Puolustusvoimien tutkimuslaitos
Tutkimuskatsaus 3–2024

21.02.2024

# Voiko informaatioajan valtio vapautua maantieteestä?

*Mari Ristolainen*
*Informaatiotekniikkaosasto*

**Josef Stalinin kerrotaan sanoneen J.K. Paasikivelle talvisodan aattopäivänä suoraan, että ”maantieteelle emme voi mitään, ettekä te voi sille mitään”[1]. Vuonna 2016 Venäjän maantieteellisen seuran palkintojenjakotilaisuudessa Vladimir Putin totesi viileästi naurahtaen vastauksena omaan kysymykseensä ”mihin Venäjän rajat päättyvät?”, että ”Venäjän rajat eivät pääty mihinkään”[2]. Vuoden 2024 presidentinvaaleissa Vladimir Putin käyttää tätä ”humoristista heittoa” uhmakkaana vaalisloganinaan.[3] Historian saatossa Venäjän naapurimaille on jäänyt maantieteellisiin realiteetteihin sopeutujan kylmä rooli. Venäjä ei kuitenkaan perusta vaikuttamistaan ainoastaan fyysiseen maantieteeseen, vaan toimii rajojen ja alueidensa ”uudelleenmäärittelyssä” aktiivisesti myös informaatio- ja kybertilassa[4]. Venäjän suoraa sotilaallista hyökkäystä Nato-maahan pidetään epätodennäköisenä, jolloin vaihtoehtoisten laaja-alaisten[5] vaikutusoperaatioiden mahdollisuus ei-fyysisissä toimintaympäristöissä vastaavasti kasvaa. Valtioiden aluevaltauksia ja miehityksiä informaatio- ja kybertilassa ei ole aikaisemmin nähty juurikaan mahdollisina. Tämä ei ole kuitenkaan estänyt Venäjää kehittämästä uudenlaisia epätavanomaisia toimintatapoja sekä informaatiopsykologisiin että informaatioteknologisiin[6] valloituspyrkimyksiin Ukrainassa. Vastaavasti informaatioajassa Venäjän naapurimaat ovat yrittäneet löytää ratkaisuja maantieteellisten realiteettien nujertamiseksi ja pyrkineet turvaamaan oman jatkuvuutensa myös fyysisen valtioalueen ulkopuolella informaatio- ja kybertilassa. Tässä katsauksessa kuvataan sekä Venäjän että sen naapurimaiden toimia ja pohditaan, voiko informaatioajan valtio ”vapautua maantieteestä”. Esitetyt tapaukset kuvaavat informaatio- ja kybertilan valtaamista ja valtiollisuuden haastamista sekä informaatio- ja kybertilasta irrottautumista valtiollisuuden suojaamiseksi. Tutkimuskatsaus on osa laajempaa kyberilmiöiden seurantaa ja niiden vaikutusten analysointia, jota Puolustusvoimien tutkimuslaitoksen Informaatiotekniikkaosastolla suoritetaan kybersodankäynnin menetelmä- ja strategiaseurannan tutkimustehtävän puitteissa.**

## Informaatioajan valtio ja sen rajat

Informaatioaika (*Information Age*) – tunnetaan myös nimellä tietokoneaika (*Computer Age*), digitaalinen aika (*Digital Age*), piiaika (*Silicon Age*) ja uuden median aika (*New Media Age*) – on historiallinen ajanjakso, joka alkoi 1900-luvun puolivälissä. Aikakaudelle on ominaista nopea siirtyminen teollisen vallankumouksen aikana vakiintuneista perinteisistä teollisuudenaloista informaatiotekniikkaan perustuvaan talouteen.

[1] Lause löytyy ilmeisesti Paasikiven omista muistiinpanoista neuvotteluista Moskovassa 1939. Lausahdus on eri tulkintojen mukaan jonkinlainen pikakäännös Stalinin pidemmästä lauseesta. Tämän geopoliittisen realiteetin hyväksyminen on ollut pitkään Suomen ulkopolitiikan kulmakivi. Paasikiven päiväkirjoista löytyy myös ”masentunut” lause: ”Kohtalo on asettanut meidän maamme Venäjän suurvallan naapuriksi.” Sitaatti teoksesta: Iloniemi, J. (2015): *Maantieteelle emme mahda mitään*. Docendo: Helsinki, 23.

[2] Премия Русского географического общества (2016): А где заканчивается граница России? Граница России нигде не заканчивается! – Путин. *Премия Русского географического общества* 25.11.2016 (online): https://www.youtube.com/watch?v=Q7PRO0FzFqA (luettu 2.5.2023).

[3] ”Venäjän rajat eivät pääty mihinkään”, julistaa Vladimir Putin mainosnäytöllä Moskovassa, *Helsingin sanomat* 16.1.2024 (online): https://www.hs.fi/ulkomaat/art-2000010121015.html (luettu 16.1.2024).

[4] Tässä tutkimuskatsauksessa käytetään käsitettä "kybertila", jonka Juha Kukkola (2021, 11) on suomeksi määritellyt tarkoitettavan ihmisen luomaa ja hallinnoimaa globaalia tilaa informaatiotoimintaympäristön sisällä, jonka erityinen luonne perustuu elektroniikan ja sähkömagneettisen spektrin käyttämiseen informaation luomiseksi, muokkaamiseksi, vaihtamiseksi ja hyödyntämiseksi toisiinsa liitettyjen informaatioteknologiaa käyttävien verkkojen kautta. Korostettaessa kybertilan luonnetta nimenomaan toiminnan ympäristönä käytetään käsitettä kybertoimintaympäristö. Tällöin huomio ei ole pelkästään tilassa, sen luonteessa tai ominaisuuksissa vaan myös prosesseissa, tiedonhallinnassa ja subjektien vuorovaikutuksessa verkkojen kautta. Kybertila vertautuu mereen, maahan, ilmaan ja avaruuteen – se on toiminnan kehys ja rakenne. Kybertilan ja toimintaympäristön leikkauspisteessä on kybertaistelutila tai -ulottuvuus (*domain*). Kukkola, J. (2021): *Rakenteellisen kyberasymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä*. Puolustusvoimien tutkimuslaitoksen julkaisuja 13: Riihimäki. Informaatiotila (*информационное пространство*) puolestaan on alun perin laaja venäläinen käsite, joka liittyy informaation muodostamiseen, luomiseen, muokkaamiseen, välittämiseen, käyttöön ja säilyttämiseen ja joka vaikuttaa yksilö- ja yhteiskunnan tasolla informaatioinfrastruktuuriin ja itse informaatioon. Venäläiseen informaatiotilaan kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet (vrt. ”kybertoimintaympäristö”). Informaatiotila on venäläisen ajattelun mukaan monimutkainen ”järjestelmä”, jossa valtio pyrkii vaikuttamaan tiedonkulkuun ja säilyttämään valvontansa viestinnässä. Venäjällä informaatiotilan hallintaan liittyvät ainakin: mediavalvonta, viestinnän rajoitukset, propaganda ja informaatiovaikuttaminen, internetin hallinta ja kansainväliset vaikutuspyrkimykset. Yksinkertaistetusti venäläisessä ajattelussa informaatiotila pitää sisällään myös kybertilan. Tässä tutkimuskatsauksessa käytetään läntisen ajattelutavan mukaisesti molempia sekä kybertila että informaatiotila -käsiteitä, koska ne nähdään vielä erillisinä, joskin toisiaan täydentävinä ja kiinteästi toisiinsa liittyvinä.

[5] Tässä katsauksessa käytetään Puolustusvoimissa yleisesti ”hybridi-” käsitteen sijasta käytettyä käsitettä ”laaja-alainen”. Ks. esim. Kauppinen, R. (2021): Hybridivaikuttaminen vs. laaja-alainen vaikuttaminen, *Sotatieteen päivät 2021* (online): https://www.doria.fi/bitstream/handle/10024/182626/KAUPPINEN%20RIITTA%20-%20KOKONAISTURVALLISUUDEN%20TY%C3%96RYHM%C3%84.pdf?sequence=1 (luettu 9.2.2024).

[6] Venäläisessä ajattelussa operaatiot informaatiotilassa (vrt. edellä esitetty määritelmä) jaetaan informaatiopsykologiseen ja informaatioteknologiseen vaikuttamiseen. Informaatiopsykologinen toiminta keskittyy vaikuttamaan ihmisten ajatteluun, mielipiteisiin ja käyttäytymiseen. Läntisessä käsitejärjestelmässä tämän tyyppistä toimintaa kutsutaan informaatiovaikuttamiseksi. Informaatioteknologinen toiminta liittyy teknisiin keinoihin, joiden avulla vaikutetaan tietojärjestelmiin ja tekniseen infrastruktuuriin. Tämä vastaa läntisen käsitejärjestelmän kybervaikuttamista. On kuitenkin huomioitava, että molemmissa (informaatiopsykologisessa ja informaatioteknologisessa vaikuttamisessa) ja voidaan käyttää hyväksi mm. kyberhyökkäyksiä.

Informaatioaika ei ole kuitenkaan vain teknologinen muutos, vaan se on myös yhteiskunnallinen ja kulttuurillinen muutos, joka on vaikuttanut ihmisten tapaan elää, työskennellä ja kommunikoida – mahdollisesti myös sotia.[7]

Informaatioaikakaudella valtiot ovat pakotettuja uudelleenmäärittelemään valtioalueensa ja pohtimaan sen todellisia rajoja maantieteellisen sijainnin ulkopuolella. Informaatioajan valtiolla on fyysisen sijainnin ja maa-alueen lisäksi valtioalueeseen rinnastettava ”alue” informaatio- ja kybertilassa. Informaatioajan valtion rajat ovat yhtäältä sidottuja fyysiseen paikkaan maa- ja merialueella sekä ilmatilassa, mutta toisaalta informaatioajan valtion rajat ovat määrittelemättömiä ja nopeasti muuttuvia teknologisia ratkaisuja kybertilassa. Informaatiotilassa valtioiden rajat ovat vielä mutkikkaampia ja muuntautumiskykyisempiä kielellis-kulttuurillisia konstruktioita (vrt. esim. Русский мир – ”venäläinen maailma”[8]). Fyysisen valtioalueen suhde tähän ns. ”digitaaliseen valtioalueeseen” on vielä hyvin pitkälle kansainvälispoliittisesti määrittelemätöntä ja juridisesti vahvistamatonta.

Informaatioajan valtion digitaalisen valtioalueen voidaan yhtäältä katsoa koostuvan ”kyberterritoriosta”, joka voidaan määritellä seuraavasti: ”valtion suvereenin toimivallan piiriin kuuluvat tietoverkot ja tekninen infrastruktuuri ja niiden tarjoamat palvelut sekä niissä käsiteltävä data”[9]. Vastaavasti ”valtion informaatioalueen” voidaan ajatella täydentävän kyberterritoriota, koska se liittyy valtion kykyyn hankkia, käsitellä, tallentaa, välittää (hallita), suojella ja käyttää informaatiota ja dataa. Informaation (tieto) ja datan käsitteet liittyvät toisiinsa, mutta niillä on erilaiset merkitykset. Data ymmärretään raakana faktana, joka on tallennettu ja/tai kerätty jossain muodossa. Data voi pitää sisällään numeroita, tekstiä, symboleita tai muita merkkejä, jotka eivät sisällä merkitystä sellaisenaan. Datasta muodostuu informaatiota, kun se tulkitaan määritellyssä kontekstissa. Informaatio on merkityksellistä ja jäsenneltyä tietoa, joka tuo ymmärrystä ja luo merkityksiä. Fyysisen valtioalueen turvaamisen lisäksi informaatioajan valtion olemassaolon turvaaminen ja jatkuvuuden hallinta liittyy hyvin pitkälti informaation ja datan hallintaan. On määriteltävä, mikä kaikki informaatio ja data ovat kriittistä valtion jatkuvuuden kannalta eli minkä informaation ja/tai datan tuhoutuminen vaarantaisi koko informaatioajan valtion olemassaolon. Valtion informaatioalueen hallinta on myös osa sen subjektien hallintaa perustuen kulloisenkin valtion suhteeseen sen kansalaisiin. Näiden lisäksi, valtion toiminnan kannalta olennaiset yhteydet eli tietoverkot ja tekninen infrastruktuuri on myös suojattava ja niiden toimivuus turvattava.

Informaatio- ja kybertilan valtioalueellistaminen on vielä käynnissä oleva prosessi, jossa valtiot pyrkivät hyvin erilaisin toimenpitein turvaamaan jatkuvuutensa. Tätä ”digitaalisen valtioalueen” keskeneräisyyttä eli esimerkiksi kansainvälisen-normipohjaisen sääntelyn puuttumista, voidaan myös käyttää varsin luovasti ennen varsinaisia kineettisiä sotatoimia.

## Informaatioajan valtion valloittaminen

Ajatus Venäjän rajojen ”päättymättömyydestä” liittyy vahvasti ajatukseen Venäjän imperiumin ja vanhan keisarikunnan maantieteellisten rajojen palauttamisesta, jonka on arvioitu olevan Vladimir Putinin varsinaisena päämääränä. Putin on useaan otteeseen ilmaissut pyrkimyksensä vahvistaa Venäjän asemaa kansainvälisessä politiikassa ja palauttaa sen rooli tai kehittää sen asemaa suurvaltana. Suurstrategisten tavoitteiden saavuttamiseksi Venäjä on käyttänyt sotilaallista voimaa hankkiakseen osia naapurimaidensa valtioalueesta. Ennen varsinaisia sotilaallisia toimia ja niiden aikana Venäjä on käyttänyt epätavanomaisia keinoja alueiden haltuunotossa.[10]

Helmikuussa 2014 niin kutsutut ”ystävälliset vihreät miehet” ilmestyivät Krimille turvaamaan strategisia kohteita ja kansanäänestystä, jolla Krim lopulta liitettiin osaksi Venäjää. Samana keväänä Itä-Ukrainassa alkoi separistien kapina, joka liittyi Venäjän tukemaan liikehdintään.[11] Ukrainan hallitus ja separatistit taistelivat vuosia. Syntyi erilaisia aselepoja ja suunnitelmia rauhasta (nk. Minskin rauhansopimukset), jotka eivät kuitenkaan tyydyttäneet kaikkia osapuolia. Yksi keskeisimmistä oli helmikuussa 2015 allekirjoitettu Minskin II sopimus. Siinä sovittiin tulitauosta, raskaiden aseiden vetäytymisestä, humanitaarisista kysymyksistä ja paikallisten vaalien järjestämisestä Itä-Ukrainassa. Käytännössä sopimus ei kuitenkaan koskaan täysin toteutunut ja taistelut jatkuivat alueella.[12]

Lopulta tilanne kiristyi ja Venäjä aloitti avoimen sotilaallisen hyökkäyksen Ukrainaan 24. helmikuuta 2022. Venäjän johdon mukaan hyökkäys oli vastaus väitettyihin uhkiin Venäjän etuja ja venäläisväestöä kohtaan Ukrainassa. Venäjä väitti sen toimien olleen välttämättömiä ”denatsifioidakseen” Ukrainan ja estääkseen sen liittymisen Natoon.[13]

Venäjän sotatoimet ja kineettinen vaikuttaminen ovat ymmärrettävästi saaneet laajaa huomioita mediassa ja tutkimuksessa. Venäjän tavoitteena Ukrainassa on nähty olevan valtion itsemääräämisoikeuden täydellinen tuhoaminen, ja ainakin Itä-Ukrainan alueiden miehittäminen ja lopulta liittäminen Venäjään. Vähemmälle huomiolle ovat sekä mediassa että tutkimuksessa jääneet uudenlaiset ei-kineettiset epätavanomaiset vaikuttamiskeinot, joista Suomessa käytetään käsitettä laaja-alainen vaikuttaminen, joilla on mahdollisesti pyritty valloittamaan ja/tai ottamaan haltuun Ukrainan alueita informaatio- ja kybertilassa jo vuodesta 2014 lähtien.[14]

Seuraavaksi esitetään kaksi esimerkkiä mahdollisista aikaisemmin tunnistamattomista informaatio- ja kybertilan ”digitaalisen

[7] Alunperin käsitteen “informaatioaika” on lanseerannut sosiologi ja tietoyhteiskuntatutkija Manuell Castells. Tämän jälkeen sitä on käytetty lukemattomissa teoksissa ja tutkimuksissa – usein ilman määritelmää ja alkuperäistä lähdettä. Ks. esim. Castells, M. (1996): *The rise of the Network Society. The Information Age: Economy, Society and Culture.* Blackwell Publishers: Cornwall.

[8] ”Venäläinen maailma” on käsite, jolla viitataan yleisesti laajempaan kulttuuriseen, poliittiseen ja historialliseen identiteettiin, joka yhdistää venäläiset ja venäjänkieliset. ”Venäläinen maailma” kuvaa myös Venäjän vaikutuspiiriä tai pyrkimystä laajentua ja/tai ylläpitää vaikutusvaltaansa Venäjän historiallisesti hallitsemilla alueilla. Käsitettä on käytetty Venäjällä myös kulttuuripoliittisesti eli kannustamaan ”venäläisen maailman” tukemiseen ja edistämiseen erityisesti venäjän kielen ja kulttuurin ylläpitämisen ympäri maailmaa. Lisätietoja ja tarkempi tausta ”venäläisestä maailmasta” suomeksi ks. esim. Kari, M.J. & Holmila, A. (2023): *Miksi Venäjä toimii niin kuin se toimii*. Docendo: Helsinki.

[9] Ristolainen, Mari (2021): Softaa kyberrajalle! Katsaus kybertilan valtioalueellistamisprosessiin meillä ja maailmalla. *Tutkimuskatsaus* 1/2021, Puolustusvoimien tutkimuslaitos.

[10] Kukkola, J. (2022): *Oveluuden lupaus. Asymmetria, epäsuoruus ja ei-sotilaalliset toimenpiteet uuden venäläisen sotataidon kiintopisteenä.* MPKK, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 22: Helsinki.

[11] Ukrainan kriisin taustoja, sen kehitystä ja laajempia vaikutuksia on tutkinut syvällisesti esim. emeritus professori Richard Sakwa. Ks. esim. Sakwa, R. (2015): *Frontline Ukraine. Crisis in the Borderlands*. I.B. Taurus: London & New York; Sakwa, R. (2023): *The Lost Peace. How the West Failed to Prevent a Second Cold War.* Yale University Press: London.

[12] ibid.

[13] Sakwa 2023.

[14] Yksi uusimmista laaja-alaisen vaikuttamisen menetelmiin mahdollisesti liittyvä toimenpide on Vladimir Putinin tammikuussa 2024 antama määräys Venäjän valtionomaisuuden etsimiseksi, rekisteröimiseksi ja suojaamiseksi niin nyky-Venäjän alueella, kuin myös Neuvostoliiton ja Venäjän keisarikunnan alueilla. TASS (2024): РФ выделит средства на поиск за рубежом имущества СССР и Российской империи, *TASS* 18.1.2024 (online): https://tass.ru/ekonomika/19764679 (luettu 24.1.2024).

valtioalueen" valloitukseen ja haltuunottoon liittyvistä toimenpiteiden kokonaisuuksista, joita Venäjä on tehnyt Ukrainan ns. fyysisen valtioalueen ulkopuolella. Venäläisen ajattelutavan mukaan, ensimmäinen esimerkki on enemmän informaatiopsykologinen ja jälkimmäinen informaatioteknologinen toimenpiteiden kokonaisuus.

## "Novorossija" – valloituspyrkimys Ukrainan informaatioalueella

Vladimir Putin lanseerasi virallisesti Novorossija (Новороссия) -projektin[15] huhtikuussa 2014 järjestetyssä "Suora linja" (Прямая линия) kysymys-vastaus-ohjelmassaan, jossa toistuvasti viittasi Kaakkois-Ukrainaan nimellä Novorossija – kirjaimellisesti käännettynä "Uusi Venäjä". Novorossija on historiallinen termi Mustanmeren pohjoispuolella sijaitsevalle alueelle, jonka Venäjän keisarikunta valloitti 1700-luvulla. Putinin mukaan Novorossijan alueet – Harkova, Luhansk, Donetsk, Herson, Nikolajev ja Odessa – eivät ole koskaan olleet osa Ukrainaa. Hän jatkoi, että vain "jumala tietää", miksi alueesta tuli osa Ukrainaa 1920-luvulla, ja korosti Novorossijan historiallisia, kulttuurisia ja kielellisiä siteitä Venäjään.[16] Toukokuussa 2014 Donetskin ja Luhanskin alueiden johtajat julistivat perustuslakiensa yhdistämisestä.[17] Tämän seurauksena he allekirjoittivat "Novorossijan kansantasavaltojen liiton" (Союз народных республик Новороссии) muodostamisen. Heidän lanseeraamansa uuden perustuslain mukaan Donetsk oli pääkaupunki ja venäläinen ortodoksinen kristillisyys virallinen valtionuskonto. Perustuslaissa määrättiin myös tärkeimpien teollisuudenalojen kansallistamisesta. Virallinen hallintoelin nimettiin "Novorossijan parlamenttiksi", jonka jäseniä olivat erinäiset liikemiehet ja poliitikot. Poliitikko Oleg Tsarev nimitettiin parlamentin puhemieheksi.[18]

Kesäkuussa 2014 ensimmäisessä virallisessa tiedotustilaisuudessaan Oleg Tsarev julisti avoimen verkkokilpailun valtion symboleista, kuten vaakunasta, lipusta, valuutasta ja myös kansallishymnistä. Lisäksi hän kehotti ihmisiä osallistumaan Novorossijan historian kirjoittamiseen. Tsarev halusi julkaista uuden kirjan Novorossijan historiasta ennen syyskuuta, jotta koululaiset saisivat uuden oppikirjan ja tietoa uudesta kotivaltiostaan heti uuden kouluvuoden alussa.[19]

Tämän jälkeen Novorossija alkoi elää virtuaalivaltiona kuin mikä tahansa moderni valtio. Novorossijalla oli oma valuutta, Novorossijan rupla, joka muistutti ulkoisesti Venäjän ruplaa. Novorossijalla oli oma *Novorossia Today* -uutistoimisto, joka julkaisi uutisia englanniksi, ranskaksi, saksaksi, espanjaksi, puolaksi ja venäjäksi, sekä erilaisia YouTube-kanavia ja sosiaalisen median tilejä.[20] Näiden lisäksi kesällä 2014 Helsinkiin perustettiin "Donetskin kansantasavallan (DNR) suurlähetystö", jolla oli omat verkkosivut Novorossijan valtioon viittaavassa osoitteessa: www.novorossiyaembassy.org.[21] Venäjällä järjestettiin myös Novorossijan kansallishymnikilpailu, johon osallistui tunnettuja venäläisiä artisteja (esim. Joseph Kobzon ja Vika Tsyganova)[22]. Kilpailu televisioitiin ja Vika Tsyganovan esityksen jälkeen Oleg Tsarev totesi: *"Itse asiassa Novorossijan tärkein taistelu on taistelu ihmisten sydämistä, mielistä ja sieluista. Kuka tahansa voittaa ... tämän tärkeän taistelun – voittaa koko taistelun. Tässä taistelussa poliitikot eivät pelaa suurta roolia. Tämän taistelun tärkeimmät taistelijat ovat toimittajia, kirjailijoita, taiteilijoita... ja tietenkin laulajat. Ja monien joukossa Vika Tsyganova on etulinjassa tässä taistelussa."*[23] Myös tavalliset venäläiset ja ukrainalaiset osallistuivat Novorossijan kirjoittamiseen osaksi "fyysistä maailmaa" ja virtuaaliseen aluevaltauksen yritykseen esim. kirjoittamalla runoja ja luomalla Novorossijalle omaa kulttuuria ja kirjallisuutta.[24]


**Kuva 1:** "Putinin Novorossijan" kartta.[25]

"Novorossijan" luominen ei kuitenkaan aivan onnistunut. Tämä johtui mahdollisesti separatistien sisäisestä valtakamppailusta ja eri ryhmien ristiriitaisista tavoitteista. Myös Vladimir Putin lopetti Novorossija-termin käytön puheissaan ja hanke hiipui myös Venäjän mediassa. Toukokuussa 2015 Oleg Tsarev julisti Novorossija-projektin päättyneeksi, koska se oli hänen mukaansa

[15] Novorossija-projektin "isänä" oli varsinaisesti kuitenkin Aleksandr Dugin, radikaali poliittinen tutkija, jonka työ on keskittynyt "Euraasian unelmaan", joka tarkoittaa tiivistetysti Venäjän keisarikunnan palauttamista yhdistämällä venäjänkieliset ja venäjänkieliset alueet sekä Venäjän ortodoksikristityt. Ks. esim. Dugin, A. (2014*): Eurasia Mission: An Introduction to Neo-Eurasianism*. London: Akrtos

[16] Putin, V. (2014): Прямая линия с Владимиром Путиным. *Стенограммы* 17.4.2014 (online): http://kremlin.ru/transcripts/20796 (luettu 24.1.2024).

[17] Sakwa 2015, 154.

[18] Sakwa 2015, 178.

[19] Tsarev, O. (2014) *Пресс-конференция спикера Парламента СНР. Конкурс на создание гос. символов Новороссии* (online): https://www.youtube.com/watch?v=UVwm1TIMBNA (luettu 3.7.2014); Tsarev, O. (2014): Олег Царёв: "Украина –исторический антирусский проект". *Вестник Кавказа* 8.10.2014 (online): http://www.vestikavkaza.ru/articles/Oleg-TSarev-Ukraina-%E2%80%93istoricheskiy-antirusskiy-proekt.html (luettu 24.1.2024).

[20] Bērziņa, I. (2014): Branding Novorossiya. *Strategic Review,* No. 10. National Defense Academy of Latvia, Center for Security and Strategic Research (online): https://www.naa.mil.lv/sites/naa/files/document/10_SA-10_NOVORUS_1.pdf (luettu 5.11.2014).

[21] Kyseinen verkkosivu ei ole enää toiminnassa, mutta se on dokumentoitu mm. Matti Rossin teoksessa vuonna 2015. Ks. Rossi, M. (2015): *Raunioista nousee Donbass*. Suomen antifasistinen komitea SAFKA, Donetskin kansantasavallan (DNR) suurlähetystö Helsingissä & Johan Bäckman Publications: Helsinki.

[22] Ks. esim. Vika Tsyganovan esittämä "Novorossijan hymni" https://www.youtube.com/watch?v=X67qb2l1h3Y Esitys on taltiointi Это родина моя ("tämä on isänmaani) -ohjelmasta pietarilaiselta tv-kanavalta (5-канал).

[23] Tsarev, O. (2014): Facebook -julkaisu, sitaatti *Московский комсомолец* 20.10.2014, 9.

[24] Novorossijan "kulttuurisen rakentamisen" tutkimus oli osa allekirjoittaneen aikaisempaa kulttuuriseen rajatutkimukseen liittyvää tutkimusta Itä-Suomen ja Tromssan yliopistoissa vuosina 2014-2016. Tässä esitetty kuvaus on tiivistetty julkaisemattomista konferenssiesityksistä: Ristolainen, M. (2015): *The Written Borders of "New Russia" at War and Peace*. EuPRA, The Framing of Europe: Peace Perspectives on Europe´s Future, 2-4.9.2015, Tromsø, Norway; Ristolainen, M. (2015): *The Written Borders of New Russia.* Association for Borderlands Studies Annual Meeting, 8.-11.4.2015 Portland, OR, USA.

[25] Edmaps.com sivuston mukainen "Putinin Novorossijan" kartta vuodelta 2021: https://edmaps.com/html/novorossiya_2021_d.html (luettu 9.2.2024). Sivustolta löytyy myös mm. historiallisen Novorossijan kartta 1796-1800: https://edmaps.com/html/novorossiya_1796_1800.html (luettu 9.2.2024) ja muita Ukrainan eri historian vaiheiden karttoja.

Minskin II rauhansopimuksen vastainen.[26] On vaikea arvioida kuinka paljon ajatus Novorossijasta valtiona elää vielä Ukrainassa Venäjää tukevien ihmisten mielissä tänä päivänä. Koulunsa uusien Novorossijan historiankirjojen kanssa mahdollisesti aloittaneet lapset ovat nyt aikuisuuden kynnyksellä. Novorossijan nimeä kantava venäjänkielinen uutissivusto[27] ja sanomalehti[28] löytyvät yhä. Rinnastamalla ”Putinin Novorossijan” kartan (kuva 1) lähes pysymättöminä jo pidemmän ajan oleviin rintamalinjoihin (tilanne 6.2.2024) (kuva 2), voidaan löytää yhtäläisyyksiä ja mahdollisesti arvioida Venäjän tavoitteita.


**Kuva 2.** Rintamalinjojen tilanne 6.2.2024 arvion mukaan.[29]

Tänä päivänä tarkasteltuna ”Novorossijaan” liittyvien toimenpiteiden kokonaisuutta voidaan pitää esimerkkinä Venäjän informaatiopsykologisesta valloituspyrkimyksestä Ukrainan informaatioalueella. Projektin tavoite saattoi olla valmistella alueen väestöä tulevaan fyysisen miehitykseen. Projektia edesauttoi merkittävästi väestön venäjänkielisyys (vrt. ”venäläinen maailma”). Kaikki tuotettu ”virallinen digitaalinen informaatio” muodostaa helposti tulkittavan poliittisen narratiivin esim. valtiojohtoiselle poliittisen historian tutkimukselle, mikä on osa laajempaa historian manipulointia. Tapaus ”Novorossija” kertoo omalla tavallaan väistämättömästä informaatiotilan valtioalueellistumisprosessista eli valtiollisen informaatioalueen muodostumisesta. Informaatioalue on osa valtion valtioaluetta, jonka koskemattomuus on myös pystyttävä jollain tavalla turvaamaan.[30] Vastaavanlaisten ”projektien” tunnistaminen voi olla merkityksellistä myös mahdollisten tulevien konfliktien tunnistamisessa Venäjän naapurimaissa.[31] Viitteitä samantyyppisestä ”informaatioalueen valloitusyrityksestä” ”virtuaalivaltion” luomisen kautta oli esim. Artsakhin alueella Kaukasuksella 2020-luvun alussa.[32]

## Krimin, Itä-Ukrainan ja Hersonin alueen uudelleenreititys – Ukrainan kyberterritorion haltuunottoyritys

Uudelleen reititys viittaa tilanteeseen, jossa tietoliikenne ohjataan tai ohjelmoidaan kulkemaan eri reittiä kuin mitä alun perin oli suunniteltu. Liikenteen uudelleen reititystä on perinteisesti käytetty hyvin erilaisten tavoitteiden saavuttamiseksi (toiminnan piilottamiseksi, turvallisuustoimenpiteiden ohittamiseksi, tietoliikenteen seurantamahdollisuuksien kaventamiseksi jne.). Uudelleenreititys voi tapahtua eri tasoilla, kuten verkkokerroksella tai sovelluskerroksella[33]. Toisin sanoen, reititys voidaan toteuttaa ilman tarvetta rakentaa tai purkaa fyysisiä rakenteita, kuten kaapelointeja ja laitetiloja. Internetin reititys on kokonaisuudessaan hyvin monimutkainen järjestelmä, joka mahdollistaa tietoliikenteen tehokkaan ja luotettavan siirtymisen eri verkkojen välillä. Internetin reitityspolitiikkaa voidaan ajatella ohjeina, joita tietokoneet ja verkot seuraavat siirtäessään tietoa toisilleen. Yksinkertaistetusti reititykseen liittyvät seuraavat käsitteet ja toiminnot:

1) Reititys ja AS (*Autonomous System*): internet on jaettu osiin, joita kutsutaan autonomisiksi järjestelmiksi (AS). Jokainen AS on kuin oma ”alueensa” internetissä;

2) BGP (*Border Gateway Protocol*) on keskeinen protokolla, joka mahdollistaa reititystaulukoiden jakamisen ja päivittämisen internetin laajuisesti. BGP auttaa AS:iä päättämään, mikä on paras tapa lähettää tietoa toisille AS:lle;

3) Reitityspäätökset: AS:t tekevät päätöksiä siitä, mikä on nopein tai tehokkain tapa lähettää dataa. Ne voivat myös määrittää sääntöjä, kuten kenelle antaa etusija tai kenen kanssa tehdä kaupallisia sopimuksia;

[26] Uatoday.tv (2025): Russian-backed 'Novorossiya' breakaway movement collapses, *Uatoday.tv* 20.5.2015 (online): https://web.archive.org/web/20150521051525/http://uatoday.tv/politics/russian-backed-novorossiya-breakaway-movement-collapses-428372.html (luettu 24.1.2024).

[27] Новороссия (online): https://www.novorosinform.org/ (luettu 24.1.2024).

[28] Lehti Новороссия. Русская газета Донбасса on perustettu vuonna 2014 ja sen arkistoidut viikoittain ilmestyneet numerot on löydettävissä vuodesta 2014 lähtien (online): https://novopressa.ru (luettu 7.2.202024).

[29] Kartta lainattu Iltasanomien Ukraina -seurannasta: *Iltasanomat* (2024): (online) https://www.is.fi/ulkomaat/art-2000010119847.html (luettu 9.2. 2024).

[30] vrt. esim. Bērziņa, I. & Voinoff, S. (2024): The Russo-Ukraine War: the implications for the security of Finland and Latvia. *Research Bulletin* 2–2024, 6.2.2024, Finnish Defence Research Agency.

[31] Esim. Venäjällä on myös olemassa jo valmiita tunteisiin vetoavia konsepteja ja käsitteitä tämän tyyppiseen vaikuttamiseen informaatiotilassa tietyllä alueella. Yksi näistä voisi olla ns. ”pikkuisänmaa” (малая родина) -käsitteen valjastaminen tähän tarkoitukseen. ”Pikkuisänmaalla” viitataan kotiseutuun, juuriin ja kaipuuseen johonkin, jota ei ehkä juuri nyt enää ole, mutta jota vahvistamalla Venäjän eri naapurimaista tällaisen saattaisi historian uudelleen tulkinnoilla monikin kansalainen mahdollisesti löytää.

[32] ”Artsakhin tasavalta” on itsenäiseksi julistautunut armenialaisenemmistöinen alue Kaukasuksella Azerbaidzhanin rajojen sisällä. Vuosina 1991–2017 sen nimi oli Vuoristo-Karabahin tasavalta. Eri käsitysten mukaan se oli joko itsenäinen valtio, Azerbaidzhanin tai Armenian osa. Artsakhia rakennettiin samantyylisenä virtuaalivaltiona kuin Novorossijaa, kunnes syyskuun 2023 lopussa Artsakhin presidentti allekirjoitti asetuksen kaikkien tasavallan instituutioiden lakkauttamisesta 1. tammikuuta 2024 mennessä. Asetus yritettiin myöhemmin kumota, mutta lokakuuhun 2023 mennessä lähes koko alueen väestö oli paennut Armeniaan ja Artsakh lakkasi käytännössä olemasta. Havaintoja Artsakhin alueen tilanteen kehittymisestä teki alun perin tutkija Miika Aaltonen, PVTUTKL, 2022 (julkaisematon raportti).

[33] OSI-malli (*Open Systems Interconnections*) on viitekehys, jonka tarkoituksena on luoda yhteinen perusta erilaisten tietoliikenneprotokollien ja -tekniikoiden ymmärtämiseen ja määrittämiseen. OSI-malli jakaa tietoliikenteen seitsemään kerrokseen, joista kukin vastaa tietynlaista toiminnallisuutta: 1) Fyysinen kerros (*Physical layer*); Siirtoyhteyskerros tai siirtokerros (*Data Link layer*); 3) Verkkokerros (*Network layer*); 4) Kuljetuskerros (*Transport layer*); 5) Istuntokerros (yhteysjakso, *Session layer*); 6) Esitystapakerros (*Presentation layer*); 7) Sovelluskerros (*Application layer*).

4) *BGP-peering*: AS:t keskustelevat keskenään BGP:n avulla ja kertovat toisilleen parhaista tavoista lähettää tietoa. Ne voivat myös päättää, mitä tietoa jakaa ja mitä ei;

5) Tavoite: yleinen reitityspolitiikan tavoite on löytää nopein ja tehokkain polku tietoliikenteelle, jotta tieto pääsee kohteeseensa mahdollisimman nopeasti ja luotettavasti.[34]

Internetin reitityspolitiikka on siis kuin ohjeet, joiden avulla eri osat internetistä päättävät, miten parhaiten lähettää tietoa toisilleen. BGP auttaa näitä osia tekemään päätöksiä, ja reitityspolitiikka määrittelee säännöt näille päätöksille. Reitityspolitiikkaan voidaan yrittää vaikuttaa esim. manipuloimalla AS:ien reittitietoja. AS:n hallinta mahdollistaa sen, että verkko-operaattorit voivat päättää, mitä reittiä data kulkee tai ei kulje verkossa – esimerkiksi Ukrainan alueen kautta tai Venäjälle.

Venäjä on toimeenpannut mobiili- ja verkkoliikenteen uudelleen reitistä Ukrainassa maaliskuussa 2014 Krimillä, elokuussa 2018 Itä-Ukrainassa ja toukokuussa 2022 Hersonin alueella. Näitä tapauksia voidaan pitää esimerkkeinä fyysisen valtion kyberterritorion osan haltuunottoyrityksenä. Venäjä yritti korvata ko. alueiden reitityspolitiikan ja verkkoinfrastruktuurin omallaan ennen alueen varsinaista ”fyysistä” liittämistä Venäjään.

Maaliskuusta 2014 alkaen Krim siirtyi Venäjän internet-lainsäädännön piiriin, mutta seuraavat asiat tapahtuivat jo ennen sitä. Ensimmäiseksi ukrainalaiset teleyritykset alkoivat poistumaan alueelta – jotkut vapaaehtoisesti (esim. MTS Ukraina myi omaisuuttaan) ja toiset väkisin (esim. Ukrtelecom, jonka toimitiloja ”ystävälliset vihreät miehet” ottivat haltuunsa ja siirsivät toiminnot Venäjän tukemalle Krymtelekomille). Toiseksi suoria yhteyksiä Ukrainan mantereelle alettiin sabotoida. Kolmanneksi Venäjän valtion omistama televiestintäyhtiö Rostelekom rakensi ja otti nopeasti käyttöön 110 Gbps:n merenalaisen yhteyden Venäjältä Krimille, Kertsinsalmen kaapelin. Tämä fyysinen toimenpide mahdollisti loogisen tason reitittämisen. Palveluista vastasi Rostelecomin (verkko-operaattori) vastaperustettu paikallinen edustaja Miranda Media (AS). Näin pieni kaistanleveys merkitsi Krimin kansalaisille hitaampia nopeuksia. Venäläisoperaattoreilla on myös laajat tiedonkeruuvelvoitteet käyttäjistään.[35]

Ennen valtausta Krimin internetpalveluntarjoajat (verkko-operaattorit) toimivat välittäjinä suuremmille ukrainalaisille ja kansainvälisille internetpalveluntarjoajille, jotka yksinkertaisesti siirsivät tietoja niiden suuntaan. Tutkimuksen mukaan vuodelle 2014 on ominaista riippuvuuden merkittävä lisääntyminen uuden AS:n, Miranda Median, ja sen emoyhtiön, Rostelecomin, osalta. Krimiltä tulevat polut kulkivat Miranda Median kautta ja sen jälkeen Rostelecomin kautta. [36] Tämä reititysmuutos vähensi huomattavasti Ukrainan kautta kulkevien reittien määrää joka vuosi aina vuoden 2017 puoliväliin asti, jolloin ”Ukrainan liitännäisjärjestelmien kautta kulkevia polkuja ei enää näkynyt”.[37]

Elokuussa 2018 myös Itä-Ukrainan separatistialueiden yhteydet uudelleenreititettiin. Paikallisten internetyhteyksien reititys muuttui ja käytettävissä olevat Donetskin ja Luhanskin saapuvat tai niiltä lähtevät datapolut kulkivat yhtäkkiä vain Venäjän kautta eivätkä enää Ukrainan kautta. Reititysmuutoksia Itä-Ukrainassa oli havaittu jo vuosia, mutta kesällä 2018 ne saatiin lopulliseen päätökseen. [38]

Toukokuussa 2022 Venäjä korvasi ukrainalaisen teleoperaattorin yhteydet omillaan myös Hersonin alueella. Hersontelekom-teleoperaattorin Skynet-verkkoyhteydet katkesivat Hersonissa eteläisessä Ukrainassa, ja ne käännettiin osittain toimimaan noin vuorokauden viiveellä venäläisen Rostelecomin verkon kautta. Ukraina onnistui kuitenkin palauttamaan ja kytkemään Hersonin yhteydet takaisin omaan infrastruktuuriinsa muutaman päivän kuluttua.[39] Silloinen Ukrainan valtionhallinnon erityisviestintäpalvelun johtaja Yurii Shchyhol piti Venäjän suorittamaa yhteyksien uudelleenreititystä kansainvälisen oikeuden vastaisina ja tulkitsi näin kyseiset toimenpiteet kybertilassa Ukrainan valtioalueen koskemattomuuden rikkomisena.[40]

Tämäntyyppisen informaatioteknologisen valloituspyrkimyksen vaikutukset ovat sekä informaatiopsykologisia että informaatioteknologisia. Verkkoliikenteen reitittäminen liittyy oleellisesti sekä psykologiseen että teknologiseen kontrolliin eli viranomaiset voivat valvoa ja tarvittaessa rajoittaa liikennettä. Verkkoliikenteen uudelleenreitityksellä Venäjä pakotti alueella mobiili- ja verkkoyhteyksiä käyttävät ihmiset Venäjän internetkuplaan, jossa ihmisten kohtaama informaatio on rajoittunutta ja vahvistaa Venäjän asettamia päämääriä. Venäjä pystyi myös ulottamaan oman sensuurijärjestelmänsä uudelleen reititettyyn verkkoliikenteeseen eli esim. estämään läntisten sosiaalisen median ja uutispalveluiden käytön. Venäjän kautta reititetty liikenne on Venäjän lainsäädännön alaista, joka vaatii esim. palveluntarjoajia tallentamaan käyttäjien viestiliikenteen ja tarvittaessa antamaan viranomaisille pääsyn siihen.[41]

Verkkoliikenteen uudelleenreititys on usein kohtalaisen helposti havaittavissa, koska internetin runkoverkossa AS-alueiden välisellä tasolla internetliikenteen reitityssäännöt ovat julkisia. Tästä johtuen liikenne pystytään normaalioloissa palauttamaan suhteellisen nopeasti. Kriisitilanteessa palauttaminen voi kuitenkin viivästyä ja tämäntyyppisellä operaatiolla on

[34] Hyvä perusteos internetin reitityksensä on mm. Halabi, S. (2000): *Internet Routing Architectures*. Cisco Press: Hoboken.
[35] Fontugne, R. et al. (2020): The Internet in Crimea: a Case Study on Routing Interregnum. 2020 IFIP Networking Conference, Jun 2020, Paris, France (online): https://hal.science/hal-03100247/document (luettu 21.1.2024).
[36] ibid.
[37] ibid.
[38] Limonier, K. et al. (2021): Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine. *First Monday*, Vol. 26, No. 5 - 3 May 2021 (online): https://firstmonday.org/ojs/index.php/fm/article/download/11700/10128 (luettu 25.1.2024).
[39] Reuters (2022): Russia reroutes internet traffic in occupied Ukraine to its infrastructure, Reuters 3.5.2022 (online): https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/ (luettu 25.1.2024); Madory, D. (2022): Rerouting of Kherson follows familiar gameplan. Blogi-kirjoitus 9.8.2022 (online): https://www.kentik.com/blog/rerouting-of-kherson-follows-familiar-gameplan/ (luettu 25.1.2014).
[40] Hüsch, P. (2022): Rerouting Parts of Ukrainian Internet Traffic – A Violation of the Principle of Non-Intervention? *OpinioJuris*, 10.5.2022 (online): https://opiniojuris.org/2022/05/10/rerouting-parts-of-ukrainian-internet-traffic-a-violation-of-the-principle-of-non-intervention/ (luettu 9.2.2024).
[41] Kun liikenne siirtyy Venäjän lainsäädännön alaiseksi, sitä voidaan valvoa SORM-järjestelmän (Система оперативно-розыскных мероприятий) kautta, joka on Venäjän turvallisuusviranomaisten käytössä. Tämän lisäksi liikenne kulkee GosSOPKA (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) järjestelmän kautta, joka on valtakunnallinen tietoverkkohyökkäysten monitorointi- ja torjuntajärjestelmä, joka kattaa tietoverkkoon tunkeutuvan vihollisen havaitsemiseen, estämiseen, tuhoamiseen ja hyökkäyksestä palautumiseen tarkoitettuja toimenpiteitä. Näiden lisäksi Venäjän verkkoliikennettä turvataan TsMUSSOP (Центр мониторинга и управления сети связи общего пользования) keskitetyn verkonhallinta- ja valvontajärjestelmän avulla, joka tavoitteena on kerätä tietoa tietoverkkojen toiminnasta ja estää haitallinen ja uhkaava toiminta. Tähän järjestelmään liittyvien operaattoreiden verkkoihin asennettaviin TSPU-laitteiden (техническое средство противодействия угрозам) avulla voidaan valikoivasti rajoittaa liikennettä ja tarvittaessa eristää Venäjän tietoliikenneverkot globaalista internetistä. Lisätietoja suomeksi, ks. esim. Kukkola 2021.

mahdollista saada aikaan merkittäviä katkoksia halutun informaation levittämiseen.

## Informaatioajan valtion turvaaminen ennen ja nyt

Yleismaailmallisesti kyberpuolustus-käsite tuli merkittäväksi informaatioajan valtioissa vasta 2000-luvun alkupuolella, kun digitalisaatio ja tietotekniikan rooli yhteiskunnassa kasvoivat merkittävästi. Kansallisia nyanssieroja kyberpuolustus-käsitteen määrittelyssä löytyy, mutta yleisesti ns. läntisessä ajattelumallissa siihen liitetään ensisijaisesti pyrkimykset suojata tietojärjestelmiä ja verkkoja, jotka ovat haavoittuvia erilaisille kyberhyökkäyksille.

Informaatiopuolustuksesta on länsimaissa alettu laajemmin puhua vasta 2010-luvun loppupuolella, jolloin alettiin ymmärtää valtion tarvitsevan toimenpiteitä informaatiovaikuttamisen estämiseen ja/tai siihen vastaamiseen. Käytännössä nämä toimet ovat monessa maassa vielä varsin olemattomia.

Venäjä on lähestynyt informaatioajan valtion turvaamista oman ajatusmaailmansa kautta. Venäjän kehittämää mallia on tutkimuksessa kutsuttu ”kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmäksi”[42]. Tämän järjestelmän avulla Venäjä on kehittänyt ja kehittää valtioalueensa suojaa myös em. tyylisiä informaatiopsykologisia ja informaatioteknologisia operaatioita vastaan. Pystyykö Venäjä todellisuudessa pakottamaan kamppailun vihollisena pitämänsä valtion olemassaolosta informaatio- ja kybertilaan on kysymys, johon ei vielä tässä ajassa ole vastausta.

Informaatioajan valtiossa informaatio- ja kyberpuolustuksen tulisi muodostaa yhdessä perinteisten valtion koskemattomuuden turvaamisen keinojen kanssa kokonaisuus, jonka avulla valtio pystyy turvaamaan jatkuvuutensa ja takaamaan olemassaolonsa kaikissa tilanteissa.

Seuraavaksi tässä tutkimuskatsauksessa tarkastellaan muutamia Venäjän naapurimaihin liittyviä erilaisia tapauksia, joissa valtio on joutunut taistelemaan olemassaolostaan informaatio- ja kybertilassa, sekä miten Venäjän naapurimaat ovat varautuneet tähän taisteluun fyysisen valtioalueen ulkopuolella ennen ja nyt.

## Viro: kybernetiikan neuvostomaasta ”datasuurlähetystön” kehittäjäksi

Viroa pidetään yleisesti digitalisaation edelläkävijänä. Kuvattaessa Viron digitaalista kehitystä aloitetaan usein vuoden 2007 Pronssisoturi-patsaskiistaan liittyneistä palvelunestohyökkäyksistä (DDoS)[43] ja niiden jälkeisestä kehityksestä ja Naton kyberturvallisuuskeskuksen (CCDCOE) perustamisesta Tallinnaan vuonna 2008.[44] Viron digitalisaatiovalmiuksilla ja -kehityksellä on kuitenkin vahvat neuvostoliittolaiset juuret. Vuonna 1960 Tallinnaan perustettu Kybernetiikan instituutti (Институт кибернетики академий наук эстонской ССР) toimi Tallinnan teknisen yliopiston[45] edeltäjänä. Neuvostoliitto keskitti Viroon merkittävän määrän tietoteknistä koulutusta ja loi alaan liittyvää osaamista.[46] Neuvostoliiton hajottua ja Viron palautettua itsenäisyytensä vuonna 1991 Viron toimintaa on leimannut äärimmäinen Venäjä-kielteisyys ja ärhäkkyys Venäjän suuntaan sekä korostetun länsimaisiin arvoihin pohjautuva ulko- ja turvallisuuspolitiikka. Kaiken tämän taustalla on ollut kokemus, että sotilaallinen puolueettomuus on sama kuin yksin jääminen. Virosta tuli EU-maa ja Naton jäsen vuonna 2004. Nato-jäsenyys oli Viron ulkopolitiikan tärkeä päämäärä jo heti 1990-luvulla.

Digitalisaation merkitys valtion jatkuvuuden ja toiminnan turvaamisen kannalta on Virossa ymmärretty jo pitkään. Teknologinen kehitys oli se, millä Viro pyrki irrottautumaan lopullisesti ”neuvostomaan” maineestaan. Vuonna 1996 Virossa käynnistettiin ”Tiikerin loikka” -ohjelma (*Tiger Leap -program*), jolla kehitettiin Viron koulujärjestelmää vastaamaan informaatioyhteiskunnan vaatimuksiin. Kouluihin hankittiin modernia ICT-infraa, koulut liitettiin internetiin, opettajia koulutettiin käyttämään ICT-järjestelmiä ja opetuksessa käytettävien ohjelmistojen kehittämistä tuettiin. ”Tiikerin loikka” -projektin alullepanijoina olivat Toomas Hendrik Ilves (tuolloin Viron USA:n suurlähettiläs), opetusministeri Jaak Aaviksoo ja presidentti Lennart Meri.[47]

Digitalisaatiokehitykseen panostaminen realisoitui vuonna 2007 Venäjän provosoiduttua Viron suunnitelmista siirtää venäläisen toisen maailmansodan muistomerkin ja venäläisten sotilaiden hautoja. Venäjä kosti tämän hajautetuilla palvelunestohyökkäyksillä valtion virastoihin ja rahoituslaitoksiin sekä häiritsi viestintää (27.4.–18.5.2007).[48]

Palvelunestohyökkäysten seurauksena Viron viranomaispalvelut olivat jonkin aikaa kokonaan poissa käytöstä. Tämä vahvisti havaintoa siitä, että on tärkeää varmistaa valtion digitaalinen jatkuvuus ja kriittisten palveluiden saatavuus kaikissa tilanteissa. Tänä päivänä nykyisten runkoverkon nopeuksien ja DDoS-suojausten ansiosta minkään valtion ei varmastikaan tarvitsisi enää irtautua verkosta. Viron tapahtumat olivat kuitenkin lähtölaukaus monelle teknologialle, joka on tullut sen jälkeen suojaamaan vastaavalta. Esimerkiksi Viro on systemaattisesti kehittänyt e-Estonia-palvelua (tunnetaan myös nimillä: e-Eesti tai e-Viro), joka tarkoittaa Viron yhteistä digitaalista valtiota ja yhteiskuntaa. Siinä kaikki yhteiskunnan palvelut ovat saatavissa samasta sähköisestä järjestelmästä, joka toimii henkilökortin avulla. e-Estonia on kehityksessään saavuttanut tilanteen, jossa keskeiset ja kriittisiksi määritellyt rekisterit (esim. maarekisteri, maanomistusrekisteri) ovat olemassa vain digitaalisessa muodossa.[49]

Krimin miehityksen (2014) jälkeen Viro on jatkanut maantieteestä irrottautumista kehittämällä ”datasuurlähetystö”-toimintamallia, jossa e-Estonia säilyy olemassa, vaikka fyysinen valtioalue miehitettäisiin. Vuonna 2015 Viro lähti yhdessä Microsoftin kanssa etsimään ratkaisua fyysisten rajojensa ulkopuolelta turvatakseen kriittisen informaationsa sotilaallisen hyökkäyksen

[42] Tarkempi suomenkielinen kuvaus: Kukkola 2021, 153-159; Lisätietoja ks. myös: Kukkola, J. (2020): *Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas.* National Defence University, Series 1: Research Publications no. 40, Helsinki.

[43] DDoS (*Distributed Denial of Service*) eli hajautettu palvelunestohyökkäys, joka toteutetaan yhtä aikaa useista eri lähteistä. Hajautettuun palvelunestohyökkäykseen käytetään usein bottiverkkoa (kaapatuista tietokoneista muodostuva verkko, jota sen haltija käyttää huomaamattomasti haitallisiin tai laittomiin tarkoituksiin). Palvelunestohyökkäysten tavoitteena on kuormittaa ja siten lamaannuttaa jokin palvelu tai tietojärjestelmä. Kyberturvallisuuden sanasto 2018, *s.v. palvelunestohyökkäys*. *Kyberturvallisuuden sanasto* (2018): (online): https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf (luettu 13.2.2023).

[44] Ks. esim. Robinson, N. & Hardy, A. (2021): Estonia: From the “Bronze Night” to cybersecurity pioneer. *Routledge Companion to Global Cyber-Security Strategy*, Scott N Romaniuk & Mary Manjikian (toim.). Routledge: New York, 211-225; Robbins, M. (2019): *Myths, Values and Digital Transformation: The Exceptional Case of Estonia*. The Institute on Governance, 8.5.2018; Budnitsky, S. (2022): A Relational Approach to Digital Sovereignty: e-Estonia Between Russia and the West, *International Journal of Communication*, 16(2022), 1918–1939.

[45] https://taltech.ee/

[46] Ks. esim. Susiluoto, I. (2006): *Suuruuden laskuoppi. Venäläisen tietoyhteiskunnan synty ja kehitys*. WSOY: Helsinki.

[47] Kattel, R. & Mergel, I. (2019): Estonia’s Digital Transformation. Mission Mystique and the Hiding Hand. *Great Policy Success*, Mallory E. Compton & Paul Hart (toim.). Oxford University Press: Oxford.

[48] ibid.

[49] ibid.

tai muun suuren hätätilanteen varalta.[50] Viro halusi sen tietojen olevan täysin omassa hallinnassaan ja toimivallan alaisuudessa, joten se valitsi toimintamallikseen ns. ”datasuurlähetystön” kehittämisen.

Viron ”datasuurlähetystö”-toimintamalli on kohtalaisen innovatiivinen ja ainutlaatuinen lähestymistapa valtion jatkuvuuden turvaamiseksi. Ideaa ”datasuurlähetystöstä” muokkasivat ja kehittivät lopulliseen muotoonsa hallituksen tietohallintojohtaja Taavi Kotka ja Tallinnan teknillisen yliopiston apulaisprofessori Innar Liiv. ”Datasuurlähetystöön” ei liity suurlähettiläitä tai diplomaattisia edustustoja, vaan se tarkoittaa Tier 4 -tason[51] datakeskusta (konesalia). Toisin kuin tavanomaisessa suurlähetystössä, ”datasuurlähetystö” ei ole muuta kuin huone täynnä palvelimia, joissa säilytettään tietoja, jotka ovat välttämättömiä Viron hallituksen ja sen keskeisten julkisten palveluiden ylläpitämiseksi, jos maan pääpalvelimet tuhoutuisivat kotimaassa. ”Datasuurlähetystö” ei siis ole suurlähetystö perinteisessä mielessä, mutta sen perustamissopimuksessa viitataan diplomaattisia suhteita koskevaan Wienin yleissopimukseen. Datasuurlähetystö on kansainvälisen oikeuden piirissä täysin uusi asia. Datasuurlähetystö on täysin Viron valtion hallinnassa eli sillä on täysin samat oikeudet kuin fyysisillä suurlähetystöillä (valtioalueen koskemattomuus). Viron perustama ”datasuurlähetystö” sijaitsee Luxemburgissa.[52]

Kesäkuussa 2017 Viron pääministeri Jüri Ratas ja Luxemburgin pääministeri Xavier Better allekirjoittivat Viron ja Luxemburgin hallitusten välisen kahdenvälisen sopimuksen, jonka tarkoituksena oli varmistaa Luxemburgin valtion omistamaan datakeskukseen tallennettujen tietojen ja järjestelmien koskemattomuus. Tähän, maailman ensimmäiseen ”datasuurlähetystöön”, sijoitettiin ”keskeiset tiedot ja kriittiset tietokannat” (maarekisteri, väestörekiseri, yritysrekisteri ja valtion virallinen lehti sekä ”muita valtion toiminnan kannalta kriittisiä tietojärjestelmiä”) Viron valtion toiminnan jatkuvuuden varmistamiseksi.[53]

Viron ”datasuurlähetystö” on kansainvälispoliittinen ennakkotapaus ja merkittävä hanke ”maantieteestä vapautumiseksi”. ”Datasuurlähetystö”-hankkeen myötä kaksi maata sopi ensimmäistä kertaa maailmassa kahdenvälisesti diplomaattisia suhteita koskevan Wienin yleissopimuksen laajentamisesta koskemaan myös tietojen ja tietojärjestelmien isännöintiä. ”Datasuurlähetystö” on myös teknisesti kiinnostava hanke. Herää kuitenkin kysymys miten toimipaikkojen välille rakennetaan toimiva yhteys ja tietojen tasausratkaisu, joilla estetään tietojen häviäminen yhteyden katketessa (luotettavuuden, eheyden, saatavuuden varmistaminen) sekä miten rekisterimerkinnät ja niiden järjestys voidaan säilyttää ja todistaa. Mahdolliset haasteet ovat siis sekä juridisia että teknisiä.

## Georgia: kyberhistorian ensimmäinen valtion palveluiden ja informaation siirto valtioalueen ulkopuolelle kriisitilanteessa

Viron esimerkki kuvaa hyvin nykyaikaista korkean tason varautumista valtion jatkuvuuden turvaamiseen ”digitaalisella valtioalueella”. Vastaavasti Georgian vuoden 2008, jo kyberhistoriaan kuuluva, tapaus kuvaa ”kotikutoista” valtion palveluiden ja informaation siirtoa valtio-alueen ulkopuolelle kriisitilanteessa. Georgian tapahtumat ovat kuitenkin hyvä muistutus siitä, että hätätilanteessa saatetaan joutua tekemään hyvinkin luovia ja nopeita ratkaisuja.

Heinäkuussa 2008 alkoi tulla ensimmäisiä raportteja Georgian internetsivustoihin kohdistuvista palvelunestohyökkäyksistä. Elokuussa 2008 havaittiin vielä laajempia palvelunestohyökkäyksiä georgialaisia verkkosivuja vastaan, jotka näyttivät tapahtuvan samaan aikaan Venäjän joukkojen siirtymisen kanssa Etelä-Ossetiassa vastauksena Georgian sotilasoperaatioihin, jotka käynnistettiin alueella päivää aiemmin. Muutaman päivän päästä palvelunestohyökkäykset olivat tehneet useimmat Georgian hallituksen verkkosivut toimintakyvyttömiksi. Hyökkäysten seurauksena Georgian hallitus joutui toimimaan ilman verkkoyhteyksiä, eikä pystynyt juuri kommunikoimaan internetissä.[54] Hyökkäykset rajoittivat merkittävästi hallituksen kykyä reagoida tapahtumiin ja yhteydenpitoa ulkomaisiin hallituksiin, mikä heikensi merkittävästi Georgian hallituksen asemaa ja loi Venäjälle aikaa ja tilaa muokata konfliktin kansainvälistä kertomusta. Tapahtuma mainitaan usein yhtenä ensimmäisistä esimerkeistä siitä, että Venäjän kyberhyökkäykset (informaatioteknologinen vaikuttaminen) ovat sotilasoperaatioon liittyvän informaatiovaikuttamisen (informaatiopsykologisen vaikuttamisen) tukemista.[55]

Kyberhyökkäykset aiheuttivat lopulta vain vähän vahinkoa, sillä suurinta osaa Georgian taloudesta ja kriittisestä infrastruktuurista ei ollut vielä vuonna 2008 integroitu internetiin. Siitä huolimatta nationalististen hakkeriaktivistien (haktivistien) kampanja, jota kannustettiin toimintaan venäläisten online-hakkerifoorumien avulla, häiritsi tehokkaasti Georgian hallituksen tiedon levittämistä konfliktin ratkaisevassa vaiheessa.[56] Venäjä on käyttänyt ns. mobilisoituja haktivisteja myös Ukrainassa[57].

Vastauksena kyberhyökkäyksiin Georgian hallitus ryhtyi moniin epätavanomaisiin toimenpiteisiin. Georgian hallitus haki ”kyberturvapaikkaa” Yhdysvalloista, mutta ei saanut sille Yhdysvaltain hallituksen hyväksyntää. Google kuitenkin suostui yhteistyöhön, ja Googlen luvalla Georgian ulkoministeriön sivut ja Civil.ge siirrettiin osaksi Blogspot-verkkopalvelua[58]. Atlantassa Yhdysvalloissa toimiva internetpalveluntarjoaja Tulip Systems

[50] Vuonna 2015 Microsoft ja Viro tekivät yhteistyötä Virtual Data Embassy -tutkimushankkeessa, jossa tutkittiin, miten julkisen ja yksityisen sektorin kumppanuus voisi tukea Viron hallituksen pilvipolitiikan tavoitteita. Lisätietoja Microsoftin sivuilta: https://www.microsoft.com/en-us/cybersecurity/content-hub/implementation-of-the-virtual-data-embassy-solution ja hankkeen white paper: Estonian Ministry of Economic Affairs and Microsoft Corporation (2015): *Implementation of the Virtual Data Embassy Solution. Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation* (online): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmcb (luettu 27.4.2023).

[51] Tier 4 eli korkein datakeskusten turvataso. Tier 4 -taso takaa konesalin toiminnan suurienkin sähkönjakelun ja virtalähteiden vikojen aikana, kaikki verkkolaitteet, virtajärjestelmät, yhteydet kahdennettu jne.

[52] E-Estonia (2020): *Data Embassy. Factsheet*. E-Estonia 2020 (online): https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-data-embassy.pdf (luettu 23.4.2023).

[53] OECD (2018): *Establishing the first Data Embassy in the world*. OECD (online): https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf (luettu 23.4.2023).

[54] Tiivistetty esitys tapahtumista. Georgian vuoden 2008 kybertapahtumia on kuvattu tarkasti ja analysoitu laajemmin monessa tutkimuksessa, ks. esim. Korns, S.W. & Kastenberg, J.E. (2008): Georgia's Cyber Left Hook. The US Army War College Quarterly: Parameters, 38/4, 60-76, (online): https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2455&context=parameters (luettu 28.2.2023); Tikk & al. (2010): *International Cyber Incidents: Legal Considerations*. CCDCOE: Tallinn, 66-90; Abaimov, S. & Martellini, M. (2020): *Cyber Arms: Security in Cyberspace*. CRC Press.: Milton.

[55] ibid.

[56] Abaimov & Martellini 2020.

[57] Kukkola, J. (tulossa 2024): *Suvereenit hiekkamadot. Venäjän kybertoiminta osana valtioiden välistä kamppailua eilen, tänään ja huomenna.* MPKK. Sotataidon laitos. Julkaisusarja 2: Tutkimusselosteita.

[58] Bloggerista puhuttaessa käytetään usein termiä Blogspot, koska Bloggerissa luotujen blogien osoitteet ovat blogspot.com päätteisiä. (Blogspot.com on siis verkkotunnus ja sen alle luodut blogit/sivustot ovat

Inc., jonka omistaa georgialaissyntyinen Nino Doijashvili, alkoi isännöidä Georgian presidentin verkkosivustoa. Tarinan mukaan Doijashvili oli lomalla Georgiassa ja tilanteen vakavuuden huomattuaan hän otti yhteyttä Georgian hallituksen virkamiehiin ja tarjosi apua Georgian internetominaisuuksien palauttamisessa ja palvelimiaan ”suojellakseen” Georgian valtion internetsivustoja haitalliselta liikenteeltä. Päivää myöhemmin Georgian hallitus siirsi kriittisiä kybervalmiuksia ko. yrityksen Yhdysvalloissa sijaitseville palvelimille, mukaan lukien Georgian presidentin ja puolustusministeriön verkkosivustot. Vastaavasti Puolan presidentti Lech Kaczynski tarjosi solidaarisuuden eleenä Georgian hallituksen virallisille lehdistötiedotteille julkaisutilaa verkkosivuillaan. Myös Viro oli mukana auttamassa Georgiaa. Viron hallitus antoi merkittävää apua sijoittamalla Georgian ulkoasiainministeriön verkkosivuston virolaiselle palvelimelle ja lähettämällä kaksi kokemus- ja tietoturva-asiantuntijaa vahvistamaan Georgian kyberpuolustusta.[59] Georgian tapauksessa AS-alueiden ja runkoreitityksen tasolla ei tehty mitään, vaan muutokset tehtiin nimipalvelun tasolla, jotta civil.ge ohjautui amerikkalaisille palvelimille.

Georgian tapaus on esimerkki paniikinomaisesta, kotikutoisesta, yksittäisten henkilöiden organisoimasta valtion kyberterritorion kyberpuolustuksesta, mutta kuitenkin eräänlainen kyberhistorian ennakkotapaus valtion kriittisen informaation ja/tai palveluiden evakuoinnista ulkomaille kriisitilanteessa ja näin ainakin todellisesta yrityksestä ”vapautua maantieteestä”.

## Ukraina: pilvipalvelusiirtymä kriisitilanteessa

Marraskuussa 2022 Ukraina ilmoitti siirtäneensä valtion kriittistä informaatiota[60] kaupalliseen Amazon Web Services -pilvipalveluun (AWS)[61]. Julkisen kertomuksen mukaan datakeskus, jossa Ukrainan hallitus säilytti kaikkia ”varmuuskopiotaan kansalaisten ja eri instituutioiden tiedoista”[62] oli yksi Venäjän ohjusiskujen ensimmäisistä kohteista sodan laajentuessa[63]. Kertomukseen sopiva ohjusisku on tapahtunut Harkovassa maaliskuun 2022 alussa. Iskussa vaurioitui MAXNET-palveluntarjoajan datakeskus, joka oli yksi Ukrainan suurimmista ja jolla oli runsaasti viranomais- ja yritysasiakkaita.[64] Tarinan mukaan tapahtumakulkuun oli varauduttu ja toimenpiteisiin oli ryhdytty voimassaolevan datalokalisaatiolainsäädännön[65] muuttamiseksi.

Todennäköisesti Ukraina alkoi jollain tasolla valmistella valtion kriittisen informaation pilvipalvelusiirtoa Venäjän vallattua Krimin ja osia Itä-Ukrainasta vuonna 2014. Varsinainen pilvipalvelusiirtymisen mahdollistava lainsäädännöllinen valmistelu alkoi kuitenkin vasta vuonna 2019[66] ja saatiin ja saatiin hyväksyttyä juuri ennen Venäjän laajentaman hyökkäyksen alkua (17.2.2022). Ukrainan presidentti Volodymyr Zelenskyi allekirjoitti lain 15.3.2022 ja se astui voimaan puolen vuoden päästä allekirjoituksesta 16.9.2022.[67] Ukrainan sotatilan aikana voimassa oleva lainsäädäntö mahdollisti pilvipalveluiden käytön Ukrainan valtioalueen ulkopuolella maaliskuusta 2022 lähtien.[68] Ukrainan pilvipalvelusiirtymä jouduttiin siis suorittamaan käytännössä suhteellisen nopeana datan evakuointitoimenpiteenä kriisitilanteessa sotatilalain suomin valtuuksin, vaikka lainsäädäntöä ja siirtoa oli alettu valmistelemaan jo muutamaa vuotta aikaisemmin.

Pilvipalvelulain valmistelun aikaisia lausuntoja tarkastelemalla[69] näyttää siltä, että kaupallinen toimija (Amazonin AWS-pilvipalvelu) oli voimakkaasti mukana valmistelutyössä. Ukrainan tapaus osoittaa, kuinka hidasta valtion kriittisen informaation siirtäminen todellisuudessa on – lainsäädännöllisestä valmistelusta itse fyysiseen siirto-operaatioon ja sen jälkeen datan käytettävyyden (luotettavuuden ja eheyden) varmistamiseen sekä yhteyksien turvaamiseen. Julkisten lähteiden perusteella on mahdotonta sanoa, kuinka kauan aikaa tässä operaatiossa on todellisuudessa kulunut ja onko se jo päättynyt. Datan sijainti ennen lain voimaantuloa ei myöskään ole tiedossa

Viron tavoin Ukraina on myös kehittänyt voimakkaasti valtion sähköisiä palveluja. Vuodesta 2020 Ukrainassa kaikki valtion palvelut ja asiakirjat ovat olleet saatavilla yhdestä sovelluksesta. Tiedon saatavuus on Ukrainassa ratkaistu omalla Dija[70] -sovelluksella (Дія – lyhenne sanoista Держава і я eli – ”Valtio ja minä”).[71] Dija-sovelluksella on samankaltaisuuksia Viron e-Estonia-ratkaisun kanssa ja näitä onkin kehitetty yhdessä.[72]

Ukrainassa on myös kymmeniä erilaisia Ukrainan valtion ja vapaaehtoisten kehittämiä sotilaskäyttöön tarkoitettuja pilvipalvelusovelluksia (esim. Delta, Kropiva, GisArta, Trivoga). Oletettavasti kyseisillä sovelluksilla käsitellään sellaista turvaluokiteltua tietoa, jonka käyttäminen ja tallentaminen Ukrainan valtioalueen ulkopuolella ei Ukrainan pilvipalvelulain mukaan ole sallittua. Näitä sovelluksia käytetään kuitenkin Ukrainassa pilvipalveluteknologian avulla.

Ukraina on siis todennäköisesti siirtänyt julkiset ja kansalaisia koskevat palvelut pilvipalveluun Ukrainan fyysisen valtioalueen

ko. verkkotunnuksen alidomaineja, joita blogger-blogit voivat käyttää ilmaiseksi, kunhan haluttu alidomain on vapaa.)

[59] ibid.

[60] On huomautettava, että missään asiaa koskevassa virallisessa asiakirjassa tai julkaisussa ei ole täysin yksiselitteisesti määritelty mitä ”valtion kriittinen informaatio” tarkasti tarkoittaa tai mitä palveluita se ukrainalaisen määritelmän mukaan pitää sisällään.

[61] AWS, Amazon Web Services eli kokoelma etätietojenkäsittelyresurssien palveluja, jotka muodostavat yhdessä Amazon.comin kautta tarjottavan pilvipalvelualustan.

[62] Data Center Map:n mukaan Ukrainassa on 34 datakeskusta. *Ukraine Data Centers* (2023): (online): https://www.datacentermap.com/ukraine/ (luettu 1.3.2023).

[63] Amazon (2022): Ukraine minister on how technology is helping his people plan for the future. *About Amazon* (30.12.2022) (online): https://www.aboutamazon.com/news/aws/aws-reinvent-2022 (luettu 1.3.2023); Schweizer, P. (2022): How the Conflict in Ukraine Could Impact Datacenters. *Blog: Eyes on the Future of IT & Business Trends* (14.4.2022) (online): https://blog.451alliance.com/how-the-conflict-in-ukraine-could-impact-datacenters/ (luettu 1.3.2023).

[64] Ballard, M. (2022): Battle Intensifies to Keep Ukraine Online. *Data Center Knowledge*, 11.3.2022 (online): https://www.datacenterknowledge.com/networks/battle-intensifies-keep-ukraine-online (luettu 7.3.2023).

[65] Datalokalisaatio viittaa käytäntöihin, joissa dataa tallennetaan, käsitellään ja hallitaan tietyllä maantieteellisellä alueella. Esim. lainsäädännössä voidaan määritellä, että tietyntyyppinen data on säilytettävä fyysisesti tietyn maan tai alueen palvelimilla tai missä dataa voidaan käsitellä tai siirtää.

[66] *Проект Закону про хмарні послуги* (2019): (online) https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=2655&conv=9 (luettu 17.2.2023).

[67] *Закон України: ”Про хмарні послуги”* (2022): (online): https://zakon.rada.gov.ua/laws/show/2075-20#Text (luettu 17.2.2023).

[68] *Закон України: Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів* (2022): (online): https://zakon.rada.gov.ua/laws/show/2130-20/print (luettu 17.2.2023).

[69] *Пояснювальна записка* (2019): 27.12.2019 (online): https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=2655&conv=9 (luettu 23.2.2023).

[70] Huom. Dija-sanan translitterointi on erilainen riippuen eri kielissä käytettävästä translitterointitavasta eli я -kirjain voidaan translitteroida ainakin ”ia”, ”ya” tai ”ja” (vrt. Diia, Diya, Dija).

[71] Dija-portaalin kotisivu: https://diia.gov.ua/

[72] Fedorov, M. (2023): Ukrainalainen Julia Ovtšarenko, 28, todistaa henkilöllisyytensä kännykkänsä avulla – ”Jos tällainen palvelu tulisi Euroopan maihin, ihmiset olisivat paljon onnellisempia”. *Yle* (online): https://yle.fi/a/74-20019297 (luettu 23.2.2023).

ulkopuolelle, mutta säilyttänyt turvaluokitellut materiaalit ja sotilassovellukset fyysisesti Ukrainassa eli Ukraina on osittain pilvessä, mutta osittain pilvipalvelut sijaitsevat Ukrainassa (vrt. ero pilvipalveluiden ja pilvipalveluteknologian käytön välillä).

Ukrainan kriittisen informaation evakuointi ja käyttö kaupallisessa pilvipalvelussa tähtäävät kansalaisten näkökulmasta yhteiskunnan kriittisten palveluiden turvaamiseen. Ukraina on siis tehnyt omanlaisiaan ratkaisuja ”maantieteestä vapautumiseksi”.

## Mahdammeko maantieteelle jotain?

Venäjä vetoaa voimakkaasti fyysiseen maantieteeseen ja uhoaa rajojensa olevan loppumattomat. Toisaalta Putinin ”Venäjän rajat eivät pääty mihinkään” -lausahdusta voi myös tulkita syvemmin ja pohtia viittaako hän todellisuudessa nimenomaan ”rajattomaan” ja uusia vaikutusmahdollisuuksia avaavaan informaatio- ja kybertilaan. Venäjän suoraa sotilaallista hyökkäystä Nato-maahan pidetään epätodennäköisenä, jolloin vaihtoehtoisten laaja-alaisten vaikutusoperaatioiden mahdollisuus ei-fyysisissä toimintaympäristöissä vastaavasti todennäköisesti kasvaa. Venäjä toimii aktiivisesti informaatio- ja kybertilassa edistääkseen poliittisia päämääriään. Venäjä on kokeillut rajojensa uudelleenmäärittelyä kehittämällä uudenlaisia toimintatapoja sekä informaatiopsykologiseen että informaatioteknologiseen valloitukseen ja alueiden haltuunottoon. Venäjän tässä onnistuessaan tulevaisuuden kamppailu valtioiden itsemääräämisoikeudesta voidaan mahdollisesti ulottaa ja pakottaa informaatio- ja kybertilaan. Valtion voi edellä esitetyillä toimenpiteillä mahdollisesti eristää ja/tai ottaa hallintaan informaatio- ja kybertilassa, mutta voiko valtion tai kansakunnan jo tuhota kokonaan informaatio- ja/tai kybertilassa on kysymys, jota on syytä pohtia. Esitetyt esimerkkitapaukset osoittavat Venäjän ainakin keränneen kokemusta tämän tyyppisestä vaikuttamisesta. Venäjän suorittamat informaatiopsykologiset ja informaatioteknologiset operaatiot voivat tukea merkittävästi myös fyysisen valtioalueen haltuunottoa aseellisesti tai ilman eli haltuun otetun maan ja/tai alueen toimintakyvyn lamauttamista ja omien toimintojen mahdollistamista.

Venäjän naapurimaat ovat vuosien saatossa tiedostaneet maantieteelliset realiteetit ja monet valtiot ovat myös ryhtyneet kehittämään toimenpiteitä ”maantieteestä vapautumiseksi”. Tässä tutkimuskatsauksessa esitettiin Viron, Georgian ja Ukrainan erilaisten toimenpiteiden kokonaisuutta, joilla nämä ovat eri aikoina ja erilaisissa tilanteissa pyrkineet turvaamaan ainakin toiminta- ja viestintäkykykynsä fyysisen maantieteellisen sijainnin ulkopuolella. Osa esitellyistä toimista on tapahtunut hetkessä hätäratkaisuna, mutta osaa on myös suunniteltu ja valmisteltu pidemmän aikaa. Ensisijaisesti tässä työssä on tarvittu luovaa ja uudenlaista ajattelua. Venäjällä on ollut tahto ja kyky informaatiopsykologiseen ja informaatiotekniseen vaikuttamiseen, mutta tätä ei ole laajasti tunnistettu. Mahdollisesti siksi kohteet ovat joutuneet reagoimaan yllättäviin tilanteisiin.

Informaatioajassa Venäjän naapurimaiden ”maantieteestä vapautuminen” on valtion olemassaolon turvaamiseen ja jatkuvuuden hallintaan liittyviä toimenpiteitä informaatio- ja kybertilassa ”digitaalisella valtioalueella”. Joissain tapauksissa valtioalueen laajentaminen fyysisen valtioalueen ulkopuolelle voi olla ainoa tai paras keino suojautua. Toisaalta on hyvä pohtia, mitkä ovat niitä tekijöitä, jotka vaikuttavat siirtämisen sijasta maantieteellisen aseman vahvistamiseen. Olisi hyvä tunnistaa ne tekijät, jotka mahdollistavat ulkopuolelle suojautumisen tai toisaalta taas maantieteellisen aseman vahvistamisen. Valtioiden välille on luotava erilaisia toimintamalleja, joita pitää myös hyvin konkreettisesti harjoitella. Vähintään voidaan sanoa, että tulevaisuuden informaatio- ja kyberpuolustus on – tai ainakin pitäisi olla – muutoksessa.

## Kiitokset

Haluan kiittää Puolustusvoimien tutkimuslaitoksen Informaatiotekniikkaosaston Johtamisjärjestelmien tutkimusalan tutkimusalajohtaja, insinöörimajuri Uula-Petteri Purojärveä katsauksen alkuperäisestä ”maantieteestä vapautumisen” ideasta ja taustamateriaalin hankinnasta. Haluan myös kiittää luonnosversiota kommentoineita MPKK:n ja PVTUTKL:n Informaatiotekniikka- ja Doktriiniosaston tutkijoita tarkoista huomioista ja korjauksista, jotka paransivat katsausta merkittävästi.

## Lisätietoja

*FT, vanhempi tutkija Mari Ristolainen (p. 0299 800) on Puolustusvoimien tutkimuslaitoksen Informaatiotekniikkaosaston Kyberpuolustus tutkimusalan tutkija.*