Puolustusvoimien tutkimuslaitos
Tutkimuskatsaus 1 – 2021

19.11.2021

Softaa kyberrajalle!

Katsaus kybertilan valtioalueellistamisprosessiin meillä ja maailmalla

Vanhempi tutkija Mari Ristolainen
Informaatiotekniikkaosasto

Nykymuotoinen globaali kybertila on todennäköisesti tulevaisuudessa toisenlainen, mutta toistaiseksi ei ole olemassa yhtä yhtenäistä käsitystä millaiseksi se on muotoutumassa. Kybertilaan on alkanut kohdistua kansallisvaltioiden valtarakenteita muistuttavia ilmiötä ja yrityksiä kontrolloida globaaleja informaatiovirtoja. Valtioiden intresseissä on pitää oma kansallinen kybertilansa koskemattomana ja omien kansallisten järjestelmien suojelu erilaisilla teknisillä ja hallinnollisilla keinoilla. Syyskuussa 2021 julkaistussa Puolustusselonteossa puolustusvalmiuteen kohdistuvat vaatimukset ulotettiin myös kybertilaan, mikä heijastelee kybertilan valtioalueellistamisprosessia ja halua kansallisen kybertilan puolustusvoimalliseen hallintaan. Tämän tutkimuskatsauksen tavoitteena on selvittää kybertilan valtioalueellistamisprosessiin vaikuttavia taustatekijöitä ja meneillään olevia toimia sekä arvioida mahdollisia kehityskulkuja. Näiden lisäksi katsauksessa nostetaan esille ratkaistavia kysymyksiä käsitemäärittelyistä toimintamahdollisuuksiin ja -valtuuksiin, jotka vaikuttavat kyberpuolustukseen ja todennäköisesti myös Puolustusvoimien toimintaan tulevaisuudessa. Tutkimuskatsaus liittyy laajempaan kybertilan tulevaisuusnäkymiä analysoivaan tutkimuskokonaisuuteen, joka toteutetaan Puolustusvoimien tutkimuslaitoksen Informaatiotekniikkaosastolla vuosina 2021–2024.

Johdanto

Globaalin internetin tarkoituksena oli alun perin yksinkertaisesti yhdistää maantieteellisesti eristetyt intranetit yhdeksi verkkojen verkoksi. Idealistisesti globaalin tietoverkon haluttiin häivyttävän maantieteelliset alueet, rajat sekä valtiokontrollin ja muodostavan maailmanlaajuisen yhteiskäyttöisen toimintaympäristön (*global commons*), jossa data liikkuu ja varastoituu vapaasti valtioalueiden yli ja/tai niistä riippumatta.[1] Tässä niin kutsutussa "deterritorialisaatioprosessissa" verkkojen verkosta kehittyi valtioiden territoriaalisesta (fyysiseen alueeseen sidotusta) tilasta (valtioalueesta) ulkopuolinen tila, joka on toisaalta keskinäisriippuvainen ja yhteen sulautunut, mutta myös monimutkainen, osittain päällekkäinen ja sekava yhdistelmä julkisia ja yksityisiä palveluja sekä kriittisiä toimintoja, joita käyttävät kaikki turvallisuusviranomaisista yksittäisiin kansalaisiin.

Idealistisista tavoitteista huolimatta, kybertilan[2] hallinnasta ja valvonnasta on keskusteltu jo 1980-luvulta lähtien[3]. Pääasiallisena julkilausuttuna tavoitteena on ollut löytää keinoja kybertilan vakauden ja turvallisuuden takaamiseksi. Karkeasti keskustelu kybertilan hallinnasta ja valvonnasta voidaan jakaa monitoimijamallin (*multistakeholder*) ja valtiojohtoisen hallintamallin (*multilateral*) puolestapuhujiin. YK:n piirissä käydyissä keskusteluissa on välillä edetty yksi askel eteen ja sitten kaksi taaksepäin. Kybertilan tulevaisuuden kehitystä arvioitaessa on jo pitkään myös puhuttu kybertilan pirstaloitumisesta eli hajoamisesta (fragmentaatio) ja/tai murtumisesta osiin (balkanisaatio).[4] Näkökulmasta hieman riippuen, globaalin kybertilan pirstaloituminen on nähty nopeana tai hitaampana, mutta kuitenkin lähes väistämättömänä kehityksenä. Pirstaloituminen jaetaan yleisesti kolmeen erilaiseen kehityskulkuun.[5] Tekninen pirstaloituminen liittyy internetin infrastruktuurin kehittymiseen, joka vaikuttaa laitteiden yhteentoimivuuteen ja datan liikkuvuuteen. Valtiollinen pirstaloituminen käsittää kaikki valtioiden toimet, jotka rajoittavat tai estävät pääsyn internetiin ja kontrolloivat datan liikkuvuutta. Kaupallinen pirstaloituminen pitää sisällään erilaisten kaupallisten toimijoiden internetin käyttöä ja datan liikkuvuutta estävät tai haittaavat toimenpiteet.[6] Kaikki pirstaloitumiseen liittyvät kehityskulut palvelevat jonkun toimijan intressejä, mutta on myös esitetty, että koko pirstaloitumiskeskustelun varsinainen tavoite on alistaa internet valtiollisille lainsäädännöille ja luoda kybertilaan kansallisvaltioiden valtarakenteita[7] ja tukahduttaa internetin luomat globaalit informaatiovirrat.[8] Tätä kehitystä voi yleisesti nimittää kybertilan valtioalueellistamisprosessiksi (tai territorialisaatioprosessiksi, *territorialisation*) – prosessin lopputulosta "kyberoituneeksi westfaaliseksi aikakaudeksi"[9] (*cybered Westpahalian age*)[10].

[1] Kehityksestä saa kattavan kuvan lukemalla aikalaisia akateemisia kirjoituksia, joissa pohditaan miten kansallisvaltiot, niiden lainsäädäntö ja rajat häviävät globaalin verkon paineessa. Ks. esim. *Borders in Cyberspace: information policy and the global information infrastructure* (1997): edited by Brian Kahin and Charles Nesson. The MIT Press, Cambridge, Massachusetts, and London, England; Goldsmith, J. & Wu, T. (2006): *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, New York.

[2] 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 elektromagneettisen spektrin käyttämiseen informaation luomiseksi, muokkaamiseksi, vaihtamiseksi ja hyödyntämiseksi toisiinsa liitettyjen informaatioteknologiaa käyttävien verkkojen kautta. Korostettaessa kybertilan luonnetta nimenomaan *toiminnan* ympäristönä käytetään käsiteitä *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, Juha (2021): *Rakenteellisen kyberasymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä*. Puolustusvoimien tutkimuslaitoksen julkaisuja 13: Riihimäki.

[3] Ks. esim. Radu, Roxana (2019): *Negotiating Internet Governance*. Oxford Scholarship Online.

[4] Muller, Milton (2017): *Will the Internet Fragment?* Polity Press, Cambridge.

[5] Drake, William J., Cerf, Vinton G. & Kleinwächter, Wolfgang (2016): *Internet Fragmentation: An Overview*. Future of the Internet Initiative White Paper. World Economic Forum (online): https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (luettu 12.10.2021).

[6] ibid.

[7] Valtarakenteilla viitataan tässä Motevideon yleissopimuksen (1933) määritelmään valtion tunnusmerkeistä eli pysyvä väestö, rajattu alue, hallitus ja kyky solmia suhteita muiden valtioiden kanssa.

[8] Muller (2017), 18-19.

[9] Suomennos: Kukkola 2021, 16.

[10] Demchak, C. & Dombrowski, P. (2011): Rise of the Cybered Westphalian Age. *Strategic Studies Quarterly*, 5(1), 32-61; Demchak, C. & Dombrowski, P. (2013): Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs,* Volume International Engagement on Cyber III, 29-38.

Tämän tutkimuskatsauksen tavoitteena on aluksi taustoittaa kybertilan valtioalueellistamisprosessia avaamalla erilaisten hallintomallien kannattajien näkemyksiä kybertilan hallinnasta sekä tiivistää YK:n piirissä käytyä keskustelua kansainvälisen lainsäädännön soveltamisesta valtioiden toimintaan kybertilassa. Toiseksi tarkastellaan kybertilaan liitettyjä erilaisia suvereniteettikäsityksiä ja kansallisia kannanottoja suvereniteetista kybertilassa. Kolmantena nostetaan esille mahdollisten teknistaloudellisten liittoumien muodostuminen tulevaisuudessa. Näiden lisäksi katsauksessa pohditaan ratkaistavia kysymyksiä käsitemäärittelyistä toimintamahdollisuuksiin ja -valtuuksiin, jotka vaikuttavat kyberpuolustukseen ja todennäköisesti myös Puolustusvoimien toimintaan tulevaisuudessa.

Kybertilan hallintamallit muutoksessa

Kybertilan hallinnasta ja valvonnasta on keskusteltu jo 1980-luvulta lähtien.[11] Pääasiallisena julkilausuttuna tavoitteena on ollut löytää keinoja kybertilan vakauden ja turvallisuuden takaamiseksi. Karkeasti keskustelu kybertilan hallinnasta ja valvonnasta voidaan jakaa monitoimijamallin (*multistakeholder*) ja valtiojohtoisen hallintamallin (*multilateral*) puolestapuhujiin.[12] On kuitenkin syytä huomioida, että keskusteluun vaikuttavat välillisesti myös ylikansalliset yritykset (mm. Google, Alibaba, Yandex) sekä globaalin kansalaisyhteiskunnan verkostot (ml. rikolliset ja ääriliikkeet).

Valtiojohtoisen hallintamallin kannattajat tavoittelevat maiden tai maaryhmien alueellisia tai omia kansallisia internetsegmenttejä ja pyrkivät valtiolliseen suvereniteettiin kybertilassa. Kybertilan kansallisessa ja globaalissa sääntelyssä etusijalla halutaan olevan itsenäiset valtiot ja niiden maantieteelliset rajat. Erityisesti Venäjän ja Kiinan ajamassa mallissa kybertilaan liittyvä päätöksenteko olisi ns. "monenkeskeisellä yhteisöllä" eli esim. ITU:lla (*ITU, International Telecommunication Union* eli YK:n alainen kansainvälinen televiestintäliitto).[13]

Kybertilan globaalia, avoimia ja yhteensopivia järjestelmiä korostava monitoimijamalli taas vastustaa kybertilan aluesidonnaisuutta. Monitoimijamallin kannattajien mukaan kybertilan ei haluta olevan riippuvainen yksittäisten valtioiden hallitusten kontrollista. Pääasiassa USA:n ajamassa monitoimijamallissa kybertilan hallinta on keskitetysti "globaalilla yhteisöllä" tai "sidosryhmien yhteisöllä" eli esim. ICANN:lla (*ICANN, Internet Corporation for Assigned Names and Numbers* eli amerikkalaisella yhtiöllä, joka on oman määritelmänsä mukaan organisoitunut "globaaliksi monitoimijayhteisöksi"). Monitoimijamallin kannattajat vastustavat maiden tai maaryhmien alueellisia tai omia kansallisia internetsegmenttejä ja pyrkivät säilyttämään kybertilan "vapauden ja avoimuuden".[14]

Kybertilan hallinta- ja valvontamallit ovat pohjimmiltaan kansainvälisen oikeuden kysymyksiä, joita ratkotaan YK:n piirissä.[15] Venäjä on vuodesta 1998 ajanut YK:n aseistariisunnan toimisto UNODA:ssa (*UNODA, United Nations Office for Disarmament Affairs*) päätöslauselmaa, jossa kybertilassa pätee kansallinen itsemääräämisoikeus globaalin avoimuuden sijaan. Tällaista päätöslauselmaa ei ole toistaiseksi hyväksytty, mutta vuodesta 2004 hallitusten välinen asiantuntijaryhmä (*GGE, Group of Governmental Experts*)[16] on pyrkinyt muodostamaan kahden vuoden välein kybertilan hallintaan liittyviä konsensusraportteja YK:n yleiskokoukselle hyväksyttäväksi. Raporteissa on analysoitu, miten kansainvälinen lainsäädäntö koskee valtioiden toimintaa kybertilassa ja etsitty kaikkien hyväksymiä tapoja edistää olemassa olevien kybernormien noudattamista.

YK:n yleiskokous vahvisti vuosina 2010, 2013 ja 2015 hallitustenvälisen asiantuntijaryhmän suosituksesta, että kansainvälinen oikeus sääntelee valtioiden toimintaa kyberympäristössä. Samalla vahvistettiin tarve käydä keskustelua siitä, miten kyberympäristön erityiset ominaisuudet kuten nopeus, keskinäisriippuvuus, kompleksisuus ja anonymiteetti vaikuttavat olemassa olevien sääntöjen ja periaatteiden soveltamiseen.[17] Vuoden 2015 päätöslauselmassa muodostettiin vapaaehtoisia, ei-sitovia, normeja valtioiden vastuulliselle käyttäytymiselle kybertilassa. Tämän päätöslauselman jälkeen keskustelut kuitenkin juuttuivat paikoilleen.

Vuonna 2017 hallitusten välinen asiantuntijaryhmä ei kyennyt enää yksimielisesti hyväksymään raporttia ja työ keskeytettiin. Erityiseksi ongelmaksi nousi kansainvälisen lain soveltaminen kybertilassa. Vuonna 2018 YK:n yleiskokous hyväksyi Venäjän ajaman päätöslauselman, jossa päätettiin muodostaa uusi OEWG-työryhmä (*OEWG, Open-Ended Working Group*) analysoimaan GGE-ryhmän aikaisempia raportteja ja normeja, jotta voitaisiin tunnistaa uusia normeja ja tutkia mahdollisuutta muodostaa YK:n alaisen instituution välistä dialogia.[18] Kaiken epäselvyyden nimissä, vuonna 2018 YK:n yleiskokous hyväksyi myös USA:n ajaman päätöslauselman, joka oli osittain ristiriitainen Venäjän ajaman päätöslauselman kanssa. Amerikkalaisten päätöslauselmassa päätettiin perustaa jälleen uusi YK:n hallitustenvälinen asiantuntijaryhmä (GGE) kirjoittamaan yksimielisiä raportteja valtioiden toiminnasta kybertilassa. Uusien perustettujen asiantuntijaryhmien kokoonpanoissa oli kuitenkin merkittäviä eroavaisuuksia. OEWG-ryhmään pääsivät mukaan kaikki YK:n jäsenvaltiot (193), kun taas GGE-ryhmässä on ollut vaihtelevasti mukana 20–25 maata. Myös ryhmien toimintatapaan kirjattiin eroja: OEGW-ryhmä toimii niin kauan, kunnes päästään sopimukseen; GGE-prosessilla on ollut kahden vuoden aikaraja aina kerrallaan.[19]

OEGW-prosessin käynnistyttyä, yksittäiset valtiot katsoivat tarpeelliseksi tuoda julki kansallisia näkemyksiään kansainvälisestä oikeudesta kyberympäristössä – Suomi mukaan lukien.[20] Tässä vaiheessa monitoimijamallin kannattajien keskuudessa alkoi nousta erilaisia kansallisista irtiottoja ja uusia aloitteita liittyen erityisesti valtioiden suvereeniuden periaatteen tuomisesta kybertilaan.[21]

Vaikka alkuperäisen monitoimijamallin kannattajat luottivat edelleen globaalista järjestelmästä lähtevään turvallisuuteen, niin monitoimijamallista alkoi irrottautua mm. eurooppalaisia maita, jotka näkivät, valtiojohtoisen hallintamallin kannattajien mukaisesti, kyberuhkat yhä enemmän kansallisessa viitekehyksessä kuin globaa-

[11] Radu, 2019.
[12] Aiheesta on kirjoitettu paljon, ks. esim. Glen, Carol M. (2014): Internet Governance: Territorializing Cyberspace? *Politics & Policy*, 42(5), 635-657.
[13] Singh, J P (2009): Multilateral Approaches to Deliberating Internet Governance, *Policy & Internet*, 1(1), 91-111.
[14] Strickling, Lawrence E. & Hill, Jonah Force (2017): Multi-stakeholder internet governance: successes and opportunities. *Journal of Cyber Policy*, 2(3), 296-317.
[15] Hyvä suomenkielinen kuvaus prosessista, sen historiasta, erilaisista näkemyksistä: Blomqvist, Aleksi (2021): *Rajanvetoa verkostoissa: Venäjän ja Yhdysvaltojen näkemykset kyberavaruuden järjestyksestä*. Pro-gradu tutkielma, valtio-oppi, Turun yliopisto, kevät 2021. Kattava kuva Venäjän kybertoimista YK:n piirissä: Korzak, Elaine (2021): *Russia's Cyber Policy Efforts in the United Nations*. Tallinn Paper No. 11: CCDCOE.
[16] *Group of Governmental Experts on developments in the Field of Information and Telecommunications in the Context of International Security*, *GGE*. Suomi oli ryhmän jäsen 2016–17.
[17] Ulkoministeriö (2020): *Kansainvälinen oikeus kyberympäristössä: Suomen kansallisia kantoja* (online), https://um.fi/documents/35732/0/KyberkannatPDF-FI.pdf/c69fce1e-5753-3731-0b46-356b8216df51?t=1603097434415 (luettu 11.10.2021).
[18] Ruhl, C., Hollis, D., Hoffman, W. & Maurer, T. (2020): *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads*. Carnegie Endowment for International Peace, February 2020 (online), https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf (luettu 11.10.2021).
[19] ibid.
[20] Ulkoministeriö 2020.
[21] ibid.

lilla tasolla. Alkoi muodostua jonkinlainen osittainen monitoimijamalli, joka pohjautuu nousevaan ns. kybertilan territoriaaliseen maailmanjäsennysmalliin. Kehitykseen vaikuttaa kyberuhkien kohdistuminen valtioiden elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin, taloudelliseen kilpailukykyyn, kansalliseen turvallisuuteen ja kansalaisiin joko suoraan tai välillisesti. Nykyään monien valtioiden intresseissä on pitää oma kansallinen kybertila koskemattomana ja omien kansallisten järjestelmien suojelu. Kybertilan kansallinen kontrolloitavuus ja erilaisten järjestelmien itsenäisen puolustuksen selkeä suunnitelmallisuus lisäävät kyberturvallisuuden tunnetta, jotka taas vastaavasti heijastelevat kybertilan valtiojohtoisen hallintamallin kannattajien alkuperäisiä ajatuksia. Valtioiden pyrkimys vastustaa ylikansallisten yritysten ja kansalaisyhteiskunnan verkostojen sekä rikollisten ja terroristien vaikutusta, vetää myös suurvaltoja yhteen ja tekee valtiojohtoisesta hallintamallista kaikille valtioille houkuttelevan vaihtoehdon.

Kesällä 2021 sekä OEWG-ryhmä että GGE-asiantuntijat pääsivät jonkinlaiseen lopputulokseen.[22] OEWG-ryhmän toimintaa päätettiin jatkaa vielä viidellä vuodella ja ryhmässä saatiin aikaan loppulauselma, jonka sekä USA että Venäjä hyväksyivät.[23] Samoin GGE-asiantuntijat hyväksyivät loppuraportin, joka vahvistettiin YK:n yleiskokouksessa kesällä 2021. GGE-loppuraportti on käytännössä vuoden 2015 raportin toisinto.[24]

Molemmissa loppulauselmissa suvereenisuuden kybertilassa todettiin olevan vain yleinen periaate, josta ei voisi johtaa oikeudellisia seurauksia kyberympäristössä. YK:n toimivaltaa ei myöskään laajennettu. Valtiojohtoisen hallintamallin kannattajat saivat kuitenkin OEWG:n toiminnan pidentämisen kautta laajennettua kybertilan hallintamallikeskustelun koko YK:n tasolle sekä loivat erimielisyyttä alkuperäisen monitoimijamallin kannattajien joukossa ja mahdollisuuden vaikuttaa useamman maan näkökantaan tulevaisuuden kybertilan hallinnasta. Tätä voidaan pitää valtiojohtoisen hallintamallin kannattajien ponnistuksena kasvattaa oman hallintamallinsa laillisuuskapasiteettia, joka viittaa myös suunnitelmalliseen normatiiviseen toimintalinjaan.[25]

Suvereniteetti kybertilassa

Viimeaikaiseen muutokseen kybertilan hallintamalleissa liittyy vahvasti suvereniteetin eli valtion täysvaltaisuuden[26] vaatimus ja halu käyttää klassisia kansainvälisen oikeuden periaatteita eli noudattaa kybertilassa samoja lakeja, jotka määrittävät valtioiden välisiä suhteita fyysisessä maantieteellisessä ympäristössä. Tästä muodostuu kuitenkin määrättyjä ongelmia, koska ns. kansallinenkaan kybertila ei välttämättä noudata valtion fyysisiä rajoja, eikä kansainvälisesti ole yhtenäistä käsitystä mitä suvereniteetti kybertilassa tarkoittaa.

Kybertilaan on liitetty hyvin erilaisia suvereniteettikäsityksiä – usein puhutaan "digitaalisesta suvereniteetista"[27], jolla viitataan toisaalla datan liikkuvuuden kansalliseen säätelyyn eli ns. "datasuvereniteettiin"[28]. Jossain yhteydessä digitaalisen suvereniteetin liittyen saatetaan puhua laajemmasta informaatiosuvereniteetista[29] ja toisaalla digitaalinen suvereniteetti tarkoittaa itsenäistä globaalista verkosta irrotettavaa kansallista internetsegmenttiä.[30] Ei siis ole yhtä yhtenäistä käsitystä mitä suvereniteetti kybertilassa tarkoittaa, vaikka kansainvälisesti käytetään samaa "digitaalisen suvereniteetin" käsitettä. Suomenkieliseen keskusteluun oman vivahteen tuo vielä tunteisiin vetoava käännös "digitaalinen itsenäisyys", jolla on viitattu mm. "kyvykkyyteen toimia digitaalisesti" ja sen turvaamista pidetty osana "modernia maanpuolustusta".[31] Itsenäisyyden rinnalle on myös julkisuudessa nostettu synonyymisia, mutta lähes määrittelemättömiä käsitteitä, kuten esim. "kyberomavaraisuus"[32].

Kuten edellä mainittiin, Suomi oli yksi maista, joka katsoi tarpeelliseksi esittää kansallisen kannanoton suvereniteetin ulottamisesta kybertilaan. Ulkoministeriön lokakuussa 2020 julkaisemassa kannanotossa todetaan, että […] "vaikka kyberympäristö kokonaisuudessaan ei ole minkään valtion vallattavissa, valtiolla on alueellinen toimivalta suhteessa sekä alueellaan sijaitsevaan kyberinfrastruktuurin että siellä kybertoimintoihin osallistuviin henkilöihin"[…].[33] Lausunnossa ei määritellä mitä "kyberinfrastruktuuri" tarkoittaa, mutta lausunto on suora sitaatti Tallinnan manuaalista 2.0, jossa "kyberinfrastuktuurin" määritellään pitävän sisällään "viestintä-, tallennus- ja laskentalaitteet, joiden avulla tietojärjestelmät rakennetaan ja joiden avulla tietojärjestelmät toimivat"[34]. Kärjistetysti, tämän määritelmän mukaan valtiolla on toimivalta kaikkeen alueellaan sijaitsevaan tieto- ja viestintätekniikkaan (ICT, *Information and Communication Technology*), mikä tuskin on tarkoituksenmukaista.

Kannanoton mukaan suvereniteettiin kybertilassa sisältyy fyysisen maantieteellisen valtiorajan sisäpuolella (valtioalueella) oleva "kyberinfrastruktuuri", jossa omistajuus on kuitenkin hajautunut julkishallinnon, elinkeinoelämän, järjestöjen ja yksityishenkilöiden kesken, sekä kansallisesti että kansainvälisesti. Kannanotosta ei käy ilmi kuuluvatko "valtion alueelliseen toimivaltaan" globaaleissa pilvipalveluissa oleva strateginen data ja palvelut, jotka eivät sijaitse fyysisesti ko. valtion alueella. Toisaalta fyysiseen sijaintiin sidotun määritelmän ongelmaksi saattaa myös muodostua se, että fyysisellä valtioalueella saattaa sijaita myös vieraan valtion omistuksessa olevaa "kyberinfrastruktuuria" ja "kybertoimintoihin

[22] United Nations (2021): *Developments in the field of information and telecommunications in the context of international security* (online): https://www.un.org/disarmament/ict-security/ (luettu 11.10.2021).
[23] United Nations (2021): *Open-ended Working Group* (online): https://www.un.org/disarmament/open-ended-working-group/ (luettu 11.10.2021).
[24] United Nations (2021): *Group of Governmental Experts* (online): https://www.un.org/disarmament/group-of-governmental-experts/ (luettu 11.10.2021).
[25] Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2017): *Game Changer: Structural Transformation of Cyberspace*. Finnish Defence Research Agency Publications 10: Riihimäki, 54.
[26] Täysvaltaisuudesta voidaan erottaa sisäinen ja ulkoinen täysvaltaisuus. Sisäisellä täysvaltaisuudella tarkoitetaan valtion yksinomaista oikeutta käyttää valtiovaltaa valtion alueella. Ulkoinen täysvaltaisuus viittaa valtion alueelliseen loukkaamattomuuteen, itsenäisyyteen ja riippumattomuuteen suhteessa muihin valtioihin. Täysvaltaisuus s.v. *Tieteentermipankki* 2021 (online): https://tieteentermipankki.fi/wiki/Termipankki:Etusivu (luettu 13.10.2021).
[27] Ks. esim. Pohle, Julia, Thiel Thorsten (2020): Digital Sovereignty. *Internet Policy Review*, 9(4), 1-19.
[28] Ks. esim. Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021): The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Network*, 35(2), 4-5.
[29] Ks. esim. Efremov, A.A. (2017): Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva. *Pravo. Žurnal Vyssej ekonomiki*, 1, 201-215.
[30] 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.
[31] Kaikkonen, Antti (2021): Puhe Paasikivi-seurassa 19.1.2021(online): https://www.anttikaikkonen.fi/2021/01/19/kaikkosen-puhe-paasikivi-seurassa-19-1-2021/ (luettu 11.10.2021); Kaikkonen, Antti (2021): *Puolustusministeri Kaikkonen: Digitaalinen itsenäisyys on puolustamisen arvoinen*, Erve Foorumi 2021 (online): https://www.erillisverkot.fi/puolustusministeri-kaikkonen-digitaalinen-itsenaisyys-on-puolustamisen-arvoinen/ (luettu 11.10.2021).
[32] Kulmuni, Katri (2020): *Puheenvuoro: rauhaa, kestävää kehitystä ja vakautta*, Ulko- ja turvallisuuspoliittinen puheenvuoro 26.2.2020 (online): https://www.katrikulmuni.fi/blogi/puheenvuoro-rauhaa-kestavaa-kehitysta-ja-vakautta/ (luettu 11.10.2021).
[33] Lausunnossa viitataan GGE:n vuoden 2015 raporttiin. Sama määritelmä on julkaistu myös englanniksi Tallinnan manuaalissa: "A State enjoys sovereing authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017): Schmitt, M.N. et al. (eds.). Cambridge University Press: Cambridge, 13.
[34] "Cyber infrastructure: The communications, storage, and computing devices upon which information systems are built and operate" (ibid., 564).

osallistuvia henkilöitä", jotka eivät ole esim. ko. valtion kansalaisia. Kysymyksiä herättävät myös satelliitit, elektromagneettinen spektri tai kansainvälisellä merialueella kulkevat tietoliikennekaapelit, jotka ovat kriittisiä eri valtioiden kyberinfrastruktuurin toiminnalle. On mahdollista, että joku valtio määrittelee nämä osaksi omaa "digitaalista suvereniteettiaan", joka voi johtaa laaja-alaisen vaikuttamisen keinoin hyväksikäytettäviin ristiriitatilanteisiin. Suvereniteetti kybertilassa vaatii vielä "kyberrajojen" määrittelyn, jota ei ole toistaiseksi juurikaan tehty.[35]

Kybertilan teknistaloudelliset liittoumat

Arvioitaessa mahdollisia tulevia kehityskulkuja, näyttää mahdolliselta, että kybertilan territoriaalinen maailmanjäsennysmalli johtaa tulevaisuudessa liittoumiin, jotka perustuvat kilpaileviin teknisiin alustoihin ja kansallisiin ratkaisuihin – mikään valtio ei kuitenkaan yksin voi saavuttaa "kyberomavaraisuutta". Näitä alliansseja voidaan kutsua teknistaloudellisiksi liittoutumiksi[36], jotka kehittävät kansallisella tasolla uusia teknologioita ja niiden pohjalta rakennetaan liittoumalle palveluita, jotka perustuvat kansalliseen tekniikkaan. Monet maat tavoittelevat omavaraisuutta ja digitaalista suvereniteettia, mutta säilyttääkseen kilpailukykynsä niiden on joko liityttävä kehittyviin teknistaloudellisiin liittoumiin tai vahvistettava niitä.

Mahdollisia teknistaloudellisia liittoumia voi muodostua Yhdysvaltojen johtamana anglosaksisen maailman ympärille, Kiinan ympärille, Venäjän sekä mahdollisesti EU:n ympärille.[37] Taloudellisesti tiiviisti integroituneet Yhdysvallat, Kanada, Australia ja Uusi-Seelanti vetävät mukaansa myös Meksikon kaltaisia maita omaan liittoumaansa. Tämä liittouma käyttää etuoikeutettua asemaansa maailmanjärjestelmässä luodakseen itselleen parhaat edellytykset. Vastaavasti Kiina laajentaa järjestelmällisesti liittoumaansa naapurimaihin, jotka ovat sidottuja Kiinan talouteen ja infrastruktuuriin. Kiinan malli perustuu absoluuttisen omavaraisuuden periaatteeseen, ja sillä on pääsy valtaville markkinoille, jotka ovat suurelta osin suljettu kilpailijoiden teknologiamarkkinoilta ja käyttäjätiedoilta. Venäjä haluaa säilyä itsenäisenä suurvaltana ja sivilisaationa ja tämä on mahdollista vain osana jonkinlaista teknistaloudellista liittoumaa. Venäjän liittouma olisi riippuvainen kotimarkkinoista ja julkisista investoinneista. Venäjän luonnollisia kumppaneita ovat Euraasian Unionin jäsenvaltiot, yksittäiset entisen Neuvostoliiton valtiot (Valko-Venäjä, Azerbaidzhan, Kazakstan, Uzbekistan, Tadzhikistan, Moldova).[38] EU:n Digitaalistrategiassa (2020) todetaan, että EU:n on lujitettava digitaalista suvereniteettiaan ja asetettava standardeja sen sijaan, että se kulkisi muiden jäljessä.[39] EU:n ympärille muodostuvan liittouman painopisteenä ovat data[40], teknologia ja infrastruktuuri. Tavoitteena olisi vahvistaa Euroopan teknologista kyvykkyyttä, itsenäisyyttä ja luottamusta sekä parantaa Euroopan asemaa globaalissa kilpailussa luottamusta vahvistamalla, mutta omana teknistaloudellisena liittoumana EU:n tulevaisuus näyttää kuitenkin epävarmalta.

Teknistaloudellisten liittoutumien välinen raja on teknologinen. Voidaan väittää, että globaalin kybertilan aikakaudella, kyberrajat kulkevat kilpailevien kriittisten infrastruktuurien teknologistenalustojen välisessä kilpailussa, joita hallitukset ohjaavat kansallisella tai liittouman tasolla. Kansallisen turvallisuuden vuoksi on mahdotonta päästää ulkopuolisia itsenäiseen kriittiseen infrastruktuuriin. Liittoumat edellyttävät halua käyttää klassisia kansainvälisen oikeuden periaatteita uudessa todellisuudessa eli noudattaa kybertilassa lakeja, jotka määrittävät valtioiden välisiä suhteita fyysisessä maantieteellisessä ympäristössä. Liittoumat ovat siis myös sotilaallisia ja poliittisia ja näillä on strategista merkitystä.[41]

Kansallisen kybertilan käsitteellistäminen

Edellä esitettyihin keskusteluihin ja tilannekatsaukseen perustuen voidaan arvioida, että kybertilan territoriaalinen maailmanjäsennysmalli saa todennäköisesti tulevaisuudessa yhä enemmän kannattajia. Kybertilan valtioalueellistaminen on kuitenkin suhteellisen uusi ilmiö eli se vaatii perusteellista käsitteellistämistä. Viime aikoina myös Suomessa on esitetty vaatimuksia "kansallisen kybertilan" määrittelystä, jotta "Suomen kybertilan" koskemattomuuden valvonta ja turvaaminen voitaisiin toteuttaa.[42] Samalla on kuitenkin havaittu ja myönnetty määrittelemisen vaikeus.[43] Puolustusvoimien tutkimuslaitoksella (PVTUTKL) järjestettiin keväällä 2021 sotilas- ja siviiliasiantuntijoiden tutkimuspaja[44], jossa "kansalliselle kybertilalle" lähdettiin hakemaan määritelmää niin teknisestä kuin poliittisesta ja oikeudellisesta näkökulmasta.

Käsitteiden määrittelyssä on tärkeää, ei ainoastaan kuvata tiettyä ilmiötä, mutta myös selvittää mihin laajempaan pääkäsitteeseen se kuuluu ja mitkä käsitteet ovat sen kanssa rinnakkaisia tai lähikäsitteitä. Tässä tapauksessa "kansallinen kybertila" -käsitteen nähdään linkittyvän laajempaan "territoriaalisuuden" käsitteeseen. Territoriaalisuus merkitsee klassisen määritelmän[45] mukaan yksilön tarvetta tai ryhmän pyrkimystä ohjata ja kontrolloida ihmisiä ja ilmiötä näiden hyödyntämän tilan kontrollin kautta. Käytännössä tämän kontrollin ja ohjauksen on varmistanut tilan selkeä määritteleminen ja rajaaminen.

Kansainvälisen politiikan ja oikeuden piirissä tilan selkeään määrittelyyn on kehitetty "valtioalue" -käsite, jolla tarkoitetaan itsenäisen valtion kansainvälisten oikeuksiensa nojalla omistamaa ja suvereenisti hallitsemaa valtakunnan rajojen sisäpuolelle sijoittuvaa aluetta.[46] Valtioalueet ovat syntyneet ja muuttuneet historiallisen kehityksen mukana. Aikaisemmin valtiokarttaan vaikuttivat voimakkaasti sotatoimet. Usein aluemuutokset perustuivat alueen väkivaltaiseen valloittamiseen ja sitä seuranneeseen rauhantekoon. Valtiorajat määräytyvät esimerkiksi alueellisen yhteisymmärryk-

[35] Ks. esim. Kukkola, J. & Ristolainen, M. (2018): Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', *Journal of Information Warfare*, 17(2), 83-100.
[36] MGIMO (2019): *Meždunarodnye ugrozy 2020: Každyj za sebja*. Laboratorija analiza meždunarodnyh protsessov MGIMO MID Rossii (online): https://mgimo.ru/upload/iblock/2ac/int-threats-2020.pdf (luettu 11.10.2021).
[37] ibid.
[38] ibid.
[39] *Shaping Europe's digital future* (2020): Luxembourg: Publications Office of the European Union (online): https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (luettu 11.10.2021).
[40] Erityisesti yksilön oikeus omistaa omasta itsestään oleva data (vrt. *GDPR, General Data Protection Regulation*, 2018).
[41] Kukkola 2021.
[42] Kukkola, J. (2020): Cyber Sovereignty - Anarchical Dreams Meets Westphalian Necessities, 40-41. *Cyberwatch, Quarterly review* 15.10.2020, 03/2020 (online), https://www.cyberwatchfinland.fi/cyberwatch-finland-q3-magazine-every-day-is-cyber-security-day/ (luettu 13.10.2021); Lehto, Martti (2021): Päätoimittajalta: Kybertoimintaympäristön suojaaminen edellyttää sen määrittelyä, *Sotilasaikakausilehti* 3/2021 (online): https://upseeriliitto.fi/verkkolehti/kybertoimintaympariston-suojaaminen-edellyttaa-sen-maarittelya/ (luettu 11.10.2021).
[43] ibid.
[44] Tutkimuspaja järjestettiin 29.-31.3.2021 Puolustusvoimien tutkimuslaitoksella. Tutkimuspajaan oli kutsuttu 10-15 sotilas- ja siviiliasiantuntijaa, joiden työskentelyyn tämä alaluku pohjautuu. Osallistujien luvalla kommentteja on muokattu ja yhdistelty sekä ne esitetään nimettöminä.
[45] Sack, Robert D. (1986): *Human Territoriality. Its Theory and History*. Cambridge: Cambridge University Press, 19.
[46] Valtioalue koostuu maa- ja ilma-alueesta sekä rannikkovaltioilla myös merialueesta. Valtion ilma-alueen ja avaruuden välistä rajaa ei ole onnistuttu määrittämään. Oikeudellisesti on kuitenkin selvää, että valtioalue ei voi ulottua avaruuteen eikä taivaankappaleisiin. Rannikkovaltio ei voi ulottaa aluettaan 12 meripeninkulmaa kauemmaksi niistä perusviivoista, joista sen aluemeren leveys mitataan. Valtioalue s.v. *Tieteentermipankki* 2021 (online): https://tieteentermipankki.fi/wiki/Oikeustiede:valtioalue/laajempi_kuvaus (luettu 13.10.2021).

sen tai rajasopimuksen perusteella. Usein rajajärjestelyistä on päätetty rauhansopimuksissa, joille on ollut tyypillistä hävinneen osapuolen alistuminen voittajan ehtoihin.[47] Kybertilan valloittaminen ja/tai valtaaminen sotatoimien kautta ei ole käytännössä mahdollista[48], joten sen "valtioalueellistaminen" on tapahduttava muulla tavoin.

Valtioalueeseen liittyy tiiviisti suvereniteetin käsite. Yksinkertaisen määritelmän mukaan suvereeneilla valtiolla on maantieteellinen alue ja hallinto, jolla on alueen hallitsemiseen täydellinen, ehdoton ja riippumaton valta (valtiosuvereniteetti eli täysvaltaisuus). Hallinnolla on vapaus päättää itsenäisesti suhteistaan toisiin valtioihin ja kansainvälisiin toimijoihin. Valtioiden tunnusmerkkinä ovat rajat, joiden sisällä valtiot voivat päättää asioistaan itsenäisesti.[49] Nykymuotoiset valtioiden väliset rajat perustuvat Westfalenin rauhansopimukseen (1648), jossa valtion ja rajan käsite sidottiin tiukasti toisiinsa. Rajojen ylitykseen liittyvät käytänteet (passit, viisumit, rajavalvonta) kehittyivät vähitellen 1800-luvulla.[50]

Kansainvälisiin sopimuksiin pohjautuen suvereenin valtion oikeuksiin kuuluvat alueellinen koskemattomuus ja rajojen loukkaamattomuus. Alueellinen koskemattomuus tarkoittaa, että valtiolla on oikeus suojata, ettei omaa aluetta kosketa eli että vieraat valtiot eivät tule alueelle. Alueellinen koskemattomuus edellyttää aluevalvontaa (AKV, alueellisen koskemattomuuden valvonta). YK:n peruskirja määrää, että valtioiden välisiä asioita ei saa ratkaista voimankäytöllä, eikä toisten valtioiden alueelliseen koskemattomuuteen, poliittiseen riippumattomuuteen tai sisäisiin asioihin saa puuttua. Valtiolla on oikeus valvoa alueellista koskemattomuuttaan ja turvata se tarvittaessa voimakeinoja käyttäen (AKT, alueellisen koskemattomuuden turvaaminen). Suomessa Aluevalvontalaki (18.8.2000/755) säätää Suomen alueellisen koskemattomuudesta ja valvonnasta: ”Suomen alueella [tarkoitetaan] valtakunnan maa- ja merirajojen sekä aluemeren ulkorajan sisäpuolella olevia maa- ja vesialueita sekä niiden yläpuolella olevaa ilmatilaa”.[51]

Kaikki edellä mainitut toimintatavat ja käsitteet ovat kehittyneet perinteisiin valtioalueisiin ja niiden maantieteellisiin (fyysisen ulottuvuuden) rajoihin liittyen, eikä niiden määrittely ole täysin selkeää ja yksimielistä edes perinteisessä mielessä. Esimerkiksi valtioalue, suvereniteetti ja rajat ovat luonteeltaan sekä poliittisia että oikeudellisia.[52] Kybertilassa valtioalueesta ja suvereniteetista tulee myös teknologisia käsitteitä ja rajoista teknisiä toteutuksia. Kansallisen kybertilan käsitteellistäminen eli valtioalueeksi määrittäminen (valtioalueellistaminen) ja rajaaminen ei-fyysisessä, ihmisen rakentamassa, kuvitteellisessa tilassa, jota voi muokata jatkuvasti on erittäin haasteellista niin poliittisesti, oikeudellisesti kuin teknisestikin.

"Kansallisen kybertilan" -käsitteen nähdään siis linkittyvän laajempaan "territoriaalisuuden" käsitteeseen. "Kansallinen kybertila" on fyysisestä valtioalueesta irrallaan oleva virtuaalinen/digitaalinen tila. Tästä syystä "kansallinen kybertila" -käsite ehdotettiin korvattavaksi "kyberterritorio" -käsitteellä PVTUTKL:n tutkimuspajassa. Territorio-käsite otettiin "kansallisen kybertilan" lähtökohdaksi, koska sitä on perinteisesti käytetty kuvaamaan jostain valtiosta riippuvaista hallintoaluetta, joka ei kuitenkaan ole tuon valtion täysvaltainen osa; tai suoraan keskushallinnon alaisesta vajaaoikeuksisesta liittovaltion alueesta; tai alueesta, joka on valtion tai osavaltion keskushallintoa alempi ja yleensä sille alisteinen alue.[53] Käsite ”kyberterritorio” on mahdollisesti ensimmäisen kerran mainittu suomeksi teoksessa Aaltola et al. 2017, s. 133[54], haastattelussa, jossa haastateltava nosti esiin tarpeen Suomen "kyberterritorion" tarkemmalle määrittelylle huoltovarmuuden näkökulmasta.

PVTUTKL:n tutkimuspajassa lähdettiin liikkeelle siitä, että kyberterritorion määritelmässä pitäisi teknisten määreiden lisäksi jotenkin täyttyä rajaamisen (alue voidaan jollain tavalla teknisesti rajata) ja itsenäisyyden (suvereeniuden, riippumattomuuden, täysvaltaisuuden, itsemääräämisoikeuden) vaatimus. Kyberterritoriokäsitteellä tulisi siis viitata mahdolliseen abstraktiin ja tekniseen valtioalueen kaltaiseen virtuaaliseen tilaan, jonka sijainti ei välttämättä ole ko. valtion maantieteellisellä alueella tai se ei täytä perinteistä valtioalueen määritelmää, mutta joka on ko. valtion jollain tavalla hallitsemaa ja "digitaalisten rajojen" (kyberrajojen) sisäpuolelle sijoittuvaa "digitaalista aluetta" (vrt. maa- ja merialue, ilmatila).[55]

Tästä johdettuna keskustelun tuloksena PVTUTKL:n tutkimuspajassa kyberterritorion määritelmäksi muotoutui **"valtion suvereenin toimivallan piiriin kuuluvat tietoverkot ja tekninen infrastruktuuri ja niiden tarjoamat palvelut sekä niissä käsiteltävä data"**.

Perustelu tutkimuspajassa esitetylle määritelmälle on, että se liittää kyberterritorion valtioon, mutta jättää toimivallan määrittelyn käsitteen ulkopuolelle, koska se on poliittinen – ei akateeminen – kysymys. Määritelmä mahdollistaa yksityisen, säädellyn yksityisen ja julkisen infrastruktuurin sisällyttämisen käsitteeseen, sekä huomioi palvelut, jotka ovat myös sääntelyn kohde ja vallan lähde. Toisaalta, määritelmä ei rajoita datan sisältöä, tarkoitusta tai omistajuutta. Kyberterritorioita voi myös olla erilaisia: suurvalloilla, pienillä valtioilla jne. Seuraavassa em. määritelmään johtaneita keskusteluja ja käytettyjä sanamuotoja eritellään ja perustellaan tarkemmin.

Suvereeni

Määritelmässä esiintyvä käsite "suvereeni" herätti eniten keskustelua. Tässä määritelmässä "suvereeni" liittää kyberterritorion määritelmään täysivaltaiseen, alueellisesti määriteltyyn valtioon, mutta ei rajaa sen sijaintia perinteiseen valtioalueeseen. Suvereeni toimivalta on valtion itsensä määriteltävissä, pitää sisällään kaikki toimivallan muodot ja näin ollen toimivallan määrättyyn laajuuteen tai piirteisiin ei tarvitse määritelmässä kiinnittyä. Suvereenin lisäämistä määritelmään ei pidetty huonona, mutta todettiin, että

[47] Valtioalue s.v. *Tieteentermipankki* 2021 (online): https://tieteentermipankki.fi/wiki/Termipankki:Etusivu (luettu 13.10.2021).
[48] Vrt. Libicki, Martin (2009): *Cyberdeterrence and Cyberwar*. RAND. Puolustaja voi aina sulkea hyökkääjän ulos tai sammuttaa tilan perustana toimivat järjestelmät. Molemmat voivat kiistää tilan käytön toiselta. Tilan valloittaminen ilman puolustajan hyväksyntää on periaatteessa mahdotonta. Data voidaan toki varastaa.
[49] Kireev, A. (2015): State border. Sevastianov, S., Laine, J. & Kireev, A. (eds.) *Introduction to border studies*. Dalnauka, Vladivostok, RU, 98-117.
[50] Moisio, S. (2002): Rajat, Identiteetti ja valta: Laajentumisen poliittinen maantiede. Raunio, T. & Tiilikainen, T. (toim.) *Euroopan rajat. Laajentuva Euroopan Unioni.* Helsinki: Gaudeamus.
[51] *Aluevalvontalaki* (18.8.2000/755) (online): https://www.finlex.fi/fi/laki/ajantasa/2000/20000755 (luettu 13.10.2021).
[52] Vrt. esim. YK:n merioikeusyleissopimus (UNCLOS 1982), joka puhtaasti oikeudellinen sopimus merialueiden rajaamisesta ja monella tavalla puhtaan mielivaltainen periaatteiltaan, vaikkakin yhteiseen sopimukseen perustuva.
[53] Territorio s.v. *Kielitoimiston sanakirja* 2020 (online): https://www.kielitoimistonsanakirja.fi/#/ (luettu 13.10.2021).
[54] *Huoltovarmuus muutoksessa: Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössä* (2016): Aaltola, Fjäder, Innola, Käpylä, Mikkola (toim.). FIIA raportti 49, UPI, 133-135; […] "Osa huoltovarmuutta on se, miten turvataan meidän kyberterritorio". Fyysinen kuutio tiedetään, mutta mikä on meidän kyberterritorio? Kukaan ei ole sitä määritellyt, mitä siihen kuuluu." Haastateltava […] s. 133 "Kuluttaja ei tiedä missä palvelu on, no se ei yksittäisen ihmisen kannalta olekaan niin tärkeää, mutta kriittiset palvelut ovat eri asia. Olisi viisasta tarkastella sitä, missä palvelu on, minne se on varmennettu, mitä kautta se kulkee. Missä data sijaitsee, sitä ei moni tiedä. Saako palvelun sellainenkin taho, jota ei toivota? Sekin voi olla mahdollista. Tilanne tästä eteenpäin tulee olemaan samankaltainen." Haastateltava s. 133-134
"Ja miten paljon meillä on valtiolle kriittistä kybertilaa?" Haastateltava s. 134
[55] DI Jori-Pekka Rautavan väitöstutkimuksessa (Oulun yliopisto, yhteistyössä PVTUTKL) on tavoitteena kehittää teoreettinen ”Kyberterritorio 1.0” -malli, jossa kuvataan miten valtiollinen kyberterritorio olisi teknisesti toteutettavissa.

omassa abstraktiudessaan se voi johtaa tilanteeseen, jossa määritelmän jälkeen joudutaan kuitenkin lisäämään selitysosio mitä "suvereeni" tässä yhteydessä tarkoittaa.

On kuitenkin ymmärrettävä, että suvereeniuutta ei ole, jos toiset valtiot eivät sitä tunnusta. Eli periaatteessa valtio voi vaatia suvereeniuutta, mutta ilman muiden valtioiden hyväksyntää, se ei ole suvereeni. Näin ollen voisi todeta, että kyberterritorioon liittyvä toimivalta on kansainvälispoliittinen kysymys (ei pelkästään poliittinen) ja täten jatkuvan neuvottelun kohde.

Tietoverkot ja tekninen infrastruktuuri

Toinen laajoja kysymyksiä herättänyt kohta määritelmässä oli "tietoverkot ja tekninen infrastruktuuri", koska sen pitäisi laajasti ottaen sisältää myös toiminnan kannalta välttämättömät palvelut. Palvelut päätettiin sisällyttää määritelmään, koska niiden sisällyttäminen jättää oven auki myös sille, että virtuaalisesti jokin suvereenin toimivallan alla oleva palvelu voi sijaita fyysisten rajojen ulkopuolella.

Data

"Datan" ja "tiedon" välillä käytiin pitkällistä keskustelua. Tietoa pidettiin liian epämääräisenä käsitteenä ja sen monimerkityksellisyys eri kielillä nostettiin esille. Käsitteenä datan voidaan nähdä muodostavan selkeän objektin suhteessa valtion toimivaltaan. Data nähtiin oleellisena osana palveluita. Ja tietojärjestelmän turvaaminen tarkoittaa usein käytännössä nimenomaan sen sisältämän datan turvaamista. Toisaalta, esille nostettiin myös kysymys, että vaatiiko kyberterritorion olemassaolo, että siellä on dataa vai voisiko kyberterritorio olla olemassa ilman dataakin ja kyberterritoriossa voitaisiin vain siirtää ja käsitellä dataa.

Näiden lisäksi kysymyksiä herätti kyberterritorioon kohdistuvien toimien tarkastelu "datan" kautta eli mitä kyberterritoriolle tapahtuu, jos vihamielinen toimija 1) tuhoaa datan, 2) kopioi datan talteen ja tuhoaa/salaa sen alkuperäisestä paikasta (esim. kiristyshaittaohjelma) tai 3) pelkästään kopioi datan (varkaus/tietovuoto). Heräsi kysymys, onko data siis osa kyberterritoriota, vai pikemminkin analoginen fyysisen valtioalueen asukkaiden, ihmisten, tai vaikkapa yritysten kanssa eli jos kyberterritorion haltija (valtio) jättää kriittisen datan suojaamatta, onko asia analoginen sen kanssa, että fyysinen valtioraja jäisi valvomatta.

Toimivalta

Määritelmässä esitetty "toimivalta" tarkoittaa lainsäädäntöä ja sen puitteissa toteutuvaa toimintaa. Se, miten kriittiset palvelut ja muu toiminnallisuus taataan sekä normaalioloissa että poikkeusoloissa, edellyttänee valmiuslainmukaisia toimenpiteitä eli kirjauksia lakiin. Toisin sanoen, kriittinen informaatio- ja viestintäinfrastruktuuri (ICT) valtion toimintojen ylläpitämiseksi täytyy määrittää ja sen toimintaedellytykset varmistaa sekä normaali- että poikkeusoloissa. Toimivalta voi ulottua territorion sisäpuolelle ja määrätyissä tilanteissa ulkopuolellekin.

Luonteensa vuoksi kyberterritorio on jatkuvassa muutoksessa. Kyberterritoriota on jatkuvasti ylläpidettävä teknisin keinoin. Tämä tarkoittaa, että kyberterritorion valvomiseen ja turvaamiseen liittyvät viranomaiset ovat merkittävässä roolissa kyberterritorion muodostumisessa, ylläpidossa, vahvistamisessa ja hallinnassa, joka taas vastaavasti nostaa esiin toimivalta-kysymyksen, joka on poliittinen kysymys.

Lopuksi

Tämän tutkimuskatsauksen ensimmäisenä tavoitteena oli selvittää kybertilan valtioalueellistamisprosessiin vaikuttavia taustatekijöitä ja meneillään olevia prosesseja sekä arvioida mahdollisia kehityskulkuja. Katsauksessa tiivistettiin kybertilan hallintamalleihin liittyvää keskustelua ja selitettiin YK:n toimintapiirissä tapahtuvan prosessin kulkua. Mielipiteiden kybertilan hallintamalleista voi nähdä olevan muutoksessa, koska yhä useampi maa on halunnut esittää kansallisia kantojaan julkisesti. Suvereniteetti kybertilassa on yksi keskeisimmistä ja vaikeimmista kysymyksistä kansainväliselle yhteisölle ratkaista. Valtioiden kasvava suvereniteetin tavoittelu kybertilassa ja globaalin verkon avoimuus luovat ristiriitaisen dynamiikan, jonka vaikutuksia ei ehkä vielä ymmärretä täysin. Kybertilan territoriaalinen maailmanjäsennysmalli voi johtaa tulevaisuudessa teknistaloudellisiin liittoumiin, jotka perustuvat kilpaileviin teknisiin alustoihin ja kansallisiin ratkaisuihin. Tämä luo kybertilaan täysin uuden kilpailutilanteen, jossa jokainen valtio joutuu valitsemaan liittoumansa.

Tutkimuskatsauksen toinen tavoite oli aloittaa julkinen kansallisen kybertilan käsitteellistäminen. Käsitteellistäminen on merkittävä osa valtioalueellistamisprosessia. Katsauksessa esitettiin PVTUTKL:n tutkimuspajassa tuotettu määritelmä "kyberterritoriolle". Tämä määritelmä avaa peräänkuulutetun akateemisen keskustelun "kansallisen kybertilan" määrittelystä. Tässä katsauksessa esitetty kyberterritorion määritelmä on tarkoitettu akateemiseksi työvälineeksi monimuotoisen poliittisen todellisuuden jäsentämiseksi, eikä esim. lainsäädännön tai poliittisten ohjelmien perustaksi.

Syyskuussa 2021 julkaistussa Puolustusselonteossa[56] puolustusvalmiuteen kohdistuvat vaatimukset ulotettiin myös kybertilaan, mikä heijastelee kybertilan valtioalueellistamisprosessia ja halua kansallisen kybertilan puolustusvoimalliseen hallintaan. Julkisessa poliittisessa keskustelussa lähes huudetaan "softaa kyberrajalle", mutta, kuten tämä tutkimuskatsaus osoittaa, olemme vielä kaukana siitä, että tietäisimme miten valtiollista "kyberterritoriota" valvotaan ja turvataan ja millä kansainvälisellä ja kansallisella oikeutuksella se tehdään.

Tulevassa tutkimuksessa tulisi löytää uusia tapoja ymmärtää perinteisiä fyysisiin rajoihin liittyviä käsitteitä ja toimintamalleja sekä selvittää kuinka valtiollinen "kyberterritorio" voitaisiin rajata teknisesti eli löytää vastaus kysymykseen – miten kyberrajat muodostuvat. Näiden lisäksi tulisi aloittaa poliittinen ja lainsäädännöllinen keskustelu, miten ja kenen toimesta "kyberterritorion" alueellinen koskemattomuus olisi valvottavissa ja turvattavissa.

Lisätietoja

FT, vanhempi tutkija Mari Ristolainen (p. 0299 800) on Puolustusvoimien tutkimuslaitoksen informaatiotekniikkaosaston tutkija.

[56] *Valtioneuvoston puolustusselonteko* (2021): Valtioneuvoston julkaisuja 2021:78, 9.9.2021 (online): https://julkaisut.valtioneuvosto.fi/handle/10024/163405 (luettu 13.10.2021).