Valvonta ja teknologia: Tapaus Venäjä

Outi Helin[1] & Katri Pynnöniemi[2]

Koronapandemian myötä eri maissa on otettu käyttöön kansalaisten normaalia elämää rajoittavia määräyksiä pandemian leviämisen ehkäisemiseksi. Liikkumisrajoitusten valvonnassa on hyödynnetty erilaisia teknologiasovelluksia, kuten QR-kulkulupia sekä puhelintietoihin ja sijaintiin perustuvaa seurantaa. Demokraattiset ja autoritaariset maat kuitenkin eroavat siinä, missä tarkoituksessa erilaisia valvontateknologioita käytetään. Tässä artikkelissa luomme katsauksen viimeaikaiseen tutkimukseen koskien uusien teknologioiden vaikutuksia autoritaaristen maiden resilienssiin. Aikaisempi tutkimus on pyrkinyt mallintamaan erilaisia vaikutuspolkuja, ja siitä käy myös ilmi autoritaaristen maiden pyrkimys toteuttaa ennakoivaa verkkovalvontaa. Artikkelin lopuksi käsittelemme muutamia politiikkaohjelmia, joiden puitteissa Venäjä kehittää muun muassa verkkovalvontaa.

Avainsanat: autoritaariset hallinnot, teknologia, valvonta, Venäjä

Johdanto[3]

Koronapandemian myötä eri maissa on otettu käyttöön kansalaisten normaalia elämää rajoittavia määräyksiä pandemian leviämisen ehkäisemiseksi. Liikkumisrajoitusten valvonnassa on hyödynnetty erilaisia teknologiasovelluksia, kuten QR-kulkulupia sekä puhelintietoihin ja sijaintiin perustuvaa seurantaa. Esimerkiksi Venäjällä on otettu käyttöön mobiilisovellus kotona koronaa sairastaville. Kasvojentunnistuksen ja teleoperaattoritiedot yhdistävä mobiilisovellus on väline paitsi pandemian hillitsemiseen, mutta se tuottaa myös materiaalia tekoälyn kehittämiseen. Moskovan alueella on pandemian aikana luotu hallinnolliset puitteet tekoälyteknologioiden kehittämiseksi. (Interfax 2021.)

Keväällä 2020 tunnettu venäläinen toimittaja, *Novaja gazeta* -lehden politiikan toimituksen esimies Kirill Martynov tiivisti käynnissä olevan muutoksen nimeämällä sen algoritmien ja autoritaarisen poliittisen järjestelmän liitoksi: ”algoritmikratiaksi”. Martynovin (2020) arvio pohjautuu ajatukseen, jonka mukaan valvontateknologiat saavat sitä enemmän valtaa, mitä heikompia demokraattiset instituutiot ovat. Tältä osin Venäjän tilanne näyttää erityisen synkältä. Tässä artikkelissa luomme katsauksen aikaisempaan tutkimukseen koskien digitaalisten teknologioiden hyödyntämistä autoritaaristen maiden resilienssin vahvistamiseksi. Lisäksi pohdimme, miten aikaisempaa tutkimusta voisi hyödyntää arvioitaessa Venäjän teknologiahankkeiden merkitystä autoritaarisen valvonnan näkökulmasta.

Artikkeli etenee siten, että seuraavassa kappaleessa käymme lyhyesti läpi aikaisemmassa tutkimuksessa esiin nostettuja näkökulmia internetin ja laajemmin digitaalisten teknologioiden hyödyntämisestä osana autoritaaristen maiden poliittisen vakauden vahvistamista.

1 YTM, projektitutkija (2021), Helsingin yliopisto, <outi.helin@gmail.com>

2 YTT, apulaisprofessori, Helsingin yliopisto & Maanpuolustuskorkeakoulu, <katri.pynnoniemi@helsinki.fi>

3 Artikkeli on kirjoitettu osana MATINEn vuonna 2021 rahoittamaa tutkimushanketta ”Epävarmuustekijät toimintaympäristöanalyysissä”.

Käymme lyhyesti läpi erilaisia malleja, joiden avulla tutkijat ovat selittäneet digitalisaation vaikutusta autoritaaristen poliittisten järjestelmien tasapainoon. Yksi keskeisistä johtopäätöksistä on se, että teknologia ei korvaa väkivaltaisen repression keinoja, vaan se kohdentaa niitä. Peliteoriaa hyödyntävä tutkimus puolestaan osoittaa, että digitaalisten teknologioiden kehittyessä autoritaariset valtiot todennäköisesti pyrkivät entistä tarkemmin ennalta-ehkäisemään poliittisen opposition toimintaa (erityisesti massamielenosoituksia). (Dragu & Lupu 2021.) Artikkelin lopuksi luomme katsauksen Venäjällä toteutettaviin politiikkaohjelmiin, joissa kehitetään yhteiskunnallisen toiminnan digitalisaatiota ja verkkovalvontaa.

Katsaus aikaisempaan tutkimuskirjallisuuteen

Autoritaaristen maiden suhdetta tieto- ja viestintäteknologiaan (ICT) tarkastellaan usein peilaamalla sitä teknologian kansalaisia voimaannuttavaan ja vapauttavaan voimaan. Tämä näkökulma hallitsi esimerkiksi vuoden 2013 Arabikevään tapahtumien tulkintaa. Toisaalta tiedetään, että autoritaariset maat käyttävät uutta teknologiaa kansalaisten yhteiskunnallisten ja poliittisten oikeuksien rajoittamiseen. Konstanzin yliopiston tutkijat Espen Rød ja Nils Weidmann (2015, 338) huomioivat omassa tutkimuksessaan nämä molemmat näkökulmat: teknologian vapauttavan voiman näkökulman (engl. *liberation technology*) lisäksi teknologian repressiivisen puolen (*repression technology*). Toronton yliopiston politiikan tutkija Seva Gunitsky on samoilla linjoilla ja erottelee toisistaan kyber-optimistit ja kyber-pessimistit. Kyber-optimistit näkevät teknologian työkaluna, jonka avulla voidaan mobilisoida hallinnon vastaista toimintaa, kun taas kyber-skeptiset uskovat, että hallinto voi hyödyntää teknologioita sensuurissa ja kontrollissa (Gunitsky 2015, 44). Autoritaarisen hallinnon kontrolli voi ulottua myös maan ulkopuolelle. Sosiologi Dana Moss on tutkinut Syyrian hallinnon keinoja vaikuttaa ja jopa estää hallinnonvastaisen diasporan toimintaa ulkomailla. Moss (2018, 265) kuvaa tätä toimintaa digitaalisesti mahdollistetuksi repressioksi (engl. *digitally-enabled repression*).

Rødin ja Weidmannin (2015, 338, 348) mukaan ICT-teknologian käyttö vahvistaa autokraattista selviytymistä, sillä se mahdollistaa julkisen mielipiteen muokkauksen ja toisinajattelijoiden tunnistamisen. Seva Gusnitsky (2015, 42) argumentoi, että erityisesti sosiaalisella medialla on roolinsa autokraattisen hallinnon kestävyyden vahvistamisessa. Myös Andrea Kendall-Taylorin, Erica Franzin ja Joseph Wrightin mukaan teknologia vahvistaa autokratiaa. Näiden tutkijoiden mukaan teknologia ei korvaa vanhoja väkivaltaisia repression keinoja vaan kohdentaa niitä: teknologian avulla autoritaarinen hallinto tunnistaa paremmin vastarinnan, johon fyysinen väkivalta voidaan kohdentaa (Kendall-Taylor ym. 2020, 108–109).

Venäläisen taloustieteilijä Sergei Gurievin ja yhdysvaltalaisen politiikan tutkija Daniel Treismanin kehittämä *informaatioautokratian teoria* pyrkii selittämään digitaalisten teknologioiden ja poliittisen legitimiteetin välistä monimutkaista vuorovaikutussuhdetta. Tutkijoiden lähtökohtana on ajatus, että autoritaariset valtiot eivät enää entiseen tapaan nojaa massamaisiin pidätyksiin ja mielivaltaan vaan pyrkivät säilyttämään valtansa ensisijaisesti informaation manipuloinnin avulla. Teorian keskeisiä muuttujia ovat poliittisen ja taloudellisen eliitin koko sekä sen kyky vastustaa tai päinvastoin myötäillä maan poliittisen johdon kantoja median välityksellä. Autoritäärisen järjestelmän kyky manipuloida väestön mielialoja

median välityksellä kuitenkin heikkenee taloudellisen modernisaation myötä. Näin syntyy tilaa demokraattiselle muutokselle, tutkijat toteavat johtopäätöksissään. (Guriev & Treisman 2020, 1–2, 9.)

Kuitenkin monissa eri tutkimuksissa on osoitettu, että internetin ja sosiaalisen median käytön laajentuminen tarjoavat autoritaarisille hallinnoille uusia mahdollisuuksia toteuttaa valvontaa. Kansalaisten digitaalisessa muodossa lähettämät tiedot kulkevat internet-infrastruktuurissa, joka saattaa olla valtion kontrollissa tai häiriön kohteena. Digitaalista valvontaa hyödynnetään erityisesti vastustuksen tukahduttamisessa ja laajojen protestien ehkäisyssä. Verrattuna perinteisiin, fyysistä läsnäoloa vaativiin keinoihin, verkossa tapahtuva valvonta on helpompi salata ja se on myös kustannustehokasta. (Xu 2021, 313, 323.)

Toisaalta on hyvä muistaa, että valvontajärjestelmän rakentaminen vaatii erityisosaamista sekä mittavia investointeja. Carnegie keskuksen tutkija Steven Feldstein on tutkinut tekoälyn käyttöä osana verkossa tapahtuvaa, toisinajattelijoiden muodostamien verkostojen valvontaa. Tavoitteena on tunnistaa verkostoista yksittäisiä toimijoita ja hyödyntää tätä tietoa esimerkiksi massamielenosoitusten ennaltaehkäisemisessä. Lisäksi tekoälyä hyödyntävän kasvojentunnistusteknologian avulla voidaan seurata väkijoukkojen muodostumista tai etsiä poliittisia tunnuksia kantavia ihmisiä. (Feldstein 2019, 43–44.) Palaamme näihin esimerkkeihin artikkelin viimeisessä kappaleessa.

Verkkomaailman valvonnan ja ohjailun neljä tasoa

Kuten Konstanzin yliopiston tutkijat Eda Keremoğlu ja Nils Weidmann ovat esittäneet, vaikuttamis- ja rajoittamistoimet voivat kohdistua internetin infrastruktuuriin, verkon toimintaan tai erilaisiin palveluihin ja sovelluksiin. Infrastruktuurilla tarkoitetaan laitteistoja, joiden kautta yhteydet rakennetaan. Verkon avulla varmistetaan tiedonsiirto lähteestä määränpäähän, ja sovellustyökaluilla käyttäjä lähettää ja vastaanottaa tietoa. (Keremoğlu & Weidmann 2020, 1690–1692.) Tässä kappaleessa tarkastelemme aikaisempaan tutkimukseen nojautuen autoritaaristen maiden keinoja rajoittaa yhteiskunnallista toimintaa seuraavilla neljällä eri tasolla: internet-infrastruktuuri, ylikansalliset ja kansalliset toimijat, verkossa tapahtuva toiminta sekä yksilön digitaalinen jalanjälki.

Internet-infrastruktuurin hallinta

Autoritaariset maat pyrkivät tyypillisesti saamaan internet-infrastruktuurin joko suoraan tai välillisesti poliittisen johdon hallintaan (Keremoğlu & Weidmann 2020, 1690–1692; DeNardis 2012, 720). Monissa maissa, kuten Venäjällä, valtio vastaa digitaalisen tietoliikenneinfrastruktuurin rakentamisesta syrjäisille alueille. Venäjällä monet infrastruktuuriyritykset ovat valtion omistamia tai hallinnolle läheisten tahojen omistamia (Vendil Pallin 2017, 17; Kukkola 2020, 13, 17). Autoritaariset maat ovat turvautuneet myös tietoliikenneyhteyksien katkaisuun hillitäkseen yhteiskunnallista liikehdintää tai levottomuuksia (DeNardis 2012, 729–731). Viimeksi näin tehtiin Kazakstanissa tammikuussa 2022 tapahtuneiden mielenosoitusten aikana. Näin yhteiskunnalliset muutokset ja valtakamppailut heijastuvat suoraan tai välillisesti infrastruktuurin toimintaan (ma.).

Tutkija Mari Ristolaisen (2017, 113, 125) mukaan Venäjä pyrkii luomaan itsenäisen verkon kontrolloimalla internettietoliikennettä Venäjän sisällä. Venäjän tavoite suvereenista internetistä kattaa myös riippumattomuuden globaalista internet-infrastruktuurista. Tavoitteena on ollut luoda niin kutsuttu *internetin pysäytyspainike* (engl. *internet kill switch*) ja muita keinoja, joilla voidaan seuloa ja torjua ei-haluttua sisältöä Venäjän alueella. Tämä tarkoittaa, että kaikki Venäjän alueella toimivat internetintarjoajat velvoitetaan asentamaan laitteisto, joka estää käyttäjien pääsyn hallinnon laittomaksi määrittelemään sisältöön. Venäjän viestinnän ja informaatioteknologian valvonnasta vastaavalla viranomaisella Roskomnadzorilla on jatkossa merkittävä osa Venäjän internetliikenteen solmukohtien kontrolloinnissa (Vendil Pallin & Hjelm 2021, 2). Juha Kukkola (2021, 21) käsittelee Venäjän internetsegmenttiä *suljetun kansallisen verkon* käsitteen kautta. Suljetulla kansallisella verkolla tarkoitetaan valtion kontrolloimaa kybertilaa, joka on mahdollista kytkeä irti globaalista internetistä kriittisten peruspalveluiden toimintaa vaarantamatta.

Venäjän pyrkimys eristää venäläinen internet globaalista verkosta ilmenee esimerkiksi vuonna 2019 säädetyn *"suvereenin internetin"* lain myötä (Duma 2019). Lakimuutosten päätavoitteena on luoda edellytykset maan sisäisen internetliikenteen tehokkaalle valvonnalle, saattaa kaikki internetliikenne valtion sääntelyn alaisuuteen ja siten luoda valtion "digitaaliset rajat" sekä levittää valtiojohtoisen internetin mallia kansainvälisesti (Epifanova 2020, 2). Internet-infrastruktuurin kontrolloinnin näkökulmasta keskeistä on lakiin kirjattu kohta, jossa velvoitetaan internet-palveluntarjoajat asentamaan laitteistoa, jolla ehkäistään Venäjän vakauteen, turvallisuuteen ja verkon toiminalliseen yhtenäisyyteen kohdistuvia uhkia (Venäjän federaation laki 2019). Lehtitietojen mukaan internet-palveluntarjoajilla on ilmennyt yhteysongelmia laissa vaadittujen laitteistojen käyttöönoton myötä (Gavriljuk 2021).

Kansallisten ja ylikansallisten toimijoiden toiminnan säätely

Ylikansalliset teknologiayhtiöt ovat kasvattaneet valtaansa maailmassa. Vapaissa yhteiskunnissa internetissä tapahtuva tiedonvaihto on usein yksityisten teknologiayritysten hallinnassa (Yayboke & Brannen 2020, 6). Monet maat ovat alkaneet suhtautua teknologiayhtiöiden digitaaliseen johtoasemaan vakavasti ja pyrkineet rajoittamaan näiden yhtiöiden toimintaa (Moore & Tambini 2018, 402). Autoritaarisissa poliittisissa järjestelmissä yritykset on pyritty saattamaan hallinnan alaisuuteen. Esimerkiksi Venäjä on vaatinut kansainvälisiä yrityksiä rekisteröitymään Venäjällä, jolloin ne tulisivat Venäjän federaation lakien alaisuuteen.

Venäjällä on myös säädetty lakeja, joilla pyritään rajoittamaan kansainvälisten yritysten toimintaa Venäjän verkkoympäristössä. Esimerkiksi vuonna 2014 säädetty laki velvoittaa operaattoreita tallentamaan henkilötiedot Venäjällä sijaitseviin palvelimiin. Lisäksi Venäjä on velvoittanut kansainväliset yritykset perustamaan toimiston Venäjälle, jos niiden hallinnoimilla verkkosivuilla käy päivittäin yli 500 000 ihmistä Venäjältä ja sisältö on venäjänkielistä. Jos ulkomaalainen yritys ei noudata laissa asetettuja määräyksiä, voidaan äärimmäisenä keinona estää sivustolle pääsy Venäjältä (Balashova 2021). Vuonna 2016 Venäjän valvontaviranomainen Roskomnadzor esti pääsyn LinkedIn-palveluun, sillä sen on katsottu rikkovan henkilötietojen säilyttämistä koskevaa lakia: venäläisten henkilötietoja tulee säilyttää Venäjän

alueella (Bondarev ym. 2016). Osa kansainvälisistä yrityksistä on taipunut Venäjän asettamiin sääntöihin, mutta osalle se tuottaisi mainehaittaa (Vendil Pallin 2017, 27).

Vuoden 2020 alkupuolella Aleksei Navalnyn tukimielenosoitusten aikana Roskomnadzor pyrki rajoittamaan sosiaalisen median internetliikennettä ja pyysi sosiaalisen median alustaa Twitteriä poistamaan mielenosoituksiin kannustavaa sisältöä. Roskomnadzor on myös vaatinut Googlea poistamaan hakutuloksia palvelustaan. (Roache 2021.) Venäjän toimet kansainvälisiä alustoja kohtaan ovat tuntuvasti tiukentuneet, mutta vielä ollaan kaukana Kiinan kaltaisesta kontrollista, jossa Google, Facebook ja Twitter eivät toimi maassa laisinkaan.

Verkossa tapahtuvan toiminnan valvonta ja hallinta

Edellä on jo käsitelty lyhyesti Keremoğlun ja Weidmannin tutkimuksen johtopäätöksiä koskien autoritaaristen maiden tapoja rajoittaa verkossa tapahtuvaa toimintaa. Viitaten aikaisempaan tutkimukseen tutkijat erittelevät neljä keinoa, joiden avulla autoritaariset maat hyödyntävät internetiä omiin tarkoituksiinsa. Ensinnäkin tietoa kontrolloidaan ja sensuroidaan esimerkiksi sosiaalisen median seurannalla ja hallinnolle uhkaavat sisältö poistetaan. Toiseksi sensuuria täydennetään proaktiivisella tiedon kehystämisellä ja manipulaatiolla. Kolmas keino on julkisen verkkotilan valvonta esimerkiksi sosiaalisen median osalta, josta voi löytyä tärkeää tietoa toisinajattelijoista ja opposition aktiivisuudesta. Neljäntenä Keremoğlu ja Weidmann mainitsevat internetin roolin autokraatin informaatiodilemman helpottamisessa: autokraatit hyödyntävät hallinnon digitaalisia alustoja julkisen keskustelun palautekanavina. (Keremoğlu & Weidmann 2020, 1693–1694.)

Verkossa tapahtuvan tiedonjakamisen kontrolloinnista ja sensuurista löytyy runsaasti aikaisempaa tutkimusta. Venäjän on omaksunut erityisesti Kiinalta kansalaisten elämää kontrolloivia menetelmiä. Yksi esimerkki yksilön digitaalisen ja fyysisen jalanjäljen kohtaamisesta on Kiinan sosiaalinen pisteytysjärjestelmä. Hallinto kerää kansalaisista suuren määrän tietoa, esimerkiksi pankki-, ostos- ja terveystietoja. Tekoälyn avulla hallinto arvioi kerättyä tietoa ja koostaa kansalaisten sosiaaliset pisteet, joiden avulla pyritään ohjaamaan kansalaisten käyttäytymistä: epäluotettavien henkilöiden elämää voidaan rajoittaa esimerkiksi matkustamisen rajoittamisella tai etuuksia pois sulkemalla. (Kendall-Taylor ym. 2020, 109.)

Tutkija Rui Houn mukaan Kiina hyödyntää verkossa tapahtuvassa mielipiteen valvonnassa kaupallisia yrityksiä, eli omaa poliittista toimintaa toteutetaan ostopalveluina markkinointistrategioita hyödyntäen. Hou huomauttaa, että mielipiteen analysoinnista ja datanlouhinnasta (engl. *data-mining*) löytyy esimerkkejä myös demokratioista: esimerkiksi poliittiset puolueet voivat toteuttaa kohdennettua kampanjointia palveluita tarjoavien yritysten avulla (henkilötietojen keräys ja analysointi). Valtionhallinnon ja tiedonkäsittelyä harjoittavien yritysten yhteistyö kasvattaa autoritaaristen maiden kykyä käsitellä suuria tietomääriä ja avaa mahdollisuuden verkostoituneempaan ja monitasoiseen sosiaaliseen kontrolliin. Autoritaarisessa yhteiskunnassa kaupalliseen markkinointiin tarkoitettuja välineitä, kuten kohdennettua markkinointia, voidaan hyödyntää verkossa toimivien toisinajattelijoiden valvonnassa. (Hou 2017, 419, 422–423.) Houn (2020, 2251) mukaan internetin kontrollointi Kiinassa ei ole vain valtion toimijoiden käsissä, sillä teknologiayritykset ja muut toimijat osallistuvat valvontaan ja mielipiteen manipulaatioon samalla kasvattaen valtion kykyä käsitellä suuria tietomääriä.

Edellä olemme käsitelleet lähinnä keinoja, joilla hallinnot pyrkivät rajaamaan tai estämään verkossa tapahtuvaa yhteiskunnallisesti merkittävää toimintaa. Tämän lisäksi aikaisempi tutkimus on selvittänyt autoritaaristen maiden suosimia epäsuoria tapoja hallita verkossa käytyjä keskusteluja ja toimintaa. Esimerkiksi Johannes Gerchewskin ja Alexander Dukalskisin (2018, 13–14) tutkimuksesta ilmenee, että joissakin tapauksissa autoritaariset maat pyrkivät mieluummin muokkaamaan uhaksi kokemaansa verkon mielipideilmapiiriä kuin estämään kokonaan pääsyn internetiin. Myös Seva Gunitsky (2015, 42–45) on esittänyt, että internetin ”negatiivisen kontrollin” (verkossa tapahtuvan toiminnan sensurointi ja kontrolli) sijaan autoritaariset maat pyrkivät muokkaamaan verkkoa mieleisekseen. Gunitskyn mukaan autoritäärisen järjestelmän vallan vahvistamiseksi käytetään neljää eri toimintatapaa, joita ovat: vastamobilisaatio (engl. *counter mobilization*), diskurssin kehystäminen (*discourse framing*), preferenssien paljastaminen (*preference divulgence*) ja eliitin koordinointi (*elite coordination*).

Kohdatessaan verkossa vastarintaa hallinto voi mobilisoida omia tukijoitaan samoin kuin oppositiojohtajat mobilisoivat kannattajia protesteihin. Diskurssien kehystämisessä on kyse julkisen tilan hallinnasta sosiaalisessa mediassa. Tämä kanava toimii myös toiseen suuntaan eli sosiaalisen median kautta hallinto saa tietoa epäkohdista ja kansalaisten mielipiteistä ja voi ehkäistä niiden eskaloitumista protesteiksi (Gunitsky 2015, 42–45). Tutkijoiden Chun-Chin Chan ja Thun Hong Lin mukaan internetin sensuuri onkin ennen kaikkea reaktiivinen strategia kansalaisyhteiskunnan vaientamisessa. Autokratiat hyödyntävät internetin sensuuria erityisesti informaation manipuloinnissa ja kansalaisyhteiskunnan demobilisaatiossa. Demobilisaatioon pyrkivää sensuuria lisätään silloin, kun hallinto kohtaa välittömän poliittisen riskin. (Chang & Lin 2020, 874, 889–890.)

Politiikkaohjelmien avulla uusia keinoja Venäjän verkon valvontaan?

Tässä kappaleessa pyrimme soveltamaan edellä kuvattua jaottelua (verkossa tapahtuvan toiminnan valvonnan tasot) ja muodostamaan käsityksen Venäjällä käynnissä olevien teknologian kehityshankkeiden merkityksestä osana autoritaarisen hallinnon resilienssin vahvistamista. Tarkasteltavat neljä politiikkaohjelmaa *Turvallinen kaupunki*[4], *Moskovan älykaupunkihanke*[5], *Digitaalinen talous*[6] -hanke ja *Tekoälyn kehittäminen*[7] ovat keskenään erilaisia, vaikka yhdistäviäkin tekijöitä niiden välille löytyy. Hyödynnämme analyysissä näiden ohjelmien perustamisasiakirjoja ja muita viranomaisaineistoja. Tämän suppean aineiston pohjalta emme voi siis muodostaa kokonaisvaltaista näkemystä näiden ohjelmien ja niihin sisältyvien konkreettisten teknologiahankkeiden yhteiskunnallisesta merkityksestä tai edes niistä käydystä keskustelusta Venäjällä.

Kaikkia näitä eri politiikkaohjelmia yhdistävä strategisen tason dokumentti on vuonna 2017 hyväksytty *Venäjän informaatioyhteiskunnan kehittämisen strategia vuosille 2017–2030* (myöhemmin *Informaatioyhteiskunnan kehittämisen strategia*). Strategiassa luodaan suunta-

4 Http://government.ru/docs/16082/

5 Https://docs.cntd.ru/document/537906652#8OO0LM

6 Http://government.ru/docs/28653/

7 Http://www.kremlin.ru/acts/bank/44731

viivat digitalouden kehittämiselle ja linjataan, että kansallinen turvallisuus on huomioitava osana tietoyhteiskunnan kehittämistä (Venäjän presidentti 2017). Jo tätä ennen erilaisissa strategioissa ja kehitysohjelmissa on asetettu tavoitteeksi yhteiskunnan eri osa-alueet kattavan hallinta- ja valvontajärjestelmän kehittäminen (Pynnöniemi 2011; Pynnöniemi & Kari 2016).

Vuonna 2014 Venäjällä ryhdyttiin toteuttamaan koko maan kattavaa *Turvallinen kaupunki* -hanketta. Sen tavoitteena on luoda koko Venäjän kattava yhtenäinen järjestelmä, jonka avulla voidaan vahvistaa yhteiskunnallista turvallisuutta, lain noudattamista ja elinympäristön turvallisuutta. Järjestelmä yhdistää tietoa välittävät, säilyttävät ja analysoivat informaatio- sekä telekommunikaatiosysteemit ja tätä kautta luo edellytykset laaja-alaiselle valvonnalle (Venäjän hallitus 2014, 29). Tätä ennen erilaisia kokeiluita ja laajempia hankekokonaisuuksia on toteutettu Moskovassa ja muissa pilottikaupungeissa (Moskovan kaupunginhallinto 2011). Esimerkiksi *Moskovan älykaupunki* -hankkeen puitteissa on tarkoitus hyödyntää massadataa päätöksenteossa sekä tehostaa kaupungin taloutta ja hyödyntää julkisen ja yksityisen kumppanuuden mahdollisuuksia tieto-, digi- ja tietoliikenteen alalla.

Digitaalinen talous -projekti on puolestaan kansallinen hanke, jonka tavoitteena on lisätä digitaalisten ratkaisujen hyödyntämistä taloudessa ja yhteiskunnassa koko Venäjän laajuisesti. Hankkeen vastuuministeriö on Venäjän digitaalisesta kehityksestä, kommunikaatiosta ja massamediasta vastaava ministeriö (Minkomsvjaz). Tämänkin digitalisaatiota eri elämänalueilla edistävän hankkeen tavoitteet ovat suurisuuntaisia. Hanke jakautuu seitsemään alaohjelmaan: *Digitaalisen ympäristön normatiivinen sääntely*, *Työvoimaa digitalouden tarpeisiin*, *Tietoinfrastruktuuri*, *Tietoturvallisuus*, *Digitaaliset teknologiat*, *Digitaalinen valtionhallinto* ja *Tekoäly* (Minkomsvjaz 2021). Venäjällä on myös vuoteen 2030 ulottuva erillinen tekoälyn kehittämisen strategia (Eskonmaa 2021). Tässä strategiassa (Venäjän presidentti 2019) määritellään tekoälyn kehittämisen keskeisimmät tavoitteet ja tehtävät sekä linjataan, miten tekoälyä voidaan hyödyntää kansallisen edun ja kansallisten strategisten prioriteettien tavoitteissa. Strategian on tarkoitus toimia pohjana eri valtiontoimijoiden, kuten federaatiosubjektien tai valtio-omisteisten yritysten tekoälystrategioille. Kuten edellisetkin teknologiahankkeet ja ohjelmat, myös tekoälystrategian toteuttaminen nähdään kokonaisvaltaisena, kaikkia eri yhteiskunnan osa-alueita koskettavana tehtävänä. (Mt.)

Venäjän digitalisaatio- ja teknologiahankkeita tarkastellessa on syytä huomioida, että alueelliset erot hankkeiden osalta voivat olla suuria. Osa käsiteltävistä hankkeista on paikallisia, osa koko Venäjän laajuisia. Toimijoiden osalta hankkeita yhdistää monipuolinen toimijakenttä: valtiojohtoisissa projekteissa on mukana niin eri tason viranomaisia, eri organisaatioita kuin yrityksiäkin. Hankkeet eivät ole toisistaan irrallisia vaan ne ovat osittain päällekkäisiä. Ainakin *Digitaalinen talous* -hankeen ja *Turvallinen kaupunki* -hankkeen yhteyksistä on selkeitä viitteitä. Kumpaankin hankkeeseen liittyvistä projekteista löytyy esimerkkejä tekoälyn hyödyntämisestä. Digitalisaatio ja teknologiahankkeiden mahdollistaminen näkyy myös lainsäädännössä. Vuoden 2020 heinäkuussa allekirjoitettiin laki, joka tuo helpotuksia digitaalisten innovaatioiden kehittämiseen. Laki sallii digitaalisten ratkaisujen kehittämistä koskevien erityislakikokeilujen lanseeraamisen tietyillä aloilla, esimerkiksi terveydenhuollossa,

maataloudessa ja teollisuuden alalla. Lain tavoitteena on esimerkiksi luoda uutta taloudellista toimintaa, parantaa kilpailua ja tuotteiden sekä tuotteiden laatua. (Venäjän federaation laki 2020.)

Viime vuosina yksi keskeisistä lähtökohdista Venäjän internet-infrastruktuurin kehittämisessä on ollut pyrkimys korvata ulkomainen teknologia kotimaisilla laitteistoratkaisuilla. Tämä todetaan suoraan *Informaatioyhteiskunnan kehittämisen strategiassa,* joka linjaa, että informaatioinfrastruktuurin vakaan toiminnan edellytyksenä on tuontilaitteiston korvaaminen venäläisillä vaihtoehdoilla (Venäjän presidentti 2017). Tekoälyn kehittämisstrategiasta puolestaan todetaan, että Venäjän teknologinen suvereniteetti on yksi tekoälyn kehittämisen perusperiaattein (Venäjän presidentti 2019). Yhteenvetona eri strategioista voidaan todeta, että ne viestivät Venäjän halusta eriytyä globaalista internetistä ja lisätä kotimaisen internet-infrastruktuurin käyttöä. On kuitenkin hyvä muistaa, että lähitulevaisuudessa Venäjä on riippuvainen kiinalaisesta teknologiasta (Sinkkonen & Lassila 2020, 7).

Lopuksi

Koronapandemian alkuvaiheessa arvioitiin, että tilanteen pitkittyminen muodostaisi vakavan haasteen Venäjän poliittiselle järjestelmälle (Bovt 2020; Galeotti 2020; Kolesnikov 2020). Pandemian pitkittyessä Venäjän poliittinen johto on pyrkinyt (ja tätä kirjoittaessa onnistunut) rajamaan nykyisen poliittisen järjestelmän avoimesti haastavat poliittiset vaihtoehdot keskustelun ulkopuolelle. Näin se pyrkii estämään tilanteen, jossa yhteiskunnallinen tyytymättömyys kanavoituisi Kremlille epämieluisana tai nykyisen poliittisen johdon asemaa horjuttavana poliittisena toimintana (Pynnöniemi & Helin 2020).

Samalla on kuitenkin syytä tähdentää, että autoritaarisen hallinnon resilienssiin liittyy monia epävarmuustekijöitä, joiden vuoksi poliittisten vaikutusten arviointi on vaikeaa. Tätä artikkelia varten läpikäydystä tutkimuskirjallisuudesta nousee kuitenkin selkeästi esiin ajatus, että autoritaariset maat hyödyntävät uutta teknologiaa ennakoivasti. Kyse on kokonaisvaltaisesta varautumisesta erilaisiin häiriötilanteisiin sotilaallisista konflikteista sisäpoliittisiin levottomuuksiin ja luonnonkatastrofeihin. Venäjän osalta verkossa tapahtuva toiminta nähdään herkästi alustana, jonka kautta pyritään vaikuttamaan Venäjän poliittiseen tasapainoon (Sotilasdoktriini 2014). Aikaisemmissa tutkimuksissa on eritelty erilaisia vaikuttamisen tasoja, joista verkossa tapahtuva toiminta on vain yksi. Näitä muita tasoja ovat internet-infrastruktuuri, ylikansalliset ja kansalliset toimijat sekä yksilön digitaalinen jalanjälki.

Tässä artikkelissa lyhyesti esitellyt teknologian kehityshankkeet vaikuttavat kaikilla näillä tasoilla. Analysoiduissa viranomaisaineistoissa nimetään erilaisia turvallisuusuhkia ja riskejä, mutta jätetään avoimeksi konkreettiset keinot turvallisuuden parantamiseksi. Erimerkiksi Moskovan kaupungin hankkeissa verkon kautta tapahtuva valvonta (videokameroiden tuottaman datan analysointi) nähdään osana yhteiskunnallisen ja yksilöiden turvallisuuden parantamista. Eri hankkeille asetettujen tavoitteiden analysointi ei kuitenkaan riitä niiden laajemman yhteiskunnallisen vaikutuksen arvioimiseksi. Tarvitaan tarkempaa analyysiä teknologiahankkeiden toteutuksesta käytännössä, niitä ohjaavan lainsäädännön muutoksista

sekä laajemmin hankkeiden yhteiskunnallisesta vaikuttavuudesta – tai sen puutteesta. Toivomme, että tämä katsausartikkeli osaltaan inspiroi tutkijoita syvällisemmän analyysin äärelle.

Lähteet

Balashova, Anna (2021): "Vlasti objasnili 'prizemlenie' IT-kompanij povedeniem Google i TikToks Rossijskie jurlitsa etih kompanij ne mogut otvetit". *RBC*, 25.5.2021. Https://www.rbc.ru/technology_and_media/24/05/2021/60aa27c69a794721ea341752, 17.3.2022.

Bondarev, Denis, Dmitri Nosonov & Anna Balašova (2016): "Roskomnadzor natšal blokirovku LinkedIn". *RBC*, 17.11.2016. Https://www.rbc.ru/technology_and_media/17/11/2016/5829cb809a7947c578b9cfcd, 17.3.2022.

Bovt, Georgy (2020): "Can Russia's Power Vertical deal with a pandemic?". *Riddle*, 13.4.2020. Https://www.ridl.io/en/can-russia-s-power-vertical-deal-with-apandemic/, 17.3.2022.

Chang, Chun-Chih & Thung-Hong Lin (2020): "Autocracy login: Internet censorship and civil society in the digital age". *Democratization*, 27(5), 874–895.

DeNardis, Laura (2012): "Hidden levers of internet control: An infrastructure-based theory of Internet governance". *Information, Communication & Society*, 15(5), 720–738.

Dragu, Tiberiu & Yonatan Lupu (2021): "Digital authoritarianism and the future of human rights". *International Organization*, 75, 991–1017.

Duma (2019): Prinjat zakon o "suverennom internete", 16.4.2019. Http://duma.gov.ru/news/44551/, 17.3.2022.

Epifanova, Alena (2020): "Deciphering Russia's 'sovereign internet law' – Tightening control and accelerating the splinternet". *DGAP Analysis*, 2. Https://dgap.org/de/node/33332, 17.3.2022.

Eskonmaa, Juuso (2021): *Tekoäly ja voimatasapaino: Venäjän federaation kansallinen tekoälystrategia ja Venäjän asema suurvaltana*. Politiikan tutkimuksen pro gradu -tutkielma, Johtamisen ja talouden tiedekunta. Tampere: Tampereen yliopisto.

Feldstein, Steven (2019): "The road to digital unfreedom: How artificial intelligence is reshaping repression". *Journal of Democracy*, 30(1), 40–52.

Galeotti, Mark (2020): "If Putin wants to use the military against the coronavirus, he'll need to trust his governors or step up himself". *Moscow Times*, 14.4.2020. Https://www.themoscowtimes.com/2020/04/14/if-putin-wantsto-use-the-military-against-covid-hell-need-either-to-trust-his-governors-orstep-up-himself-a69982, 17.3.2022.

Gavriljuk, Anastasija (2021): "Sboi za nezavisimost". *Kommersant*, 9.4.2021. Https://www.kommersant.ru/doc/4763212, 17.3.2022.

Gerschewski, Johannes & Alexander Dukalskis (2018): "How the internet can reinforce authoritarian regimes: The case of North Korea". *Georgetown Journal of International Affairs*, 19(1), 12–19.

Gunitsky, Seva (2015): "Corrupting the cyber-commons: Social media as a tool of autocratic stability". *Perspectives on Politics*, 13(1), 42–54.

Guriev, Sergei & Daniel Treisman (2020): "A theory of informational autocracy". *Journal of Public Economics*, 186, art. 104158. DOI: 10.1016/j.jpubeco.2020.104158.

Hou, Rui (2017): "Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China". *Surveillance &* Society, 15 (3–4), 418–424.

Hou, Rui (2020): "The commercialisation of Internet-opinion management: How the market is engaged in state control in China". *New Media & Society*, 22(12), 2238–2256.

Interfax (2021): "V Moskve s ijulja vvedut pravovoi režim dlja vnedrenija tehnologij iskustvennogo intellekta". *Interfax*, 24.4.2020. Https://www.interfax.ru/moscow/705872, 17.3.2022.

Kendall-Taylor, Andrea, Erica Frantz & Joseph Wright (2020): "The digital dictators: How technology strengthens autocracy". *Foreign Affairs*, 99(2), 109–115.

Keremoğlu, Eda & Nils B. Weidmann (2020): "How dictators control the internet: A review essay". *Comparative Political Studies*, 53(10–11), 1690–1703.

Kolesnikov, Andrei (2020): "Are Russian's finally sick of Putin?". *Carnegie Moscow Center*, 7.4.2020. Https://carnegie.ru/commentary/81485, 17.3.2022.

Kukkola, Juha (2020): "The Russian national segment of the internet as a source of structural cyber asymmetry". Teoksessa: A. Ertan, K. Floyd, P. Pernik & T. Stevens (toim.) *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinna: NATO CCDCOE Publications, 9–30.

Kukkola, Juha (2021): *Rakenteellisen kyberassymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä*. Puolustusvoimien tutkimuslaitos, julkaisuja 13. Helsinki: Puolustusvoimat.

Martynov, Kirill (2020): "Svojeobraznaja tragedija diktatury". *Echo Moskvy*, 14.4.2020. Https://echo.msk.ru/blog/kirillmartyn/2624654-echo/, 17.3.2022.

Minkomsvjaz (2021): Tsifrovaja ekonomika RF. Https://digital.gov.ru/ru/activity/directions/858/, 17.3.2022.

Moore, Martin & Damian Tambini (2018): *Digital dominance: The power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press.

Moskovan kaupunginhallinto (2011): Ob utverždenii gosudarstvennoi programmy goroda Moskvy "Razvitie tsifrovoi sredy i innovatsii", 9.8.2011. Https://docs.cntd.ru/document/537906652#8OO0LM, 17.3.2022.

Moss, Dana M. (2018): "The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora". *Globalizations*, 15(2), 265–282.

Pynnöniemi, Katri (2011): *Securing Russia? New security law raises more questions than it answers*. FIIA Comment. Helsinki: Ulkopoliittinen instituutti. Http://www.fiia.fi/fi/publication/168/securing_russia/, 17.3.2022.

Pynnöniemi, Katri & Martti Kari (2016): Uusi informaatioturvallisuuden doktriini: Venäjä tehostaa piiritetyn kyberlinnakkeen vartiointia. FIIA Comment 26. Helsinki: Ulkopoliittinen instituutti. Https://www.fiia.fi/julkaisu/uusi-informaatioturvallisuuden-doktriini, 17.3.2022.

Pynnöniemi, Katri & Outi Helin (2020): *Muuttaako koronaepidemia Venäjää? Lähtökohtia kriisin poliittisten vaikutusten arviointiin*. Sotataidon laitos, julkaisusarja 3: Työpapereita 17. Helsinki: Maanpuolustuskorkeakoulu.

Ristolainen, Mari (2017): "Should 'RuNet 2020' be taken seriously? Contradictory views about cyber security between Russia and the West". *Journal of Information Warfare,* 16(4), 113–131.

Roache, Madeline (2021): "How Russia is stepping up its campaign to control the internet". *Time*, 1.4.2021. Https://time.com/5951834/russia-control-internet/, 17.3.2022.

Rød, Espen Geelmuyden & Nils B. Weidmann (2015): "Empowering activists or autocrats? The Internet in authoritarian regimes". *Journal of Peace Research,* 52(3), 338–351.

Sinkkonen, Elina & Jussi Lassila (2020): *Digital authoritarianism in China and Russia: Common goals and diverging standpoints in the era of great power rivalry*. FIIA Briefing Paper. Helsinki: Ulkopoliittinen instituutti. Https://www.fiia.fi/julkaisu/digital-authoritarianism-in-china-and-russia, 17.3.2022.

Sotilasdoktriini (2014): Voennaja doktrina Rossijskoi Federatsii, 25.12.2014. Https://docs.cntd.ru/document/420246589.

Vendil Pallin, Caroline (2017): "Internet control through ownership: the case of Russia". *Post-Soviet Affairs*, 33(1), 16–33.

Vendil Pallin, Caroline & Mattias Hjelm (2021): *Moscow´s digital offensive: Building sovereignty in cyberspace*. FOI Memo, 7521, Https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI%20Memo%207521, 17.3.2022.

Venäjän federaation laki (2019): O vnesenii izmeneni v Federalnyi zakon "O svjazi" i Federalnyi zakon "Ob informatsii, informatsionnyh tehnologijah i o zaštšite informatsii", 1.5.2019. Http://www.kremlin.ru/acts/bank/44230/page/1, 17.3.2022.

Venäjän federaation laki (2020): Ob eksperimentalnyh pravovyh režimah v sfere tsifrocyh innovatsij v Rossijskoi Federatsii, 31.7.2020. Http://www.kremlin.ru/acts/bank/45796, 17.3.2022.

Venäjän hallitus (2014): KONTSEPTSIJA postrojenija i razvitija apparatno-programmnovo kompleksa ”Bezopasnyi gorod”, 3.12.2014. Http://government.ru/docs/16082/, 17.3.2022.

Venäjän presidentti (2017): Ukaz Prezidenta Rossijskoi Federatsii ot 09.05.2017 g. No 203 – O strategii razvitija informatsionnogo obštšestva v Rossijskoi Federatsii na 2017 – 2030 gody, 9.5.2017, Http://www.kremlin.ru/acts/bank/41919, 17.3.2022.

Venäjän presidentti (2019): Natsionalnaja strategija: razvitija iskusstvennogo intellekta na period do 2030 goda, 10.10.2019. Http://www.kremlin.ru/acts/bank/44731, 17.3.2022.

Xu, Xu (2021): ”To repress or to co-opt? Authoritarian control in the age of digital surveillance”. *American Journal of Political Science*, 65(2), 309–325.

Yayboke, Erol & Sam Brannen (2020): *Promote and build – A strategic approach to digital authoritarianism*. Washington DC: Center for Strategic and International Studies (CSIS). Https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism, 17.3.2022.

English Summary

Surveillance and technology: The case of Russia

Outi Helin & Katri Pynnöniemi

With the corona pandemic, regulations restricting the normal life of citizens have been introduced worldwide. To track the movement of people, different countries have used various technology applications, such as QR passes and tracking based on telephone data and location. However, the way in which these technologies are used varies between democratic and authoritarian countries. In this article, we provide an overview of recent research on the effects of new technologies on the resilience of authoritarian countries. Previous research has sought to model different paths of influence, and it also reveals the efforts of authoritarian countries to implement proactive online surveillance. At the end of the article, we will discuss a few policy programs under which Russia will develop these technologies.

Keywords: authoritarian governance, technology, surveillance, Russia