaimamatud tegutsejad, kelle tõlgendus ega agenda ei pruugi narratiivi autori soovidega kattuda. Infojulgeoleku tagamist võib seega mõtestada igapäevase väljakutsena muutunud infokeskkonnas.

Tänu loodud pretsedentidele on informatsioonilise mõjutustegevuse tuvastamine Eestile ja NATOle olulisem kui varem. Vastupanuvõime tõstmiseks kasutatakse psühholoogilise kaitse ja strateegilise kommunikatsiooni tööriistu. See töö kõnelebki informatsioonilisest mõjustamisest kaasaegses teabekeskkonnas, kirjeldades meediatekstide narratiive Eesti ja NATO küberkaitse võimekuse kohta. Sealjuures ei keskendu töö faktikontrollile ega paku tehnilisi lahendusi küberturbeks, vaid läheneb teemale riigikaitse laia käsituse kontekstis. Eesti julgeolekupoliitika aluste (2017: 3) järgi on turvatunde edendamises oluline roll sidusal kodanikuühiskonnal ning iseseisva kaitsevõime kõrval ka NATO kollektiivkaitsel. Arusaam sellest, milliseid narratiive Eesti või liitlaste küberkaitse võimekuse kohta leidub, millisena konstrueeritakse võimusuhteid ja tegutsejaid ning mida võib järeldada mitte-öeldust, on julgeolekukeskkonna mõtestamisel võtmetähtsusega.

Ehkki varem on uuritud e-ohtude narratiivset konstrueerimist Zapadi kontekstis (Madisson ja Ventsel, 2018), strateegilise kommunikatsiooni erinevusi Baltikumis (Voltri, 2021) ning julgeolekukommunikatsiooni Eestis (Paas, 2021), pole autorile teadaolevalt keskendutud sellele, *kuidas* muutunud infokeskkonda ja potentsiaalseid e-ohtusid, tegutsejaid ning lahendusi Eesti ajakirjandusväljaannetest konstrueeritakse. Samuti võiks uuring pakkuda mõtteainest poliitikakujundajatele ja riigikaitse valdkonna spetsialistidele, sest lisaks kirjeldamisele analüüsin ka seda, kui mõjusad välja joonistunud narratiivid on ning mida nendega teha saab.

Analüüsiks kasutan Madissoni ja Ventsli (2020) strateegiliste narratiivide mudelit, mis ühendab endas rahvusvaheliste suhete ja semiootika distsipliinid, aga töö kombineerib mitut andmete kogumise meetodit. Esmase analüüsi valimiks oli kahe küberkaitse võimekuse seisukohast olulise sündmuse – 2020. a detsembri TEHIKu ning 2021. a veebruaris avalikuks tulnud CityBee rünnaku ja andmelekke – eel, ajal ja järel Eesti uudisajakirjanduses ilmunud artiklid. Kodeerisin 109 artikli suurust valimit MaxQDA tarkvara abil. Järgmiseks tegin fookusgrupi, kus osalesid kuus eksperti, kes töötavad Riigikantseleis, Kaitsepolitseiametis, Kaitseväe Akadeemias, NATO StratComis, Propastopis ning Riigi Infosüsteemi Ametis. Fookusgrupis osalenute kommentaarid täiendavad tulemuste peatükki. Narratiivide kirjeldamine sõltub paljuski uurija tõlgendusest ning uurijana ei saa enda kultuuriruumi, tähendusvälja, kogemusi ja neist tulenevaid eelhoiakuid täielikult välja lülitada. Täiendava uurimismeetodi kaasamine aitab võimalikke riske maandada.

Käesolev magistritöö koosneb viiest peatükist. Esimene peatükk algab terminoloogiaga ning annab seejärel ülevaate töö aluseks olnud kommunikatsiooni- ja poliitikauuringute, rahvusvaheliste suhete distsipliini ning semiootika teoreetilistest lähtepunktidest. Teises peatükis sõnastan töö eesmärgi ja uurimisküsimused ning kolmandas peatükis tutvustan meetodit ja valimit. Tulemused on koondatud neljandasse peatükki ning viiendas peatükis on järeldused, autori diskussioon ja soovitused edasisteks uuringuteks. Kokkuvõtte järel on välja toodud viidatud kirjandus ning esmase analüüsi valimiks olnud artiklite täisloend, samuti leiab lisadest fookusgrupi stiimulmaterjali kuvatõmmised grupiintervjuu alguses ja lõpus.

Tänan kannatlikkusse, vastutulelikkuse ja erakordse tähelepanelikkuse eest oma juhendajat Mari-Liis Madissoni, kelleta seda tööd ei eksisteeriks. Samuti tänan oma retsensenti ja komisjoniliikmeid eelkaitsmiselt, kellelt sain väärtuslikku tagasisidet, mida tõlkida edasisideks, ning ideid, kuidas uuringu tulemusi kaasahaaravalt presenteerida.

Selle magistritöö valmimist on toetanud teadusprojekt SHVFI19127 "Strateegiline narratiiv julgeolekudilemma kujundajana".

1. TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD

Käesolevas magistritöös on kontseptsioone, mille tähendus võib erinevates teadusdistsipliinides ja keeltes erineda. Töö kõneleb küberkaitse võimekusest (ingl *cyber security capability*), lähtudes sellest, et ka infojulgeolek, taju võimalike e-ohtude suhtes ning turvatunne digivahendite kasutamisel on selle osa. Ehkki sõna küberkaitse (ingl *cyber security*) tähistab inglise keeles nii küberjulgeolekut, küberturvet kui ka küberturvalisust, ei keskendu see töö seadmete ega võrkude turvalisusele. Keelelised erinevused tulevad mängu just turvalisuse tagamise jooksva tegevusena kujutamise ning turvalisuse kui saavutatud lõppstaadiumi mõtestamisel. Terminoloogilise segaduse vältimiseks toon esmalt välja kesksed definitsioonid, millest magistritöös läbivalt lähtun.

Diskursus – teatud teemaga seotud keelekasutus või tekstikooslus, mis määrab kuidas temaatikat esitleda ja uurida, aga ka kuidas teemast mõelda või selle suhtes käituda. „Diskursus ei puuduta üksnes rääkimise viise ja teadmiste vorme, vaid ka viise, kuidas diskursuse kaudu luuakse võimusuhteid, reguleeritakse käitumist, luuakse identiteete.“ (Kull jt, 2018: 503)

Hübriidsõda – hõlmab lisaks relvajõudude kasutamisele või hirmule relvajõudude kasutamise pärast ka informatsioonilist mõjutustegevust (Nissen, 2015: 9).

Infokonflikt – lahkarvamus selle kohta, kuidas teavet tõlgendada (Cronin, Weingart, 2007: 9).

Informatsiooniline mõjutustegevus – strateegiline kommunikatsioonioperatsioon kas sõja- või rahuajal, mille nn. relvaks on informatsioon ning eesmärgiks muuta sihtmärgi olukorrataju ja käitumist mõjutaja huvides (Murphy, 2008: 13-14). Üks hübriidsõja tööriistadest.

Küberjulgeolek (ingl *national cyber security*) – „seisund, kus riigi julgeolek on kaitstud võrgu- ja infosüsteemide kaudu tekkivate ohtude eest“ (Küberturvalisuse strateegia 2019-2022: 41).

Küberkaitse (ingl *cyber security*) – küberrünnakute ennetamiseks ja tõrjumiseks tehtavad tegevused või tegevusplaanid; üldjuhul kasutusel riigikaitse valdkonnas (Küberturvalisuse strateegia 2019-2022: 41); sajandivahetuse ajal olid need teooriad ja praktikad tuntud ka arvuti turvalisuse (ingl *computer security*) tähise all (Schatz, Bashroush, Wall, 2017: 54).

Küberturvalisus (ingl samuti *cyber security*) – „seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest“ (Küberturvalisuse strateegia 2019-2022: 40).

Narratiiv – sündmuste representatsioon, mis näitab loo jutustaja eesmärke või seisukohta, loob sündmuste vahel seoseid, on ajaliselt piiritletud ning viitab tegelastele ja tegevuspaikadele (Coulter, Smith, 2009: 579-583).

Psühholoogiline kaitse – üks kuuest Eesti riigikaitse tegevussuunast, mis tegeleb „ühiskonna teavitamisega ja teadlikkuse suurendamisega infotegevusest“ ning mille eesmärgiks on „ennetada kriise, aidata kaasa ühiskonna julgeolekuteadlikkuse suurendamisele ning neutraliseerida inforünnakuid, mis manipulatsiooni ja valeteabe abil provotseerivad ühiskonnas vägivalda või propageerivad kriiside lahendamist põhiseaduslikku korda eiravate vahenditega“ (Eesti julgeolekupoliitika alused, 2017: 19).

Strateegiline kommunikatsioon – „riigi poliitiliste, majanduslike ja riigikaitseliste sõnumite ja tegevuse plaanimine ning koondamine ühtseks informatiivseks tervikuks ja selle edastamine ühiskonnale“ (Eesti julgeolekupoliitika alused, 2017: 19).

Strateegiline narratiiv – vahend, mille abil poliitilised tegutsejad konstrueerivad jagatud tähendust mineviku, oleviku ja tuleviku kohta, et kujundada siseriiklike ja rahvusvaheliste toimijate käitumist (Miskimmon, O’Loughlin, Roselle, 2013: 3).

1.1 Võim ja informatsiooniline mõjutustegevus

Esimene alapeatükk tutvustab magistritöö teoreetilist raamistikku ning keskseid kontseptsioone nagu pehme jõud ja diskursiivne võim, selgitab diskursuse ja (strateegilise) narratiivi erinevusi ning avab tänapäevase infokeskkonna tahke, mis informatsioonilist mõjutustegevuse eesmärkide saavutamist indiviidi, institutsiooni või ühiskonna tasandil soodustavad.

1.1.1 Pehme jõud ja (sotsiaalne) konstruktivisim

Poliitikateadlane Joseph Nye tutvustas 80-ndate lõpus pehme jõu kontseptsiooni, mida ta käsitles kui rahumeelset, aga võrreldes kõva jõuga (tollel hetkel veel) üsna ebaefektiivset viisi

maailmapoliitikas oma tahtmist saada. Jõud või võim on Nye (2004: 8) nägemuses võimekus mõjutada teiste rahvusvahelise süsteemi tegutsejate (ingl *actors*) käitumist enda soovitud tulemuste saavutamiseks. Kõva jõu peamisteks vahenditeks on majanduslikud sanktsioonid ja sõjaline jõud; pehme jõu vahenditeks poliitilised väärtused ja ideed, kultuur ning (välis-) poliitilised strateegiad ja meetmed. Pehme jõu arsenali kasutas nt Tšehhi valitsus siis, kui 2021. aasta aprillis tuli avalikuks Venemaa luurajate seotus seitse aastat varem toime pandud plahvatusega: ühes liitlastega olid meetmeteks suursaadiku väljakutsumine ja diplomaatide väljasaatmine, avalik hukkamõist ja toetuse avaldamine ning ühisavaldused rahvusvahelistes organisatsioonides (Poom, 2021). Vastandamise asemel võiks pehmest jõust mõelda kui kõva jõu käepikendusest, mille puhul jõutakse strateegiliste eesmärkidele avalikkusele lihtsamini aktsepteeritavate vahendite ja meetoditega kui sõda (Mattern, 2005: 589).

Esmapilgul tundub Nye (1990) võimu kontseptsioon sobituvat konstruktivismi mõttevoolu, mis peab Christine Agiuse (2016: 50) järgi oluliseks ideid, identiteeti ja interaktsiooni. Tegelikult rõhutas Nye hiljem, et pehme jõud ei ole normatiivne kontseptsioon, st ei kõnele sellest, kuidas asjad võiksid olla, vaid (tegelikku olukorda) kirjeldav kontseptsioon ning ei vastandu realismi traditsioonile (Nye, 2011: 81). Sellegipoolest on konstruktivism üheks käesoleva magistritöö teoreetiliseks raamistikuks, sest ka julgeolekustamise (ingl *securitization*) teooriad (vt ptk 1.2.3) kuuluvad konstruktivistliku mõttevoolu ja laiemalt post-positivistliku traditsiooni juurde (Jørgensen, 2010: 160).

Julgeolekut võib läbi konstruktivismi läätse käsitleda kui sotsiaalset konstruktsiooni, mille mõtestamist mõjutavad sotsiaalsed faktorid nagu ideed, normid, jagatud tähendusväljad, keel, kultuur ja kollektiivne teadmine (Spindler, 2013: 198). Kui lähtuda Wendti (1992: 404) seisukohast, et oht ei pole loomulik, vaid sotsiaalne konstruktsioon, siis on arusaadav ka konstruktivismi kriitika, mis heidab ette vähest võimalust väiteid empiiriliselt testida (Agius, 2016: 66; Spindler, 2013: 207). Meyeri ja Strickmanni (2011) loogikale toetudes oleks nt küberkaitseline võimekus (sarnaselt sõjalisele võimekusele) konstruktivistidele oluline siis, kui rahvusvahelise süsteemi tegutsejad ise usuks, et see on oluline.

Sarnaselt Nye (1990) pehme ja kõva võimu kontseptsioonile leidis ka Michael Foucault (2011: 298-300), et kuna võim ei mõju otseselt inimesele, vaid inimese tegevusele, on see järelikult käitumist suunav või mõjutav valitsemisviis. Kuidas selliseid abstraktseid ja mitmeti tõlgendatavaid kollektiivseid konstruktsioone uurida?

1.1.2 Diskursiivne ülekanne

Poliitiline semiootika püüab konstrueeritud poliitilise reaalsuse tähendusloome ja tähendusväljade empiirilist uurimist lihtsustada. Näiteks kontseptualiseerivad Peeter Selg ja Andreas Ventsel (2008: 169) võimu toimimist läbi diskursuse ühendades Laclau hegemooniateooria Juri Lotmani bilinguaalse tähendusloome teooriaga. Sellist ajaloolis-diskursiivset lähenemist nimetatakse ka foucault'likuks diskursusanalüüsiks (FDA) (Kalmus, 2015). Käesolev magistritöö lähtub selle lähenemise viimasest edasiarendusest, kasutades ühe uurimismeetodina Mari-Liis Madissoni ja Andreas Ventsli (2020) semiootilist strateegiliste narratiivide analüüsimise mudelit (vt ptk 1.1.3 ja 3.1.2), mistõttu on siinkohal sobiv mõtestada diskursuse ja (strateegiliste) narratiivide omavahelist suhestumist.

Kui diskursus on Foucault' (1972) järgi üks mitmest võimu teostamise vahendist või praktikast, siis diskursiivset võimu näeb ta võimusuhete varjutasandina, mis on juba eksisteerivatest võimumustritest lahutamatu; selle viljelemine on seega sihipäratu paratamatus (Koppel, 2017: 5; Puumeister, 2008: 16). Ernesto Laclau, nn Essexi diskursusanalüüsi koolkonna esindaja, näeb diskursust aga objektiivsuse moodustamise esmatasandina (Laclau, 2005: 68), ning selle läätse läbi muutub diskursiivne võim praktiliseks, eesmärgipäraseks ja paremini analüüsitavaks.

Kommunikatsiooniuurija Manuel Castellsi (2009: 10) järgi on kõige olulisem võimu liik oskus inimmõistust vormida nii, et eelistatuks muutuvad mõjutaja tahe, huvid ja väärtused. Seda ilmestab Martin Reisigli (2008: 99) käsitlus diskursiivsest ülekandest poliitilise retoorika teoreetilises raamistikus: diskursus liigub ühest diskursiivsest väljast teise ning ka erinevate võimu realiseerimise tasandite vahel, nt seadusloomest nn. avaliku arvamuse kohtusse. Diskursiivne ülekanne toimib ka erinevate meediumite, vormide ning platvormide vahel. Nii võivad ka mittefiktsionaalsed (sh strateegilised) narratiivid läbida erinevaid kommunikatsioonikanaleid ja tekste – seda võib täheldada nt siis, kui pressiteatest saab uudis,

mida jagatakse sotsiaalmeedias ning kommentaariumis korratakse pressiteates välja joonistatud narratiivi (Ventsel, Hansson, Madisson, Sazonov, 2018: 106).

Narratiiviga saab näidata eesmärke ja kavatsusi, luua sündmuste vahel seoseid, osutada aja mõjule ning luua tähendust (Coulter, Smith, 2009: 579-583) ning see on mõjukas, sest „pakub korrastatud ning lihtsustatud tähendusraamistikku, mida on kerge kommunikeerida, hoomata ning meelde jätta, aga ka suhestada tõlgendaja isiklike kogemustega," (Ventsel, Hansson, Madisson, Sazonov, 2018: 107). Narratiiv on diskursiivne nähtus. Kui foucault'lik diskursuse uurimine on võrdlemisi abstraktne, siis narratiiv omab kindlalt piiritletud tunnuseid, nagu nt ajalis-põhjuslik sündmuste representatsioon ning tahtevõimelised tegelased. Loo jutustaja või vahendaja tonaalsus ja hinnanguid väljendav keelekasutus võimaldab uurida ka seda, kuidas sõnumi saatja soovib, et vastuvõtja narratiivist mõtleks või sellega suhestuks (Coulter, Smith, 2009: 584). Diskursus võib olla ka argumenteeriv või kirjeldav (Kalmus, 2015), aga narratiivi diskursust uurides vastatakse pigem küsimusele, *kuidas* midagi juhtus. Narratiivist võib seega lihtsustatult mõelda kui diskursuse jalajäljest või ilmingust.

Narratiive on nii ilukirjanduslikke kui ka mittefiktsionaalseid, nt uudismeedia narratiivid. Mittefiktsionaalsed narratiivid esinevad sageli hajusalt ja üksteisega põimunult; vahel esitab üks meediatekst ka vastandlikke narratiive (Ventsel, Hansson, Madisson, Sazonov, 2018: 106). Ajakirjandusliku diskursuse jagatud aluspõhimõtet ehk diskursiivset formatsiooni võib läbi foucault'liku läätse mõtestada võimu ja avaliku kõne kasutamisena keskse, standardiseeritud või laialdaselt heaks kiidetud tõe versiooni avalikus ruumis vahendamise või tootmisena (Dent, 2008: 213) ning uudismeedia narratiivid näitlikustavad seda protsessi, andes nt aimu ajakirjaniku toonist ja positsioonist (Buozis, Creech, 2018: 1430). Toimub pidev diskursiivne ülekanne, mis muutub eriti oluliseks narratiivide mittelineaarsel sotsiaalmeediasse üle kandumisel, sest strateegiline autor ei saa orgaaniliselt levinud narratiivi ega tõlgendaja tähendusvälja enam mõjutada (Madisson ja Ventsel, 2020: 29). Uudisajakirjandus dikteerib, millest ja kuidas ühiskond mõtleb, mis toonis olukorda näeb, milliseid omadusi uudiste subjektile omistab ning keda üldse oma tähelepanu väärilisteks peab (Vu, Guo, McCombs, 2014: 669). Meedia vastutus ja roll on ühiskonnas kõneaine kujundajana suur ning seetõttu on ka selle magistritöö esmase

analüüsi valimiks meediatekstid (vt ptk 3.1). Lisaks meedianarratiividele otsin meediatekstidest ka strateegilisi narratiive.

1.1.3 Strateegilised narratiivid

Strateegiliste narratiivide abil edendavad poliitilised tegutsejad rahvusvahelises süsteemis oma huve, väärtuseid ja tulevikuambitsioone ilma selge ja vägivaldse vastasseisuta (Antoniades, Miskimmon, O'Loughlin, 2010: 14). Seega võib strateegiline narratiiv olla üheks pehme jõu tööriistaks ning diskursiivse võimu teostamise vahendiks. Strateegilisi narratiive on meedia ja võimu kontekstis hea uurida sellepärast, et nende puhul on võimalik kaardistada, kas ja kuidas mõjutamine aset leiab, samas kui pehme võimu analüüsid on siiani mõju asemel keskendunud hoopis pehme võimu tööriistadele ja teoreetilisele võimekusele (Roselle, Miskimmon, O'Loughlin, 2014: 71).

Poliitilised tegutsejad sätestavad strateegilise narratiiviga oma identiteedi, lõppsihi, takistused ning takistuste ületamise viisid, kasutades selleks kõiki meediatööriistu ja -kanaleid ning arvestades samas sihtgrupi kultuurilises mälus olemasolevate (ja mitmeti tõlgendatavate) narratiividega (Miskimmon, O'Loughlin, Roselle, 2012: 3-4). Ehkki strateegiline narratiiv võib viidata minevikule või olevikule, on eesmärgiks suunata või mõjutada tulevikku (Miskimmon, O'Loughlin, Roselle, 2012: 4). Rahvusvaheliste suhete distsipliinis võib eristada kolme tüüpi narratiive:

- Süsteeminarratiivid kõnelevad rahvusvaheliste suhete strukturaalsest olemusest;
- Identiteedinarratiivid kirjeldavad pidevas läbirääkimiste ja võistlemise protsessis olevaid rahvusvahelisi tegutsejaid;
- Poliitika-/probleeminarratiivid (ingl *issue narratives*) püüavad mõjutada poliitiliste arutelude keskkonda. (Miskimmon, O'Loughlin, Roselle, 2013: 10-11)

Ühise, jagatud tähenduse konstrueerimine võimaldab raamida teatud kogukonna taju, uskumusi ja käitumismustreid (Lepik, 2008: 1). Strateegilise narratiivi funktsooniks võib olla poliitiliste eesmärkide või meetmete õigustamine, rahvusvaheliste liitude loomine või tugevdamine ning avaliku arvamuse mõjutamine või kujundamine (Antoniades, Miskimmon, O'Loughlin, 2010: 4).

See tähendab, et strateegiline narratiiv vastab nii riigi kui poliitilise süsteemi osas küsimustele „Kes me oleme?“ ja „Millist maailmakorda me tahame?“ (Miskimmon, O’Loughlin, Roselle, 2012: 3).

Strateegiliste narratiividega saavad poliitilised toimijad oma mõju laiendada, (avalikkuse) ootusi juhtida ning muuta diskursiivset keskkonda, kus nad tegutsevad (Miskimmon, O’Loughlin, Roselle, 2013: 3). Selleks võib kasutada hirmutamistaktikat – hirmust on saanud tõhus viis ühiskonda mobiliseerida (Castells, 2009: 417, Ventsel, Hansson, Madisson, Sazonov, 2018: 104 kaudu). Rahvusvaheliste suhete uurija Janice Mattern (2005) nimetab seda ka kõneleja kujundatud narratiiviks („Kui sa ei arva igas osas nii nagu mina, siis on tagajärjed ennenägematult kohutavad...“). Näiteks vene emakeelega eestlaste inforuumi juba aastakümneid Venemaalt paisatav korduv sõnum: meie vendasid ja õdesid, Eestis elavaid venelasi, kiusatakse nende juurte pärast taga ning kui asi läheb üle piiri, tuleme meie, suurvõim, enda inimestele appi. Krimmis see taktika töötas, kusjuures veel ühes paralleelseks narratiiviks oli toona ka „õigussõjapidamine“ („Kuna USA ja NATO rikuvad rahvusvahelist õigust Kosovos, on legitiimne ka Venemaa tegevus Krimmis“) (Beltadze, 2018), seega on narratiivide edasiseks uurimiseks üksnes Eesti riigikaitse vaatenurgast küllalt põhjust.

Kui strateegilisi narratiive käsitletakse rahvusvahelistes suhetes poliitiliste tegutsejate jagatud mineviku, oleviku ja tuleviku tähendust konstrueeriva kommunikatsioonivahendina (Miskimmon, O’Loughlin, Roselle, 2012: 5), siis semiootikud lisasid tähendusvälja mõtestamiseks ka semiootilise mõõtme ning kombineerivad rahvusvaheliste suhete mudelit Umberto Eco (2005) mudellugeja ja mudelautori kontseptsioonidega (Madisson ja Ventsel, 2020). Mudellugeja all peab Eco (2005: 62) silmas pigem teksti lugemise strateegiat või reeglistikku – autor loob teksti mudellugejale, kes tõlgendab seda nii, nagu autor on planeerinud ning jagab teksti mõistmiseks vajalikku (kultuurilist) tähendusvälja, sõnavara ja väljendusviisi. Nii võib mudellugejat mõtestada narratiivi autori strateegia kohaselt teksti aktualiseerimiseks vajalikku eeltingimuste või ideaalse lugeja omaduste komplekti (Eco, 2005: 65). Autori tegelike kavatsuste välja uurimise või teoretiseerimise asemel võimaldab Eco mudeli strateegiat otsida tekstis väljendatud kavatsustest, mille alusel teeb järeldused ka auditoorium (Madisson ja Ventsel, 2020: 30).

Diskursiivne ülekanne uudisajakirjandusest sotsiaalmeediasse ning orgaaniline levik erinevate sotsiaalmeedia kanalite ja kasutajate vahel muudab narratiivi esmase autori tuvastamise ja ta kavatsuste analüüsimise keeruliseks, sest on raske tõmmata piiri kavatsusliku tegevuse ja lugeja omaalgatusliku tõlgenduse ja narratiivi taasloome vahele (Madisson ja Ventsel, 2020: 24). Seetõttu on Madisson ja Ventsel (2020: 30) oma mudelis mudelautori kontseptsiooni põiminud nii narratiivi loonud või levitanud tegeliku autori kui ka narratiivi sotsiaalmeedias võimendajad, lähtudes selles, et mõlemat ühendab strateegilise narratiivi puhul ühine eesmärk ja see väljendub diskursiivselt ka tekstis. Nii saab analüüsida autorit, kelle jaoks on eeldatavasti narratiivi tagajärjed kasulikud, ning lugejat, kes samuti (teadlikult või enese teadmata – vt ptk 1.1.5) autori strateegilisi eesmärke teenib (Puumeister, 2020).

Riigikaitse valdkonnas on infooperatsioonid ning strateegiline kommunikatsioon tihti vääriti mõistetud või alahinnatud (Murphy, 2008: 11) – eesmärgistatud, planeeritud ja proaktiivse tegevuse asemel pöördutakse strateegilise kommunikatsiooni poole reaktiivseks probleemilahenduseks kriisiolukorras (Muprhy, 2008: 12). See võib tuleneda konnotatsioonist, et „strateegiline“ tähendab „eesmärgistatud“, samas kui strateegilise kommunikatsiooni kontseptsioon viitab pigem süstemaatilisele rahvuslike huvide edendamisele läbi ühise tähendusvälja loomise. Strateegiliste operatsioonidega saab infokonflikti kujundada (Weedon, Nuland, Stamos, 2017) ning vastase otsustusprotsesse mõjutada, mis on tänapäevases rahvusvahelises konfliktis või sõjas isegi prioriteetsem siht kui territooriumi füüsiline hõivamine (Nissen, 2015: 52). Kui strateegilisi narratiive mõista kui avalikkuses levitatavaid representatsioone, millega määratakse tähtsate (ajalooliste) sündmuste ahelad ja tähendused ning mis mõjutavad inimeste käitumist (Ventsel, Hansson, Madisson, Sazonov, 2018: 104), siis sõjategevuse käigus muutub diskursiivne võim oluliseks ka liberaalsete demokraatiate jaoks, kes tegelevad nn. valitud sõdadega, mis nõuavad tugevat ja pidevat õiguspärasuse põhjendamist (Nissen, 2015: 23). Kui kaasaegse riigi keskne funktsioon on kaitsta ühiskonda väliste ja sisemiste ohtude eest ning tagada vabadus ja materiaalne heaolu (Spindler, 2013: 26), siis peab ka infojulgeoleku tagamine olema riigi ülesanne.

Informatsiooniline õõnestamine pole aga pelgalt hübriidsõjaga seonduv – strateegilisi narratiive kasutatakse avaliku arvamuse kujundamiseks, vaenlase eksitamiseks või kogukonna olukorrataju

muutmiseks ka rahuajal. Näiteks on Eestis uuritud, kuidas Zapadi õppuse eel, ajal ja järel levitati strateegilisi narratiive, mille abil konstrueeriti ja toodeti hirmu diskursiivselt (Ventsel, Hansson, Madisson, Sazonov, 2018: 104). Samas ei pea strateegiline eksitamine üldse seonduma militaarvaldkonnaga – käsikäes koroonapandeemiaga on Maailma Terviseorganisatsioon hoiatanud ka infodeemia eest (WHO, 2020), mis viirusest kiiremingi levib ja mida on põhjustanud vähene teaduspõhise informatsiooni analüüsioskus, infomüra ning tänapäevase infokeskkonna valeinformatsiooni levikut soodustavad eripärad.

1.1.4 Informatsioonilist mõjutustegevust soodustavad tingimused

Lähtun magistritöös teadmisest, et tänapäevane ühiskond on sügavalt mediatiseerunud. Stig Hjarvard (2008: 113) kirjeldab mediatiseerumist kui meedia intensiivistuvat ja pidevalt muutuvat tähtsust kultuuris ja ühiskonnas, mistõttu on ühiskond järjest enam meedia loogikast sõltuv. Meedia loogika osaks loeb Hjarvard (2008: 113) materiaalse ja sümboolse kapitali, tehnoloogilised ja institutsioonilised töömeetodid ning ametlikud ja kirjutamata reeglid, lähtudes Altheide ja Snow (1979) lähtepunktist, et meedia loogika mõjutab teadmist, mida ühiskonnas toodetakse ja levitatakse. Mediatiseerumise duaalsus seisneb selles, et ühelt poolt on meedia integreeritud osa teistest sotsiaalsetest institutsioonidest, teisalt ka oluline sotsiaalne institutsioon, sest vahendab suurt osa sotsiaalsest suhtlusest (Hjarvard, 2008: 113). Seetõttu sõltuvad ka autonoomsed institutsioonid erineval määral meediast (mida käsitlen töös selle kõige laiemas tähenduses, hõlmates ka uued meediumid ning sotsiaalmeedia, mitte ainult uudismeedia).

Meedia loogika on seega mediatiseerumise järjel kandnud ka teistesse eluvaldkondadesse. Inimese tähelepanu on saanud meedia- ja tehnoloogiasektori poolt hinnatud ja turu küllastumise tõttu ka järjest piiratumaks ressursiks. Professor Tim Wu kirjeldab tänapäevast meediamaastikku kui tähelepanumajandust, kus tähelepanu vahendajad – olgu nendeks Google, Facebook või veebipõhised osad traditsioonilisest meediast – pakuvad avalikkusele meelelahutust, uudiseid vm tasuta teenuseid ning müüvad selle tähelepanu seejärel reklaamiostjatele edasi (2019: 771-772). Selle piiratud ressursi kätte saamisel on abiks uued tehnoloogilised arendused.

Seda, kuidas oma tähelepanu jagame, jälgivad ühtmoodi nii uudis- kui ka sotsiaalmeedia platvormid. Tehisintellekt kogub personaliseeritud sisu pakkumiseks küpsiste abil andmeid meie digitaalse jalajälje ja käitumismustrite kohta (Kumar, Rajan, Rajkumar, Lecinski, 2019) – teisisõnu müüakse meie tähelepanu koos teadmisega, kuidas seda tähelepanu võita. Sobivat sisu esile tõstes ja sobimatut välja filtreerides saab tehisintellekti abil sujuvama kasutajakogemuse, sest näeme ainult meile sümpaatset sisu, aga see loob paratamatult virtuaalset paralleelreaalsust. See mõjutab ka meie käitumist – masinõppimise abil on võimalik 95% täpsusega ennustada, mida kasutajad järgmisena postitavad, isegi kui saadaval on *ainult* kasutaja sõprade andmed (Bagrow, Liu, Mitchell, 2019). Veebiuudiste ja sotsiaalmeedia populaarsus peamise uudiseallikana kasvab, samas kui televisioon ja trükimeedia on 9. aastat Reutersi raporti järgi langustrendis (Newman, Fletcher, Schulz, Andı, Nielsen, 2020: 14) – ka meediumite valik, mille kaudu infot saame, soodustab kallutatud ja subjektiivse maailmavaate teket.

Algoritmid soodustavad homogeensete rühmade koondumist, aga pärsivad diskussiooni ja lahkarvamusi, sest teisitimõtlejate seisukohad võivad tänu algoritmile varjatuks jääda. Nii Youtube'i kui ka Google'i otsingu-algoritmid näitavad varasemate tõekspidamistega sobituvat sisu ning see soodustab kõlakambrite (ingl *echo chambers*) teket. Kõlakambreid võib mõista kui keskkondi, kus sarnaselt mõtlevad inimesed võimendavad üksteisele sümpaatseid ideid või uskumusi (Cinellia, Morales, Galeazzi, Quattrociocchi, Starnini, 2021: 1). Seda toetavad sotsiaalmeedia funktsioonid nagu kommentaaridele reageerimine Facebookis ja suhtlusäppides või nende populaarsuse alusel lõimes kõrgemale tõstmise poolt hääletamine (ingl *upvote*), mis oli varem foorumite nagu Reddit või 4chan pärusmaa, aga on hiljuti ka Facebooki jõudnud.

Meie tähelepanu soovivaid äppe, platvorme ja meediumeid aina lisandub. Kui varem võis (sotsiaal-)meediatarbimist eraelu virtuaalse pikendusena mõtestada, siis nüüd võib rääkida tervetest valdkondadest, teenustest ja suhetest, mis eksisteerivadki ainult virtuaalsfääris. Muutused on inimkonna ajaloo toimunud nii lühikese aja jooksul, et see on meid teabekriisi lävele viinud – inimese mõistus pole mõeldud nii suures mahus reaalajas saabuvat infot vastu võtma, rääkimata selle analüüsimisest või kontrollimisest. Nii ongi otsustusprotsesse mõjutavad tehnoloogilised arengud nagu soovitusalgoritmid, informatsioonist üleküllastunud keskkond ning

aeglaselt kohanenud kasutajaskond loonud soodsa pinnase informatsiooniliseks mõjutustegevuseks.

1.1.5 Infokorratus ja informatsiooniline mõjutustegevus

Uurisin oma bakalaureusetöös (2018) vale- ja võltsuudiste levimist uudisajakirjanduses, mis oli 2016. aasta USA ja 2017. aasta presidendivalimiste ning Brexiti kontekstis sel hetkel nii kommunikatsiooni- ja poliitikauuringute vallas kui ka uudisajakirjanduses populaarseks teemaks. Sellest ajast on aga ingliskeelse termini „*fake news*“ konnotatsioon muutunud – poliitikud on termini kaaperdanud, et endale mittesobivat kajastust, ajakirjanikku või uudisetoimetust diskrediteerida (Wardle, Derakhshan, 2017: 5). Termin ei kirjelda enam informatsioonilise mõjustamise täit reaalsust: nt ei pruugi jagatav info olla uudise kuues, vaid levida meemi, manipuleeritud video (ingl *deepfake*) või uude konteksti asetatud pildina (Wardle, Derakhshan, 2017: 5). Samuti on strateegilised eksitajad – kelleks võib olla nii indiviid, rühm inimesi, riik kui ka organisatsioon – mõistnud, et eksitavaid narratiive on lihtsam uskuda kui neis on väike tõetera sees, seega ei pruugi info olla täielikult fabritseeritud (Wardle, 2019: 6). Seetõttu on siin töös Wardle ja Derakhsani (2017) eeskujul läbivalt kasutuses katustermin infokorratus (ingl *information disorder*), kontseptsioon, mis kogub ka rahvusvahelises teadusväljas populaarsust. Infokorratuse raami läbi on uuritud soolisi erinevusi valeinformatsiooniga tegelemisel (Almenar, Aran-Ramspott, Suau, Masip, 2021), analüüsitud platvormide tegevust valeinformatsioonile vastu seismisel (Ferreira, 2021); kaardistatud valeuudiste ühiskonnas leviku mehhanisme (Lazer, Baum, Benkler, Berinsky, Greenhill jt, 2018); analüüsitud infokorratuse pealetungi eksistentsiaalsena kujutavaid teadusartikleid, kus on valeuudiste leviku kohta eksitav info (Miró-Llinares, Aguerri, 2021) ning kaardistatud kaitsetaktika masinkirjutatud uudiste vormi imiteerivate valenarratiivide leviku vastu (Zellers, Holtzman, Rashkin, Bisk, Farhadi jt, 2019).

Infokorratust võib tekitada väärinformatsioon (ingl *misinformation*), mis on kogemata leviv vale, ebatäpne või mitmeti tõlgendatav informatsioon; desinformatsioon (vn *Дезинформация*), mis on fabritseeritud eesmärgiga info vastuvõtjat eksitada (Karlova, Fisher, 2013: 3) ning vaenulik informatsioon (ingl *malinformation*), mis on faktipõhine, aga levitatud strateegilisel ajahetkel eesmärgiga isikut, gruppi või organisatsiooni kahjustada (Wardle, 2019: 8). Väärinformatsioon

muutub desinformatsiooniks siis, kui info avaldaja tahab sihilikult vastuvõtjat eksitada (Karlova, Fisher, 2013: 4), ning sarnaselt võib desinformatsioon muutuda väärinformatsiooniks kui pahaaimamatu lüli infot heas usus edasi jagab (Wardle, 2019: 8).

Seega – eksitavat informatsiooni tuleks sisuka analüüsi huvides levitaja motiivide alusel eristada. Wardle ja Derakshan (2017: 20) kuuluvad uurijate sekka, kelle arvates võiks motiive jaotada selle järgi, kas eksitava informatsiooni levitamise eesmärgiks oli subjektile kahju tekitada. Jaotust võib Karlova ja Fisheri (2013: 3) eeskujul teha ka eksitamise sihipärasuse järgi. Sõltuvalt eksitajast võib saadud kasu ja kasutatud eksitamise vorm erineda, ent kavatsus eksitada on leide konteksti asetades siiski tajutav.

Kavatsuslik eksitamine võib olla motiveeritud soovist saada rahalist, poliitilist, psühholoogilist või sotsiaalset kasu (Wardle, 2019: 8). Rahalist kasu teenitakse infokorratusest reklaamiraha abil, mida toob sisse veebilehe liiklus (Wardle, Derakshan, 2017: 26) ning võib eeldada, et ka sisu produktsiooni eest. Poliitiline kasu võib hõlmata konkurendi diskrediteerimist, aga ka üldisemaid püüdeid informatsioonilise mõjustamise abil avalikku arvamust ja käitumist mõjutada (Wardle, Derakshan, 2017: 26) ehk strateegilisi narratiive levitada.

Venemaa hübriidoperatsioone, mis võivad hõlmata nt automatiseeritud trollivabrikuid, sotsiaalmeedia kontosid ja klikifarme, on Eesti geopoliitilise asukoha ja ajaloolise kogemuse tõttu üsna palju uuritud. Näiteks on 2017. aasta Venemaa ja Valgevene suurõppuse Zapadi hirmu õhutamise mehhanisme läbi strateegiliste narratiivide uurinud Andreas Ventsel, Sten Hansson, Mari-Liis Madisson ja Vladimir Sazonov (2018), kelle eeskujul ja juhendamisel on valminud lõputöid ka Zapadi meediakajastustest ja narratiividest (nt Tamm, 2018; Siik, 2018). Läbi strateegilise kommunikatsiooni läätse on uuritud Baltimaade kujutamist Lääne veebimeedias Zapad-2017 kontekstis (Onno, 2019) ning samuti on uuritud (propagandistlikke) narratiive Ukraina kohta Vene meedias (nt Synitsyna, 2018; Halilov, 2015). Mari-Liis Madisson ja Andreas Ventsel (2018) on uurinud Zapad 2017 meediakajastustes ka fobofoobiat seoses küberohtude diskursusega. Uuritud on ka populistlikke diskursiivsed strateegiaid Eesti peavoolumeedias ja vastu-avalikkuses (Koppel, 2017). Wasin Punthong (2018) magistritöö keskendus Eesti strateegilisele vastulöögile Vene hübriidohtudele ning Johannes Voltri (2021)

kaardistas oma magistritöös Venemaa informatsioonilise mõjustamise vastu võitlemise strateegiad Baltikumis.

Eksitamise maailmalaval paistab riigi tasandil informatsioonilist mõjustamist korraldava maana silma ka Hiina, kelle nn 50-sendi armee (mis on nime saanud ühe postituse hinna järgi) tootis 2015. aastal 448 miljonit sotsiaalmeediapostitust eesmärgiga avalikkuse tähelepanu kõrvale juhtida asjaoludelt ja narratiividelt, mis võiksid protestide või režiimi vastu astumisega lõppeda (King, Pan, Roberts, 2016: 26). Samas ei pruugi desinformeerimise eesmärk tingimata olla info vastuvõtjat veenmine fabritseeritud sisu tõepärasuses, vaid pigem külvata kahtlusi ja üldist usaldamatust institutsioonide, organisatsioonide või riikide vastu (Wardle and Derakhshan, 2017: 30). Informatsiooniliseks õõnestamisstrateegiaks võib olla ka infoudu (vn *дезинформация*) loomine (2015: 11). Infoudu luuakse kasutades infokilde, vasturääkivusi, fabritseeritud või kontekstist välja rebitud teavet, et auditoorium ei teeks enam vahet õigel ja valel (Nissen, 2015: 12). Info üleküllus või narratiivi intensiivne kordamine võib segadust veelgi süvendada (Hansson, 2015).

Lisaks rahalisele ja poliitilisele kasule, võib kavatsusliku eksitamise motivatsiooniks olla ka sümboolses kapitalis väljenduv sotsiaalne kasu (Wardle, 2019: 8). Näiteks UN Refugee Agency pidi 2014. aastal vaeva nägema, et võidelda eksitavalt nende organisatsioonina esinenud smuugeldajate Facebooki postitustega: UNHCR logo kleebiti kaunite jahtide piltide peale koos numbriga, kuhu helistada, kui tahetakse turvaliselt Vahemerd ületada (Wardle, 2019: 33). Nii kasutati ära organisatsiooni usalduse krediiti, kleepides inimkaubanduse reklaamidele nende logo. Sama on tehtud ajakirjandusväljaannete kodulehtede disaini kopeerimisega üle maailma. Kavatsuslik eksitamine võib lisaks tuua veel ka psühholoogilist kasu – mõned eksitajad (ingl *trolls*) teevad seda lihtsalt lõbu pärast (Karlova ja Fisher, 2013: 6).

Mittekavatsuslik eksitamine võib tuleneda kiiresti muutunud infokeskkonnast ning vähe kohanenud kodanike kehvadest info tarbimise ja jagamise praktikatest – teisisõnu puudulikest info-, digi- ja meediapädevustest. Tehnoloogiline hüpe on sisu loomise ja levitamise teinud lihtsamaks kui kunagi varem, samas on info tootmine ja tarbimine kolinud privaatsfäärist avalikku (Wardle, Derakshan, 2017: 11) – see on omakorda teinud võimalikuks performatiivse

infokäitumise. Näiteks on uurijad (Gabielkov, Ramachandran, Chaintreau, Legout, 2016: 8) on leidnud, et enamikke uudiseid on Twitteris rohkem kordi jagatud kui avatud. Küsimus pole infokülluse tõttu vähese tähelepanu pööramises või allikakriitilisuse puudumises – informatsiooni jagatakse edasi sellega ise tutvumata.

Institutsionaalsel tasandil, nt ajakirjanduses, võivad mittekavatsuslikku eksitamist soodustada 24/7 uudisetsükliga kaasnevad tööpraktikad. Craig Silverman (2015: 2-3) on välja toonud, et kiiruse survel tehakse allikapesu ehk refereerimist (väljaanne ei töötle ise informatsiooni, vaid jagab teise väljaande avaldatud sisu), kontrollitakse allikaid liiga vähe (nii kirjalikke kui ka inimallikate faktiväiteid), ei looda terviklikku konteksti (lugude edasine arengukäik või jätkulood) ning kasutatakse pealkirjastamisel sensatsioonilisust ja demagoogiavõtteid. Tarbija ootab uudisajakirjanduselt ajakirjanduslikele standarditele vastamist, professionaalset informatsiooni töötlemist ning seega usaldab informatsiooni (Silverman, 2015: 3).

Infokorratus on seega nii mõneski aspektis tänapäevase infokeskkonna süvenevate probleemide sümptom. Informatsioonilise mõjutustegevuse ning sellele vastu seismise olulisus kasvab, sest „küberruumist on kujunenud üleilmse inimarengu, aga ka poliitilise võitluse ja sõjapidamise osa, küberruumist olenevad avalikud teenused," (Eesti julgeolekupoliitika alused, 2017: 5).

1.2 Küberohud ja küberkaitse võimekus

Teise alapeatüki eesmärkideks on esiteks välja tuua küberohtude ning küberkuritegevuse erinevused, et mõista uuringu fookuses olevat küberkaitse võimekust, teiseks näitlikustada küberohtude narratiivse konstrueerimise olulisust Eesti kui e-riigi mainekujunduse kontekstis ning kolmandaks anda ülevaade strateegiatest, millega Eesti riigi ja NATO tasandil ühiskonna sidusust ja vastupanuvõimet tõstetakse.

1.2.1 Küberkuritegevus

Küberkaitse võimekusest kõneledes tekib küsimus, mille vastu kaitsevõime töötama peaks ning mis on küberohu ja küberkuritegevuse vahe. Eesti Küberturvalisuse strateegia 2019-2022 (2019: 41) sedastab, et küberoht on võrgu- või infosüsteemi kaudu või vahendusel tekkinud sündmus

või asjaolu, mis võib tekitada kahju; küberkuritegevus on aga IKT-vahendite vahendusel toime pandud kuritegu. Semantilise käsitluse järgi võib olla küberoht hüpernüüm ehk ülemmõiste ning kübersõda, küberterrorism, küberkuritegevus ning küberspionaaž selle hüponoomid ehk alammõisted (Kuusk, 2013: 17).

Küberkuritegevuse vormideks võivad olla veebi poolt vahendatud või tehnoloogia poolt võimendatud rünnakud, häkkimisteenuste osutamine, musta turu kauba (relvamüük, narkootikumid, võltsitud dokumendid) veebis müümine, virtuaalse ja FIAT-valuuta rahapesu, pedofiiliafoorumitesse postitamine, aga ka *botnet*i (viirusega nakatunud või kaaperdatud kontode võrgustiku) abil seadmete kaugelt juhtimine ning nakatunud arvutisse „tagaukse“ jätmine korduvaks sissetungiks (Europol, 2020). Lunavararünnakud, mille käigus pahavara kas lukustab ohvri arvuti või varastab, krüpteerib, ähvardab avalikustada arvutis olevad andmed, oli Europoli Internet Organised Crime Threat Assessment (2019) raporti järgi jätkuvalt suurimaks ohuks. Küberkaitse võimekus erineb Euroopas riigiti märkimisväärselt: 2019. aasta jaanuari ja oktoobri vahel rünnati Hollandis 17.64% masinatest, samas kui Iirimaal kõigest 1.08% (McCarthy, 2020).

Küberkuritegude motiivid on erinevad: mõned neist sooritatakse rahalise kasu eesmärgil, mõned on kire- ja vihakuriteod, mõned ideoloogiast kantud (Leukfeldt, Lavorgna, Kleemans, 2017: 288). Samas võivad motiiviks olla ka uudishimu või igavus – nt tellis Rapla koolipoiss kooli IP-aadressile hajusa ummistusründe (DdoS), mille sai tumeveebist tasuta teenusenäidisena (Orav, 2021). Rõhk on enamasti just kasutaja või süsteemi andmete ära kasutamisel või varastamisel (Europol, 2020). Rikkumiste toimepanijad on tõenäoliselt korraga seotud mitut liiki küberkuritegudega (Leukfeldt, Lavorgna, Kleemans, 2017: 288).

See magistritöö ei keskendu mitte ülalkirjeldatud riigipiiride ülesele *de facto* küberkuritegevusele, vaid uurib Eesti ja NATO küberkaitse võimekuse konstrueerimist läbi diskursiivse mõjutamise. Teisisõnu ei ole fookuses mitte konkreetsed küberrünnakud või -intsidendid, vaid strateegilised narratiivid selle kohta, mis järeldusi nende intsidentide kontekstis Eesti või NATO tasandil tuleviku kohta tegema peaks (vt ptk 1.1.3). Nagu nenditakse Eesti Küberturvalisuse strateegias (2019: 8): kui küberturvalisus on tehnoloogilise ja institutsionaalse võimekuse ning teadliku rakendamise küsimus, siis ühiskonna turvatunnet mõjutab ka see,

kuidas küberturvalisust *tajutakse*. Kui infokeskkond koosneb kolmest – füüsilisest, informatsioonilisest ja tunnetuslikust – mõõtmest, siis just tunnetuslikus dimensioonis reageerib inimene informatsioonile ning teeb otsuse, kuidas edasi käituda (Nissen, 2015: 40). See soodustab informatsioonilise mõjutustegevuse edu: oluline pole mitte see, mis on objektiivne reaalsus, vaid see, kuidas tajub reaalsust subjekt.

Narratiivid ebapädevusest või puudujääkidest IKT-valdkonnas on riikidele nagu Eesti, kus riik pakub kodanikele hulgaliselt e-teenuseid, mõistagi olulisem kui mõnele teisele. Ka Eesti bränd toetub tugevalt IKT-alaste innovatsiooniliste lahenduste rõhutamisele.

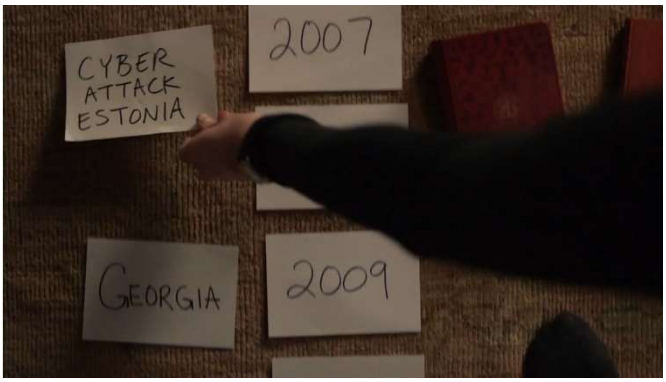
1.2.2 Digiriik Eesti

Pärast Eesti taasiseseisvumist hakati avalike enesekirjelduste läbi rõhutama, et Eestil on võimalik innovaatiliste IKT-lahendustega demokraatia ja valitsemise vallas maailma areenile tõusta (Madisson, 2016: 13). Küberoptimistlik diskursus langes ajaliselt kokku Eurovisiooni võõrustamisega 2002. aastal, mis viis brändiloome tellimiseni ettevõttelt Interbrand, eelarveks 13.31 miljonit krooni ehk 850 000 eurot (Jansen, 2008: 128). Arendati välja ka „Welcome to Estonia“ loosung (Jõesaar, 2015: 37), mida kasutas lisaks eraettevõtetele veel ka näiteks lennujaam.

Narratiivist on saanud reaalsus. Küsimusele, kas enne tuli Eesti kui digiriigi brändiloome või tuli brändiloome, sest digiriik eksisteeris, on tagantjärele sama keeruline vastata kui küsimusele, kas enne oli muna või kana. 2002. aastal tutvustati ID-kaardi süsteemi, 2005. aastal sai kohaliku omavalitsuse valimistel ja 2007. aastal Riigikogu valimistel e-hääletada ning 2014. aasta oktoobris võeti vastu eelnõu, millega sai seadusliku aluse e-residentsuse projekt (Tammpuu, Masso, 2018: 548). 2000-ndate alguse narratiivid Eestist kui progressiivsest ja kaasaegsest põneva ajalooga riigist, mis on üleminekuperioodist väljunud ja maailmale avatud; Eestist kui uuest Skandinaaviast või omamoodi Põhjamaast ning Eestist kui IT-riigist (Jansen, 2008: 128) on ka täna levinud, ehkki 2008. aasta kampaania taaskäivitamise ajal sai paremaks muutumise narratiivist hoopis loosung heade üllatuste maa“ (Jõesaar, 2015: 39). E-Eesti rahvusliku identiteedi disainimise käigus tekkinud tähendustepakett kujutab meid innovaatilise paberivaba

ja digitarga riigina (Madisson, 2016: 13) ning Eesti auditoorium on seetõttu tõenäoliselt e-ohunarratiivide suhtes ka tundlikum (Madisson ja Ventsel, 2018: 183).

E-edulugu täiendab heroilise nüansiga 2007. aasta Pronkssõduri kuju eemaldamisele järgnenud aprillirahutuste ja küberrünnakutele, mille käigus halvati Riigikogu, ministeeriumite, ajalehtede, pankade jm oluliste organisatsioonide lehed, vastu pidamine ja nendest tugevamana väljumine (Madisson, 2016: 13). Seda käsitletakse tagantjärele kui ühte esimest ainult küberruumis toimunud sõda (Jansen, 2008: 130) või kui esimest Lääneriigi küberründamist teise riigi poolt (McDermott, 2017: 1). NATO Küberkaitsekeskuse Oivakeskus avati aasta hiljem, vähem kui 200 meetri kaugusel Pronkssõduri uuest asukohast Rahumäe kalmistul (Juurvee, Mattiisen, 2020: 33). Intsident on isegi igaveseks popkultuuri raiutud: 26. aprillil 2020 linastunud Kodumaa (ingl *Homeland*) seriaali 8. hooaja 12. osas paneb peategelane Carrie kokku ajajoont suurimatest Venemaa salajastest mõjutusoperatsioonidest alates Külmast sõjast, kus on esindatud ka Eesti küberrünnakud.



Kuvatõmmis 1 - 2007. a küberrünnak seriaalis Homeland

Tagant järgi on leitud, et diplomaatilised meetmed ja Eesti negatiivses valguses Vene riigimeedias kajastamine algas juba jaanuaris 2007, mil salaoperatsiooni läbi viiv üksus tõenäoliselt oma käsud sai (Juurvee, Mattiisen, 2020: A-2). Vladimir Putin pidas 10.02.2007 Müncheni julgeolekukonverentsil, milles kritiseeris Ameerika Ühendriikide unipolaarset ja rahvusvahelist õigust eiravat hegemooniat ning NATO laienemist Ida-Euroopasse, osutades 90ndatest pärit tsitaadiga justkui oleks NATO peasekretär lubanud, et Saksamaast kaugemale NATO väed ei liigu (Kreml, 2007). Putin lubas eelmainitule vastu seista ning kinnitas, et Venemaa tõuseb edaspidi rahvusvahelisel areenil arvestavaks mängijaks (Kreml, 2007). Prohvetlikule kõnele järgnesid konkreetsed teod. Eestis kasutati kõiki hübriidsõja meetmeid nagu ka 2008. aastal Gruusias ning 2014. aastal Ukrainas, ainsaks erinevuseks on see, et seal oli ka militaarne jõud kaasatud – ei Gruusia ega Ukraina pole NATO liikmed (Juurvee, Mattiisen,

2020: 16). NATO Artikkel 5 mängib geopoliitilise olukorra stabiilsena hoidmise juures olulist rolli ning peasekretär Jens Stoltenberg on kinnitanud, et artikkel 5 käivitub ka küberrünnaku korral – seda juhul kui tagajärjed piisavalt tõsised on (NATO, 2015).

E-ohtude tõsidust ja võimalikke mõjusid rõhutavad narratiivid võivad destabiliseerida (Madisson ja Ventsel, 2018: 182). Strateegiliste narratiivide levitamine hetkel, mil pinnas on selleks soodne, sest teema on relevantne või on avalik arvamus mõne pretsedendi tõttu muutumiseks küps, võimaldab neil orgaaniliselt kaugemale levida ka teadmatuses vahendajate kaudu (ingl *useful idiots*). Selline diskursiivne nihe toimus näiteks ID-kaartide turvalisusega seoses kui 2017. aasta sügisel avastati kiipides teoreetiline turvarisk ning meediakajastus maalis väga tumeda pildi (Ventsel, Madisson, 2018: 127), selmet rõhutada kuidas turvariski avastamine kontrolli käigus enne kui rünnak on saanud toimuda, näitab tugevaid turvalisuse tagamise ja ennetamise tööprotsesse.

Seetõttu on selle magistritöö valim (vt ptk 3.1) meediatekstid, mis ilmusid kahe viimase aasta jooksul toimunud tõsisema Eestiga seotud küber-intsidendi eel, ajal ja järel: novembris 2020 rünnati korduvalt majandus- ja kommunikatsiooniministeeriumi (MKM) ning tervise ja heaolu infosüsteemide keskust ehk TEHIKut (Liive, 2020a). Terviseametist lekkis 180 MB jagu terviseandmeid kehva digihügieeni tõttu: hoolimata spetsialistide hoiatustest hoiti krüpteerimata kujul Drupali sisuhaldustarkvaras LimeSurvey andmebaasi koroonapositiivsete andmetega (Liive, 2020b). Teine intsident ei juhtunud mitte riigi, vaid eraettevõttega Citybee, kelle 100 000 kliendi andmed varastati ja riputati veebruaris 2021 avalikult üles hinnaga umbes 2,1 eurot kogu andmestiku eest (Liive, 2021). Ehkki rünnak ise leidis tõenäoliselt aset 2018. aastal, kui Citybee Eestis veel ei tegutsenud (Liive, 2021), pakub see huvitavat analüüsimaterjali just narratiivse konstrueerimise ja järgnenud avaliku arutelu poolest.

1.2.3 Julgeolekustamine ja ühiskonna vastupanuvõime

Eelnevalt välja toodud Citybee andmelekke ja TEHIKu rünnaku puhul võib tekkida küsimus, millised tehnilised või protseduurilised lahendused oleks aidanud intsidente vältida, aga see magistritöö ei püüa võtta seisukohta arvuti, võrgu, ettevõtte või riigi küberkaitse võimekuse *tehnilise* täiendamise ja arendamise osas. Lähtun Kopenhaageni koolkonna seisukohast, et

küberkaitse ühendab endas arvuti turvalisust ning julgeolekustamist (ingl *securitization*) (Hansen, Nissenbaum, 2009: 1160) – viimase all peetakse riigikaitse kontekstis silmas (strateegiliste) narratiivide loomet ja sõnumite levitamist (Paas, 2021: 10) ning seal lasub ka magistritöö fookus.

Julgeolekustamine on diskursiivne akt, mille käigus kujutatakse osutatavat objekti ehk referentobjekti erakorraliselt ohustatuna ning kiiret kaitset ja abi vajavana (Hansen, Nissenbaum, 2009: 1156). Julgeolekustamise aktiga konstrueeritakse teemast eksistentsiaalne oht (Waever, 1995: 54), selleks et julgeolekustaja saaks auditooriumilt raskete otsuste tegemiseks heakskiidu (Paas, 2021: 10). See ei pruugi aga olla auditooriumi huvides: näiteks Madisson ja Ventsel (2018: 185) on välja toonud, et „sageli toob teatud ohule (nt küberterrorismile) jõuline reageerimine (nt kui internetikasutust hakatakse rangelt kontrollima) kaasa tõsisemaid probleeme teistes valdkondades (nt piiratakse sõnavabadust ja jälgitakse kõike).“

Kui ajalooliselt vaadati julgeolekustamise referentobjekte kui (enamasti) kavatsuslikke tegutsejaid riigi või organisatsiooni tasandil, siis Hansen ja Nissenbaum (2009: 1160) rõhutavad küberkaitse aspektist ka süsteemitasandi ohte. Seda võib tajuda isegi suurema ohuna – näiteks Madisson ja Ventsel (2018: 181) on märkinud, et „IKTd tajutakse normaalseks eluks vajaliku pidevalt areneva taristuna, kuid samas ka seni tundmatute ja tavamõistuse jaoks raskesti hoomatavate riskide allikana.“ Kui valdkonda seostatakse keeruliste kontseptsioonide ning kitsaste spetsialistide ringiga, võib tavainimesel tekkida mure, et potentsiaalselt ohtlikud seadmed ja vähene teadlikkus võivad neist ja nende kontaktide võrgustikust teha vaenulike jõudude ohvri (Hansen, Nissenbaum, 2009: 1166-1167). Kuidas selle vastu võideldakse?

Kodanikuühiskonna võimestamise ning vastupanuvõime tõstmise oluliseks komponendiks on teadlikkuse tõstmine (Pamment, Nothhaft, Agardh-Twetman, Fjällhed, 2018: 83). Teadmiste suurendamisele põhinevad faktipõhine lähenemine, mis rõhutab faktikontrolli, ümberlükkamise ning valede või kahjulike narratiivide ümber raamistamise olulisust; vastu-narratiivide lähenemine, mis hõlmab eksitava narratiivi kitsaskohtadele osutamist ja ümber raamistamist ning vastu-propaganda lähenemine, mis on selle agressiivsem vorm ja hõlmab riigi tasandil strateegiliste narratiivide loomet ja levitamist (Pamment jt, 2018: 83-84). Sealjuures võivad need

lähenemised esineda ka põimunult või vahelduvalt: nt Eestis teostavad faktikontrolli erameediakanalid Delfi ja Postimees, meediapädevuste suurendamist koordineerib Haridus- ja Teadusministeerium, samas kui rahvusringhäälingu projekt Meediataip on võtnud ette ühiskonna mitteformaalse harimise ning strateegilise kommunikatsiooniga tegeleb Riigikantselei. Nende lähenemiste seast võiks eristada ennetuse ning tagantjärele olukorra silumist või kriisikommunikatsiooni. Faktikontrolli või vastunarratiivide levitamise lähenemise miinuseks on võimalus, et eksitava informatsiooni levikut võimendatakse tahtmatult veelgi enam, sest seda võivad näha ka inimesed, kelleni esialgne informatsioon ei jõudnud – samas eksitavat infot tarbinud algsed lugejad ei pruugi jälle faktikontrollini jõuda (Guess, Nyhan, Reifler, 2018: 6). Inimeste psühholoogia tõttu on keeruline ka väärarusaamu jäädavalt muuta, sest inimesed muudavad kinnistunud tõekspidamisi harva (Lewandowsky, Ecker, Seifert, Schwarz, Cook, 2012: 114) ja klammerduvad vastuolude esitamisel veelgi tugevamalt varasemalt tuttava ja tõeks peetud info külge (Silverman, 2015: 46).

Üheks vastupanutaktikaks on veel ignoreerimine, mille eesmärk on minimeerida informatsioonilise mõjustamise levikut ühiskonnas, keeldudes neile kõlapinda andmast (Pamment jt, 2018: 85). Kui julgeolekustamise eesmärk on auditooriumit veenda koheses, erakorralises, tagasipööramatus hädaohus (Hansen, Nissenbaum, 2009: 1164), siis ignoreerimise abil saab mingil määral levikut piirata. Läheneda võib ka koostööpõhiselt, rõhutades vajadust rohkemate riiklike ja piiriüleste koostöövõrgustike järele, et ühiselt informatsioonilisele mõjustamisele parimaid praktikaid jagades vastu seista (Pamment jt, 2018: 84). Ka see on Eestile omane lähenemine, sest 2021. aasta koalitsioonileppe Euroopa Liidu sektsioonis seisab lubadus: „Oleme Euroopa Liidus eestvedajad väärinfo ja avaliku inforuumi manipuleerimise vastases võitluses," (Valitsuse moodustamise kokkulepe…, 2021).

Regulatiivse lähenemise eesmärk on luua selgust hallis alas, kus meediaettevõtted tegutsevad ning lävendi tõstmise meetod hõlmab kombineeritult hea vastupanuvõimega riigiasutuste üles ehitamisest, elanikkonna teadlikkuse tõstmist ning aktiivset rikkujate (eksitajate või mõjutajate) üles otsimist ja karistamist (Pamment jt, 2018: 85). Kõige karmim ja vastuolulisem nö silm silma vastu lähenemine võib hõlmata näiteks rangete regulatsioonide tutvustamist meediaettevõtete tegevuse piiramiseks, ülekande takistamist või tsensuuri või kineetilisi küberoperatsioone

(Pamment jt, 2018: 85) – küberrünnakuid, mis tagajärjed võivad otseselt või kaudselt füüsilist kahju, vigastusi või surmajuhtumeid põhjustada (Applegate, 2013: 2).

Johannes Voltri (2021) analüüsis oma magistritöös Baltikumi valitsuste lähenemisviise Venemaa informatsioonilisele mõjustamisele vastu seismiseks neljal tasandil: kodanikuühiskonna õõnestamisest kõnelemine strateegilistes dokumentides, strateegilise kommunikatsiooni taktikad, meediakirjaoskuse arendamine formaalhariduses ning meediapoliitika ja regulatsioonide tasandil tegutsemine. Voltri uuringust selgus, et Balti riikide lähenemine ei ole ühtlane: kui Leedu on keskendunud informatsiooni turvalisuse tagamisele, siis Eesti lähenemine kõneleb avarast julgeolekust ja psühholoogilisest kaitsest ning Läti lähenemine, nagu ka geograafiline asukoht, on kuskil nende kahe vahel (Voltri, 2021: 106).

1.2.4 Eesti ja NATO strateegiline koostöö

Avar julgeolek tähendab Eesti kontekstis julgeoleku mõistmist kui „riigi ja selle rahva võimet kaitsta endale omaseid sisemisi väärtusi ja eesmärke mitmesuguste väliste poliitiliste, sõjaliste, majanduslike ja ühiskondlike ohtude ja riskide ning nende koosmõjude eest ja saavutada nende ohtude ja riskide tasalülitamine. Selleni jõudmiseks rakendatakse koordineeritult stabiilse ja rahuliku keskkonna kujundamisel ja alalhoidmisel oma osa etendanud riiklikke ning valitsusväliseid kehameid ja vahendeid,“ (Eesti julgeolekupoliitika alused, 2017: 2). See lähenemine toetub paljuski strateegilise kommunikatsiooni, mille all peetakse silmas poliitiliste, majanduslike ja riigikaitseliste sõnumite ja tegevuse plaanimist ning ühtseks informatiivseks tervikuks koondamist, ja psühholoogilise kaitse teineteist täiendavale kombinatsioonile (Eesti julgeolekupoliitika alused, 2017: 19). Psühholoogiline kaitse ehk elanikkonna teavitamine vaenulikust infotegevusest on suuresti reaktiivne, aga strateegiline kommunikatsioon peab ka võimendatud infomüras ühiskonnani ja oluliste välismaiste sihtrühmadeni jõudma (Eesti julgeolekupoliitika alused, 2017: 19). See hõlmab ka Eesti inforuumi, liitlassuhete ja kuvandi kaitset (Narits, 2015: 51).

Riigikaitse seisukohast on Eestile väikeriigina, mille sõjaline võimekus ei küündiks näiteks Venemaaga aastaid konventsionaalset sõda pidama, oluline strateegiliselt edendada riiklikku julgeoleku kommunikatsiooni, et arendada oma iseseisvat kaitsevõimet (Paas, 2021: 61). Kadri

Paas (2021: 62) jõudis empiirilises uuringus järeldusele, et riikliku julgeoleku kommunikatsiooni senise kaootilisuse juurpõhjuseks on selle poliitilisus ning seotus valimistsüklitega, mille vastu aitaks eesmärkide püstitamine näiteks 7ks-10ks aastaks; samuti soovitas ta asutuste- ja valdkondade üleselt välis-, sise- ja küberjulgeoleku kommunikatsioon ühendada, et sõnumeid ühtlustada.

Küberjulgeolek saavutatakse seega strateegiliselt alapeatükis 1.1 välja toodud ohtudeks valmistudes, ennetavaid kaitsemehhanisme luues, uusi strateegiaid arendades ning ühiskonna liikmete teadlikkust tõstes. „Eesti küberruum on kaitstav, kui riik ja ühiskond tervikuna selle kaitsmises osalevad, kui selleks on ette valmistatud vastavad spetsialistid ning ühiskond teab virtuaalmaailma ohtusid ja oskab neid parimal viisil vältida ning probleemide korral reageerida," (Eesti julgeolekupoliitika alused, 2017: 16). Ehkki julgeolekut käsitlevad NATO liikmesriigid erinevalt, on kõik Cyber Defense Pledge leppega ühinejad – sh Eesti – kinnitanud täielikku pühendumist riikliku infrastruktuuri ja võrkude kaitsele (Küberturvalisuse strateegia 2019-2022: 16).

Küberkaitsestrateegiate ühtlustamine on NATO fookuses olnud viimased 20 aastat. Kui NATO koos liitlasvägedega 1999. aastal nn Kosovo kriisi sekkus, sattusid nii NATO kui ka alliansis osalenud riikide valitsuste kodulehed küberrünnaku alla (Narits, 2017: 5). Intsident näitas esmakordselt liikmesriikide potentsiaalselt haavatavust ning järgmisel tippkohtumisel Prahas võeti vastu NATO Küberkaitseprogramm (ingl *NATO Cyber Defence Program*) (Narits, 2017: 10). See oli siiski deklaratsioonis teisejärguline teema ja seotud uute kasvavate ohtudega üldisemal tasandil, samamoodi nagu ka 2004. aasta Istanbuli tippkohtumisel kui ka 2006. Riia tippkohtumisel (Narits, 2017: 11). Teema aktualiseerumisele NATOs aitas kaasa 2007. aasta mai küberrünnak, mil paralleelselt Pronkssõduri rahutustega rünnati Eesti valitsuse asutuste, meediaväljaannete ning erakondade veebilehti hajusa ummistusründega (DdoS) (Herzog, 2011: 53).

Eesti valitsus ja meedia tituleerisid Venemaa rünnakute süüdlaseks enne, kui oli leitud vettpidavaid tõendeid, et küberrünnaku taga oli justnimelt Venemaa Föderatsiooni valitsus – tõendid on kaudsed, põimunud läbi erinevate kanalite ning paljuski teoretiseeritud lähtudes

kontekstist, paralleelselt toimunud sündmustest, rünnakute koordineeritusest ning sellest, et pole palju teisi rahvusvaheliste tegutsejaid, kelle huve selline rünnak võiks teenida (Herzog, 2011: 53). Sarnase käekirjaga küberrünnakud tabasid ka Leedut 2008. aastal, Gruusiat sõjalise agressiooni eel 2008. aastal ning Kõrgõzstani 2009. aastal. Kuna selleks ajaks oli Eesti e-riigi lahendusi juba arendanud ja rakendanud ning sõltuvus digiteenustest samuti teistest riikidest seega suurem, oli Eesti ahvatlev sihtmärk – teisalt oldi nii hästi ette valmistatud, et riik ei kaotanud kontrolli elektrijaamade, veepumpade ega relvasüsteemide üle (Herzog, 2011: 51-52).

Ettepaneku rahvusvahelise küberkaitsekeskuse rajamiseks tegi Eesti juba 2003. aastal NATOga läbirääkimisi pidades, aga enne 2007. aasta rünnakuid polnud selget otsust, millisesse mitmetest kandideerinud riikidest keskus rajada (Narits, 2017: 15). NATO Kooperatiivne Küberkaitse Kompetentsikeskus (milles kõik liikmesriigid ei osale) on NATO sõjaväestruktuuri kuuluv teadus- ja uurimiskeskus, mille üheks esimeseks projektiks oli Tallinna Käsiraamat (ingl „*Tallinn Manual on the International Law Applicable to Cyber Warfare*“, 2013) – töötati välja põhimõtted, kuidas küberrünnakuid rahvusvahelise õiguse kontekstis käsitleda, kuidas end kaitsta ning kuidas peaks riik või liikmesriigid reageerima (Schmitt, 2015: 12-14). 2014. aasta Walesi tippkohtumise deklaratsioon sätestab juba, et rahvusvaheline õigus kehtib ka küberrünnakutele, et küberkaitse on osa kollektiivkaitsest ning et sellest tulenevalt võidakse ka küberrünnaku puhul artikkel 5 ellu (NATO, 2014).

2. UURINGU EESMÄRGID JA UURIMISKÜSIMUSED

Töö eesmärk on näidata, kuidas Eesti ja NATO küberkaitse võimekust Eesti ajakirjandusväljaannetes narratiivselt konstrueeritakse, et sellest omakorda teha nii riigikaitsega tegelevatele asutustele kui ka teaduslikku teadmisesse laiemalt omad järeldused.

Uurimisküsimused:

1) Kuidas konstrueeritakse Eesti ja liitlasvägede küberkaitse võimekust ajakirjandusväljaannetes?
    a) Millised on meediatekstides esitatud peamised temaatilised narratiivid, s.h. strateegilised narratiivid?
    b) Milliseid tegelasi konstrueeritakse ning kuidas nende aktiivsust või passiivsust kujutatakse?
    c) Milliseid tegevusi konstrueeritakse? Kuidas neid mineviku- ja tulevikunarratiividega seotakse?
    d) Millise narratiivide puhul on märgata intensiivistunud julgeolekustamisele omaseid tunnuseid? Millisena kujutatakse süsteemitasandit?
2) Kuidas hindavad valdkonna eksperdid välja joonistunud narratiive?
    a) Kuidas suhestuvad need ekspertide seniste kogemustega valdkonnas?
    b) Mis on sellise narratiivi laialdase leviku potentsiaalsed ohud ning võimalused?
    c) Milline tegutseja võiks nende hinnangul sellise narratiivi levitamisest kasu lõigata?
    d) Milline on korrelatsioon NATO küberkaitse võimekuse narratiivide ning Eesti-spetsiifiliste küberkaitse võimekuse narratiivide vahel?

3. MEETOD JA VALIM

Käesolev magistritöö toetub kvalitatiivsele uurimismeetodile, mis on sobiv sotsiaalse kogemuse uurimiseks, kirjeldamiseks ja tõlgendamiseks (Laherand, 2012: 15) ning millegi kirjeldamiseks, mida pole varem piisavalt uuritud (Laherand, 2012: 290). Kvalitatiivne uurimismeetod sobib ka töö sotsiaalse konstruktivismi raamistikku, sest tugineb põhimõttele, et reaalsus on taju-põhine, subjektiivne ja muutub ajas (Joubish, Khurram, Ahmed, Fatima, Haider, 2011: 2083). Varasemates narratiivide uuringutes (vt ptk 1.1.5) on kombineeritud kriitilist diskursuseanalüüsi, kontentanalüüsi temaatilist analüüsi; on toetutud nii mänguteeoriale ja konfliktiuuringutele; laenatud teadmist nii meediauuringutest, semiootikast kui ka militaarse retoorika uuringutest.

Kasutasin magistritöö esimeses etapis strateegiliste narratiivide analüüsiks oma juhendaja Mari-Liis Madissoni ja Andreas Ventseli semiootilist mudelit (2020) (vt ptk 1.1.3), mis kombineerib Miskimmoni, O'Loughlini ja Roselle'i (2012) rahvusvaheliste suhete poliitikanarratiivide uurimismeetodi Umberto Eco (2005) mudellugeja kontseptsiooniga. Miskimmoni jt mudelit on lõputöös kasutanud ka Kapitolina Synytsina (2018), Priit Tamm (2018) ning Johannes Voltri (2018), kes on meedianarratiive uurinud kriitilise diskursusanalüüsiga. Kaasasin ka Kopenhaageni koolkonna julgeolekustamise teooria (vt ptk 1.2.3), mis oli mõned aastad tagasi nii temaatilistes kodumaistes lõputöödes (nt Gering, 2015; Listmann, 2014; Oksaar, 2014) kui ka rahvusvahelistes uuringutes (nt Balzacq, Léonard ja Ruzicka, 2016; Gad ja Petersen, 2011; Lacy ja Prince, 2018) populaarne analüüsiraamistik. Tegutsejate kirjeldamiseks kasutan Bergstrandi ja Jasperi (2018: 231) arhetüüpe, et analüüsida kuidas tegelasi kujutati – seda on hiljuti kasutatud ka nt meemides kujutatud tegelaste kirjeldamiseks (de Saint Laurent, Glăveanu ja Literat, 2021).

Rakendasin mudelit valimil, milleks olid artiklid, mis ilmusid kahe küberkaitse võimekuse seisukohast olulise sündmuse (vt ptk 1.2.2) eel, ajal ja järel ning tulemuste sünteesimiseks ka kahe sündmuse vahelisel küberintsidentide poolest „rahulikul" testperioodil. Analüüsisin artikleid MaxQda tarkvaraga, mis oli mu eelistatud töövahendiks ka bakalaureusetöö (Klaassen, 2018) tarvis transkribeeritud materjali kodeerides. Töö teises etapis kodeerisin meediatekstid, et vastata esimesele uurimisküsimusele (vt ptk 2) ning selle alaküsimustele. Esitan välja joonistunud narratiivid neljandas peatükis. Kolmandaks etapiks oli fookusgrupp, mis aitas uuringust selgunud tulemusi laiemasse konteksti paigutada. Sellist tüüpi kombineeritud

uurimismeetodiga magistritöös annab fookusgrupp võimaluse siduda teoreetiline teadmine praktikute kogemuspõhise teadmisega ning aitab filtreerida ka trende ning anomaaliaid, lisades magistritöö tulemustele juurde usaldusväärsust ja seega ka praktilist väärtust.

3.1 Meediatekstide kvalitatiivne sisuanalüüs

Meediatekstide valimiks olid uudisajakirjanduses ilmunud artiklid, mis ilmusid kahe küberkaitselisest aspektist olulise sündmuse – 2020. aasta detsembris avalikuks tulnud TEHIKu rünnaku ja andmelekke ning 2021. aasta veebruaris avalikuks tulnud Citybee kliendiandmete varastamise ja veebis müümise – eel, ajal ja järel. Ehkki selle töö fookuseks pole analüüsida ainult konkreetsete sündmustega seotud diskursiivset mõjutamist (vt ptk 1.2.2), on uudisväärtustest tulenevalt mõistlik eeldada, et konkreetsed küberintsidendid ning nende meedias kajastamine aktiveerib laiema avaliku arutelu valdkonna ohtude ja riskide üle.

3.1.1 Valimi kitsendamine

Ajavahemikuks, mille sees valimiks olevad artiklid ilmusid, on seega 01.11.2020 – 31.03.2021. Kuna Eesti veebiväljaannete otsingumootorite funktsionaalsus ja tundlikkus erineb, otsisin valimiks olevad artiklid välja meediamonitooringu tarkvara Station ja märksõnapõhise otsingu abil. Kodumaise Station.ee tööriista kasutamise eeliseks on lisaks ühesugusele otsinguloogikale ka kattuvate artiklite ühe tulemuse alla liitmine, nii et nt väheste muudatustega avaldatud pressiteated või teistest väljaannetest refereeritud sisu koondatakse kokku. Kitsendasin Stationis otsingut lisaks ajavahemikule veel kahe parameetriga: 1) otsisin ainult eestikeelseid artikleid ning 2) valisin väljaannete kategooriast üleriigilised ja piirkondlikud ajalehed ning online meedia (jättes seega kõrvale raadio- ja telekanalid, ajakirjad ja uudisteagentuuride teated).

Märksõnade valik arenes lumepalli meetodil, mille käigus üks leid (või valimi subjekt) viib järgmiseni. Algul lähtusin kahe valitud küberintsidendi (vt ptk 1.2.2) meediakajastuste teemaviidetest: „andmebaas“, „andmeleke“, „isikuandmed“, „citybee“, „leke“, „küberrünnak“, „küberhügieen“, „digihügieen“, „LimeSurvey“, „küberkaitse“, „küberturvalisus“. Magistritöö eelmärgiks pole aga koguda andmeid ainult nende kahe intsidendi, vaid küberkaitse võimekuse konstrueerimise kohta laiemalt.

Liis Kuusk (2013) on teinud küber-sõnaliite ning valdkonna terminoloogia semantilise analüüsi. Tema eeskujul kaasasin küberohtude hüponüümid „kübersõda“, „küberterrorism“, „küberkuritegevus“ ja „küberspionaaž“ (Kuusk, 2013: 17) ning tegutsejate kirjeldamiseks „küberterrorist“, „häkker“, „kräkker“, „küberspioon“ ning „küberpolitseinik“ (Kuusk, 2013: 26). Alapeatüki 1.1.5 eeskujul lisasin algselt märksõnade hulka ka „infohäire“, „infokorratus“, „infokonflikt“, „infosõda“, „desinformatsioon“, „väärinformatsioon“, „vaenulik informatsioon“, „infoudu“, „infoküllus“, „infooperatsioon“ ning „fake news“ ning ptk 1.2 eeskujul „küberkaitse võimekus“, „küberjulgeolek“, „e-riik“, „phishing“, „lunavara“, „pahavara“.

Seejärel kitsendasin märksõnakogumit lähtudes selle magistritöö eesmärkidest ning eemaldasin esimeses etapis kõik märksõnad, mis on seotud küberkuritegevuse ehk politsei igapäevase vastutusvaldkonnaga, nt „küberrünnak“, „phishing“ ja „küberterrorist“. Teises etapis tegin alles jäänud märksõnadega esmaseid otsinguid ning eemaldasin strateegiadokumentides ja teadusartiklites kohatud märksõnad, mis otsingutulemuste järgi polnud (vähemal sel perioodil) laiatarbe kasutuses, nt sõnale „digihügieen“ oli vaid 2 vastet ning „infohäire“ ei toonud ühtegi tulemust. Nii jäi meediatekstide filtreerimiseks järgi 10 märksõna, mis tõid kokku vasteks 607 artiklit:

Tabel 1 - Märksõnade esinemissagedus

Märksõna	Vasteid 01.11.2020 – 31.03.2021 kokku
julgeolekuoht	130
desinformatsioon	105
küberkaitse	93
infosõda	87
andmeleke	64
infooperatsioon	43
häkker	42
küberjulgeolek	20
inforünnak	14
kübersõda	9
	607

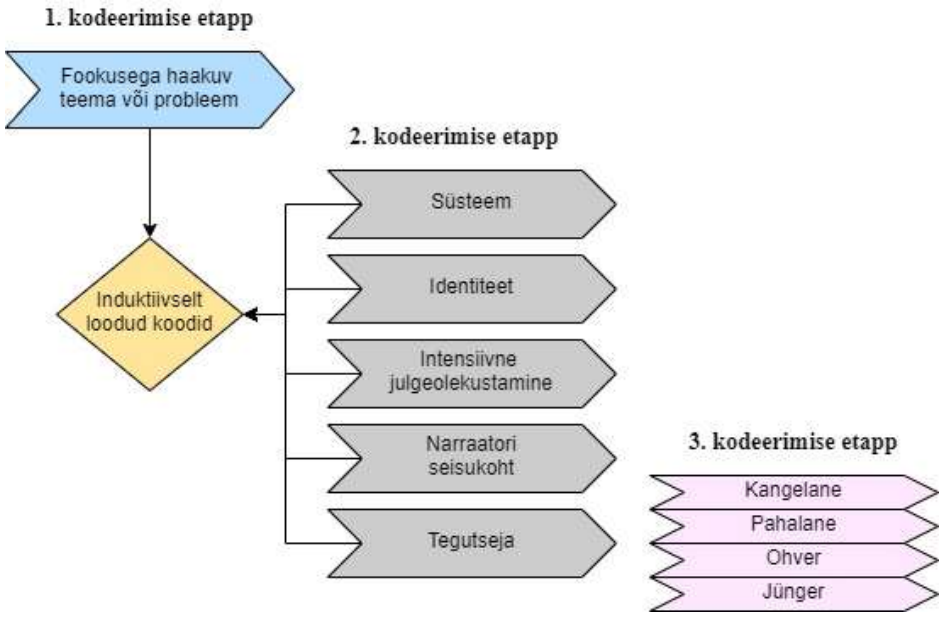
Magistritöö maht on 15 EAP ehk 390 tundi, mistõttu täies mahus valimi läbi töötamine pole võimalik, samuti pole kvalitatiivse uurimismeetodi puhul representatiivne valim vajalik. Sellest

lähtudes kitsendasin kolmandas etapis valimit ning selekteerisin kodeerimise etapiks iga viienda artikli. Meediatekstide otsinguks märksõnade kitsendamine ning 5-kuune avaldamisperiood võimaldavad vajaliku variatiivsusega valimi. Tegin seda Excelis, sisestades Stationist kõikide märksõnade puhul tabelisse iga viienda artikli koos autori, kuupäeva ja pealkirjaga. Vigade vältimiseks kandsid artiklid esialgu numbreid 1, 5, 15 jne, ning said koondtabelis lõpliku numbri, millele ka käesoleva töö tulemuste peatükis viitan, vahetult enne kodeerimist. Mõned artiklid olid juhuslikult valimisse sattunud mitme märksõnaga, ning pärast korduvate artiklite eemaldamist asusin lõpuks kodeerima valimit, millesse kuulus 109 artiklit (vt Lisa 1).

3.1.2 Narratiivianalüüs ja kodeerimine

Kombineerisin andmeanalüüsis deduktiivset ehk teooriast lähtuvat ning induktiivset ehk tulemustest lähtuvat lähenemist. Koostasin alguses deduktiivselt kodeerimisskeemi (vt Skeem 1), mida järgisin ning seejärel kodeerisin edasi alamkoode ning uusi kategooriaid luues induktiivselt. Kodeerimise esimeseks etapiks oli selle töö fookusest tulenevalt küberjulgeoleku või küberkaitse teema, keskse probleemi või poliitika kaardistamine. Nii sain veenduda, et valimisse pole sattunud artikleid, kus märksõna on sees, aga kasutuses teises kontekstis või teemaväliselt (nt artiklid nr 10 ja 15, vt Lisa 1), aga samas vabaneda ka analüüsitava materjaliga tutvumisel silma jäänud teemavälisest artiklitest (nt artiklid nr 36 ja 45). See vähendas uuritavat valimit 24-ja artikli võrra.

Teist etappi planeerides pidasin silmas Mari-Liis Madissoni ja Andreas Ventseli semiootilist analüüsimudelit (2020: 26), mis ühendab klassikalise süsteemi-, identiteedi- ja poliitikanarratiivide analüüsi (Miskimmon, O'Loughlin, Roselle, 2013: 10-11) Umberto Eco (2005: 60) mudellugeja ja mudelautori kontseptsioonidega. Poliitikanarratiivide analüüsimudelit Niisiis lõin esmalt koodid „Süsteem“ ja „Identiteet“, seejärel Kopenhaageni koolkonna eeskujul veel ka „Intensiivne julgeolekustamine“ ning Eco mudelautori tekstis väljendatud kavatsuste uurimiseks strateegilistes narratiivides (Madisson ja Ventsel, 2020: 30) veel ka koodi „Jutustaja seisukoht“. Pidades silmas Bolini, Jordani ja Ståhlbergi (2016: 14) tõdemust, et piirid (riigi) brändiloome, (avaliku) diplomaatia ja pehme jõu vahel on hägunemas ning rahvusvahelised tegutsejad liiguvad nende sfääride vahel võrdlemisi vabalt, lõin „Tegutseja“ juurde alamkoodid.



Joonis 1 - kodeerimisskeem

Bergstrand ja Jasper (2018: 231) on välja toonud arhetüübid, mille läbi analüüsida, kas tegelasi kujutati aktiivse või passiivse, heatahtliku või pahatahtlikuna. *Kangelased* on heatahtlikud ja tugevad ning nende moraalne kompass viib nad õigele teele ka juhul kui tegelast on alguses raske motiveerida (Bergstrand ja Jasper, 2018: 231). *Pahalased* on tugevad ja tihti intelligentsed nagu kangelasedki, ent pahatahtlikud ning seetõttu auditooriumi poolt kardetud ja vihatud (Bergstrand ja Jasper, 2018: 232). Tugevate ja aktiivsete tegelastena on kangelastel ja pahalastel tihti oma käsilased (ingl *sidekick*): *ohvrid* on heatahtlikud, aga nõrgad, mistõttu äratavad nad auditooriumis kaastunnet ning *jüngrid* on nii nõrgad, et on kahjutud kui just mõni pahalane neid massina mõjutama ei hakka (Bergstrand ja Jasper, 2018: 232). Niisiis lõin kolmandaks kodeerimiseks etapiks alamkoodid „Kangelane“, „Pahalane“, „Ohver“ ja „Jünger“.

Neljandas etapis jätkus töö induktiivselt loodud koodidega. Korrastasin neid, moodustasin analüüsikategooriaid ning korrastasin uuesti kuni jäin variatiivsusega rahule. Tulemused, mis magistritöö fookusega haakusid, esitan neljandas peatükis.

3.2 Fookusgrupp

Kombineeritud meetoditega magistritöö täiendavaks kvalitatiivseks andmekogumise meetodiks oli fookusgrupp. Bloor jt (2001: 17) on fookusgruppi soovitanud kvantitatiivsete meetodite, nt ankeetküsitluse täiendina, aga see sobis eesmärgiga saada magistritöö tulemuste konteksti asetamiseks ekspertide hinnanguid tulemuste asjakohasusele ja/või erakordsusele (Krueger, 2009: 6). Fookusgrupiga vastasin teisele uurimisküsimusele (vt ptk 2) ning selle alaküsimustele. Kuna meediatekstide analüüsi valimi ilmumisperioodiks oli 5 kuud, aitasid valdkonna eksperdid narratiive ka pikemasse ajalisse perspektiivi asetada – nii sain teada, millised narratiivid on värsked ning millised on juba mitmendat korda ringluses. Samuti võimaldas see täita infoauke, sest nagu ka Eco (2005: 58) on sedastanud, tõlgendab iga lugeja mitte-öeldut erinevalt. Oma tõlgendusväli on ka minul uurijana ning ekspertide kaasamine aitab seda subjektiivsust vähendada.

Eelistasin seda meetodit ekspertidel täiendava informatsiooni kogumiseks süvaintervjuu meetodile kolmel põhjusel. Esiteks on vastutusvaldkonnad psühholoogilise kaitse, strateegilise kommunikatsiooni ja küberjulgeoleku teemal Eestis erinevate institutsioonide vahel killustunud – seega üks inimene saab pakkuda vaadet narratiivi ühele poolele, teine jällegi oma teadmistega selle taustal täiendada. Teiseks on fookusgrupis info liikumine kindel ka juhul kui mõni inimene on loomu poolest napisõnaline või vajab usalduse tekkimiseks kauem aega – kindla kava, protseduuri ja plaani alusel saab fookusgrupis luua kõikidele mugava keskkonna, kus oma arvamusi ausalt avaldada (Krueger, 2009: 5). Kolmandaks oleks süvaintervjuusid vaja teha nii paljude erinevate inimestega, et see paisutaks magistritöö üle 15 EAP mahu. Grupivestlus kuue inimesega võimaldas eri vaatenurki analüüsi kaasata mõistlikuma töökoormusega.

Kutsusin 7. mail 2021 kella 10st 11.15ni toimunud grupivestlusesse sise- ja välisjulgeoleku strateege KAPO-st ja Välisluureametist, infooperatsioonide tuvastamise ja ennetamisega tegelevaid spetsialiste Kaitseministeeriumist, Küberväejuhatusest, NATO Kooperatiivsest Küberkaitsekeskusest, Propastopist kui ka, küberkaitse valdkonna eksperte Riigi Infosüsteemide Ametist, Rahvusvahelisest Kaitseuuringute Keskusest, Balti Kaitsekolledžist, Kaitseväe Akadeemiast ja Sisekaitseakadeemiast ning strateegilise kommunikatsiooniga tegelejaid

Riigikantseleist ja NATO StratComist – kokku ühendusin 14-ne organisatsiooni või eksperdiga. Tegemist oli seega sihipärase valimi ning homogeense valikuga töövaldkonna järgi; sotsiaal-demograafilistest tunnustest ma selle fookusgrupi kontekstis ei huvitunud.

3.2.1 Valim ja värbamise strateegia

Ekspertide strateegiline värbamine fookusgruppi toimus kahes etapis. Esmalt arutasime juhendajaga, millised organisatsioonid või eksperdid informatsioonilise mõjustamise ja küberkaitse võimekuse teemal kaasa võiksid rääkida. Organisatsioonide puhul, mille kodulehel polnud struktuuri või töötajate otsekontakte välja toodud, edastasin standardiseeritud kutse (vt Lisa 2) üldmeilile palvega see edastada informatsioonilise mõjustamisega tegelevale spetsialistile. Kodulehel avalikult välja toodud vastutusvaldkonna ja kontaktidega, juhendajale või mulle varasemalt tööalaselt tuttavad ning meedias asjatundjana sõna võtnud eksperdid said kutse fookusgruppi otsepöördumisena, samuti meiliga. Sellele järgnes veidi pikem kui nädala pikkune seisak. Teine etapp käivitus iseeneslikult vahetult pärast seda, kui kaks päeva enne fookusgrupi toimumisaega, st 5. mail, saatsin osalejatele kokkuleppeliselt koos Zoomi lingiga meeldetuletuse grupivestluse toimumise ning andmete kogumise ja kasutamise kohta. Andsin mh teada, et võime planeeritud 1h 45min asemel loodetust väiksema seltskonna tõttu pool tundi lühema ajaga arvestada – osaluse oli selleks hetkeks kinnitanud neli eksperti. Seepeale jagas üks osaluse kinnitanud ekspertidest mulle telefoninumbreid, mille järel kommunikatsioonikanalid avanesid ning ööpäeva jooksul kinnitas oma osaluse veel kaks eksperti.

Kokku osales fookusgrupis kuus eksperti, kes töötavad Riigikantseleis, Kaitsepolitseis, NATO StratComis, Riigi Infosüsteemi Ametis, Propastopis ning Kaitseväe Akadeemias, aga jäid töös vastavalt fookusgrupi eel tehtud kokkuleppele anonüümseks, kandes siin töös NATO kuuldekoodi tähiseid (vt Tabel 2). Ainsa tunnusena palusin allikatel välja tuua oma subjektiivse hinnangu tööstaažile, mis võiks allika pädevuse hindamisel olla üks anonüümsust hoidev, aga lugejale lisateadmist pakkuv detail. Lisaks olen Tabelis 2 välja toonud ka fookusgrupi sisulise osa kõnevoorude arvu, selleks et lugejale grupi-sisest dünaamikat näitlikustada.

Tabel 2 - Ekspertide tähised, kogemus informatsioonilise mõjustamise valdkonnas ning kõnevoorude arv

Eksperdi tähis	Kogemust valdkonnas (aastaid)	Kõnevoorude arv (kokku)
Alfa	3	11
Bravo	5	5
Charlie	4	5
Delta	20	12
Echo	5	6
Foxtrot	14	7

Otsustasin anonüümsuse tagada, sest uurimuse fookuses polnud mitte infoallikate isik või nende tööandja avalik seisukoht, vaid individuaalne kogemus ja ekspertarvamus. Poliitiliselt ja diplomaatiliselt korrektse, asutuse huvisid esindava vastuse formuleerimine ja isikustatult presenteerimine oleks asjakohane nt riikliku või NATO-ülese strateegia elluviimist konkreetses asutuses uurides, aga mind huvitas allikate kogemus ka *eelnevates* riigikaitsega valdkonna ametipositsioonides. Näiteks Alfa ja Echo on esimesel informatsioonilise mõjustamise ja/või avara riigikaitsega seonduval töökohal, samas kui Charlie praegusele ametile eelneb 10 aastat mitmes erinevas asutuses riigikaitse valdkonnas. Allikad oleksid nimelise viitamise korral pidanud sõnu valima ka seetõttu, et valdkonna organisatsioonide avalikud seisukohad ka ühe ja sama narratiivi või tegutseja osas erinevad olenevalt ajaperioodist – nii ei oleks salastatud infoga tegelema harjunud spetsialistid pruukinud üldse eelnevate riigikaitsega seonduvate ametipositsioonide kogemusi üldse edastada.

Tegemist oli ka eetilise valikuga – tean, et uurin teemat, millel on mitmeid uudisväärtuslikke tunnuseid nii kodumaise meedia kui ka vaenuliku infomatsiooni levitajate jaoks. Mitmed allikad on oma organisatsioonide tuntud kõneisikud, mis teeb nende kommentaaride kontekstist välja rebimise ahvatlevamaks. Seetõttu otsustasin, et ainus viis uurijana käesolevas magistritöös väljendatud seisukohtade eest täielikult ja ainuisikuliselt vastutada, on oma allikate identiteeti kaitsta. Kogutud andmeid hinnates arvan, et allikate isik üheskoos mõningate kommentaaride värvika sõnakasutusega, oleks uudisajakirjandusele kindlasti huvi pakkunud. Seega oli otsus grupivestlusest kogutud andmete mitmekülgsena hoidmiseks allikate anonüümsus tagada minu hinnangul õigustatud (vt ptk 3.3).

3.2.1 Fookusgrupi strateegiline kava ja kulg

Fookusgrupi viisin läbi poolstruktureeritud kava järgi (vt Lisa 3). Deakin ja Wakefield (2014: 604) on välja toonud, et veebiintervjuusid saab ja peabki käsitlema eraldiseisva uurimismeetodina. Videokõne formaat ei tulenenud pandeemiaga seotud riiklikest piirangutest, vaid planeerisin sünkroonse grupivestluse algusest peale digitaalsesse keskkonda, sest kõik allikad ei ela ega tööta Eestis. Lähtusin varem koostatud strateegilisest kavast, aga muutsin vastavalt vestluse kulule küsimuste järjekorda, jätsin tehniliste tõkete ja ajapuuduse tõttu kõiki osalejaid kaasavad ülesanded planeeritud kujul vahele ning küsisin kuulamispõhiselt ja selle töö teooriapeatükis välja toodut silmas pidades täpsustavaid küsimusi. Fookusgrupi eesmärk, milleks oli koguda kõigi 11 välja joonistunud narratiivi kohta ekspertidelt täiendavat informatsiooni, sai täidetud. Strateegilist kava ma selleks rangelt ei järginud, eelistades moderaatorina hoopis tahaplaanile jääda.

Sissejuhatavas grupivestluse osas avasin uuesti oma magistritöö tagamaad lähtuvalt vestluse eel tekkinud küsimustest. Näiteks tõin välja, millise läätse läbi neid narratiive arutame ning millisel analüüsitasandil võiks mõelda; tutvustasin analüüsimise plaani ning vastasin lisaküsimustele. Lähtudes Murumaa-Mengeli (2020: 713) tähelepanekust, et veebis ei ole füüsilist tegevust nagu nt diktofoni lauale panemine, mis selgelt vestluse salvestamise algust markeeriks, toonitasin ka uuesti üle fookusgrupi kutses välja toodud vestluse salvestamise, transkribeerimise ning andmete talletamise aja ja koha. Osalejad tutvustasid ennast, ehkki õhkkond oli koheselt sõbralik: enamik osalejatest olid üksteisega varem tööalaselt kokku puutunud, sh teadis autor tööalaselt kuuest osalejast kolme. Ehkki valim oli sihipärane, võib siit välja lugeda ka mugavusvalimi tunnuseid: kuna osalejatel ei palutud täpsustada, miks nad otsustasid fookusgrupist osa võtta, ei saa põhjuslikku seost välja tuua, aga on võimalik, et varasemast tööalasest kokkupuutest tekkinud usaldus kandus üle ka uurija positsiooni.

Jagasin kogu fookusgrupi vältel oma ekraani, kus oli varasemalt ette valmistatud töölaud Miro platvormil (vt Lisa 4, Kuvatõmmis 2). Kaasasin ka vestlust toetava visuaalse stiimulmaterjali, lähtudes veebikoosolekute hüppelisest kasvust pandeemia-aasta jooksul ning Zoomi keskkonna tüdimust (ingl k *Zoom fatigue*) kaardistanud uuringute soovitustest. Näiteks Brenda Wiederhold

(2020: 437-438) on välja toonud, et tavapärasest erinevate tehnoloogiliste vahendite kaasamine aitab videokonverentside väsitavat loomust leevendada, aga hoiatab samas osalejate taju liigse stimuleerimise eest. Nii otsustasin osalejatele lisaks videokonverentsile veel vestlust stimuleerivat visuaalset tuge pakkuda. Algselt kaardistasin grupivestlust toetavate võimalike digivahenditena Miro, Murali, Jamboardi, Padleti, Slido ning Wonder.me, mis on kõik sarnase funktsiooniga ja võimaldavad ühisel virtuaalsel töölaual koostööd teha, nt mõistekaarte luua, märkmeid teha ning eelnevalt ette valmistatud tööalasid nt ajurünnaku käigu kaardistamiseks organiseerida. Valik langes lõpuks Mirole, sest seal on @ut.ee lõpuga meiliaadressiga võimalik saada tasuta hariduslitsents, mis pakub oluliselt rohkem võimalusi kui tasuta versioon.

Grupivestluse alguseks olin Miro töölauale välja toonud 11 esmase analüüsi käigus välja joonistunud narratiivi, mille olin koondanud platvormi vasakusse serva. Olin värvikoodidega uuringu eesmärke silmas pidades tähistanud märkmepaberid, milleks olid „Süsteem“, „Varasem kogemus“, „Ennetamine“, „Hinnang, millal tekkis“, „Tegutseja“ ning „Ohu eksistentsiaalsena kujutamine“ (vt Lisa 4, Kuvatõmmis 2). Vestluse käigus hakkasin ekspertide esmaseid reaktsioone ja seoseid mõistekaardile kandma ning narratiivide ümber organiseerima, mis toimus paralleelselt Zoomi vestlusega, nii et osalejad dokumendile ligipääsu ei saanudki. Leidsin, et ekraani jagades ise allikate sõnade järgi platvormil märkmete korrastamine väldib Miro-sarnaste platvormide riski, kus mitmekesi koos töötades võib lehe elemente kogemata paigast liigutada. Samuti sai nii vältida ekspertidele uue platvormi tundmaõppimise näol lisakoormuse andmist. Sellest oli uurijana kasu, sest nii sain prioriteetsed esile kerkinud teemad ning grupivestluse tulemused (vt Lisa 4, Kuvatõmmis 3) ka visuaalselt kaardistatud ning sain fookusgrupi vältel jooksvalt jälgida, milline teemavaldkond veel käsitlemata on ja lisatähelepanu vajab. Kodeerisin fookusgrupi transkriptsiooni lähtudes analüüsi esimeses osas välja joonistunud narratiividest. Fookusgrupi tulemused olen neljandas peatükis välja toonud täiendavate kommentaaridena narratiivide kirjelduste juures.

3.3 Uurijarefleksioon ja meetodikriitika

Käesoleva töö peamine analüüsimeetod toetub mitmel moel uurija tõlgendustele. Narratiivianalüüs meediatekstide põhjal, eriti narratiivi ühtsuse konstrueerimine ning sihi

kaardistamine, on alati teatud piirini uurija mentaalne konstruktsioon (Madisson ja Ventsel, 2020: 24). Mittefiktsionaalsed narratiivid esinevad meediatekstides hajusalt ja põimunult (Ventsel, Hansson, Madisson, Sazonov, 2018: 106) ning kilde kokku pannes ei pruugi uurija tabada mudelautori sihti. Mudellugeja ja -autori kontseptsioonide puhul tuleb arvestada ka mitte-öelduga, mis tähistab pealispinnal väljendamata seisukohti – eriti kehtib ajakirjanduslike tekstide puhul, kus ruum on piiratud (Eco, 2005: 58). Selle riski maandamiseks otsustasin kaasata täiendava andmekogumise meetodina fookusgrupi intervjuu riigikaitse valdkonna ekspertidega.

Fookusgrupp toimus Zoomi keskkonna vahendusel, mis 2021. aasta kevadeks oli kõikidele osalejatele tuttav. Kaasasin visuaalse stiimulmaterjalina ka Miro platvormi, mida ekraani jagades osalejatele näitasin. Kuna tegutsesin ainsana virtuaalsel töölaual, siis valitud platvormid tehnilisi väljakutseid ei pakkunud. Küll aga katkes kahe osaleja internetiühendus mitmeid kordi ja sealjuures üsna pikalt, mis viskas mitmes mõttes fookusgrupi kava paigast ära – näiteks tuli osaleja Delta pärast katkestust tagasi sisse ning asus korraga rääkima kolmest narratiivist, mille arutelust oli esialgu kõrvale jäänud. Seejärel kohandasin ka ülejäänud arutelu teemaklastrite põhiseks – samade klastrite alusel on moodustatud ka neli tulemuste alapeatükki.

Tehnilised viperused ja hakkimine tekitasid ajakulu, mis nõudsid minult moderaatorina jooksu pealt kohanemist. Kavas planeeritud ühiselt tehtavaid ülesandeid ma ei kaasanudki, sest kui juba on tehnilisi raskusi, ei tasu uusi vahendeid kaasata. Samuti polnud ma kavas arvestanud iga narratiivi arutamiseks piisavalt aega, mistõttu tekkis mul põhjendatud hirm, et ei jõua planeeritud aja jooksul kõiki 11 narratiivi käsitleda. Klastrite kaupa rääkimine säästis aega ning võimaldas ka esmaste reaktsioonide ja üksteise vastustest inspireeritud või stimuleeritud täiendite jagamist ilma, et ma narratiivi ette lugemiseks vahele segan. Nii sain uurijana jääda tahaplaanile ning Miros räägitut visuaalselt kaardistada (vt Lisa 4).

Ootamatu, aga positiivne oli osalejate profiili arvestades ka meeleolu, mille suutsime esimese kümne minuti jooksul luua: töine, aga informaalne ja sõbralik. Kuna narratiivide kaardistamine meediatekstidest nõuab väga neutraalselt keelekasutust – eks seda nõua akadeemiline keskkond laiemalt – siis ma ei lootnud, et omavaheline sünergia grupivestluses eneseväljenduse niivõrd värvikaks muudab. Samas kinnitab see, et otsus anonüümsust hoida oli õige: mõned värvikad

tsitaadid oleks tulenevalt kõneleja ametipositsioonist kindlasti uudisväärtuslikud ning võiksid välismeedias kontekstiväliselt esitatuna diplomaatilisi probleeme tekitada.

Algse uurimiskavandi järgi soovisin kolmanda täiendava uurimismeetodina kaasata ka sotsiaalmeedia monitooringutööriista BuzzSumo, et narratiivianalüüsi ja grupiintervjuu tulemusi konteksti asetada. BuzzSumo abil on eksitava informatsiooni levikut sotsiaalmeedias uuritud ka varem, nt on kaardistatud koroonat vältima õpetavate uudiste (Obiała, J., Obiała, K., Mańczak, Owoc, Olszewski, 2021) ja muude meditsiinialaste müütide (Waszak, Kasprzycka-Waszak ja Kubanek, 2018) levikut, aga ka valeinfo leviku trende üldisemalt (Allcott, Gentzkow ja Yu, 2019). See tööriist eeldab aga uurimuse tehnilistele võimalustele vastavaks disainimist, ehk teisisõnu oleks Stationi meediamonitooringu asemel pidanud kogu uurimuse seal läbi viima. 30-päevane tasuta prooviperiood pole ilmselgelt piisav, et kõik magistritööks vajalikud andmed koguda, analüüsida ning kontrollida. Ehkki BuzzSumo lõpuks minu uuringus kasutust ei leidnud, oli tegemist intuitiivselt õpitava ja kasutajasõbraliku platvormiga, mille kaasamist tulevastesse uuringutesse soovitaksin ka teistele.

4. TULEMUSED

Järgnevalt toon välja kombineeritud andmeanalüüsi tulemusel välja joonistunud mittefiktsionaalsed narratiivid Eesti ja NATO küberkaitse võimekusest. Keskendun analüüsis teooria peatüki eeskujul järgmistele valdkondadele: temaatiliste narratiivide kirjeldus, tegelaste konstrueerimine (aktiivsus, passiivsus, võim, hinnangud tegelaste hea- või pahatahtlikkusele), tegevuste konstrueerimine ning mineviku- ja tulevikunarratiividega sidumine, süsteemitasandi kujutamine ning lõppsihi konstrueerimine, julgeolekustamisele omased tunnused ning loo esitaja kui mudelautori tonaalsus. Olen narratiivid temaatiliselt jaotanud nelja suuremasse alapeatükki, milles on läbivalt välja toodud ka fookusgrupis osalenud ekspertide täiendavad kommentaarid.

4.1 Venemaa hübriidohud

Siia alapeatükki koondasin narratiivid, mille puhul on keskse rahvusvahelise tegutsejana konstrueeritud Venemaa. Rahvusvaheliste suhete distsipliini narratiivide eristuse järgi (Miskimmon, O'Laughlin, Roselle, 2013: 10-11) jaotuvad need:

- identiteedinarratiivideks, nagu 1. narratiiv „Infosõda on Venemaa puhul eriti ohtlik, sest see on sõjalise agressiooni eelmäng" ning 2. narratiiv „Lääs on Vene propagandamasina töö osas paranoiline" ning
- probleeminarratiiviks, nagu 3. narratiiv „Venemaa infooperatsioonid on paljusid veennud, et Sputnik on ainus turvaline vaktsiin".

Järgnevalt kirjeldan kõiki kolme narratiivi lähemalt.

4.1.1 Infosõda on Venemaa puhul eriti ohtlik, sest see on sõjalise agressiooni eelmäng

1. narratiiv ilmestab Venemaa hübriidsõjalise võimekuse või informatsioonilise õõnestustegevuse ohtlikuna konstrueerimist. Seoseid luuakse nii minevikusündmustega 1992. aastal Moldovas, mil „hoogustus elanikkonnaga manipuleerimine ja infosõda propaganda näol, mis lõhestas ja vastandas jõe kahte kallast" (artikkel nr 49); osaliselt annekteeritud Ukrainaga, mille praegune president „väidab, et nemad on ju Venemaa vastases infosõjas eesrinne" (artikkel nr 51) kui ka käimasolevate inforünnakutega Baltikumis ja minevikus lähi-välismaa nime

kandnud endistel Nõukogude Liidu okupatsiooni ja mõjusfääri territooriumitel (artiklid nr 13, 62 ja 105).

Fookusgrupi eksperdid hakkasid 1. narratiivi puhul esmajoones arutama, kuivõrd uue narratiiviga tegemist on. Bravo tõi välja, et narratiiv „on viimase aasta-poolteisega läinud rohkem nö tavakäibesse, et nii siin Eestis kui ka ilmselt kogu Euroopas“ ehk levik on tunnetuslikult intensiivistunud, aga Delta täiendas, et idee on pärit 2013. aastast nn. Gerassimovi ettekandest (tuntud ka Gerassimovi doktriini nime all).

Narratiiv on ekspertide arvates (Echo, Foxtrot) oma olemuselt paradoksaalne: ehkki sõda pole selles tähenduses konventsionaalne, tuleneb tajutud oht siiski konventsionaalse sõja hirmust. Foxtrot tõi välja, et see on väga geograafiliselt spetsiifiline narratiiv, mis tõenäoliselt viitab kineetilistele operatsioonidele:

> *„Kui me räägime Venemaa sekkumisest USA valimistesse, siis ega keegi tõsiselt eelda, et see nüüd on mingisugune sõjalise agressiooni eelmäng USAs. Kui nad teevad sedasama asja Eestis, Baltikumis, laiemalt Ukrainas, siin piirkonnas, siis on nagu lihtsam seda narratiivi sinna külge pookida.“* *- Foxtrot*

Alfa märkis, et nn. „lähivälismaa“ eriliselt haavatavana konstrueerides võib narratiivi laialdase mõju tulemus olla see, et „ iga teine Lääne ajakirjanik, kes Eestisse tuleb, küsibki siis, et kas Narva on siis järgmine?“. Narratiiv on strateegiline ning konstrueerib Venemaad lisaks traditsioonilistele domeenidele ka informatsioonilise mõjustamise domeeni liidrina, luues soodsa pinnase Kremli infooperatsioonide tähenduse või sellest tuleneva ohu üle hindamiseks.

Leedu Delfi faktikontroll tõi välja koordineeritud informatsioonilise mõjustamise Venemaa sidemetega infoportaalides, mis levitavad „desinformatsiooni, propagandat ja valefakte Balti riikide ja läänemaailma kohta," (artikkel 105). Üks konkreetne sündmus, millega narratiivi on sidunud näiteks Leedu luureteenistus, on nn. Putini koka infooperatsioonid Leedus – „Venemaa korraldas eelmisel aastal Leedu vastu ebaõnnestunud inforünnaku, kasutades selleks Kremlile lähedase oligarhi, „Putini kokaks” nimetatud Jevgeni Prigožini teisikut,“ (artikkel nr 62). Teisik lasi end 2020. aasta alguses pildistada transpordi- ja kommunikatsiooniministeeriumi, teisel

korral parlamendi, Leedu rahvusmuuseumi ja suurvürsti palee juures, et jätta mulje isiklikest sidemetest (artikkel nr 62) ning külvata usaldamatust Leedu riigi institutsioonide vastu. Tõenäoliselt on seetõttu ka Leedu samal ajaperioodil ilmunud toetus annekteeritud Krimmile ja Ukrainale laiemalt kindlasõnalise tonaalsusega:

> *Leedu toetab vaba ja demokraatlikku Ukrainat, tema iseseisvust ning territoriaalset terviklikkust ning samuti Ukraina jõupingutusi enda kaitsel Venemaa desinformatsiooni ning hübriidagressiooni eest.*
>
> *- väljavõte artiklist nr 13*

Paradoksaalselt mängib 1. narratiiv ka 2. narratiivi mudelautori huvidega kokku – kui narratiivi eesmärk on tekitada hirmu inforünnakute ees, sest neile võib järgneda Ukraina-sarnane annekteerimine, loob see soodsa pinnase ka paranoiaks. Samas võib mudelautorina sama eesmärki – Venemaa ohtliku kuvandi võimendamine – kanda ka nt Eestis meedia- ja infopädevuste arendamiseks raha taotlev spetsialist, kes geopoliitilist asukohta õigustatult riskifaktorina esitab. Narratiiv pakub indiviidide pädevuste tõstmise kõrval ka teisi lahendusi, näiteks informatsiooni leviku piiramine regulatiivsete võtetega. Nii toetab narratiiv püüdlusi venekeelseid propagandakanaleid sulgeda.

> *Eesti saatkond Ukrainas tervitas de facto propagandakanalitena töötanud jaamade kinnipanekut. Tema Twitteri leheküljel seisab: „Eesti mõistab ning toetab samme, mida Ukraina on astunud oma seaduste raames, et seista vastu tema iseseisvuse, suveräänsuse ning territoriaalse terviklikkuse vastu suunatud sammudele."*
>
> *- väljavõte artiklist nr 13*

Tihti on narratiivi osistega läbi põiminud ka seisukoht, et Venemaa kasutaks meelsamini sõjalist jõudu, ent ei oma selleks rahalist ressurssi – nii konstrueeritakse arusaam justkui oleks konventsionaalne sõjaline oht kadunud ainult majanduslanguse tõttu (artikkel nr 12). Venemaa majandusliku jõu vähenemisest tulenevat rahvusvahelise positsiooni nõrgenemist konstrueeriti ühes artiklis käsikäes Hiina tõusva mõju eest hoiatamisega:

Demograaline auk. Majanduslik prügikast. Vehivad oma relvadega ja mängivad, aga nad on kõrvaline lugu. Oli lootus, et Venemaast võiks saada liitlane Hiina vastu, aga Washingtoni poliitika lükkas venelased Hiina rüppe. Hiina ehitab avalikult üleaasialist koalitsiooni. Venemaa on teise või kolmandajärguline, ajutine probleem.

- väljavõte artiklist nr 35

Infosõda ei käsitletud agressiooni komponendina valitud perioodil ainult Venemaa kontekstis. Liitlaste operatsiooni raskuste osas Kesk-Aafrika Saheli piirkonnas (džihadistide-vastane võitlus on piirkonnas käinud 2013. aastast) tuuakse lisaks sõdurite elude kaotamisele järgmisena välja ka infosõja kaotamine (artikkel nr 50). Eesti Euroopa Parlamendi saadik Yana Toom arvas, et „Eesti infoväljas on sõna otseses mõttes käimas lahingud. Kusjuures need lahingud on suunatud Eesti ühe maakonna – Ida-Virumaa vastu," (artikkel nr 55). Sellegipoolest on käesoleva narratiivi tegutsejana konstrueeritud peamiselt tugeva ja võitmatu pahalasena Venemaa ning nn. „lähivälismaa" alla kuuluvad riigid kategoriseeruvad Bergstrandi ja Jasperi (2018) raamistikus (vt ptk 3.1.2) jüngriteks, sest neid kujutatakse hübriidsõja kontekstis nõrga ja teovõimetuna.

4.1.2 Lääs on Vene propagandamasina töö osas paranoiline

2. narratiiv pole autorile uus - antud narratiivi kaardistasid ka Andreas Ventsel, Sten Hansson, Mari-Liis Madisson ja Vladimir Sazonov (2018) uurides strateegiliste narratiivide hirmu mehhanisme Zapad 2017 õppuse näitel. Mitmes artiklis oli näha narratiivi sidumist minevikusündmustega, viidates näiteks sellele et „Kremli mõjutusmeetodites ei ole 21. sajandil midagi uut. Nõukogude Liit praktiseeris kogu oma eksistentsi vältel läänes aktiivset mõjutustegevust," (artikkel nr 44).

Narratiivi päevakajalisus kerkis taas esile seotuna kahe päevakajalise meediasündmusega: nn Maša ja Karu intsident ning Sputnik V vaktsiini saatvad infovood. Esimene neist on seotud 2020. aasta sügisel mitmes Euroopa riigis ja USAs levinud analüüside või arvamustega, mille kohaselt on tuntud multifilm propaganda tööriist, mille eesmärgiks on lapsi alateadlikult indoktrineerida (artikkel nr 70). Selline narratiiv toetab otseselt ka Vladimir Putinit, sest süvendab arusaama

mille järgi „kollektiivne Lääs vihkab Venemaad ja selle elanikke ning juba seetõttu on Venemaale vaja tugevat otsustavat juhti“ (artikkel nr 70).

> *Kirjutasid multifilmist soliidsed lehed, nagu Times või Washington Post. Tõelised Lääne analüütikud naersid selle üle, ent asi oli kokkuvõttes naljast kaugel. Venemaa propaganda haaras sellest kõigest ootuspäraselt kinni. Multifilmi tootva erafirma omanikust sai Venemaal üleöö meediastaar ja muidugi jagus pikemaks ajaks Euroopa lolluse üle irvitamist. Enamikel venelastel oli hea meel – välismaa kardab meid, isegi meie lastele mõeldud multifilmid on ohtlikud.*
>
> - *väljavõte artiklist nr 70*

Delta võttis narratiivi olemuse kokku järgmiselt: „Стратегическая маскаровка oleks diagnoos. Kes teisele ütleb, see ise on.“. Informatsiooniline vastasseis pole Venemaa jaoks lihtsalt eelmäng, vaid osa laiemast vaatest, mis „katab tervet spektrit eskaleerimisest de-eeskaleerimisse, sest tegelikult Venemaa strateegilises pildis on kõik riigid omavahel sõjas ja kaitse on rünnakuks ettevalmistamine,“ (Delta). Selles narratiivis on Venemaa Bergstrandi ja Jasperi (2018) karakterite jaotuse järgi konstrueeritud kangelasena, kes on kaval, aktiivne ja vääritimõistmiseni intelligentne, samas kui lääneriike konstrueeritakse pahalastena, kohati ka teovõimetute jüngritena (viimast eriti NATO-t käsitledes, kusjuures teovõimetus väljendub selle narratiivi kontekstis ka liitlaste rahvusvahelise õiguse järgimises). Seda selgitab osaliselt ka Venemaa informatsioonilise vastasseisu tekitamise strateegia.

> *„Venemaa lähenemine või Kremli müstiline lähenemine on see, et meid austatakse. Что уважают, et oleks respekt. Ja Venemaa suhtes on see, et kui neist peetakse lugu, siis lugu peavad ainult need, kes kardavad ja sellepärast on vaja külvata hirmu. /---/ Paljas teadmine juba, et Venemaa on võimeline sekkuma demokraatlikku valimisprotsessi, näiteks Ameerika Ühendriikides, see on juba hirmutav - et ameeriklased, käituge korralikult, muidu me paneme teile järgmise klouni presidendiks.“* - *Delta*

Strateegia on sealjuures ekspertide sõnul kaheosaline: ühelt poolt mõjutatakse või üritatakse mõjutada demokraatiat, teisalt lõhutakse sõnavabadust ajakirjanduse usaldusväärsuse

ründamisega (Delta). Foxtrot märkis, et see on pigem Venemaa kontrollitud meediaruumi spetsiifiline ning „vabas ajakirjanduses see narratiiv, isegi kui ta olemas on, siis ta ei ole domineeriv“. Tema sõnul on selle narratiiviga kaasneva ettevaatlikkuse mõju pigem positiivne.

> *„Meil on veel tükk maad minna sinna, et me oleks liiga palju mures Vene propagandamasina töötamise osas. /---/ Pigem käib Eesti kultuuriruumis kaasas selline põhjendamatu arusaam, et me justkui oleme emapiimaga Vene propaganda vastu immuunsed juba siin. Noh, reaalsus on teistsugune, ma julgeks öelda.“ - Foxtrot*

Bravo tõi KAPO aastaraamatut näiteks tuues välja, et selle narratiivi intensiivsem levitamine võimaldab aimata, mis on Venemaa informatsioonilise vastasseisu osas nn. tuleviku tööfront, kuhu fookus seatakse, samas kui Echo juhtis tähelepanu, et „see on pigem ekspertide või huviliste tasandil toimiv narratiiv“ ning tõi paralleele valdkonna konverentsidel arutletuga.

> *„Väga lihtne on leida selline välisvaenlane, kes põhjustab probleeme, selmet vaadata oma ühiskonda ja näha neid tänase üleminekufaasi suuri, struktuurseid probleeme, mitte ainult majanduslikke, vaid üldse selliseid sotsiaalseid, kultuurilisi, ja neid siis adekvaatselt adresseerida. Ma arvan, et see on hea vabandus ka teistpidi.“ - Echo*

Ühe meediateksti kohaselt pole paranoia põhjendamatu, vaid Venemaa infooperatsioonid „ei jäta enam küsimärke Venemaa hoiaku ja eesmärkide suhtes“ (artikkel nr 64). Mudelautori eesmärgiks võib olla ka lääneriikide uinutamine. Eksperdid rõhutasid, et lääs omistab kohati Kremlile rohkem võimu kui neil tegelikult on, seostades või välistades Venemaa riiklike organite seotust mingisuguste juhtumitega liiga kergekäeliselt. Näiteks toodi kollavestide protestid Prantsusmaal: alguses kahtlustati „vene karvast kätt“ (Alfa), aga tegelikkuses hüppas Venemaa tõenäoliselt alles olukorra arenedes ja eskaleerudes oma võimalust märgates paati (Foxtrot). Nii manatakse nn. vaenlasest reaalsusest jõulisem ja võimsam pilt, samas kui praktiliselt on tegemist oportunismiga: kus on edu, sinna suunatakse veel jõupingutusi (Delta).

Nagu eelnevalt välja tõin, on see narratiiv osaliselt läbi põimunud ka järgmises alapeatükis välja toodud vaktsiini-teemalise narratiiviga. Sputnik V hankest loobumise põhjuseid konstrueeritakse Lääne tagakiusamisena ning Venemaad vaheldumisi kangelase või ohvrina, sh konstrueerides

lääneriikide Venemaa-suunalist paranoiat nii tugevana, et selle nimel riskitakse riigi kodanike eludega (artikkel nr 100).

> *See on nonsenss. Vene eriteenistused ei ole vaktsiinide kritiseerimisega seotud," ütles Peskov. „Kui meie peaksime iga publikatsiooni Sputnik V kriitikaga Ameerika eriteenistuste töö tulemuseks, läheksime hulluks: täheldame ju selliseid publikatsioone kõigis anglosaksi massiteabevahendites iga päev, iga tund."*
>
> *- väljavõte artiklist nr 96*

> *Väga kahju, et koroonapandeemia ajal on jälle esikohal poliitika. Olen juba arvamust avaldanud, et meditsiini ja tervishoidu on tunginud poliitika ja selle asemel, et teha koostööd, on Putini vaktsiin kuulutatud toksiliseks. Olen mõelnud, et Jumal on koroonapandeemia saatnud inimkonnale mõttega, et lõpetada maailmas infosõda. Istugem ühe laua taha ja lahendage see inimkonna jaoks nii tähtis probleem, kuidas säästa inimelusid.*
>
> *- väljavõte artiklist nr 57*

Lääne liigset või põhjendamatut paranoiat konstrueeritakse probleemina ka koroonast laiemas kontekstis, viidates et olenemata sellest, kas on põhjust või mitte, on kõiges Venemaa või Kremli mõjuagentide tegevuse otsimine kahjulik, sest veename „iseennast ja teisi, et Eestimaa venelased on propaganda suhtes eriti haavatavad (erinevalt eestlastest, loomulikult)" (artikkel nr 55). Vene emakeelega eestlaste selle narratiivi kontekstis, aga ka laiemalt kodumaises uudisajakirjanduses abitu ja passiivse propaganda vastuvõtja ja ellu viijana kujutamine võib isetäituvaks ennustuseks osutuda. See võib omakorda olla ka mudelautori implitsiitseks agendaks kui Lääne paranoia Vene propagandamasina suhtes mõtestada ümber paranoiaks vene emakeelega kodanike suhtes.

4.1.3 Venemaa infooperatsioonid on paljusid veennud, et Sputnik V on ainus turvaline vaktsiin

3. narratiiv kõneleb taas kaudselt Venemaa propagandamasina võimest, näidates Sputniku populariseerimiseks mõeldud infooperatsioone seostatuna madalate vaktsineerimisnäitajate või

kõrgete nakatumisnäitajatega venekeelse emakeelega elanikkonna enamusega geograafilistes ruumides (artikkel nr 103 ja 97). Tegutsejana kirjeldatakse Venemaa valitsust (artikkel nr 64) või luureteenistust (artikkel nr 95), aga ka otsustusvõimetuid ja segaseid sõnumeid saatvaid valitsusi, tuues näiteks ka Eesti.

> *Kui peaminister ütleb intervjuus, et ta ei välista Sputniku vaktsiini kasutuselevõttu, kuid ei oska selgitada, millistel tingimustel ta Sputniku vaktsiini kasutuselevõttu toetaks, tekitab see asjatut segadust. Teises inforuumis elava inimese jaoks tähendab see seda, et ta võib keelduda Pzeri, Moderna või AstraZeneca vaktsiinist lootuses, et varsti tuleb see „õige" vaktsiin. Kui valitsusjuht ütleb selgelt, et Sputnikut Venemaa seniste infooperatsioonide tõttu kasutusele ei võeta, valitseb ühiskonnas aga selgus, mis aitab vaktsineerimisega edasi liikuda.*
>
> *- väljavõte artiklist nr 66*

Narratiivse konstrueerimise osa ei pruugi olla tingimata Sputniku kiitmine, vaid ka teiste vaktsiinide turvalisuses kahtlemine. Näiteks püüdsid neli väljaannet, mis USA välisministeeriumi ametnike hinnangul Vene luure heaks Pfizeri vaktsiini efektiivsusi osas kahtlusi levitasid, tõstatada küsimust, kas USA kiirustas Pfizeri vaktsiini heakskiitmise protsessiga (artikkel nr 95 ja 96). Teisalt oleks sellise narratiivi presenteerimine koos otsesõnalise Sputnikuga kiitmise või selge paralleeli tõmbamisega vastuoluline, sest Sputnik sai teatavasti esimesena riiklikult ravimiametilt kasutusloa. Edukat levikut näitlikustab nt AstraZeneca paradoks: mitmetes Euroopa Liidu liikmesriikides peatati AstraZeneca kasutamine tromboosiohu tõttu, mis suurendas survet Sputniku vaktsiini ostmiseks ja toomiseks, ehkki „AstraZeneca vaktsiini ja Sputnik V-d on arendatud sama mikrobioloogilise tehnoloogia põhimõttel" (artikkel nr 64). See sobitub Wardle ja Derakhshani (2017: 30) tõdemusega, et infooperatsioonide eesmärk pole alati sõnumi vastuvõtjat selle tõepärasuses veenda, vaid külvata skepsist – antud kontekstis siis „lääne" vaktsiinide osas – ning tekitada Vene „imevaktsiinile" nõudlus (artikkel nr 97).

Venemaa infooperatsioone konstrueeritakse nimetute ekspertide hinnangul eduka ja mõjukana (artikkel nr 53) ning põhjusena, miks Eestis on koroonaviirusega kõige enam nakatunud kohad

„valdavalt venekeelse elanikkonnaga piirkonnad - Maardu, Lasnamäe, Ida-Virumaa“ (artikkel nr 97). Leviku põhjusena ei nimetata otsesõnu Venemaa edukaid infooperatsioone, vaid viidatakse just vene emakeelega elanikkonnale, kasutades näiteks terminit „elanikkondlikud tegurid“ (artikkel nr 103). Ehkki eelmainitut on esitatud kindlas kõneviisis, on info vastuolus riikliku statistikaga, sest „Sotsiaalministeeriumi tellimusel regulaarselt läbi viidavate küsitluste kohaselt ammutab vaid 14% mitte-eestlastest teavet koroona kohta Venemaa meediast“ ning loob seega silla aastakümneid vana narratiiviga, mille järgi Eestis elavaid vene emakeelega inimesi taga kiusatakse (vt ptk 1.1.3). Venemaa on konstrueeritud kangelasena, vene emakeelega inimesi taga kiusav riik mõistagi pahalasena ning kõnealused väljaspool Venemaad elavad kodanikud valesti mõistetud ohvritena.

Ootamatult tõstab narratiiv pead ka näiteks vaktsineerimist kiitvas artiklist, mille autor lisas täiendava kommentaari et „Euroopa Ravimiamet ei ole Sputnik V-le kasutusluba veel andnud, sest Liidu nõuded on põhjendatult kõrged“ (artikkel nr 64), mis sobitub narratiivi Lääne poolt taga kiusatud maailma päästva vaktsiini tootjamaast (artikkel 100). Samas ei esita see narratiiv tingimata tegutsejana ainult Venemaad, vaid rõhub ka pandeemiast tingitud mure ja mittekavatsusliku tegevuse mõjule informatsiooni leviku hoogustumises. Nii võib ka piirangute vastu protestijast saada Venemaa agenda edasikandja.

> *“Minu sotsiaalmeediasse jõudsid kaadrid, mis algavad sellega, kuidas mehele lastakse näkku gaasi, ta üritab ära joosta ning murtakse maha ja kõige tipuks annab mingi suvaline tüüp talle veel lõuga,” räägib Laine. Kuna kontekst on videost välja jäänud, sai see ideaalseks propgandarelvaks, ühendades omavahel vandenõuteoreetikud, valitsuskriitikud ja Kremli-meelsed (isik rääkis vene keelt ja selle baasilt oli võimalik levitada narratiivi, kuidas venelasi kiusatakse).“*
>
> *- väljavõte artiklist nr 65*

Fookusgrupis osalenud eksperdid kõnelevad 3. narratiivi juures taas Venemaa oportunismist, mida ilmestab see, et algselt demoniseeriti Pfizerit, aga kuna AstraZeneca kommunikatsioon läks niigi kehvasti, siis suunas ka Venemaa jõupingutuse sinna (Delta). Oportunism selgitab ka narratiivi konstrueerimise juures tekkinud nn. AstraZeneca demoniseerimise paradoksi. Kui

narratiiv sobib mõjutustegevuse laiemate eesmärkidega, siis seda võimendatakse juhul kui „isetekkelised hüpoteesid toetavad teatud vaenulike jõudude strateegilisi huve“ (artikkel nr 61), nii võibki narratiiv sisuliselt vastuoluliseks kujuneda.

4.2 Hiina väärtusruumi ja mõjuvõimu laienemine

Siia alapeatükki koondasin narratiivid, mille puhul on keskse rahvusvahelise tegutsejana konstrueeritud Hiina. Rahvusvaheliste suhete distsipliini narratiivide eristuse jaotuvad need:

- identiteedinarratiivideks, nagu 4. narratiiv „Hiina kasutab spionaaži, manipulatsiooni ja majanduslikku jõudu inimõiguste rikkumise kriitika vältimiseks“ ning 5. narratiiv „Tehnoloogia eelisarendamine teeb Hiinast ohtliku suurvõimu“ ning
- süsteeminarratiivideks, nagu 6. narratiiv „Hiina eesmärk on partei autoritaarseid väärtusi eksportida ja rahvusvahelisel areenil realiseerida“.

Need narratiivid on selle töö kontekstis olulised just seetõttu, et kujutavad spionaaži, manipulatsiooni ja majandusliku jõu rakendamise peamise domeenina tehnoloogiavaldkonda, mis toob geograafiliselt kaugel asuva riigi ja/või narratiiviga kaasneva ohu tunnetuslikult „kodule“ lähemale. Järgnevalt kirjeldan neid kolme kohati läbi põimunud narratiivi lähemalt.

4.2.1 Hiina kasutab spionaaži, manipulatsiooni ja majanduslikku jõudu inimõiguste rikkumise kriitika vältimiseks

4. narratiiv esitab Hiina informatsioonilist mõjutustegevust tööriistana, millega vältida rahvusvaheliste tegutsejate ja toimijate kriitikat (artikkel nr 31) üha halvenevate inimõiguste olukorra (artikkel nr 12) ning rahvusvaheliste kokkulepete eiramise, nagu nt Hong Kongis poliitilise pluralismi ja arvamusvabaduse kõigutamise kontekstis (artikkel nr 32).

> *„Euroopas on mitu eri formaadiga foorumit, kuhu Hiina kutsub kõrgetasemelised diplomaadid, poliitikud ja ettevõtjad kokku ilmse eesmärgiga isiklike suhete sisseseadmise kaudu mõjutada sihtriikide Hiinapoliitikat“. Nende algatustega loodab Hiina saavutada seda, et Eesti poliitikud ja arvamusliidrid ei kritiseeriks Pekingi tegevust ülemäära, austaks Hiina terviklikkust ega sekkuks Hiina riigi siseasjadesse.*

- väljavõte artiklist nr 13

> *Euroopa-USA teljel on Hiina mõjutustegevuse selgeks sihtmärgiks just esimene, sest siinne killustatus muudab vana maailma palju haavatavamaks. Hiina eesmärgiks pole sealjuures mitte laialdane koostöö Euroopaga, vaid oma suuruse ja võimuga summutada Hiinat kritiseerivad hääled.*

- väljavõte artiklist nr 18

Siin võib täheldada süsteemitasandi kirjeldusi: Hiina soovib hegemoonilise maailmakorra muutumist, mida proovib saavutada kiilu lüües Euroopa ja Ameerika Ühendriikide vahele ning sellega saavutatav jõupositsioon vähendab ka Hiina soovi rahvusvahelistest lepetest kinni pidada (artikkel nr 31). Tegutsejatena ongi narratiivi kaasatud Euroopa (mis ei välista EL-i mitte kuuluvaid NATO liitlasi, vaid viitab pigem jagatud kultuuriruumile), Ameerika Ühendriigid, ja Hiina – esimesi konstrueeritakse riigi tasandil kangelastena, ehkki indiviide selle narratiivi kontekstis pigem passiivsete jüngritena, samas kui Hiina on aktiivne, ettearvamatu ja võitmatu pahalane, kes pahaaimamatute indiviidide läbi kangelasteni jõuab. Mudelautori strateegiaks võib selle narratiivi kontekstis olla nii ohust teavitamine konstruktiivse vastu-strateegia välja töötamiseks kui ka tulevase hegemoonilise maailmakorra paratamatuna kujutamine. Hiina hegemooniat presenteerib Steve Bannon usutluses eksistentsiaalse ohuna (artikkel nr 35) – selles narratiivis võib täheldada julgeolekustamise tunnuseid, mis on viinud ka konkreetsete sammudeni. Näiteks uiguuride represseerimisega seotud ametnikud kandsid Euroopa Liidu järel musta nimekirja ka Ühendkuningriigid, Kanada ja USA (artikkel nr 94).

> *Pealtnäha avatud meelelaadi varjus on aga laiemalt pinda võtnud mall, et Hiinat kritiseerida tohib, kuid vaid kindla piirini, misjärel tuleb „aga“ – „Aga Hiinata ei saa, uue maailmakorraga jääb üle vaid kohaneda.“ Selline näiline Hiina kritiseerimine levib Euroopas ning ähmastab ja õõnestab Hiinast lähtuva julgeolekuohu tajumist.*

- väljavõte artiklist nr 18

Narratiiv esitab informatsioonilise mõjustamise, küberspionaaži ning Hiina tehnoloogia kasutamisega ohte Kremli-sarnase strateegiaga luuretegevuse kontekstis (artikkel nr 17). Fookusgrupis toob Alfa välja, et ehkki narratiiv on tema arvates välismeedias levinud, on see Eestis pigem uuepoolne, „sest meil on suurem vastasmängija palju lähemal ja tajume seda palju ohtlikuma“. Diskursiivne nihe ja ohu lähemale jõudnuna tunnetamine Eesti kontekstis sai osalejate meenutuste kohaselt alguse Välisluureameti 2020. aasta aastaraamatu kajastuse, ajakirjanik Holger Roonemaa Hiinat käsitleva artikliseeria ja sellele järgnenud avaliku arutelu ning KAPO aastaraamatu käsitlusega. Foxtrot leiab, et narratiiv on veidi eksitav, sest ei näita tervikut.

> *„Hiina ei kasuta neid oma jõuõlgasid ainult selleks, et inimõiguste rikkumist summutada, vaid et ikkagi ennast globaalseks liidriks mängida. Muuhulgas on selleks loomulikult vaja summutada kriitikat inimõiguste rikkumisest, mis on lääne ühiskonnale nagu punane rätik, et kui me muidu oleme väga sõltuvad praeguseks hetkeks ja oleme valmis ka Hiinaga koostööd tegema, siis see on valdkond, mis takistab Hiinal edasi liikumast nii jõuliselt nagu nad sooviks.“ - Foxtrot*

See pisendab Echo arvates ka inimõiguste problemaatikat – näiteks on Skandinaavias Hiina ärihuvid selgemini esindatud, sellest tulenevalt ka Hiina luureoht kõrgendatud ning ka diplomaatiline nn. köiel kõndimine aktuaalsem küsimus kui Eestis.

USA julgeolekudokumentides on Hiina suurim strateegiline väljakutse ning nn pööre Aasiasse (*ingl* Pivot to Asia) algas juba president Obama ajal (artikkel nr 31). President Bideni poja Hunteri parandusse unustatud läptopist välja tulnud võimalikud perekondlikud ärisuhted Hiinaga põhjustasid USAs skandaali (artikkel nr 35), mis kinnitab narratiivi mõjukust ja laia kõlapinda ning tähendab, et tõenäoliselt „ei pääse ka Joe Bideni administratsioon keskendumisest Hiinale“ (artikkel nr 34). Hiina on fookusesse asetatud kui pahalane, kelle pahedega kangelased – lääneriigid ja liitlased – peavad arvestama ise samale tasemel laskumata.

4.2.2 Tehnoloogia eelisarendamine teeb Hiinast ohtliku suurvõimu

5. narratiiv esitab Hiina tehnoloogilise hiiuna, mille võimekuse arendamiseks „jahitakse andekaid inimesi üle maailma ja proovitakse neid kas Hiinasse meelitada või muudmoodi üle osta“ (artikkel nr 18), esitades seda tehnoloogilist võimekust samas julgeolekuohuna, sest „erakapital ja ärimehed pole oma käitumises vabad“ (artikkel nr 12).

> *Hiina puhul peavad nii Lääs tervikuna kui ka Eesti arvestama sellega, et liiga tihe integreerumine majandusvaldkonnas võib muuta meid sõltuvaks ja haavatavaks. Tuleb arvestada, et pea kõik suured Hiina investeeringud on Hiina riigi ja kommunistliku partei kontrollitavad.*
>
> *- väljavõte artiklist nr 12*

Narratiiv ei eita kuidagi Hiina tehnoloogilist võimekust või konkurentsivõimet - sealjuures tuuakse sageli välja väärtuste põrkumist andmekaitse, uute tehnoloogiate, nagu nt 5G reguleerimise osas – aga kuna Hiina on süsteemne rivaal (artikkel nr 31), on riigist või seal toodetavast tehnoloogiast liialt sõltumine julgeolekuoht. Peamist tegutsejat nähakse aktiivse, jõulise ja domineerivana. Hiina tehnoloogia laienemise eesmärgina esitatakse nt „Ühe vööndi, ühe tee“ algatusega liitunud riikidesse Hiinas loodud Beidou navigatsioonisüsteemi eksportimine (artikkel nr 13).

> */---/ enam GPS-süsteemi, vaid satelliitnavigatsioon toimuks läbi kohaliku Beidou – see olla palju parem ja täpsem! „Eesti integreerimine Hiina autonoomse tehnoloogia ökosüsteemiga muudab Eesti haavatavaks ja sõltuvaks Hiinast,“ hoiatab välisluure.*
>
> *- väljavõte artiklist nr 18*

See haakub mõneti 4. narratiiviga: ohtlikuna kujutatakse tehnoloogilist sõltuvust mh. sellepärast, et Hiinaga häid suhteid hoida püüdvad tegutsejad on majanduslikest või poliitilistest sidemetest kammitsetud ning seega ei kritiseeri rahvusvahelisel areenil Pekingit otsesõnu (artikkel nr 13). Grupivestluses toodi ühelt poolt välja, et sarnaselt Venemaale kujutatakse ka Hiinat selliste narratiividega liialdatult ohtliku rahvusvahelisel areenil tegutsejana – nt võivad ka Eestis ja

läänes julgeolekuteenistused sarnastel alustel informatsiooni välja nõuda, aga Hiina seadusest rääkides, mis kohustab ettevõtteid riiklike asutustega koostööd tegema, seda kõrvutamist teiste riikidega ei tehta (Alfa). Teisalt on majandusliku koostöö rõhutamise kõrval ekspertide arvates oluline silmas pidada, et Hiinas pole turumajandus vaba ja nad ei täide Maailma Kaubandusorganisatsiooni nõudeid (Delta), ning et õigusriigis saavad ettevõtted julgeolekuteenistuse sooviga mittenõustumisel kohtusse pöörduda, samas kui Hiinas on fundamentaalselt teine olukord (Foxtrot). Kaalutluskohaks selle juures, kas koostööd tehakse, võikski ekspertide arvates olla küsimus sellest, kas sellest koostööst tekib sõltuvus (Charlie), millega võidakse üritada meie kultuuri- või väärtusruumi proovida mõjutada (Foxtrot) ning tehnoloogilise jõu ja näiteks Eesti, Huawei ja 5G võrgu laiendamise kontekstis ikkagi see, mis digivahenditest saadud informatsiooniga tehakse.

> *„Tegelikkuses ei seisne oht ju konkreetses tehnoloogilises vahendis, vaid selles, kes vahendit kontrollib, milliste reeglite järgi ta mängib ja kas me mängime kõik ühte mängu või mitte.“* *- Foxtrot*

Seost tehnoloogiaettevõtetega toetavad kodumaise auditooriumi puhul ka varasemad meediakajastused Huawei koostöölepingutest ning Hiinale meelepärase informatsioonilise mõjutustegevuse ilmingutest Eestis.

> *Eesti meedias on Hiina ja ka Huawei korraldanud mitmeid PR-kampaaniaid, millega inimesi püütakse veenda eeskujulikus inimõiguste olukorras Xinjiangis või Huawei sõltumatuses Hiina riigist.*
>
> *- väljavõte artiklist nr 12*

> *Alates 2019. aastast on käsitletud Hiinat eelkõige aga juba riigisesese julgeolekuohuna, mis peegeldab selget muutust nii Pekingi ambitsioonides kui ka Eesti ühiskonna meelsuses.*
>
> *- väljavõte artiklist nr 13*

Julgeolekustamise tunnused narratiivis viisid vaadeldaval perioodil ka lisaks (eksistentsiaalse) ohu konstrueerimisele ka konkreetsete lahenduste pakkumise ja neile poliitilise toe otsimiseni: veel detsembris 2020 tegeles toonane väliskaubandus- ja infotehnoloogiaminister Raul Siem määruse välja töötamisega, mille kohaselt „keelataks Euroopa Liitu, NATOsse ja OECDsse mittekuuluvate riikide tootjate seadmete kasutamine sidevõrkudes“, aga mille osas, nagu minister rõhutas, „ei tohi jätta ka sellist muljet, et see on Huawei määrus. Vastasel korral devalveerub määruse sisu,“ (artikkel nr 26). Olgu öeldud, et määrusega ei ole edasi liigutud, tõenäoliselt hilisema õiguskantsler Ülle Madise hinnangu ning valitsuse ja ministri vahetuse tõttu.

Ei saa välistada ka vastaspoole lobitöö edu. Selle narratiivi puhul esines valimis ka vastu-narratiivi levitamise katse, nt Eesti Huawei müügijuht konstrueeris ettevõtte peakorteri asukoha põhjal julgeolekuohuna käsitlemist ohuna ausale konkurentsile, sest „vaja pole keerukaid kontrollimehhanisme ja isegi sidevaldkonna asjatundlikkust. Piisab, kui ametniku laual seisab papist gloobus. Otsustaja ei vaja sellisel juhul isegi gümnaasiumi haridust,“ (artikkel nr 26). Vastu-narratiivis on omakorda vastuolu: ehkki rõhutatakse korduvalt, et Huawei ei kujuta endast julgeolekuriski, nenditakse samas et „Huaweid tuleb umbusaldada täpselt samuti nagu iga selles äris osalevat ettevõtet“, pidades „selle äri“ all silmas tehnoloogiavaldkonda. Artikkel rõhus õigusriigile mittekohasele käitumisele lisaks ka kirjeldamatule majanduslikule kahjule, mis Huawei seadmete julgeolekuriskina käsitlemisel kaasnevad.

> *Rahandusministeeriumi nägemuse kohaselt võivad praeguses eelnõus määruse rakendamisega kaasnevad kulud olla olulises mahus alahinnatud. Puudub ülevaade, mis ulatuses võib sideettevõtetel olla õigus nõuda riigilt hüvitist, kui nad peavad teenuse osutamiseks kasutatavaid seadmeid välja vahetama.*
>
> *- väljavõte artiklist nr 26*

Mõneti on narratiiv olemuselt paradoksaalne, sest ehkki sätestab, et „digitaalse ajastu reeglite kujundamist ei juhiks Venemaa ja Hiina“ (artikkel nr 31) erinevate väärtusruumide, st digitaalses ruumis inimõiguste austamise põhimõtete tõttu, leiab peaaegu kõikidest artiklitest ka seisukoha, et „Euroopale on tähtis säilitada vastastikku kasulikud ja pragmaatilised suhted Hiinaga“ (artikkel 31). Just tehnoloogia keskmesse seadmine näitab, et antud narratiiv on Eestis alles

lapsekingades ja pealiskaudne (Charlie) ning kuigi pole otsesõnu eksitav, esitab ainult poolt tõde (Foxtrot). Tehnoloogiline jõud on vahendiks üldise Hiina hegemoonia strateegia või pika plaani juures (Delta), aga eesmärgiks on ikkagi hegemoonia. See narratiiv kirjeldab võimaliku tulevase ülemvõimu esimest domeeni.

4.2.3 Hiina eesmärk on partei autoritaarseid väärtusi eksportida ja rahvusvahelisel areenil realiseerida

6. narratiiv sätestab süsteemitasandil maailmakorda, mida Lääs ei tohiks tahta. Eesti kontekstis esitatakse võimalikku Hiina ülemvõimu tulevikustsenaariumit ka Nõukogude Liidule omaste väärtuste tagasitulekuga:

> */---/ on HKP pärinud oma minevikust suhtumise, et nii ühiskonda kui ka selle üksikuid liikmeid saab ja tulebki riigi sõnastatud eesmärkide saavutamiseks ümber vormida. Inimesed on esmajärjekorras riigi tarvis, mitte riik inimeste tarvis. /---/ Niisiis ei kujuta Hiina meile julgeolekuohtu mitte pelgalt seepärast, et ta on suur või autoritaarne, vaid seepärast, et sealsed mõttemustrid rakendavad selle riigi meist radikaalselt teistsuguste eesmärkide teenistusse.*
>
> *- väljavõte artiklist nr 13*

Väärtuste importi Läände näidatakse enamasti just informatsioonilise mõjutamise kontekstis, kusjuures lisaks sellele, et Hiinat kujutatakse kui „väga usinat desinformatsiooni levitajat“, tuuakse esile ka Pekingile omane salatsemine, sest see „annab ainult moona vandenõuteooriatele“ (artikkel nr 101). Võõra väärtusruumi kehtestamise ohutaset kõrvutatakse sõjalise agressiooniga (artikkel nr 12). Koroonapandeemia ajal on Hiina usalduse krediit vähenenud:

> *„Rõhutati vajadust astuda kõik koos apoliitiliselt vastu inimkonda laastavale viirusele. Samal ajal tegeles Hiina Kommunistlik Partei (HKP) tugeva kontrolli all olev meedia aktiivselt Lääne demokraatia mustamise, demoniseerimise ja naeruvääristamisega, öeldes, et vaid Hiina-suguse autoritaarse süsteemiga suudetakse viirus edukalt alistada.*

- väljavõte artiklist nr 18

> *Sellise hoiaku taga on Hiina poliitilise eliidi veendumus, et lääne liberaaldemokraatia on „katki“ ja et vaid Hiina – tuginedes nii Mao õpetusele kui ka konfutsianistlikule humanismile – suudab luua nüüdisaja maailma probleemidega arvestava poliitfilosoofia.*

- väljavõte artiklist nr 13

Hiina on konstrueeritud aktiivse ja võimsa pahalasena, kusjuures kangelasena ei kujutata mitte konkreetset riiki, vaid riikide kogumit, kes vastanduvad Hiina väärtussüsteemile. Rahvusvaheliste tegutsejate tasandil on siin narratiivis pandud Hiina kõrval rõhku ka riigi tihedale koostööle Venemaaga ning sellest tulenevale ohule, aga võrreldes alapeatükis 4.1 kaardistatud narratiividega, konstrueeritakse kultuurilist imperialismi Hiina puhul tunnetuslikult suurema probleemi või tõsisema ohuna. Mudelautori agenda on aga ühesugune.

> *Korraldatakse ühiseid sõjalisi õppusi, koordineeritakse hääletusi ÜROs, luuakse regionaalseid majandusühendusi. Mõlema eesmärk on lääneriikide ühtsuse murendamine, eelkõige USA poliitilise ning majandusliku mõjuvõimu vähendamine ja oma globaalse mõjuvõimu suurendamine.*

- väljavõte artiklist nr 31

Sarnaselt Venemaale, on ka siin narratiivis informatsiooniline mõjustamine välja toodud süveneva probleemina Hiina süveneva geopoliitilise agressiooni kontekstis – nt Lõuna-Hiina merel Hiina kontrolli alla võetud territooriumid, mis rahvusvahelise merearbitraaži otsusel kuuluvad Filipiinidele (artikkel nr 12). Samas ei tohiks grupivestluses osalenud ekspertide arvates unustada, et globaliseerumise mustri alustõed kehtivad kõigi rahvusvaheliste tegutsejate kohta, ehk nagu Echo sõnastas: nii kaua kuni riigid kontrollivad oma territooriume ja Hiina teeb hiiglaslikke välisinvesteeringuid, on ka Hiina infrastruktuuri investeeringute tõttu teisest riigist sõltuv ja riskiolukorras. Hiinat ja Venemaad võrreldes kujutasid osalejad suurema ohuna pigem Hiina hegemooniat.

„Kui me täna vaatame, et kes nagu lääne elustiilile või demokraatiale võib väljakutse esitada, siis hoolimata meie suurest idanaabrist on see ikkagi ainult Hiina. /---/ Hiinal on tahe, majanduslik jõud, tehnoloogiline jõud, sõjaline jõud ja ka inimressurss. Venemaal on ainult tuumalõhkepead ja oportunism.“ *- Delta*

Sealjuures rõhutasid eksperdid Hiina hegemoonia idee kultuurilist ja ajaloolist konteksti, näiteks vabaduse ja individuaalsuse Läänest kardinaalselt erinevalt mõistmist, samas kui meediatekstides kõneldi pigem praegusest valitsusest ja Kommunistlikust Parteist.

„Hiina on sipelgapesa, aga me oleme kõik indiviidid, see ongi fundamentaalne vahe. Ja teine on muidugi ajatelg. Meie liigume deadline-st deadline-i ja meil on tähtis midagi mingis ajavahemikus saavutada, aga hiinlastel ei ole ajal mingit tähendust. Et vallutage, vallutage meid, ükskord räägite kõik hiina keeles ja toote meile andamit.“ - Delta

Läänes pole Hiina hegemooniasoov ja väärtusruumi laiendamise ambitsioon midagi uut, aga Eesti ajakirjandus ja julgeolekuteenistused on teemat alles viimastel aastatel käsitlema hakanud, mis näitlikustab ekspertide arvates, et ehkki Hiina asub meist geograafiliselt kaugel, on oht tänu Hiina majanduslikule ja tehnoloogilisele jõule – mille suurust ja võimu 4., 5. ja 6. narratiiv võimendavad – tunnetuslikult lähemale tulnud.

4.3 Eesti kui digiriigi nõrgemine rahvusvahelisel areenil

Siia alapeatükki koondasin narratiivid, mille puhul on keskse rahvusvahelise tegutsejana konstrueeritud Eesti. Rahvusvaheliste suhete distsipliini narratiivide eristuse järgi need probleeminarratiivideks, püüdes mõjutada (poliitiliste) arutelude keskkonda. Nendeks on:

- 7. narratiiv „Eesti on e-riigina läbi kukkunud, sest pandeemia ajal ei ole piisavalt e-lahendusi kasutatud“ ning
- 8. narratiiv „Eestis pole poliitilist tahet infojulgeolekut rahuldavalt koordineerida“.

Järgnevalt kirjeldan neid kahte narratiivi detailsemalt.

4.3.1 Eesti on e-riigina läbi kukkunud, sest pandeemia ajal ei ole piisavalt e-lahendusi kasutatud

7. narratiiv kujutab e-Eestit eduka asemel läbikukkununa. Eeldatavasti tulenevalt valimi ajaperioodist, joonistus kriitika välja just pandeemia raskuste leevendamise, nt vaktsineerimise korraldamise osas (artikkel nr 89).

> *Eesti on e-riik ja e-riik tuleb olla ka vaktsineerimise küsimuses. Täna antakse vaktsineerimisvõimalustest teada telefoni teel. Selleks, et panna end järjekorda ei tohi jääda lootma erinevate ametiasutuste võimekusele Exceli tabelit täita ja infot edastada. Hiljemalt märtsis tuleb käivitada ühtne registreerimissüsteem, mis oleks ühendatud terviseportaaliga. Inimene ei pea olema seotud oma perearstiga nagu pärisori oma maaisandaga. Iga inimene peaks saama portaalis valida endale sobiva koha ja aja vaktsineerimiseks.*
>
> *- väljavõte artiklist nr 66*

Samas laieneb kriitika üldisele elukorraldusele pandeemia ajal. Näiteks kritiseeriti suutmatust tänavust Eesti Vabariigi aastapäeva paraadi digitaalsete vahendite abil korraldada, soovitades et „kui füüsiliselt ei saa paraadi pidada, siis pakume Eestis toodetud tehnikast virtuaalse ülevaate," (artikkel 76). Pandeemia kontekstis tabas kriitika ka kodumaist HOIA äppi, laienedes samas ka vanematele tervishoiu infosüsteemide arendustele ja lahendustele.

> *Eesti riik on koroonaviiruse tõrjega seotud digilahenduste arendamisel katastrofaalselt halvas seisus ja see puudutab nii uut äppi HOIA kui ammu olemasolevat keskkonda Digilugu, leiavad president Toomas Hendrik Ilves ja Euroopa parlamendi saadik ja ÜRO digikoostöö paneeli liige Marina Kaljurand.*
>
> *- väljavõte artiklist nr 89*

E-lahenduste vähese kaasamise ja nn e-tiigri eduloo peatumise osas konstrueeritakse süüdlase või pahalasena enamasti poliitilisi jõude, nt EKREIKE koalitsiooni. Sarnaselt 3. narratiivile, on ka siin Eesti valitsust kujutatud otsustusvõimetu ohvrina.

Meil on olnud kaks kuni viis aastat rahulolevat soiku jäämist, neist viimased kaks aastat aktiivset tagasipööramist, kus digilahendustele vaadati viltu, ja inimesed, kes vastutasid digi eest, ei saanud tegelikult üldse teemale pihta," rääkis ta.

- väljavõte artiklist nr 89

Alfa nendib grupivestluses, et nii 7. kui 8. narratiiv näitavad selgelt, et Eesti on enesekriitika maailmameister. Samal ajal kui Lääne meedia presenteerib edulugusid suhteliselt digitaliseeritud haridussüsteemist, „raputame iseendale meedias hästi palju tuhka pähe, samas kui meie suured lääne sõbrad pigem vaatavad meie poole väga selgelt positiivses võtmes ja toovad meid eduloona esile“ (Alfa). Eesti läbikukkumine e-riigina on tegelikult varasema vaenuliku narratiivi edasiarendus, nagu Delta välja tõi – võltsitavatest ja ebausaldusväärsetest valimistest ning läbikukkunud riigist kõneledes on varemgi ühiskonda proovitud lõhestada. Siin peitub ka selle narratiivi paradoks: mudelautori seisukohast on eesmärk e-tiigri eduloo pisendamine, mis võib olla kasulik nii riigi vaenlastele või konkurentidele maailmaareenil kui ka e-Eesti arenduseks lisaraha või poliitilise tahte kindlustamiseks. Pandeemia kontekstis ebaõnnestumise narratiiv sai alguse konstruktiivse kriitika ja avaliku debati käigus, mis on iseenesest tervitatav.

„Eestis lihtsalt tehnoloogiahuvilised ja äpitaustaga inimesed andsid mõista, et tegelikult saab seda kõike efektiivsemalt teha ja justkui, noh, riik ei kasuta neid võimalusi. Ma arvan, et see levis osaliselt ka seetõttu, et kogu see vaktsineerimise teema on niivõrd emotsionaalne ja sellega on olnud jama. Kui enam-vähem ükskõik mida saab süüdistada, olgu see siis e-riik või midagi muud, siis sellest võimalusest on kinni haaratud.“

- Charlie

Osaliselt tuleneb 7. narratiiv Bravo arvates ka Eesti ajakirjanduse üldisest tonaalsusest koroonaperioodi ja kaasnevate teemade kajastamisel – läbivalt on toon negatiivsem ja kriitilisem kui muu maailma meedias. Echo pakub, et see on osati ka nõukogude aja pärand: oleme väikesed, meil on üks rahvavaenlane, üks õige suund jne. Sealjuures ei välistata ka väikeriigile omast nö Napoleoni kompleksi – Delta tõi välja, et ka Läti võiks enesekriitika maailmameistri tiitlile pretendeerida.

Narratiivi näiliselt e-riigi ja digilahendustega seotud kriitika puudutab väikeses osas ka riiklikku vaktsineerimise kommunikatsiooni – nt on välja toodud, kuidas kahe kuu jooksul tõusis Kreekas vaktsineerimist toetavate inimeste hulk absoluutarvestuses (st kõikide parteide üleses arvestuses; artiklis eristati erinevate erakondade valijate eelistusi) üle 10%, sest Kreeka tipp-poliitikud lasid end avalikult vaktsineerida ning sellest sai mõjus meediasündmus (artikkel nr 67). Lahendusena jäi kõlama soovitus, et ka Eesti tipp-poliitikud peaksid sel kujul eeskuju näitama.

4.3.2 Eestis pole poliitilist tahet infojulgeolekut rahuldavalt koordineerida

8. narratiiv kujutab Eesti infojulgeoleku keskkonda killustatuna ning koordineerimata. Narratiivi alguseks võib pidada selle-teemalist konstruktiivset teadustööd (mis on kaasatud ka käesoleva magistritöö teoorias ptk 1.2.3 ja 1.2.4) ning edukat teaduskommunikatsiooni, sest kui valimis, mis hõlmas iga viiendat artiklit, oli sel teemal lisaks töö autorile veel kolm artiklit, võib eeldada et ajaperioodil ilmus neid kokku veelgi rohkem.

> *Kui poliitikutele läheks iseseisva Eesti kestmine korda ka väljapool kõnesid ja valimiste-eelset aega, oleks Eesti elanikud vaenulike inforünnakute mõju eest senisest märksa paremini kaitstud, riiklik kommunikatsioon oleks süsteemne, paindlik ja loominguline ning vastaste järjepidev mõjutustegevus ei kannaks nii priskeid vilju. /---/ Seega jätkub Eestis omajagu osakondi ja keskusi, kes peaksid seisma hea infojulgeoleku eest. Vähemasti nii palju, kui on poliitilist tahet ja soovi seda tagada.*
>
> *- väljavõte artiklist nr 89*

> *Tasub ehk märkida, et ka küberkaitseliitlase Paasi enda kriitika riiklike institutsioonide vastu on üsna terav ja võib mõneti olla samasuunalise mõjuga kui neil vaenlastel, kelle eest ta hoiatab.*
>
> *- väljavõte artiklist nr 61*

Kõnealuse magistritöö eesmärk oli anda soovitusi julgeolekukeskkonna parendamiseks ning julgeolekukommunikatsiooni ühtlustamiseks (Paas, 2021). Ka NATO arendusväejuhatuse ülem kindral André Lanata nentis, et „peame lülituma reaktiivselt toimimiselt proaktiivsele“ ning

vaatama traditsioonilisest kaitsesektori vahenditest kaugemale (artikkel nr 74). Narratiivi kasutavad siseriiklikuks tarbimiseks veel ka infokeskkonda populistliku retoorikaga segaseks ajavad poliitikud, kes kahjustavad sellega nii kohalikul kui rahvusvahelisel tasandil ühiskonda õõnestades Eesti julgeolekut, mainet ja heaolu (artikkel nr 68).

> *Mart Helme nimetas valitsuse lagunemist ning uue valitsuse moodustamist riigipöördeks – väga tõsine ja hirmutav väide. Coup d'état ehk riigipööre on ebaseaduslik ja põhiseadusvastane valitsuse kukutamine, mida tavaliselt teostatakse jõuga.*
>
> *- väljavõte artiklist nr 68*

Poliitilist tuge Eesti psühholoogilise kaitse koordineerimiseks pole selle narratiivi esituses kas üldse või on see ebapiisav. Pigem tuuakse esile poliitilise vastasseisu tõttu üksteisele vastu töötamine, nt strateegilise kommunikatsiooni bürood on valitsus olev koalitsioonipartei kutsunud teise riigi propagandaametiks (artikkel nr 58). Ka 8. narratiivi puhul tekkis fookusgrupis osalenud ekspertide vahel arutelu sellest, miks on narratiivi keskmes taas iseenda võimete väiksemaks mängimine, sest ka infojulgeoleku vallas tuuakse Eestit eduloona esile.

> *„Meil on strateegiline kommunikatsioon laiapindse riigikaitse üks kuuest sambast; meil julgeolekukomisjoni all käib koos valdkondlik grupp partnereid regulaarselt, jadajada… See ei ole universaalne ja seda nähakse tugevana.“ - Alfa*

Välja toodi taas Venemaa oportunism kontekstis, kus tõenäoliselt on nemad sellise narratiivi peamised kasulõikajad, et Eesti „nagunii ei suuda oma infojulgeolekut koordineerida; et keegi väljas, suur, kuri, osav, tehnoloogiliselt arenenum ja teeb teiega seda, teist ja kolmandat, mis muidugi ei ole tõsi,“ (Delta). Osalejad nentisid, et nii 7. kui ka 8. narratiiv illustreerivad, kuidas Eestis ei osata kriitikaga adekvaatselt toime tulla: „Kui on midagi pahasti, siis on kohe väga pahasti, et me oleme läbi kukkunud või siis et me ei saa hakkama,“ (Foxtrot). Ka selle narratiivi puhul võib narratiiv olla kasulik ka tagasisidena, mida tõlkida riiklike strateegiate arendamisel edasisideks. Ohtlikuks muutub selline suhtumine ekspertide sõnul siis, kui sellega kaasneb alla andmine või käega löömine.

See narratiiv tõi esile huvitava paradoksi: psühholoogilise kaitse vaatevinklist ohtlik narratiiv võib julgeolekuvaldkonna ümber korraldamiseks olla vajalik konstruktiivne kriitika. Mõlema Eesti-keskse narratiivi puhul eeldasid eksperdid, et tegemist on siseriikliku narratiiviga, mis pole või on väga vähesel määral välisriikidesse ja nende uudisajakirjandusse levinud.

4.4 Tänapäevane infokeskkond kui üleilmne julgeolekuoht

Siia alapeatükki koondasin narratiivid, mille puhul pole ainult ühte keskset rahvusvahelist tegutsejat võimalik välja tuua, ent mis kannavad Kopenhaageni koolkonna julgeolekustamise (vt ptk 1.2.3) tunnuseid. Rahvusvaheliste suhete distsipliini narratiivide eristuse järgi jaotuvad need:

- probleeminarratiivideks, nagu 9. narratiiv „Küberruumis küpsevad radikaalid, et minna füüsilisse maailma kaost külvama“ ja 10. narratiiv „Infokeskkond on spionaaži ja riigi süsteemide ründe lihtsaks ning kurjategijad raskesti tabatavaks teinud“ ning
- identiteedinarratiiviks, nagu 10. narratiiv „NATO ei ole suutnud uue strateegilise keskkonnaga piisavalt kohaneda“.

Järgnevalt kirjeldan neid kolme narratiivi detailsemalt.

4.4.1 Küberruumis küpsevad radikaalid, et minna füüsilisse maailma kaost külvama

9. narratiivi esile tõusmiseks oli 2021. aasta esimestel kuudel pinnas soodne. Koroonapandeemia ning teooriapeatükis mainitud infodeemiaga seoses on meediakirjaoskustest hakatud avalikus ruumis rohkem rääkima, niisiis on teadlikkus inimestel suurem. Aruteluväärtust avalikus ruumis tõstsid ka võrdlemisi värsked intsidendid. Rahvusvahelisel tasandil sai näiteks Trumpi toetajate organiseeritud rahutused Kapitooliumis ning korraldusega seotud organisatsioon Proud Boys Kanada julgeolekuametilt terrorirühmituse staatuse (artikkel nr 20). Kodumaal kajastati Eestis sündinud ning 6-aastasena Rootsi kolinud noormehe radikaliseerumist rahvusvahelistes fašistide sotsiaalmeediagruppides Instagramis ja Discordis (artikkel nr 21). Tegelasi kujutatakse pahalastena, aga nende tegevust ei seostata riigiga, vaid hoopis indiviidi või kogukonnaga.

Ehkki seda narratiivi esines valimis vaid killustunult ning see sobib esmapilgul ka 10. narratiivi alamnarratiiviks, tõin selle eraldi välja, sest see näitlikustab e-ohtude küberruumist füüsilisse

keskkonda kandumist. Kineetilised küberoperatsioonid ehk küberrünnakud, mille tagajärjel saab otseselt või kaudselt põhjustada ka füüsilist kahju, vigastusi või surmajuhtumeid (Appelgate, 2013: 2), leidsid valimi moodustanud artiklite avaldamisperioodil kandepinda tõenäoliselt ka seetõttu, et septembris 2020 suri Düsseldorfis küberrünnaku tõttu inimene.

> */---/ kiirabi pidi Düsseldor ülikooli haiglat tabanud küberrünnaku tõttu eluohtlikus seisundis patsiendi viima teise haiglasse. See võttis liiga kaua aega ja patsient suri. Häkkerid krüpteerisid haigla infosüsteemi ära ning nõudsid dekrüpteerimise eest lunaraha. Düsseldorfis juhtunut peetakse üheks esimeseks küberrünnakuks, milles kaotas elu inimene.*
>
> *- väljavõte artiklist nr 87*

Nii 9. kui ka 10. narratiiv kannavad julgeolekustamise tunnuseid. Selle narratiivi puhul on eksistentsiaalse ohuga võitlemise meetodiks pakutud regulatsioonide muutmine selliselt, et korrakaitse ja julgeoleku organitel oleks varasemast lihtsam ligipääs andmetele, mis aitaks küberuumi vahendusel sooritatavaid kuritegusid ennetada.

> *Kellelgi ei teki küsimust, kui politseil on juveelivarga tabamiseks vaja magamistoa vaibalt DNA proov võtta, kuid samas toas peetud Messengeri vestluse küsimist peetakse jämedaks privaatsuse riiveks. Paradoks, kas pole? Usaldame oma isiklikud andmed pimesi teadmata isikute ja ettevõtete käsutusse üle maailma, aga oma politseile mitte. Las selle paradoksi põhjuste otsimine jääda sotsiaal- ja kultuuriteadlaste pärusmaaks.*
>
> *- väljavõte artiklist nr 2*

Ka fookusgrupis oli esmane reaktsioon narratiivile lahenduste pakkumine. Näiteks Alfa tõi üles veebiplatvormide õigusliku raamistamise – kuna oleme Euroopa Liiduna jäänud raamistamisega hiljaks, seisab probleemi leevendus (mitte lahendus) ka selgete piiride seadmise taga. Alfa arvates võiks alustada kasvõi sellest, et seadused, mis kehtivad *offline*-s, kehtivad ka *online*-s. See viis arutelu edasi agentsuse juurde: kui vaadelda indiviidi, riigi ja üleilmse tehnoloogiahiiu tasandil, siis kes eeskätt vastutab selle eest, kui informatsiooniline mõjustamine õnnestub? Seega

oli julgeolekustamise edu märgata ka ekspertide mõttekäigus, sest ohu (tehnoloogiahiiud) eksistentsiaalsena kujutamise kõrval pakuti ka lahendusi (rohkem regulatsioone ja kontrolli), mis ei pruugi lõppkokkuvõttes indiviidile parimad olla. Siin võib täheldada ka Madissoni ja Ventsli (2018: 182) poolt välja toodud süsteemitasandi ohtu, mille juures tajutakse IKTd igapäevaeluks vajaliku taristuna, kus varitsevad samas tavainimeste jaoks raskesti hoomatavad riskid. Oht peitub ka selle narratiivi puhul käega löömises.

4.4.2 Infokeskkond on spionaaži ja riigi süsteemide ründe lihtsaks ning kurjategijad raskesti tabatavaks teinud

10. narratiiv räägib samuti piiriülesest, jagatud ohuna tajutavast riskist: üksikute näidete najalt on narratiivina kanda kinnitanud heaoluks vajalike infosüsteemide väljalülitamine. Näiteks küsiti Florida veejaama vett küberrünnakuga mürgitada püütud endise töötaja puhul koheselt kommentaar ka selle tõenäosuse kohta Eestis (artikkel nr 39).

> *Küberrünnakuga saab välja lülitada elektrivõrgu, ja kui pole elektrit, ei tööta tanklad, ei toimi teenused ega pangaautomaadid. Valitseb üleüldine pimedus, pole voolu ega saa sooja. Nagu ulmefilmi stsenaarium, mis kergesti võib saada reaalsuseks. Panustame 2,5protsendiste kaitsekulutuste asemel enam tervishoidu ja sotsiaalkaitsesse. Mõtleme küberjulgeolekule. Tuleviku sõjad on tehnoloogia ja bakterite päralt. Aeg oleks kindralitel ja kaitseministril silmadavada, et näha, mida teevad Hiina, Venemaa ja USA. Meie tervis ja julgeolek sõltuvad meistendist. Vaevalt tahame oma rumaluse eest lõivu maksta.*
>
> *- väljavõte artiklist nr 88*

Lisaks eluks vajalike süsteemide halvamisele, konstrueeritakse küberohuna ka küberkuritegevuse hüppelist kasvu viimase aasta jooksul, mis ohustavad nii välisriike (artiklid nr 8, 38, 39, 42, 87 ja 91) kui ka Eestit (artiklid nr 1, 9, 39, 40 ja 77). Narratiiviga süvendatakse arusaama, et küberrünnakud muutuvad „aina kavalamaks ja keerulisemaks ning küberkurjategijate sihtrühmad aina laiemaks. Kaitstud pole keegi," (artikkel nr 8). Küberkurjategijaid konstrueeritakse intelligentsete pahalastena, laiemat avalikkust aga jüngritena, kelle teovõime sõltub sellest, mida

pahalane soovib või lubab. Selle narratiivi tegelaste konstrueerimise juures on huvitav ka pahalaste eesmärkide vähene strateegilisus, pigem kumab implitsiitselt läbi indiviidi või ettevõtte kohustus pahalasega kohtumise tõenäosust minimaliseerida. Pahalasega kohtudes saab jüngrist ohver – heatahtlik, kaastunnet väärib, aga endaga juhtunus osaliselt süüdi osapool.

Koordineeritud küberrünnakutega on Eestil kogemus olemas (nagu ptk 1.2.2 välja tõin), mis võimaldab seoseloomet ka selle võimaliku ohunarratiiviga. Infokeskkonna ohtude eksistentsiaalsena kujutamise lahendusena pakutakse sarnaselt 9. narratiivile andmeregulatsioonide (või vähemalt ühiskonna suhtumise) muutmist ning ka uurimistoiminguteks varasemast rohkemat või kergekäelisemat andmete loovutamist.

> *Õiguskaitse eksperdina saame kinnitada, et andmed on digitaalse maailma DNA. Ilma andmeteta virtuaalmaailma kuritegu ei lahenda. Ja mida vähem on andmeid või mida raskemini kättesaadavad need on, seda keerulisem on juhtunut välja selgitada ning kuritegusid tõendada.*
>
> *- väljavõte artiklist nr 2*

Charlie tõi välja, et 10. narratiivi relevantsus on hiljutiste Solar Windi ja Microsoft Exchange'i jt tarneahelate rünnakutega seotud ning arvab, et ka selle teema puhul tuleb teatav ettevaatlikkus pigem kasuks.

> *„Konkreetselt selle Microsoft Exchange'i haavatavuse puhul me nägime ja imestasime, et see ohu ja riski tolereerimine Eestis on ikkagi endiselt suhteliselt kõrge, ehk et need nii-öelda teenuse pakkujad, kellele saadeti hoiatus, et neil on need haavatavused ja palun kohe esimesel võimalusel ära lappida, võtsid neid suhteliselt lahjalt vastu, ehk et ei kiirustanud neid haavatavusi kõrvaldama."* - *Charlie*

See seostub mõneti ka 8., infojulgeoleku koordineerimise tahte puudumisest kõnelenud narratiiviga – ka siin jõuti vestluse käigus järeldusele, et pigem kipume Eestis neid teemasid liiga vabalt võtma ning ei teadvusta ohu tegelikku määra. Samas ei saa otseselt ka öelda, et tegemist on eksitava narratiiviga, sest nagu Bravo välja tõi: netist narkootikumide tellimisest rääkimine,

tapmisähvardused sotsiaalmeedias ning selle varjatud, karistamatu tegevuse konteksti asetamine on tunnetuslikult viimase paari aasta teema.

Ka selle narratiivi puhul võis täheldada valimis fragmente vastu-narratiividest, mis konstrueerisid Eestit rahvusvahelisel areenil tunnustatud küberkaitse eksperdina (artiklid nr 85, 90 ja 92) ning tõid näiteid nii Eesti kui liitlaste ühisõppustest, mille käigus mängitakse läbi võimalikke küberrünnakutest tingitud katastroofistsenaariumeid (artikkel nr 79) kui ka ühisest heidutuskoalitsioonist (artikkel nr 90).

4.4.3 NATO ei ole suutnud uue strateegilise keskkonnaga piisavalt kohaneda

12. narratiiv on grupivestluses osalenud ekspertide sõnul korduv ning erineva rõhuasetusega esinenud aastaid. Narratiivi edasiarendust iseloomustab just rõhuasetus muutunud infokeskkonna kontekstis kognitiivse sõjapidamise dimensiooni senisest varasemale tähtsusele.

> *Vastaste eesmärk on mõjutada sihtriigi elanike tajusid, hoiakuid, käitumist ja otsuseid. Võitlus ei käi enam ammugi soodes, rabades ega kaevikutes, vaid meie kõigi peas.*
>
> *- väljavõte artiklist nr 44*

> *NATO vajab uut Atlandi-ülest tõuget strateegilise tugevuse väljanäitamiseks nii sõjalistele kui ka artiklis 5 käsitletud «halli ala» ohtudele (küberrünnakud, infooperatsioonid jm) vastamisel. Järgmine tippkohtumine, NATO 2030 ja strateegilise kontseptsiooni ülevaatus annab selleks hea võimaluse.*
>
> *- väljavõte artiklist nr 31*

Narratiiv esitab geopoliitilise asukoha kõrval muutunud ohu vormina ka „uued hübriidohud, mis muudava muudavad mängu veelgi keerukamaks, olgu siis tegu küberrünnete, desinformatsiooni või terrorismiga“ (artikkel nr 102). Informatsioonilise üleoleku saavutamine inforuumis on Lääneriikide jaoks selles uues infokeskkonnas elulise tähtsusega, sest „kui laseme oma moraali laostada ning eneseusu ja -kindluse mutta trampida, ei aitaks meid ka brittide Abramsi tankid ega jänkide tuumarelvad“ (artikkel nr 44). Ühiskonna vastupanuvõimet esitatakse seega vajaliku

eeltingimusena ka konventsionaalsete konfliktide võitmiseks, sätestades et „allianss peab jätkuvalt tulema toime nii otseste sõjaliste kui ka ebakonventsionaalsete ja uute ohtudega“ (artikkel nr 90).

Narratiivi strateegiline sidumine minevikusündmustega nagu külm sõda toetab pakutud lahendust, milleks on Atlandi-üleste suhete tugevdamine, heidutuse jätkamine ning Euroopa Liidu julgeolekupoliitikas NATO poliitika dubleerimise minimaliseerimine (artiklid nr 29 ja 31). Soovitav tulevik saavutatakse Euroopa Liidu ja NATO eduka koostöö läbi hübriidjulgeoleku tagamisel (artikkel nr 74), aga teel on takistusi, näiteks üksikute riikide vetoõigusest ja „obstruktsiooni nõiaringist mööda pääsemine“ (artikkel nr 29).

Kohati on narratiivi kasutamisel märgata julgeolekustamist ka Venemaa poolt. Näiteks on Venemaa kaitseministri nõunik Andrei Ilnitski sõnul “Lääneriigid USA-ga eesotsas alustanud Venemaa vastu uut tüüpi mentaalset sõda, mille eesmärk on venemaalaste eneseteadvuse hävitamine ja mille tagajärjed ei ilmne kohe,“ (artikkel nr 43).

> *Mentaalses sõjas vastupanu osutamiseks on Ilnitski sõnul vaja internet „suveräänseks” muuta, valmistada ette kaadrid informatsiooniliseks vastutegevuseks, teha tööd noortega ja pidada dialoogi elanikkonna konservatiivse osaga. Ilnitski arvates kujutab see osa elanikkonnast endast enamust ja on praeguse võimu alusvalijaskond.*
>
> *- väljavõte artiklist nr 43*

Julgeolekustamine selle narratiivi juures on taas paradoksaalne – kuidas saab NATO korraga olla infokeskkonnas Venemaa eneseteadvust hävitav eksistentsialane oht ning samaaegselt ka strateegilises julgeolekukeskkonnas nõrgas positsioonis? Seda vastuolu võib selgitada julgeolekustamise ehk interneti informatsioonilise sõjategevuse lahingutandrina presenteerimise juurde pakutud lahendus. Vihjatakse interneti muutmisele ning ehkki ka ülal toodud väljatõstes kõneletakse suveräänsusest, võib see olla osa avalikkuse mentaalsest ettevalmistamisest ning näide näiliselt välispoliitilisest sõnumist, mida levitatakse siseriiklikuks tarbimiseks, et tulevikus internetikasutuse või väljendusvabaduse piiramist põhjendada.

Delta arvas, et 11. narratiiv on vähemalt kümme aastat ning vana baseerub varasemast tuttaval paradoksaalse olemusega narratiivil, mis korraga diskrediteerib NATO-t, nimetades teda võimetuks või konstrueerides koalitsiooni „ajusurma“ ohvrina (tuntud Emmanuel Macroni 2019. aasta tsitaat The Economistile), aga samas maalib NATO-t ka Venemaa (kangelase) kiusaja või agitaatorina.

> *„Mida Kreml ütleb, et NATO lähenemine Vene piiridele on ohtlik ja provotseerib ja Venemaa peab reageerima kohe. Ja samas nad ütlevad, et NATO on aegunud ja ei suuda midagi kaitsta ja on nii sõjaliselt kui poliitiliselt võimetu. Noh, mis on vastuoluline narratiiv, aga Kremlile käib küll. Ja kuidagi see töötab ka.“* - *Delta*

Tegelikkuses näitab Delta sõnul kasvõi see, et Eestis „loobitakse alla langevarjureid otse Ameerikast“, et koostöö on viljakas ja heidutus töötab. Lisaks räägib NATO ka kuuenda sõjapidamise domeeni ehk kognitiivse domeeni käsitlemist strateegiates ja plaanides. See ongi justkui lahendus, mida narratiiv pakub – NATO peab laiendama arusaama sõjapidamisest.

> *„Esimene domeen on väga klassikaline maasõda, teine meresõda, kolmas õhusõda, neljas kübersõda, viies kosmosesõda ja nüüd arutletakse kuuenda domeeni, mis on kognitiivne domeen, ja mis ei ole ainult tehnoloogilised vahendid, vaid ka see, mis on meie kõrvade vahel. Mis on nagu muutunud, on muutunud see, et see platvorm, millega mõju on inimesi võimalik mõjutada, on tänu tehnoloogia arengule muutunud, et sa põhimõtteliselt võid sihtmärgiks võtta iga üksikisiku, kes on võrku ühendatud üle terve maailma.“*
>
> - *Delta*

Nii on Delta arvates heidutusena toiminud ka Ameerika presidendivalimiste ajal Sankt-Peterburi kuulsa Savushkina 55 aadressil asuva trollikontori välja lülitamine, aga on ka üldisemalt mõistetud, et mõttemaailmas sõdimine on võtmetegur. Valeri Gerassimov, kelle doktriinist põgusalt ka ülal juttu oli, on öelnud et kuna inforuum ei kuulu mitte kellelegi ja seal riigipiire pole, võib seal teha, mida soovid. Narratiiv pakub ka lahenduse: NATO ja Eesti ühine strateegiline eesmärk peaks olema inforuumi Metsikust Läänest kontrollitud ja reguleeritud valdkonna kujundamine, et pahalasena konstrueeritud tegutsejate informatsioonilisele mõjustamisele, nagu nt Hiina ja Venemaa, vastu seista.

5. JÄRELDUSED JA DISKUSSIOON

Analüüsis joonistus välja üksteist narratiivi, mille üle arutlesin kuue eksperdiga fookusgrupis. Olulisemad tulemused võiks jagada kolme kategooriasse: enesekindlus Eesti kui digiriigi brändiloomes, tehnoloogilise jõu esile kerkimine rahvusvahelistes jõujoontes ning küberohtude julgeolekustamise võõrandav mõju tavakodanikule.

5.1 E-tiiger või enesekriitika maailmameister?

Räägin brändiloomest Bolini, Jordani ja Ståhlbergi (2016: 14) eeskujul seetõttu, et piirid (riigi) brändiloome, (avaliku) diplomaatia, pehme jõu ja ajakirjanduses levitatud narratiivide vahel on hägused. Vaieldamatult on e-Eesti ka pehme jõu tööriistaks ning osa avalikust diplomaatiast, aga kasutan sõna brändiloome just seetõttu, et narratiivi juured pärinevad Welcome to Estonia ajast. Selgus, et Eesti digiriigi brändiloomega kaasnenud küberoptimistlik diskursus, mis langes ajaliselt kokku Eurovisiooni võõrustamisega 2002. aastal (Jansen, 2008: 128), on aja möödudes muutunud sügavaks enesekriitikaks. Kriitika läbikukkunu Eesti e-riigi, nt e-hääletuse suunal, oli ekspertidele varasemast tuttav vaenulik narratiiv, mille edasiarendus 7. narratiivi näol taas siseriiklikult levima on hakanud. Grupiintervjuus osalenud eksperdid arvasid, et tõenäoliselt moodustus narratiiv e-lahenduste vähese rakendamise kohta IKT-valdkonna spetsialistide konstruktiivse kriitika baasilt ning levib enamjaolt siseriiklikult (kui üldse välismaises uudisajakirjanduses esineb, siis väga vähesel määral).

Eesti on suisa enesekriitika maailmameister, nagu nentisid fookusgrupi eksperdid. Enesekriitikal seni midagi häda, kuni see ei vii täieliku käega löömiseni või suhtumiseni, et kuna oleme niigi maha jäänud, pole enam midagi muud teha kui oma kunagise eduka digiriigi saatusega leppida. Kriitikat tuleb osata adekvaatselt vastu võtta ning sellele reageerida, mitte kogu riigi brändi ümber mõtestada, sest vabatahtlike välja töötatud HOIA äpp või pandeemia eel rahvusvahelise eduloona välja toodud Digilugu polnud kriisiolukorras loodetud tasemel. Kui toetuda Denti (2008: 213) tähelepanekule, et foucault'liku läätse läbi võib ajakirjandust mõtestada avalikus ruumis justkui standardiseeritud tõde tootjana, siis saab ekspertide murest ka aru. Kui meedias piisavalt korrutada, et e-tiiger on tukkuma jäänud ning digiriik pole enam Eesti peamine nn müügiartikkel laiemas maailmas, siis võivad seda uskuma jääda ka meie liitlased. Meie kuvand

avatud, kiiresti arenenud, innovatsioonile ja tehnoloogilise võimekuse arendamisele keskendunud väikeriigist ongi Eesti pehme jõud. E-riigi lahenduste osas toovad teised riigid ja rahvusvahelised ühendused meid eeskujuks ning soovivad koostöös Eestiga samas suunas areneda. Miks näevad välispartnerid meie e-tiigrit oluliselt positiivsemas valguses kui me ise?

Võimalikke põhjendusi läbikukkunud digiriigi narratiivsele konstrueerimisele on kaks. Eksperdid tõid välja, et küsimus võib olla ka eestikeelse uudisajakirjanduse üldises tonaalsuses koroonakriisi kajastamisel: kui teistes riikides suunati kriitika teravik enamasti vaktsiinitootjate või rahvusvaheliste ühenduste poole, siis Eesti uudismeedias on nende hinnangul fookus olnud valitsusasutuste töö ja otsuste kritiseerimisel. Uudisajakirjanduses kajastatu kandub kas terve narratiivi või fragmentidena diskursiivse ülekande läbi sotsiaalmeediasse, kus selle levikut ja tõlgendusi ajakirjanikud enam kontrollida ei saa. Ehkki ajakirjandus võib ka konstruktiivseid lahendusi pakkuda, ei ole need suurte teemade puhul, mida mitmes loos kajastatakse, pinnapealse lugeja jaoks selgelt välja toodud (nt ei kohta Eesti meedias uudist pealkirjaga „HOIA äpi populariseerimine kukkus läbi – aga pole hullu, sest nakatumiskordaja on tegelikult OK!“). Tagasiside, mida tõlkida edasisideks, on igati väärtuslik, aga lahendusteta kriitika süvendab aja jooksul taju, et nüüd ongi kõik halvasti.

Teise võimaliku põhjusena näen Eesti brändiloome siseriikliku kommunikatsiooni läbikukkumist. Kahtlemata on innovatiivse digiriigi kuvand rahvusvahelisel areenil jätkuvalt Eesti jaoks oluline pehme võimu alustala ning nt pandeemia kontekstis toodi fookusgrupis osalenud ekspertide sõnul ka meie paljuski digitaliseeritud haridussüsteemi positiivse näitena välja. Kuidas suhtub sellesse aga lapsevanem, kelle kolmel erinevas koolis käival lapsel on kõigil erinev e-kool, erinevad koduõppe digikeskkonnad ning seega ka erinevad tehnoloogilised vajadused õppetöö sooritamiseks? Tõenäoliselt tekitaks välismeedias meie digihariduse kiitmise lugemine temas kognitiivse dissonantsi. Kui Welcome to Estonia brändiloome käis käsikäes uute digilahenduste tutvustamisega, alustades ID-kaardi süsteemist 2002. aastal ning tuues järjepanu välja ka e-hääletamise, e-tulumaksuaruanded, e-tervishoiusüsteemid ja digiretseptid, e-residentsuse jpm, siis nüüd oleme teises arengujärgus. Digipädevad kasutajad märkavad, kuidas 20 aastat vanad süsteemid hanguvad, riiklike e-teenuste kasutamine on suure liikluse puhul häiritud ning Flashi baasil üles ehitatud kaardiregistrid, mida Adobe kasutajatoe lõppemisel

kohandati, vajaksid täielikku uuenduskuuri. Virtuaalkeskkonda võõristavalt suhtuvad kodanikud jällegi ei näe suures e-teenuste ampluaas tõenäoliselt samasugust väärtust, sest riik pole siiani võtnud seisukohta selle osas, kas kõik e-tiigri kodanikud peaksid olema vähemalt info- ja digipädevuste algtasemel ning kui jah, siis kuidas tagada tasuta ligipääs vastavasisulistele koolitustele?

Konstruktiivse või vähem konstruktiivse avaliku kriitika vili on ka narratiiv Eesti infojulgeoleku vähesest koordineeritusest, millest on kinni haaranud ka populistlikud poliitikud ning mis rahvusvahelisel areenil kuidagi Eesti mainele kasuks ei tule, eriti kontekstis, kus vaenulikke narratiive levitav Venemaa ehitab oma strateegia paljuski üles oportunismile. Julgeolekukommunikatsiooni kujundajatele võiks see tõstatada küsimuse, kuidas avalikus ruumis (info-)julgeolekut kritiseerida ilma vaenulike mõjutajate narratiividesse kätte mängimata. Psühholoogilise kaitse ehk rahva informatsioonilisest mõjustamisest või kodanikuühiskonna õõnestamise katsetest teavitamine peavad olema tasakaalus narratiividega sellest, kuidas probleeme lahendatakse. Kas lahenduseks võiks olla mingite institutsioonide avalikus diskussioonis vastu-narratiivide levitamine või apoliitiliste ekspertide lahenduste pakkumine kriitilise diskursuse osana, jäägu valdkonna ekspertide otsustada. Oluline on see, et jõutaks riigikaitsega tegelevate institutsioonide-ülese lahenduseni – poliitikud vahetuvad ja retoorika muutub, samas kui poliitikakujundamise alused ja strateegilised tegevuskavad on püsivamad.

5.2 Tehnoloogilise jõu roll tuleviku maailmakorra visandamisel

Delta kasutas Hiinast rääkides fraasi tehnoloogiline jõud, mis võtab e-ohtudega seonduvate narratiivide olulisuse hästi kokku: üheks uuringu järelduseks on tehnoloogilise (sh küberkaitselise) võimekuse konstrueerimine tulevikus rahvusvahelisel areenil domineerimise eeltingimusena. Esimese kolme narratiivi keskmes on tegutsejana Venemaa, kelle informatsioonilise mõjustamise ning ühiskonna lõhestamise võimekust konstrueeritakse hirmsama ja võimsamana kui see tegelikult on. Tõenäoliselt omistatakse Kremli seotust kohati liiga kergekäeliselt, teisalt ei tohi ka valvsust kaotada: on selge, et geograafiliselt Venemaa jaoks soodsates piirkondades asuvate riikide jaoks on informatsiooniline vastasseis konventsionaalse sõja ohu tõttu destabiliseerivam.

Ehkki Hiina asub meist geograafiliselt kaugel, on ka see oht tunnetuslikult lähemale tulnud. Läänes pole Hiina hegemooniasoov ja väärtusruumi laiendamise ambitsioon midagi uut, aga Eesti ajakirjandus ja julgeolekuteenistused on teemat alles viimastel aastatel käsitlema hakanud seoses Huawei 5G seadmete kasutusele võtmise ning nt ka Tartu ülikooli teadusprojektidega. Võimalik, et seda võib tõlgendada ka digiriigi eduna: ehk on Hiina rahvaarvu kõrval imepisike Eesti suurvõimule huvipakkuv just tehnoloogilise võimekuse ja innovatsioonile avatud suhtumise tõttu? Igatahes on huvi vastastikune: Eesti sideettevõtted tahavad tõenäoliselt ka edaspidi Euroopas toodetust oluliselt odavamaid „Made in China“ IKT-taristu jaoks vajalikke kaupasid, samas kui Hiina on huvitatud 5G ja muude uute tehnoloogiate arendamise lipulaeva tiitlist. Selles osas on Hiina ja Eesti brändiloome sarnane: mõlemad soovivad end tehnoloogiliselt võimeka digiriigina positsioneerida. Paistab, et suurvõimu huvid on Eestis kaitstud, sest Pekingit kritiseerivate narratiivide kohta ilmus koheselt ka saatkonna vastus, samuti ilmus Eesti uudisajakirjanduses ka vastunarratiive – siin paistab olevat rohkem strateegiat ja vähem oportunismi kui Kremli puhul, mis koos Hiina majandusliku ja tehnoloogilise jõuga teeb hoolimata geograafiliselt kaugusest ohu hoopis reaalsemaks.

Oht seostub taas ka digiriigi brändiloomega: kui Hiinas toimub tehnoloogiline innovatsioon ning meie digiriigina tahame uusi Hiina leiutisi kasutada, siis peame arvestama ka Hiina autoritaarse riigikorraga ning mitmetes küsimustes silma kinni pigistama. Näiteks on Hiinas kasutusel üks maailma võimsamaid näotuvastussüsteeme ning kodanike käitumist suunatakse jälgimisühiskonnas üsna palju, aga seda tehakse autoritaarselt, isikuvabadusi ja andmekaitset eirates. Selles osas Eesti ega Euroopa tõenäoliselt Hiinale järgi jõuda ka ei soovi, pigem võib Hiina sotsiaalse krediidi süsteemi tuua näiteks siis, kui rääkida küberjulgeolekustamise käigus pakutud andmete laialdasema jagamise lahenduse tumeidamast tulevikustsenaariumist. Koostöös autoritaarse ja tehniliselt võimeka Hiinaga tuleb nii Eestil kui ka NATOl korraga püüelda parimate lahenduste ja praktikate ülevõtmise poole, aga samas ei tohi end pimestada lasta. Tuleb silmas pidada nt Hiina ettevõtete kohustust riigivõimuga koostööd teha. Ehkki julgeolekuasutustel on ka Läänes võimalik tehnoloogiaettevõtetelt andmeid välja nõuda, on neil võimalus ka riigi otsus kohtus vaidlustada ning enda eest võidelda, mis muudab grupiintervjuus osalenud ekspertide hinnangul olukorda kardinaalselt.

Tehnoloogiline jõud või õigemini selle puudumine mängib rolli ka Venemaa tulevikustsenaariumite konstrueerimisel. Ehkki kahe riigi koostööd nähakse probleemina, on Hiina hegemoonia nii välja joonistunud narratiivide kui ka grupiintervjuus osalenud ekspertide arvates tõenäolisem, sest neil on reaalne toode, millega kaubelda. Näiteks on enamike nutitelefonide kiibid pärit Hiinast, mistõttu venis ka pandeemia alguses uute mobiiltelefonide tootmine. Venemaaga seonduvatest e-ohtudest rääkides on jutt aga indiviidide mõttemaailma mõjutamisest. Näiteks kuulus Savushkina 55 trollivabrik tegutses Ameerika Ühendriikide presidendivalimistesse sekkudes eeldusel, et ehkki seal töötavad inimesed ei saa ise oma häältega tulemusi mõjutada, on neil võimalik hääleõiguslikke USA kodanikke mõjutada. Mõnes mõttes on see riiklikust küberrünnakust nagu 2007. aastal isegi ohtlikum, sest iga internetiühendusega kodanik on potentsiaalselt mõjutatav ning tänu sotsiaalmeedia mittelineaarsele ja orgaanilisele info levikule ka potentsiaalne mõjuagent. Tõsiste tagajärgedega küberrünnaku korral NATO liitlase vastu käivituks ka Artikkel 5, mida Venemaa mõistagi püüab vältida. Sotsiaalmeedias koordineeritud infooperatsioonid võimaldavad aga Kremlil enda seotust varjata. Samuti pole sellisele mikrotasandi mõjustamisele Eesti kontekstis nii kiiret lahendust kui nt küberrünnaku puhul, millega CERT-EE koheselt tegelema hakkaks, sest ühiskonna vastupanuvõime tõstmine eeldaks indiviidipõhist pädevuste arendamist. Kui kaua läheks, et iga Eesti inimene oleks piisavalt kursis infokeskkonna ja platvormide loogikaga ning enam osava trollimise ohvriks ei langeks? Samas võiks tehnoloogilise võimekuse keskne roll tulevase maailmakorra visandamise juures olla inspireeriv Eesti arenguvisioonide visandajatele ja elluviijatele, sest tehnoloogilise võimekuse arendamine on erinevalt sõjalise võimekuse arendamisest midagi, mille edu pole otseses seoses rahvaarvu ega riigieelarvega, vaid seda saab ennetada ka nt välismaistele tehnoloogiaettevõtetele soodsate maksutingimuste loomise ja muul moel rahvusvaheliselt tunnustatud tegijate Eestisse meelitamisega.

5.3 Küberjulgeolekustamisest võimestamiseni

Küberohtude julgeolekustamine on paradoksaalselt korraga kasulik ja kahjulik. Kasulik, sest see paneb ekspertide sõnul indiviide või ettevõtteid probleemi teadvustama ja seega ettevaatlikumalt käituma. Kahjulik aga seetõttu, et vastandub täielikult UNESCO kontseptsiooniga, mille järgi peaks meedia-, info ja digipädevuste arendamine olema *võimestav*. Nagu Kopenhaageni

koolkonna eeskujul on välja toonud ka nt Madisson ja Ventsel (2018: 182): kui e-ohte tajutakse tavainimese jaoks liigselt keerulisena ning ohtudest hoidumiseks vajalikke teadmisi IKT-valdkonna spetsialistide pärusmaana, tekib ka siin käega löömise oht. Digivahendite kasutamine igapäevaelus tekitab seega taju riskist, mida tavakodanik ei oska ega saa maandada. See tekitab küsimuse: kuidas inimesi virtuaalmaailmas teadlikumalt käituma panna ilma neid ohte eksistentsiaalseks paisutamata? Tean meediakoolitajana omast käest, et keeruliste teemade selgitamine erandlike ja dramaatiliste näidete najal on koolitatavate tähelepanu tõmbamiseks küll kasulik, aga samas võib valdkonnast kaugele inimesele jätta mulje, et musta tulevikustsenaariumi eest pole pääsu. Ühe hea võimestava kampaania näitena võiks siinkohal välja tuua RIA „Ole IT-vaatlik“, mis esitab küberohte käsikäes lahendustega, kuidas riske organisatsioonis maandada.

On problemaatiline, et küberkurjategijaid konstrueeritakse intelligentsete pahalastena, laiemat avalikkust aga jüngritena, kelle teovõime sõltub pahalase soovidest või tujudest. Kui pahalane indiviidi sihilikule võtab, saab isikust jüngrite massist esile tõstetud ohver, kes väärib küll kaastunnet, aga keda konstrueeritakse samas ka osalise süüdlasena (võtkem nt raamatupidajad, kes langevad õngitsuskirjade ohvriks). See tõstatab huvitava küsimuse agentsusest: kas infojulgeoleku tagamine on indiviidi õlgadel ning sõltub isiklikust huvist või vajadusest digipädevusi arendada, või on see riigi vastutus ning vajab regulatiivset tuge, või peaks hoopis üleilmsed tehnoloogiaettevõtted varasemast rohkem oma platvormide läbi teostatavat informatsioonilist mõjustamist kontrollima? Ka grupiintervjuus osalenud ekspertide mõttekäikudes võis kohati märgata küberjulgeolekustamise tunnuseid, sest kaasaegse infokeskkonna ja platvormipoliitika eksistentsiaalse ohuna kujutamisele pakuti lahendusena rohkem regulatsioone. Sarnast trendi on märgata ka rahvusvahelisel tasandil.

NATO ja Eesti osas on e-ohtude konstrueerimise juures nii strateegiliste eesmärkide sõnastamine kui ka ühiste vaenlaste – nt Hiina ja Venemaa – konstrueerimine enamjaolt sarnane. Nii NATO, Euroopa Liit kui ka Eesti on seadnud julgeoleku tagamise fookusesse heidutuse, mitte agressioonide läbi sõjalise võimekuse näitamine. Erisused tulevad isegi Balti riikide vahel sisse just prioriteetide seadmisel: kas info- ja meediapädevuste suurendamine ühiskonnas on vajalik eeskätt sellepärast, et infokeskkond ongi ohtlikult muutunud, või sellepärast et meil on kaks konkreetset riiki, mille valitsuste strateegia osa on informatsiooniline mõjustamine? Sõltuvalt

rõhuasetusest peaks erinema ka ennetamiseks kasutatud strateegiad – esimesel juhul võiks lahenduseks olla nt riigiasutuste, teadlaste ja valdkonna praktikute koosloomes välja töötatud universaalne digikursus, teisel juhul aga intensiivistunud psühholoogiline kaitse avalikus ruumis.

Näen jagatud ohtudes ka võimalusi e-Eesti brändi tugevdamiseks. Oleme end juba rahvusvahelisel areenil positsioneerinud esimese digiriigi ambitsioonide ja välja töötatud e-teenustega maana, seega on loogiline ka tulevikus rõhuda sellele, et Eesti on juba läbinud õppetunde, mida e-teenuseid alles arendav avalik sektor teistes riikides ei pruugi olla ette näinud. Avaliku diplomaatia osaks võiks taas saada narratiiv Eestist kui edukast, arukast ja hästi kaitstud digiriigist – see on kooskõlas ka praeguse Reformierakonna ja Keskerakonna 2021. a alguses sõlmitud koalitsioonilepinguga, mis sätestab et „oleme Euroopa Liidus eestvedajad väärinfo ja avaliku inforuumi manipuleerimise vastases võitluses“.

Kaasaegse infokeskkondade ohtude teadvustamine on vajalik, aga tuleb leida tasakaal liigse hirmutamise ja ohu vähesest tajumisest tingitud tegevusetuse vahel. Narratiiv sellest, kuidas seisame e-ohtude näol silmitsi vääramatu jõuga, nõrgestab Eesti ja NATO heidutust ja ka kodanike tahet kanda avara riigikaitse käsituses ette nähtud võrdlemisi proaktiivset rolli infojulgeoleku tagamises. Vajadus lähenemist muuta ning küberkuritegevuse kõrval ka infokorratuse ennetamist või valenarratiivide leviku vastu võitlemist julgeoleku tagamise osana mõtestada ei tähenda, et senine lähenemine on tingimata olnud vale. Rahvusvaheline kogukond on pärast infooperatsioonide abil valimistesse sekkumist ning ka koroonaviiruse levikuga käsikäes käinud nn infodeemiat neist ohtudest varasemast teadlikum. Oleme infojulgeoleku mõtestamisel uues arengujärgus ning vastavalt sellele on vaja kohandada ka strateegilist vastupanuvõime tõstmist.

5.4 Soovitused edasisteks uuringuteks

Uuring tõstatas mitmeid huvitavaid küsimusi. Madisson ja Ventsel (2020) kasutasid oma analüüsimudelit vandenõuteooriatel, sest üheks Eco (2005) mudelautori kontseptsiooni poliitikanarratiivide teooriaga sidumise kasuteguriks ongi lisaks narratiivi autorile ka sotsiaalmeedias infot võimendavate tegutsejate kaasamise võimalus. E-ohtudega seotud narratiivide diskursiivset ülekannet sotsiaalmeediasse tasub uurida. Huvitav oleks kvantitatiivne

uuring, kus võrreldakse uudisajakirjandusest narratiivide üle kandumist erinevatesse sotsiaalmeedia kanalitesse, et teada saada, millisel rindel järgmine võitlus oodata võib. Tahaksin teada, kuidas toimib narratiivide ülekanne nt Facebookis tekstilisel kujul levivatest narratiividest Instagrammi või TikTokki meemide või audiovisuaalsete klippidena. Kas narratiivi fragmendid ja alustalad säilivad või muutub koos formaadiga ka tõlgendus?

Teine uurimissuund seostub Eesti digiriigi kuvandiga. Kas käesolevas peatükis tehtud järeldus, et e-tiigri kuvand on välismaal tugevam kui siseriiklikult, vastab tõele? Kas enesekriitika on kandunud ka liitlaste ja välispartnerite suhtumisse? Kuidas leida tee tagasi küberoptimistliku diskursuseni? Mida hindavad e-riigi tugevustena välispartnerid, mida Eesti elanikud? Analüüsimeetodina sobiks siia nii kodumaiste ja välismaiste meediatekstide juhtumiülene analüüs kui ka ekspertintervjuude tegemine. Tulemused panustaksid terviklikumasse Eesti brändiloomesse ning aitaksid mõista kahe kümnendi jooksul muutunud suhtumise tagamaid.

Uurimist vajaks ka see, kuidas saavutada tasakaal psühholoogilise kaitse ja vaenulike narratiivide leviku piiramise, konstruktiivse kriitika ja vaenulike jõudude agenda toetamise vahel. Selleks peaks analüüsima riigipoolset kommunikatsiooni ning võrdlema seda vaenulike narratiivide esile kerkimisega või koguma individuaal- või grupiintervjuude abil sisendit valdkonna ekspertidelt. See aitaks avaliku ruumi arutelukultuuri kooskõlla viia avara riigikaitse käsitusega.

Kiiresti vajaks tähelepanu ka küsimus sellest, kuidas ühiskonna vastupanuvõimet tõsta ilma e-ohte eksistentsiaalseks paisutamata. Nii riiklikes ja rahvusvahelistes strateegiates kui ka teaduskirjanduses pakutakse valeinfo leviku tõkestamise lahenduseks interdistsiplinaarset lähenemist, mille keskmes peaks olema indiviidide pädevuste arendamine. Aga kus läheb piir võimestamise ja hirmutamise vahel? Mina uuriksin seda nt induktiivselt välja töötatud koolitusprogrammi ning kahe kontrollgrupiga – ühe puhul kasutataksin võimestavat didaktikat, teisega klassikalisemat erakordsel juhtumil põhinevat probleemianalüüsi. Mõlemate gruppide teadmisi võiks standardiseeritud testiga koolituse alguses ja lõpus mõõta, et seejärel järeldusi teha. Praktiliseks väljundiks võiks olla võimestav info-, meedia- ja digipädevuste arendamise raamistik.

KOKKUVÕTE

Magistritöö eesmärgiks oli näidata, kuidas konstrueeritakse Eesti ja NATO küberkaitse võimekust Eesti ajakirjandusväljaannetes. Tahtsin teada, millised on meediatekstides esitatud temaatilised narratiivid, kuidas kujutatakse tegelasi ja tegevusi ning milliste narratiivide puhul on näha julgeolekustamise tunnuseid. Selleks kogusin Station.ee monitooringutööriista abil eelnevalt paika pandud märksõnu kasutades artikleid, mis ilmusid Eesti uudisajakirjanduses kahe küberkaitse võimekuse seisukohast olulise sündmuse eel, ajal ja järel ajavahemikus 01.11.2020 – 31.03.2021. Valimi kitsendamise järel analüüsisin lõpuks 109-t temaatilist artiklit erinevatest väljaannetest, mida kodeerisin MaxQda tarkvaraga. Välja joonistus 11 narratiivi:

1. Infosõda on Venemaa puhul eriti ohtlik, sest see on sõjalise agressiooni eelmäng.
2. Lääs on Vene propagandamasina töö osas paranoiline.
3. Venemaa infooperatsioonid on paljusid veennud, et Sputnik on ainus turvaline vaktsiin.
4. Hiina kasutab spionaaži, manipulatsiooni ja majanduslikku jõudu inimõiguste rikkumise kriitika vältimiseks.
5. Tehnoloogia eelisarendamine teeb Hiinast ohtliku suurvõimu.
6. Hiina eesmärk on partei autoritaarseid väärtusi eksportida ja rahvusvahelisel areenil realiseerida.
7. Eesti on e-riigina läbi kukkunud, sest pandeemia ajal ei ole piisavalt e-lahendusi kasutatud.
8. Eestis pole poliitilist tahet infojulgeolekut rahuldavalt koordineerida.
9. Küberruumis küpsevad radikaalid, et minna füüsilisse maailma kaost külvama.
10. Infokeskkond on spionaaži ja riigi süsteemide ründe lihtsaks ning kurjategijad raskesti tabatavaks teinud.
11. NATO ei ole suutnud uue strateegilise keskkonnaga piisavalt kohaneda.

Narratiivid esinevad meediatekstides hajusalt ja läbi põimunult, mistõttu on narratiivianalüüs, nagu sageli ikka, mingi piirini subjektiivne ja sõltub uurija tõlgendustest. Selle riski maandamiseks soovisin lisaks teada saada, kuidas hindavad valdkonna eksperdid välja joonistunud narratiive – on need uued või varasemate narratiivide edasiarendused, milline tegutseja võiks levikust kasu lõigata ning kas narratiivid on mõjusad või mitte. Selleks viisin

Zoomi vahendusel läbi ka fookusgrupi kuue eksperdiga, kes töötavad Riigikantseleis, Kaitsepolitseis, NATO StratComis, Riigi Infosüsteemi Ametis, Propastopis ning Kaitseväe Akadeemias.

Selgus, et ehkki mitmed narratiivid on varasemate vaenulike narratiivide edasiarendused, ei ole ka nt Eesti-kriitiliste narratiivide autoriks tingimata vaenulikud jõud, vaid ka konstruktiivne kriitika. E-tiigrit kritiseerivad narratiivid teeb mõjusaks siseriiklik digiriigi kuvandi nõrgenemine – liitlased ja välispartnerid toovad meid pigem eduloona esile, samas kui eestlased on enesekriitika maailmameistrid. Kui kriitikat võetakse adekvaatselt vastu ja sellele reageeritakse arendustegevusega, on see kasulik. Kui see mõjub heidutavalt ning viib käega löömiseni, siis enam mitte. Sarnaselt ei näinud grupiintervjuus eksperdid e-ohtude eksistentsiaalsena kujutamist tingimata murekohana, sest see manitseb ka ettevaatlikkusele.

Magistritöö tulemused tõstatavad küsimuse sellest, kuidas tehnoloogilise võimekusest avalikus ruumis kõneleda valdkonda eksistentsiaalse ohuna kujutamata. E-ohtude konstrueerimine igapäevase digivahendite kasutamisega kaasneva riskina, mille osas ei saa IKT-valdkonnast kauge inimene midagi ette võtta, on ohtlik; ehk isegi ohtlikum kui kõnealused e-ohud ise, sest see võib viia jõuetuse ja alla andmiseni. Järgnevates uuringutes võiks süvitsi vaadata seda, kuidas õpetada info-, meedia ja digipädevusi *võimestavalt* ning tõsta ühiskonna vastupanuvõimet elanikke hirmutamata.

Selle magistritöö valmimist on toetanud teadusprojekt SHVFI19127 "Strateegiline narratiiv julgeolekudilemma kujundajana".

Summary

The aim of this Master's thesis was to demonstrate how Estonia and NATO's cyber defence capability is constructed through narratives found in Estonian online media publications. I wanted to outline the thematic narratives, how the characters and activities are portrayed, and which narratives featured signs of securitization. To this end, I searched for articles, which had appeared in the Estonian news press before, during and after two cyber security incidents between 01.11.2020 and 31.03.2021, with predetermined keywords by using the Station.ee media monitoring tool. After constricting the sample, I analysed 109 thematic articles from various publications that I coded with MaxQda software. 11 narratives were outlined in the media texts:

1. The information war is particularly dangerous in Russia's case, as it is a precursor of military aggression.
2. The West is overly paranoid about Russia's propaganda machine.
3. Russia's information operations have convinced many that Sputnik is the only safe vaccine.
4. China uses spying, manipulation and economic power to avoid criticism on human rights violations.
5. The advancement of technology makes China a dangerous superpower.
6. China aims to export and realise the party's authoritarian values on the international stage.
7. Estonia has failed as an e-state, because not enough e-solutions have been used during the pandemic.
8. There is no political will in Estonia to coordinate information security adequately.
9. Radicals develop in cyberspace and then go on to wreak havoc in the physical world.
10. The information environment has made spying and attacking national systems easy and catching criminals hard.
11. NATO has not been able to adequately adapt to the new strategic environment.

Narratives can be fragmented and intertwined in media texts, which is why narrative analysis is –

as is often the case – subjective to some degree and open to the researcher's interpretation. In order to mitigate this risk, I also wanted to know how experts in the defense field evaluate the narratives – whether they are new or developed from earlier narratives, which actors could benefit from their spread, and whether the narratives are effective or not. For this purpose, I also carried out a focus group with six experts working at the Chancellory of the State, The Estonian Internal Security Service, NATO StratCom, the Information System Authority, Propastop and the Estonian Military Academy.

It turned out that although several narratives are further developments of previous hostile narratives, then the Model author of narratives critical of Estonia, for example, is not necessarily a hostile force, but could just stem from constructive criticism. Narratives that criticise e-Estonia can be influential as the image of Estonia as the digital state has tarnished within – eventhough allies and foreign partners highlight us as a success story, whilst Estonians could be the world champions of self-criticism. If criticism is adequately received and responded to by developing further, it is useful. If it makes people feel powerless and like giving up, then not so much. At the same time, experts in the group interview also highlighted, that painting e-risks as more dangerous than they are is not always a matter of concern, as it also encourages caution.

The results of the thesis raise the question of how to portray cyber defense threats in the public sphere without portraying it as existential threat. Constructing e-risks as something that comes with the territory of using technology on a daily basis, but is too complicated for anyone outside the ICT field, is dangerous; perhaps even more dangerous than the e-risks themselves, as it can lead to idleness and surrender. In following studies, one could look at how to teach media and information literacy in an *empowering* manner and increase the resilience of society without intimidating the inhabitants.

The completion of this Master's thesis has been supported by the research project SHVFI19127 "Strategic narrative as a designer of the security dilemma".

KASUTATUD KIRJANDUS

Agius, C. (2016). Social Constructivism. (Toim.) A. Collins, *Contemporary Security Studies*. Oxford University Press.

Allcott, H., Gentzkow, M., & Yu, C. (2019). Trends in the diffusion of misinformation on social media. *Research & Politics*, 6(2), 2053168019848554.

Almenar, E., Aran-Ramspott, S., Suau, J., ja Masip, P. (2021). Gender Differences in Tackling Fake News: Different Degrees of Concern, but Same Problems. *Media and Communication*, 9(1), 229-238.

Antoniades, A., Miskimmon, A., O'Loughlin, B. (2010). *Great power politics and strategic narratives*. Sussexi Ülikool, maailmapoliitika ja poliitökonoomika osakond.

Applegate, S. D. (2013). The dawn of kinetic cyber. *2013 5th international conference on cyber conflict (CYCON 2013),* 1-15. Kasutatud 02.05.21, https://ieeexplore.ieee.org/iel7/6560495/6568361/06568376.pdf

Bagrow, J. P., Liu, X., Mitchell, L. (2019). Information flow reveals prediction limits in online social activity. *Nature Human Behaviour*, 3, 122–128.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization'revisited: Theory and cases. *International Relations*, 30(4), 494-531.

Beltadze, G. (2018). Mark Voyger: Venemaa hübriidsõda võib veel üllatusi pakkuda. *Postimees*, 17. juuni. Kasutatud 18.03.21, https://arvamus.postimees.ee/4505728/mark-voyger-venemaa-hubriidsoda-voib-veel-ullatusi-pakkuda

Bergstrand, K., ja Jasper, J. M. (2018). Villains, victims, and heroes in character theory and affect control theory. *Social Psychology Quarterly*, 81(3), 228-247.

Bloor, M., Frankman, J., Thomas, M & Robson, K. (2001). *Focus groups in social research*. London: Sage.

Bolin, G., Jordan, P., Ståhlberg, P. (2016). From Nation Branding to Information Warfare: Management of Information in the Ukraine-Russia Conflict. *Media and the Ukraine Crisis: Hybrid Media Practices and Narratives of Conflict*, 3-18. New York: Peter Lang.

Buozis, M., ja Creech, B. (2018). Reading news as narrative: A genre approach to journalism studies. *Journalism Studies*, 19(10), 1430-1446.

Castells, M. (2009). *Communication Power.* Oxford: Oxford University Press.

Cinellia, M., Morales, G., Galeazzi, A., Quattrociocchi, W., Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9).

Coulter, C. A., ja Smith, M. L. (2009). The construction zone: Literary elements in narrative research. *Educational Researcher*, 38(8), 577–590.

Cronin, M. A., ja Weingart, L. R. (2007). Representational gaps, information processing, and conflict in functionally diverse teams. *Academy of management review*, 32(3), 761-773.

de Saint Laurent, C., Glăveanu, V. P., & Literat, I. (2021). Internet memes as partial stories: Identifying political narratives in coronavirus memes. *Social Media+ Society*, 7(1), 2056305121988932.

Deakin, H. & Wakefield, K. (2014). Skype interviewing: reflections of two PhD researchers. *Qualitative Research*, 14(5), 603-616.

Dent, C. (2008). 'Journalists are the confessors of the public', says one Foucauldian. *Journalism*, 9(2), 200–219.

Eco, U. (2005). *Lector in fabula.* Tartu: Tartu University Press.

Eesti julgeolekupoliitika alused. (2017). *Riigi Teataja*. Kasutatud 18.03.21, https://www.riigiteataja.ee/akt/306062017002

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) report*. Kasutatud 13.04.21 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Europol. (2021). Cyber Crime. *Europoli koduleheküIg*. Kasutatud 13.04.21, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Ferreira, R. R. (2021). Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content. *Journalism Practice*, 1-21.

Foucault, M. (2011). *Teadmine, võim, subjekt: valik räägitust ja kirjutatust*. Tallinn: Varrak.

Gabielkov, M., Ramachandran, A., Chaintreau, A., Legout, A. (2016). Social Clicks: What and Who Gets Read on Twitter? *ACM Sigmetrics konverentsi materjalid*, 13. aprill. Kasutatud 09.04.2021, https://hal.inria.fr/hal-01281190/document

Gad, U. P., & Petersen, K. L. (2011). Concepts of politics in securitization studies. *Security Dialogue*, 315-328.

Gering, M. (2015). Venemaa kaasmaalaste poliitika julgeolekustamine Kaitsepolitseiameti diskursuses. *Magistritöö*, Tartu Ülikool.

Guess, A., Nyhan, B., & Reifler, J. (2018). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign. *European Research Council*, 9(3), 4.

Halilov, I. (2015). Propagandistliku narratiivi muutumine konfliktsituatsioonis: Ukraina kriisi näitel. *Magistritöö*, Tartu Ülikool.

Hansen, L, Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4).

Hansson, S. (2015). Calculated Overcommunication: Strategic Uses of Prolixity, Irrelevance, and Repetition in Administrative Language. *Journal of Pragmatics*, 84, 172–188.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2), 49-60.

Hjarvard, S. (2008). The Mediatization of Society. A Theory of the Media as Agents of Social and Cultural Change. *Nordicom Review*, 29(2), 105-120.

Jansen, S. C. (2008). Designer Nations: Neo-liberal Nation Branding – Brand Estonia. *Social Identities*, 14(1), 121–142.

Jørgensen, K. E. (2010). *International Relations Theory. A New Introduction*. London: Palgrave Macmillan.

Joubish, M. F., Khurram, M. A, Ahmed, A., Fatima, S. T & Haider, K. (2011). Paradigms and Characteristics of a Good Qualitative Research. *World Applied Science Journal*, 12(11), 2082–2087.

Juurvee, I., Mattiisen, M. (2020). The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict. *Raport, Rahvusvaheliste Kaitseuuringute Keskus*. Kasutatud 07.04.21, https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf

Jõesaar, M. (2015). Balti riikide mainekujunduse tulemused: Eesti, Läti ja Leedu kuvandi võrdlus välismeedias. *Magistritöö*, Tartu Ülikool.

Kalmus, V. (2015). Diskursusanalüüs. *Sotsiaalse analüüsi meetodi ja metodoloogia andmebaas*. Kasutatud 11.04.21, https://sisu.ut.ee/samm/diskursusanalyys

Karlova, N. A. ja Fisher, K.E. (2013). "Plz RT": A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour. *Information Research*, 15. märts. Kasutatud 16.13.2021, https://www.hastac.org/sites/default/files/documents/karlova_12_isic_misdismodel.pdf

King, G., Pan, J., Roberts, M. (2016). *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*. Cambridge University Press. Kasutatud 13.04.21, http://gking.harvard.edu/files/gking/files/50c.pdf?m=1463587807

Klaassen, M. (2018). *Vale- ja võltsuudiste avaldamine peavoolumeedias: Eesti meediaväljaannete peatoimetajate selgitused tekkepõhjustele.* Bakalaureusetöö, Tartu Ülikool.

Koppel, K. (2017). Populism Eesti peavoolumeedias ja vastuavalikkuses. *Magistritöö*, Tallinna Ülikool.

Kreml. (2007). Speech and the Following Discussion at the Munich Conference on Security Policy. *Kremli koduleheküIg*. Kasutatud 30.05.21, http://en.kremlin.ru/events/president/transcripts/24034

Krueger, R. A. (2009). *Focus groups: a practical guide for applied research.* California: SAGE.

Kull, K., Lindström, K., Lotman, M., Magnus, R., Maimets, K., Maran, T., Moss, R. T., Pärli, Ü., Pärn, K., Randviir, A., Remm, T., Salupere, S., Sarapik, V., Sütiste, E., Torop, P., Ventsel, A., Verenitš, V., Väli, K. (2018). *Semiootika*. Tartu: Tartu Ülikooli Kirjastus.

Kumar, V., Rajan, B., Rajkumar, V., Lecinski, J. (2019). Understanding the Role of Artificial Intelligence in Personalized Engagement Marketing. *California Management Review*, vol 69 (4).

Kuusk, L. (2013). Kübersõja ja julgeoleku sõnavara semantiline analüüs. *Bakalaureusetöö*, Tartu Ülikool.

Küberturvalisuse strateegia 2019-2022. (2019). Majandus- ja Kommunikatsiooniministeerium. Kasutatud 05.04.21, https://www.mkm.ee/et/eesmargid-tegevused/arengukavad#kyber

Laclau, E. (2005). *On Populist Reason*. Verso: New York.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, 8(1), 100-115.

Laherand, M. (2012). *Kvalitatiivne uurimisviis*. Tallinn: Sulesepp.

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... ja Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094-1096.

Lepik, P. (2008). *Universals in the Context of Juri Lotman's Semiotics*. Tartu: Tartu Ülikooli Kirjastus.

Leukfeldt, E.R., Lavorgna, A. ja Kleemans, E.R. (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 23, 287–300.

Lewandowsky, S., Ecker, U., Seifert, C., Schwarz, N., Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest*, 13(3), 106–131.

Liive, R. (2020a). RIA: MKM ei kasutanud infoturbe osas parimaid praktikaid, algatasime järelevalvemenetluse. *Geenius*, 1. detsember. Kasutatud 08.04.21, https://digi.geenius.ee/rubriik/uudis/ria-mkm-ei-kasutanud-infoturbe-osas-parimaid-praktikaid-algatasime-jarelevalvemenetluse/

Liive, R. (2020b). Terviseametist lekkinud 9158 inimese isikuandmed olid krüpteerimata. Geenius, 3. detsember. Kasutatud 08.04.21, https://digi.geenius.ee/rubriik/uudis/terviseametist-lekkinud-9158-inimese-isikuandmed-olid-krupteerimata/?nocache=1

Liive, R. (2021). Üle saja tuhande CityBee kliendi andmed lekkisid internetti. *Geenius*, 16. veebruar. Kasutatud 08.04.21, https://digi.geenius.ee/rubriik/uudis/ule-saja-tuhande-citybee-kliendi-andmed-lekkisid-internetti/

Listmann, K. (2014). Euroopa Liidu küberjulgeoleku strateegia rakendamine küberrünnakute korral Eesti kriitilise infrastruktuuri näitel. *Magistritöö*, Tartu Ülikool.

Madisson, M. (2016). Snowdeni skandaali kujutamine eesti meedias: hirmu ja ohtude konstrueerimine. *Acta Semiotica Estica*, XIII, 10−36.

Madisson, M., ja Ventsel, A. (2018). Fobofoobia: Küberohtude ja infosõja diskursused Zapad 2017 õppuste meediakajastuse kontekstis. *Sõjateadlane*, 8, 181−199.

Madisson, M., ja Ventsel, A. (2020). *Strategic Conspiracy Narratives: A Semiotic Approach.* Routledge.

Mattern, J. B. (2005). Why «Soft Power» Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics. *Millennium – Journal of International Studies*, 33, 583-612.

McCarthy, N. (2020). Cybercrime: Europe's Most ja Least Secure Countries. *Statista*, 21. veebruar. Kasutatud 03.04.21, https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/

McDermott, R. N. (2017). Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. *Raport, Rahvusvaheline kaitseuuringute keskus*. Kasutatud 05.04.21, http://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

Meyer, C.O., Strickmann, E., (2011). Solidifying constructivism: how material and ideational factors interact in European defence. *JCMS: journal of common market studies*, 49(1), 61-81.

Miró-Llinares, F., ja Aguerri, J. C. (2021). Misinformation about fake news: A systematic critical review of empirical studies on the phenomenon and its status as a 'threat'. *European Journal of Criminology,* 1477370821994059.

Miskimmon, A, O'Loughlin, B., Roselle, L. (2013). *Strategic Narratives, Communication Power and the New World Order.* New York: Routledge.

Miskimmon, A., O'Loughlin, B., Roselle, L. (2012*). Forging the World: Strategic Narratives and International Relations*. Londoni, Eloni ja Duke'i ülikool.

Murphy, D. (2008). *Fighting Back – New Media and Military Operations*. Center for Strategic Leadership, United States Army War College.

Murumaa-Mengel, M. (2020). Veebiintervjuud, projektiivtehnikad ja loovuurimismeetodid. S. Ratso (Toim.), *Kuidas mõista andmestunud maailma? Metodoloogiline teejuht,* (lk 707-739). Tallinn: TLÜ kirjastus.

Narits, H. (2017). NATO küberkaitsestrateegiad aastatel 2007-2015. *Bakalaureusetöö*, Tartu Ülikool.

Narits, T. (2015). Psühholoogiline kaitse Eesti julgeolekupoliitika kujundajate käsitluses. *Magistritöö*, Sisekaitseakadeemia.

Newman, N., Fletcher, R., Schulz, A., Andı, S., Nielsen, R. K. (2020). *Reuters Institute Digital News Report 2020*. Kasutatud 03.04.21, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf

Nissen, T. E. (2015). *Sotsiaalmeedia kasutamine relvasüsteemina*. Tänapäeva konfliktide omadused. Riigikaitse raamatukogu, Tallinn.

North Atlantic Treaty Organization. (2014). Wales summit declaration. *North Atlantic Treaty Organizationi koduleheküIg*. Kasutatud 28.04.21, https://www.nato.int/cps/en/natohq/official_texts_112964.htm

North Atlantic Treaty Organization. (2015). Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar. *North Atlantic Treaty Organizationi koduleheküIg*. Kasutatud 28.05.21, https://www.nato.int/cps/en/natohq/opinions_118435.htm

Nye, J. Jr. (1990). *Bound to Lead: The Changing Nature of American Power*. New York: Basic Books.

Nye, J. Jr. (2004). *Soft Power: The Means to Success in World Politics.*

Nye, J. Jr. (2011). *The Future of Power*. New York: Public Affairs.

Obiała, J., Obiała, K., Mańczak, M., Owoc, J., & Olszewski, R. (2021). COVID-19 misinformation: Accuracy of articles about coronavirus prevention mostly shared on social media. *Health Policy and Technology*, 10(1), 182-186.

Oksaar, K. (2014). Küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi Eesti Vabariigi diskursuse näitel. *Magistritöö*, Tartu Ülikool.

Onno, K. (2019). Baltimaade kujutamine lääne veebimeedias Zapad-2017 kontekstis: õppetunnid strateegilise kommunikatsiooni seisukohalt. *Magistritöö*, Sisekaitseakadeemia.

Orav, A. (2021). Rapla põhikooli õpilane korraldas oma koolile küberrünnaku. *Eesti Päevaleht*, 14. aprill. Kasutatud 14.04.21, https://epl.delfi.ee/artikkel/93124255/rapla-pohikooli-opilane-korraldas-oma-koolile-kuberrunnaku

Paas, K. (2021). Eesti riikliku julgeoleku kommunikatsiooni võimalused vaenulike inforünnakute mõju leevendamiseks infosõjas. *Magistritöö*, Sisekaitseakadeemia.

Pamment, J., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A. (2018*). Countering Information Influence Activities: The State of the Art.* Raport, Lundi Ülikool.

Poom, R. (2021). Tšehhi saadik: Vene luure seotus laskemoonalao plahvatusega šokeeris kogu maad. *Eesti Päevaleht*, 22. aprill. Kasutatud 04.04.2021, https://epl.delfi.ee/artikkel/93201867/tsehhi-saadik-vene-luure-seotus-laskemoonalao-plahvatusega-sokeeris-kogu-maad

Punthong, W. (2018). A Poststructuralist Approach to Strategic Culture: Estonia's Strategic Response to Russia's Hybrid Threat. *Magistritöö*, Tartu Ülikool.

Puumeister, O. (2018). On Biopolitical Subjectivity: Michel Foucault's perspective on biopolitics and its semiotic aspects. *Doktoritöö*, Tartu Ülikool.

Puumeister, O. (2020). Konspiratiivne ratsionaalsus – vandenõuteooriad poliitikas. *Sirp*, 23. oktoober. Kasutatud 10.03.2021, https://www.sirp.ee/s1-artiklid/c9-sotsiaalia/konspiratiivne-ratsionaalsus-vandenouteooriad-poliitikas/

Reisigl, M. (2008). *Analyzing political rhetoric*. In Koller, V., & Wodak, R. (Ed.) Handbook of Communication in the Public Sphere. Berlin: De Gruyter Mouton.

Roselle, L., Miskimmon, A., O'Loughlin, B. (2014). Strategic narrative: A new means to understand soft power. *Media, War & Conflict*, (7)1, 70-84.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2), 53-74.

Schmitt, M. N. (2015). The law of cyber targeting. *Naval War College Review*, 68(2), 10-29.

Selg, P., Ventsel. A: (2008). Towards a Semiotic Theory of Hegemony: Naming as Hegemonic Operation in Lotman and Laclau. *Sign Systems Studies,* 36(1), 167–183.

Siik, I. (2018). Kuidas konstrueeriti Eesti ajakirjanduses Venemaa sõjalist õppust Zapad 2017? *Magistritöö*, Tartu Ülikool.

Silverman, C. (2015). LIES, DAMN LIES, AND VIRAL CONTENT - How news websites spread (and debunk) online rumors, unverified claims and misinformation. *Columbia Journalism School Tow Center*.

Spindler, M. (2013). Social constructivist theory. Rmt: International Relations. *A Self-Study Guide to Theory*. Toronto: Barbara Budrich Publishers.

Synytsina, K. (2018). The Construction of the Image of Ukraine as the Other in Russian Media. *Magistritöö*, Tartu Ülikool.

Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., & Choi, Y. (2019). Defending against neural fake news. *arXiv preprint arXiv:1905.12616*. Kasutatud 21.04.2021, https://arxiv.org/pdf/1905.12616

Tamm, P. (2018). Kuidas konstrueeritakse Eesti ajakirjanduses Venemaa sõjalist võimekust? *Magistritöö*, Tartu Ülikool.

Tammpuu, P., Masso, A. (2018). 'Welcome to the Virtual State': The Estonian e-residency and Digitalised State as a Commodity. *European Journal of Cultural Studies*, 21(5), 543–560.

Waever, O. (1995). *Securitization and Desecuritization. On Security*. New York: Columbia University Press.

Wardle, C. (2019). Understanding Information Disorder. *Raport*, First Draft.

Wardle, C., Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Raport*, Council of Europe.

Waszak, P. M., Kasprzycka-Waszak, W., & Kubanek, A. (2018). The spread of medical fake news in social media–the pilot quantitative study. *Health policy and technology*, 7(2), 115-118.

Weedon, J., Nuland, W., Stamos, A. (2017). Information Operations and Facebook. *Facebook Inc.,* 27. aprill. Kasutatud 20.04.2021, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International Organization*, 46, 391-425.

Ventsel, A. (2018). Semiotics of threats: Discourse on the vulnerability of the Estonian identity card. *Sign Systems Studies* 47(1/2), 126–151.

Ventsel, A., Hansson, S., Madisson, M., Sazonov, V. (2018). Hirmu mehhanismid strateegilistes narratiivides õppuse Zapad 2017 näitel. *Sõjateadlane*, 8, 103-127.

Wiederhold, B. K. (2020). Connecting through technology during the coronavirus disease 2019 pandemic: Avoiding “Zoom Fatigue”. *Cyberpsychology, behavior and social networking*, 23(7), 437–438.

Winnerstig, M. (toim). (2014). *Tools of Destabilization. Russian Soft Power and Non-military Inlfuence in the Baltic States*. Raport FOI-R-3900-SE.

Voltri, J. (2021). Comparison of Governmental Approaches to Counter Russian Information Influence in the Baltic States. *Magistritöö*, Tartu Ülikool.

Vu, H.T., Guo, L. ja McCombs, M.E. (2014). Exploring "the World Outside and the Pictures in our Heads": A Network Agenda Setting Study. *Journalism & Mass Communication Quarterly*, 91, 669-686.

Wu, T. (2019). Blind Spot: the Attention Economy and the Law. *Antitrust Law Journal,* 3(82), 771-806.

LISAD

Lisa 1 – Analüüsitud artiklite täisloend

		Märksõna: **andmeleke**		
1	BNS	RIA: veebruaris oli kaks juhtumit, mis sarnanesid ministeeriumide küberründega	Postimees	25.03.21
2	Aas, Krista; Gross, Oskar	Andmed on digitaalse maailma DNA	Postimees	11.03.21
3	Mägi, Kristjan Ats	Kõikide andmelekete ema: häkkerid postitasid veebi 3 miljardi kasutaja paroolid	Geenius	15.02.21
4	Randlo, Toomas	Andmeleke paljastab: Hannes Võrno saade aitas MMSi müüki suurendada	Postimees	10.02.21
5	Kartau, Aare	ANDMELEKE: Hiina kommunistliku partei liikmed tegutsevad lääneriikide ettevõtetes ja saatkondades	Õhtuleht	14.12.20
6	Liive, Ronald	Suur isikuandmete leke ei too terviseametile trahvi kaela	Geenius	04.12.20
7	Liive, Ronald	Koroonapositiivsete andmed lekkisid LimeSurvey teenusest, terviseamet lõpetas selle kasutamise	Geenius	02.12.20
8	Truu, Joosep	Küberkuritegevus on epideemia: 2020. aasta levinumad petuskeemid	Delfi	02.12.20
9	Saarpuu, Kuido	Oktoober Eesti küberruumis: Emoteti pahavara levik pole raugenud	Järva Teataja	26.11.20
		Märksõna: **julgeolekuoht**		
10	Kivil, Karl	USA valitsus: lääs peab lubama islamistide perekondadel naasta kodumaale	ERR	31.03.21
11		Raport: Vene tehnoloogial töötavad Saksa allveelaevad on julgeolekuoht	Postimees	29.03.21
12	Kannik, Indrek	Indrek Kannik: traditsioonilised ohud ei ole maailmast kuhugi kadunud	ERR	23.03.21
13	Hõbepappel, Urmas	Hiinat kannustavad partei ülemvõimule allutatud ideaalid	Ekspress	17.03.21
14	Orav, Anna Teele	FOTOD ja VIDEO | Gao sõjaväebaasis asuv Eesti rahvusliku toetuselemendi tööala sai nimeks Kratt	Delfi	12.03.21
15	Sepp, Andres	Vene laevad meie vetes "tormivarjus": kas julgeolekuoht või näeme sääses elevanti?	Saarte Hääl	06.03.21
16	Tähismaa, Inno	Gao sõjaväebaasis tähistati Eesti Vabariigi aastapäeva	Lõunaeestlane	25.02.21
17		Rootsi tehnoloogiakonsultanti süüdistatakse Venemaa heaks luuramises	Postimees	22.02.21
18	Voog, Viljar	VÄLISLUURE AASTARAAMAT | Hiina kogub ajusid – mitte koostöötahtest, vaid enda huvides	Õhtuleht	17.02.21
19	Seeder, Helir-Valdor	Isamaa kaks aastat valitsuses	Järva Teataja	16.02.21
20	Nuka, Berit	Kanada pani USA paremäärmuslased ISISega samale pulgale	Postimees	05.02.21
21	Laine, Martin	Jooksku Eestis! Rootsi kaitsepolitsei näeb noores Eesti neonatsis julgeolekuohtu ja pagendab ta kodumaale	Ekspress	03.02.21
22	Ots, Mait	Biden kinnitas Merkelile soovi kahe riigi suhteid parandada	ERR	26.01.21
23		Läheduses puhkenud põleng põhjustas USA Kapitooliumis häireolukorra	Postimees	18.01.21
24	Pau, Aivar	Siemi viimaseid otsuseid: kuulutati välja hange e-valimiste turvalisuse auditeerimiseks	Delfi	14.01.21

25	Lensment, Jaanus	FOTOD | Malis teenivatel Eesti sõduritel käis jõuluvana	Delfi	24.12.20
26	Heikla, Alar	Alar Heikla: Huawei vajab aega, et tõestada oma süütust	Eesti Päevaleht	21.12.20
27	Soidro, Mart	Malepartii, mis ei lõpe viigiga	Õhtuleht	18.12.20
28	Nuka, Berit	Bulgaaria rahvuslik jonn hoiab Põhja-Makedooniat ELi ooteruumis	Postimees	11.12.20
29	Ots, Mait	Raport: NATO peaks oma fookust laiendama	ERR	02.12.20
30		Kaitseminister Luik vestles oma Briti kolleegi Wallace'iga	Delfi	26.11.20
31	Marmei, Eerik	Vaba maailm tõmbetuultes	Postimees	14.11.20
32		EL nõuab Hiinalt Hongkongi parlamenti puudutavate reeglite tühistamist	Postimees	12.11.20
33	Põld, Anna	Helmete retoorika läks vastuollu koalitsioonileppesse raiutuga	Postimees	09.11.20
34	Mihkelson, Marko	Marko Mihkelson: Eesti-USA suhted Joe Bideni võidu järel	ERR	07.11.20
35	Salu, Mikk	EKSKLUSIIVINTERVJUU | Valge Maja endine hall kardinal Steve Bannon: Trump võidab, Bideni toetajad hakkavad märatsema	Ekspress	04.11.20
		Märksõna: **häkker**		
36		Midagi igale maitsele: 12 parimat filmi, mida sel nädalal telekast tasuta vaadata	Postimees	30.03.21
37	Randlo, Toomas	Hiina ja Vene häkkerid ründasid mullu Euroopa ravimiametit	Postimees	08.03.21
38	Randlo, Toomas	Häkker varastas paremäärmuslaste suhtlusvõrgustikust tuhandete kasutajate andmed	Postimees	02.03.21
39	Randlo, Toomas	Floridas üritas häkker joogivett mürgitada. Kas selline asi võib juhtuda ka Eestis?	Postimees	16.02.21
40	Ojamets, Indrek	Saaremaa firma sai imekombel Rumeenia kelmidelt raha tagasi	Postimees	23.01.21
41		Häkkerid panid internetti üles Pfizeri koroonavaktsiini salastatud dokumendid	Postimees	14.01.21
42	Kalev, Matthias	Häkkeri raske argipäev: pereisa üritas varastatud andmetega rikkaks saada, aga jäi vahele	Ekspress	11.11.20
		Märksõna: **kübersõda**		
43	Laugen, Lauri	Venemaa kaitseministri nõunik: Lääs on alustanud Venemaa vastu mentaalset sõda venemaalaste eneseteadvuse hävitamiseks	Delfi	25.03.21
44	Paas, Kadri	Vaenlasele kasulikuks idioodiks võib saada igaüks	Postimees	15.03.21
		Märksõna: **infosõda**		
45		Telia vaatamissoovitused: suurepärased näitlejad ja palju fantaasiat!	Delfi	30.03.21
46	Laanet, Kalle	KALLE LAANET ⟩ Mere- ja õhukaitse tugevamaks!	Saarte Hääl	20.03.21
47	Laanet, Kalle	Kalle Laanet: heidutus Venemaa suunal toimib - muidu oleks ju konflikt juba puhkenud	Eesti Päevaleht	17.03.21
48	Harju, Ülle	Infosõjas sobivad kõik relvad	Postimees	11.03.21
49	Guzun, Victor	Sõda Nistru jõel Moldova Vabariigi vastu – Venemaa Föderatsiooni esimene hübriidsõda	Postimees	04.03.21
50	Kivil, Karl	Macron: lähikuudel Prantsusmaa kohalolekut Sahelis ei vähendata	ERR	16.02.21
51	Levin, Adik	Vaktsineerimine Ukraina moodi	Õhtuleht	10.02.21
52	Tali, Piret	Karmen Joller netitrolle ei karda: eks sõimama hakatakse siis, kui argumendid on otsa saanud	Õhtuleht	03.02.21
53	Roonemaa, Holger	Teolt tabatud: kõrge Vene diplomaat sai salaja juba teise COVID-i vaktsiini. Haigla alustas siseuurimist	Eesti Päevaleht	28.01.21

54	Liinat, Laura	Testime „Ole valmis!" äppi – milleks see täpselt valmistuda aitab?	Õhtuleht	05.01.21
55	Toom, Yana	POLIITKOLUMNIST | Yana Toom: infosõda Ida-Virumaaga – kellele küll on vaja kujutada üht Eesti piirkonda zombidena?	Eesti Päevaleht	19.12.21
56	Kartau, Mari	Mari Kartau: mis oleks, kui kaotaks seadustest üldse soo mõiste?	Eesti Päevaleht	15.12.21
57	Levin, Adik	Laseksin end esimesel võimalusel vaktsineerida	Õhtuleht	08.12.21
58	Minnik, Taavi	Intervjuu Ratase valitsuse stratkomi juhiga: „me oleme apoliitilised, demoniseerimise talumine käib meil palga sisse!"	Delfi	12.11.21
59	Maasikamäe, Sirje	Kulutulena levivadk kuulujutud: kui midagi pekki läheb, kirjutatakse surma põhjuseks koroona! Seda pole olemaski!	Õhtuleht	10.11.21
60	Tõnsing, Triin	MILITAARTURISMI PÄRLEID | Albaania — tohutus koguses punkreid ja Ameerika lennuki saladus	Delfi	04.11.21
		Märksõna: **inforünnak**		
61	Kunnus, Mihkel	Infosõda käib koroonast Kremlini	Postimees	15.03.21
62	Laugen, Lauri	Leedu luure: Venemaa saatis inforünnaku korraldamiseks Vilniusse „Putini koka" Prigožini teisiku	Delfi	04.03.21
63	Himma, Marju	Marju Himma: kõneisikud vajavad kaitset avalike inforünnakute eest	ERR	01.02.21
		Märksõna: **infooperatsioon**		
64	Stoicescu, Kalev	Kalev Stoicescu: Sputnik V kui geopoliitiline relv	Postimees	22.03.21
65	Laine, Martin	KUULA SAADET | Kuidas FBI poolt tagaotsitav oligarh Eesti ja Läti riigimehed enda pilli järgi tantsima pani	Eesti Päevaleht	04.03.21
66	Sester, Sven	Sven Sesteri 10 soovitust uuele valitsusele: ka algaja juht peab julgema otsustada ehk kuidas lõpetada kaos vaktsineerimises	Eesti Päevaleht	24.02.21
67	Joakit, Ekvard	PÄEVAKOMMENTAAR | Ekvard Joakit: Kallas, Helme ja Kõlvart - kätest kinni ja üheskoos vaktsineerima!	Eesti Päevaleht	15.02.21
68	Viin, Ronald	Ronald Viin: tulgem äärmuslikest ja kallutatud inforuumidest välja	Eesti Päevaleht	28.01.21
69	Vest, Mariliis	Kehtna KHK ja kaitsevägi ühitasid õppe ajateenistusega	Raplamaa Sõnumid	30.12.20
70	Ventsel, Aimar	Aimar Ventsel: iga nimekiri pole see õige nimekiri	ERR	27.12.20
71		IT-õppurid saavad ajateenistuses läbida praktika	Delfi	21.12.20
		Märksõna: **küberkaitse**		
72	Hurt, Martin; Sõmer, Tiia	Küberajateenistus kogub populaarsust	Postimees	18.03.21
73	Punamäe, Sander	Endine kaitseväe juhataja ja riigikogu liige Johannes Kert saadeti viimsele teekonnale	Postimees	14.03.21
74	Kaldoja, Evelin	Kindral Lanata: koroonakriis on kõiki ohte vaid hullemaks teinud	Postimees	12.03.21
75		Riigimees selle sõna kõige austavamas mõttes	Postimees	06.03.21
76	Koort, Erkki	Erkki Koort: vabariigi aastapäeva paraad ei jäänud ära	Postimees	25.02.21
77		Kelmid saadavad tehnikaülikooli rektori nime alt petukirju	Postimees	18.02.21
78		Tallinnast juhitakse üle-euroopalist küberkaitseõppust	Postimees	18.02.21
79	Tähismaa, Inno	Eesti e-eluviisi nähtamatud kaitsjad jõudsid kõurikuikka	Lõunaeestlane	28.01.21
80	Vilo, Jaak	Jaak Vilo: teadusrahastus uute reformide ootel	ERR	10.01.21
81	Randlaid, Sven	Eesti ja USA viisid läbi ühise küberoperatsiooni	Postimees	03.12.20
82	Laikoja, Linda-Liis	Karl-Erik Taukar asutas tuntud küberfirmaga uue äri	Geenius	27.11.20

83		Tehnikaülikooli teadusprorektor valiti Euroopa Komisjoni peateadusnõustajaks	Geenius	24.11.20
84		Eesti firma ehitab Luksemburgi küberharjutusväljaku	Postimees	20.11.20
85		Eesti ettevõtted sõlmisid lepingu Euroopa Kosmoseagentuuriga	Postimees	19.11.20
86		Eestlane, kes hakkab Euroopa suurimaid otsustajaid nõustama: COVIDi tagajärgi näeme me veel väga kaua	Geenius	18.11.20
87	Riives, Armas	Küberkaitsespetsialist Hans Lõugas: internetis peab mõtlema nagu häkker	Tartu Postimees	03.11.20
		Märksõna: **küberjulgeolek**		
88	Paavo, Vambola	Vambola Paavo: Elu õpetab valusalt	Pärnu Postimees	27.03.21
89	Pau, Aivar	Ilves ja Kaljurand: Eesti seis COVIDile mõeldud IT-lahendustega on katastrofaalne	Delfi	25.02.21
90	Liimets, Eva-Maria	Eva-Maria Liimets: Eestil tuleb vapralt enda eest seista	ERR	16.02.21
91		Bideni meeskond kavandab vastust Vene küberrünnakule	Õhtuleht	21.12.20
92	Randlaid, Sven	Küberjulgeolek, 5G ja Navalnõi: välisminister Reinsalu arutas USA kolleegiga rahvusvahelist olukorda	Postimees	21.12.20
		Märksõna: **desinformatsioon**		
93	Ratt, Silja	Valeuudiste pealetung proovib inimeste kriitikameelt	Järva Teataja	30.03.21
94	Kaldoja, Evelyn	ELi sanktsioonid vihastasid Hiinat	Postimees	24.03.21
95		USA taunis Venemaa desinformatsioonikampaaniat vaktsiinide osas	Postimees	09.03.21
96	Laugen, Lauri	WSJ: USA luure usub, et Venemaa levitab Pfizeri vaktsiini kohta kahtlusi, et upitada oma Sputnikut	Delfi	08.03.21
97	Samorodni, Oleg	VENE MEEDIA PÄEVIK | Miks on Maardus ja Lasnamäel nii kõrged nakatumisnäitajad? Vastust võib otsida EKRE sümbioosist Kremli-TV-ga	Eesti Päevaleht	03.03.21
98		Läti keelab Vene telesaatejuhil Vladimir Solovjovil riiki siseneda	Postimees	18.02.21
99	Oja, Tõnis	Vene meedia promob välismaal oma vaktsiini ja mustavad USA toodangut	Postimees	08.02.21
100	Laugen, Lauri	EL-i välispoliitikajuht Borrell ei lubanud Moskvas uusi sanktsioone, küll aga kiitis Vene koroonavaktsiini	Delfi	05.02.21
101		Juhtkiri: WHO rasked ülesanded	Postimees	30.01.21
102	Kull, Clyde	Clyde Kull, Eric Lamouroux: sada aastat diplomaatilist koostööd Prantsusmaaga	Postimees	26.01.21
103	Ruutsoo, Rein	Rein Ruutsoo: Mihhail Kõlvart kasutab koroonasegadust ära, et vene keel teiseks riigi keeleks teha	Eesti Päevaleht	14.01.21
104	Tsupsman, Oliver; Raudsik, Heliis	TOP 5 | Milliseid valesid jäid Eesti inimesed tänavu uskuma? Maskivalede ning ebaravi lubaduste õnge langeti ohtralt	Eesti Päevaleht	31.12.20
105		Leedu Delfi valedetektor nimetati Euroopa parimate faktikontrollide hulka	Delfi	17.12.20
106	Bregin, Aleksandr	YouTube kustutab Trumpi pooldajate videoid	Postimees	10.12.20
107		Twitter annab @POTUS konto Bidenile üle inauguratsioonipäeval	Postimees	21.11.20
108	Raestik, Triin	Karmen Joller: "Palun, raamatumüüjad ja reklaamikaupmehed: käivitage oma südametunnistus ja lõpetage inimeste valeinfoga mürgitamisele kaasaaitamine!"	Geenius	04.11.20
109	Korsten, Teet	Karina Orlova: sel korral on valimistel kaalukausil demokraatia ise	Postimees	03.11.20

Lisa 2 – Kutse fookusgruppi

Tere!

Korraldan grupivestluse osana oma magistritööst pealkirjaga „Eesti ja NATO küberkaitse võimekuse narratiivne konstrueerimine Eesti ajakirjandusväljaannetes“. Magistritöö esimeses etapis analüüsisin 109-t artiklit, mille põhjal joonistus välja nii strateegilisi narratiive kui ka meedianarratiive Eesti ja NATO küberkaitse võimekuse kohta.

Fookusgrupi eesmärgiks on neid narratiive üheskoos arutada ning ekspertteadmiste abiga laiemasse konteksti asetada. Nii saan tulemusi enne töö avaldamist kontrollida, mis tõstab selle praktilist väärtust.

Kasutegurid osalejatele:

1. Meeldiv (ja minu poolt põhjalikult ette valmistatud) reedehommikune **vestlus kolleegidega teistest asutustest psühholoogilise kaitse, strateegilise kommunikatsiooni, (küber-)julgeolekustamise ning informatsioonilise mõjustamise teemal.**
2. Vahetu teadmine mu magistritöö huvitavamatest tulemustest ilma, et peaks teadustöö läbi lugema.
3. Isiklik panus järelkasvu tekkimisse valdkonnas ja heas toonuses karma.

Kõik osalejad jäävad **anonüümseks** – ainus identifitseeriv tunnus on staaž valdkonnas (aastates), et anda lugejatele võimalus varinimega tähistatud allikate pädevust hinnata. Salvestan meie kohtumise transkribeerimise tarbeks ülikooli serverisse. Transkribeeritud materjali hakkan kohe pärast anonüümsuse tagamises veendumist analüüsima. Magistritöö kaitsmise järel 7. juunil 2021 kustutan salvestuse; transkriptsiooni ainus koopia jääb CD-plaadil koos töö originaaliga sotsiaalteaduste valdkonna raamatukokku.

Toon töös välja, mis asutustest arutelul esindajad on, ent ei seo asutusi konkreetse vastajaga. Loodan kaasata esindajaid:

- KAPOst,
- Välisluureametist,
- Kaitseministeeriumist,
- Riigikantseleist,
- RIAst,
- Balti Kaitsekolledžist ja/või Sisekaitseakadeemiast,
- Rahvusvahelisest Kaitseuuringute Keskusest,
- NATO STtratComist,
- Küberväejuhatusest ning
- NATO Küberkaitsekeskusest.

Toimumisaeg on **7. mail kell 10:00 - 11:45**, millest sisulist osa on poolteist tundi ning 15 minutit ajavaru. Nagu viimasel aastal kombeks, toimub grupivestlus veebis **Zoomi vahendusel**. Saadan kolm päeva enne kohtumist meeldetuletuse koos lingiga osalemiseks.

Teie võiksite omalt poolt arvestada, et viibite hea internetiühendusega paigas (WiFi võib kohati olla nõrgem kui nutitelefoni 4G), saate sisse lülitada oma kaamera (loodame laste ja koduloomadel taustal lustimist näha) ning kasutada võimalusel mikrofoniga kõrvaklappe.

Mitte mingisugust ettevalmistavat tööd vestlusele ei eelne ega järgne.

Tänan Teid juba ette, et leiate aega uuringu tulemusi oma kogemustepagasiga täiendada. Küsimuste korral olen olemas!

Lugupidamisega

Maia Klaassen
ajakirjanduse ja kommunikatsiooni magistrant

Lisa 3 – Fookusgrupi strateegiline kava

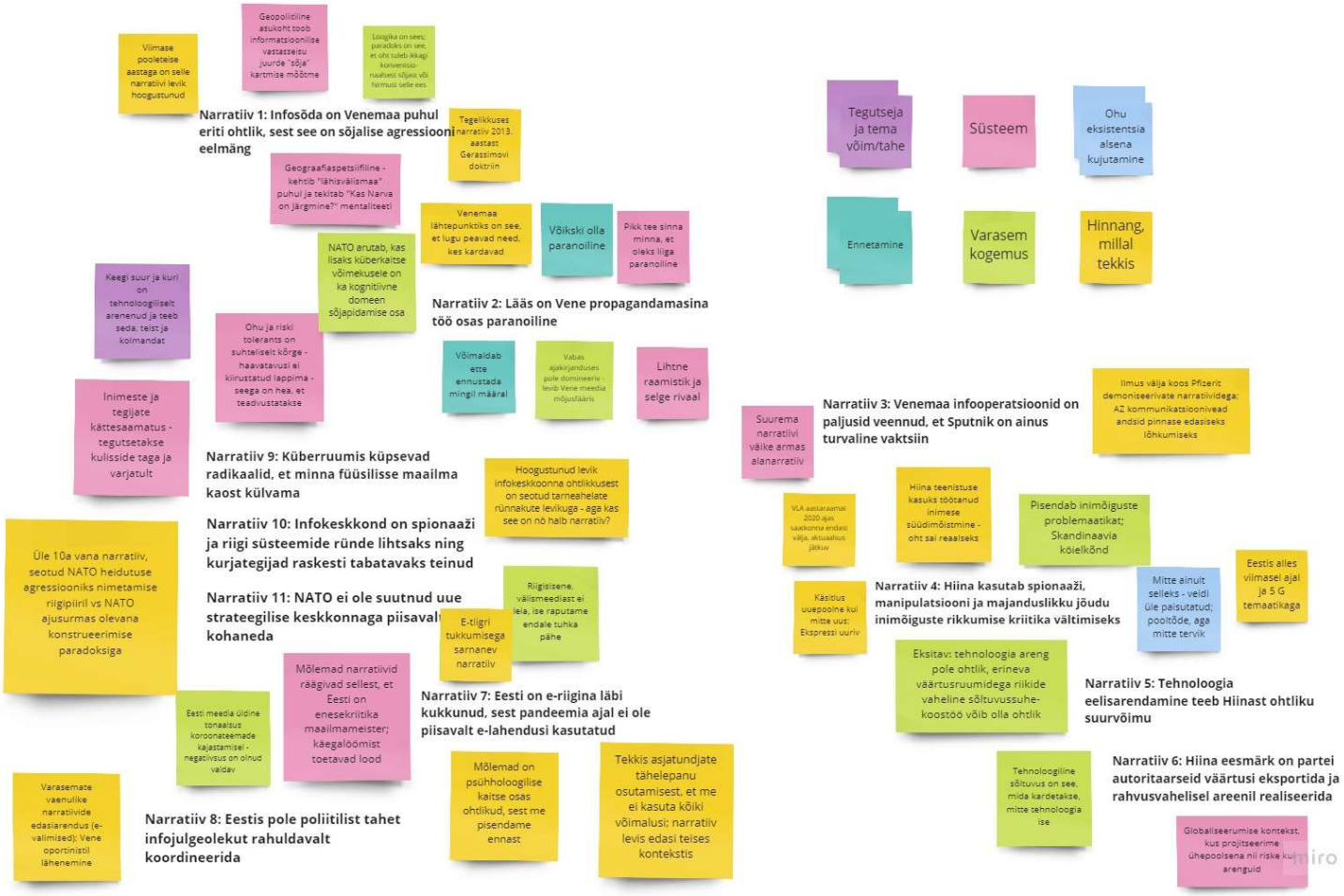
Alateema	Mida küsin?	Aeg	Kommentaarid
Sissejuhatus I	Kes ma olen? Mida, miks ja kuidas ma uurin? Millise teoreetilise läätse läbi magistritööle olen lähenenud? *Kordan üle andmete analüüsimise ja säilitamise plaani.* *Vastan jooksvalt küsimustele.*	3 min	Tutvustan põgusalt ennast, magistritöö läbi viimise metoodikat ja teoreetilist tausta.
Sissejuhatus II	Kes te olete? Nimi ja amet. *Tutvustame nimeliselt ja lepime kokku, et kõik vähegi isikut või asutust tuvastav info jääb meie vahele.* Kaua valdkonnas töökogemust on? Mis magistritöös varjunimeks olla võiks?	7 min	Valmistan ette koosloome „tahvli“ Miro keskkonda. Tutvustan seda neile ekraani jagades ning olen ainsana märkmete liigutaja, et eksitusi vältida. Tutvumisalale teen nende juttu kuulates staaži kohta märkmeid ning valime varinimed (peamiselt tutvumise ja soojaks rääkimise eesmärgil).
I – Korrelatsioon tegelikkusega ja seos minevikuga	*Tutvustan narratiive järgemööda, lähtudes ühest ja samast loogikast ning klastrite järjekorrast.* Kas ja kuidas olete y narratiiviga varem kokku puutunud? On see üllatav või korduvalt esinev, juba tuttav narratiiv? *Paigutame Miros ette valmistatud ajajoonele, et püüda narratiivi tekkimise faasi ajaliselt määratleda.*	12 min	Miros on peamised strateegilised narratiivid märkmepaberitel valmis seatud koos analüüsitasanditega (6tk).

II – Tegutsejad	Milline tegutseja võiks sellise narratiivi levitamisest kasu lõigata? Kas levik on olnud pigem kavatsuslik (nt botid, kineetilised küberoperatsioonid) või mittekavatsuslik (nn *useful idiots*)?	12 min	Võtame ette narratiivide tegutsejad, lähtudes Eco mudelautori ja mudellugeja kontseptsioonidest. Ma ei ütle siinkohal tegutsejaid narratiivide põhjal ette, sest tahan just teada, milline on nende esmane hinnang.
III – Eesti ja NATO huvide kattumine	*Narratiivid on töölaual jätkuvalt reas – nüüd hakkan lisama märkmepabereid vastavalt sellele, kas eksperdid peavad seda meie isiklikuks mureks või liitlaste ühiseks mureks.* Kuidas sarnaneb teiste riikide kogemus Eesti omale? Milline on strateegiline koostöö sel teemal siiani olnud?	12 min	Olles Eestile keskendunud, saab nüüd fookuse laiemaks ajada ning tulemused geopoliitilisse konteksti asetada.
IV – Tulevik ja lahendused	Millisesse tähtsuse järjekorda seaksid nad uuringu tulemustest välja joonistunud narratiivid julgeoleku kaalutlustel – millega tuleks esmajoones tegeleda? Kuidas võiks praktiliselt välja näha x, y või z narratiivi dekonstrueerimine ning selle uuega asendamine? Milline võiks olla Eestile kasulik vastunarratiiv? Kelle vastutusala see on?	12 min	<u>Harjutus</u>. Nüüd palun ma neil 10 min jooksul intuitiivselt antud skoori abil kokku leppida, milline on nende tähtsuse järjekord – mis vajab kõige kiiremini tähelepanu ja/või vastumeetmeid ning milliseid.

Lõpetamine	*Tänusõnad*. *Tagasisidestamise põhimõte.* Kas kellelgi on küsimusi andmete töötlemise osas?	2 min	Tänusõnad. Teadaanne, et saadan uuringus osalemise tingimused uuesti meilile koos mõne tagasiside-küsimusega mulle uurijana ning olen tänulik kui nad leiavad aega vastata.

Lisa 4 – Miro kuvatõmmised fookusgrupi algusest ja lõpust

Kuvatõmmis 2 - Miro töölaud fookusgrupi alguses



Kuvatõmmis 3 - Miro fookusgrupi lõpus

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Maia Klaassen,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Eesti ja NATO küberkaitse võimekuse narratiivne konstrueerimine Eesti ajakirjandusväljaannetes“, mille juhendaja on Mari-Liis Madisson, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Maia Klaassen

31.05.2021