Ruth Kaila

VENÄJÄ KANSAINVÄLISENÄ TALOUTENA JA SUVEREENI INTERNET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Kaila, Ruth
Venäjä kansainvälisenä taloutena ja suvereeni Internet
Jyväskylä: Jyväskylän yliopisto, 2021, 53+12 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Kari, Martti

Internetin avoimuutta on alettu kyseenalaistaa viimeisten vuosien aikana, ja monet valtiot ovat lisänneet kontrollia Internetin segmentistään. Venäjä onnistui joulukuussa 2019 hetkellisesti irrottamaan oman Internetin segmenttinsä kansainvälisestä verkosta. Tämän tutkimuksen tavoitteena on selvittää, mitä edellytyksiä Venäjän kaltaisella kansainvälisellä taloudella kansainvälisine rahoitusjärjestelmineen on sulkea Internetin segmenttinsä. Tutkimusmenetelminä käytetään verkostoja ja dynaamisia systeemejä mallintavaa verkkoteoriaa sekä vertailevaa tutkimusta.

Tutkimuksen ensimmäisessä osassa todetaan, että vaikka Venäjällä lähitulevaisuudessa olisi tekniset edellytykset sekä suvereeniin Internetin segmenttiin, tulisi tilannetta tarkastella laajemmasta näkökulmasta. Irtautuminen ei näytä yksinkertaiselta, kun tarkasteluun otetaan mukaan vaikutukset Venäjän talous- ja rahoitusjärjestelmiin. Nämä järjestelmät ovat erottamaton osa globaaleja keskinäisriippuvia talous- ja rahoitusjärjestelmiä, joiden voima on nimenomaan maailmanlaajuisessa käytössä. Järjestelmiä ei voi täysin korvata kotimaisilla järjestelmillä.

Talous- ja rahajärjestelmien lisäksi Venäjällä on kiinteät yhteydet länsimaihin Internetin tarjoaman sisällön kautta. Erityisesti suurimmat länsimaiset sosiaalisen median alustat ovat Venäjällä erittäin suosittuja ja niitä on vaikea täysin korvata kotimaisilla vastaavilla alustoilla.

Tutkimuksen toisessa osassa Venäjää verrataan Kiinaan, jolla on suvereeni Internetin segmentti. Valtiot eroavat toisistaan niin Internetin segmenttien kuin talous- ja rahoitusjärjestelmienkin rakentumisessa. Venäjän Internetin segmentti on syntynyt osana kansainvälistä verkostoa, ja sen kautta Venäjän talous- ja rahoitusjärjestelmät ovat kiinteässä yhteydessä kansainvälisiin järjestelmiin. Kiinan Internetin segmentti on alun perin suunniteltu mahdollisimman irralliseksi globaalista Internetistä. Kiinan talous- ja rahoitusjärjestelmien tavoin sitä ollaan hallitusti avaamassa kansainväliseen talouden ja rahoituksen toimintaympäristöön. Siinä, missä Venäjä pyrkii varmistamaan Internetin segmenttinsä suvereeniuden sulkeutumalla, Kiinan strategiana on monipuolisesti ja monialaisesti varmistaa sellainen valta-asema kansainvälisessä yhteistyössä, että se pystyy pitämään Internetin segmenttinsä suvereenina. Pitkällä tähtäimellä Kiinan valitsema strategia tuntuu suvereenin Internetin projektin kannalta toimivammalta.

Asiasanat: Venäjän suvereeni Internet, Venäjän rahoitusjärjestelmä, Kiinan suvereeni Internet, kyberturvallisuus, strateginen autonomia, kriittinen infrastruktuuri, globaali keskinäisriippuvuus, tietoverkot

ABSTRACT

Kaila, Ruth
Russia as an International Economy and the Sovereign Internet
Jyväskylä: University of Jyväskylä, 2021, 53+12 pp.
Cyber Security, Master's Thesis
Supervisor: Kari, Martti

In recent years, voices have been raised to question the openness of the Internet, and many states have increased control over their Internet segments. In December 2019, Russia momentarily succeeded in disconnecting its Internet segment from the international network. This study aims to find out what conditions a state like Russia with its international economic and financial systems has for a sovereign segment of the Internet. Network theory and comparative research were used as research methods.

The study concluded that even if Russia had the technical conditions for a sovereign Internet segment soon, the situation should be viewed from a broader perspective. The effects of sovereign Internet on Russia's economic and financial systems should be included in the analysis. Russia is an active player in international trade and international finance. The power of the Internet as well as the economic and financial systems lies precisely in their worldwide use. These systems cannot be completely replaced by domestic systems.

In addition to international economic and financial systems, Russia has important connections to Western countries through the content provided by Internet. In particular, the largest Western platforms are popular in Russia, and replacing them with similar domestic ones is difficult.

The study compared Russia to China, which has a sovereign Internet segment. These two states differ in the way their Internet segments have evaluated, as well as in their economic and financial systems. The Russian Internet segment has emerged as part of a global network, and its economic and financial systems are part of global systems. The Chinese Internet segment was designed to be as sovereign as possible. Like China's economic and financial systems, it is being opened up to the world in a controlled manner.

The study concludes that where Russia seeks to secure the sovereignty of its Internet segment through closure, China's strategy is to secure such dominance in international cooperation and trade that the state will be able to hold the sovereignty of its Internet segment in the future. In the long run, the strategy chosen by China seems more effective in the project of sovereign Internet.

Keywords: Russia's sovereign Internet, Russia's financial system, China's sovereign Internet, cybersecurity, strategic autonomy, critical infrastructure, global interdependence, communication networks

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Internetin alkuperäiset arkkitehdit uskoivat avoimuuteen sekä käytännöllisistä että aatteellisista syistä. (Drake ym., 2016) Avoimuus ja avoimet teknologiat ovat edesauttaneet Internetin maailmanlaajuista kehittymistä ja leviämistä. Viimeisten vuosien aikana Internetin täydellistä avoimuutta on alettu kyseenalaistaa muun muassa yksityisyyden suojaan ja kansalliseen turvallisuuteen vedoten. Monet valtiot ovat lisänneet kontrollia Internetin segmenteistään. Keskustelua ovat johtaneet Kiina ja Venäjä. (Budnitsky & Jia, 2018). Näyttää siltä, että Internet on fragmentoitumassa.

Venäjän Internetin segmentti syntyi liberaalissa ympäristössä. Se on sittemmin liitetty narratiiviin Internetistä länsimaisena kumouksellisena teknologiana, sosiaalisten ja poliittisten paheiden lähteenä sekä uhkana Venäjälle. (Tselikov, 2014) Vuoden 2016 Informaatioturvallisuuden doktriini laajentaa kyberturvallisuuden informaatioturvallisuudeksi, joka määritetään yksilön, yhteisön ja valtion turvallisuutena sisäisistä ja ulkoisista informaatiouhkista. Informaatioalue käsitetään laajasti, siihen sisältyvät informaation lisäksi muun muassa informaatio-objektit, informaatiosysteemit, kommunikaatioverkot ja informaatioteknologiat. (Ministry of Foreign Affairs of the Russian Federation, 2016) Venäjän tehtävänä ei ole turvata ainoastaan informaatiota vaan koko venäläinen kulttuuri.

Venäjän vuoden 2019 'Suvereenin Internetin lain' mukaan Internet-palveluntarjoajien tulee taata toiminnan jatkuvuus myös tilanteessa, jossa ulkomainen taho yrittää eristää Venäjän kansainvälisestä verkosta. Tässä tilanteessa Venäjän tiedotusvälineitä valvova Roskomnadzor koordinoisi verkkoliikennettä. (Epifanova, 2020) Joulukuussa 2019 uutisoitiin, että kokeilu venäläisen segmentin irrottamiseksi kansainvälisestä verkosta oli tehty onnistuneesti. (BBC News, 2019)

Venäjä on perustellut pyrkimystä suvereeniin Internetiin ja oman segmentin irrottamiseen defensiivisellä tarpeella. Suvereeni verkko suojaisi riskiltä joutua suljetuksi kansainvälisestä verkosta ulkopuolisen tahon toimesta. (Ministry of Digital Development, Communications and Mass Media of Russian Federation, 2014) Venäläisen segmentin irrottaminen on kuitenkin yhdistetty myös maan haluun kontrolloida omia kansalaisiaan, sitä minne heillä on pääsy sekä mitä verkossa liikkuu.

Venäjän täytyy suvereenia verkkoa varten toisintaa ne laitteet ja ohjelmistot, jotka Internet-liikennettä ohjaavat. Erityisesti Venäjä tarvitsee oman verkkotunnuksia IP-osoitteiksi muuntavan nimipalvelujärjestelmän (Domain Name System DNS). Tällä hetkellä maailman 13 nimipalveluoperaattorista vain 3 on Yhdysvaltojen ulkopuolella. (IANA, 2021b) Venäjä on ilmoittanut kehittävänsä oman nimipalvelujärjestelmänsä. Sillä on myös hallussaan kopioita verkon ydinosoitekirjasta. Kansainvälisestä verkosta irrotettu segmentti voi käyttää näitä kopioita, mutta niihin ei tule päivityksiä. Oman nimipalvelujärjestelmän rakentaminen ei teknisesti ole mahdotonta, muiden käyttäjien saaminen siihen sen sijaan saattaa olla.

Vaikka Venäjä pystyisi selvittämään suvereenin Internetin tekniset haasteet, hankaloittavat keskinäisriippuvaisessa maailmassa useat seikat kansainvälisestä verkosta irtautumista. Venäjä on kansainvälinen talous, jolla on kiinteät taloudelliset ja yhteiskunnalliset suhteet maan rajojen ulkopuolelle. Vuonna 2016 Venäjän valtio budjetista 36 prosenttia tuli öljyn ja kaasun viennistä. (EIA, 2017) Puolestaan tuonnin osuus elintarvikkeista arvolla mitattuna oli vuonna 2020 arviolta 30 prosenttia. (Statista, 2021s) Internetin tavoin rahoitusjärjestelmä muodostaa kansainvälisen verkoston kriittisine toimijoineen. Venäjä tuskin pystyy tai edes tahtoo täysin eristäytyä kansainvälisestä taloudesta ja investoinneista.

Venäjä ja Kiina ovat 2000-luvulla nousseet modernin ajan merkittäviksi kansainvälisiksi tekijöiksi. Ne ovat aktiivisesti osallistuneet keskusteluun Internetin hallinnasta sekä Yhdysvaltojen teknologisesta ja hallinnollisesta valta-asemasta. (Polyakova & Meserole, 2019) Kiinan sosiaalisen median alusta Baidu ja Venäjän alusta Yandex ovat olleet kiinteästi ja näkyvästi mukana rakentamassa maabrändiä. Nämä kaksi valtiota ovat myös niitä harvoja maita, joissa kotimaiset verkkohakupalvelut ja sosiaalisen median alustat ovat kansainvälisiä suositumpia. (Budnitsky & Jia, 2018)

Kiinan konkreettisin suvereenin Internetin mahdollistaja on Kiinan suuri palomuuri, the Great Firewall of China. Palomuuri estää selektiivisesti tiettyjä Internet-osoitteita, sanoja ja IP-osoitteita. Ratkaisu ei ole täydellinen, koska ohjelmistopohjaisena suodatusta voidaan kiertää. (Griffiths, 2019) Tätä palomuuria tuskin suoraan voitaisiin toisintaa Venäjällä, joka on sekä Kiinaa avoimempi ja sitä huomattavasti pienempi talous. (Polyakova & Meserole, 2019) Lisäksi Kiinasta poiketen Venäjällä käytetään omien sosiaalisen median yritysten lisäksi aktiivisesti yhdysvaltalaisia alustayrityksiä, erityisesti Googlea, Facebookia ja Amazonia. (Statista, 2021x)

1.1 Tutkimusongelma, tutkimuskysymykset ja tutkimuksen rajaus

Tutkimusongelma on, missä määrin Venäjä kansainvälisenä taloutena pystyy irrottamaan oman Internetin segmenttinsä kansainvälisestä verkosta. Ongelmaa tarkastellaan kolmen tutkimuskysymyksen kautta:

1. Mitä edellytyksiä Venäjällä on suvereenille Internetille, kun projektia tarkastellaan Internetin teknisen, loogisen ja sosiaalisen tason kautta?
2. Miten suvereeni Internet sopii Venäjälle avoimena ja hyvin verkottuneena kansainvälisenä taloutena?
3. Kiinalla on suvereeni Internet. Miten maiden suvereenin Internetin strategiat eroavat toisistaan? Voisiko Venäjä seurata Kiinan tekemiä ratkaisuja, vai ovatko maat lähtökohdiltaan liian erilaiset?

Tutkimusongelma on laaja, ja tutkimuksessa yhdistetään monia näkökulmia. Kutakin näkökulmaa, muun muassa kyberturvallisuutta ja kansainvälisiä talous- ja

rahoitusjärjestelmiä taustoitetaan vain niiltä osin kuin se tutkimuksen kannalta on tarpeellista.

Tutkimus kohdistuu Venäjän maantieteellisen alueen Internetin segmenttiin, ei Runetiin, joka viittaa venäjänkieliseen Internetin sisältöön myös Venäjän rajojen ulkopuolella. Tutkimusaineisto joudutaan rajoittamaan englanninkieliseen materiaaliin, minkä seurauksena käytetään paikoin sekundäärisiä lähteitä.

1.2 Tutkimuksen tavoite, rajoitukset, tutkimusmenetelmä ja tutkimustulokset

Tutkimuksen tavoitteena on selvittää, mitä edellytyksiä Venäjän kaltaisella kansainvälisellä taloudella kansainvälisine rahoitusjärjestelmineen on sulkea Internetin segmenttinsä. Tutkimuksen ensimmäisenä tavoitteena on tunnistaa tärkeimpiä kriittisiä tekijöitä, joilla on vaikutusta Venäjän suvereenin Internetin toteuttamiseen. Nämä tekijät liittyvät Internet-järjestelmän lisäksi talouden järjestelmiin. Tutkimuksen toisena tavoitteena on laadullisesti arvioida, miten kriittisiä tunnistetut tekijät lopulta ovat suvereenin Internetin projektin kannalta ja miten realistinen suvereenin Internetin projekti tästä näkökulmasta on.

Tutkimuksessa tarkastellaan suvereenin Internetin projektia talouden ja rahoitusjärjestelmän näkökulmasta. Valittu tutkimusnäkökulma on väistämättä moninkertainen pelkistys. Digitalisoituneessa keskinäisriippuvassa maailmassa Internet vaikuttaa myös moniin muihin sektoreihin, kuten liikenteeseen, energiajärjestelmään, terveydenhuoltoon, tietoliikenteeseen, turvallisuuteen, demokratian toteutumiseen, avaruuteen ja puolustukseen. (EU, 2020) Rahoitusjärjestelmän lisäksi monet muut verkostot ja järjestelmät muodostavat osan kriittistä infrastruktuuria. Suvereenia internetiä ei ole mahdollista tutkia arvioiden kaikkia niitä erilaisia vaikutuksia, joita sen toteuttamisesta voisi syntyä.

Tutkimus toteutetaan dokumentaariseen aineistoon perustuvana teoreettisena laadullisena tapaustutkimuksena. Tutkimuksessa on kaksi osaa, joihin sovelletaan erilaisia tutkimusmenetelmiä ja aineiston analyysimenetelmiä. Ensimmäisessä osassa, jossa tutkitaan avoimia verkostoja ja pyritään tunnistamaan niiden kriittisiä solmuja, käytetään verkostoja ja dynaamisia systeemejä mallintavaa verkkoteoriaa sekä tilastollista dataa. Toisessa osassa tehdään vertailevaa tutkimusta Venäjän ja Kiinan välillä. Vertailukohteiden valinnassa tukeudutaan ensimmäisen osan tuloksiin sekä makroekonomisiin indikaattoreihin.

Ensimmäisen ja toisen osan tutkimustulokset täydentävät ja vahvistavat toisiaan. Venäjä on avoin kansainvälistä kauppaa käyvä talous, jonka Internetin segmentti on historiallisesti syntynyt osana kansainvälistä Internetiä. Venäjän talous- ja rahoitusjärjestelmät ovat osa kansainvälisiä talous- ja rahoitusjärjestelmiä. Kumpikin järjestelmä on riippuvainen Internetin toiminnasta. (EU, 2020) Internetin segmentin ja sen myötä talouden ja rahoitusjärjestelmän osittainenkin sulkeminen on haastavaa. Historiallisesti sulkeutunut Kiina puolestaan on halli-

tusti avannut suljettuna syntynyttä Internetin segmenttiään sekä talous- ja rahoitusjärjestelmiänsä. Näiden suljettujen järjestelmien osittainen avaaminen on helpompaa kuin vastaavien avointen järjestelmien osittainen sulkeminen.

Erityisesti Kiinan strategiana on ollut luoda sellaisia kansainvälisiä taloudellisia ja muita suhteita ja kannustimia, jotka vahvistavat mahdollisuutta suvereenin Internetin ylläpitämiseen. Venäjän suvereenin Internetin strategia on rajoitetumpi ja perustuu lähinnä sulkemiseen, ei kansainväliseen vuorovaikutuksen voimistamiseen. Tuntuisi siltä, että mikäli tavoitteena on suvereeni Internet, Kiinan strategia on pitkällä aikavälillä toimivampi.

Tutkimustuloksia voidaan soveltaa Venäjän suvereenin Internetin projektia laajemmin. Tutkimuksessa tarkastellaan monia strategiseen autonomiaan liittyviä kysymyksiä. Kuka hallitsee ja miten Internetiä? Miten kansainvälistä rahoitusjärjestelmää hallinnoidaan? Entä sosiaalisen median alustoja? Kenellä on Internetin edellyttämä teknologia, komponentteja ja tekoälyyn pohjautuvia ohjelmistoja? Miten tietoverkkoja koskevat ratkaisut heijastuvat huoltovarmuuteen? Mikä on erityyppisten järjestelmien kriisinsietokyky eli resilienssi?

1.3 Tutkimuksen rakenne

Tutkimuksen johdannossa esitellään tutkimuksen aihe, tutkimusongelma ja tutkimuksen tavoite. Sitä seuraa tiivis kirjallisuuskatsaus luvussa 2. Luvussa 3 esitellään tutkimusaineisto ja tutkimusmetodi. Luvuissa 4 ja 5 taustoitetaan Venäjän lähtökohtia oman Internetin segmentin irrottamiseen. Näissä luvuissa vastataan ensimmäiseen ja toiseen tutkimuskysymykseen. Luku 4 käsittelee Internetin avoimia ja suljettuja verkostoja, luku 5 puolestaan tarkastellaan rahoitusjärjestelmän avoimia ja suljettuja verkostoja sekä taloutta yleisemmin. Luvussa 6 verrataan Venäjää sekä Kiinaa soveltuvin osin. Tässä luvussa vastataan kolmanteen tutkimuskysymykseen. Luku 7 esittelee tutkimustulokset, ja johtopäätökset päättävät tutkimusraportin luvussa 8.

2 KIRJALLISUUSKATSAUS

Luvussa määritetään aluksi tutkimuksessa käytetyt keskeiset käsitteet. Tämän jälkeen kuvataan tutkimuskirjallisuutta ja esitetään kirjallisuutta täydentävä uusi tutkimusnäkökulma.

2.1 Käsitteiden määrittely

Tutkimuksen keskeisiä käsitteitä ovat suvereeni Internet, kyberturvallisuus, informaatioturvallisuus, fragmentoituminen sekä avoin talous ja rahoitusjärjestelmä. Internetin segmentillä tarkoitetaan tässä tutkimuksessa tietyn valtion maantieteellisellä alueella sijaitsevaa Internet-verkoston osaa. Suvereenilla Internetillä tai suvereenin Internetin segmentillä viitataan sellaiseen Internetin segmenttiin, joka pystyisi pidemmän aikaa toimimaan irrallaan kansainvälisestä Internetistä.

Kyber-sana esiintyy tutkimuksessa määriteosana sanoissa kyberturvallisuus, kyberuhat ja kybersuvereenisuus. Sanaa käytetään Turvallisuuskomitean (2018) kuvailun mukaisesti sellaisissa merkitysyhteyksissä, jotka liittyvät digitaalisessa muodossa olevan informaation käsittelyyn. Kyber-sana esiintyy myös kirjallisuustutkimusta esittelevässä luvussa. Tässä yhteydessä sanalla viitataan kunkin tutkimuksen käyttämään tulkintaan. Tutkimusten käyttämiä tulkintoja ei erikseen avata.

Kyberturvallisuus voidaan määritellä monilla tavalla. Yleisesti sillä viitataan digitaalisessa muodossa olevan informaation turvallisuuteen. Kyberturvallisuuden sijasta Venäjä puhuu informaatioturvallisuudesta, joka liittyy informaatioalueen turvallisuuteen. Venäjän vuoden 2016 informaatioturvallisuuden doktriini kuvaa informaatioalueen yhdistelmäksi informaatiota, informaatio-objekteja, informaatiosysteemejä ja verkkosivuja internetin informaatio- ja telekommunikaatioverkossa, kommunikaatioverkkoja, informaatioteknologioita, entiteettejä, joita käytetään informaation tuottamiseen ja prosessointiin, yllä esitettyjen teknologioiden käyttöä, informaatioturvallisuuden takaamista ja julkisten yhteyksien rajoittamismekanismeja. (Ministry of Foreign Affairs of the Russian Federation, 2016) Informaatioturvallisuutta käsitellään luvussa 4.

Tutkimuksen muita keskeisiä termejä ovat fragmentoituminen, avoin talous ja rahoitusjärjestelmä. Internetin fragmentoituminen eli jakautumista erillisiin verkostoihin on kuvailtu luvussa 4. Valtiollisella fragmentoitumisella tarkoitetaan kehitystä, jossa valtiot alkavat kontrolloida omien maantieteellisten alueidensa Internetiä täten heikentäen kansainvälisen internetin yhtenäisyyttä.

Avoin talous on kansainvälistä kauppaa käyvä talous. (Suomen Pankki, 2021a) Avoimia talouksia on tarkemmin kuvattu luvussa 5.

Rahoitusjärjestelmä kuvaa muun muassa keskuspankeista, muita pankeista, luottolaitoksista, pörsseistä ja maksujärjestelmistä koostuvaa kansainvälistä rahaliikennettä hallinnoivaa verkostoa. Rahoitusjärjestelmää kuvataan tarkemmin luvussa 5.

2.2 Aiempi tutkimus ja uusi näkökulma

Tämä tutkimus sijoittuu Venäjän suvereenia Internetiä käsittelevään tutkimusalaan. Soldatovin ja Boroganin (2015) teos The Red Web on yksi alan keskeisimmistä teoksista. Siinä kuvataan kokonaisvaltaisesti ja kattavasti Venäjän Internetin segmentin kehitystä, liberaalia alkua, valvonnan lisääntymistä sekä valvontakoneiston rakentumista ja rakennetta. Teoksessa on hyvin paljon primääriä, muun muassa haastatteluihin perustuvaa tietoa.

Pääteoksensa lisäksi Soldatov ja Borogan ovat julkaisseet myös kohdistetumpia tutkimuksia. Vuoden 2013 artikkelissa he käsittelevät Venäjän valvontajärjestelmää ja varoittavat Internetin kansallisesta fragmentoitumisesta, vuoden 2015 artikkelissa he puolestaan keskittyvät konkreettisemmin ja yksityiskohtaisemmin valvontajärjestelmän vahvistumiseen. (Soldatov & Borogan, 2013; 2015b)

Nocetti (2011) kuvailee, miten Venäjän nousussa digitaaliseksi maailmanvallaksi on kaksi puolta. Yhtäältä Venäjä pitää Internetiä hyvänä poliittisen vaikuttamisen ja kontrollin välineenä, toisaalta valtio tahtoo kansainvälisesti käyttää Internetiä pehmeän vallan välineenä maabrändinsä luomisessa. Nocetti varoittaa Venäjän kontrollin voimistumisesta Internetin segmentissään. Nocetti (2015) keskittyy lähinnä Venäjän pyrkimyksiin politisoida Internetin rakenteeseen ja sisältöön liittyvää ympäristöä sekä muovata kansainvälistä Internetiä tarpeidensa mukaan.

Ristolainen (2017) kiinnittää huomiota siihen, että länsimainen käsitys kyberturvallisuudesta avoimessa jaetussa Internetissä eroaa Venäjän laajasta informaatioturvallisuuden käsitteestä. Jos tahdotaan ymmärtää Venäjän suvereenin Internetin projekti, tulisi myös tämä informaatioturvallisuuden käsite ymmärtää.

Kari ja Kuusisto (2017) analysoivat, millä tavoin kyberuhka ja sen kohteet esitetään Venäjällä julkisessa keskustelussa. Kari (2018a) esittää kriittisen informaation infrastruktuurin yhdeksi Venäjän tärkeimmistä kyberturvallisuuden suojelukohteista, Kari (2018b) tutkii Venäjän valtion viranomaisten keskinäistä vastuunjakoa kyberuhkiin puolustautumisessa, ja Kari (2019a) arvioi kyberuhkia Venäjän strategisen kulttuurin näkökulmasta.

Kari (2019b; 2019c) esittää Venäjän strategisen kulttuurin pohjalta ajatuksen, että suvereenin Internetin taustalla on Venäjän ajatus piiritetystä kyberlinnakkeesta, jota sen tulee suojella. Ajatus juontaa niin historiasta, maantieteellisestä sijainnista kuin teknologisesta kilpailukyvyn puutteestakin. Kari ja Pynnöniemi (2019) syventävät piiritetyn linnakkeen ajatusta esittäen analyyttisen viitekehyksen, jolla voidaan tutkia Venäjän kokeman kyberuhan kehitystä osana strategista kulttuuria.

Kukkola (2018) tuo esille periaatteita ja tapoja, joilla Venäjä pyrkii suojaamaan ja kontrolloimaan Internetin segmenttiään. Kukkola (2019) esittää, että Venäjä pyrkii digitaalisella suvereenisuudella saavuttamaan epäsymmetrisen aseman kybermaailmassa. Kukkola ja Ristolainen (2019) kuvaavat Venäjän digitaalisten rajojen infrastruktuuria.

Nikkarila ym. (2019) esittää matemaattisen mallin suljetun kansallisen verkon ja sen vaikutuksien kuvaamiseksi. Siukonen ym. (2019) puolestaan esittää tavan kuvata valtion Internetin segmentin teknistä riippumattomuutta ja esittelee saavutettavuusmatriisin, jonka avulla tutkittavan valtion Internetin segmentin avoimuus-sulkeutuneisuuskehityksen astetta voidaan arvioida.

Kukkola (2020) käsittelee Venäjän suvereenin Internetin projektia hyvin kattavasti. Hän esittää projektin luonnolliseksi vastaukseksi maailmassa tapahtuneille geopoliittisille ja teknologisille muutoksille.

Domańska (2019) esittää, että Internet tarjoaa taistelualustan, jolla Venäjän valtio voi käydä informaatiosotaa vaihtoehtona perinteiselle sodalle länttä vastaan. Koska venäläisten suosimat sosiaalisen median alustat ovat pitkälti länsimaisia ja valtio käy maan sisäistä informaatiosotaa lähinnä perinteisten joukkotiedotusvälineiden kautta, muodostaa Internet hänen mukaansa Venäjälle riskin.

Venäjän ja Kiinan välisestä Internetiin liittyvästä yhteistyöstä ei erikseen ole kovin paljon tieteellistä tutkimusta. Kattavin kokonaisuus lienee Lukinin (2020) tutkimus maiden yhteistyön kehittymisestä tulevaisuudessa.

Tässä tutkimuksessa Venäjän suvereenin Internetin projektia tutkitaan uudesta näkökulmasta, jossa Internetin lisäksi huomioidaan Venäjän talous- ja rahoitusjärjestelmät osana kansainvälisiä vastaavia järjestelmiä. Tavoitteena on näiden järjestelmien kautta selvittää, millaisia vaikutuksia Internetin segmentin pitkäaikaisella sulkemisella olisi venäläiseen yhteiskuntaan ja miten realistinen suvereenin Internetin projekti on.

3 AINEISTO JA MENETELMÄ

Luvussa selitetään tutkimusaineisto ja tutkimusnäkökulma sekä kuvataan tutkimusote ja tutkimusmenetelmä. Lopuksi esitellään tutkimusmenetelmänä käytettävä verkkotoria.

3.1 Aineisto

Tutkimusaineisto koostuu ensi sijassa Venäjän Internetin segmenttiä sekä talous- ja rahoitusjärjestelmiä käsittelevästä dokumentaarisesta materiaalista. Toissijaisesti käytetään kansainväliseen Internetiin ja Kiinan suvereeniin Internetiin liittyvää dokumentaarista materiaalia. Materiaalina käytetään tieteellisiä julkaisuja, tunnustettujen tutkimuslaitosten julkaisuja, kansainvälisten organisaatioiden omilla verkkosivuilla olevaa tietoa, virallisia tiedonantoja, tunnustettujen uutistoimistojen välittämiä uutisia sekä tilastollista tietoa. Tutkimusmateriaalia valittaessa kiinnitetään huomiota tiedon luotettavuuteen sekä erilaisten näkökulmien mahdolliseen subjektiivisuuteen. Lähteet ovat ensisijaisia lähteitä aina silloin, kun se on mahdollista.

Tutkimusaineisto kerätään iteratiivisesti tutkimusprosessin edetessä tietokantoja ja avainsanoja hyväksi käyttäen. Tämän lisäksi etsitään kohdennetusti tietoa suoraan Internetistä. Ensimmäisessä vaiheessa, pyrittäessä tunnistamaan tutkittavien järjestelmien kriittisiä tekijöitä, käydään läpi sekä Internetin rakennetta että talous- ja rahajärjestelmiä käsitteleviä tieteellisiä julkaisuja sekä etsitään tietoa tunnustettujen tutkimuslaitosten ja julkishallinnon laitosten verkkosivuilta. Venäjän suvereenin Internetin vaiheita ja toteutumista selvitetään tieteellisten julkaisujen lisäksi virallisista tiedonannoista ja uutisista. Venäjän rahoitusjärjestelmä puolestaan on esitetty varsin kattavasti Venäjän keskuspankin sivuilla.

Tutkimuksen toisessa vaiheessa, jossa arvioidaan kriittisten tekijöiden merkitystä, käytetään ensi sijassa tilastollista dataa. Data etsitään pääasiallisesti Statista-tietokannasta. Statista-tietokantaan on kerätty dataa suurilta tunnustetuilta organisaatioilta ja tutkimuslaitoksilta. Ellei etsittyä tietoa löydy tästä tietokannasta, sitä etsitään suoraan kansainvälisten talouden alan tunnustettujen organisaatioiden sivuilta ja julkaisuista. Tilastollisen datan lisäksi tietoa etsitään tieteellisistä julkaisuista ja tunnustettujen tutkimuslaitosten julkaisuista.

Tilastollinen data valitaan siten, että se liittyy verkkoteorian avulla tunnistettuihin kriittisiin solmuihin. Lisäksi datana käytetään kansainväliseen kauppaan ja rahoitukseen liittyviä makroekonomisia indikaattoreita, kuten bruttokansantuotetta, öljyn hinnan kehitystä ja viennin ja tuonnin suhdetta, sekä sosiaalisen median käyttöä kuvaavia mittareita.

Tutkimuksen aluksi analysoidaan sekä Internetiä että talouden verkostoja verkkoteorian kautta. Hahmottamalla kummankin järjestelmän solmut ja kaaret luodaan kuva järjestelmän välttämättömistä toimijoista, niiden keskinäisistä suhteista, painoarvoista sekä kriittisistä kohdista. Pääpaino on järjestelmien kannalta

kriittisissä solmuissa, jotka yhtäältä tuovat valtaa haltijalleen, mutta toisaalta ovat systeemin vakauden kannalta kriittisiä ja haavoittuvia.

Venäjän suvereenin Internetin projektia tarkastellaan kolmella eri tasolla: teknisellä, loogisella ja sosiaalisella tasolla. (JP 3-12, 2018) Näiden tasojen välisiä suhteita pyritään kuvailemaan siinä määrin, kuin se tuntuu luontevalta. Venäjää kansainvälisenä taloutena tarkastellaan kolmesta näkökulmasta: rahoitusjärjestelmän, kansainvälisen kaupan ja kansainvälisten sijoitusten näkökulmista.

3.2 Tutkimusote ja tutkimusstrategia

Tutkimus sijoittuu kyberturvallisuuden ja taloustieteen rajapinnalle. Tutkimusote on konstruktivistinen ja tutkimusstrategiana on tapaustutkimus. Tutkimusmenetelmänä käytetään verkkoteoriaa ja vertailevaa analyysiä. Tutkimus on kvalitatiivinen, mutta tutkimusaineistona käytetään sekä kvalitatiivista että kvantitatiivista dokumentaarista aineistoa.

Konstruktiivisessa tutkimusotteessa ymmärrystä todellisuudesta pyritään mallintamaan tutkijoiden subjektiivisten tulkintojen ja niiden välisen dialogin avulla. Riege (2003) Tietoa pidetään teoriasidonnaisena, tutkija ja tutkimuskohde ovat toisistaan riippuvaisia, samoin teoria ja käytäntö. (Mir & Watson, 2000) Konstruktivisimin metodologia on dialektinen painon ollessa ymmärtämisessä ja konsensuksen löytämisessä. (Guba & Lincoln, 1994)

Tapaustutkimus on iteratiivinen tutkimusote, joka sopii silloin, kun esitetään miten- ja miksi-kysymyksiä eikä tutkijalla ei ole kontrollia tutkimustapahtuman kohteeseen. (Yin, 1994) Tavoitteena on ymmärtää ja selittää todellisen elämän tapahtumaa sekä saada siitä kokonaisvaltainen tai yksityiskohtainen käsitys mahdollisen teorian rakentamiseksi. (Riege, 2003) Tapaustutkimuksessa teoriaa kehitetään vaiheittain kiinteässä yhteydessä aineistoon. (Eisenhardt, 1989)

Tapaustutkimuksen kohde on tyypillisesti monitahoinen, minkä seurauksena rajallisen tutkimusaineiston ja datapisteiden valinta voi olla haasteellista. Yksi mahdollisuus on lähestyä tutkimusta useammasta toisiaan täydentävästä näkökulmasta. (Yin, 1994)

Tapaustutkimukseen perustuvien teoreettisten tulosten arvioiminen ei aina ole suoraviivaista, eikä yleisesti hyväksyttyjä suuntaviivoja ole. (Eisenhardt, 1989) Validiteetin eli pätevyyden ja reliabiliteetin eli luotettavuuden varmistaminen saattaa olla haastavaa. Validiteetti kuvaa tutkimusmenetelmän kykyä mitata sitä, mitä on tarkoitus mitata. Oleellista on, että tutkimusmenetelmät ja niissä käytetyt mittarit on valittu oikein. (Britannica, 2021a) Reliabiliteetti kuvaa tutkimusmenetelmän kykyä antaa ei-sattumanvaraisia tuloksia. Reliabiliteetti voidaan varmistaa toistamalla koejärjestely ja mittaukset. (Britannica, 2021b)

Riege (2003) esittää, että tapaustutkimuksissa voidaan käyttää positivistissa tieteissä käytettyjen validiteetin ja reliabiliteetin testejä sekä neljää muuta testiä. Konstruktiovaliditeetin (construction validity) haaste on se, että tutkija tahtomattaan tuo omia ennakkokäsityksiään ja arvojaan valitessaan mitattavia kohteita. Sisältövaliditeetin (internal validity) testissä on tärkeää pystyä osoittamaan, että

lukuisista tekijöistä juuri valitut ovat merkityksellisiä tutkimustuloksen kannalta. Ulkoisen validiteetin (external validity) testissä tärkeää on, että analyyttisesti tehdyt yleistykset ja tutkimuksen aluksi tehdyt teoreettiset rakennelmat sopivat toisiinsa. Luotettavuustestin (reliability) haasteena on, ettei tapaustutkimus aina ole täysin toistettavissa eikä eri tutkijoiden keräämä aineisto välttämättä lähesty objektiivista tutkimusaineistoa. (Riege, 2003)

Edellä esitettyjen testien lisäksi Riege (2003) ehdottaa neljää muuta testiä. Vahvistettavuustestissä (confirmability test) arvioidaan, ovatko aineistosta tehdyt päätelmät loogisia ja objektiivisia. Uskottavuustesti (credibility test) muistuttaa pätevyystestiä. Siinä tarkistetaan, ovatko aineiston kuvaukset merkityksellisiä, ovatko löydökset sisäisesti koherentteja ja liittyvätkö käytetyt konseptit systemaattisesti toisiinsa. Siirrettävyystesti (transferability) liittyy ulkoiseen validiteettiin ja tulosten yleistettävyyteen vastaaviin tutkimuskohteisiin. Riippuvuustesti (dependability) on analoginen reliabiliteetin kanssa. Sen tavoitteena on varmistaa tutkimuksen aikaisten toimintatapojen ja tekniikoiden yhtenevä soveltaminen ja vakaus. (Riege, 2003)

Konstruktiivinen tutkimusote ja tapaustutkimus ovat luontevia valintoja käytännönläheiseen Venäjän suvereeniin Internetiin liittyvään tutkimusongelmaan. Tutkimuksessa ei pyritä löytämään lopullista totuutta vaan esittämään yksi näkökulma laajempaan Venäjän suvereenin Internetin projektiin liittyvään tutkimusalueeseen. Tutkimusongelmaan liittyy paljon sidosryhmiä ja tekijöitä, joista tutkimuksen valitaan sopiva määrä. Valinta voidaan tehdä monella tavalla, ja se riippuu tutkimuksen tekijästä. Tutkimustulokset liittyvät lähinnä Venäjään, mutta saattavat osin olla yleistettävissä laajemmin. Tutkimuksen validiteettia ja reliabiliteettia vahvistetaan käyttämällä kahta toisiaan täydentävää tutkimusmenetelmää sekä yleisesti tunnustettuja makroekonomisia indikaattoreita. Lisäksi huomioidaan Riegen (2003) esittämät muut tavat validiteetin ja reliabiliteetin vahvistamiseksi.

3.3 Tutkimusmenetelmä

Tutkimuksessa käytetään kahta tutkimusmenetelmää, verkkoteoriaa ja vertailevaa tutkimusta. Tutkimusongelmaan liittyvät kriittiset tekijät pyritään tunnistamaan verkkoteorian avulla. Kriittisten tekijöiden merkitystä tutkitaan tilastollisen ja dokumentaarisen aineiston avulla. Lisäksi niitä käytetään vertailevan tutkimuksen pohjana.

Verkkoteoria on teoreettinen ja metodologinen näkökulma, jolla mallinnetaan tutkittavan järjestelmän elementtien välisiä suhteita. Oh & Monge (2016) arvioi verkkoteorian tehokkaaksi työvälineeksi rakenteeltaan monimutkaisen ja dynaamisen kommunikaation tutkimiseen.

Verkkoteoriassa verkot muodostuvat solmuista ja kaarista. (Newman, 2010) Kommunikaatioverkoissa kaaret välittävät dataa, informaatiota tai tietoa. (Monge ym., 2003). Kun solmut ovat yksittäisiä ihmisiä, ryhmiä tai organisaatioita, on kyse sosiaalisesta verkosta. (Wasserman & Faust, 1994) Verbovszky (2018) tunnistaa geopoliittisiin verkostoihin kuuluvaksi kansainvälisen kaupan

virrat, rahavirrat, muuttoliikevirrat, energiavirrat, väkivallan virrat ja informaatiovirrat.

Tutkimukseen Venäjän suvereenista Internetistä liittyy monenlaisia yhteyksiä ja verkkoja: fyysisiä, loogisia ja sosiaalisia yhteyksiä ja verkkoja sekä talouden järjestelmän ja rahoitusjärjestelmän yhteyksiä ja verkkoja. Verkkoteoriaa voidaan soveltaa näihin kaikkiin.

Internetiä on verkkoteorian avulla tutkittu paljon erityisesti teknisestä näkökulmasta tai toimijaverkkoteoriaa (Actor Network Theory ANT) soveltaen. Verkkoteoriaa on luontevasti sovellettu myös talouden tutkimuksessa. Kirman (1997) kuvaa taloutta kehittyvänä järjestelmänä, Dicken ym. (2001) puolestaan systeeminä. Journal of Network Theory in Finance -aikakauskirja (Journal of Network Theory in Finance, 2021) on erikoistunut rahoitusjärjestelmän verkkoteorian tutkimuksiin. Tyypillisesti tutkimukset liittyvät rahoitusjärjestelmän kriiseihin ja niiden leviämiseen, eivät niinkään nyt tutkittavaan näkökulmaan.

Verkkoteorian käytön tavoitteena ei tässä tutkimuksessa ole yksityiskohtaisesti mallintaa erilaisia informaatio- ja materiaalivirtoja vaan tunnistaa Venäjän suvereenin Internetin kannalta kriittisiä tekijöitä, solmuja. Kriittisten solmujen merkitystä arvioidaan tilastollisen ja dokumentaarisen aineiston avulla.

Kriittisiä solmuja käytetään myös Venäjän ja Kiinan vertailevan tutkimuksen pohjana. Vertailevassa tutkimuksessa ei yleensä voida tarkastella samanaikaisesti kovin monia piirteitä, joten tarkasteltavien piirteiden esivalinta on suotavaa.

Ragin (1987) tunnistaa monia vertailevaan tutkimukseen liittyviä piirteitä, jotka sopivat tutkimukseen Venäjän suvereenista Internetistä. Vertaileva tutkimus kannustaa yhteisten piirteiden syvälliseen perehtymiseen, auttaa identifioimaan syy-seuraussuhteiden variaatioita sekä pakottaa tutkijan tarkastelemaan tapausta kokonaisvaltaisesti. Toisaalta vertaileva tutkimus voi jäädä kapeaksi vertailtavien piirteiden rajoitetun määrän takia.

Venäjän ja Kiinan vertailevassa tutkimuksessa tarkastellaan yhtenevyyksiä ja eroja valtioiden Internetin segmenttien sekä talous- ja rahoitusjärjestelmien välillä. Vertailevan tutkimuksen lopullisina tavoitteina on ymmärtää, miten valtioiden valitsemat strategiat eroavat toisistaan ja missä määrin suvereeni Internet olisi mahdollinen ratkaisu Venäjälle, kun se Kiinalle sitä on ollut.

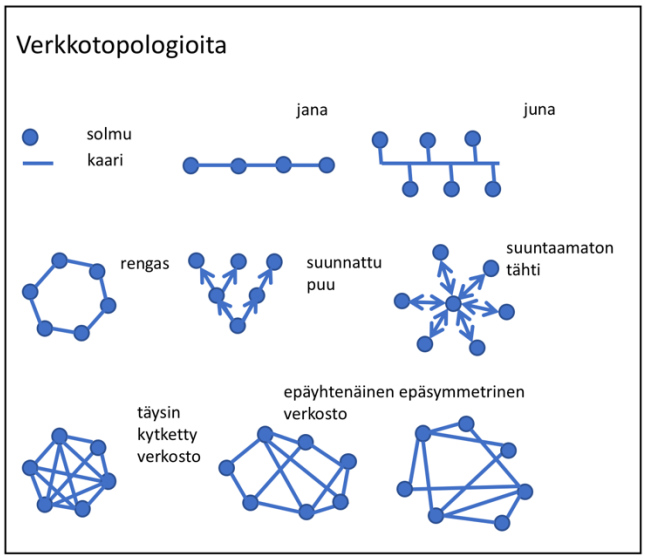
3.4 Verkkoteoria

Verkot matemaattisina objekteina tarjoavat abstraktin viitekehyksen monen tyyppisten systeemien tutkimiseen. Erityisesti ne soveltuvat systeemeihin, joiden tilastollinen kuvaaminen olisi liian monimutkaista. Viime aikoina verkkoteoriaa on käytetty myös talouden ja sen rakenteen, topologian, tutkimiseen. (Allen & Babus, 2009)

Verkkon peruselementit ovat solmut ja kaaret. Verkko voi olla suuntaamaton, jolloin informaatio tai materia voi liikkua kahden solmun välillä kumpaankin suuntaan, tai se voi olla suunnattu, jolloin liikenne kahden solmun välillä on

yksisuuntaista. Painotetussa verkossa solmuilla tai kaarilla on painot. Verkko voidaan esittää luettelona, joka sisältää kaikki yhteydet, tai yhteysmatriisina, jossa 1 kuvaa yhteyttä ja 0 ei-yhteyttä. Suuntaamaton matriisi on symmetrinen. (Brandes, 2005)

Verkko voi olla yhtenäinen tai epäyhtenäinen, ja se voi olla avoin tai suljettu ketju. Suuntaamatonta verkkoa kutsutaan metsäksi, jos siinä ei ole suljettuja ketjuja. Yhtenäistä verkkoa, jossa ei ole suljettuja ketjuja, kutsutaan puuksi. Puu on optimaalinen verkko. Kaaren poistaminen johtaa epäyhtenäiseen verkkoon, sen lisääminen puolestaan suljettuun ketjuun. (Brandes, 2005) (kuvio 1)



KUVIO 1. Verkkotopologioita (Brandes, 2005)

Internetiä voidaan kuvata suuntaamattomana verkkona. (Maslov ym., 2004) Suvereeni Internet on suljettu verkko. Sosiaalisen median verkosto on hierarkkisesti järjestäytymätön ja klusteroinut. (Hansen, 2010; Ugander ym., 2011) Vaikka sen solmuilla, ihmisillä, saattaa olla erilaisia painoarvoja, yksittäinen solmu ei ole edellytys verkoston toiminnalle.

Internetin tavoin rahoitusjärjestelmää voidaan kuvata suuntaamattomana verkkona. Rahoituslaitokset ovat rahoitusjärjestelmän painotettuja solmuja ja rahavirrat tai informaatiovirrat ovat painotettuja kaaria.

Verkoston solmun tai linkin tärkeyttä verkossa voidaan mitata monin tavoin. Yleisesti käytettyjä mittareita ovat:

1. välittäjyys (betweenness centrality), joka mittaa solmun tärkeyttä verkostossa ja joka lasketaan lyhimpien kaarien avulla lähtösolmusta kohdesolmuun;
2. keskeisyys (closeness centrality), joka mittaa solmun mahdollisimman nopeaa yhteyttä muihin solmuihin;
3. solmujen yhteysaste (node degree), joka kuvaa solmun yhteyksien lukumäärää muihin solmuihin. (Brandes, 2005)

Tärkeimpien solmujen ja linkkien avulla voidaan arvioida tietoverkkojen tai rahoitusjärjestelmän riskejä. Esimerkiksi vuoden 2008 finanssikriisin jälkeen havahduttiin siihen, miten suuret, hyvin monipuolisesti muihin rahoituslaitoksiin kytkeytyneet pankit aiheuttavat koko rahoitusjärjestelmän systeemisen riskin.

Verkostoja voidaan analysoida ylhäältä alas tai alhaalta ylös. (Brandes, 2005) Rahoitussektorilla ensin ylhäältä alas -analyysi soveltuu ryhmittelyyn eli klusterointiin, luokitteluun, systeemisuunnitteluun tai systeeminhallintaan. Alhaalta ylös -analyysi puolestaan soveltuu muun muassa analysoitaessa toimitusketjuja ja rahanpesuketjuja.

Verkostoanalyysissä voidaan myös lähteä datan ominaisuuksista tai agenttipohjaisista malleista. Agenttipohjainen mallinnus sopii rahoitusjärjestelmän tutkimiseen. (Chakrabarti ym., 2019) Pystyäkseen tehokkaasti toimimaan on valtion rahoitusjärjestelmässä oltava tietyt toimijat: keskuspankki, pankkeja ja luottolaitoksia, selvittelytalo, pörssi tai muu kauppapaikka sekä maksujärjestelmä kansainvälisine taseensiirtojärjestelmineen. Luottolaitokset ja pankit tyypillisesti klusteroidaan koon ja toimialan laajuuden perusteella.

Monitasoista Multiplex-verkkoteoriaa voidaan käyttää, kun tutkittavat eri dimensioiset systeemit ja verkot ovat keskenään vuorovaikutuksessa. (Kivelä ym., 2014) Keskinäisriippuvassa digitalisoituneessa maailmassa rahoitussektorin verkosto liittyy sekä Internetin tietoverkkoihin että ihmisten muodostamaan käyttäjäverkkoon. (EU, 2020) Rahoituksen verkkoteoria, Network Theory in Finance, pyrkii ymmärtämään rahavirtoja, kaupankäynnin virtoja, taloudellisia altistumisia riskille ja markkinoiden dynamiikkaa. (Allen & Babus, 2009)

4 INTERNETIN AVOIMIA JA SULJETTUJA VERKOSTOJA

Luvun tavoitteena on hahmottaa lähtökohdat Venäjän suvereenille Internetille. Aihetta taustoitetaan kuvailemalla Internetin rakennetta ja tunnistamalla sen kriittisiä solmuja sekä niihin liittyviä valtarakenteita. Lisäksi kuvaillaan avoimen ja suljetun Internetin kahta narratiivia sekä Internetin fragmentoitumiskehitystä. Lopuksi arvioidaan Venäjän suvereenin Internetin projektia teknisestä, loogisesta ja sosiaalisesta näkökulmasta, huomioiden tunnistetut kriittiset solmut.

4.1 Internetin rakenne

Internet on kansainvälinen tietokoneista ja tietoverkoista koostuva verkosto. Osa tietokoneista toimii palvelimina. Internet on luotu järjestäytymättömäksi verkoksi, jolla ei ole varsinaista ydinrakennetta tai keskeistä ydintä. Se onkin yksittäisen yhteydenoton kannalta vakaa. Jos jokin yhteys katkeaa, lähetetty tieto saadaan todennäköisesti perille toista kautta. Järjestelmänä Internet on kuitenkin monin tavoin haavoittuvainen. Sitä ei ole suunniteltu nykyiseen kriittiseen rooliinsa, jossa yhteiskunta on sen palveluista hyvin riippuvainen. (Pastor-Satorras & Vespignani, 2007)

Internet kommunikoi TTP/IP-kielellä. (Clark, 2003) Tietokoneiden ja niitä vastaavien IP-osoitteiden säilyttämisestä sekä verkkotunnusten kääntämisestä IP-osoitteiksi vastaava nimipalvelu DNS (Domain Name Service) on Internetin toiminnan kannalta kriittinen. (Pastor-Satorras & Vespignani, 2007) Tämä rakenteeltaan puumainen verkosto on hajautettu tietokanta, joka koostuu 13 ylimmän luokan juurinimipalvelimesta sekä noin 1400 nimipalvelimesta. (Enisa, 2016) Keskenään samanlaiset juurinimipalvelimet sisältävät tiedon seuraavan tason nimipalvelinten osoitteista. Nämä nimipalvelimet vastaavat tietyn alueen, esim .ru IP-osoitteista. Ellei palvelimelle ole tietoa kysytystä domain-nimestä, ohjaa se kyselyn toiselle DNS-palvelimelle. (Pastor-Satorras & Vespignani, 2007)

Verkkoteorian näkökulmasta Internetin tietokoneet ovat kaarin toisiinsa yhdistettyjä solmuja. Verkon toiminnan kannalta kriittiset juurinimipalvelimet saavat solmuina erittäin suuren painoarvon. Ilman nimipalvelujärjestelmää Internetistä ei pystyisi etsimään mitään verkkosisältöä tai lähettämään sähköposteja. Tässä tutkimuksessa juurinimipalvelimia tarkastellaan suvereenin Internetin kriittisinä solmuina.

Vaikka Internet luotiin hajautetuksi järjestelmäksi, jonka välityksellä kaikki tietokoneet, solmut, voisivat vapaasti ja tasa-arvoisesti kommunikoida keskenään, on se nykyään hyvin keskittynyt muutaman suuren palveluntarjoajan ympärille. Jos painoarvoja annetaan lähtevien ja tulevien kaarien perusteella, saavat muutamat suuret teknologiayritykset erittäin suuren painoarvon. Tässä tutkimuksessa suuria kansainvälisiä teknologiayrityksiä tarkastellaan suvereenin Internetin hyvin merkittävinä solmuina.

4.2 Avoin ja suljettu verkko - Internetin kaksi narratiivia

Internetin alkuperäiset arkkitehdit uskoivat avoimuuteen. Syyt olivat sekä käytännöllisiä että aatteellisia. (Drake ym., 2016) Ilman avoimuutta ja avoimia teknologioita Internet tuskin olisi pystynyt kehittymään ja skaalautumaan yhtä hyvin kuin nyt.

Vielä muutama vuosikymmen sitten keskustelu Internetin hallintaan liittyvistä teknisistä ja juridisista kysymyksistä käytiin lähinnä akateemisten ja geopoliittisten piirien marginaaleissa. (Mueller, 2017) Keskustelu on kuitenkin Internetin taloudellisen ja poliittisen merkityksen kasvun myötä siirtynyt keskiöön. (De Nardis, 2016; Powers & Jablonski, 2015) Valtiot ovat alkaneet ottaa kontrollia siitä, mitä niiden virtuaalisilla rajoilla tapahtuu. Kehitys näkyy sekä suurten teknologiajättien vallan rajoittamisena että keskusteluna laajemmasta Internetin valvomisesta. Erityisesti voidaan erottaa kaksi toisilleen täysin vastakkaista narratiivia: vapaan Internetin ja suvereenin Internetin narratiivit.

4.2.1 Vapaan Internetin narratiivi

Vapaan ei-kansallisen Internetin narratiivin mukaan informaation tulisi saada virrata vapaasti kansallisista rajoista riippumatta. Vapaan Internetin ajatellaan vahvistavan demokratiaa, vakautta ja tiedonvälitystä. (Budnitsky & Jia, 2018) Internetin vapautta perustellaan oikeusvaltioperiaatteella, ihmisoikeuksilla ja ilmaisuvapaudella. Vuonna 2016 Yhdistyneet kansakunnat (YK) määritti pääsyn Internetiin perusihmisoikeudeksi. (YK, 2016) YK:n ihmisoikeusneuvosto vahvisti vuonna 2018, että jokaisen ihmisen oikeus etsiä, vastaanottaa ja olla osana kaikkien medioiden tarjoamasta informaatiota rajoista riippumatta koskee myös verkossa olevaa informaatiota. (YK, 2018)

Vapaata ei-kansallista Internetiä ajavat perinteisesti ohjelmistoja, standardeja ja sovelluksia kehittävät tekniset yhteisöt ja yksilöt. Sitä kannattavat aktiivisesti myös digitaalisia oikeuksia puolustavat ei-valtiolliset toimijat sekä Internetin palveluntarjoajat Facebookin ja Netflixin kaltaisista kansainvälisistä teknologiajäteistä pienempiin yrityksiin. (Mueller, 2017)

Länsimaiset valtiot kannattavat lähtökohtaisesti vapaata Internetiä. Keskusteluissa vähälle huomiolle jäävät Yhdysvaltojen ja muiden tärkeiden teknologiavaltioiden taloudelliset ja geopoliittiset tavoitteet, joita tämänhetkinen tilanne palvelee. (Budnitsky & Jia, 2018). Vapaa Internet johtaa myös siihen, että valtioiden itsensä lisäksi kansalaisjärjestöt, yritykset ja muut kiinnostuneet osapuolet voivat ottaa kantaa ja vaikuttaa valtion sisäisiin asioihin. (Mueller, 2017).

Vapaa Internet on tuonut mukanaan myös kiistattoman negatiivisia asioita. Tällaisia ovat muun muassa lapsiporno, tekijänoikeusrikkomukset ja demokratian massamanipulointi. (Drake ym., 2016; Mengü & Mengü, 2015)

4.2.2 Suvereenin Internetin narratiivi

Suvereenin Internetin narratiivi pyrkii tuomaan esiin valtioiden laillisen oikeuden suojella kansallista kulttuuria ja poliittisia eroja. Tässä keskustelussa valtiolliset rajat ja valtioiden autonomia ovat ensisijaisia säänneltäessä Internetiä niin kansainvälisesti kuin kansallisestikin. Lähtökohtana on, ettei Internet eroa muista kommunikaatioteknologioista, joten sen sääntely tapahtuu kansallisella tasolla radion ja television tavoin. Suvereeniin Internetiin liittyvät rajoittavat ja painostavat toimintamallit usein unohtuvat keskustelussa. (Budnitsky & Jia, 2018)

Kiinan ja Venäjän hallitukset pyrkivät edistämään ajatusta Internetin suvereenisuudesta vastapainona Yhdysvaltojen teknologiselle ja hallinnolliselle ylivoima-asemalle. (Budnitsky & Jia, 2018) Kiina ja Venäjä ovat niitä harvoja maita, joissa kansallinen hakupalvelu ja sosiaalinen media on suositumpi kuin yhdysvaltalaiset vastaavat teknologiajätit. (Statista, 2021k; 2021x) Muun muassa Kiinan Baidulla ja Venäjän Yandexilla on merkittävä rooli osana suvereenin Internetin projektia. (Budnitsky & Jia, 2018)

Budnitskyn ja Jian (2018) mukaan valtiot eivät käytännössä juuri toteuta puhtaasti kumpaakaan Internetin avoimesta tai suljetusta narratiivista, vaan avoimuuden ja protektionismin käytännönläheistä sekoitusta. Stadnik (2019) korostaa, että narratiivit Internetin vapaudesta ja suvereenisuudesta sisältävät kumpikin monia keskenään ristiriitaisia osia, ne ovat ideologisia näkemyksiä. Esimerkiksi suvereenia kansallista Internetiä sovellettaisiin mielellään kansainväliset taloudelliset ja infrastruktuuriin liittyvät edut säilyttäen.

Tyypillisesti Kiinaa arvostellaan digitaalisen kommunikaation rajoittamisesta. Se ei ole kuitenkaan yksin, sillä myös monet muut valtiot valvovat rutiininomaisesti Internet-liikennettä omilla rajoillaan. Zittrain ym. (2017) tunnistaa 26 tällaista valtiota tutkimiensa 45 valtion joukosta.

4.3 Internetin fragmentoituminen

Internetin fragmentoitumiskehitys on jo vuosia aiheuttanut kansainvälistä huolta. (Mueller, 2017) Sen takana on sekä teknisiä että poliittisia syitä.

Drake ym. (2016) jakaa fragmentoitumisen kolmeen kategoriaan:

1. tekninen fragmentoituminen esimerkiksi yhteen sopimattomien teknologioiden, protokollien ja standardien seurauksena;
2. valtiollinen fragmentoituminen, lähinnä globaalin Internetin jakautuminen digitaalisin rajoin kansallisiin verkkoihin; ja
3. kaupallinen fragmentoituminen esimerkiksi kaupallisten alustojen seurauksena.

Kategoriat heijastelevat tämän hetkisiä neljää näkemystä siitä, mitä Internetin tulisi olla. Internetin alkuperäiset arkkitehdit ja suunnittelijat ovat pyrkineet mahdollisimman suureen avoimuuteen sekä käytännöllisistä että aatteellisista syistä. Yhdysvalloissa puolestaan on kehittynyt kaupallinen Internet, joka alkuperäisen

Internetin idean mukaisesti ei painota ihmisten vaan yksityisten operaattoreiden vapautta. Eurooppalaista Internetiä tietosuojasääntelyineen voitaisiin kutsua porvarilliseksi Internetiksi. Kiinalle ja Venäjälle Internet on suljettu ja autoritäärinen, ja valtio kontrolloi sen sisältöä. (O'hara & Hall, 2018)

4.3.1 Internetin valtiollinen fragmentoituminen

Muellerin (2017) mukaan teknisen fragmentoitumisen uhkaa liioitellaan, mikä hämärryttää todellisen uhan, valtioiden suvereenin Internetin tavoitteet. Ennemminkin tulisi keskustella siitä, kuka tekee intentionaalisia rajoitteita ja kenelle. Tällaisia rajoitteita voisivat olla esimerkiksi se, että autoritatiivinen valtio rajoittaa opposition pääsyä kansainvälisille verkkosivuille. Internetin kansallinen sulkeminen voi yhtäältä olla todella houkuttelevaa, mutta toisaalta mahdotonta täydellisesti toteuttaa muun muassa taloudellisten seurausten takia. (Mueller, 2017)

Valtiollinen fragmentoituminen voi tapahtua monella dimensiolla ja merkitystasolla. Drake ym. (2016) mainitsee seuraavat fragmentoitumistyypit:

1. verkkosivujen suodattaminen ja estäminen, joka kohdistuu ainakin sosiaalisiin verkkoihin ja muiden resurssien epätoivottuun sisältöön;
2. hyökkääminen epätoivottuja sisältöjä tarjoaviin informaatioresursseihin;
3. digitaalinen protektionismi, jonka tavoitteena on estää käyttäjien pääsy avainalustaoille ja työkaluille e-kaupankäyntiä varten;
4. kansainvälisten kontaktien keskittäminen ja lopettaminen;
5. hyökkääminen kansallisiin verkkoihin ja avainresursseihin;
6. paikallisen datan prosessointivaatimukset ja säilytysvaatimukset;
7. arkkitehtuurin ja reitittämisen muutokset datan pitämiseksi territoriolla;
8. kiellot tietynlaisen datan siirtämisestä yli rajan;
9. strategiat kansallisten Internet-segmenttien tai kybersuvereniteetin rakentamiseksi;
10. kansainväliset viitekehykset rajoituskäytäntöjen legitimoimiseksi.

Monet näistä strategioista ovat käytössä Kiinassa ja vähintäänkin kuuluvat Venäjän suvereenin Internetin suunnitelmiin. Kumpikin maa ajaa aktiivisesti kansainvälisen viitekehyksen luomista rajoituskäytäntöjen legitimoimiseksi. (Budnitsky & Jia, 2018; Griffiths, 2019)

4.3.2 Internetin fragmentoitumisesta aiheutuvia kustannuksia

Internetin fragmentoitumisen ja pitkäaikaisen sulkemisen kustannuksia on vaikea arvioida. Plaksin ym. (2017) mukaan edes Internetin olemassa olevia taloudellisia vaikutuksia on vaikea mitata eikä standardoituja mittareita ole. Joitain viitteitä voidaan saada siitä, millaisia kustannuksia lyhytaikaiset sulut ovat aiheuttaneet. Global Network Initiativen (GNI) arvion mukaan hyvin verkostoitu-

neet maat menettävät noin 1.9 % päivittäisestä bruttokansantuotteesta (BKT) jokaisena päivänä, jolloin Internet on suljettu. (GNI, 2018) Deloitte (2016) puolestaan arvioi hetkellisen täydellisen katkon kustannuksiksi hyvin verkottuneelle maalle keskimäärin 23.6 miljoonaa dollaria 10 miljoonaa henkeä kohti.

Global Network Initiative tunnistaa Internetin sulkemiselle ja rajoittamiselle 14 vaikutusta. Ihmisoikeuksien loukkaamisen ja kansalaisten turvallisuuden vaarantamisen lisäksi GNI on tuonut esille talouteen liittyviä vaikutuksia. Katkot voivat vaikeuttaa rahoituspalvelujen toimintaa, eikä digitalisoitunut talous toimi ilman online tai mobiilimaksamista. Rahoitussektorin ongelmat heijastuvat eteenpäin muun muassa palkanmaksuun, terveydenhuoltoon ja koulutukseen. (GNI, 2018b)

Katkojen vaikutukset ovat sekä lyhytaikaisia että pitkäaikaisia. Paikallinen liiketoiminta ja turismi kärsivät, kun maksutoimeksiannot eivät liiku, verkkokaupat eivät toimi eikä sen enempää paikallisia kuin kansainvälisiäkään asiakastoimeksiantoja kaikilta osin pystytä hoitamaan. Kansainvälisten yrityskumppanien sanktiot ovat myös mahdollisia. (GNI, 2018b) Ulkomaiset suorat sijoitukset vähenevät epäluotettavan toimintaympäristön takia. Yksi ulkomaisten suorien sijoitusten allokointikriteeri on informaation saatavuutta kuvaava 'Access to Information' -indikaattori.

Katkot tekstiviestijärjestelmässä, sosiaalisessa mediassa, hakukoneissa ja uutissivuilla ovat lisääntyneet voimakkaasti viime vuosina. (GNI, 2018) Sulut ovat useimmiten olleet valtion vastatoimia protesteihin erityisesti vaalien ja kansallisten kriisien aikana. (Lamensch, 2021) Vuoden 2019 jälkeen merkittäviä katkoja tai sulkuja on Internetin toiminnassa ollut ainakin 223 kertaa 39 maassa. (Woodhams & Migliano, 2021) Vuonna 2020 suurempia katkoja tai sulkuja oli yhteensä 93 kertaa. Nämä häiriöt kestivät yhteensä yli 27 000 tuntia, mikä on 50 prosenttia edellisvuotta enemmän. (Lamensch, 2021) Vuoden 2019 jälkeisten katkojen tai sulkujen arvioidaan maksaneen noin 13.4 biljoonaa dollaria. Suurimmat kustannukset suluista aiheutuivat vuonna 2019 Irakille: 2.3 miljardia dollaria olivat noin prosentti maan bruttokansantuotteesta. (Woodhams & Migliano, 2021; Statista, 2021j)

Edes liberaalit demokratiat eivät ole immuuneja Internetin sulkemiselle. Vuonna 2020 Intia sulki Internetin osia 75 kertaa, mikä on enemmän kuin missään muussa maailman maassa. Pääasiallinen syy sulkemiseen ovat olleet Kashmirin alueen levottomuudet. (Lamensch, 2021) Sulkujen kustannuksiksi on arvioitu 2.8 miljardia dollaria, mikä on noin promille Intian bruttokansantuotteesta. (Woodhams & Migliano, 2021; Statista, 2021i)

4.4 Kuka hallitsee avointa Internetiä?

Internetin kriittisimpiin ydinsolmuihin kuuluu nimipalvelujärjestelmä nimipalvelujärjestelmä (Domain Name System DNS) 13 juurinimipalvelimineen. (Enisa, 2016) Järjestelmästä vastaa ICANN (Internet Corporation for Assigned Names and Numbers), Yhdysvalloissa sijaitseva voittoa tavoittelematon organisaatio.

(ICANN, 2021) Kolmetoista riippumatonta operaattoria, joista kymmenen sijaitsee Yhdysvalloista, muut Ruotsissa, Japanissa ja Alankomaissa, hallinnoi juurinimipalvelimia sekä 1400 hajautettua nimipalvelinta. (IANA, 2021b)

IANA (Internet Assigned Numbers Authority) on ICANN:in osasto, joka jakaa muun muassa IP-osoitteita ja koordinoi Internetissä käytettyjen protokollien parametrien arvoja. (IANA, 2021a) IANA toimi kiinteässä yhteydessä Yhdysvaltain kauppaosastoon lokakuuhun 2016 asti. (Snyder ym., 2017) Venäjä on usein esittänyt huolensa siitä, että Yhdysvallat sekaantuu ICANN/IANA:n toimintaan. (Becker, 2019)

Kiinalle ja Venäjälle kansalliset Internetin segmentit ovat osa valtioiden suvereenia tilaa, minkä takia niillä jaetulle sisällölle ja infrastruktuurille tahdotaan enemmän kontrollia. Kumpikin valtio vaatii enemmän sananvaltaa siihen, miten ICANN:ia johdetaan. Vuonna 2015 Kiina ja Venäjä esittivät toteutumatta jääneen ehdotuksen informaatioturvallisuudesta Yhdistyneiden kansakuntien (YK) yleiselle sihteerille. General Shanghai Cooperation Organization Joint Initiative -nimellä kulkenut ehdotus esitti, että kaikilla mailla tulisi olla yhtäläinen asema kansainvälisen Internetin hallinnoimiseen. Lisäksi osia ICANN:in tehtävistä tulisi siirtää YK:n alajärjestölle International Telecommunications Unionille (ITU). (Gabuev, 2015)

Vuonna 2020 ITU:n kokouksessa muun muassa Venäjä, Kiina, Yhdistyneet Arabiemiraatit ja Saudi-Arabia ehdottivat päätöslauselmaa kybersuvereenisuuden pääperiaatteista. Päätöslauselman mukaan YK olisi saanut aiempaa suuremman vallan Internetiin. Yhdysvallat ja enemmistö Euroopan maista esittivät hyvin voimakkaita vasta-argumentteja ja kieltäytyivät allekirjoittamasta päätöslauselmaa, jota ei voitu hyväksyä ilman heidän allekirjoituksiaan. (Chalk, 2019)

4.5 Venäjän suvereeni Internet

Venäjällä oli vuonna 2020 noin 110,7 miljoonaa Internetin käyttäjää. (Statista, 2021c) Tämä on noin 75 prosenttia kansasta (Statista, 2021o), mikä on selvästi Länsi-Euroopan 93 prosentin keskiarvoa alhaisempi. (Statista, 2021d) Internetin käyttäjien lukumäärä on Venäjällä kasvanut nopeasti: kun se vuonna 2000 oli vain 3 prosenttia, oli käyttäjiä vuonna 2010 noin 43 prosenttia. (Statista, 2021c)

Venäläiset käyttävät Internetiä päivittäin keskimäärin 4.5 tuntia, joista sosiaalisessa mediassa kuluu 2.5 tuntia. (Statista, 2021a) Selaimena yhdysvaltalaisen Googlen Chrome on ylivoimaisesti suosituin, ja suosituimmat verkkosivut ovat Yandex.ru, Google.com, VK.com, Mail.ru ja Youtube.com. Sosiaalisen median suosituin alusta on Googlen omistama Youtube (85,4%), VKontakte (78,0 %), Whatsapp (75,8 %), Instagram (61,2 %). Vastaavaa venäläistä Telegramia käyttää vain 27,4 %. (Statista, 2021x)

Venäjä on Kiinan ohella yksi niistä harvoista maista, joissa kotimainen hakupalvelualusta ja sosiaalisen median alustat ovat suositumpia tai yhtä suosittuja kuin vastaavat kansainväliset alustat. Kiinassa tämä selittyy sillä, että ulkomaiset alustat ovat kiellettyjä. Toisin kuin Kiinassa, monet Venäjän palveluista on alun

perin kehitetty yksityisesti. Verkon suosituimmista kotimaisista palveluista sähköpostipalvelu Mail.ru ja verkkolehtipalvelu Gazeta.ru perustettiin vuonna 1998, (Mail.ru, 2021; Gazeta.ru, 2021), hakupalvelu Yandex perustettiin vuonna 2000 (Yandex, 2021) ja sosiaalisen median alustat VKontakte (VK) ja Odnoklassniki vuonna 2006. (VK, 2021; Odnoklassniki, 2021)

Kotimaisten verkkopalvelujen lisäksi myös Google, Facebook ja Amazon ovat Venäjällä suosittuja. Googlen omistama Youtube on sosiaalisen median alustoista kaikkein suosituin, kilpaillen asemasta television kanssa. (Statista, 2021x) Venäjän hallinto saattaa kokea sen vaaralliseksi erityisesti vaikeasti kontrolloitavan sisällön takia. Tähän mennessä on kattavan valvonnan sijaan näytösomaisesti rangaistu ankarasti joitakin sisällöntuottajia.

4.5.1 Venäjän Internetin segmentin alkuvaiheita

Venäjän hallinto tiedosti tietoverkkojen potentiaalin kommunikaatiossa jo 1990-luvulla. 2000-luvun puoleen väliin asti Internet oli kuitenkin niin harvojen käytössä, että sen taloudellinen ja poliittinen valta oli rajallinen. (Tselikov, 2014; Budnitsky & Jia, 2018) Käyttäjiä oli vuonna 2000 vain 2 prosenttia, vuonna 2008 niitä oli 27 prosenttia. (World Bank, 2021b).

Internetiä kehitettiin aluksi yksityisin voimin varsin liberaalissa ilmapiirissä. Muun muassa ensimmäinen kansainvälinen Internet-viesti lähetettiin Neuvostoliiton vuoden 1991 vallankaappausyrityksen yhteydessä. (Press, 1991) Samassa yhteydessä Internetiä käytettiin Venäjällä ensimmäistä kertaa todellisessa reaaliaikaisessa tiedonvälityksessä. Valtio ei oleellisesti puuttunut Internet-yritysten ja digitaalisen median toimintaan ennen 2000-luvun loppua, jolloin muun muassa hakuyhtiö Yandex lähti globalisoitumaan. (Tselikov, 2014; Yandex, 2021)

Presidentti Medvedevin kaudella 2008-2012 Internet-yritysten ja valtion yhteistyö oli vielä rakentavaa vuorovaikutusta. Tavoitteena oli yhtäältä yhdessä viestiä maailmalle Venäjän teknologiajohtajuudesta, toisaalta monipuolistaa Venäjän raaka-aineriippuvaa taloutta. Viimeistään vuoden 2014 jälkeen teknologiayrityksistä tuli valtion intressien alaisia. (Budnitsky & Jia, 2018)

Internetin kontrollia lisättiin vastauksena vuoden 2011 presidentinvaalien suurin mielenosoituksiin. (Tselikov, 2014) Vuonna 2012 Putinin palattua valtaan nähtiin neuvostoajan jälkeiset suurimmat opposition mielenosoitukset. Kreml arvioi ne verkkoaktivismiksi, vastaten sekä sosiaalisella että poliittisella konservatiivisuudella. (Budnitsky & Jia, 2018) Valtio aloitti narratiivin Internetistä länsimaisena kumouksellisena teknologiana, sosiaalisten ja poliittisten paheiden lähteenä, ja uhkana Venäjälle. Kolme lakia Internetin mustista listoista ja blogien kirjoittamisesta julkaistiin, perustellen tavoitteeksi aiempaa turvallisemman verkkoympäristön. Samaan aikaan kuitenkin poliittisia vastustajia ja aktivisteja suljettiin ulos verkosta. (Tselikov, 2014)

Internetin liberaalista alusta huolimatta ei venäläinen media ole koskaan ollut vapaa länsimaisessa mielessä. 1990-luvulla se oli oligarkkien hallinnassa, kunkin välittäessä omaa viestiään. Putinin valtakaudella vuodesta 1999 se palasi

neuvostoaikojen valtiollisen median muotoon. (Budnitsky & Jia, 2018) Neuvostoaikainen System of Operative-Search Measures (SORM) -järjestelmä päivitettiin digitaaliseen aikaan jo vuonna 1998. (Polyakova & Meserole, 2019)

4.5.2 Venäjän informaatioturvallisuuden doktriini ja sulkeutuva Internetin segmentti

Venäjä ilmoitti onnistuneesta kokeilusta oman Internetin segmentin irrottamiseksi joulukuussa 2019. (BBC News, 2019) Vaikka irrottaminen teknisesti on ainakin hetkellisesti ollut mahdollista, on Venäjän kaltaisella kansainvälisellä taloudella paljon ratkaistavia asioita ennen täysin suvereenisti toimivaa Internetiä. Helmikuussa 2021 Medvedev esitti, että vaikka Venäjällä on jo lailliset ja teknologiset valmiudet suvereeniin Internetiin, ei merkkejä irtaantumisesta ole. (Interfax, 2021)

Mueller (2017) on esittänyt, että joillakin valtioilla on pyrkimys Internetin kansalliseen kontrolliin kansainväliset taloudelliset edut säilyttäen. Tavoitteeseen pyritään kolmessa vaiheessa: Internetin ja sen infrastruktuurin kansallisen turvallisuuden varmistaminen, Venäjän maantieteellisellä alueella olevien informaatiovirtojen rajoittaminen ja lopulta Internetin kriittisen infrastruktuurin kontrolloiminen omalla maantieteellisellä alueella. Stadnik (2019) on analysoinut Venäjän Internetin kehitystä näiden vaiheiden valossa.

4.5.2.1 Internetin ja sen infrastruktuurin kansallisen turvallisuuden varmistaminen

Muellerin (2017) mukaan suvereenin Internetin ensimmäinen kehitysaskel on Internetin ja sen infrastruktuurin kansallisen turvallisuuden varmistaminen. Venäjän informaatioturvallisuuden doktriini vuodelta 2016 määrittää informaatioalueen yhdistelmäksi informaatiota, informaatio-objekteja, informaatiosysteemejä ja verkkosivuja internetin informaatio- ja telekommunikaatioverkossa, kommunikaatioverkkoja, informaatioteknologioita, entiteettejä, joita käytetään informaation tuottamiseen ja prosessointiin, yllä esitettyjen teknologioiden käyttöä, informaatioturvallisuuden takaamista ja julkisten yhteyksien rajoittamismekanismeja. (Ministry of Foreign Affairs of the Russian Federation, 2016)

Venäjän informaatioturvallisuuden doktriinista käy hyvin ilmi Venäjän ja länsimaiden erilainen suhtautuminen kyberturvallisuuteen. Länsimaisen käsityksen mukaan verkon neutraliteetin perusteella informaatio on turvassa, jos sitä kuljettava teknologinen infrastruktuuri on turvallinen. Kunkin maan hallituksen tehtävänä on varmistaa, että sen kansalaiset voivat käyttää turvallista teknologiaa. Venäjä näkee uhkan tulevan ulkopuolelta. Teknologisen kehityksen sijaan paino on informaatiovirroilla, niiden sisällöllä ja arvolla sekä sosiaalisilla, psykologisilla ja kulttuurisilla seikoilla. Venäjä näkee tehtäväkseen yhtäältä turvata kansalaisen oikeuden informaatioon pääsyyn ja vapauteen informaatiokanavan

valinnassa, mutta toisaalta vastuuseen tarjota oikeaa paikkansapitävää informaatiota sekä rajoittaa valtiota mahdollisesti vahingoittavaa informaatiota. Venäjän tehtävänä ei ole turvata ainoastaan informaatiota, vaan koko venäläinen kulttuuri. (Pynnöniemi & Kari, 2016; Epifanova, 2020)

Yksi konkreettinen askel Internetin ja sen infrastruktuurin kansallisen turvallisuuden varmistamisessa on tietoverkkoihin kohdistuvien uhkien valvonnan ja tiedottamisen kansallistaminen. (Stadnik, 2019) Vuonna 2013 perustettiin kansallinen GOSSOPKA-järjestelmä, jonka tavoitteena on tietojärjestelmien hyökkäyksien jäljittäminen ja estäminen sekä niistä aiheutuvien seurausten minimoiminen muun muassa jakamalla tietoa kyberhyökkäyksistä suurimpien organisaatioiden kesken. Tähän Venäjän turvallisuuspalvelu FSB:n valvonnassa toimivaan järjestelmään kerääntyy tieto kaikista maan kyberhyökkäyksistä. (Pursiainen, 2020)

Venäjän suljetun kansallisen verkon suunnitelmiin kuuluu, että 99 prosenttia kriittisestä infrastruktuurista kaksinnetaan. Vuonna 2017 säädettiin FSB:n aloitteesta laki kriittisestä informaatioinfrastruktuurista, ja vuonna 2018 FSB:n perusti NCCCI:n (National Coordination Center for Computer Incidents). (Stadnik, 2019; NCCCI, 2021) Kaikki maan rajojen yli kulkeva informaatio kyberhyökkäyksistä kulkee NCCCI:n läpi. Lisäksi NCCCI on ottamassa kansallisen CERTin tehtäviä. Yksityisiä CERT-toimijoita on maassa monia. (Stadnik, 2019)

Venäjän informaatioturvallisuuden doktriinin mukaan ulkoa tulevaan uhkaan vastataan kehittämällä kokonaisvaltaisesti omaa kyberturvallisuusteknologiaa, kryptografiaa ja standardeja. Doktriini esittää velvoittavat tavoitteet venäläisvalmisteiseen teknologiaan siirtymiseen. Myös venäläisen kryptografian käyttöä on tarkoitus lisätä. (Ministry of Foreign Affairs of the Russian Federation, 2016) Vaikka Venäjä tahtoisi siirtyä laiteomavaraisuuteen, ei sillä kuitenkaan ole toimivia standardeja. Näitä tarvittaisiin turvallisten sovellusten ja kyberfyysisten systeemien luomiseen. (Stadnik, 2019)

Informaatioturvallisuuden doktriinin mukaan Venäjä pyritään kehittämään uuden kansainvälisen informaatioturvallisuuskehikon. Valtiolla olisi kehikossa oleellinen rooli. (Ministry of Foreign Affairs of the Russian Federation, 2016)

4.5.2.2 Territorion informaatiovirtojen rajoittaminen

Muellerin (2017) mukaan suvereenin Internetin toinen kehitysaskel on sen maantieteellisen alueen informaatiovirtojen rajoittaminen. Rajoittaminen käsittää niin maantieteellisen rajoittamisen kuin sisällön suodattamisenkin. Ensimmäiset suodattamiseen liittyvät toimet olivat vuoden 2012 mustien listojen määrittäminen niistä verkkotunnuksista ja -osoitteista, jotka sisältävät laitonta materiaalia. Venäjän tiedotusvälineitä valvova Roskomnadzor vastaa mustien listojen rekisteristä. (Tselikov, 2014)

Verkon suvereenisuuteen liittyvänä tavoitteena vuoden 2016 informaatioturvallisuuden doktriini esittää, että ulkomaiden kautta reititetyn datan määrä

tulisi tippuisi nopeasti 10 %. Venäläisen kulttuurin turvaamiseksi tuetaan perinteisten tiedonsiirtokanavien käyttöä lisääntyvän digitaalisen kommunikaation rinnalla. (Ministry of Foreign Affairs of the Russian Federation, 2016)

Doktriinin mukaan sosiaalisen median tulee säilyttää Venäjän kansalaisia koskeva data Venäjän territoriolla. Lisäksi operaattoreiden ja Internet-palveluntarjoajien tulee säilyttää data käyttäjistä, heidän aktiivisuudestaan ja kommunikaatiostaan Venäjän maantieteellisellä alueella vuoden ajan. Jo vuonna 2017 Venäjä oli ilmoittanut tavoitteekseen, että vuoteen 2020 mennessä 95 prosenttia Internet-liikenteestä voitaisiin reitittää sisäisesti.

4.5.2.3 Internetin kriittisen infrastruktuurin kontrolloiminen territorion alueella

Muellerin (2017) mukaan suvereenin Internetin kolmas kehitysaskel on Internetin kriittisen infrastruktuurin kontrolloiminen territorion alueella. Vuonna 2018 Venäjä esitteli ohjelman, the Digital Economy National Program, jonka mukaan Venäjän Internet-palveluntarjoajien tulee taata toiminnan jatkuvuus myös tilanteessa, jossa ulkomainen taho yrittää eristää Venäjän kansainvälisestä verkosta. Vastaava laki, jota epävirallisesti kutsutaan Suvereenin Runetin laiksi, vahvistettiin keväällä 2019. (Russian Federation, 2017; Epifanova, 2019)

Suvereenin Runetin lain mukaan Roskomnadzor vastaa kriisitilanteessa keskitetysti tietoverkoista ja Venäjän Internetin segmentin turvallisuudesta. Se voi myös säädellä sitä, miten verkkoliikennettä ohjataan. Internet-palveluntarjoajien tulee puolestaan asentaa järjestelmiin verkkoliikennettä suodattava niin kutsuttu musta laatikko. (Epifanova, 2019) Voidaan ajatella, että Roskomnadzor on Venäjän suvereenin Internetin kriittinen piste, jolla yhtäältä on erittäin suuri valta, mutta joka samalla on riski esimerkiksi kyberhyökkäyksissä. Sillä ei ole tarvittavaa kapasiteettia suodatettavan datan hallintaan. (Ramesh ym., 2020)

Vuonna 2018 Venäjän tiedonvälityksen valvoja Roskomnadzor ohjasi Internet-palveluntarjoajat estämään Telegramin viestipalvelusovelluksen toiminnan yrityksen kieltäydyttyä tarjoamasta Venäjän tiedustelupalvelulle takaovea. Yli 1.8 miljoonan IP-osoitteen estäminen aiheutti tahattomasti häiriöitä myös ulkopuoliselle palveluntarjoajalle, erityisesti Googlen ja Amazonin palvelinten asiakkaille. (Stadnik, 2019) Lisäksi sen lopputuloksena hakkereille avautui tietoturvaaukko Roskomnadzorin järjestelmiin.

5 TALOUDEN AVOIMIA JA SULJETTUJA VERKOSTOJA

Luvun tavoitteena on hahmottaa, miten valmis Venäjä kansainvälisenä avoimena taloutena olisi suvereenille Internetille. Kysymystä taustoitetaan kuvailemalla avoimia ja suljettuja talouksia sekä kansainvälistä rahoitusjärjestelmää verkostona. Tämän jälkeen Venäjää ja suvereenin Internetin projektia arvioidaan kolmen avoimelle taloudelle tärkeän verkoston näkökulmasta: rahoitusjärjestelmän, ulkomaankaupan ja kansainvälisten investointien näkökulmasta. Erityisesti kiinnitetään huomiota verkkoteorian avulla tunnistettuihin kriittisiin solmuihin.

Venäjä on erityisesti vuoden 2014 pakotteiden seurauksena kehittänyt sekä talouden että rahoitusjärjestelmänsä omavaraisuutta. Maa on kuitenkin hyvin riippuvainen öljyn viennistä ja sen hinnan vaihteluista. Pääomapako on ollut ongelma jo pitkään. Voidaan ajatella, että suvereeni Internet heikentää kansainvälistä kaupankäyntiä ja Venäjän houkuttelevuutta investointikohteena. Vaikutukset saattavat olla saman suuntaisia kuin vuoden 2014 pakotteiden vaikutukset.

5.1 Avoin ja suljettu talous

Taloutta voidaan kuvata joko suljettuna tai avoimena verkostona. Suljettu talous ei ole vuorovaikutuksessa maailman muiden talouksien kanssa; sillä ei ole vientiä, ei tuontia eikä rahansiirtoja. Avoin talous on vapaasti vuorovaikutuksessa muiden talouksien kanssa. Se käy kauppaa tavaroilla, palveluilla ja pääomilla. (Asada ym., 2012)

Vaihtotase on tietyn valtion viennin ja tuonnin erotus, nettorahavirta puolestaan on ostetun ja myydyn ulkomaisen valuutan erotus. Kumpaankin vaikuttavat sekä kotimaan ja ulkomaan välinen korkoero että taloudelliset ja poliittiset riskit. Avoimessa taloudessa nettovienti ja nettorahavirta ovat yhtä suuret. (Suomen Pankki, 2021a) Täysin suljettuja talouksia ei maailmassa ole.

Talouden avoimuutta voidaan kuvailla avoimuusindeksillä (Openness Index), joka on viennin ja tuonnin yhteissumman suhde bruttokansantuotteeseen. Pienet rahoitussektoria lähellä olevat maat kuten Luxembourg, Singapore, Hongkong ja San Marino ovat indeksin perusteella kaikkein avoimimmat taloudet. Skandinavian maat sijoittuvat indeksin luokittelussa keskivaiheille Alhaisin indeksiluku on Sudanilla, Yhdysvalloilla, Pakistanilla ja Brasilialla. Yhdysvaltojen ja Brasilian sijoitus kertoo, ettei indikaattoria voi aivan suoraan tulkita. Pohjois-Korea ei ole mukana listalla. Venäjä ja Kiina sijoittuvat talouden avoimuuden häntäpäähän, Venäjän ollessa noin 10 sijaa Kiinaa avoimempi. (World Bank, 2021c)

Globaalissa maailmassa kansainvälinen kauppa houkuttelee talouksia olemaan avoimia. Vuonna 2019 viisi suurimmista öljynviejistä teki kauppa yhteensä yli 841 miljardilla dollarilla, josta tärkeimpien öljyntuottajien osuudet jakautuivat

seuraavasti: Yhdysvallat 17.9 prosenttia, Saudi Arabia 12.4 prosenttia, Venäjä 12.1 prosenttia, Kanada 5.9 prosenttia ja Irak 5 prosenttia. (Statista, 2021u)

5.2 Rahoitusjärjestelmän verkostot

Rahoitussektori tarjoaa kriittisiä palveluita yhteiskunnalle. Ilman maksupalvelujärjestelmää, rahoitusta ja tietoa omistajuudesta taloudellinen toiminta loppuu nopeasti. Häiriöt rahoituspalveluissa heijastuvat nopeasti logistiikkaverkkoihin, ruoan tuotantoon jne. Jopa lyhyet keskeytykset voivat aiheuttaa suuria taloudellisia tappioita, mutta myös sosiaalista levottomuutta. (ECOFIN, 2019)

Teknologian ja sääntelyn kehittyminen ovat luoneet mahdollisuuden hyvin integroidulle rajat ylittävälle infrastruktuurille, ja palveluntarjoajat voivat usein toimia ympäri maailmaan. Samalla, kun nämä uudistukset ovat tehostaneet toimintaa ja laskeneet kustannuksia, ovat ne tuoneet rahoitussektorille uusia riskejä keskinäisriippuvuuden kasvaessa. Valtiot ovat aiempaa riippuvaisempia rajat ylittävän kommunikaation jatkuvuudesta. (ECOFIN, 2019)

Rahoitusjärjestelmän keskeisenä tehtävänä taloudessa on kanavoida rahoitusta sen tarvitsijoille niiltä, joiden menot ovat tuloja pienemmät. Pankkien ja muiden luottolaitosten lisäksi rahoitusta välitetään laskemalla markkinoille liikkeelle arvopapereita. Kotitaloudet ovat tärkeimpiä lainanantajia, yritykset ja julkisyhteisöt puolestaan pääasiallisia lainanottajia. Rahoitusmarkkinoiden toimet toteutetaan rahoitusjärjestelmän infrastruktuurina toimivissa maksu- ja selvitysjärjestelmissä. (Suomen Pankki, 2021b)

Rahoitusjärjestelmän fyysisen verkoston muodostavat keskuspankit, muut pankit ja luottolaitokset, pörssi ja muut markkinapaikat sekä selvittelytalot. Keskuspankit ovat rahoitusjärjestelmän kriittisiä solmuja. Niiden ensisijainen tehtävä on ylläpitää valuutan vakautta ja inflaatiota sekä huolehtia rahavarannosta. Ne myös hoitavat pankkien välisten maksujen selvittelyä. Selvityksessä keskuspankki laskee kullekin pankille lähtevien ja saapuvien maksujen perusteella position saamisia tai velkoja. Positio hoidetaan taseensiirrolla. (Suomen Pankki, 2021c)

Arvopaperien ja johdannaisten selvittelystä vastaavat yksityiset selvittelytalot. Selvitysjärjestelmällä tarkoitetaan laajasti niitä järjestelyjä ja järjestelmiä, joita käytetään talouden transaktioiden määrittämiseen, toteuttamiseen ja tallentamiseen.

Rahoitusjärjestelmän loogisia verkostoja ovat muun muassa maksuselvittelyihin liittyvistä viesteistä vastaava kansainvälinen SWIFT-maksuviestijärjestelmä sekä erilaiset maksukorttijärjestelmät. Erityisesti SWIFT-järjestelmä on koko rahoitusjärjestelmän kriittinen solmu, mutta sitä ovat myös maksukorttijärjestelmät.

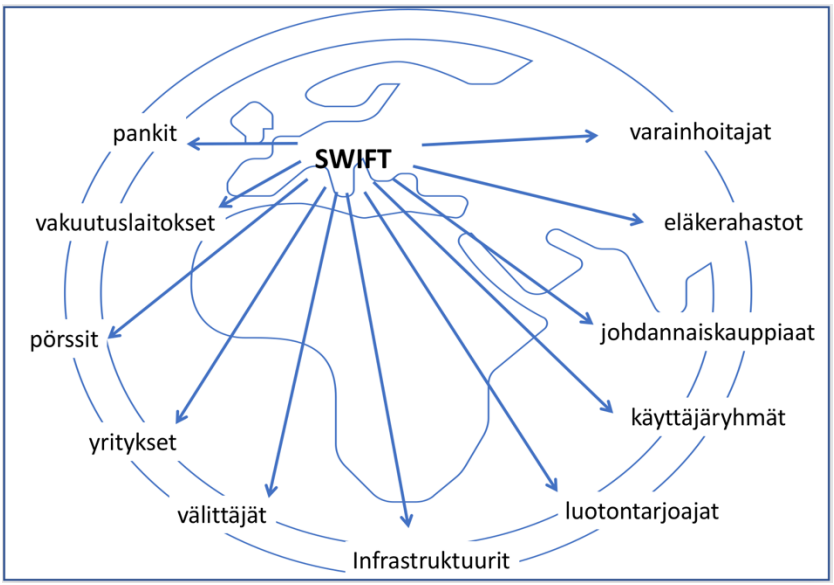
Rahoitusjärjestelmän lopulliset asiakkaat, ihmiset, muodostavat käyttäjäverkoston. Käyttäjäverkoston rakenne ja yhteys muihin verkostoihin riippuu muun muassa siitä, miten paljon käyttäjillä on tilejä ja maksukorttej sekä miten paljon he maksavat käteisellä tai tekevät kansainvälisiä verkko-ostoksia.

5.2.1 SWIFT-maksuviestijärjestelmä

Vuonna 1973 käyttöön otettu Society for Worldwide Interbank Financial Telecommunications SWIFT on maksuviestijärjestelmä, jonka kautta rahoituslaitokset voivat lähettää ja vastaanottaa viestejä rahansiirroista turvallisesti, standardoidusti ja luotettavassa ympäristössä. SWIFT on jo pitkään ollut kansainvälisen rahaliikenteen vallitseva järjestelmä. Se on levittynyt lähes 215 maahan, ja sen jäseninä on noin 11 000 rahoituslaitosta tai muuta yritystä. (SWIFT, 2021a; 2021b) Kuvio 2 esittää SWIFT-maksuviestijärjestelmän keskeistä asemaa rahoitusjärjestelmässä.

SWIFT-organisaation päämaja on Brysselissä Belgiassa. Sen kaksi muuta keskusta ovat Amsterdamissa Alankomaissa ja New Yorkissa Yhdysvalloissa. (SWIFT, 2021a; 2021b)

SWIFT välittää vuodessa yli 5 miljardia pankkien välistä viestiä. Vuonna 2013 sen viestien perusteella siirrettiin triljoona dollaria. SWIFT ei toimeenpane maksunsiirtoja, talleta asiakkaiden rahoja tai tee selvityksiä ja taseensiirtoja. Se ainoastaan tarjoaa infrastruktuurin kommunikaatiolla omine kielineen, standardeineen ja protokollineen. Ilman SWIFT-järjestelmää kansainvälinen kaupankäynti ja investoiminen olisivat hitaampia, kalliimpia ja vähemmän luotettavia. SWIFT-järjestelmän avulla rahoituslaitokset voivat tehokkaasti käyttää myös kolmansien maiden rahoitusinfrastruktuuria. (SWIFT 2021a; Xu, 2020)



KUVIO 2. SWIFT-maksuviestijärjestelmä on rahoitusjärjestelmän kriittinen solmu. (International political economical zone, 2015)

5.2.2 Maksukorttijärjestelmä

Länsimaissa kasvava osa maksutapahtumista tehdään maksukorteilla ja yhä pienenevä määrä käteisellä. Esimerkiksi Suomessa ihmisistä vain noin 23 prosenttia käyttää käteistä ensisijaisena maksutapana. Eurooppalaisilla on keskimäärin 1,7 maksukorttia. (ECB, 2021) Siirtymistä pois käteisestä perustellaan muun muassa rahanpesun estämisellä. Maksukorttijärjestelmä tuottaa palveluntarjoajalle hyvin paljon dataa ostokäyttäytymisestä. Käteisestä poiketen se on kuitenkin häiriöaltis.

Maksukorttijärjestelmää dominoi vuonna 2018 yhdysvaltalainen Visa 43 prosentin osuudella. Kiinalaisen Unionpayn osuus oli 26 prosenttia ja yhdysvaltalaisen MasterCardin osuus oli 24 prosenttia. (Statista, 2021n) Euroopan unionin tavoitteena on yhtenäinen digitaalinen markkina-alue sekä yhteinen maksukortti. Yhteisen EU-maiden maksukortin edistämiseksi kansalliset maksukortit kiellettiin ensimmäisen maksupalveludirektiivin PSD1:n yhteydessä vuonna 2007. Yhteisen maksukortin sijaan yhdysvaltalaiset korttiyhtiöt täyttivät tyhjiön.

5.3 Kuka hallitsee avoimen rahoitusjärjestelmän verkostoja?

Rahoitusjärjestelmän tärkeitä verkostoja ovat maksuviestijärjestelmät ja maksukorttijärjestelmät. Yhdysvalloilla ja Kiinalla on omat kansainvälisesti toimivat maksukorttijärjestelmänsä. Yhdysvaltain maksukorttijärjestelmä on ensisijainen järjestelmä myös Euroopassa. (ECB, 2021) Venäjällä on oma MIR-maksukorttinsa, mutta sen rinnalla kansalaisilla on käytössä myös ulkomaisia maksukortteja. (Bank of Russia, 2021b)

Vaikka suurimmat maksukorttijärjestelmät ovat suosittuja ympäri maailmaa ja ne voidaan arvioida rahoitusjärjestelmän tärkeiksi solmuiksi, ei yksikään maksukorttijärjestelmä ole kansainvälisen rahoitusjärjestelmän kannalta korvaamaton. Lisäksi monissa maissa ollaan siirtymässä yhä enemmän mobiilimaksamiseen. Kansallistem maksukorttijärjestelmien toiminta kuitenkin yleensä riippuu SWIFT-maksuviestijärjestelmästä, joka puolestaan on kriittinen solmu.

SWIFT on Belgian lainsäädännön alaisuudessa toimiva osuuskunta, jonka omistavat ja jota hallinnoivat sen osakkaat, noin 3500 rahoitusalan yritystä ympäri maailmaa. SWIFT-järjestelmää valvoo G-10-maiden keskuspankit – Alankomaiden, Belgian, Italian, Japanin, Kanadan, Ranskan, Ruotsin, Saksan, Sveitsin, Yhdistyneiden kuningaskuntien ja Yhdysvaltojen keskuspankit. (SWIFT, 2021a) Vuonna 2012 myös muiden suurten maiden keskuspankit liittyivät valvovaan elimeen. (SWIFT, 2021b)

Syyskuun 2001 terroristi-iskujen jälkeen yhdysvaltalaiset tiedustelu- ja rahoitusturvallisuusorganisaatiot ovat hiljalleen lisänneet kontrolliaan SWIFT-järjestelmästä, perustellen tarvetta terrorismin vastaisella taistelulla. Vuonna 2011 Yhdysvaltain valtiovarainministeriö alkoi seurata SWIFT:in kautta kulkevaa dataa ja laittaa mustalle listalle epänormaaliksi arvioimiaan pankkeja. Järjestelmän kaikki pankit lopettavat taseensiirtonsa mustalle listalle joutuneeseen pankkiin.

On esitetty arvioita, että SWIFT-järjestelmästä on hiljalleen tullut Yhdysvaltain ulkopolitiikan väline.(De Goede, 2012)

SWIFT-järjestelmästä irrottaminen tarkoittaa varsin täydellisestä eristämistä kansainvälisestä rahoitusjärjestelmästä sekä täysin kestämätöntä kyvyttömyyttä tehdä rahansiirtoja tai maksutoimeksiantoja valtioiden, yritysten ja rahoituslaitosten välillä. Yhdysvaltojen ensimmäinen valinta rahoitussektorin liittyville sanktioille on pankkikorttien maksutoiminnon katkaiseminen SWIFT-järjestelmän kautta. Venäjä suljettiin vuoden 2014 pakotteiden yhteydessä SWIFT:in avulla Visa- ja Mastercard-korttimaksujärjestelmistä, Venezuela puolestaan maaliskuussa 2019. (Xu, 2020)

Tehokkuudeltaan pakotteiden kohteena olevan maan rahoituslaitosten irrottaminen SWIFT-järjestelmästä on äärimmäinen toimi, minkä takia järjestelmä on aktiivisesti mukana pakotekeskusteluissa. Maaliskuussa 2012 Euroopan unioni kielsi SWIFT-järjestelmää tarjoamasta palveluja Euroopan ja Iranin pankkien välillä. Belgiassa sijaitseva SWIFT-organisaatio joutui noudattamaan asemamaansa lakien mukaisesti kieltoa, ja 30 iranilaista rahoituslaitosta suljettiin SWIFT-järjestelmästä. Maaliskuussa 2017 puolestaan Pohjois-Korea suljettiin järjestelmästä vastalauseena ydinaseohjelman jatkamiselle. (Xu, 2020)

Ensimmäinen venäläinen pankki liittyi SWIFT-järjestelmään vuonna 1989. Nykyään järjestelmään kuuluu yli 600 venäläistä rahoituslaitosta. Arviolta jopa yli 90 prosenttia venäläisten pankkien kansainvälisistä transaktioista hoidetaan SWIFT-järjestelmän kautta, ja järjestelmästä on tullut Venäjän rahoitusjärjestelmän avaintekijä. Venäjä on 360 000:lla päivittäisellä viestillään SWIFT-järjestelmän toiseksi aktiivisin käyttäjä. (Amos, 2015)

Yksi Yhdysvaltojen ja EU:n vuoden 2014 Venäjän pakotteisiin liittyvä suunnitelma oli ehkäistä venäläisiltä pankeilta pääsy SWIFT-järjestelmään. (Xu, 2020) Venäjän pääministeri Dmitri Medvedev vastasi tällöin selkeästi, että Venäjän vastareaktio olisi rajoittamaton, itse reaktiota tarkemmin täsmentämättä. (Rapoza, 2015) Yksi mahdollinen vastakeino olisi kaasuntoimitusten katkaiseminen Keski-Eurooppaan. Venäjän tuontiosuus Euroopan kaasusta oli 39 prosenttia vuonna 2019. (Statista, 2021v) Venäjää ei suljettu SWIFT-järjestelmästä. Sen sijaan yhdysvaltalaiset pankit menettivät markkinaosuuksiaan Venäjällä.

SWIFT on painottanut neutraliteettiaan ja tahtoaan kunnioittaa riippumatonta tiedonvälitystä eikä toimia politiikan välikappaleena. Se ei ota kantaa järjestelmässään kulkeviin maksuviesteihin. Viestit kulkevat salattuina, mutta esimerkiksi Yhdysvaltain tiedustelupalvelu CIA:lla on oikeus avata joitakin viestejä rahanpesun ja terrorismin rahoituksen estämiseksi. SWIFT-organisaatio ei itse ole ollut innostunut toimimaan minkään maan ulkopolitiikan välineenä ja rajaamaan Venäjää tai muita pakotemaita ulos järjestelmästään. (SWIFT, 2021c)

Maksuviestijärjestelmä on sitä tehokkaampi, mitä globaalimpi se on. SWIFT-järjestelmän kannalta ei ole toivottavaa, että rinnalle syntyy rinnakkaisjärjestelmiä ja kansainvälinen maksuviestijärjestelmä pirstoutuu. Suojautuakseen pakotteilta ja turvatakseen rahoitussektoriaan Venäjä nopeasti perusti oman kansallisen maksuviestijärjestelmän System for Transfer of Financial Messages (SPFS) että oman maksukorttijärjestelmän MIR. (Bank of Russia, 2021a; 2021b)

SWIFT-järjestelmä on toiminut luotettavasti ja diskreetisti. (SWIFT, 2021c) Mikäli syntyisi rinnakkaisia vähemmän luotettavia maksuviestijärjestelmiä, on olemassa riski, että laittomat rahansiirrot siirtyisivät näihin.

SWIFT-organisaatio ei ollut ainoa, jolla saattoi olla syytä vastustaa suunnitelmaa sulkea Venäjä maksuviestijärjestelmästä. Venäjällä toimii kotimaisten toimijoiden lisäksi myös vieraiden maiden pankkeja ja rahoituslaitoksia, jotka hoitavat lähinnä venäläisten asiakkaiden toimeksiantoja ja ovat läheisissä suhteissa paikallisiin osapuoliin. Ongelmat SWIFT-järjestelmän sulkemisessa heijastuisivat vääjäämättä myös näihin pankkeihin ja sitä kautta ulkomaisiin sijoittajiin.

Ulkomaiset sijoittajat omistavat myös venäläisiä arvopapereita, joista maksetaan säännölliset osingot ja korot. Se, ettei näitä maksuja maksujärjestelmän vaikeuksien takia voida maksaa ajoissa, saattaa aiheuttaa jopa rahoituslaitoksen luottotapahtuman. Pahimmillaan ongelmat maksuhäiriöistä tai velvoitteiden laiminlyönneistä siirtyvät ketjunomaisesti muihin rahoituslaitoksiin myös Venäjän rajojen ulkopuolelle.

Ulkomaisten sijoittajien lisäksi myös kotimaiset sijoittajat reagoivat tilanteeseen, jossa maksujärjestelmään ei voida luottaa tai se ei toimi tehokkaasti. Toisin kuin esimerkiksi tuotantolaitoksen siirtäminen, on rahan siirtäminen helppoa ja hyvin nopeaa. Raha tyypillisesti siirtyy sinne, missä se yhtäältä voi tuottaa eniten ja toisaalta niin infrastruktuuriin, sääntelyyn kuin poliittiseen tilanteeseenkin liittyvät riskit ovat mahdollisimman alhaiset.

Internetin tavoin kansainvälinen maksujärjestelmä tahdottaisiin pitää politiikan yläpuolella. Kumpaakin järjestelmää pidetään liian riippuvaisena Yhdysvalloista. Yhtenä uhkakuvana on maksujärjestelmän pirstoutuminen ja rinnakkaisten järjestelmien syntyminen SWIFT:in rinnalle. Sekä Kiinalla että Venäjällä on jo oma maksujärjestelmänsä. Itse järjestelmän rakentaminen ei ole haaste, käyttäjien saaminen ja järjestelmien maantieteellinen laajentaminen sitä sen sijaan saattaa olla.

5.4 Venäjän suvereeni rahoitusjärjestelmä

Venäjän rahoitus- ja maksujärjestelmä pystyisi toimimaan suvereenisti sekä fyysisenä että loogisena verkkona. Vuoden 2014 Ukrainan pakotteet saivat Venäjän aktiivisesti kehittämään omaa riippumatonta SPFS -maksuviestijärjestelmää ja kansallista NPCS-korttimaksujärjestelmää. (Bank of Russia, 2021a) Lisäksi sillä on oma satelliittipaikannusjärjestelmä (Glonass, 2021), jota voidaan käyttää yhdysvaltalaisen GPS:n sijaan muun muassa seteli- ja maksuautomaattien toimintajärjestelmässä. Tästä huolimatta Venäjän rahoitus- ja maksujärjestelmä tuskin voisi toimia irrallaan globaaleista järjestelmistä.

Neuvostoliiton pankkijärjestelmästä kehittynyt Venäjän pankkijärjestelmä koostuu kahdesta tasosta: Venäjän keskuspankki (Bank of Russia), joka perustettiin 1990, on ensimmäisen tason hallinnollinen elin, ja liikepankit muodostavat toisen tason. (Bank of Russia, 2021c) Keskuspankki on lähinnä vastuussa ruplan liikkeelle laskemisesta, finanssi- ja luottopolitiikan määrittämisestä, inflaation

hallinnasta sekä kaupallisten pankkien valvomisesta ja toiminnasta. Se myös huolehtii kansallisesta maksujärjestelmää, johon kuuluu 31 erillistä maksujärjestelmää. Yli 73 prosenttia maksuista Venäjällä hoidetaan ilman käteistä. (Bank of Russia, 2021)

Venäjän valtio omistaa oleellisen osan pankkisektoria. Tässä mielessä Venäjän rahoitusjärjestelmä muistuttaa Kiinan ja Keski-Idän suurten talouksien rahoitusjärjestelmiä. (Vernikov, 2015) Kaupalliset pankit voidaan jakaa erikoistuneisiin ja yleisiin pankkeihin. Viimeksi mainitut hoitavat kaikkia rahoitusalan toimintoja, muun muassa antolainausta, taseensiirtoja ja rahoitusta. (Xu, 2020; Bank of Russia, 2021c)

Venäjällä on 364 pankkitoimintaa harjoittavaa laitosta ja 41 muuta rahoituslaitosta. (Bank of Russia, 2021c) Pankkisektori on jakautunut kahtia. Kansalaisia palveleva verkosto on varsin itsenäinen ja pystyisi toimimaan, vaikka kansainvälisissä yhteyksissä olisi vaikeuksia. Valtion tukien seurauksena viisi pankkia on oleellisesti muita suurempia. Nämä pankit saattavat olla rahoitusjärjestelmän kriittisiä solmuja kriisitilanteessa. Ne myös tietävät olevansa liian suuria päästettäväksi kaatumaan – too big to fail. Tämä saattaa aiheuttaa moraalivääristymiä.

Venäjän johtava pörssi, Moscow Exchange, on pääomaltaan yksi maailman 20 suurimmasta pörssistä. Se perustettiin vuonna 2011 kahden suuren, 1990-luvulla perustetun pörssin yhteensulautumana. (Moscow Exchange, 2021) Luottoluokituslaitos ACRA perustetiin vuonna 2015. (ACRA, 2021)

Venäjän maksuselvittelytalo National Clearing Centre (NCC) perustettiin vuonna 2005. (National Clearing Centre, 2021a) Se tekee aktiivista kansainvälistä yhteistyötä muiden selvittelytalojen kanssa ja on aktiivinen jäsen Global Association of Central Counterparties CCP12:ssa ja European Association of Central Counterparty Clearing Houses EACH:ssa. Jäseniä NCC:llä on yhteensä 522, joista 497 on paikallisia rahoituslaitoksia 20 on ulkomaalaisia rahoituslaitoksia ja 2 on kansainvälisiä organisaatioita. (National Clearing Centre, 2021)

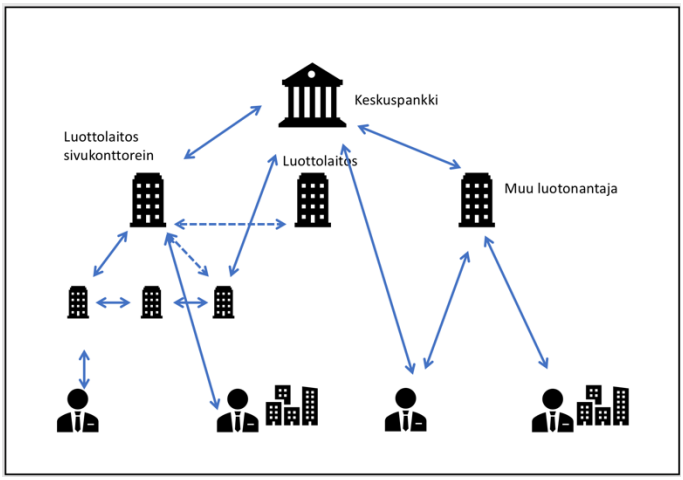
Venäjä on vuodesta 2014 kehittänyt omaa maksuliikenteen viestijärjestelmäänsä, System for Transfer of Financial Messages (SPFS). Tämän päälle rakennettiin Faster Payment System (FSP). SPFS-järjestelmä käyttää samoja standardeja kuin SWIFT. (Bank of Russia, 2021a) Noin 18 prosenttia Venäjän maksuliikenteen viesteistä menee SPFS:n kautta. On mahdollista, että suurin haaste tulee olemaan sekä omien kansalaisten että ulkomaisten yritysten vakuuttaminen käyttämään Venäjän vaihtoehtoista verkkoa.

Monet Venäjän pankit ovat liittyneet myös Kiinan viestijärjestelmään, China International Payments System (CIPS). SPFS-järjestelmä ja CIPS-järjestelmä välittivät yhdessä noin 10 prosenttia maailman maksuliikenteen viesteistä vuonna 2018. (RT news, 2019)

Venäjän keskuspankki otti käyttöön vuonna 2014 kansallisen korttimaksujärjestelmän (National Payment Cards System NPCS). Tämä maksujärjestelmä toimii yhteistyössä muutaman kansainvälisen maksujärjestelmän kanssa. Venäläinen MIR-maksukortti sekä FSP-järjestelmä prosessoidaan NPCS:n kautta, samoin kansainvälisiä kortteja käyttäen tehdyt maksut. MIR-korttijärjestelmä toimii yksinomaan venäläisten järjestelmien varassa. Vuoden 2020 lopussa MIR-kortteja oli 95 miljoonaa. Kortti hyväksytään Venäjän lisäksi monissa IVY-maissa

ja niiden ulkopuolellakin. Sillä tehdään lähes neljännes Venäjän maksutransaktioista. Uusista korteista noin 30 prosenttia on MIR-kortteja (Bank of Russia, 2021b) MIR-maksukorttia voi käyttää vapaasti Venäjällä, mutta muualla sen käyttö on rajoitettu. Kesäkuussa 2016 esiteltiin Venäjän ja Japanin yhteinen MIR-JCB kortti, ja vuotta myöhemmin China Unionpay tarjosi käyttöön MIR-BA-kortin. (Xu, 2020)

Venäjän keskuspankki on sen rahoitusjärjestelmän tärkein fyysinen solmu. (Kuvio 3) SWIFT-maksuviestijärjestelmä on tärkein looginen solmu. Vaikka Venäjän sulkeminen SWIFT-järjestelmän ulkopuolelle ei hajottaisi koko rahoitusjärjestelmää, aiheuttaisi se vakavia ongelmia erityisesti kansainväliseen maksutoimintaan. Kotimaiset maksut pystyttäisiin kömpelösti hoitamaan kierrättämällä ne keskuspankin kautta. Internetin käyttäminen ulkomaisiin maksuihin ei olisi riittävän turvallista. Niitä voitaisiin yrittää kierrättää sellaisten pankkien kautta, joilla on kansainvälisiä yhteistyökumppaneita tai omia toimipisteitä ulkomailla. (Stuenkel, 2015)



KUVIO 3. Keskuspankki on Venäjän rahoitusjärjestelmän keskeinen solmu. (Bank of Russia, 2003)

Venäjän kaltaista kansainvälisesti verkostoitunutta taloutta olisi poissulkeminen SWIFT-järjestelmästä haitannut huomattavasti enemmän kuin Iranin tyyppistä valtiota. Se todennäköisesti entisestään työntäisi Venäjää tiivistämään yhteistyötä Kiinan kanssa. Tyypillisesti maiden välinen yhteistyö on ollut hyödyllistä erityisesti Kiinalle. Kiinalais-venäläiset kaasusopimukset ovat tästä yksi esimerkki. (Stuenkel, 2015)

Venäjän ulossulkeminen heikentäisi SWIFT-järjestelmää kansainvälisenä standardina. Jo nyt 45 prosenttia maailman kaikista maksu- ja luottokorteista on kiinalaisen Chinese Interbank Creditcard -yhdistyksen luottokortteja, jotka käyvät 135 maassa. (Stuenkel, 2015)

Venäjän rahoitusjärjestelmä ja sen mahdolliset rajoitukset tai ongelmat heijastuvat myös käyttäjiin. Venäläisistä noin 75 prosentilla on tili, mutta vain noin 20 prosentilla on luottokortti. Lähes 40 prosenttia tekee verkko-ostoksia tai maksaa laskuja verkon kautta. Digitaalisia maksuja tekee 62 miljoonaa, ja Internetin

käyttäjistä verkkokauppoja selasi vuoden 2021 alussa 80 prosenttia Internetin käyttäjistä, verkko-ostoksia teki 60 prosenttia käyttäjistä. (Paypers, 2021)

Venäjällä on itsenäisesti toimivat maksupalvelusysteemi ja kuluttajapankkiverkosto. Kansainvälisillä yrityksillä on merkittävä asema Venäjän digitaalisilla markkinoilla. Kiinalaisilla verkkokaupoilla on suurin osuus siten, että pelkästään AliBaba -konsernin AliExpress-yritys vastaa arvoltaan 58 prosenttia ja volyymiltään 79 prosentista rajan ylittävistä paketeista. Länsimaiden osuus on vain 27 prosenttia kaupan arvosta ja 5 prosenttia volyymistä. Viisi tärkeintä verkkokauppaa Venäjällä ovat AliExpress, eBay, Joom, iHerb ja Asos. Ulkomaisia verkko-ostoja on jonkin verran hillinnyt venäläisten heikko englanninkielentaito. Tähän on tullut korjaus, kun kauppasivuja on muutettu venäjänkielisiksi. Valtaosan kuljetuksista hoitaa Venäjän posti. (Paypers, 2021)

5.5 Venäjä kansainvälisenä taloutena

Venäjä on kansainvälinen talous, jonka vuoden 2020 viennistä energiasektorin osuus oli Itsenäisten valtioiden yhteisön (IVY) -maiden ulkopuolisen viennin kokonaisarvosta noin 70 prosenttia ja IVY-maiden viennin kokonaisarvosta noin 30 prosenttia. (Statista, 2021r) Vuonna 2020 tuonnin osuus elintarvikkeista arvolla mitattuna oli arviolta 30 prosenttia. (Statista, 2021s) Venäjä pyrkii elintarvikeomavaraisuuteen ja vähentämään tuonnin osuutta, joka 2014 elintarvikkeiden arvosta oli 40 prosenttia. (Liefert & Liefert, 2020) Venäjän keskuspankin mukaan 67 prosenttia viennistä maksettiin vuonna 2019 dollareina, 17 prosenttia euroina ja 14 prosenttia ruplina. (Suomen Pankki, 2019)

Venäjä on maailman kolmanneksi suurin öljyntuottaja ja toimittaa noin 13 prosenttia maailman öljystä. (Statista, 2021u) Venäjä ei ole öljyntuottajamaiden Organization of the Petroleum Exporting Countries OPEC:in jäsen, mutta on tyypillisesti osallistunut OPEC:in neuvotteluihin ja sopimuksiin. (Mann, 2009) Vuonna 2020 Venäjä kuitenkin irtaantui hinta- ja tuotantosopimuksista ja aloitti oman hintakilpailun, mitä voidaan pitää riskinä Venäjälle.

Venäjän talous on hyvin riippuvainen öljystä. (Pönkä & Zheng, 2019) Maa vei öljyä yli 74 miljardin dollarin arvosta vuonna 2020, jolloin öljyn keskihinta oli noin 42 dollaria tynnyriltä eli noin 160 litralta. (Statista, 2021z; Statista, 2021p) Venäjän bruttokansantuotteesta, 1.4 biljoonaa dollaria. (Statista, 2021t) Öljyn hinnan huippuvuonna 2012, jolloin sen keskiarvo oli 112 dollaria tynnyriltä, viennin arvo oli 4.5-kertainen, 180 miljardia dollaria. (Statista, 2021z; Statista, 2021p).

Venäjän talous on Yhdysvaltojen taloutta herkempi öljyn hinnalle, jonka OPEC-maat määrittävät poliittistaloudellisena päätöksenä. Kansainvälinen valuuttarahasto (International Monetary Fund, IMF) on ennustanut, että öljyn keskimääräinen hinta vuonna 2021 olisi noin 46 dollaria tynnyriltä, vain hieman Venäjälle kriittistä hintaa korkeampi. IMF:n arvion mukaan öljyn hinnan taloudellisesti kriittinen kannattavuuspiste on Venäjälle 30-40 dollaria tynnyriltä, kun se maailman suurimmalle öljyntuottajamaalle Yhdysvalloille on 28 dollaria tynnyriltä ja toiseksi suurimmalle Saudi-Arabialle on 76 dollaria tynnyriltä. (IMF, 2021)

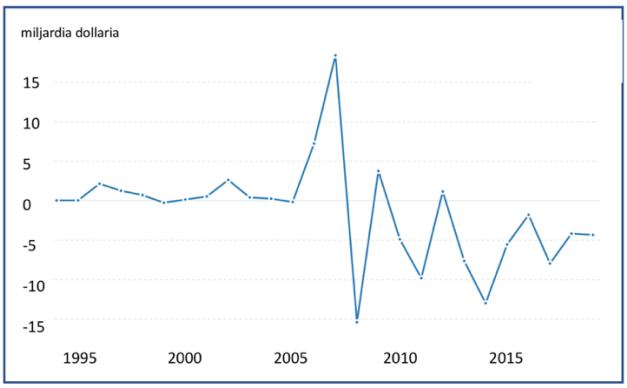
Venäjän talouden lisäksi myös rupla on hyvin herkkä öljyn hinnan vaihteluille, ja ruplan arvo on historiallisesti seurannut öljyn hintaa. (Pönkä & Zheng 2019) Ruplan alhainen hinta yhtäältä auttaa vientiä, mutta toisaalta saattaa lisää valuuttapakoa.

Vuonna 2014 öljyn hinnan aleneminen ja samanaikaiset pakotteet ja vastapakotteet johtivat oleelliseen valuuttapakoon: pääomaa siirrettiin ulkomaille 151.5 miljardia dollaria, mikä on 90 miljardia dollaria enemmän kuin edeltävänä vuonna ja 20 miljardia dollaria enemmän kuin finanssikriisin ennätysvuonna 2008. (Tyll ym., 2018).

Vuoden 2014 Ukrainan kriisin seurauksena suorat investoinnit Venäjälle loppuivat lähes kokonaan vuoden. Tätä ennen lähes 75 prosenttia suorista investoinneista tuli EU-maista. Vuonna 2014 määrä tippui 30 prosenttia ja seuraavana vuonna 92 prosenttia. (CBRF 2016) Pääoman puute johti korkojen nousuun, ja lopulta suuri määrä investointeja lykättiin tai peruttiin. (Dreyer & Popescu, 2014)

Suvereeni Internet vaikuttaisi Venäjän talouteen monella tavalla. On erittäin todennäköistä, että kansainvälisen kaupankäynnin edellytykset heikkenisivät. Konkreettisia vaikutuksia on vaikea arvioida. Esimerkiksi siitä, miten suvereeni Internet on vaikuttanut Kiinan kansainväliseen kauppaan, ei ole tarkkoja arvioita. Voidaan kuitenkin ajatella, että seuraukset rahoitusmarkkinoilla olisivat samansuuntaiset kuin vuoden 2014 Ukrainan kriisi pakotteineen: pääomaa karkaisi entisestään, ja suorat investoinnit Venäjälle vähenisivät.

Venäläisellä rajojen ulkopuolella olevalla pääomalla on monenlaisia kytkentöjä. On epätodennäköistä, että pääoman karkaamista pystyttäisiin tai edes täysin tahdottaisiin estää. Pääomapako on erityisen ikävä Venäjän kaltaiselle maalle, jonne pitäisi tehdä suuria pitkäaikaista kasvua tukevia investointeja. Pääomaa voidaan kerryttää ulkomaille sekä siirtämällä valuuttaa että tekemällä joko passiivisia portfoliosijoituksia, joissa ei tavoitella valtaa kohdeyrityksessä, tai aktiivisia suoria sijoituksia, joissa tavoitteena on myös osallistua yrityksen toimintaan. (kuvio 4) Ulkomaisista sijoituksista kerätyt rahat voidaan pitää ulkomaisilla tileillä. Abalkinin ja Whalleyn (1999) arvioivat Venäjän pääomapaon liittyvän pääoman turvaamiseen, ei niinkään maksimaaliseen voitontavoitteluun.



KUVIO 4. Venäjän portfoliosijoitusten arvo vuosina 1995-2019. Vuonna 2019 portfoliosijoitusten arvo oli - 4.3 miljardia dollaria. (World Bank, 2021b)

Pääomapako on ollut ongelma Venäjälle jo 1990-luvun alussa. Vuoden 2008 finanssikriisin seurauksena pääomaa pakeni yli 300 miljardia dollaria. Pako hidastui lähes kolmannekseen vuonna 2009, mutta kiihtyi jälleen vuoden 2014 pakotteiden seurauksena. Vuoteen 2018 mennessä kumulatiivinen summa oli kasvanut 700 miljardiin. Tämä on suunnilleen kaksinkertaisesti Venäjän kiinteät investoinnit vuonna 2017. (Becker, 2019)

Venäjän pääomapako ei ole ainoastaan sisäinen ongelma. Se on herättänyt kiinnostusta myös siksi, että sillä saattaa olla yhteyksiä rahanpesuun, veronkiertoon terrorismin rahoittamiseen ja muuhun rikollisuuteen. Rahaa kierrätetään niin länsimaisten pankkien kuin suorien sijoitustenkin kautta. Venäjän suorat sijoitukset Kyprokselle ovat olleet 12 kertaa suuremmat kuin maan BKT. (Becker, 2019) Tämä on erikoista, koska suorat sijoitukset lähtökohtaisesti tehdään tavoitteena aktiivinen osallistuminen sijoitusyrityksen toimintaan.

6 SULKEUTUVAN VENÄJÄN JA AVAUTUVAN KIINAN VERTAILUA

Venäjä ja Kiina alkoivat 2000-luvulla haastaa yksinapaiseksi luisunutta maailmaa taloudellisen kasvun ja kulttuurisen nationalismin tukemina. (Larson & Shevchenko, 2010) Kumpikin maa on korostanut valtiollisen suvereniteetin ulottuvan myös Internetin maasegmenttiin. ((Budnitsky & Jia, 2018; Griffith, 2019)

Kiina on onnistunut yhdistämään suvereenin Internetin ja kansainvälisen talouden hyvin. Sekä IMF että Maailmanpankki ovat ennustaneet, että vuonna 2024 Kiina on maailman suurin talous, Yhdysvaltojen jäädessä toiseksi. Venäjä olisi vuonna 2024 maailman kuudenneksi suurin talous, kun se vuonna 2020 oli sijalla 11. (Statista, 2020b) Shen (2016) on tähdentänyt, että Kiinan tavoitteena on alusta alkaen ollut yhtäältä kontrolloida Internetin segmenttiään ja toisaalta käyttää sitä kansainvälisen kaupan välineenä.

Tässä luvussa verrataan Venäjän ja Kiinan Internetin segmenttejä ja talouden rakenteita. Erityisesti yritetään tunnistaa seikkoja, jotka ovat mahdollistaneet Kiinan suvereenin Internetin. Lisäksi kuvaillaan Venäjän ja Kiinan yhteistyötä tässä tutkimuksessa käsitellyillä sektoreilla.

6.1 Internet

Yhdysvaltain hallituksen perustama Freedom House arvioi, että Internet on vähiten vapaa Kiinassa, muttei Venäjäkään sijoitu erityisen hyvin. Ylipäätään tilanne on huonontunut 26 muussa tutkituista 65:stä. (Freedom House, 2021) Maailman 3.7 miljardista Internetin käyttäjästä 71 prosenttia elää ympäristössä, jossa saattaa tulla tuomituksi tai vangituksi poliittisesti, sosiaalisesti tai uskonnollisesti aran sisällön julkaisemisesta. Käyttäjistä 48 prosenttia asuu maissa, joissa käyttäjät voidaan jopa tappaa, ja 47 prosenttia maissa, joissa viranomaiset voivat estää sosiaalisen verkon käytön. Freedom Housen tutkimuksessa Islanti ja Viro sijoittuivat kärkeen, samoin Saksa, Kanada, Australia ja tutkimuksen kotimaa Yhdysvallat. Myös Armenia ja Georgia on arvioitu vapaan Internetin maiksi. (Freedom House, 2021)

Kiinassa oli vuoden 2020 lopussa yli lähes miljardi käyttäjää, mikä on noin 70 prosenttia kansasta ja yli 21 prosenttia kaikista maailman käyttäjistä. (Statista, 2021m) Venäjällä käyttäjiä on 124 miljoonaa, mikä on lähes 83 prosenttia kansasta ja noin 3 prosenttia kaikista maailman käyttäjistä. (Statista, 2021x) Markkinapotentiaaliltaan Kiinan Internetin segmentti on kahdeksankertainen Venäjän segmenttiin verrattuna.

Venäjän ja Kiinan Internetin segmentit ovat kehittyneet hyvin eri tavoin. Venäjän segmentti sai 1990-luvulla kehittyä varsin rauhassa yksityisissä liberaaleissa piireissä. Alussa uudet teknologiayritykset nähtiin arvokkaina yhteistyö-

kumppaneina maabrändin rakentamisessa. Valtio kuitenkin otti tiukemman otteen Internetin Venäjän segmentistä vuoden 2014 jälkeen. Sittemmin Internetiä on rajoitettu lukuisin laein. (Tselikov, 2014)

Internet tuotiin Kiinaan vuonna 1994 presidentti Jiang Zemingin aikana. (Griffith 2109) Taustalla oli ajatus maailman siirtymisestä toisen aallon industrialismin ajasta kolmannen aallon informaatioaikaan, ja tavoitteena oli lisätä Kiinan kansainvälistä kilpailukykyä. (Negro, 2017)

Kiinan valtio on kontrolloinut Internetiä alusta alkaen. Yksityisillä yrityksillä on ollut jonkinlainen sija Internetin kehittämisessä: ne ovat saaneet tehdä investointeja ja aloitteita. Myös kilpailu palveluntarjoajien välille on ollut sallittua. (Tan ym., 1999) Tällä hetkellä maailman suurimmista kymmenestä Internetyrityksestä viisi on kiinalaisia, toiset viisi yhdysvaltalaisia. (Statista, 2021f)

Jo presidentti Zemingin edeltäjä, presidentti Deng Xiaoping oli vuonna 1979 aloittanut niin kutsutun Avoimien ovien politiikan. Tavoitteena oli yhtäältä tuoda länsimaista osaamista Kiinaan ja toisaalta avata maata ulkomaiselle kaupalle ja investoinneille. (Huan, 1986) Avoimien ovien politiikan toteuttamisen seurauksena Kiina on tasapainoillut länteen avaamisen ja länsimaisten vaikutteiden etäällä pitämisen välillä. Yhtäältä Kiina hyötyy paljon Internetistä, mutta toisaalta Internet vaikuttaa maan poliittiseen vakauteen. Tasapainoa pyritään ylläpitämään muun muassa Kultaisen kilven Golden Shield -projektilla.

Golden Shield -projektia on kehitetty jo 1990-luvulla, mutta se esiteliin julkisuudessa vasta vuonna 2000 suuressa vientinäyttelyssä Pekingissä. Se on yksi 12 Golden-projektista Kiinan kehittämiseksi. Muut projektit liittyvät muun muassa vientiin, elektroniseen valuuttaan, rahoitussektoriin ja verotukseen. Alkuaikoina Golden Shield -projekti keskittyi sisällön yleiseen kontrollointiin, mutta paino on siirtynyt sisällön suodattamiseen palomuurein ja täten yksilön kontrolloinniksi verkon loppupäissä. Se pystyy suodattamaan käytännössä kaiken verkkoliikenteen. (Chandel ym., 2019)

Monet länsimäiset yritykset kuten kanadalainen Nortel Networks, Motorola, Sun Microsystems ja Cisco Systems osallistuivat Kiinan reitittimien ja palomuurien verkon rakentamiseen. (Chandel ym., 2019) Viime aikoina Kiina vie sensuurin liittyvää teknologiaansa ainakin 18 maahan. (Polyakova & Meserole, 2019)

Kiinan palomuuri toimii tehokkaasti teknologiansa ohella myös itsesensuurikulttuurin takia. Yritysten edellytetään ottavan vastuun julkisesta sisällöstään. Itsesensuuri koskee myös kansainvälisiä yrityksiä. (Roberts, 2018) Vaikka sensuuri loukkaa länsimaista ideologiaa, kiinalaiset markkinat ovat liian tuottoisat, jotta tämä mahdollisuus ohitettaisiin.

Venäjältä puuttuu sekä teknistä osaamista, infrastruktuuria että resursseja toteuttaa Kiinan Suuren palomuurin kaltainen järjestelmä. (Gilmore, 2021) Koska Venäjän verkko on rakenteeltaan hajautunut, ei siinä voida systemaattisesti käyttää samoja suodatusmenetelmiä kuin Kiinassa. (Ramesh ym., 2020)

Venäläiset käyttäjät ovat tottuneet Kiinaa vähemmän kontrolloituun Internetiin, jossa myös opposition ääni on kuuluvissa. Systemaattisen datan suodattamisen sijaan Venäjä kontrolloi Internetin segmenttiään satunnaisemmin, nostaen yksittäisiä rangaistavia tapauksia julkisuuteen pelotteeksi.

Kiinassa on maailman eniten Internetin käyttäjiä. Kiinalaiset viettävät Internetissä yli kolme tuntia päivässä, josta sosiaalisessa mediassa keskimäärin 2

tuntia. (Statista, 2021b) Monet yhdysvaltalaiset sosiaalisen median alustat kuten Facebook, Google, Twitter, Instagram, Snapchat, Yahoo, Slack ja YouTube on estetty Kiinan Internetissä kokonaan. (Chandel ym., 2019) Käyttäjiä sosiaalisen median suosituimmissa palveluissa on seuraavasti: WeChat (Weixin) 730 miljoonaa käyttäjää, Sina Weibo 47 miljoonaa käyttäjää, Kuaisihou 45 miljoonaa käyttäjää ja Douyin 41 miljoonaa käyttäjää. (Statista, 2021k) Käyttäjämäärät ovat hyvin suuria, mitä voidaan pitää houkuttelevana seikkana sosiaalisen median alustoille. Yhdysvaltalaisille verkkoalustoille voi kirjautua virtuaalisen erillisverkon, VPN:n kautta. Virallisia tietoja käyttäjämääristä ei kuitenkaan ole.

Venäläiset viettävät Internetissä keskimäärin 4.5 tuntia päivässä vuonna 2020. (Statista, 2021a) Sosiaalisessa mediassa aikaa kului keskimäärin 2.5 tuntia vuonna 2019. Suosituimmat alustat ovat yhdysvaltalaisia: 85 prosenttia käytetystä ajasta kului Youtubessa, 78 prosenttia kotimaisessa VK:ssa, 76 prosenttia Whatsappissa ja 61 prosenttia Instagramissa. Näiden alustojen jälkeen suosittuja ovat kotimaiset Odnoklassinki ja Viber sekä yhdysvaltalainen Facebook ja kiinalainen Tiktok. (Statista, 2021x) Esitettyjen lukujen valossa olisi yllättävää, elleivät käyttäjät reagoisi tilanteeseen, jossa suvereenin Internetin segmentin nimissä kaikki ulkomaiset verkkoalustat suljettaisiin.

Kaikki kansalaisten digitaaliset transaktiot ja liikkuminen verkossa jättävät valtavan määrän dataa. Kiinassa hyvin suuri osa päivittäisistä ostoksista, rahatransaktioista, liikkumispalveluiden tilaamisista tehdään AliBaba-konsernin alustalla. Aktiivisia käyttäjiä alustalla oli vuonna kesäkuussa 2020 lähes 760 miljoonaa, ja se kilpailee koossa yhdysvaltalaisen Amazonin kanssa. (Statista, 2020a) Alustan käyttöön kannustetaan jakamalla pisteitä, joilla saa erilaisia etuja. On todennäköistä, että alustan käyttämisestä saatu erittäin monipuolinen data päätyy Kiinan valtiolle. Voidaan ajatella, että AliBaba-konserni on Kiinassa monessa mielessä hyvin painava ja vaikutusvaltainen solmu sekä Internetin että kaupankäynnin verkostossa.

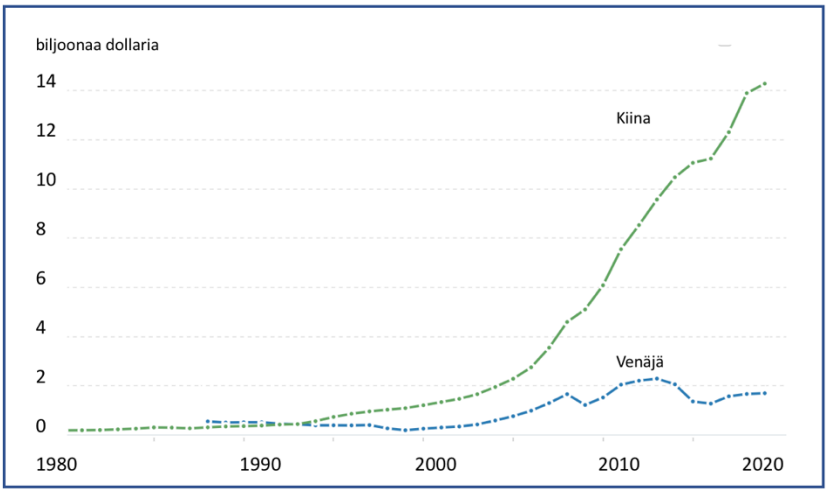
Kaupallisen AliBaba-alustan pistejärjestelmää ollaan laajentamassa valtion hallinnoimaksi järjestelmäksi, jossa elämällä ’oikein’ ja jakamalla itsestään dataa valtiolle voi ansaita sosiaalista statusta parantavia pisteitä. Puhtaan vakoilun sijaan kansalaisia palkitaan siitä, että heidän toiminnastaan jää digitaalinen jälki. (Mac Sithigh & Siems, 2019).

Venäläiset käyttävät kotimaisten verkkoalustojen lisäksi hyvin paljon niin yhdysvaltalaisia kuin kiinalaisiakin suurten teknologiayritysten alustoja. (Statista, 2021x) Ainakin osa datasta päätyy Venäjän sijaan alustojen omistajille. Venäjällä yksikään yritys ei ole lähellekään AliBaba-konsernin tai Amazonin suuruinen sen enempää liikevaihdolla kuin toiminnan laajuudellakaan mitattuna. Omaa AliBaban tai Amazonin kaltaista vaikutusvaltaista alustatalouden solmua Venäjällä ei ole.

Kiina on onnistunut kasvattamaan kansainvälistä yhteistyötä suvereenista Internetistä huolimatta. Siinä, missä Venäjä pyrkii sulkeutumalla suojautumaan ainakin ulkoiselta uhalta, Kiina rakentaa aktiivisesti omaa kotimaista ja ulkomaista verkostoaan vastapainoksi Yhdysvaltojen dominanssille. Yhdysvaltain tavoin Kiinalla on suuria teknologiayrityksiä, joita se käyttää kansainvälisessä

ympäristössä niin kaupallisiin kuin kulttuurisiinkin tarkoituksiin. Kiina tekee itseään korvaamattomaksi. Tämä on yksi ratkaiseva tekijä siinä, miksi Kiina pystyy ylläpitämään suvereenin Internetin segmentin ja miksi se Venäjälle olisi erittäin haastavaa, ellei pitkällä aikavälillä myös mahdotonta. Shen (2016) on tuonut esille, miten Internetin ja kansainvälisen kaupan yhdistäminen on ollut Kiinan strategia alusta alkaen.

Kiina on maailman toiseksi suurin talous, jonka bruttokansantuote BKT oli vuonna 2020 yli 14.7 biljoonaa dollaria. (Statista, 2021h) Venäjän BKT on tästä noin 11 prosenttia, 1.46 biljoonaa dollaria. (Statista, 2021g) (kuvio 5) Kiinan markkinat ovat liian houkuttavat, jotta ulkomaiset yritykset malttaisivat boikotoida Kiinaa. Vaikka Kiina sensuroi ylikansallisia yrityksiä samalla tavalla kuin kotimaisiakin yrityksiä, monet yhdysvaltalaiset yritykset toimivat tai ovat toimineet markkinoilla sensuurin vaatimuksista ja Suuresta palomuurista huolimatta. Näiden yritysten tulee Kiinassa noudattaa maan lakeja, vaikka lait loukkaisivat Yhdysvaltojen puhevapautta tai sitä, miten ulkomaiden näkökulmasta Kiinan tulisi kohdella kansalaisiaan. Yritykset ovat perustelleet olemassaoloaan sillä, että se vähäinen informaatio, jota he tuottavat, on kiinalaisille hyväksi. (D'Jaen, 2007; Roberts, 2018)



KUVIO 5. Venäjän ja Kiinan bruttokansantuotteen kehitys vuosina 1990-2019. Vuonna 2019 Venäjän BKT oli 1.7 biljoonaa dollaria ja Kiinan BKT oli 14.3 biljoonaa dollaria. (World Bank, 2021a)

Kiina on avannut rahoitusjärjestelmäänsä ja valuuttakauppaa hyvin hallitusti. Kiinan renminbin arvo oli 1990-luvun alkuun kiinteä ja yliarvostettu, eikä sitä voinut vapaasti vaihtaa. Noin 15 vuoden aikana siirryttiin hiljalleen järjestelmään, jossa renminbin arvo määräytyi ulkomaisen kysynnän ja tarjonnan mukaan. Vuonna 1979 vienninharjoittajat saivat luvan säästää itsellään osan kaupankäynnistä saadusta vieraasta valuutasta, ja vuonna seuraavana vuonna vientiyritykset saivat luvan myydä ylimääräisen valuutan. Vuonna 1993 hyväksyttiin suunnitelma ehdollisesti vaihdettavasti renminbistä ja helpotettiin sääntelyä suorista sijoituksista. Kiinaan alkoi virrata pääomaa. Vuodesta 2013 renminbiä on saanut vaihtaa vapaasti tietyin rajoituksin. (Maswana, 2011) Toukokuussa 2019

renminbistä on tullut maailman kuudenneksi suosituin kansainvälisen kaupan valuutta Yhdysvaltain dollarin, euron, punnan, jenin ja Kanadan dollarin jälkeen. (Statista, 2021l)

Erityisesti kehittyvien, investointeja tarvitsevien maiden kannalta on edullista, että niihin virtaa ulkomaista pääomaa niin suorina sijoituksina kuin portfoliosijoituksinakin. Kiinan vahvuuksina yrityksille ja investoijalle mainitaan muun muassa maailman suurimmat markkinat, joilla on 1.44 miljardia potentiaalista asiakasta. (Statista, 2021y) Yksinään markkinoiden valtavan koon takia monet yritykset ja investoijat eivät voi rajoituksista huolimatta pysyä ulkopuolella. Työkustannukset ovat suhteellisen alhaiset, tuotantosektori on kehittynyt ja maantieteellinen sijainti on edullinen. Investointien houkuttelevuutta lisäävät Silkkitien kehittäminen ja uusi vientiverkosto.

Kiinan heikkouksia investointikohteena ovat jatkuvasti muuttuva lainsäädäntö, byrokratia ja hallinnon monimutkaisuus, läpinäkyvyyden puute, kulttuuriset erot sekä ammattitaitoisen työväen vähäisyys. Kiina asettaa rajoituksia vieraille sijoituksille muita maita voimakkaammin, ja osa aloista on niiltä kokonaan suljettu. (Davies, 2013)

Venäjän vahvuuksia investointikohteena ovat maan vahva, erityisesti suurille luonnonvaroille perustuva taloudellinen pohja, ammattitaitoinen työvoima, julkisen velan vähäisyys ja hyvä valuuttavaranto. Heikkouksina voidaan nähdä talouden suuri riippuvuus hiilivetyjen ja muiden raaka-aineiden hinnasta sekä muun muassa teknologian riippuvuus tuonnista. Kiinan tavoin lainsäädäntö on joskus monimutkaista ja ristiriitaista, immateriaalioikeuksien loukkaaminen on todellinen ongelma, ja monet strategiset alueet on suljettu ulkomaisilta. Geopoliittisia jännitteitä ja sanktioita ei voi jättää huomioimatta.

Venäjän talous ei houkuttelevuudessa pysty kilpailemaan Kiinan kanssa, eikä maa tarjoa lähellekään yhtä suurta markkinapotentiaalia kuin Kiina. On epätodennäköistä, että kansainväliset yritykset, kauppakumppanit ja sijoittajat sopeutuvaisivat Venäjän suvereenista Internetistä aiheutuviin suoriin ja välillisiin kustannuksiin yhtä hyvin kuin taloudeltaan sitä 11 kertaa suuremman Kiinan suvereenista Internetistä aiheutuviin kustannuksiin.

Kiinan kaikkein aikojen suurin investointi infrastruktuuriin, Belt and Road -aloite, sisältää digitaalisen silkkitien, kiinalaisen valokaapeliverkon, joka tavoittaisi 62 prosenttia maailman asukkaista ja jonka kautta ainakin osaa käyttäjistä voisi potentiaalisesti seurata. (Chalk, 2019)

SWIFT-maksuviestijärjestelmää vastaava Cross-Border Interbank Payment System (CIPS) perustettiin vuonna 2015. Tämä rajat ylittävä järjestelmä käyttää syntaksissaan SWIFT:in standardeja. Sen tavoitteena oli edesauttaa renminbi-valuutan kansainvälistymistä. (Xu, 2020).

Maksuviestijärjestelmä on yksi rahoitusjärjestelmän kriittisistä solmuista. Oma maksuviestijärjestelmä vähentää Kiinan riippuvuutta yhdysvaltalaisesta SWIFT-järjestelmästä. Vuoden 2019 alkupuolella CIPS-järjestelmällä oli 31 suoraa jäsentä ja 847 epäsuoraa jäsentä, joista 356 oli Kiinassa, 294 oli muualla Aasiassa, 105 oli Euroopassa ja 25 oli Pohjois-Amerikassa. (Xu, 2020).

Aasian infrastruktuurin investointipankin perustaminen on yksi merkittävä askel Kiinan strategiassa turvata kulku elintärkeiden resurssien luo ja kansainvälisille markkinoille. Tavoitteena on saada remninbistä kansainvälisen kaupan ja rahoituksen merkittävä valuutta. Tähän mennessä Yhdysvallat on voinut käyttää dollaria ulkomaanpolitiikan työkaluna. Noin 87 prosenttia kansainvälisestä kaupasta käydään yhä dollareilla. Erityisesti suurten kehittyvien BRICS-maiden sisäisessä kaupankäynnissä mielellään vältettäisiin dollaria sen korkean hinnan takia. (Stuenkel, 2015) Kiinalla kuitenkin on maailman suurin valuuttareservi, jonka vuonna 2019 oli yli 310 biljoonaa dollaria. Tämä hieman alle prosenttia Kiinan BKT:stä. Reservistä kokoonpano ei ole julkista tietoa, mutta vuonna 2014 noin 60 prosenttia valuuttareservistä oli dollareina. (Xin, 2019)

Maailman toiseksi suurimpana taloutena Kiina on houkutteleva kauppakumppani sen asettamista rajoituksista huolimatta. Talouden vuotuinen kasvuvauhti, joka on viime aikoina ollut yli 6 prosenttia, on maailman nopeinta. Venäjä on taloutena selvästi pienempi, ja sen vuotuinen kasvuvauhti on ollut muutaman prosentin luokkaa. Kiinalla on oma suvereenisti toimiva ja hallitusti ulkomaailmalle avattu rahoitusjärjestelmä CISP-maksuviestijärjestelmineen. Myös Venäjällä on toimiva maksuviestijärjestelmä, mutta sen käyttäjäkunta on huomattavasti pienempi. Internetin tavoin myös maksujärjestelmän kannattaa olla mahdollisimman globaali.

6.2 Venäjän ja Kiinan yhteistyö

Neuvostoaikojen veljellisten suhteiden tavoin Kiina ja Venäjä auttavat toisiaan vastavuoroisesti. Kiinan kansankongressin kesällä 2015 julkaistu kyberturvallisuuslaki sisältä osia Venäjän senaatin vuoden 2014 kyberturvallisuuslakiluonnoksesta. Venäjä puolestaan on saanut apua sisällönsuodattamisarkkitehtuurin luomisessa, jossa on monia piirteitä Kiinan suuresta palomuurista. (Griffiths, 2019) Kiina on palomuuriin liittyvässä teknologisesti Venäjää huomattavasti edellä.

Venäjä ja Kiina allekirjoittivat vuonna 2014 kahdenkeskisen sopimuksen kansainvälisen informaatioturvallisuuden yhteistyötä ja määrittivät laajalti yhteistyön eri muotoja. (Epifanova, 2020) Vuonna 2018 kiinalainen Huawei sopi venäläisten yritysten kanssa yhteistyöstä 5G-verkon, pilvipalvelujen ja tekoälyteknologian kehittämiseksi. Kesällä 2019 maat sopivat yhteisestä korkean teknologian kehittämiseen keskittyvästä investointirahastosta. Puhetta on ollut myös yhteisestä satelliittiverkosta.

Venäjä on esittänyt, että uuteen DNS:ään voisivat liittyä BRICS-maat, jotka Venäjän lisäksi ovat Kiina, Intia, Brasilia ja Etelä-Afrikka. BRICS-maat edustavat noin 41 prosenttia maailman väkiluvusta ja noin 23 prosenttia maailman BKT:stä. Marraskuussa 2017 Venäjän turvallisuusneuvosto yhtyi ehdotukseen, että vaihtoehtoinen verkko olisi BRICS-maiden saatavilla. Järjestelmässä olisi omat varmuuskopioidut juurinimipalvelinserverit kussakin maassa, riippumattomina ICANN organisaatiosta. (Securityalliance, 2020) Olisi kuitenkin todennäköistä, että Venäjä jäisi yksin oman DNS:nsä kanssa. Brasilialla, Intialla ja Etelä-Afrikalla

puolestaan tuskin on kiinnostusta liittyä järjestelmään, jota niiden kauppakumppanit Yhdysvallat ja Iso-Britannia eivät kannata. Kiinalla puolestaan on jo toimiva suvereeni Internet. Arsène (2015) arvioi, että oman nimipalvelujärjestelmän sijaan Kiina on aktiivisesti pyrkinyt vaikutusvaltaiseksi toimijaksi kansainväliseen järjestelmään.

Vuoden 2014 Edward Snowdenin paljastukset yhdysvaltalaisten teknologiayritysten ja Yhdysvaltain kansallisen turvallisuusviraston NSA:n yhteistyötä lisäsivät Venäjän tarvetta irtautua riippuvuudestaan sekä länsimaiseen Internetin sääntelyyn, että teknologiaan. Monet venäläiset siirtyivät käyttämään kiinalaista ZTE:n ja Huawein teknologiaa yhdysvaltalaisen sijaan. (Stadnik, 2019) Venäjän turvallisuusdoktriinin kuitenkin edellyttää siirtymistä kotimaisen teknologian käyttöön. (Ministry of Foreign Affairs of the Russian Federation, 2016) Suvereenin Internetin ajatus ylipäätään on ristiriidassa kriittiseen teknologiaan ulottuvan ulkomaisen yhteistyön kanssa.

Kiinan presidentti Xi Jinping esitti lokakuussa 2017 Kiinan kommunistisen puolueen kongressissa suunnitelmansa Kiinasta kybersupervaltana. (Inkster, 2018) Kiina ei ole tyytynyt ainoastaan näyttämään mallia omissa järjestelmissään. Se on myös ympäri maailmaa järjestänyt tilaisuuksia autoritaarisille vallanpitäjille. Näissä tilaisuuksissa Kiina on teknologian lisäksi jakanut periaatteitaan ja tietojaan, jotka ainakin osin ovat ristiriidassa Internetin länsimaisen näkemyksen kanssa. (Chalk, 2019)

Yhdysvaltalaisen ajatushautomon Freedom Housen mukaan ainakin 18 maata, muun muassa Singapore, Malesia, Pakistan, Egypti, Etiopia, Saudi-Arabia ja Yhdistyneet Arabiemiraatit, on saanut Kiinalta ohjeistusta sellaisen järjestelmän luomisessa, joka pystyy tunnistamaan yleistä järjestystä uhkaavia seikkoja. Ohjeistukseen kuuluu muun muassa teema: yleisen mielipiteen ohjaaminen, jota tyypillisesti pidetään sensuurin kiertoilmaisuna. (Chalk, 2019)

Kiina on Venäjän tärkein vientimaa, mutta Venäjä on Kiinalle vasta 30.:ksi tärkein. (Statista, 2021r) Siinä, missä Venäjä monella sektorilla saattaisi tarvita yhteistyötä Kiinan kanssa vastapainona länsimaiden dominanssille, on Kiina niin suuri, että se pärjää pitkälti yksinään. Lisäksi Kiina on taitavasti rakentanut kansainvälisiä ei-sotilaallisia riippuvuussuhteita kaupan ja infrastruktuurin aloilla.

Venäläiset käyttävät paljon yhdysvaltalaisten Internet-yritysten palveluja. Olisiko mahdollista, että Venäjä myös tässä siirtyisi tekemään yhteistyötä Kiinan kanssa ja esimerkiksi sulkisi pääsyn suurilta yhdysvaltalaisilta sosiaalisen median alustaoilta? Venäläisistä lähes 90 prosenttia asuu Uralin länsipuolella. (Statista, 2021o) Venäjällä on hyvin pitkä yhteinen historia ja kulttuuri muun Euroopan kanssa. Tuntuu epätodennäköiseltä, että venäläiset voisivat siirtyä ainakaan nykyisellään käyttämään kiinalaisia sosiaalisen median alustoja länsimaisten sijaan.

Yksi hakupalvelujen, sosiaalisen median alustojen ja verkkokaupan oleellinen ominaisuus on koko. Jotta tarjotut palvelut olisivat mielenkiintoisia ja kilpailukykyisiä, tulisi alustaverkostoissa olla riittävästi käyttäjiä. Tämä ominaisuus toimii tehokkaana alalle tulon esteenä antaen ylivoimaa kansainvälisille alustoille. Hakukonepalveluissa Yhdysvallat on ylivoimainen. Helmikuussa 2021

Googlen markkinaosuus hakukoneista oli lähes 87 prosenttia, Baidun 0.54 prosenttia ja Yandex 0.38 prosenttia. (Statista, 2021e) Yhdysvaltalaiset sosiaalisen median alustat on kielletty Kiinassa, joka tältä osin on suvereeni kotimaisten palvelujensa kanssa.

Budnitsky ja Jia (2018) esittävät, että ajatus suvereenista Internetistä on myös osa Kiinan ja Venäjän maabrändiä. Nämä valtiot ovat pyrkineet rakentamaan maabrändiä yhteistyössä kotimaisten teknologiayritysten kanssa. Kiinalaiset yritykset ovat huomattavasti suurempia kuin venäläiset, minkä seurauksena niiden kansainvälinen merkitys ja näkyvyys ovat suurempia. Baidu ja muut suuret kiinalaiset teknologiayritykset ovat oleellisia konkreettisia suvereenin Internetin mahdollistajia sekä kotimaan tarpeiden että kansainvälisen kaupan tarpeiden näkökulmasta.

Internetillä on paljon muutospotentiaalia uusien teknologioiden ansiosta: 5G:n, tekoälyn, pilvilaskennan, lisääntyvän laskentatehon ja kvanttilaskennan myötä. National Security Commission on Artificial Intelligence (2021) varoittaa raportissan Kiinan tekoälyn ylivallasta. Googlen entinen toimitusjohtaja Eric Schmidt on esittänyt arvion, että Internet tulee jakautumaan kahtia 10-15 vuoden sisällä. (CNBC News, 2018) Yhdysvallat hallitsisi yhtä osaa, Kiina toista. Jakautuminen tuntuu realistiselta mahdollisuudelta. Kummankin Internetin segmentin koko on riittävä. Venäjän asema Kiinan hallitsemassa Internetissä tuskin tulisi olemaan täysin toiveiden mukainen.

7 TUTKIMUSTULOKSET

Venäjä irrotti onnistuneesti oman Internetin segmenttinsä kansainvälisestä verkosta joulukuussa 2019. (BBC News, 2019) Vaikka hetkellinen irrottaminen on nykyään teknisesti mahdollista, ei täysin suvereeni Internet ainakaan vielä tunnu realistiselta suunnitelmalta. Syitä on lukuisia niin teknisellä, loogisella kuin käyttäjätasollakin. (Taulukko 1)

TAULUKKO 1. Venäjän suvereenin Internetin projektin haasteita

	Kriittinen solmu	*Ratkaisu*	*Ratkaisun heikkous*
Tekninen taso	Riippuvuus tuontiteknologista ja komponenteista	Kotimainen tuotanto	Omassa tuotekehityksessä, osaamisessa ja standardeissa on haasteita. Tuontiteknologia on tuttua.
Looginen taso	DNS	Oma järjestelmä	Entä järjestelmään kuulumattomat maat? Vaikeus saada muut maat liittymään omaan järjestelmään.
Sosiaalinen taso	Yhdysvaltalainen sosiaalinen media	Kotimaiset vastaavat palvelut/kiinalaiset vastaavat palvelut	Sosiaalinen media vaatii suhteellisen korkean käyttäjämäärän ollakseen mielekäs. Käyttäjät ovat pääosin tottuneet länsimaiseen Internet-sisältöön ja kulttuuriin.

Teknisestä näkökulmasta Venäjältä puuttuu yksi Internetin ydinsolmuista, oma juurinimipalvelin. Hetkellisen Internetin segmentin irrottamisen aikana käytettiin ulkomaisesta juurinimipalvelimesta kopioitua tietokantaa IP-osoitteiden kyselyihin. Venäjä on puhunut oman DNS:n rakentamisesta. Konkreettisia teknisiä ratkaisuja ei ole julkisuudessa esitetty. Myös potentiaalinen käyttäjäkunta on ongelma. Internetin voima on nimenomaan sen suuressa käyttäjäkunnassa.

Venäjän Internetin segmentti on pitkälti rakennettu yhdysvaltalaisin ja kiinalaisin komponentein. Vuoden 2019 turvallisuusdoktriinin mukaan venäläisten yritysten tulee kuitenkin siirtyä kotimaisiin komponentteihin. Tavoitteeseen on vielä pitkä matka. Jo lähtökohtaisesti sellaista Internetin segmenttiä, jonka kriittinen rakenne riippuu ulkomaisista komponenteista, ei voida pitää täysin suvereenina.

Venäjän Internetin segmentti on yhteydessä kansainväliseen verkkoon vain viidestä kohdasta. Tästä näkökulmasta verkko olisi helposti irrotettavissa. Se on kuitenkin historiallisesti rakentunut osana kansainvälistä verkkoa, ja venäläiset käyttävät hyvin paljon länsimaisia palveluja. Internetin käyttäjistä 85 prosenttia käyttää Youtubea, joka myös on yhteiskunnallisesti merkittävä kommunikaatiokanava. Ulkomaisten Internet-palvelujen ja alustojen sulkeminen verkosta ei käyttäjänäkökulma huomioiden ole aivan suoraviivaista.

Venäjän rahoitusjärjestelmä on sekä fyysisesti että loogisesti itsenäinen verkko. Fyysisesti se muodostuu muun muassa Venäjän keskuspankista, pankeista ja muista rahoituslaitoksista, pörssistä, selvittelytalosta ja luottoluokituslaitoksesta. Venäjän keskuspankki on verkon tärkein solmu. Venäjä loi vuoden 2014 Ukrainan pakotteiden seurauksena oman SPFS-maksuviestijärjestelmän ja oman kansallisen maksukortin MIR-maksukorttijärjestelmän. Rahoitusjärjestelmä on täten loogisesti itsenäinen. Vaikka maksuviestijärjestelmän käyttäjäkattavuus on maan rajojen sisällä suuri, on sillä skaalautuvuusongelma. Maksujärjestelmän teho perustuu laajaan käyttäjäkuntaan, ja SWIFT-järjestelmää käytetään jo 215:ssä maassa. Kiina, jolla on jo oma CIPS-järjestelmänsä, tuskin on kiinnostunut uudesta yhteisestä järjestelmästä Venäjän kanssa. Kansainvälinen kauppa tuo omat haasteensa suvereenin Internetin projektiin. (taulukko 2)

TAULUKKO 2. Venäjän talous- ja rahoitusjärjestelmän haasteita, joita suvereeni Internet todennäköisesti kasvattaisi entisestään

	Kriittinen solmu	*Ratkaisu*	*Ratkaisun heikkous*
Rahoitusjärjestelmä	SWIFT-maksuviestijärjestelmä	Oma järjestelmä	Entä järjestelmään kuulumattomat maat? Vaikeus saada muut maat liittymään omaan järjestelmään.
Kansainvälinen kauppa	Öljyn ja kaasun vienti, elintarvikkeiden ja teknologian tuonti	Talouden monipuolistaminen vientiriippuvuuden vähentämiseksi. Elintarvike- ja teknologiaomavaraisuus	Pitkäjänteisiä projekteja, tuskin pystytään kokonaan irtautumaan vienti- ja tuontiriippuvuudesta
Investoinnit	Portfolioinvestoinnit ulkomaille, suorat investoinnit Venäjälle	Ulosmenevän rahavirran vähentäminen tekemällä kotimaiset sijoitukset houkuttelevimmiksi. Kotimaisen suorien investointien ympäristön kehittäminen	Pitkäjänteisiä projekteja, olosuhteiden parantaminen on hyvin kokonaisvaltaista

Kiina on onnistunut yhdistämään suvereenin Internetin ja nopeasti kasvavan maailman toiseksi suurimman talouden. Kiinan ja Venäjän suhtautumisessa

Internetiin on paljon samankaltaisuuksia. Kumpikin maa näkee, että Internetin maa-alueen segmentti on alisteinen isäntämaalle.

Venäjä voisi hakea tiivistä yhteistyötä Kiinan kanssa. Venäjän ja Kiinan Internetin segmentit ja niiden käyttö eroavat kuitenkin monessa suhteessa. Kiinan Internetin segmentti on suvereeni niin teknisesti, loogisesti kuin käyttäjätasollakin. Sitä voitaisiin oikeastaan kuvailla maan sisäiseksi intranetiksi, jota hallitusti muun muassa kaupallisten tarpeiden mukaan voidaan avata. Venäjän Internetin segmenttiä kehitettiin aluksi vapaassa kansainvälisessä ilmapiirissä. Vaikka se teknisellä ja loogisella tasolla ainakin hetkellisesti voisi toimia itsenäisesti, sen käyttäjät ovat tottuneet myös länsimaisen verkon palveluihin ja sisällöntarjoajiin.

Huolimatta laajasta kansainvälisestä kaupasta on Kiina talouden näkökulmasta suvereeni. Se on avannut talouttaan hallitusti, ja sillä on oma täysin suvereenisti toimiva rahoitusjärjestelmä. Maa on määrätietoisesti hankkinut taloudellista valtaa sekä kauppasuhtein että kansainvälisten infrastruktuurihankkeidensa avulla. Venäjä puolestaan on sulkemassa talouttaan ja kehittämässä omavaraisuuttaan. Öljynvienti on kuitenkin Venäjän kaikkein tärkein tulonlähde. Venäjä pyrkii sulkemaan talouttaan, mutta sen tekeminen hallitusti ja toimivasti on haastavaa, ellei peräti mahdotonta.

Venäjä on pystynyt irrottamaan oman Internetin segmenttinsä kansainvälisestä verkosta, ja sillä on oma ainakin teoriassa toimiva rahoitusjärjestelmänsä. Onko sellainen realistinen uhka olemassa, että Venäjä esimerkiksi kyberhyökkäyksin lamauttaisi kansainvälisen rahoitusjärjestelmän, suojaten samalla oman rahoitusjärjestelmänsä? Tuntuu erittäin epätodennäköiseltä, että tällainen olisi mahdollista. Entä Kiina, jolla on suvereeni Internet ja suvereeni rahoitusjärjestelmä? Kiinalla on maailman suurin valuuttareservi, josta ainakin vuonna 2014 lähes puolet oli dollareissa. Dollarin arvo romahtaisi suuressa kansainvälisen rahoitusjärjestelmän kriisissä, mikä suoraan heijastuisi Kiinan valuuttareservin arvoon.

8 JOHTOPÄÄTÖKSET

Tutkimuksen tavoitteena oli selvittää, mitä edellytyksiä Venäjän kaltaisella kansainvälisellä taloudella kansainvälisine rahoitusjärjestelmineen on sulkea Internetin segmenttinsä. Tutkimuksessa lähdettiin Internetin kahdesta narratiivista, avoimesta Internetistä ja suvereenista Internetistä. Sekä Internetiä että talous- ja rahoitusjärjestelmiä tutkittiin verkostoja ja dynaamisia systeemejä mallintavan verkkoteorian avulla, pyrkien tunnistamaan kunkin järjestelmän tärkeimpiä solmukohtia. Tämän jälkeen todettiin, että solmukohdan haltijalla on tietty valta avoimessa verkostossa ja tutkittiin, miten valta-asema heijastuu koko verkkoon.

Yhdysvalloilla on Internetin toiminnan kannalta kriittisten juurinimipalvelijoiden kautta merkittävä asema Internetissä. Venäjä on esittänyt riskin, että Yhdysvallat voisi tätä kautta estää liikenteen kaikkiin .ru-päätteisiin osoitteisiin. Kansainvälisessä maksujärjestelmässä Yhdysvalloilla puolestaan on merkittävä valta SWIFT-maksuviestijärjestelmän kautta. SWIFT-maksuviestijärjestelmän kautta Venäjän rahoitusjärjestelmää olisi mahdollista huomattavassa määrin häiritä, ellei jopa on lamauttaa.

Venäjän on vastannut sekä Internetin että rahoitusjärjestelmän kansainväliseen valta-asetelmaan pyrkimällä rakentamaan itselleen suvereenin Internetin segmentin ja suvereenin rahoitusjärjestelmän. Teknisesti kummankin toteuttaminen lienee mahdollista. Venäjä todennäköisesti pystyisi rakentamaan oman juuripalvelujärjestelmän; oma SPFS-maksuviestijärjestelmä ja oma kansallinen MIR-maksukortti sillä jo on.

Se, mikä toimii teknisesti, ei välttämättä ole käytännössä toteuttamiskelpoista ja toimivaa globaalissa keskinäisriippuvassa maailmassa, jossa yhtäältä valtiollisten toimijoiden keskinäiset suhteet ja toisaalta valtiollisten ja yksityisten toimijoiden väliset suhteet ovat entistä monimutkaisempia. Samalla myös eri toimintasektoreiden väliset rajapinnat ovat muuttuneet entistä moniulotteisemmiksi ja häilyvämmiksi. Venäjä on riippuvainen kansainvälisestä kaupasta. Sekä juuripalvelujärjestelmä että maksuviestijärjestelmä toimivat järkevästi vain, mikäli niillä on riittävästi käyttäjiä. Myös Internetin voima kaikkine palveluineen ja alustoineen on sen globaaliudessa ja suuressa käyttäjämäärässä.

Venäjän tavoin Kiina katsoo, että Internetin segmentti on alisteinen isäntämaalle. Myös Kiina on reagoinut Yhdysvaltain dominanssiin niin Internetin kuin rahoitusjärjestelmänkin hallinnassa. Sillä on oma suvereenisti toimiva Internet ja rahoitusjärjestelmänsä. Toisin kuin Venäjällä, käyttäjämäärät 11 kertaa suuremmassa taloudessa ovat riittävät.

Internetin käyttäjämäärien lisäksi Venäjä ja Kiina eroavat toisistaan merkittävässä suhteessa. Venäjä pyrkii suojautumaan sulkemalla itsensä. Samalla se väistämättä vähentää myös kansainvälistä painoarvoaan ja heikentää neuvotteluasemaansa. Sulkeutuvasta Venäjästä poiketen Kiina on vastannut Yhdysvaltain ja lännen dominanssiin avaamalla hallitusti Internetiään ja talous- ja rahajärjestelmiään sekä pyrkimällä olemaan painoarvoltaan merkittävä, suvereeni jäsen kansainvälisissä verkostoissa. Kiina on sekä sisäisesti että ulkosuhteissaan raken-

tanut kumpaakin osapuolta hyödyttävää yhteistyötä. Omat kansalaiset on sitoutettu kansallisella pistejärjestelmällä ja kotimaisilla sosiaalisen median alustoilla, ulkovallat erityisesti tärkeillä kauppasuhteilla.

Kari (2019c) liittää Venäjän suvereenin Internetin projektin piiritetyn linnakkeen narratiiviin. Venäjä pyrkii hallitsemaan ja suojaamaan informaatioavaruutensa sulkemalla Internetin segmenttinsä. Syyt piiritetyn linnakkeen narratiiviin löytyvät historiasta, maantieteestä ja teknologian jälkeenjääneisyydestä. Piiritetyn linnakkeen narratiivi ja suvereeni Internet eivät ole erityisen toimiva ratkaisu Venäjän kaltaiselle kansainväliselle taloudelle.

Kukkola (2020) esittää ajatuksen, että suvereeni Internetin projekti on luonnollinen jatkumo Venäjän kehityskululle ja valtiovallan tekemille valinnoille. Tämä valinta joutuu haastetuksi, mikäli Venäjän tilannetta tarkastellaan laajemmin myös talouden näkökulmasta. Kun verrataan Venäjää Kiinaan, voidaan todeta Kiinan valtiovallan valinneen suvereenin Internetin projektille strategian, joka pyrkii yhtäältä ottamaan huomioon talouden ja kaupan tarpeet ja toisaalta entistä paremmin sitomaan Kiinan ja ulkovallat toisiinsa keskinäisen monimuotoisen yhteistyön avulla.

Tämän tutkimuksen tulokset ovat sovellettavissa myös strategisen autonomian ajankohtaisiin kysymyksiin. Tutkimuksessa kartoitettiin suvereenin Internetin projektin kannalta merkityksellisiä valta-asetelmia ja tekijöitä ja todettiin Yhdysvaltojen ja Kiinan dominoivan kenttää. Mitä edellytyksiä muilla valtioilla on rakentaa strategisesti kriittisiä tietojärjestelmiään, kun komponentit, kriittiset ohjelmistot, alustat ja muu teknologia tulevat kahdelta suurvallalta? Entä miten tilanne vaikuttaa huoltovarmuuteen siltä osin kuin kyse on kriittisestä infrastruktuurista? Myös kyberturvallisuus on olennainen tekijä.

Tutkimus kartoitti suvereenin Internetin kenttää varsin yleisellä tasolla. Sitä voisi jatkaa ja syventää valitsemalla erilaisia esille tulleita tekijöitä tarkemman analyysin kohteiksi. Lisäksi esimerkiksi kysymystä digitaalisesta riippumattomuudesta voisi laajentaa muihin sektoreihin ja infrastruktuureihin. Hedelmällistä olisi myös tarkemmin vertailla Kiinan avautumiseen ja Venäjän sulkeutumiseen liittyviä strategioita.

LÄHTEET

ACRA (2021). Analytical credit rating agency. Effective May 14, 2021. http://www.eacra.fr/?q=node/516.

Allen, F., & Babus, A. (2009). Networks in finance. In Kleindorfer, P. R., Wind, Y. R., & Gunther, R. E. (eds.). *The Network Challenge: Strategy, Profit, and Risk in an Interlinked World,* pp. 367-382.

Amos, H. (2015). What would exclusion from payment system SWIFT mean for Russia? *The Moscow Times*, 28.1.2015. Effective May 14, 2021. https://www.themoscowtimes.com/2015/01/28/what-would-exclusion-from-payment-system-swift-mean-for-russia-a43345.

Arsène, S. (2015). Internet domain names in China. articulating local control with global connectivity. *China Perspectives*, (4), pp. 25-34.

Asada, T., Chiarella, C., Flaschel, P., & Franke, R. (2012). *Open economy macrodynamics: an integrated disequilibrium approach*. Springer Science & Business Media.

Bank of Russia (2003). Russian Payment System. Effective May 14, 2021. ld.cbr.ru/Queries/XsltBlock/File/21579?fileId=9092.

Bank of Russia (2021). The Bank of Russia Payment System (BRPS). Effective May 14, 2021. https://cbr.ru/Content/Document/File/16999/psys.pdf.

Bank of Russia (2021a). Financial messaging system of the Bank of Russia (SPFS). Effective May 14, 2021. https://www.cbr.ru/eng/Psystem/fin_msg_transfer_system/.

Bank of Russia (2021b). Payment systems. Effective May 14, 2021. https://cbr.ru/eng/psystem/.

Bank of Russia (2021c). Banking sector. Effective May 14, 2021. https://cbr.ru/eng/banking_sector/.

BBC News (2019). Russia 'successfully tests' its unplugged internet. Effective May 14, 2021. https://www.bbc.com/news/technology-50902496.

Becker, M. (2019). When public principals give up control over private agents: the new independence of ICANN in internet governance. *Regulation & Governance*, 13(4), pp. 561-576.

Brandes, U. (2005). *Network analysis: methodological foundations* (Vol. 3418). Springer Science & Business Media.

Britannica (2021a). Reliability. Effective May 14, 2021. https://www.britannica.com/topic/reliability-measurement-in-social-science.

Britannica (2021b). Primary characteristics of methods or instruments. Effective May 14, 2021. https://www.britannica.com/science/psychological-testing/Primary-characteristics-of-methods-or-instruments.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), pp. 594-613.

CNBC News (2018). Former Google CEO predicts the internet will split in two — and one part will be led by China. 21.9.2018. Effective May 14, 2021. https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

Chakrabarti, A. S., Pichl, L., & Kaizoji, T. (2019). Complexity and emergence: a new paradigm for economic modeling. In *Network Theory and Agent-Based Modeling in Economics and Finance,* pp. 1-8. Springer, Singapore.

Chalk, W. (2019). China's digital imperialism: Shaping the global Internet. *SupChina*, 2.6.2019. Effective May 14, 2021. https://supchina.com/2019/07/02/chinas-digital-imperialism-shaping-the-global-internet/.

Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019). The Golden Shield project of China: A decade later—an in-depth study of the Great Firewall. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC),* pp. 111-119. IEEE Computer Society.

Clark, M. P. (2003). *Data Networks, IP and the Internet*. West Sussex, England: John Wiley & Sons Ltd.

Davies, K. (2013). China investment policy: An update. *OECD Working Papers on International Investment.* Effective May 14, 2021. https://www.oecd-ilibrary.org/finance-and-investment/china-investment-policy_5k469l1hmvbt-en.

Deloitte (2016). The economic impact of disruptions to internet connectivity a report for Facebook. October 2016. Effective May 10, 2021. https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

D'Jaen, M. D. (2007). Breaching the Great Firewall of China: congress overreaches in attacking Chinese internet censorship. *Seattle University Law Review*, 31, pp. 327-351.

Dicken, P., Kelly, P. , Olds, K. & Wai-Chung Yeung, H. (2001). Chains and networks, territories and scales: towards a relational framework for analysing the global economy. *Global networks*, *1*(2), pp. 89-112.

Domańska, M. (2019). Gagging Runet, silencing society. 'Sovereign' Internet in the Kremlin's political strategy. Ośrodek Studiów Wschodnich im. Marka Karpia. Effective May 14, 2021. https://www.ceeol.com/search/gray-literature-detail?id=834789.

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). Internet fragmentation: an overview. World Economic Forum. Effective May 14, 2021. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dreyer, I., & Popescu, N. (2014). Do sanctions against Russia work?. *European Union Institute for Security Studies* (EUISS).

ECB (2021). European Central Bank Eurosystem, Executive Summary. Effective May 14, 2021. https://www.ecb.europa.eu/pub/pubbydate/2019/html/ecb.cardpaymentsineu_currentlandscapeandfutureprospects201904~30d4de2fc4.en.html.

ECOFIN (2019). Resilience of financial market infrastructure and the role of the financial sector in countering hybrid threats. *EU2019.FI*, 9.9.2019. Effective May 14, 2021. https://eu2019.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf.

EIA (2017). Russia, overview. U.S. Energy Information Administration. Effective May 14, 2021. https://www.or.gov/international/analysis/country/RUS.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), pp. 532-550.

Enisa (2016). DDos on DNS Root Servers. Effective May 14, 2021. https://www.enisa.europa.eu/publications/info-notes/ddos-on-dns-root-servers.

Epifanova, A. (2020). Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet. *DGAP Analysis*, Vol. 2. Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.

EU (2020). Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle. EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle. *Euroopan komissio, JOIN (2020) 18 FINAL.* Aktiivinen 14. toukokuuta, 2021. *https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52020JC0018&from=EN*

Freedom House (2021). Countries. Effective May 14, 2021. https://freedomhouse.org/countries/freedom-net/scores.

Freedom House (2018). Freedom on the net 2018. The Rise of Digital Authoritarianism. 10.2018. Effective May 14, 2021. https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf.

Gabuev, A. (2015). How China and Russia see the Internet. *World Economic Forum***.** 16.12.2015**.** Effective May 14, 2021. https://www.weforum.org/agenda/2015/12/how-china-and-russia-see-the-internet/.

Gazeta.ru (2021). Gazeta.ru. Effective May 14, 2021. https://www.crunchbase.com/organization/gazeta-ru.

Gilmore, J. & Henry, M. (2021). The rise of cyber sovereignty: Russia, China, and the future of internet governance. *Young Professionals in Foreign Policy*. Effective May 14, 2021. https://www.ypfp.org/the-rise-of-cyber-sovereignty-russia-china-and-the-future-of-internet-governance/ .

Glonass (2021). Information and analysis center for positioning, navigation and timing. Effective May 14, 2021. https://www.glonass-iac.ru/en/.

GNI (2018). The consequences of network shutdowns and service disruptions: a one-page guide for policymakers. *Global Network Initiative*. Effective May 14, 2021. https://globalnetworkinitiative.org/wp-content/uploads/2018/04/Impacts-Disruptions-EN.pdf.

GNI (2018b). Weighing the Impact of Network Shutdowns and Service Restrictions. Effective May 14, 2021. https://globalnetworkinitiative.org/the-consequences-of-network-shutdowns-and-service-disruptions-a-one-page-guide-for-policymakers/.

De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), pp. 214-230.

Griffiths, J. (2019). *The great firewall of China: How to build and control an alternative version of the internet*. Zed Books Ltd.

Guba, E. & Lincoln, Y.S. (1994), Competing paradigms in qualitative research. In Denzin, N.K. and Lincoln, Y.S. (eds), *Handbook of Qualitative Research*, Sage, Thousand Oaks, CA, pp. 105-17.

Hansen, D., Shneiderman, B., & Smith, M. A. (2010). *Analyzing social media networks with NodeXL: Insights from a connected world*. Morgan Kaufmann.

Huan, G. (1986). China's open door policy, 1978-1984. *Journal of International Affairs,* 39(2), pp. 1-18.

IANA (2021a). IANA. Effective May 14, 2021. https://www.iana.org.

IANA (2021b). Internet Assigned Numbers Authority. Root Servers. Effective May 12, 2021. https://www.iana.org/domains/root/servers.

ICANN (2021). Technology@ICANN. Effective May 14, 2021. https://www.icann.org/technology.

IMF (2021). World economic outlook. Managing different discoveries. *International Monetary Fund*, April 2021. Effective May 14, 2021. https://www.imf.org/en/Publications/WEO/Issues/2021/03/23/world-economic-outlook-april-2021.

Inkster, N. (2018). *China's cyber power*. Routledge.

International political economical zone (2015). Nuclear option: UK says kick Russia out of SWIFT. Effective May 14, 2021. http://ipezone.blogspot.com/2015/02/nuclear-option-uk-says-kick-russia-out.html.

Interfax (2021). Медведев заявил о технической готовности РФ к отключению от глобальной сети. Effective May 14, 2021. https://www.interfax.ru/russia/748771.

Journal of Network Theory in Finance (2021). Effective May 14, 2021. https://www.risk.net/journal-of-network-theory-in-finance.

JP 3-12 (2018). *Cyberspace Operations*. Joint Publication JP3-12, June 2018. Effective May 14, 2021. https://fas.org/irp/doddir/dod/jp3_12.pdf.

Kari, M. and Kuusisto, R. (2017). Russia: A Cyber Fortress Besieged. *The 16th European Conference on Cyber Warfare and Security*. Dublin, Ireland. pp. 29–30 June 2017.

Kari, M. (2018a). The Concept of the Critical Information Infrastructure of the Russian Federation. *The 13th International Conference on Cyber Warfare and Security.* Washington DC, USA. 8–9 March 2018.

Kari, M. (2018b). The Protection of Russia's Critical Information Infrastructure. *The 17th European Conference on Cyber Warfare and Security*. Oslo, Norway. 28–29 June 2018.
Kari, M. (2019a). Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception. *The 14th International Conference on Cyber Warfare and Security*. 28 February–1 March 2019, Stellenbosch, South Africa.
Kari, M. (2019b). Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats. *The 18th European Conference on Cyber Warfare and Security*. 4–5 July 2019, University of Coimbra, Portugal. pp. 685-691.
Kari, M. (2019c). *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture–a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats.* 2019. JYU väitöskirjat.
Kari, M. & Pynnöniemi, K. (2019). Theory of strategic culture: An analytical framework for Russian cyber threat perception. *Journal of Strategic Studies*, pp. 1-29.
Kirman, A. (1997). The economy as an evolving network. *Journal of Evolutionary Economics*, 7(4), pp. 339-353.
Kivelä, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y., & Porter, M. A. (2014). Multilayer networks. *Journal of Complex Networks*, 2(3), pp. 203-271.
Kukkola, J. (2018). Civilian and military information infrastructure and the control of the Russian segment of Internet. In *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. pp. 1-8. IEEE.
Kukkola, J. & Ristolainen, M. (2018). Projected Territoriality. *Journal of Information Warfare*, *17*(2), pp. 83-100.
Kukkola, J. (2019). The Russian Segment of the Internet as a Resilient Battlefield. *GAME PLAYER Facing the Structural Transformation of Cyberspace*, 117. Riihimäki, Finnish Defence Research Agency.
Kukkola, J. (2020). Digital Soviet Union: the Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas. *Series 1: Research Publications No. 40*. National Defence University.
Lamensch, M. (2021). The Cost of an Internet Shutdown. *CIGI2021*. Effective May 14, 2021. https://www.cigionline.org/articles/cost-internet-shutdown.
Larson, D. W., & Shevchenko, A. (2010). Status seekers: Chinese and Russian responses to US primacy. *International Security*, *34*(4), pp. 63-95.
Liefert, W. M. & Liefert, O. (2020). Russian agricultural trade and world markets. *Russian Journal of Economics*, 6, pp. 56-70.
Lukin, A. (2020). The Russia–China entente and its future. *International Politics*, pp. 1-18.
Mac Sithigh, D. & Siems, M. (2019). The Chinese social credit system: A model for other countries?. *The Modern Law Review*, *82*(6), 1034-1071.
Mail.ru (2021). Our Story. Effective May 14, 2021. https://corp.mail.ru/en/company/timeline/.
Mann, J. (2009). Russia's Policy towards OPEC. *Middle Eastern Studies*, 45(6), pp. 985-1005.

Maswana, J. C. (2011). China's financial development and economic growth: exploring the contradictions. *Journal of Chinese Economics and Finance*, *3*, pp. 15-27.

Maslov, S., Sneppen, K., & Zaliznyak, A. (2004). Detection of topological patterns in complex networks: correlation profile of the Internet. *Physica A: Statistical Mechanics and its Applications*, 333, pp. 529-540.

Mengü, M., & Mengü, S. (2015). Violence and social media. *Athens Journal of Mass Media and Communications,* 1(3), pp. 211-227.

Ministry of Digital Development, Communications and Mass Media of Russian Federation (2014). Ministry of Telecom and Mass Communications, the Federal Security Service and Ministry of Defense have conducted training on protection of the Russian segment of the Internet. *Press release*, 28.7.2014. https://digital.gov.ru/en/events/31441/.

Ministry of Foreign Affairs of the Russian Federation (2016). Doctrine of Information Security of the Russian Federation. Effective May 14, 2021. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

Mir, R. and Watson, A. (2000), Strategic management and the philosophy of science: the case for a constructivist methodology. *Strategic Management Journal*, 21(9), pp. 941-53.

Monge, P. R., Contractor, N. S., Contractor, P. S., Peter, R. & Noshir, S. (2003). *Theories of communication networks*. Oxford University Press, USA.

Moscow Exchange (2021). Welcome to Moscow exchange. Effective May 14, 2021. https://www.moex.com/s348.

Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. London: Polity.

De Nardis, L. (2016). One Internet: an evidentiary basis for policy making on internet universality and fragmentation. *Chatham House. The Royal Institute of International Affairs*.

National Clearing Centre (2021). National Clearing Centre. Effective May 14.2021. https://www.nationalclearingcentre.com/catalog/.

National Clearing Centre (2021a). The Moscow Exchange Group established the central Clearing House. *Press release*, 3.12.2012. Effective May 14.2021. https://www.moex.com/n2108.

National Security Commission on Artificial Intelligence (2021). Final report. *National Security Commission on Artificial Intelligence.* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

NCCCI (2021). National Coordination Center for Computer Incidents. About cert.gov.ru. Effective May 14.2021. http://gov-cert.ru/en/index.html.

Negro, G. (2017). *The Internet in China. From Infrastructure to a nascent Civil Society*. Palgrave Macmillan, Cham.

Newman, M. (2010). *Networks: An introduction*. New York, NY: Oxford University Press.

Nikkarila, J. P., Åkesson, B., Kuikka, V., & Hämäläinen, J. (2018). Modelling Closed National Networks: Effects in Cyber Operation Capabilities.

In *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2*. Academic Conferences and publishing limited.
Nocetti, J. (2011). Digital Kremlin": power and the internet in Russia. *Russie. Nei. Visions*, *59*.
Nocetti, J. (2015). Contest and conquest: Russia and global Internet governance. *International Affairs*, 91(1), pp. 111-130.
Odnoklassniki (2021). Odnosklassniki. Effective May 14, 2021. https://www.crunchbase.com/organization/odnoklassniki.
O'hara, K., & Hall, W. (2018). Four Internets: the geopolitics of digital governance (CIGI Papers, 206). *The Centre for International Governance Innovation (CIGI)/*Chatham House.
Oh, P. & Monge, P. (2016). *Network Theory and Models*. Wiley Online Library. Effective May 14, 2021. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118766804.wbiect246.
Pastor-Satorras, R., & Vespignani, A. (2007). *Evolution and structure of the Internet: A statistical physics approach*. Cambridge University Press.
Paypers (2021). Cross-border e-commerce in Russia – facts and figures. Effective May 14, 2021. https://thepaypers.com/expert-opinion/cross-border-ecommerce-in-russia-facts-and-figures--1247231.
Plaksin S., Abdrakhmanova G., Kovaleva G. (2016). Approaches to Defining and Measuring Russia's Internet Economy. *Foresight and STI Governance*, 10(4), pp. 7–24.
Polyakova, A. & Meserole, C. (2019). Exporting Digital Authoritarianism: The Russian and Chinese Models. *Policy Brief, Democracy and Disorder Series*. Washington, DC: Brookings, pp. 1-22.
Powers, S. M., & Jablonski, M. (2015). *Real Cyber War*. Urbana/Springfield: University of Illinois Press.
Press, L. (1991). A computer network for democracy and development. Effective May 14, 2021. http://www.ibiblio.org/pub/docs/about-the-net/Usenet/soviet.coup.
Pursiainen, C. (2020). Russia's Critical Infrastructure Policy: What do we Know About it?. *European Journal for Security Research*, pp. 1-18.
Pynnoniemi, K. & Kari, M. (2016). Russia's New Information Security Doctrine. *FIIA 26/2016 Comment*. The Finnish Institute of International Affairs. Effective May 14, 2021. https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf.
Pönkä, H., & Zheng, Y. (2019). The role of oil prices on the Russian business cycle. *Research in International Business and Finance*, 50, pp. 70-78.
Ragin, C. (2014). *The comparative method: Moving beyond qualitative and quantitative strategies*. University of California Press.
Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., ... & Ensafi, R. (2020). Decentralized control: A case study of Russia. In *Network and Distributed Systems Security (NDSS) Symposium 2020*. Effective May 14, 2021. https://par.nsf.gov/servlets/purl/10142204.

Rapoza, K. (2015). Russia To Retaliate If Bank's Given SWIFT Kick. *Forbes*, 27.1.2015. Effective May 14, 2021. https://www.forbes.com/sites/kenrapoza/2015/01/27/russia-to-retaliate-if-banks-given-swift-kick/?sh=3f69f4fc652e.

Riege, A. M. (2003). Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative Market Research: An International Journal*.

Ristolainen, M. (2017). Should 'Runet 2020' be taken seriously? contradictory views about cyber security between Russia and the west. *Journal of Information Warfare*, *16*(4), pp. 113-131.

Russian Federation (2017). Program Digital Economy of the Russian Federation. Order of the Government of the Russian Federation No. 1632-r, July 28, 2017, No. 1632-r. Effective May 14, 2021. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.

Roberts, M. E. (2018). *Censored: distraction and diversion inside China's Great Firewall*. Princeton University Press.

RT news (2019). Russia, China & India to set up alternative to SWIFT payment system to connect 3 billion people. 28.10.2019. Effective May 14, 2021. https://www.rt.com/business/472016-russia-india-china-swift/.

Securityalliance (2018). Digital sovereignty in the age of connectivity: RuNet 2020. 5.6.2018. Effective May 14, 2021. https://www.secalliance.com/blog/runet-2020.

Seddon, M. & Foy, H. (2019). The big red Russia. Russian technology: Can the Kremlin control the Internet? *Financial Times*, 5.6.2019. https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2.

Segal, A. (2018). When China rules the web: technology in service of the state. *Foreign Affairs*, 97, pp. 10-18.

Shen, H. (2016). China and global Internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, 9(3), pp. 304-324.

Siukonen, V., Ristolainen, M., Nikkarila, J. P., & Kukkola, J. (2019). Are We There Yet?: Monitoring the Technical Deployment of the National Segments of the Internet. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. pp. 1-5. IEEE.

Snyder, J., Komaitis, K., & Robachevsky, A. (2017). The History of IANA: An Extended Timeline with Citations. *Internet Society, 2017.* Effective May 14, 2021. https://www.internetsociety.org/wp-content/uploads/2016/05/IANA_Timeline_20170117.pdf.

Soldatov, A. & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal*, *30*(3), pp. 23-30.

Soldatov, A. & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries*. Hachette UK.

Soldatov, A. & Borogan, I. (2015b). RusNet on the Offensive. *World Policy Journal*, *32*(3), pp. 102-110.

Stadnik, I. (2019). Internet Governance in Russia–Sovereign Basics for Independent Runet. *Working paper.* Saint-Petersburg State University.

Effective May 14, 2021. https://www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/.
Statista (2020a). Continental Shift: The World's Biggest Economies Over Time. https://www.statista.com/chart/22256/biggest-economies-in-the-world-timeline/.
Statista (2020b). AliBaba. China's Amazon Is Not Quite Amazon Yet. Effective May 14, 2021. https://www.statista.com/chart/13759/alibaba-vs-amazon/.
Statista (2021a). Average Daily Time Spent on the Internet by Russians by Device. Effective May 14, 2021. https://www.statista.com/statistics/1076600/average-daily-time-spent-on-the-internet-by-russians-by-device/.
Statista (2021b). Average Online Time of Users in China. Effective May 14, 2021. https://www.statista.com/statistics/265176/average-online-time-of-users-in-china/.
Statista (2021c). Forecast of Internet users' volume in Russia from 2015 to 2025. Effective May 14, 2021. https://www.statista.com/statistics/567007/predicted-number-of-internet-users-in-russia/.
Statista (2021d). Global Internet penetration rate as of January 2021, by region. Effective May 14, 2021. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/.
Statista (2021e). Global market share of search engines 2010-2021. Effective May 14, 2021. https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.
Statista (2021f). Global Societal Networks Ranked by Number of Users. Effective May 14, 2021. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
Statista (2021g). Gross Domestic Product GDP in Russia. Effective May 14, 2021. https://www.statista.com/statistics/263772/gross-domestic-product-gdp-in-russia/.
Statista (2021h). Gross Domestic Product GDP of China. Effective May 14, 2021. https://www.statista.com/statistics/263770/gross-domestic-product-gdp-of-china/.
Statista (2021i). India: Gross domestic product (GDP) in current prices from 1986 to 2026. Effective May 14, 2021. https://www.statista.com/statistics/263771/gross-domestic-product-gdp-in-india/.
Statista (2021j). Irak: Gross domestic product (GDP) in current prices from 1986 to 2026. Effective May 14, 2021. https://www.statista.com/statistics/326979/gross-domestic-product-gdp-in-iraq/.

Statista (2021k). Leading Social Network Sites in China. Effective May 14, 2021. https://www.statista.com/statistics/250546/leading-social-network-sites-in-china/.
Statista (2021l). Most used currencies in payments worldwide in 2020. Effective May 14, 2021. https://www.statista.com/statistics/1189498/share-of-global-payments-by-currency/.
Statista (2021m). Number of Internet Users in China. Effective May 14, 2021. https://www.statista.com/statistics/265140/number-of-internet-users-in-china/.
Statista (2021n). Payment Card Transactions Worldwide by Brand. Effective May 14, 2021. https://www.statista.com/statistics/762717/payment-card-transactions-worldwide-by-brand/.
Statista (2021o). Population size in Russia as of January 1, 2021, by federal district. Effective May 14, 2021. https://www.statista.com/statistics/1009384/population-size-in-russia-by-federal-district/.
Statista (2021p). Russia Annual Crude Oil Exports. Effective May 14, 2021. https://www.statista.com/statistics/1023747/russia-annual-crude-oil-exports/.
Statista (2021q). Russia Energy Contribution to GDP by Scenario. Effective May 14, 2021. https://www-statista-com.libproxy.aalto.fi/statistics/1079846/russia-energy-contribution-to-gdp-by-scenario/.
Statista (2021r). Russian Export Share by Destination and Product Category. Effective May 14, 2021. https://www-statista-com.libproxy.aalto.fi/statistics/1049165/russia-export-share-by-destination-and-product-category/.
Statista (2021s). Russia Foodstuffs and Agricultural Imports. Effective May 14, 2021. https://www.statista.com/statistics/1006520/russia-foodstuffs-and-agricultural-imports/.
Statista (2021t). Russian Nominal GDP. Effective May 14, 2021. https://www-statista-com.libproxy.aalto.fi/statistics/1055726/russia-nominal-gdp/.
Statista (2021u). Share of Global Crude Oli Production of the top 15 Oil Producing Countries. Effective May 14, 2021. https://www.statista.com/statistics/236605/share-of-global-crude-oil-production-of-the-top-15-oil-producing-countries/.
Statista (2021v). Share of Russian Gas Imports EU. Effective May 14, 2021. https://www.statista.com/statistics/1021735/share-russian-gas-imports-eu/.
Statista (2021x). Top Active Social Media Platforms in Russia. Effective May 14, 2021. https://www.statista.com/statistics/867549/top-active-social-media-platforms-in-russia/.
Statista (2021y). Total population of China 1980-2026. Effective May 14, 2021. https://www.statista.com/statistics/263765/total-population-of-china/.

Statista (2021z). UK Brent Crude Oil Price Changes Since 1976. Effective May 14, 2021. https://www.statista.com/statistics/262860/uk-brent-crude-oil-price-changes-since-1976/.
Stuenkel, O. (2015). Why China would benefit from Western SWIFT sanctions against Russia. 10.3.2015. Effective May 14, 2021. https://www.oliverstuenkel.com/2015/03/10/benefit-western-sanctions-against/.
Suomen Pankki (2019). Dollari on edelleen yleisin laskutusvaluutta Venäjän ulkomaankaupassa. Aktiivinen linkki 14.5.2021. https://www.bofit.fi/en/monitoring/weekly/2019/vw201920_2/.
Suomen Pankki (2021a). Kuvaus. Aktiivinen linkki 14.5.2021. https://www.suomenpankki.fi/fi/Tilastot/maksutase-ja-rahoitustilinpito/kuvaus/.
Suomen Pankki (2021b). Raha ja maksaminen. Aktiivinen linkki 14.5.2021. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/.
Suomen Pankki (2021c). Rahoitusjärjestelmä. Aktiivinen linkki 14.5.2021. https://www.suomenpankki.fi/fi/rahoitusvakaus/rahoitusjarjestelma-lyhyesti/.
SWIFT (2021a). SWIFT. Effective May 14.2021. https://www.swift.com.
SWIFT (2021b). Organization and Governance. Effective May 14, 2021. https://www.swift.com/about-us/organisation-governance.
SWIFT (2021c). Compliances. Swift and Sanctions. Effective May 14, 2021. https://www.swift.com/about-us/legal/compliance-0/swift-and-sanctions.
Tan, Z., Foster, W., & Goodman, S. 1999. China's State-Coordinated Internet Infrastructure. *Communications of the ACM*, 42(6), pp. 44-52.
Tselikov, A. (2014). The Tightening Web of Russian Internet Regulation. *Berkman Center Research Publication*, 2014-15.
Turvallisuuskomitea (2018). *Kyberturvallisuuden sanasto*. Huoltovarmuuskeskus. TSK 52.
Tyll, L., Pernica, K., & Arltová, M. (2018). The impact of economic sanctions on Russian economy and the RUB/USD exchange rate. *Journal of International Studies*, *11*(1).
Ugander, J., Karrer, B., Backstrom, L., & Marlow, C. (2011). The anatomy of the Facebook social graph. *Working paper.* Effective May 14, 2021. https://arxiv.org/abs/1111.4503.
Verbovszky, J. (2018). Networked geopolitics. The American academy in Berlin. Effective May 14, 2021. https://www.americanacademy.de/networked-geopolitics/.
Vernikov, A. V. (2015). Comparing the banking models in China and Russia: Revisited. *Studies on Russian economic development*, *26*(2), 178-187.
VK (2021). About us. Effective May 14, 2021. https://vk.com/about.
Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. New York, NY: Cambridge University Press.
World bank (2021a). GDP (current USD) – Russian Federation, China. Effective May 14, 2021.

https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=RU-CN.

World bank (2021b). Portfolio equity, net inflows (BoP, current USD) – Russian Federation. Effective May 14, 2021. https://data.worldbank.org/indicator/BX.PEF.TOTL.CD.WD?end=2019&locations=RU&start=1994.

World bank (2021c). Trade (% of GDP). Effective May 14, 2021. https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS.

Xu, W. (2020). The SWIFT System: A Focus on the U.S.– Russia Financial Confrontation. *Russian International Affairs Council*. Effective May 14, 2021. https://russiancouncil.ru/en/analytics-and-comments/analytics/the-swift-system-a-focus-on-the-u-s-russia-financial-confrontation/.

Woodhams, S & Migliano, S. 2021. The Global Cost of Internet Shutdowns, TOP10VPN. Effective May 14, 2021. https://www.top10vpn.com/cost-of-internet-shutdowns/.

Xin, Z. (2019). China gives up two of its best-kept forex reserve secrets. *South China Morning Post*, 29.7.2019. Effective May 14, 2021. https://www.scmp.com/economy/china-economy/article/3020410/how-much-chinas-forex-reserves-us-dollars-beijing-gives-two.

Xu, W. (2020). The SWIFT System: A Focus on the U.S.– Russia Financial Confrontation. *Russian International Affairs Council*. Effective May 14, 2021. https://russiancouncil.ru/en/analytics-and-comments/analytics/the-swift-system-a-focus-on-the-u-s-russia-financial-confrontation/.

Yandex (2021). History of Yandex. Effective May 14, 2021. https://yandex.com/company/history.

Yin Robert, K. (1994). *Case study research: Design and methods*. Sage Publications.

YK (2016). The promotion, protection and enjoyment of human rights on the Internet. United Nations, General Assembly. Oral revisions of 30 June. Human Rights Council. 27 June 2016. Effective May 14, 2021. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

YK (2018). The promotion, protection and enjoyment of human rights on the Internet. United Nations, General Assembly. Oral revisions of 30 June. Human Rights Council. 4 July 2018. Effective May 14, 2021. A/HRC/38/L.10/Rev.1 – OHCHR.

Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The shifting landscape of global Internet censorship. *Berkman Klein Center Research Publication*, (2017-4), pp. 17-38.