Tampereen yliopisto
Johtamiskorkeakoulu
Politiikan tutkimuksen tutkinto-ohjelma

Suuren palomuurin tuolla puolen:
Kiinan kyberulottuvuuden informaation turvallistaminen

Pro Gradu-tutkielma
Kansainvälinen Politiikka
Kevät 2017

Tampereen yliopisto
Johtamiskorkeakoulu
Politiikan tutkimuksen tutkinto-ohjelma

SCHMITT, AARNE: Suuren palomuurin tuolla puolen: Kiinan kyberulottuvuuden informaation turvallistaminen.
Pro gradu –tutkielma, 67s
Kansainvälisen politiikan opintosuunta
Heinäkuu 2017

Pro Gradu -tutkielmani käsittelee Kiinan kyberturvallisuuspolitiikan ja internetsensuurin muutoksia presidentti Xi Jinpingin presidenttikaudella. Kyberturvallisuuden kansainvälinen normisto on yhä muotoutumisvaiheessa ja muotoutuvien normien merkitys yhä informaatio- ja datatäyteisimmissä tulevaisuusskenaarioissa on merkittävä. Kiina itse elää voimakasta internetpolitiikan muutoksen aikaa ja näitä muutoksia mahdollisine kansainvälisine seurauksineen tarkastelen tässä tutkielmassa.

Keskityn gradussani Kiinan kansallisen turvallisuuden ja informaation turvallistamisen konseptien erittelyyn. Tarkoituksena selvittää miten ja millä perusteluin Kiina tekee informaatiosta osan kansallista turvallisuutta. Aineistoni pohjaa uutislähteisiin, lakiesityksiin ja yksittäisiin Presidentti Xin ja kyberhallinnon johtajan Lu Wein lausuntoihin vuosilta 2014-2016. Aineistoni pohjalta olen pyrkinyt erittelemään millaisia turvallistamisen muotoja Kiinan valtion internetiin ja internetissä saavutettavan informaation turvallistamiseen liittyy sekä tarkastelemaan Kiinan internetsuvereniteetin konseptin kansainvälistämisen pyrkimyksiä.

Analyysini taustalla on konstruktivistinen käsitys turvallisuuden muodostumisesta, jota tarkastelen Kööpenhaminan koulukunnan turvallistamisen teorian avulla. Hyödynnän tutkimuksessani Ole Wæverin ja Barry Buzanin tulkintoja turvallisuuden subjektiivisesta rakentumisesta, jossa turvallisuusuhan määrittely tapahtuu turvallistajan ja yleisön vuorovaikutuksessa. Lisäksi analyysissani käytän Juha Vuoren turvallistamisen tyyppejä ja näiden käyttöä turvallistamisessa autoritäärisissä järjestelmissä.

Tutkielmani johtopäätös on, että Kiina hyödyntää turvallistamisen logiikkaa rinnastaen perinteisten turvallisuusuhkien retoriikkaa informaation rajaamisen ja hallintaan. Sisäpoliittisten toimiensa tueksi Kiina on pyrkinyt aktiivisesti kampanjoimaan internetsuvereniteetin konseptia turvautuakseen kansainväliseltä kritiikiltä internetin tiedonhallinnan ihmisoikeudelliselta kritiikiltä. Teoreettisena johtopäätöksenä tutkimus viittaa turvallistamisen onnistumisen ja pelon aiheuttaman itsesensuurin rajan empiirisen havainnoinnin ongelmallisuuden.

Sisällys

1. JOHDANTO

> ”Internet ja totalitarismi eivät ole yhteensopivia.
> Totalitarismissa informaatiota täytyy kontrolloida.
> Joka kontrolloi informaatiota, kontrolloi ihmisten mieliä.”[1]

Tämä tutkielma on tutkimustavoitteeltaan ensisijaisesti ilmiökeskeinen. Tavoite on ymmärtää Kiinassa tapahtuvaa internetiin kohdistuvan turvallisuusajattelun muutosta sekä analysoida sen suhdetta ja mahdollisia seurauksia laajemmin kyberulottuvuuden turvallisuuden kontekstissa. Teoreettisena lähtökohtana turvallistamisen teorian tehtävä tässä tutkielmassa on antaa konseptuaalisia työkaluja ymmärtää Kiinan muuttuvan politiikan dynamiikkaa sekä tarkastella turvallistamista ei-demokraattisessa kontekstissa, missä sen selitysvoimaa usein kyseenalaistetaan.

Tultaessa vuoden 2016 loppuun Freedom Housen internetvapautta mittaava raportti antoi Kiinalle 0-100 asteikolla (missä 0 edustaa vapaata internetin käyttöä) tylyn pisteytyksen 88, minkä Kiina oli saanut myös vuonna 2015. Sen sijaan että Kiina olisi taipunut vaihtelevaan kansainväliseen painostukseen internetin ja kansalaisten vapauksien varmistamiseksi, ovat sen internetiin kohdistuvat rajoitukset pikemminkin vankistuneet tällä vuosikymmenellä Xi Jinpingin presidenttikaudella, joka on tuonut ideologian ja informaation takaisin valtion turvallisuusajatteluun.

Miksi sitten kirjoittaa internetin sensuurista Kiinassa? Miten Kiinan sisäpoliittinen toiminta on merkittävää yli sen rajojen? Digitalisaatio on vasta lapsen kengissä. Digitaalinen data muuttuu yhä keskeisemmäksi ja läpitunkevammaksi osaksi arkea sekä yksilön, valtioiden että yritysten toiminnassa. Muutoksen mukana määrittyy myös se miten dataa kerätään, kuka sitä hyödyntää sekä miten ja missä tieto on tavoitettavissa. Kansainvälinen säännöstö ja valtioiden omat sisäiset säännökset ovat jo nykyisessä kehityspisteessä ongelmallisessa tilanteessa uusien teknologioiden kanssa ja valtion suhdetta tähän datan aiempaa laajempaan kerättävyyteen määritellään aktiivisesti uudelleen. Viime vuosina useissa valtioissa on luotu uutta kyberturvallisuuteen ja tiedonkeruuseen liittyvää lainsäädäntöä ja tendenssi on ollut nimenomaan pyrkimys saattaa kyberulottuvuuden ”villi länsi” perinteisemmän kontrollin alaiseksi (Haukkala teoksessa Forsberg & Raunio 2013, 251-253).

---

[1] Oma käännös. Lähde: ”Castro hates the internet, so Cubans created their own” https://www.youtube.com/watch?v=FFPjJM6yYS8

[2] eng. brute facts.

[3] Tässä tutkimuksessa ei aktiivisesti käytetty, mutta tiedon ja vallan suhdetta sekä valtaa vuorovaikutussuhteena

Digitalisaation ja kytkeytyneisyyden ympärillä pyörii erilaisia skenaarioita, olivat ne sitten tietoturvallisuuden ammattilaisten kuten F-Securen Mikko Hyppösen, eri ajatushautomoiden tai akateemisten tutkijoiden visioita. On selvää että skenaarioista puhuttaessa on kyse vain mahdollisuuksista, ei varmuuksista. Kaikki suuntaviivat antaisivat olettaa vähintään tiedonkeruun merkityksen voimistumista, yhä kytkeytyneempää verkostoa ihmisten ja esineiden välillä. Kaikki toiminta voisi tällaisessa tilanteessa olla hyödynnettävää dataa, mikä ei rajoittuisi vain selaushistoriaan tai evästeiden käyttöön. Yhdysvaltojen 2016 presidenttivaalit ja Brexit-kampanja näyttivät omilla tahoillaan, mitä big data mahdollistaa ihmisten aktivoinnissa, passivoinnissa ja ohjailussa. Molempien kampanjoiden taustalla on toiminut Cambridge Analytica, joka hyödyntää julkisesti tavoitettavaa dataa ja psykologista OCEAN-profilointia tunnistaessaan tavoiteltavia ihmisryhmiä ja yksilöitä. Tämä taas mahdollista äärimmäisen yksilöllisen vaikuttamisen vaikuttajan ja vaikutuksen kohteen välillä (Vice 2017). Samaa logiikkaa voidaan käyttää myös informaatiota rajaamalla ja valikoimalla, mikä luo keskeisiä ongelmia internetsensuurin normatiivisuudelle. Kun samalla neurotiede ja ymmärrys ihmisten aivojen ja kognitiivisten prosessien algoritmipohjaisuudesta syvenee, voi internet ja sen datan hallinta avata yhä merkittävämpiä mielipiteisiin vaikuttamisen ja käyttäytymisen ohjaamisen työkaluja (Harari 2016).

Suomesta käsin Kiinan internetpolitiikan tutkimisen tekee erityisen ajankohtaiseksi suunnitteilla oleva koillisväylän datakaapeli. Liikenneministeriön tavoitteissa on ollut tuoda projektiin mukaan Japani, Kiina, Venäjä, Norja ja Saksa tai Iso-Britannia. Data ja kyberturvallisuus yhdistettynä kireisiin suhteisiin Japanin ja Kiinan välillä, sekä turvallisuuspoliittiset harkinnat vaikuttavat samalla myös Euroopan maiden osallistumiseen. Pahimmillaan Suomi voikin projektissa jäädä kolmestaan Kiinan ja Venäjän kanssa, jolloin edellä mainittujen valtioiden suhde dataan ja internetin neutraaliuteen muuttuu sekä itsessään äärimmäisen merkittäväksi että heijastuu Suomen ulkopoliittisiin suhteisiin muun muassa Yhdysvaltoihin, Ruotsiin ja Japaniin (Liikenneministeriön selvitys Koillisväylän tietoliikennekaapelihankkeesta).

Yhteinen tekijä eri kyberskenaarioille on kuitenkin informaation roolin korostuminen. Ei ole sattumaa että valtiot turvallisuustoimijoineen ja mainostamistaan pohtivat yritykset haluavat aiempaa tehokkaammin hyödyntää digitaalisesti yksityisistä ihmisistä kerättävää informaatiota. Jos näille toimijoille informaatio on näin tärkeää, on vain loogista että myös yksityisen ihmisen kyky saavuttaa informaatiota digitaalisesti voisi olla verrattavan tärkeää. Jos kerätyllä informaatiolla voidaan vaikuttaa merkittävästi käyttäytymiseemme, niin samalla tavalla saavutettavan informaation oleellinen

rajaaminen vaikuttaa käsityksiimme ja toimintaamme. Tässä informaation rajaamisessa Kiina on ollut ehdoton edelläkävijä. Sen kyky suhteellisen kattavaan hallintaan internetin kaltaisen verkoston ja Kiinan kokoisen väestön yhdistelmässä on teknologisesti ja turvallisuuspoliittisesti vaikuttavaa. Toki Kiinan suuri palomuuri ei ole aukoton ja kun muurin takana olevista tietoläheistä on käsitys, vaatii poikkeuksellisen hallinnan ylläpitäminen perusteluja eli legitimointia. Tähän legitimoinnin prosessiin pureudun pro gradussani.

Digitalisaation lisäksi ajatus että Kiina osana kansainvälistä yhteisöä muuttaisi ihmisoikeus- ja informaatiopoliittista linjaansa on osoittautumassa vääräksi. Oletus siitä että Kiina lähentäisi omaa toimintaansa Yhdysvaltojen tai Euroopan viitekehykseen on toki pitkällä aikavälillä mahdollinen kehityssuunta, muttei väistämätön. Toisaalta tietoturvallisuusmaailmaa ravisuttaneet Edward Snowdenin vuotamat tiedot sekä aloitteet, myös esimerkiksi Suomessa, kiristää internetin valvontaa, antavat aihetta myös arvioida tätä tulkintaa uudestaan (LVM 14.1.2015). On mahdollista, että kansainvälinen kehitys on itse asiassa pikemmin Kiinan edustaman linjan suuntainen, minkä vuoksi Kiinan internetpolitiikan ymmärtäminen tarjoaa työkaluja arvioida millaisia kehityspolkuja eri valtioilla saattaa olla edessään digitaalisen informaation hallinnassa. Se että esimerkiksi Suomessa digitaalisen informaation hallinta muuttuisi merkittävän lähelle Kiinan internetpolitiikkaa on toki äärimmäinen skenaario, mutta digitaalisen informaation lisääntyvä läpitunkevuus tulee määrittämään myös valtioiden ja digitaalisen informaation suhdetta uudestaan. Se miten laajalle myös informaation tavoitettavuuden rajoitukset leviävät on tutkimukseni kannalta merkittävin ulottuvuus tässä muutoksessa. Kiinan esimerkkiä ovat viime vuosina seuranneet jo sellaiset maat kuin Venäjä ja Turkki, missä internet ehti toimia aikaisemmin suhteellisen vapaasti.

Kansainvälisen politiikan tutkimusten teoriaperinteistä käytän tutkimuksessani Kööpenhaminan koulukunnan turvallistamisen teoriaa. Internet ja internetin informaation käyttämisen asema turvallisuuspolitiikassa on yhä keskeneräinen. Samalla kun verkon ja informaation rooli muuttuu ovat viimeiset vuodet myös muuttaneet turvallisuusdiskurssia internetin ja internetin informaation ympärillä. Turvallistamisen teoria mahdollistaa arvioida nimenomaan tämän muuttuvan retoriikan roolia ja mahdollisia tarkoitusperiä Kiinan tapauksessa. Turvallistamisen teorian selitysvoimaa epädemokraattisissa järjestelmissä on usein kyseenalaistettu, sillä se painottaa usein turvallistajan ja yleisön vuorovaikutussuhdetta. Tutkimuksessani esitän kuitenkin, että myös Kiinan kaltaisessa yksipuoluejärjestelmässä tapahtuu turvallistamista jo pelkästään siksi, että lopulta päästäkseen

keskeiseen rooliin suuren valtion turvallisuuspolitiikassa on internetin rooli pitänyt turvallistaa osaksi turvallisuusagendaa järjestelmän sisällä.

Tarkasteltaessa Suomesta käsin Kiinan internetpolitiikan vaikutuksia ja syitä, tarkastelua muokkaa helposti normatiivinen lataus. Suomen kulttuurissa sananvapaus ja informaatiovapaus ovat, viimeistään kylmän sodan jälkeen, olleet suhteellisen itsestään selvinä pidettyjä arvoja. Tästä perspektiivistä Kiinan poliittisen järjestelmän tarkkailu tapahtuu vääjäämättä Eurooppalaisen ihmisoikeusnormiston viitekehyksestä, mikä tarkoittaa tiettyjä pohjaoletuksia informaatiovapauden mielekkyydestä ja itseisarvosta.

Vastaan tutkielmassani seuraaviin tutkimuskysymyksiin: 1) Mitä muutoksia Kiinan internetpolitiikassa on tapahtunut Xi Jinpingin valtakauden aikana? 2) Miten muutoksia on perusteltu ja turvallistettu? Tutkimukseni tutkimusaineisto painottuu vuoteen 2015. Koska Kiinan internetpolitiikka on yhä nopeiden muutosten keskellä olen rajannut viimeiseksi tarkasteltavaksi ajankohdaksi 2016 vuoden lopun.

Tutkimukseni jakautuu kolmeen keskeiseen osioon. Osiossa 2 esittelen turvallistamisen teorian historiaa ja teorian suhdetta tutkimusaiheeseeni sekä erittelen turvallistamisprosessiin rakennetta. Turvallistamisen teoriaa kritisoidaan usein siitä, että se sopisi vain demokraattisen järjestelmien tutkimiseen. Teoriaosiossani esittelen kuitenkin näkemyksiä siitä miten turvallistamisen dynamiikka on sovellettavissa myös totalitaarisiin tai yksipuoluejärjestelmiin sekä erityisesti teorian sovellettavuudesta Kiinan sensuuripolitiikan tutkimiseen. Osiossa 3 teen läpileikkaavaan yleiskatsauksen Kiinan internetpolitiikan tilaan Presidentti Xi Jinpingin valtakaudella ja hänen alaisuudessaan tehtyihin kiristyksiin Kiinan informaatiohallinnassa sekä kansainvälisessä hallinnan oikeutuksessa. Esittelen hallinnan vaikutuksia yksityishenkilöihin, mediaan, yrityksiin sekä laajempia pyrkimyksiä turvata Kiinan itsenäinen oikeus määrittää oma internetpolitiikkansa globaalisti. Osiossa 4 analysoin näitä käytännön muutoksia ja muutosten suhdetta turvallistamisen teorian esittämään retoriseen turvallistajan ja yleisön suhteeseen. Tarkoitus on hahmottaa turvallistamistoimien onnistumista sekä tunnistettavuutta.

2. TURVALLISTAMISEN TEORIA

Tässä luvussa avaan turvallistamisen teorian pohjaoletuksia todellisuuden ja puheen suhteesta. Aloitan käymällä läpi turvallistamisen juuria kielellisessä käänteessä ja tämän käänteen muovaamissa konstruktivistista ajatusmalleista. Tämän jälkeen käyn läpi, miten turvallistaminen on omaksunut ja muovannut näitä kielellisen käänteen ominaisuuksia sekä turvallistamisen teorian käsitystä turvallisuudesta ja turvallisuuden tekijöistä. Esittelen eräitä teoriaan kohdistettuja kritiikkejä ja ongelmia turvallistamisen teorian käsitteissä. Luvussa 2.1. erittelen turvallistamisen rakenteen kahdella tasolla: turvallistamisen keskiössä olevan puheaktin rakenteen, minkä pohjana toimii pitkälle kielitieteilijä Austinin puheaktin teoria. Kielellisen rakenteen jälkeen avaan vielä turvallistamisen rakennetta nimenomaan poliittisena teoriana turvallistamisen yhteiskunnallisen kontekstin kautta. Luvussa 2.2. perehdyn tarkemmin turvallistamiseen Kiinan kontekstissa, huomioiden turvallistamisen usein kohdistetun kritiikin teorian selitysvoiman puutteesta ei-demokraattisissa konteksteissa ja yhteiskunnissa. Samassa luvussa esittelen myös Juha Vuoren turvallistamistyypit, joita hyödynnän myöhemmin Vuoren tapaan ei-demokraattisen Kiinan turvallistamisen analyysissä.

Kööpenhaminan koulukunta tuo puheen poliittisen teon muodossa osaksi kansainvälisen politiikan perinnettä. Kieli ja sanat eivät ainoastaan heijastele olemassa olevaa todellisuutta sen mahdollisine turvallisuusuhkineen vaan sanat, eli puheaktit, osaltaan luovat ja muovaavat tätä todellisuutta – asioiden lausuminen ei ole pelkästään politiikan raportointia vaan itsessään politiikkaa. Tämän tutkimussuuntauksen mahdollisti omalta osaltaan kielitieteen ja filosofian tutkimus kielen ja todellisuuden vuorovaikutuksesta.

Turvallistamisen juuret löytyvät wittgensteinilaisesta ajattelusta ja niin sanotusta kielellisestä käänteestä (eng. *linguistic turn*). Wittgenstein (1999) totesi, että kielessä merkitys on seurausta käytöstä. Sanoilla ei ole itseisarvoisia merkityksiä vaan sanojen merkitys on riippuvainen käyttönsä kontekstista. Sanoilla, toisin kuin esimerkiksi numeroilla, ei tällöin ole sisään rakennettua merkitystä vaan merkitys syntyy puhutun seurauksena (Wittgenstein 1999, §1, Vuori 2011, 52). Tällöin kysymys *mitä sana tarkoittaa* tulee korvata kysymyksellä *miten sanaa käytetään.* Tästä seuraa, että kieltä opittaessa ja omaksuttaessa opimme sanojen käyttöyhteydet, minkä *seurauksena* opimme myös sanojen merkityksen (Wittgenstein 1999, §43). Yhteisesti muodostetuista merkityksistä, tai faktoista, tulee näin vahvistus havaintojemme oikeellisuudesta, sillä yhteisesti ymmärretyt sanat ja merkitykset vaativat

ainakin asteittaista havaintojemme samankaltaisuutta. Tällöin puheaktilla on mahdollisuus osaltaan luoda ja muovata yhteistä todellisuuttamme (Austin 1962).

Ennen kuin vakaumuksellinen realisti ehtii kavahtaa on syytä huomioida, ettei lingvistinen käänne ja Kööpenhaminan koulukunta tulkitse kaikkien todellisuuden aspektien olevan kielen luomia ilmiöitä. Todellisuus voidaankin jakaa niin sanottuihin yhtäältä *raakoihin faktoihin*[2] ja konstruoituihin faktoihin. Faktat ovat seurausta yhteisistä sopimuksista, mutta ilmiöt joihin näillä faktoilla viitataan voivat olla (mutteivät välttämättä ole) ihmisistä riippumattomia (Vuori 2011, 52). On olemassa fyysiseen maailmaan kuuluvia faktoja, joihin ihmisten välinen sopimus tarvitaan faktan luomiseksi, mutta tämä kielellinen luominen ei itsessään näitä luo. Toisaalta on faktoja ja ilmiöitä, jotka nimenomaan ihmisyhteisöt ja yhteiskunnat luovat (ibid. 52). Jälkimmäinen todellisuuden kielellisen määrittelyn taso korostuu, kun puhutaan kansainvälisestä politiikasta. Kun puhutaan niinkin perustavanlaatuisista ilmiöistä kuin valta, ystävyys tai vihollisuus, puhutaan nimenomaan sosiaalisesti luoduista faktoista. Tällöin kieli itsessään tuottaa faktoja. Kansainvälisen politiikan perusyksiköt toimivat pitkälti yksiköissä, jotka kuvaavat nimenomaan ihmisen toimintaa ja ihmisten luomia yksiköitä. Myös puhuttaessa asioista kuten valtiot, suvereniteetti tai tämän tutkimuksen kannalta keskeisesti näitä mahdollisesti kohtaavat uhat.

Toki yksipuolinen aggression kohtaaminen voi luoda hyökkäyksen kohteen näkökulmasta kielestä tai konstruktiosta riippumattoman uhan. Esimerkkinä voidaan pitää terrorismia. Toisaalta tämä ihmisten välisten rakenteiden tai ryhmittymien rajapinta on tällöin aggression toteuttajan luoma. Terrorismin esimerkkiä käyttäen, joku on tällöin tehnyt kielellisesti aatteellisten kannattajiensa kanssa jostain kohteesta uhkan ryhmälle, uskonnolle tai muulle arvolle, jonka ikeestä terrorilla pyritään vapautumaan.

Searle (1969) argumentoi, että ihmisten luomien järjestelmien luonne on ihmisistä riippuvaista objektiivista totuutta. Ilman ihmistä ja ihmisten tekemiä sopimuksia kyseisiä objektiivisia totuuksia olisi olemassa. Objektiivisiksi verrattuna subjektiivisiin totuuksiin nämä tekevät näiden instituutioiden tai ilmiöiden olemassaolo subjektiivisesta havainnoinnista riippumatta. Samalla tällaisia faktoja ei kuitenkaan voi verrata täysin ihmisistä riippumattomiin faktoihin, kuten useimmat fysiikan ilmiöt. Vuori (2011, 53-55) selittää Searlen argumenttia käyttämällä esimerkkinä rahaa. Rahaseteli on objektiivisena faktana paperia. Tämä ulottuvuus rahan olemusta ei muutu vaikka rahan arvoa

[2] eng. brute facts.

määrittävät instituutiot lakkaisivat olemasta tai ihmiskuntaa ei olisi enää olemassa. Tällöin kuitenkin sosiaalisesti konstruoitu fakta, että kyseisellä palalla on joku määrätty arvo, jota ihminen voi käyttää valuuttana ilman, että kyse on itse paperin arvosta, lakkaisi olemasta. Sosiaalisesti konstruoidut faktat myös ovat usein viittaussuhteessa itseensä, tai kuten Vuori asian muotoilee: ”ontologisesti sosiaaliset faktat ovat subjektiivisia, mutta epistemologisesti objektiivisia.” Rahan objektiivinen merkitys rahana on riippuvainen siitä, että ihmiset käyttävät objektia rahana ja tulkitsevat objektin rahaksi. Jos jotain käytetään systemaattisesti rahana saa se käytännössä rahan objektiivisen merkityksen yhtälailla kuin käytöstä jätetty valuutta menettää lopulta fakta-statuksensa rahana. Samalla tavalla sosiaalisesti luodut poliittiset instituutiot käyttävät valtaa pitkälti ihmisten välisesti sovittujen käytäntöjen puitteissa. Vaikka valtiot toki käyttävät objektiivista valtaa ja valtioilla on fyysisiä vallan välineitä, määrittelemme sosiaalisesti yksiköt, joiden puitteissa tätä valtaa käytetään.[3]

Itse turvallistamisen teoria syntyi Kööpenhaminan rauhantutkimuksen keskuksen (COPRI) piirissä. Se syntyi haastamaan turvallisuutta kapea-alaisesti tarkastelleen kansainvälisen strategisen tutkimuksen perinnettä, kyseenalaistaen turvallisuuden määritelmän (Vuori 2011, 103). Kapea turvallisuuskäsitys oli kehittynyt pitkälti kylmän sodan ydinaseturvallisuuden ensisijaisuuden seurauksena (Buzan et al 1998, 3). Turvallisuus oli COPRIn tutkijoiden mukaan puutteellisesti teorisoitu, kun sen katsottiin tarkoittavan vain objektiivisia ja automaattisesti todellisiksi miellettyjä ulkoisia uhkia, joita voitiin havaita ja havaintoihin reagoida poliittisesti. Kööpenhaminan koulukunta sen sijaan rakensi käsityksensä Wolferin tulkintaan (teoksessa Vuori 2011, 103), minkä mukaan turvallisuusuhat eivät ole puhtaasti objektiivisia tai puhtaasti subjektiivisia, vaan pikemmin intersubjektiivista. Tällöin fokus siirtyi siitä mitä turvallisuus tarkoittaa, tarkastelemaan mitä turvallisuus tekee ja miten turvallisuuden tuottamisella tehdään (ibid. 103).

Osaltaan turvallistamisen teoria pyrkiikin problematisoimaan mitä *turvallisuus* itsessään on. Esimerkiksi Wæver (2004, 54) arvioi perinteisten kansainvälisen politiikan teorioiden ainoastaan tarkastelevan turvallisuutta näkökulmasta, josta käsin ne pohtivat mitä turvallisuuden piiriin tulisi kuulua pitäen turvallisuuden konseptia itsestään selvänä. Turvallistaminen haastaa kyseenalaistamaan tätä konseptia ja arvioimaan mistä ja miten asioista tulee turvallisuutta ja mikä turvallisuusstatuksen funktio on. Turvallistamisen teoria kyseenalaistaa turvallisuuden käsitteen konnotaation. Onko turvallisuus käsitteenä positiivinen vai negatiivinen? Realismin ja liberalismin piirissä turvallisuus

[3] Tässä tutkimuksessa ei aktiivisesti käytetty, mutta tiedon ja vallan suhdetta sekä valtaa vuorovaikutussuhteena tarkasteleva Foucalt, tarjoaisi myös mahdollisen kulman tarkastella informaation turvallistamista.

mielletään yleensä positiiviseksi konseptiksi, mutta esimerkiksi Wæver ja Buzan huomauttavat turvallisuuden johtavan yleensä vapauksien ja demokraattisen prosessin rajaamiseen (Vuori 2011, 115-117). Turvallistamisen teoria Kööpenhaminan koulukunnassa kuitenkin katsoo, realismin turvallisuuskäsityksen tavoin, turvallisuuden muodostavan oman erillisen osa-alueen, joka eroaa muista politiikan muodoista (Stritzel 2007, 360). Turvallistamisen puheakti jää lausuntansa jälkeen elämään, varsinkin onnistuttuaan, turvallisuuden piirissä mahdollistaen turvallisuuspoliittisia poikkeuslinjauksia.

Kun puhutaan uhkien tai todellisuustilojen muovaamisesta retoriikalla on turvallistamisessa tehtävä ero asioiden *turvallistamisen* ja *politisoinnin* välillä (Buzan et al 1998, 25). Vaikka ilmiöistä tehdään osa poliittista agendaa, ei se automaattisesta tarkoita ilmiön turvallistamista. Buzanin, Wæverin ja de Wilden julkaistaessa turvallistamisteorian keskeisiä teoksia olevan kirjansa 1998 ilmastonmuutoksen globaali turvallistaminen oli vielä alkuvaiheessa. Siinä missä ilmastokysymyksistä vuosituhannen vaiheessa oltiin tehty politisoitu kysymys, voidaan prosessin kohti turvallistamista sanoa olevan vielä kesken. Nykyisellään keskustelua ilmastonmuutoksen mahdollisesta eksistentiaalisesta uhasta, tai ilmiön todellisuudesta, käydään ympäri maailmaa. Toistaiseksi kuitenkaan ilmastonmuutoksen torjuminen ei ole johtanut perinteisen legitiimin politiikan prosessien muokkaamiseen. Tapaus valottaa *turvallistamisen* ja *politisoinnin* joskus häilyvää rajapintaa. Tämä erottelu on merkittävää jo siksi, että turvallistamisen teoria ei väitä kaiken olevan retorisesti luotua turvallisuutta. Kaikki mikä nostetaan agendalle ei ole automaattisesti turvallisuutta, eikä turvallistamisen teoria pyri vesittämään turvallisuuden tai uhan määritelmää. Päinvastoin, teoriana se on reaktiivinen siinä mielessä, että se arvioi miten toimijat (valtion tai muut) luovat uhkia, joiden suhde objektiiviseen todellisuuteen ei aina ole yksiselitteinen.[4]

Ottaen huomioon Wæverin keskeisen roolin Kööpenhaminan koulukunnan teorian piirissä on kuitenkin huomioitavaa, että koulukunnan ailahtelevaa suhdetta politiikan ja turvallisuuden erotteluun on aiheellisestikin kritisoitu (esim. Balzacq 2015). On kohtuutonta väittää turvallistamisen erottavan aiheensa kokonaan pois politiikan piiristä, tehden siitä puhtaasti osan politiikasta erillistä turvallisuutta. Sen sijaan turvallistamisen voi mieltää johtavan turvallisuuden siirtämiseen eri poliittiseen foorumiin,

[4] Tämä heijastuu myös esimerkiksi terrorismin ja tapon väliseen määritelmään. Toinen on yksittäistapaus, toinen määritellään eksistentiaaliseksi uhaksi. Esimerkiksi politiikan toimittaja Simon Jenkins (iqsquared 13.1.2017) väittää: ”I don’t think terrorism is very important. I think we make it important and by making it important we make it important.”

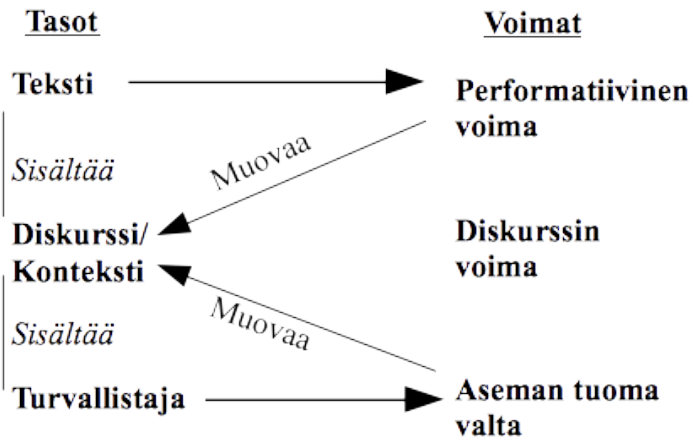
missä normaaliksi mielletyt yhteiskunnan pelisäännöt ja toimintatavat muutetaan turvallisuuden nimissä.

Buzanin ja Wæverin (1998, 25-32) määritelmässä turvallistamisen teoria tarkastelee yhtä lailla perinteistä valtaa kuin turvallisuuden ja turvallisuusuhan määrittelyn konstruktiivista luonnetta. Tällöin tutkittavana on vallan hierarkkinen rakenne, missä tietyt toimijat ovat etusijaisessa valta-asemassa. Näiden toimijoiden pyrkimykset turvallistaa asioita onnistuvat suuremmalla todennäköisyydellä, kuin verrattain heikomman toimijan pyrkimykset. Kyse on ”konseptien valtapolitiikasta.” Muun muassa Strizel (2007, 364) näkee tässä kuitenkin merkittävän sisäisen dissonanssin, missä turvallisuutta yhtäältä määrittelee objektiivinen valta, vaikka teoria toisaalta korostaa yleisön merkitystä turvallistamisen hyväksyvänä tai hylkäävänä toimijana. Nämä eivät kuitenkaan nähdäkseni ole todellisuudessa merkittävässä ristiriidassa keskenään. On luontevaa olettaa, että valta-asema tai asiantuntijuus voivat merkittävästi lisätä turvallistajan onnistumisen todennäköisyyttä, vaikka yleisöllä olisi merkittävä rooli turvallistamisen lopputulokseen.

Turvallisuuden määritelmä, varsinkin turvallisuuden käsitteen laajuus, on keskeinen myös tätä *politisoinnin* ja *turvallistamisen* rajaa tarkasteltaessa. Turvallistamisen yhteydessä puhutaan pääsääntöisesti valtiota, järjestelmää ja yhteiskuntaa kohtaavista *eksistentiaalisista* eli olomassaoloa vaarantavista uhista. Tällöin turvallisuudessa on turvallistamisen teorian yhteydessä kyse nimenomaan selviytymisestä (Buzan et al 1998, 23). Nämä eksistentiaaliset uhat voivat olla hyvin erilaisia ajasta ja paikasta riippuen. Varsinkin sosiaalisesta konsepteista kumpuat uhat ovat yleensä sidoksissa järjestelmäänsä, jota tämän uhkan koetaan vaarantavan. Yhteiskunnalliset tai kulttuuriset liikkeet voidaan määrittää uhkaksi joissain valtioissa (esimerkiksi Kiina, Venäjä), toisissa ei. Toisaalta uskonto yleisellä tasolla ei ollut perinteisesti turvallistettu Yhdysvalloissa, mutta vuoteen 2016 tultaessa pelkän terrorismin turvallistamisen ohella voidaan havaita siirtoja turvallistaa islam uskontona, liittäen tämä kokonaisuutena terrorismin uhkaan (Buzan et al 1998, 25). Yleisellä tasolla vahva nationalistinen eetos yleensä sisältää ulkopuolisten valtioiden ja kulttuurien määrittelyä kilpailijana tai turvallistamisen tapauksessa vihollisena. Kiinassa ja internetsensuurissa tämä näkyy retoriikkana, missä internetin sensuuria on yleisesti puolustettu ulkopuolisen pahantahtoisen ideologisen vaikutuksen uhalla (kts. luvut 3-4).

Turvallistamisen ja politisoinnin välinen jaottelu on kuitenkin myös herättänyt kritiikkiä. Koska turvallistamisen pohjalla on käytännössä realismin tulkinta turvallisuudesta poikkeustilana, ovat tutkijat (esim. Stritzel 2007) arvostelleet teoriaa uhkakuvassa liian staattiseksi ja yksiulotteiseksi. Tukeutumalla

realismin käsitykseen turvallisuudesta, sulkee turvallistaminen itseltään liikkumatilaa nyansoidumpien tulkintojen ja turvallistamisen lopputulosten tapaus- ja yhteiskuntakohtaiseen tarkasteluun (Stritzel 2007, 366). Stritzel itse ehdottaa turvallistamiselle täydentävää vuorovaikutteisempaa sosiaalista prosessia (Kuvio 1).



Kuvio 1: Strizelin turvallistamisen sosiaalinen prosessi

Patomäki (2015) huomioi ettei turvallistamisen teorialla ole suurten geopoliittisten muutosten ennustamisvoimaa.[5] Tämä pitää tietyssä mielessä paikkaansa. Samoin Patomäen näkemys ettei turvallistamisen teoria ole samalla tavalla kokonaisvaltaiseen kansainvälisen politiikan ilmiöiden selitykseen kykenevä teoria, kuin suuremmat perinteiset teoriat. Tämä ei kuitenkaan ole turvallistamisen teorian ensisijainen tarkoitus. Mielestäni turvallistamisen teoriasta puhuttaessa ei tarvitse pitää ongelmallisena, että teoria soveltuu nimenomaan uhkien muotoutumisen, niihin reagoimisen ja niiden normalisoimisen selittämiseen. Tässä mielessä turvallistamisen teoria toimii avustavana teoriana näille kansainvälisen teorian ”kaiken kattaville teorioille”. Itsenäisen kaiken kattavuuden sijaan se auttaa ennustamaan niin realismin, liberalismin kuin konstruktivismin puitteissa, miten mahdollisista uhista erilaisissa järjestelmissä tehdään turvallisuuskysymyksiä ja millaisiin toimiin tämä prosessi valtion voi voimauttaa.

[5] Patomäki kuitenkin esittelee ehdotuksensa tuoda tilastollista todennäköisyysnäkökulmaa vahvemmin osaksi turvallistamisen teoriaa, minkä avulla tätä ennustavuuden ongelmaa voitaisiin Patomäen mukaan korjata.

Turvallistamisen teoriaa on kritisoitu sen suhteesta objektiiviseen materialistiseen todellisuuteen (Vuori 2011, 46). Jos kerta todellisuus rakentuu konstruktivistisesti kielen mukana, ollaan kriitikoiden mukaan matkalla kohti loputonta todellisen maailman ”ydintä”. Vuori (ibid. 46-47) kuitenkin huomauttaa aiheellisesti, että vaikka loputon todellisuuden ontologisen ytimen tavoittelu olisikin mahdollista, ei se tarkoita sitä että se olisi myös hyödyllistä tai mielekästä.[6] Teorian tavoite ei niinkään ole ottaa kantaa turvallisuusuhkien todellisuuden luonteeseen, vaan se tarkastelee ja selittää prosessia, jolla tietystä kysymyksestä luodaan yhteisesti koettu turvallisuuskysymys (Buzan et al 1998, 26). Keskeisintä turvallistamisen tutkimuksessa on Buzanin (ibid. 25) mukaan hahmottaa milloin ”väitteen retorinen tai semioottinen rakenne saa niin merkittävän vaikutuksen, että yleisö suvaitsee normaalisti noudettavien säännösten rikkomisen.”[7] Fokus tällöin siirtyy uhkan ja todellisuuden suhteesta siihen, mitä muutoksia turvallistamisen puheakti aiheuttaa (Stritzel 2007, 361).

Ole Wæverin mukaan turvallistaminen on valtapolitiikkaa turvallisuuden konseptista (Buzan et al 1998, 32). Oikeissa olosuhteissa turvallisuusuhan konstruointi ei tällöin välttämättä tarvitse todellista uhkaa. Näin yksittäisistä asiakysymyksiä, toimijoita tai ilmiöitä voidaan määrittää turvallisuuskysymyksiksi vaikka nämä eivät välttämättä lähtökohtaisesti olisi turvallisuusuhkia. Konstruoimalla turvallisuuskysymys tavoitellaan legitimiteettiä tähän todelliseen tai kuviteltuun uhkaan kohdistuviin vastatoimiin, jotka ilman turvallisuusmääritelmää eivät välttämättä saisi hyväksyntää (Vuori 2011, 106). Tällaisia toimia voivat olla konkreettiset sotilaalliset toimet, tiettyjen kansalaisiin kohdistuvien rajoitusten asettaminen tai esimerkiksi valtion turvallisuussektorin budjetin suhteuttaminen valtion kokonaisbudjettiin.

Turvallistamisen osatekijöitä (kts. luku 2.1.) on teorian olomassaolon aikana teorisoitu ja analysoitu vaihtelevin painotuksin. Lingvistinen käänteen myötä tutkimuksen päähuomio kiinnittyi kielen ja todellisuuden ontologiseen suhteeseen (Huysmans 2011, 372). Tästä johtuen huomio kiinnittyi diskursseihin, sisältäen paljon turvallistamisen kielellistä tutkimusta. Sittemmin painotus on Huysmansin (ibid, 372-373) arvion mukaan siirtynyt pikemminkin kommunikaation ja merkityksen siirtymisen tutkimiseen, mikä toi puheen vastaanottajat laajemmin osaksi turvallistamisen keskustelua.

[6] Samaista ongelmaa pohti jo kielellisen käänteen keskeinen kieliteoreetikko Austin (1962), joka tunnisti niin sanojen kuin fyysisten toimien seuraussuhteiden teoriassa loputtoman ketjuttamisen ongelman.

[7] Oma käännös. Alkuperäinen teksti: ”When does an argument with this particular rhetorical and semiotic structure achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed?”

Hän kuitenkin huomauttaa aiheellisesti, että turvallistaminen ei problematisoi tai arvioi puheaktin *aktia*, siis puhetta toimintana jolla on konkreettisia seurauksia. Turvallistamisen teoria kuten puheaktien lingvistinen tutkimuskin asettaa aikomukset ja seuraukset teoretisoinnin keskiöön (Austin 1962). Tällöin korostuvat siis sanotun aikomukset ja seuraukset, itse aktin jäädessä määrittelyltään vähemmälle huomiolle. Puheaktin ja turvallistamisen poliittisuuden määrittää sen kyky muovata ja muokata poliittisia käytäntöjä, murtaa totuttua proseduurista kaavaa toimia. Samalla se, Huysmansin sanoin, ”uudelleen määrittää vallitsevan järjestyksen rajoja.” Muutokset voivat olla minimaalisia niin määrällisesti kuin ajallisesti, mutta puheakti pystyy luomaan edellytykset muovata aiemmin yhteisiksi sovittuja turvallisuuden pelisääntöjä.

Siinä missä muitakaan kansainvälisen politiikan kokonaisuuden muodostavia teoriaperinteitä, ei myöskään turvallistamisen teoriaa voida pitää yhtenä koherenttina konseptina. Thierry Balzacq (2015) arvioikin *turvallistamisen teoriaan* sisältyvän erilaisia määritelmiä *turvallistamisesta*. Tällöin turvallistaminen olisi tarkasteltavissa erilaisista katsomusperinteistä kuten filosofia tai sosiologia. Balzacq[8] itse esittää eräänlaisen ideaalisen turvallistamistyypin rakenteen, jonka pohjalta Balzacq tulkinta painottuu enemmän turvallistamisen sosiologiseen tulkintaan kuin Wæverin vastaava.

Buzan toteaa turvallistamisen teorian juurtuvan kolmeen tutkimusperinteeseen: 1) puheaktien teoriaan (kts. Luku 2.1.), 2) schmittiläiseen käsitykseen tuvallisuudesta ja poikkeustiloista sekä 3) perinteisiin turvallisuusdebatteihin (Buzan et al 2009, 213-214). Carl Schmittin arviot turvallisuudesta jakavat turvallistamisen kanssa ajatuksen siitä, kuka voi määrittää ja luoda puhumalla turvallisuutta. Muodollisen auktoriteetin korostuminen, mutta myös erityisesti turvallisuuspuheaktien onnistumiseen suhtautuminen kuitenkin erottaa Vuoren (2011, 166-167) mukaan schmittiläisen ajattelun ja turvallistamisen teorian toisistaan. Turvallistamisen teorian pohjalta myös muodollisesti turvallisuutta määrittävässä asemassa olevan henkilön turvallistamistoimet voivat epäonnistua, koska turvallistamisen yleisöllä on merkittävä rooli turvallistamisen onnistumisessa. Schmittin ajattelussa valtion päättäjä määrittää yksipuolisesti sekä poikkeustilan että vihollisen, jonka uhkan torjumiseksi poikkeustila astuu voimaan. Vuori (ibid, 172) arvioikin ajatusmallien eron kiteytyvän turvallistamisen

[8] Balzacqin ideaalityypin keskeiset turvallistamisen tekijät itsessään vastaavat Kööpenhaminan koulukunnan tulkintaa: Turvallistaminen perustuu turvallistajan ja yleisön yhteiskunnalliseen suhteeseen. Turvallistamisen teko ja konteksti ovat toisistaan riippuvaisia. Turvallistamisen pohjana on väite eksistentiaalisesta uhasta. Valtasuhteet osapuolten välillä muovaavat turvallistamisen prosessia ja lopputuloksia. Turvallistaminen kanavoituu erilaisten sosiaalisten vaikutusmekanismien kautta. Turvallistaminen luo muutoksia politiikkaan, mikä voi näkyä esimerkiksi tiettyjen oikeuksien rajaamisena. Turvallistaminen luo puhujalleen vastuun turvallistamisteostaan.

sosiaalisen vuorovaikutuksen luonteeseen, schmittiläisen sanelun sijaan. Buzan et al. (2008, 33) nostavat kolme toteutumisehtoa[9] turvallistamiseen, jotka Stritzelin mielestä (2007, 364) erottavat osaltaan turvallistamista schmittiläisestä perinteestä:

1. puheaktin sisällön tulee mukailla turvallisuuden kielioppia
2. puhujan auktoriteetti suhteessa turvallistamisen yleisöön, mikä lisää turvallistamisen onnistumisen todennäköisyyttä
3. väitetyn uhan ominaisuudet, jotka joko tekevät turvallistamisen onnistumisen todennäköisemmäksi tai epätodennäköisemmäksi.

Tämä 3. toteutumisehto on sittemmin täsmennetty Wæverin (ibid. 366) toimesta tarkoittamaan ”aspekteja, jotka historiallisesti ovat liitetty uhkaan ja mielletään yleisesti ottaen uhkaaviksi.” Näin ollen schmittiläisyydestä poiketen, turvallisuutta ei voida sanella millä keinoin tai sanavalinnoilla tahansa. Turvallistajalla tulee olla riittävä auktoriteetti pystyäkseen uskottavasti turvallistamaan ja turvallistamisen kohteena olevan uhan tulee olla uskottava. Turvallistamisessa toimii niin sanotun poikkeustilan logiikka (Borbeau 2014, 189), jonka schmittiläinen turvallisuuskäsittely sivuuttaa auktoriteetin kyseenalaistamattomalla käskyvallalla.

Patomäki (2015) kritisoi turvallistamisen teoriaa siitä, ettei se eksplisiitisti huomioi poliittisen talouden vaikutusta turvallistamisen muotoutumiseen. Patomäki sitoo epäsymmetrian poliittisessa taloudessa konfliktien todennäköisyyden lisääntymiseen ja arvioi ettei turvallistamisen teoria ota tätä konfliktien syntymisen ulottuvuutta huomioon. Vaikka turvallistamisen teoriaan voidaan kohdentaa monenlaista aiheellistakin kritiikkiä, eivät Patomäen kritiikki sekä muut vastaavat konkreettista uhkia muodostavia poliittisia virtauksia esiin nostavat kritiikit ole suoraan yhteydessä turvallistamisen teoriaan. On tärkeää erotella turvallistamisen kohteena oleva prosessit konkreettisista prosesseista. Poliittisen talouden asymmetria on täysin mahdollista turvallistaa ja tällöin turvallistaja ja turvallistamistoimien kohde valikoituvat kontekstistaan riippuen. Asymmetrian aiheuttama konfliktivaara on ymmärrettävissä turvallistamisen kautta sekä etuaseman säilyttämisen retoriikalla että poliittisessa taloudessa heikon asemassa olevien tyytymättömyyden ja koetun epäoikeudenmukaisuuden turvallistamisena. Tällöin esimerkiksi poliittisessa taloudessa altavastaajien kritiikki hallintoa kohtaan voidaan turvallistaa

[9] Eng. facilitating conditions.

kapinana ja valtion yhtenäisyyden uhkana, kuten Kiinassa on tehty Luoteis-Kiinan Uiguuri-vähemmistön kohdalla.

Kööpenhaminan koulukunta ja sen turvallistamisen teoria sekä siihen linkittyvä yhteiskunnallinen turvallisuus pyrkivät välimallin ratkaisuksi perinteisen valtiokeskeisen turvallisuustutkimuksen ja yksilöllistä turvallisuutta korostavien kriittisten turvallisuustulkintojen välille (Buzan et al 2009, 213). Teoria pitää perinteiset turvallisuuskysymykset yhä kansallisen turvallisuuden keskiössä, mutta tulkitsee turvallisuuden osittain yhteisesti konstruoiduksi kokonaisuudeksi, jonka osia neuvotellaan turvallistajan ja yleisön välillä. Tämä koskee yhtälailla turvallisuuden uhkia kuin turvallisuusuhkien varalle tehtäviä toimia. Seuraavaksi erittelen tarkemmin tämän vuorovaikutussuhteen osapuolet ja dynamiikan.

2.1. Turvallistamisen rakenne

Turvallistamisen teorian pohjalta internetin politiikan tarkastelu siis tarkoittaa retorisen ja puheaktien keinojen analyysia, jossa pyrittäisiin arvioimaan miten Kiina on tehnyt internetistä ja informaation hallinnasta osan kansallista turvallisuutta. Analyysin tekemiseksi on hahmoteltava millaiset kielelliset prosessit ja rakenteet vaikuttavat turvallistamistoimien pohjana. On hahmotettava turvallistamisen algoritmi. Koska turvallistamista voi tapahtua eri konteksteissa ja erilaisissa vuorovaikutussuhteissa ei voida puhua yhdestä selkeästä tavasta havaita turvallistamista. Voidaan kuitenkin tunnistaa tiettyjä puheakteihin ja kielelliseen ilmaisuun liittyviä johdonmukaisuuksia, jotka muovaavat turvallistamisen rakenteen.

Austin (1962) jakoi puheen ja todellisuuden suhteen kolmeen vaiheeseen 1) illokuutio (eng. illocutionary act), 2) lokuutio (eng. locutionary) ja 3) perlokuutio (eng. perlocutionary act). Illokuutiolla tarkoitetaan puheen tavoitteita eli intentiota. Toisin sanoen *illokuutio* kuvaa puheaktin tyyppiä, eli esimerkiksi pyyntöä, käskyä tai julistusta. Käytännössä voidaan puhua aktin intentiosta, jota seuraukset voivat mukailla tai olla mukailematta. *Lokuutio* taas on puheaktin verbaalinen sisältö, tarkoittaen sanotun foneettisia, semanttisia ja viittaussuhteiden ominaisuuksia. *Perlokuutio* puolestaan viittaa sekä tarkoituksellisiin että tarkoituksettomiin puheaktin käytännön seurauksiin. Tällaisia seurauksia voivat olla toimiminen tietyllä tavalla, pitäytyä toimimasta tietyllä tavalla tai muutoksia

asenteisiin tai mielentiloihin. Näitä asenteita ja mielentiloja voivat olla esimerkiksi pelottaminen tai innostaminen.

Austin toi erittelyllään esiin puheaktin muodon ja seurauksen eron. Lausunto, pyyntö tai väite ovat tapoja ilmaista kielellisesti ja nämä voidaan sitoa suoraan puhehetkeen: ”Minä pyydän sinua.” Sitä vastoin perlokuution piiriin kuuluvat seuraamukset eivät asetu suoraan puheaktin muotoon. Puhuja ei pysty kuulijansa puolesta toteamaan: ”Minä vakuutan sinut.” Vakuuttuneeksi tuleminen voi olla seuraus puhujan puheaktista, mutta vakuuttuminen itsessään on perlokuutio esimerkiksi väitteen tai julistuksen illokuutiosta.

Koska puheaktit ovat nimenomaan tekoja ja toimintaa, liittyy niihin muutakin toimimista kuvaavia ilmiöitä. Puheaktin haluttu vaikutus voi toteutua tai olla toteutumatta, puhujan intentiosta huolimatta. Toisaalta puheella voi olla seuraamuksia, joita puhuja ei aktillaan ole tarkoittanut tuottaa (Austin 1962, 105). Kaikki puheakteja ei välttämättä tehdä puhujan omasta tahdosta, vaan ne voivat olla tilanteen pakottamia ja sinänsä sanalliselta illokuutioltaan vailla normaalia merkitystään. Esimerkiksi pakotettuna tehty väärä tunnustus ei sinänsä aukottomasti vastaa tunnustuksen illokuutiota. Osa akteista ovat akteja vain konventioidensa yhteydestä. Julistaa hääpari vihityksi tai julistaa omaa maailmankatsomustaan ovat perlokuution tasolla kaksi toisistaan varsin erilaista aktia (ibid. 106).

Illokuution kautta ilmaistulla puheaktilla on varsinkin turvallistamisen kontekstissa pääsääntöisesti jokin tavoiteltu perlokuutio. Mikäli tämä perlokuutio ei syystä tai toisesta toteudu, on illokuutio epäonnistunut tavoitteissaan mikä on seurausta puutteellisista *onnistumisedellytyksistä*.[10] Puheaktin ja sen myötä turvallistamisen onnistumiselle ei ole ehtona puheaktin sisällön todenmukaisuus tai valheellisuus (Stritzel 2007). Sen sijaan puheaktin ja turvallistamisen menestys ovat pikemminkin riippuvaisia olosuhteiden luomista onnistumisedellytyksistä. Tällöin puheakti joka täyttää nämä edellytykset voi onnistua tavoitteessaan riippumatta siitä onko väite sinänsä totta vai ei.

Turvallistamisen ja kieliteoreettisen puheaktien tutkimuksen erottaa suhtautuminen intentioon. Turvallistamisen puitteissa on vaikea väittää ei-tarkoitettujen seurausten olevan osa turvallistamista, vaikka puheaktien teoria erotteleekin varsinaisen perlokuution ja perlokutiivisen tapahtumaketjun (Austin 1962, 117). Vaikka tahattomia seurauksia voi syntyä myös turvallistamisen yhteydessä, on turvallistaminen tietoinen poliittinen siirto, jonka illokuutio ja perlokuutio ovat sinänsä tarkoitettuja.

[10] Eng. felicity conditions.

Onnistuminen näissä ei ole taattua, eivätkä turvallistamisen puheaktin seuraukset aina sinänsä vastaa aiottuja seuraamuksia. On täysin mahdollista että puheakti A, jonka tavoite on saada vaste B saakin aiottua suuremman reaktion, mikä voisi johtaa B:tä kattavampiin turvallisuustoimiin.

John Searle (1969) ei jaa kielen näkökulmasta Austinin käsitystä illokuution ja lokuution erottelusta. Kielen kautta illokuutio ilman lokuutiota ei ole havaittavissa. Toisaalta on hyödyllistä erottaa puheaktin taustalla oleva pyrkimys ja itse puheakti, sillä puheaktin onnistumisen arviointi muuttuu tällöin rakenteellisemmaksi. Kaikella todennäköisyydellä puhujan lokuutio onnistuu, toisin sanoen kun tämä yrittää lausua määräyksen hän myös lausuu määräyksen. Se että saako määräys tavoitellun vasteen yleisöltään on tällöin lokuutiosta erillinen ilmiö.

Edellä esitetyn puheen sisäisen rakenteen lisäksi on turvallistamisen rakennetta tarkasteltaessa tutkittava myös turvallistamisen sosiaalista rakennetta. Turvallistaminen on toimijan ja yleisön välisen vuorovaikutussuhde. Tie turvallistamisteosta poliittiseksi ratkaisuksi voi olla monivaiheinen siinä mielessä, että turvallistaminen saattaa vaatia onnistumista useamman eri yleisön edessä. Nämä yleisöt voivat olla poliittisessa hierarkiassa eri tasoisia. Esimerkiksi turvallistaja voi kohdistaa turvallistamisen ensin päättäjiin, joiden vakuuttamisen jälkeen uhka voi olla tarve vielä turvallistaa väestölle, yleisen mielipiteen voittamiseksi ja tullakseen yleisesti hyväksytyksi. Toisaalta toiset turvallisuusuhat voidaan turvallistaa asiantuntijoiden taholta kohdistamalla turvallistaminen ensin yleiseen mielipiteeseen, pyrkien samalla luomaan lisää painetta poliittisille instituutioille tunnustaa turvallistamisen kohteen muodostama uhka turvallisuudelle. Todellisuudessa varsinkin ei perinteisten turvallisuusuhkien kohdalla turvallistamista tapahtuu monesti yhtäaikaisesti. Esimerkkinä voidaan pitää muun muassa ilmaston muutoksen kiihtymiseen liittyvä turvallistaminen. Sekä myötä että vasta-argumentit kohdistetaan sekä suoraan poliittiseen eliittiin, mutta samalla varsinkin uhan turvallistamiseen pyrkivät tahot kohdistavat samanaikaisesti huomattavasti voimavaroja myös laajemman yleisön mielipiteeseen vaikuttamiseen.

Turvallistaminen on kolmen tekijän yhdistelmä: 1) *turvallistamisen kohde*,[11] millä tarkoitetaan asioita, joiden oikeutta olla olemassa vaarantaa eksistentiaalinen uhka. 2) *Turvallistaja*,[12] jotka turvallistavat

[11] Eng. referent object.

[12] Eng. securitizing actors.

asian julistamalla sen olemassaolon uhatuksi. 3) *Funktionaaliset toimijat*,[13] joilla on käytännön merkitys turvallistamisen alan toimintaan. He eivät itsessään ole turvallistamisen kohteita, tai turvallistamisen toimeenpanijoita, mutta heillä on merkittävä vaikutus turvallistamistoimien lopputulokseen (Buzan et al 2009, 36). Internetin turvallistamisesta puhuttaessa tällaisia toimijoita ovat muun muassa ohjelmistojätit kuten Google, Microsoft ja Facebook. Kiinan kontekstissa keskeisiä toimijoita ovat myös esimerkiksi Tencent ja Baidu. Siinä missä länsimaissa internetyhtiöt ja valtiolliset turvallistajat on helpompi eritellä toisistaan, on Kiinassa valtion ja isojen yritysten päätöksenteko merkittävämmin yhteen nivoutunutta. Puolueen suora vaikutusvalta ja omistajuussuhde yrityksiin tekevät yrityksen aseman itsenäisinä funktionaalisina toimijoina parhaimmillaankin häilyväksi. Toisaalta juuri näillä yrityksillä on sekä teknologiset edellytykset että, asiakkuuksien kautta, turvallistettava data hallinnointinsa piirissä.

Turvallistamisen kohteella tarkoitetaan useimmiten valtiota tai abstraktimmalla tasolla kansakuntaa (Buzan et al 2009, 36). Turvallistamisen kohde on useimmiten kollektiivinen ja mielletään niin tärkeäksi, että sen olemassa oloa uhkaavilta vaaroilta on syytä turvata poikkeuksellisinkin keinoin. Yksilöt tai pienet yhteisöt voivat myös tehdä turvallistamiseen pyrkiviä retorisia lausuntoja, mutta Buzanin (2009, 36) mukaan liian pieneen yksikköön kohdistuva turvallistaminen on onnistuu erittäin harvoin. Tämä ei sinänsä ole yllättävää kun huomioidaan, että turvallistamisen onnistuttua puhutaan käytännössä aina koko valtioon tai kansakuntaan vaikuttavasta muutoksesta turvallisuuspolitiikassa. Autoritäärisessä järjestelmässä tähän on kuitenkin poikkeuksia, tosin tällöinkin esimerkiksi hallitsevaa eliittiä tai johtajaa turvaavat ratkaisut perustellaan usein koko valtiojärjestelmän turvallisuuden uhkina.

Toisinaan myös globaaleja uhkia voidaan turvallistaa. Buzan et al (2009, 36) nostavat esimerkiksi kylmän sodan ydinsodan uhan. Ekologiset uhat ovat myös näitä turvallistettavia globaaleja uhkia. Nämä (ja muut globaalit uhat) ovat perinteisiä valtiorajoja ylittäviä uhkia, joihin lähtökohtaisesti tarvitaan usean valtion yhteistyötä uhan torjumiseksi (Hakovirta 2012, 58-59). Myös tämä turvallisuuden skaalan pää on Buzanin (2009, 36) arvion mukaan epätodennäköisempää turvallistaa onnistuneesti, kuin skaalaan keskiväliin jäävä valtio ja yhteisötason turvallistaminen.

Turvallistaja, voi olla yksilö tai ryhmä toimijoita, jotka toteuttavat turvallistamisen puheaktit (Buzan et al 2009, 40). Pääsääntöisesti turvallistaja turvallistaa jotain itseään laajempaa tai muuta

[13] Eng. functional actors.

turvallistamisen kohdetta. Hallituksen on helpompi turvallistaa valtiota kohtaava uhka kuin sen hallinnon oman valta-aseman olemassaoloa uhkaavaa tekijää. On varsin luontevaa olettaa, että ihminen on myöntyväisempi luopumaan vapauksistaan tai sietämään poikkeusoloja, kun nämä on perusteltu uhalla, joka kohtaa entiteettiä johon hän itsekin kuuluu. Turvallistajat eivät rajoitu ainoastaan valtiollisiin toimijoihin tai yksittäisiin asiantuntijoihin. Monesti näillä vaihtoehtoisilla toimijoilla on sosiaalista pääomaa ja esimerkiksi retorisia taitoja, joilla he saavat kantansa median tai muun kanavan kautta tiettäväksi (Watson 2012, 286). Yhtälailla myös esimerkiksi yksityinen yritys voi toimia turvallistajana, pyrkien esimerkiksi turvaamaan oman tuotantonsa kannalta keskeisiä edellytyksiä.

Buzan (2009, 40) toteaa, että nimenomaan *turvallistajan* määritelmän rajaaminen on teorian kannalta haastavaa. Näkökulmasta ja tulkinnasta riippuen *turvallistajan* voi tulkita monelle eri tasolle. Esimerkiksi hallituksen jäsen voi turvallistaa puheaktilla jotain ja tällöin on mahdollista tulkita *turvallistajaksi* nimenomaan tämä hallituksen edustaja, tietty ryhmittymä hallitusta tai vaihtoehtoisesti koko hallitus.[14] Joissain tapauksissa ulkopuolelta on myös lähes mahdotonta arvioida, mikä vastaavassa tapauksessa on todellinen *turvallistaja*. Buzan korostaa, että turvallistamisen taustan erittely aina yksittäiseen henkilöön saakka ei ole myöskään mielekäs tapa analysoida turvallistamisen prosessia. Turvallistamisen teoria sen sijaan keskittyy *turvallistajan* ja *turvallistamisen kohteen* väliseen prosessiin, minkä puitteissa turvallistamisen lopputulo neuvotellaan (Stritzel 2007, 363). Toisaalta tutkijan ja analyytikon on mahdollista jäävätä itsensä määrittäjän roolista ja sen sijaan antaa muiden toimijoiden tai turvallistamisen kohteiden tulkinnan määrittää, kenet aktissa analysoidaan *turvallistajaksi*. Toisin sanoen kenet muut toimijat asettavat vastuuseen tai keskeiseksi puheaktin sisällön kantajaksi.

Globaalien uhkien[15] kohdalla jako *turvallistamisen kohteen* ja *turvallistajan* välillä voi olla häilyvämpi kuin valtiollisen turvallistamistoimen kohdalla. Valtioilla on ensinnäkin pääsääntöisesti rajallinen määrä edustajia, jotka puhuvat valtuutetusti sen puolella. Lisäksi valtio itsessään on usein suhteellisen suorassa vuorovaikutussuhteessa uhkaan nähden. Puhuttaessa globaaleista ilmiöistä kuten

[14] Turvallistajan asema ja rooli vaikuttavat samalla konkreettisesti puheaktin onnistumisedellytyksiin, siinä missä minkä tahansa puheaktin tuottajan tulee olla aktinsa aiottuun tilamuutoksen valtuutettu. Austin (1962) toteaa näin erityisesti muodollisista julistuksista, kuten esimerkiksi asioiden viralliset nimeämiset, avaamiset tai sulkemiset.

[15] Näitä suurempien ilmiöiden turvallistamisia on kutsuttu myös *makroturvallistamiseksi* (Buzan et al 2009, 214).

ilmastonmuutos syntyy kahdenlaisia ongelmia määritelmän kannalta. Ensinnäkin kysymykseksi nousee kuka voi puhua globaalin ilmiön ja sen kohteiden puolesta. Toisaalta ketkä ovat todelliset kohteet turvallistajan toimelle, kun globaalien ilmiöiden eteen tehtävät turvallistamistoimet voivat vaikuttaa hyvin eri tavalla kilpaileviin valtioihin.

Informaation turvallistaminen asettuu näiden välimaastoon. Toisaalta informaatio on helppo mieltää globaaliksi varsinkin nykyisen verkottumisen ja tiedonkulun aikakaudella. Toisaalta tietyt regiimit ja valtiot kokevat informaation vapauden hyvin eri tavalla. Informaation kontrollia voidaan perustella hallinnon ja sitä kautta valtion turvallisuuden pohjalta. Tällöin valtiota uhkaava informaatio voisi murentaa myös kansalaisten oman turvallisuuden kiihdyttäen sisäisiä ristiriitoja ja konflikteja.

Holger Stritzel (2007) kritisoi turvallistamisen teorian rakenteen linssien läpi tehtävän tutkimuksen usein korostavan liikaa puheaktien semantiikkaa, yhteiskunnallisten puitteiden sijaan. Stritzel kaipaa teorialta ytimekkäämpää konseptuaalista näkemystä, jonka tavoitteena olisi taata paremmat edellytykset empiiriselle tutkimukselle. Nykyisellään hän arvioi turvallistamisen teoriaa vaivaavan kahden kilpailevan painotuksen ristiriita. Yhtäältä puheaktiin tapahtumana painottuva sisäinen tulkinta ja toisaalta turvallistamisen prosessiin painottuva ulkoistava tulkinta. Tähän liittyen Striztel (2007, 366) toteaa Kööpenhaminan koulukunnan turvallistamisen tulkinnassa olevan jännitteitä teorian staattisten ominaisuuksien vuoksi. Usein turvallistaminen ei todellisuudessa asetu puhtaasti teorian asettamien turvallistaja, turvallistamisen kohde ja yleisö -rooleihin.

2.2. Turvallistaminen yksipuoluejärjestelmässä ja tapaus Kiina

Turvallistaminen on Eurooppalainen tutkimusperinne. Sen normatiiviset ja teoreettiset lähtökohdat ovat kiinteämmin kytköksissä demokraattiseen ajatteluperinteeseen kuin autoritäärisiin hallintajärjestelmiin. Näistä lähtökohdista turvallistamista on aiheellista tarkastella kriittisesti Kiinan kaltaisen yksipuoluejärjestelmän uhkien ja poikkeussääntöjen laatimista arvioidessa. Lähtökohtaisesti voidaan todeta, että vaikka turvallistamisella on demokraattiseen prosessiin liittyviä painotuksia, se ei tarkoita etteikö teoria olisi soveltamiskelpoinen myös ei-demokraattiseen kontekstiin (Vuori 2008, 66). Vaikka turvallistaminen tapahtuu valtasuhteiltaan epätasa-arvoisissa järjestelmissä, missä eri toimijoilla on toisistaan välillä merkittävästi eroavasti muodollista vaikutusvaltaa, ei edes yksipuoluejärjestelmä takaa turvallistamistoimen onnistumista (Buzan et al 1997, 31).

Turvallistamisen teoriaan kohdistuvia keskeisiä kritiikkejä on teorian ongelmallinen tulkinta siitä, miten huomioida puheaktien erilaisia yleisöjä. Kritiikeissä Kööpenhaminan koulukunnan tulkintojen taustalla arvioidaan olevan liian vahvasti ajatus demokraattisesta järjestelmästä (Balzacq 2010, 67). Autoritäärisissä järjestelmissä tiedon avoimuus ja päätösprosessien läpinäkyvyys ovat muun muassa Balzacqin (2005) mukaan vaikeasti sovellettavia teoriaan, jossa yleisön merkitys on keskeinen. Samalla monet turvallistamistoimet pystytään autoritäärisissä järjestelmissä pakottamaan turvallisuuskysymyksiksi ilman neuvotteluja tai kilpailevia turvallisuusnäkemyksiä (Liow teoksessa Vuori 2011, 111).

Puheaktien teorioissa akteja luokitellaan monesti näiden illokuution mukaan (esimerkiksi Searle (1979)), [16] Vuori (2008) soveltaa vastaavaa metodia ryhmitellen turvallistamisen viiteen turvallistamisen tyyppiin[17] (Taulukko 1), joilla hän osaltaan perustelee turvallistamisen relevanssia myös yksipuoluejärjestelmissä. Erittelen tässä luvussa nuo turvallistamisen tyypit, mutta tutkimukseni kannalta keskeisin on turvallistamisen kontrolli-tyyppi.

Todellisuudessa turvallistamistoimet ovat yhdistelmä eri turvallistamistyyppejä toivotun tuloksen todennäköisyyden maksimoimiseksi. Erillisten tyyppien analysointi toisistaan erillisinä on kuitenkin mielekästä, sillä ne valottavat erilaisten valtasuhteiden ja turvallistamisen onnistumisen ehtojen vuorovaikutusta. Vaikka turvallistaminen on turvallistajan ja yleisön vuorovaikutus, luovat erilaiset valtasuhteet ja erilaiset tavoitteet erilaisia ehtoja onnistumiselle. Yksipuoluejärjestelmässäkin erilaisia yleisöjä voivat olla puolueen sisäiset toimijat ja ryhmittymät. Samalla myös yksipuoluejärjestelmässä kansan pitää silti hyväksyä turvallistamisen perustelu ja siitä seuraavat olosuhteet vähintään passiivisesti.

[16] Searlen luokittelu jakaa Austenin illokuutiot viiteen lajiin: toteamukset, direktiivit (esimerkiksi käskyt), komissiivit (lupaukset, uhkaukset), ekpressiivit (kiitokset, anteksipyynnöt) ja deklaraatiot (kuten sodan julistukset).

[17] Eng. strands of securitization.

Taulukko 1: Juha Vuoren turvallistamistyypit (2009)

Turvallista-mistyypit	**Aktin tyyppi (eng. elementary speech act sequence)**	**Illokuutio**	**Perlokuutio-tavoite**	**Aktin ja ajan suhde (eng. Temp-orality)**	**Tarvittava valta**
Asian nostaminen agendalle	Ehdottaa	Ohjeistus	Vakuuttaa yleisö	Tulevaisuus	Tulee argumentoida
Legitimoida tulevat toimet	Varoittaa	Ohjeistus	Legitimiteetti	Tulevaisuus	Tulee argumentoida
Pelote (Deterrence)	Julistaa	Julistus	Uhkaaminen tai pelottelu	Tulevaisuus	Julistus: vaatii muodollista auktoriteettia
Aiempien toimien legitimointi tai aiemman turvallisuus-tilan toistaminen	Selittää	Valtaa puolustava (eng. assertive)	Legitimiteetti	Menneisyys	Tulee argumentoida
Kontrolli	Vaatia	Ohjeistus	Tottelevai-suus tai kuri	Tulevaisuus	Vaatii muodollista auktoriteettia ja syyn

Ensimmäinen Vuoren luokittelema turvallistamisen tyyppi on *asiakysymyksen nostaminen agendalle*. Käytännössä tämä turvallistamisen tyyppi on ehto tuleville turvallistamisen vaiheille, sillä juuri agendalle nostamisella luodaan pohja turvallistamistoimien perusteluille. Samalla agendalle nostaminen ei automaattisesti vaadi muodollista auktoriteettiasemaa. Esimerkiksi erilaiset asiantuntijat,

organisaatiot tai kansalaisryhmittymät voivat nostaa aiheita agendalle ja tehdä niistä turvallisuuskysymyksiä (ibid, 76), mikäli heillä on tarpeeksi sosiaalista pääomaa (Boardieu teoksessa Vuori 2008, 77). Edellä mainitun pohjalta *agendalle nostamisessa* turvallistamisen yleisönä voivat toimia siis esimerkiksi myös päättäjät, turvallistajan ollessa esimerkiksi asiantuntija tai julkisuuden henkilö. Turvallistamistyypin tavoite on vakuuttaa yleisö turvallisuusuhan olemassaolosta. Tällöin uhka nostetaan agendalle ja tavoitteena on saada ehdotetut uhkaa torjuvat toimet täytäntöön (ibid, 77). Turvallistamista voidaan tehdä tässä tyypissä esimerkiksi väitteen tai varoituksen muodossa (”Jos emme tee toimia X, Y aiheuttaa Z”).

Toinen Vuoren turvallistamistyypeistä pohjaa Wæverin määritelmään *tulevien toimien legitimoimisesta*. Tässä turvallistamistyypissä yleisönä ovat turvallistajan legitimiteetin arvioijat, kuten äänestäjät, muut poliittiset ryhmät tai lehdistö. Pyrkimyksenä on vakuuttaa yleisö uhasta ja perustella sen torjuntaan tarkoitetut toimet (”Jotta uhka Y ei aiheuta tuhoa Z, meidän tulee tehdä toimet X”). Tällöin toimet Y ovat useimmiten toimia, jotka normaalitilan vallitessa eivät olisi legitiimejä. Tässä turvallistamisen tyypissä yleisöllä on selkeä mahdollisuus olla hyväksymättä turvallistamistoimien legitimiteettiä. Hylkääminen voi koskea joko itse uhkan olemassaoloa tai vakavuutta, tai uhkaan kohdistuvien toimien suhteellisuutta. Toisin sanoen mikäli toimet X koetaan ylimitoitetuksi uhkaan Y nähden, ei turvallistaminen välttämättä onnistu ja turvallistamisen yleisö ei myönnä legitimiteettiä suunnitelluille toimille. (Vuori 2008, 78)

Tulevien toimien legitimoinnin kaltaisena turvallistamistyyppinä voidaan pitää *pelotetta*.[18] Tällöin turvallistamisen tarkoituksena ei niinkään ole legitimoida tiettyjä toimia vaan luoda pelote seurauksista, jotka toimijalla on käytettävissään. Puhujan tarvitsee tässä tapauksessa tarvittavan auktoriteettiaseman, jotta hänellä on kykyä panna puheaktin sisältämä pelota täytäntöön. Toisin kuin legitimoivalla turvallistamisella, *pelote* kohdistuu suoraan turvallistettavaan uhkaan (esimerkiksi toinen valtio tai jokin valtion sisäinen ryhmittymä). Tällöin ei siis sinänsä haeta konkreettista hyväksyntää esimerkiksi omilta kansalaisilta, jos turvallistamisen sisältämä uhkaus kohdistuu valtion ulkopuoliseen toimijaan (Vuori 2008, 80). Samalla on kuitenkin perustelua olettaa, että vaikka turvallistamisen puheakti kohdistuisi turvallistamisen kohteeseen sisältää se myös itsessään legitimoivia pyrkimyksiä oman määräysvallan tai vaikutuspiirin yleisöä kohtaan.

[18] Eng. deterrence.

Yllä mainitut turvallistamistyypit painottuvat tulevaisuuteen, mutta myös menneisyyttä ja tapahtunutta voidaan turvallistaa jälkikäteen. Tällöin turvallistamisessa on kyse joko turvallistamisen tilan ylläpitämisestä tai toistamisessa. Tätä turvallistamista Vuori (2008) kutsuu *menneiden tapahtumien legitimoimiseksi*. Jo tapahtuneille kyseenalaistetuille toimille voidaan turvallistaa perusteluja tai turvallistamisen yleisöä voidaan muistuttaa uhan olemassaolosta, mikäli turvallistajan normaaleissa olosuhteissa ei hyväksyttävien turvallisuustoimien legitimoimiseksi (ibid.) Tällöin turvallistamisen pohjalla on väite tai toteamus, että menneet (normaaleissa olosuhteissa epälegitiimit) toimet X tehtiin, jotta akuutti uhka Y voitiin torjua.

Internetin informaation hallintaa tarkasteltaessa puhutaan ensisijaisesti nimenomaan kontrolliin tähtäävästä turvallistamisesta. Internetin avulla tietoa on mahdollista levittää ennennäkemättömän nopeasti ja ennennäkemättömän laajalle. Jos samalla oletetaan, että vapaa informaatio on problemaattista totalitaariselle hallinnolle, tulee informaation kulun hallinnointi keskeiseksi hallinnon turvallisuutta uhkaavaksi tekijäksi. Samalla informaatio liikkuu tällöin hallinnan kohteiden (eli kansalaisten) välillä, mikä tarkoittaa että informaation kontrolli tulisi kyetä perustelemaan, eli turvallistamaan, riittävän vakuuttavasti. Kontrolliin tähtäävän turvallistamisen tavoite on tuottaa sanotun *seurauksena* tottelevaisuutta suhteessa turvallistajan asettamiin sääntöihin. Toisin sanoen saada kansalaiset tekemään tai olemaan tekemättä haluttuja asioita (Vuori 2008, 88-92). Tällöin turvallistajan tulee olla muodollisessa valta-asemassa ja tämä turvallistoimien yleisönä ovat esimerkiksi hallinnon jäsenet tai kansalaiset yleisesti. Vuoren (ibid.) luokittelussa kontrolliin tähtäävä turvallisuustoimi ei sisällä neuvotteluvaraa, minkä vuoksi turvallistajan ja turvallistamisen kohteiden suhde tulee olla hierarkkinen. Tällöin kansalaisen tulee joko toimia tietyllä tavalla tai pitäytyä toimimasta tietyllä tavalla, jotta valtiota tai yhteiskuntaa kohtaavalta uhkalta voidaan puolustautua.

Samoin kuin turvallistamisessa on eri tyyppejä, on myös eri kielten ja kulttuurien merkitys sanalle *turvallisuus* nyansoidumpi kuin pelkkä suora käännös. Eri kulttuureissa Euroopan sisällä, puhumattakaan Euroopan tulkintojen ja Kiinan välillä, on eriäviä konnotaatioita ja perinteitä turvallisuuden konseptin ympärillä. Siinä missä Euroopassa turvallisuus mielletään pääsääntöisesti turvallisen ja vahingolta tai väkivallalta suojelemisen konseptien kautta, on Kiinan turvallisuuden konsepti pikemmin kytköksissä vakauden ajatukseen (Vuori 2011, 224). Kiinassa voidaan puhua turvallistamisen konseptin sisään kuuluvista asioista mainitsematta sanaa *turvallisuus* ja sen sijaan painottaa nimenomaan *vakautta* (ibid 224). Vakaus ja tietynlainen muuttumattomuus turvallisuuden ydinajatuksena luo erilaisen turvallisuusparadigman kuin turvallisuusajattelu, jonka lähtöpisteenä on

itsessään väkivalta tai muu fyysisen vahingon vaara. Kontrollin turvallistaminen on ensin mainitussa huomattavasti luonnollisempi osa koko turvallisuuden ajatusta kuin turvallisuusajattelussa, joka ei niinkään suojele järjestelmää itsessään vaan pikemmin valtiota kansalaisineen. Toki kullakin järjestelmällä on omat reunaehdot, joiden sisällä vakaudesta tulee itseisarvo. Esimerkiksi demokraattiseen järjestelmään kohdistuva epädemokraattinen uhka voi kohdata samankaltaisia toimia kuin kommunistisen järjestelmän asemaa vaarantaviksi koetut ilmiöt Kiinassa. Yhdysvalloissa ja Euroopassa vastaavista esille ovat nousseet varsinkin terrorismin torjuntaan kohdistetut toimet.

Kiinassa turvallisuuden ja sisäisen järjestyksen suhteella on pitkä historia, joka on värittänyt monen poliittisen aikakauden tapahtumia (Vuori 2011, 224). Vuori arvioi vakauden konseptin olevan osa kiinalaisten *kollektiivista muistia,* jota toisinnetaan kiinalaisessa kulttuurissa. Sekä Kungfutselaisuuden että Kiinan kommunistisen puolueen eetoksissa vahva johtaja on keskeisessä roolissa harmonian ja yhteiskunnan järjestyksen (ja samalla turvallisuuden) ylläpitämisessä (Pye teoksessa Vuori 2011, 224). Tämä runsasta päätäntävaltaa nauttivan johtajan asema voidaan osaltaan tulkita olevan jatkumoa kungfutselaisuudessa esitetyllä isän asemalla perheyksikössä, jossa isällä on ehdoton auktoriteettiasema. Tällöin kansa on perhe, jota johtaja johtaa perheen isän arvovallalla ja kansa on kuuliaisten perheenjäsenten roolissa. Perheen taas tulee olla yhtenäinen ja kuuliainen menestyäkseen. Tästä johtuen epäjärjestyksen pelko on osaltaan johtanut ideologisen yhtenäisyyden ylikorostumiseen kiinalaisessa kulttuurissa (Vuori 2011, 225). Informaation aiempaa nopeamman ja laajemman leviämisen takia internet ja sen valtion sisäisiä jakoviivoja paljastavat kirjoitukset ja uutisointi (esimerkiksi uiguuri-vähemmistön tilanne) muodostavat konkreettisen uhan yllä mainitulle yhtenäisyyden ja harmonian tavoittelulle. Kiinan kansan kokoisen suuren väestön yhtenäisen ja harmonisen identiteetin ylläpitäminen useimmiten vaatii eriävien näkemysten alistamista (ter Haar teoksessa Vuori 2011, 225).

Kommunistisen järjestelmän suojelemiseksi ja niin sanottu vasta-vallankumouksellinen toiminta määriteltiin rikokseksi 1979 (Vuori 2011, 227). 1990-luvulla lakia täsmennettiin sanamuotoon *kansallista turvallisuutta* uhkaava toiminta, mutta pohjalla vaikuttaa yhä ideologinen turvallistettu Maon (Vuori 2011, 229) toteamus: ”Kansallinen järjestelmämme, kansan demokraattinen diktatuuri, on vahva turvaamaan kansan vallankumouksen voiton hedelmät sekä suojaamaan meitä

vastavallankumouksellisilta voimilta niin maamme sisältä kuin sen ulkopuolelta. Tätä asetta meidän on käytettävä."[19]

Kiinan internetsensuurin osalta Liang (2010, 106) havainnoi yhdeksän keskeistä Kiinan hallituksen harjoittaman sensuurin kategoriaa: "a) Kiinan perustuslain, lakien tai hallinnollisissa asetuksien vastainen sisältö; b) sisältö joka yllyttää valtion hallintoa tai sosialistisen järjestelmää vastaan; c) vahingoittaa valtion voimaa tai valtion yhtenäisyyttä; d) yllyttää etnisiä jännitteitä, rotusyrjintä tai vahingoittaa etnistä yhtenäisyyttä; e) levittää juoruja tai vahingoittaa kansallista järjestystä; f) edistää feudaaleja uskomuksia; levittää sopimatonta sisältöä, pornografiaa tai uhkapelaamista; synnyttää väkivaltaa, murhia tai terroritekoja; yllyttää muita rikkomaan lakeja; g) julkisesta loukkaa tai halventaa muita; h) vahingoittaa valtion mainetta tai intressejä; i) sisältää lain tai sääntöjen kieltämää materiaalia." Suurin osa näistä esitetyistä internetin sensuurin kohteista eivät sinänsä poikkea Euroopan viitekehyksestä. Turvallistamisen kannalta on kuitenkin olennaista myös, mihin näiden kategorioiden sisällä vedetään tulkinnallisia rajoja. Nämä kategoriat muotoillaan siis tavalla tai toisella uhkaksi valtiolle tai järjestykselle, mikä osaltaan vastavuoroisesti vaikuttaa Kiinan tapauksessa sisältyvän kansallisen uhkan määritelmään. Näiden kategorioiden osalta ainoa turvallistettava tekijä ei ole kuitenkaan itse kategoria vaan samalla myös kynnys, jonka ylitettyään sisältö on tulkittavissa turvallisuutta uhkaavaksi. Esimerkiksi millainen sisältö vahingoittaa kansallista yhtenäisyyttä tai valtion mainetta? Milloin median uutisointi tai sosiaalisessa mediassa levitettyä informaatiota tulee tulkita juoruna verrattuna hyväksyttävään uutisointiin? Sen lisäksi että turvallistaminen kohdistuu eri kategorioihin määrällisesti, tulisi turvallistamisen myös onnistua laadullisesti kategorioiden sisällä. Se mitä sensuroidaan ei siis itsessään ole vielä turvallistamistoimen kokonaiskuva vaan sensuurin tiukkuus kategorioiden sisällä on myös itsessään turvallistamista. [20]

[19] Oma käännös englannikielisen käännöksen pohjalta: "Our state system, the people's democratic dictatorship, is a powerful weapon for safeguarding the fruits of victory of the people's revolution and for thwarting the plots of domestic and foreign enemies for restoration, and this weapon we must firmly grasp."

[20] Oma käännös, eng.: (a) is contrary to the basic principles that are laid down in the Constitution, laws, or administration regulations; (b) is seditious to the ruling regime of the state or the system of socialism; (c) subverts state power or sabotages the unity of the state; (d) incites ethnic hostility or racial discrimination, or disrupts racial unity; (e) spreads rumors or disrupts social order; (f) propagates feudal superstitions; disseminates obscenity, pornography, or gambling; incites violence, murder, or terror; instigates others to commit offences; (g) publicly insults or defames others; (h) harms the reputation or interests of the state; or (i) has content prohibited by laws or administrative regulations.

3. NYKYTILA KIINAN INTERNETPOLITIIKASSA

Tässä luvussa esittelen Kiinan internetpolitiikan käytännön muutoksia Presidentti Xin aikakaudella. Aloitan erittelemällä ja esittelemällä aineistoni sekä aineistoon liittyviä huomioita. Esiteltävät muutokset olen jakanut erillisiin sektoreihin, joita käsittelen tarkemmin suhteessa turvallistamisen teoriaan luvussa 4.

3.1. Aineisto

Tutkittaessa informaation rajaamista valtiossa, joka rajaa nimenomaan poliittista informaatiota on aineiston keräämiselle tiettyjä luonnollisia haasteita. Kiinassa kirjoitettua tutkimusta ja aineistoa on vaikea tavoittaa, sillä valtio on varsin vähäsanainen omista toimistaan internetin säätelyyn liittyen. Toisaalta vahvasti sisäiselle yleisölle suunnatut lausunnot saattavat olla tavoitettavissa vain kiinan kielellä.

Tiedostaen edellä mainitut haasteet olen tässä tutkimuksessa käyttänyt pääosin Manner-Kiinan ulkopuolelta Kiinaa seuraavia uutislähteitä. Artikkeleilla ja uutisoinneilla mahdollisine viranomaisenlausuntoineen on keskeinen rooli tutkimuksessani. Laajimmin Kiinan sensuuripolitiikkaa päivittäisessä uutisoinnissaan käyttää China Digital Times, joka raportoinnin ohessa julkaisee myös vuodettuja kiinalaisen lehdistön saamia informaatio-ohjeistuksia. Koska nämä ohjeistukset sisältävät suoria viitteitä informaation hallintaan ja sensuurin otan alla olevissa luvuissa myös näitä huomioon. On syytä huomioida että China Digital Times on Yhdysvalloista käsin operoiva toimija, jonka oma neutraalius suhteessa uutisoimiinsa ilmiöihin on kyseenalainen. Muita keskeisiä uutislähteitä ovat olleet eri kansainväliset uutostoimijat, kuten BBC ja Wall Street Journal. Uutislähteet toimivat aineiston osalta ensisijaisesti lähteinä määrittämään konkreettisia muutoksia Kiinan internetpolitiikassa.

Kiinan tutkimuksen aikana voimaan saatetuista kansallisesta turvallisuuslaista sekä kyberturvallisuuslaista käytän aineistona epävirallista China Law Translate -sivuston käännöstä. Aineistona näiden käännösten osalta on ilmeistä pitää varauksia käännösten sanamuodoista, mikä toki koskisi myös virallisia käännöksiä. Lähden tutkimuksessani kuitenkin siitä olettamuksesta, että käännökset antavat riittävän perusteelliset lähtökohdat arvioida lakialoitteiden sisältöä turvallistamisen näkökulmasta. Käsittelen analyysissä kybertuvallisuuslain sisältämiä kohtia informaatiosta ja informaatiota käsittelevien pykälien turvallistavaa retoriikkaa. Kyberturvallisuuslain suorat viittaukset

informaation ja kansallisen turvallisuuden suhteesta, ovat tutkimuksen ja turvallistamisen teorian kannalta keskeisin lain sisältö. Laki itsessään kattaa myös verkkoturvallisuutta teknisemmässä mielessä, sisältäen erilaisia tietoverkkojen perinteiseen turvallisuuteen liittyviä artikloja, mutta informaation hallinnan ja turvallistamisen kannalta nämä ovat tutkimukselle vähemmän olennaisia. Lakiuudistusten lisäksi hyödynnän aineistona on Yhdysvaltojen viranomaisten julkisia raportteja Kiinan internetpolitiikasta.

Aineistossani olen myös hyödyntänyt Freedom Housen internetin vapautta mittaavia raportteja sekä China Internet Watchin tilastoja kiinalaisten internetin käytöstä. Nämä raportit toimivat myös indikaattorina, kun vertaan Kiinan informaatiohallintaa EU-maiden ja Yhdysvaltojen internetpolitiikkaan.

3.2. Poliittiset muutokset

Internetin käyttäjien määrän kasvu Kiinassa on ollut räjähdysmäistä. Vuoden 2006 heinäkuussa Kiinan internet verkon informaatiokeskus (CNNIC) ilmoitti internetkäyttäjiä olevan 123 miljoonaa (Wu 2007, s143), kun taas heinäkuussa 2015 vastaava lukema oli 668 miljoonaa (Kaavio 1).[21] Nopea kasvu on luonut Kiinan kommunistiselle puolueelle uusia haasteita sen pyrkimyksissä ylläpitää kontrolloitua informaatiokulkua ja sisäpoliittista vakautta.

Vuoden 2014 helmikuussa Kiinan hallintoon luotiin uusi itsenäinen internetin valvontaan keskittyvä elin, Kiinan kyberhallinto (CAC)[22] (Global Times 20.11.2014). Organisaatio on linkittynyt johtajansa Lu Wein kautta Presidentti Xin johtamaan Internetturvallisuuden ja infromatisaation johtoryhmä.[23] Käytännössä tämä tarkoittaa, että CAC vastaa suoraan Presidentti Xille.[24] CAC on perustamisensa jälkeen toiminut varsinkin kyberulottuvuuden linjavetojen äänitorvena ja kyberpolitiikan toimeenpanevana elimenä. Johtaja Lu Wei on tavannut useita läntisen yritysmaailman edustajia, kuten Facebookin Mark Zuckerbergia (Bloomberg 8.12.2014).

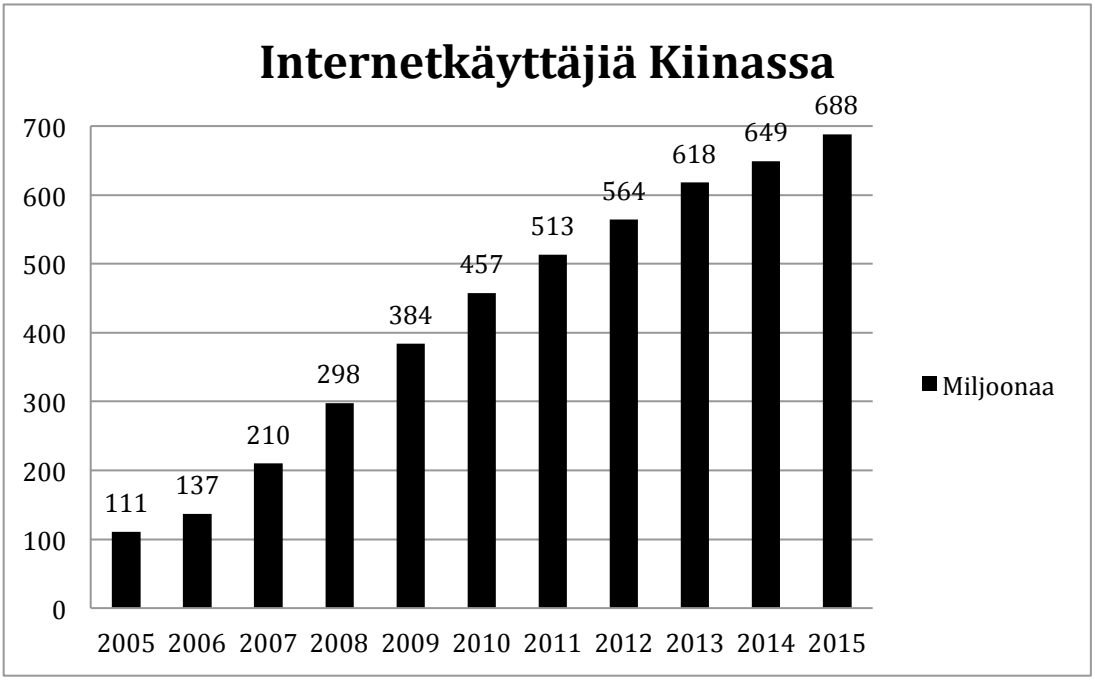
[21] CNNIC 36th Report on Internet Development in China.

[22] Cyberspace Administration of China.

[23] Central Leading Small Group on Internet Security and Informatization.

[24] CAC:n kotisivut http://www.cac.gov.cn/english/.

Kaavio 1: Internetkäyttäjien määrä Kiinassa (China Internet Watch).



Kaavio 2: Internetkäyttäjien prosenttiosuus väestöstä (China Internet Watch).

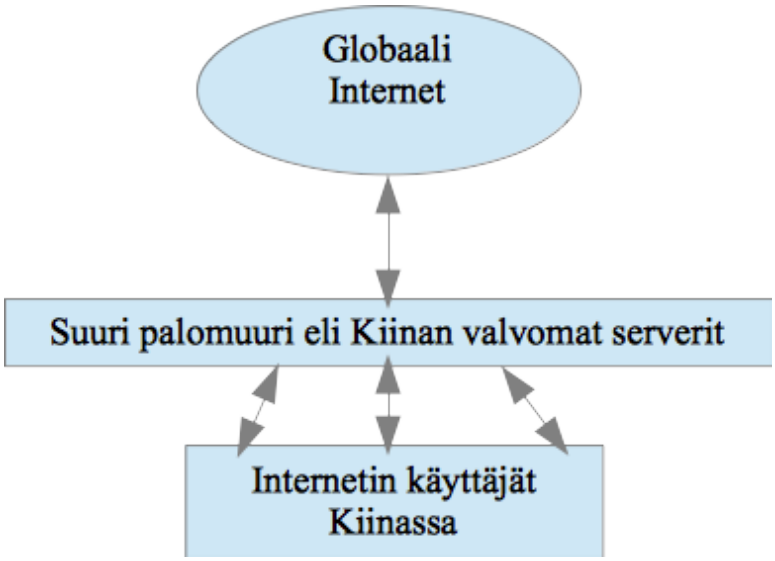
CAC:n ja Lu Wein keskeinen tehtävä onkin nimenomaan löytää tasapaino, jossa ei-toivotut nettisivut estetään ja sosiaalisessa mediassa liikkuva informaatio pystytään kontrolloimaan. Samalla tulisi kuitenkin mahdollistaa riittävästi liikkumatilaa taloudelliselle kasvulle (New York Times 1.12.2014). Yleisen mielipiteen ohjaamisessa CAC on tehnyt retorisia siirtoja,[25] joiden avulla internetissä tavoitettava informaatio ja sosiaalinen media ovat yhteydessä kansalliseen turvallisuuteen. Presidentti Xin presidenttikauden aikana Kiina on luonut sekä uuden kyberturvallisuuslain (China Law Translate) että kansallisen turvallisuuslain (China Law Translate). Muun muassa Amnesty international on kritisoinut lakeja niiden kansallisen turvallisuuden uhkien epätarkkuudesta, mikä mahdollistaa niiden tulkinnan hallituksen mielihalujen mukaan (China Digital Times 7.5.2015). Samalla uudet lait linkittävät kyberturvallisuuden ja kyberulottuvuuden informaation eksplisiitisti osaksi kansallisen turvallisuuden perustaa. Tavoitteeksi ilmaistaan turvata ja edistää kommunistisen puolueen moraaleja ja arvoja (China Digital Times 1.7.2015). Gierow (2014, 1) arvioi ettei Kiinalla ennen CAC:n perustamista ollut varsinaista koherenttia kyberpolitiikkaa, mutta viimeistään CAC:n ja Presidentti Xi Jinpingin johtaman kyberturvallisuudesta vastaavan johtoryhmän perustaminen ovat tuoneet kyberulottuvuuden mukaan Kiinan turvallisuuspolitiikan keskiöön. Lu Wei edustaa uutta turvallisuus- ja propaganda-ajattelun sukupolvea. Lu on osoittanut edeltäjiään ajankohtaisempaa tietämystä internetin ja sosiaalisen median vaikutuksista sekä sisäisestä logiikasta ja on näin itsessään ollut merkittävä muutos Kiinan kyberulottuvuuden informaatiopolitiikassa (New York Times 1.12.2014).

Kiina on aiempaa aggressiivisemmin puuttunut internetissä lehdistössä ja sosiaalisessa mediassa julkaistuihin juoruihin. Ongelmalliseksi tilanteen tekevät esimerkiksi lehdistöön kohdistuvat uudet lait, joiden perusteella valtion linjasta poikkeava uutisointi voidaan laskea juoruiksi (kts. Luku 3.1.). Iso-Britannian ja Kiinan viidennen internettapaamisen yhteydessä antamassaan puheessa Lu Wei rinnasti toimet juoruja vastaan pidätyksiin, joita Britanniassa oli tehty yksittäisiä henkilöitä kohtaan tehtyjen tappouhkausten perusteella (Xinhua 9.9.2013). Rinnastuksen avulla tarkoitus lienee verrata kansallisen vakauden ja ideologisen yhtenäisyyden turvallisuusimplikaatioita väkivaltaan tai sen uhkaan, mihin Euroopassa puututaan myös kyberulottuvuudessa

CAC:n perustamisen jälkeen Kiinan internetin kautta välitettävään informaatioon kohdistuvat toimet ovat voimistuneet. Kiinan suuren palomuurin on aiemmin voinut kiertää suhteellisen vaivatta niin

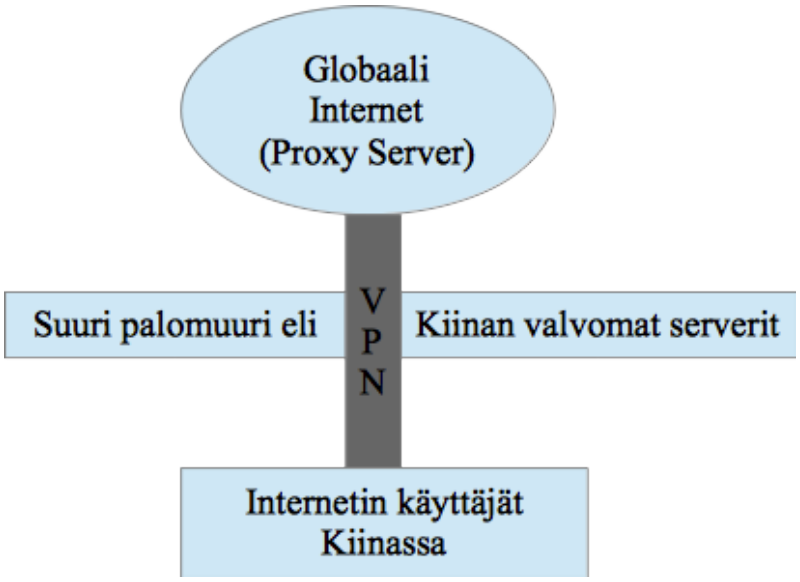
[25] Esimerkiksi Xi Jinpingin toteamus, ettei ilman kyberturvallisuutta ole kansallista turvallisuutta (Gierow 2014, s1). Kyberulottuvuuteen liittyvät toimet on toistuvasti perusteltu kansallisen turvallisuuden ja yhteiskuntarauhan nojalla.

sanotulla virtuaalisella erillisverkolla (VPN),[26] mutta 2015 vuoden alussa palomuuriin tehty päivitys esti VPN palvelujen käyttämisen muille kuin yksittäisille lisensoiduille toimijoille (Wall Street Journal 30.1.2015). VPN-yhteyksien sulkeminen vaikeuttaa yhtäältä ulkomaalaisten yhteydenpitoa Kiinan ulkopuolelle ja toisaalta yksityistä, akateemista ja ammatillista tiedonhakua ulkomaisille ja kiinalaisille toimijoille (kts. osio sosiaalinen media ja hakukoneet). Muita CAC:n perustamisen jälkeen tehtyjä toimia ja linjamuutoksia vaikutuksineen on eritelty seuraavissa luvuissa.



Kuva 1: Internetiin yhdistyminen Kiinassa

[26] Virtual Proxy Network. VPN rakentaa suojatun yhteyden käyttäjän ja palvelun serveripisteen välille, jolloin tämän tietotunnelin läpi kulkeva data ei ole luettavissa ulkopuolelta ja on aikaisemmin ollut näin ollut myös Kiinan suuren palomuurin ulottumattomissa (Vertaa Kuva 1 ja Kuva 2).



Kuva 2: Virtual proxy server luo suljetun datatunnelin, joka yhdistää käyttöpisteen suoraan palomuurin toiselle puolelle serveriin ilman palomuurin sensuurimekanismeja. Kryptattu yhteys pystyy myös suojaamaan datatunnelin läpi virtaavaa dataa.

3.3. Uutiset internetissä

Internet ja sen avaama informaatiokenttä on hallitsemattomuudessaan helposti uhka mille tahansa Kiinan hallinnon kaltaiselle vahvasti hierarkkiselle ja keskitetylle valtarakenteelle. Kiinan hallinto on mukautunut tähän haasteeseen osaltaan muuttamalla perinteistä hallintamenetelmäänsä (Wu 2007, 137). Vertikaalista valtarakenteesta on siirrytty koordinoituun horisontaaliin rakenteeseen tiedon jakamisessa kiinalaisille internetissä toimiville tietolähteille (Wu 2007, 137). Tämä on käytännössä tarkoittanut sitä, että sivustot saavat saman informaation samoin muotoiltuna samanaikaisesti, ovatpa ne sitten valtion omistamia tai yksityisesti omistettuja toimijoita (Wu 2007, 137). Tätä hallintakeinoa tehostaa lisäksi se, että vain valtion internetissä toimivilla uutisorganisaatioilla on oikeus ensikäden tietojen hankkimiseen (Wu 2007, 139). Tällöin muilla verkkotoimijoilla on vaihtoehtona lähinnä kirjoittaa uutisia uuteen muotoon ja pienemmän puolueohjauksen takia uutisointi on näissä palveluissa usein liioittelevampaa huomioarvon lisäämiseksi (Wu 2007, 139). Ilmiönä suureellinen uutisointi ei

toki eroa esimerkiksi suomalaisesta kaupallisesta verkkouutisoinnista, mutta tiedonkeruuseen kohdistuvat rajoitukset ohjaavat vahvasti uutisten varsinaista sisältöä.[27]

Kiinan valtio on myös rajannut lukuisia ulkomaisia uutissivustoja palomuurin ulkopuolelle. Viimeisempänä listalle joutui Reuters, joka liittyi BBC:n, New York Timesin, Bloombergin, Wall Street Journalin ja Hong Kongista käsin julkaistavan South China Morning Postin seuraan estettyjen uutissivustojen joukossa (China Digital Times 25.3.2015). Rajoittamalla saavutettavia uutislähteitä ja uutisiin liittyviä avainsanoja Kiinan hallitus on pystynyt määrittämään poikkeuksellisen laajasti monen uutisaiheen leviämisen. Hong Kongin sateenvarjoprotestien mittakaavaan nähden aiheen uutisointi oli kiinalaisessa mediassa lähes olematonta ja samaan aikaan sekä uutis- että sosiaalisen median sivustojen sensuuria kiristettiin. Kiinasta käsin saavutettava tieto ja siten yleinen tietoisuus Hong Kongin protesteista oli lopulta erittäin niukkaa. Tapaus antoi viitteitä Kiinan sensuurimenetelmien vaikuttavasta tehokkuudesta.

Lehdistön koskemattomuutta arvioiva ja turvaava Committee to Protect Journalists (CPJ) (30.10.2015) raportoi rikoslakimuutoksesta, jonka nojalla jatkossa toimittajat sekä bloggaajat joutuvat aiempaa ahtaammalle. Jatkossa vääriä tietoja katastrofeista tai epidemioista julkaisevat kirjoittajat voivat saada jopa seitsemän vuoden vankeustuomioita. Samaan lisäykseen sisältyy myös tahallinen yhteiskunnallista järjestystä horjuttavien väärien tietojen tietoinen levittäminen. Ongelmallinen tulkinnanvaraisuus asettaa journalistit alttiiksi tuomioille, jos esimerkiksi uhritilastot tai tapahtumakulut heidän uutisoinnissaan eivät vastaa valtion virallista linjaa. Kiina on nykyisellään määrällisesti eniten toimittajia vangitseva valtio ja uusi laki antaa aiempaa laveammat työkalut internetin pienempien toimijoiden uutisoinnin ohjaamiseen. Lain puitteissa luettavia syytteitä ovat esimerkiksi juorujen levittäminen tai riidan haastaminen ja ongelmien provosointi (CPJ 30.10.2015). Hallinnan ollessa erittäin tiukkaa, on uutistoimijoilla varsin vähäiset mahdollisuudet todentaa omat selvityksensä oikeiksi, mikäli toimija joutuu tutkinnan kohteeksi. Väärän tiedon levittämisen rangaistavuus rajoittuu CPJ:n mukaan kuitenkin nimenomaan poliittisesti arkaluontoisiin tai kiusallisiin aiheisiin ja on näin ollen lähinnä poliittinen työkalu, jolla estää valtion linjasta poikkeavia mediadiskursseja.

[27] Kiina on vuonna 2017 tarkentanut säädöksiä internetissä julkaistavia uutisia koskien (BBC 3.5.2017). Uudet säädökset koskevat verkkosivuja, applikaatioita, foorumeita, blogeja, mikroblogeja, julkisia käyttäjätilejä, pikaviestimiä sekä internetlähetyksiä. BBC:n mukaan organisaatioilla, joilla ei ole toimintalisenssiä, ei ole oikeutta julkaista uutisia ja kommentoida hallitusta, taloutta, armeijaa, ulkopolitiikkaa tai muita *yhteiskunnallisen kiinnostuksen* kohteita. Edelleen vain valtion rahoittamilla toimijoilla on oikeus tehdä omia reportaaseja.

3.4. Sosiaalinen media ja hakukoneet

Kiinan valtio on rajannut lukuisia länsimaisia sosiaalisen media sivustoja sekä esimerkiksi hakukonejätti Googlen palvelut laillisesti saavutettavien sivustojen ulkopuolelle. Eurooppalaiselle käyttäjälle tuttuja ovat esimerkiksi palvelut Facebook, YouTube, Tumblr ja Twitter, joihin pääsy Kiinassa on estetty.

Perusteluna sivustojen estämiselle viranomaiset ovat usein käyttäneet näiden yritysten vastahakoisuutta taipua Kiinan valtion lakeihin ja vaatimuksiin. Näihin lukeutuvat muun muassa käyttäjien tietojen luovuttaminen, palveluiden fyysisten palvelinten sijoittaminen Kiinan kansalaisten osalta Kiinan alueelle sekä mahdollisuus hallinnoida palveluissa julkaistavaa sisältöä (New York Times 1.12.2014). Xi Jinping ja muun muassa Kiinan ulkoministeriön lehdistövastaavat ovat toistuvasti todenneet Kiinan olevan lähtökohtaisesti avoin ja vastaanottava kaikille yrityksille, jotka haluavat tulla Kiinan, kunhan nämä toimivat Kiinan haluamalla tavalla (Wall Street Journal 22.9.2015). Näistä ehdoista kieltäytyvien yritysten katsotaan toimivan Kiinan intressejä ja vakautta vastaan. Ulkomaalaiset yritykset asemoidaan näissä lausunnoissa Kiinan intressien ja turvallisuuden kannalta uhaksi, mikäli ne eivät mukaudu poikkeuksellisiin turvallisuusjärjestelyihin.

Kiinan internetkenttä ei kuitenkaan ole tyhjiö sosiaalisen median osalta, vaan globaalien palveluiden sijaan kiinalaiset yhtiöt ovat luoneet kansalliset vastineet Suomessa tutuille sivustoille. Mikroblogi-palvelu Twitterin sijaan käytössä on Weibo, jolla kuukausitasolla on arviolta 222 miljoonaa käyttäjää (China Internet Watch 20.11.2015). Viestiohjelma WhatsAppin sijaan Kiinassa toimii WeChat, joka on saanut lisääntyvässä määrin suosiota myös Kiinan ulkopuolella. Kuukausitasolla aktiivisia käyttäjiä arviolta 650 miljoonaa (China Internet Watch 16.11.2015). Lähimpänä Facebookin ominaisuuksia vastaa sivusto Renren, jonka kuukausittain aktiivisten käyttäjien määrä oli vuoden 2014 lopulla arviolta 219 miljoonaa (China Internet Watch 24.11.2014).

Kiinan hallitus on onnistunut luomaan tilanteen, missä globaalien sosiaalisen median sivustojen käytön tarve ja houkutus on pystytty minimoimaan. Kun sisäiset markkinat ovat valtavat ja kontakti ulkomaihin rajallinen, ei vain palo- vaan myös kielimuurin takia, ei Facebookin kaltaisille kontaktien varaan rakennetuille sosiaaliselle applikaatiolla ole kansalaiselle juurikaan käyttöä kansalliseen vaihtoehtoon verrattuna. Näin Kiina on pystynyt rajamaan suuren taloudellisen siivun sosiaalisesta

mediasta kokonaan omien markkinoiden käyttöön. Samaan aikaan en tutkimukseni yhteydessä löytänyt viitteitä tai esimerkkejä siitä, että kiinalaiset palvelut kohtaisivat minkäänlaisia rajoituksia muualla maailmassa ja esimerkiksi WeChat on levinnyt hiljalleen kansallisen käyttäjäkunnan ulkopuolelle (China Internet Watch 16.11.2015).

Suurten käyttäjämäärien markkinoiden takia aiemmin mainitut länsimaiset yhtiöt ovat käyneet neuvotteluita Kiinan viranomaisten kanssa ehdoista päästä operoimaan Kiinassa. Toistaiseksi kuitenkin Kiinan viranomaisten asettamat ehdot esimerkiksi käyttäjien viestikeskustelujen lukemisesta ovat olleet liikaa (Independent 30.1.2015). Sitä vastoin valtion toimijoilla on pääsy kiinalaisten palveluntarjoajien kautta keskustelutietoihin ja käyttäjien henkilötietoihin. Lisäksi Kiinassa astui 2015 voimaan laki, jonka nojalla sivustojen käyttämiseksi ja materiaalin julkaisemiseksi on annettava täydet nimitiedot, mikä käytännössä poistaa anonyymin nettikirjoittamisen mahdollisuuden (South China Morning Post 8.7.2015).

Jo vuotta aikaisemmin niin sanotut viralliset profiilit olivat velvoitettuja henkilötietojen luovuttamiseen. Viralliset profiilit mahdollistavat esimerkiksi WeChatin kaltaisissa applikaatioissa syötteen seurannan, minkä avulla profiililla pystyy tavoittamaan massoja ja esimerkiksi bloggaajat sekä julkisuuden henkilöt käyttävät tätä profiilityyppiä. Samalla lakiin lisättiin myös uudistus, jonka nojalla vain Kiinan valtion hyväksymät viralliset uutistoimistot ja toimijat saavat jakaa poliittisia aiheita sisältäviä uutisia (Wall Street Journal 7.8.2014). Hallituksen virallinen linja on näillä uudistuksilla estää haitallisten ja vakautta uhkaavien juorujen leviäminen (South China Morning Post 8.7.2015).

Hakukoneista esimerkiksi Google on estetty kesästä 2014 Kiinassa kokonaan ja joulukuussa 2014 myös Googlen alaiset ohjelmat kuten Gmail ja Google Calendar estettiin (Independent 30.1.2015). Syynä Googlen estämiselle on mahdollisesti se, että Google on ollut vastahakoinen Kiinan hakutulosten sensuroimisen mahdollistamisessa sekä aiemmat kiistat Googlen videopalvelu YouTube-sivustoon liittyen (Independent 30.1.2015). Microsoftin Bing-hakukone on käytettävissä Kiinassa, mutta tämä selittyy kahdella keskeisellä tekijällä: 1) Microsoftilla on yhteistyösopimus kiinalaisen hakukonejätti Baidun kanssa ja 2) Microsoft on ollut myöntyväinen sensuuritoimiin (Business Insider UK 24.9.2015, The Guardian 11.2.2014). Suurista hakukoneista Kiinasta käsin tällä hetkellä käytössä ovat siis vain Baidu ja Bing. Pienempien hakukoneiden käytettävyys ei ole luotettavaa, esimerkiksi DuckDuckGo on pääosin estetty Manner-Kiinassa (Cnet 22.9.2014).

3.5. Ulkomaalaiset yritykset

Kiinan ulkopuolelle suljetut IT-yritykset eivät ole ainoa ulkomainen kärsijä yritystoiminnassaan Kiinassa. Euroopan Kiinan kauppakamarin jäsenilleen teettämän kyselyn mukaan, jopa 86 prosenttia eurooppalaisista yrityksistä kokee merkittävää haittaa Kiinan internetsäännöksistä ja sen vaikutuksista internetin käytettävyyteen (Euroopan kauppakamari 12.2.2015). Samassa kyselyssä 80 prosenttia vastaajista arvioi ongelmien lisääntyneen vuoden 2015 alussa, uusien sensuurin kiristystoimien seurauksena.

Vuotta aiempaan nähden Kiina oli tehnyt uuden kansallista turvallisuutta koskevan lain (South China Morning Post 8.7.2015), joka yhtäältä kiristi sensuuritoimien mittakaavaa ja toisaalta sisälsi yritystoimintaan suoraan vaikuttavia kohtia. Pelkkien internetongelmien lisäksi vastauksiin vaikuttanee muun muassa Kiinalle kriittisten alojen tuottajien tietoverkkoihin standardoituja turvallisuusvaatimuksia ja tuotteiden arviota ennen niiden markkinoille pääsyä (South China Morning Post 8.7.2015). Ulkomaisten yritysten kannalta tämä sisältää kaksi keskeistä ongelmaa: tuotteiden suunnittelutason jakaminen Kiinan valtiolle sekä firmojen verkkojen koodin avaaminen turvallisuusstandardien täyttämiseksi. Yhtenäinen suojauskoodaus voi South China Morning Postin (8.7.2015) professori Hargreavesin[28] mukaan myös todellisuudessa helpottaa tietomurtoja. Tämä voi myös osittain selittää, miksi kyselyssä 13 prosenttia yrityksistä ilmoitti vähentävänsä tutkimus- ja kehitystoimintaansa Kiinassa.

Edellä mainittujen lakiongelmien ohella ja tämän tutkimuksen kannalta keskeisempää on kuitenkin nimenomaan internetin käyttöön liittyvät ongelmat. 57 prosenttia Euroopan kauppakamarin kyselyyn vastanneista koki estettyjen sivujen haittaavan heidän liiketoimintaansa (China Digital Times 10.6.2015). 21 prosenttia vastaajista arvioi yhteysongelmien laskevan yritystensä tehokkuutta, kun taas 34 prosentin mielestä Kiinan internetrakenteiden takia asiakirjojen ja tietojen vaihto yhtiöiden päämajojen kanssa on normaalia hankalampaa (Wall Street Journal 10.6.2015). Nämä toimintaa rajoittavat infrastruktuuriset tekijät yhdistyvät lähtökohtaisestikin suhteellisen protektionistiseen sisämarkkina-alueeseen, missä kansainvälisten yritysten toiminta on usein vaikeaa. Kiina voi valtavista sisämarkkinoistaan huolimatta ajan myötä ajautua tilanteeseen, missä sen on parannettava kansainvälisten yritysten tietoverkkoinfrastruktuuria tai kärsittävä taloudellisia tappioita.

[28] Hong Kongin yliopistossa työskentelevä kansainvälisen oikeustieteen professori, joka on erikoistunut teknologia- ja internetlainsäädäntöön.

Yhteyden vakaus ja yhteysnopeuden ongelmat [29] ovat yhdistettävissä palomuurin toimintaan. Palomuurin ja raskaan blokkaustoiminnan mahdollistamiseksi koko Kiinan internetyhteys ulkopuolelle toimii vain kolmen pääyhteysväylän kautta (Demchak ja Dombrowski 2011, 41). Ei siis ole yllättävää, että Kiinan internetkäyttäjien määrän huomioidessa yhteysnopeus on puutteellinen. Estoja kiertävät VPN-yhteydet taas operoivat saman verkon nopeuksien ehdoilla ja joutuvat kierrättämään signaalin, jolloin nopeusongelma korostuu entisestään.

Varsinaiset sivustojen ja palvelujen estot aiheuttavat omat ongelmansa. Ensinnäkin Googlen Gmail on yksi johtavia sähköpostipalveluita maailmassa ja on käytössä myös yrityksissä. Gmailin estäminen siis joko pakottaa yrityksen vaihtamaan sisäisen viestintänsä pois Googlen palvelusta tai olemaan jatkuvasti yhteydessä VPN-palvelun kautta. Ulkopuolisten sivustojen blokkaaminen vaikeuttaa oleellisesti myös tiedonhankintaa, mikä aiheuttaa omalta osaltaan turhautumista myös Kiinan kansallisissa yrityksissä (Euroopan kauppakamari 12.2.2015). Kiinan oman tulevaisuuden kannalta tämä voi aiheuttaa ikäviä seurauksia pidemmällä aikavälillä, sillä nykyisestä sisäisten markkinoiden menestyksestä huolimatta esimerkiksi Kiinalaisten tutkijoiden ja tuotekehityksen tutkimustyö on vaikeutunut (South China Morning Post 26.1.2015). Toinen Kiinan kasvun ja ulkomaisten yritysten kannalta ongelmallinen tekijä on Kiinan kiristyneen internetsensuurin mahdollisesti negatiivinen vaikutus Kiinan ulkopuolisten osaajien rekrytointiin (China Digital Times 10.6.2015).

3.6. Kansainväliset aloitteet

Kiina on ajanut kuluvalla vuosikymmenellä kahta keskeistä internetagendaa. Ensinnäkin internetin globaalin valtioiden rajat ylittävän hallinnoinnin siirtämisen YK:n alaisuuteen (Information Office of the State Council of the People's Republic of China White Paper 2010) ja toiseksi Kiina on yhä voimakkaammin vaatinut internetin vahvempaa liittämistä kansallisen suvereniteetin piiriin (U.S.-China Economic and Security Review Comission raportti toukokuu 2014).

[29] Euroopan kauppakamarin puheenjohtaja Jörg Wuttke kommentoi Kiinan internetyhteyden olevan jopa viisi kertaa hitaampi kuin Etelä-Korean (China Digital Times 10.6.2015). Etelä-Korean internetin yhteysnopeudet ovat kansainvälisessä vertailuissa maailman nopeimmat, mutta keskimääräisten nopeuksien erot eivät niinkään johdu maan rajojen sisäisestä infrastruktuurista. Kiinan kohdalla merkittävin ero kohdistuu ulkopuolelle suuntautuvaan liikenteeseen, mikä kulkee muutaman, tiukasti tietoa haravoivaivan, palvelimen kautta.

YK:n kontekstissa Kiina on tehnyt avauksia yhdessä Venäjän kanssa, tukenaan myös Kazakstan, Kirgisia, Uzbekistan ja Tajikistan (Kirje YK:n pääsihteerille 20.11.2011). Aloite oli muotoiltu kyberavaruuden käyttäytymissäännöstöksi,[30] joka painotti myös Kiinan kansallisen kyberagendan korostamaa internetin kansallista suvereniteettia, YK:n roolia kansainvälisenä normien määrittelijänä sekä sananvapauden ehdollistaminen kansallisen turvallisuuden ja vakauden turvaamiseksi (Kirje YK:n pääsihteerille 20.11.2011, Yhdysvaltojen Kiinan kauppa- ja turvallisuusarviokomission[31] raportti toukokuu 2014). YK:n kautta Kiina toivoisi oletettavasti vahvistunutta valtioiden asemaa internetin normiston ja säännösten määrittelijänä. Yhdysvallat ja EU-maat ovat esittäneet hallinnoinnin tapahtuvan yhteistyössä ei-valtiollisten organisaatioiden kanssa (Yhdysvaltojen Kiinan kauppa- ja turvallisuusarviokomission raportti toukokuu 2014). Kiina oli myös osallinen ryhmässä,[32] joka käsitteli muun muassa edellä mainittua esitystä. Ryhmän loppulausumassa internet todetaan YK:n peruskirjan määrittelemän kansallisen suvereniteetin piiriin (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2010). Tällöin valtio on myös vastuussa omalta alueelta käsin tehtävästä kybertoiminnasta, mikä voi jatkossa vaikuttaa esimerkiksi Yhdysvaltojen ja Kiinan toistuviin kiistoihin kyberurkinnassa ja yritysvakoilussa (Diplomat 22.1.2015).

Kiina on esityksessään korostanut internetin hallinnoinnin demokratisoimista. U.S.-China Economic and Security Review Comission (2014) arvioi Kiinan pyrkivän vastustamaan Yhdysvaltojen vaikutusasemaa johtavana internetin pelisääntöjä muovaavana valtiona. Ei ole sinänsä yllättävää, että Kiina on tavoitteitansa edesauttaakseen hakenut tukea muilta valtioilta kuten Venäjä, joille näiden sisäpoliittisen tilanteen takia internetin suvereniteetti olisi toteutuessaan mieleinen. Lu Wei nosti internetin kattavamman hallinnoinnin esille esimerkiksi puheessaan Kiinan ja arabivaltioiden tapahtumassa, jossa käsiteltiin niin sanottua verkkosilkkitietä, joka käytännössä tarkoittaa lähinnä Kiinan ja arabivaltioiden verkkoyhteistyön tiivistämistä ja esimerkiksi verkkoinfrastruktuurihankkeita (China Daily 9.11.2015).

[30] Alkup. Code of Conduct.

[31] U.S.-China Economic and Security Review Comission.

[32] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Kiina ja Venäjä ovat tehneet myös kyberulottuvuutta koskevia sopimuksia jo Shanghai Cooperation Organisaation (SCO) piirissä, mutta toukokuussa 2015 valtiot solmivat bilateraalin sopimuksen, johon sisältyi aiempaa suorempia mainintoja kyberulottuvuuden ja informaationormien suhteen (Diplomat 21.8.2015). Keskinäisistä kyberaggressioista pitäytymisen lisäksi sopimuksessa muodollistetaan Kiinan ja Venäjän yhteispyrkimykset muovata globaalia internetin hallinnoinnin normistoa (Diplomat 21.8.2015).[33] Kesällä 2016 Venäjä loi uuden *Yaroslavin lain,* jossa Kiinan tapaan myös Venäjällä luotiin internettoimittajille velvoitteet säilöä käyttäjädataa (Guardian 26.6.2016).

Kiina pyrki nostamaan omaa profiiliaan kansainvälisessä kyberpolitiikassa järjestämällä ensimmäisen maailman internetkonferenssin Wuzhenissa marraskuussa 2014 (Xinhua 20.11.2014). Kiinan viranomaisten mukaan paikalle saapui noin 1000 kutsuttua vierasta sadasta maasta (China Daily 30.1.2015). Tapahtuman pääteemoja olivat internetin hallinta sekä kyber- ja mobiiliturvallisuus. Konferenssissa pitämässään puheessa CAC:n johtaja Lu Wei totesi Kiinan tavoittelen demokraattisempaa ja avoimempaa internetin globaalia hallintaa (BBC 19.11.2014). On kuitenkin olennaista erottaa että tällä tarkoitetaan nimenomaan globaalin järjestelmän valtioiden välisiä päätöksentekomekanismeja, eikä niinkään valtion ja kansalaisten suhdetta internetkysymyksissä. Presidentti Xi Jinping toivoi avajaispuheessaan internetin suvereniteetin vahvempaa tunnustamista ja valtioiden välistä luottamusta (Xinhua 20.11.2014).

Erikoisin käänne Wuzhenin konferenssissa oli kyseenalainen pyrkimys ajaa läpi Kiinan toivoma konferenssin julkilausuma. Kopiot julkilausumasta oli toimitettu osallistujille hotellihuoneiden ovien alitse kello yhdentoista jälkeen, edellisenä iltana. Muutostoiveet taas tuli palauttaa aamukahdeksaan mennessä. Julkilausuma olisi sisältänyt internetin suvereniteettia ja demokraattista globaalia hallintaa korostavat kohdat. Julkilausumaa ei lopulta koskaan julkaistu (Bloomberg 21.11.2014).

Vaikka Kiina ja sen aloitteiden tukijat ovat olleet äänekkäimpiä suvereniteetin kannattajia kyberavaruudessa, huomioivat Demchak ja Dombrowski (2011), että todellisuudessa kaikki valtiot ovat parhaillaan luomassa internetin Westphaliaa. He toteavat, että on kyse Kiinasta, Ruotsista tai Yhdysvalloista, pyrkivät valtiot etsimään keinoja säädellä mitä dataa maan rajojen sisälle pääsee ja mitä tietoa annetaan ulos. Tämä pitää osittain paikkaansa, mutta turvallistamisen näkökulmasta ilmiötä

[33] Tämän tutkielman kirjoittamisen hetkellä Kiina ja Venäjä sopivat virallisen yhteistyösopimuksen internetin tietosensuurin järjestelmistä. Kiina on luvannut tukea teknisesti ja ohjelmistotasolla Venäjän niin sanottua punaista verkkoa. Sopimusta edelsivät Venäjän Kiinan toimia muistuttavat pyrkimykset estää sosiaalisia verkostoitumissivuja (Guardian 29.11.2016).

tarkasteltaessa on huomioitava millaisin erityisin keinoin tämä turvallisuussiirto tuotetaan. Toistaiseksi Kiinan tapauksessa voidaan puhua maailman kattavimmasta ja hienostuneimmasta sensuurikoneistosta, jonka piiriin sisältyviä toimia olisi hyvin vaikea onnistuneesti turvallistaa Yhdysvaltojen ja Euroopan sananvapauden eetoksesta kiinni pitävässä yhteiskunnassa. Kansainvälinen pyrkimys suvereniteettiin ei siis ehkä ole Kiinalle uniikki, mutta suvereniteetin konseptin sisään tehtävät rajoitteet ovat idealististen universaalien arvojen kannalta ongelmallisia. Vaikka moraalisen ja laillisen toiminnan periaatteet ovat internetin käytössä hyväksyttyjä ja toivottavia normeja yli valtiorajojen, harva eurooppalainen mieltäisi valtion roolin aktiiviseksi moraalin ja kuuliaisuuden ylläpitäjäksi ja edistäjäksi (Swaine 2013, 5).

On mahdollista, että Edward Snowdenin paljastukset Yhdysvaltojen kyberurkinnasta ovat vauhdittaneet ja voimistaneet Kiinan pyrkimyksiä kansallisen suvereniteetin tunnustavan ja multilateraalisen kybernormiston luomiseksi. Suurista valtioista sekä Kiina että Venäjä pyrkivät aiempaa selkeämmin omavaraiseen kyberinfrastruktuuriin, sillä nykytilanteessa esimerkiksi servereistä suurin osa sijaitsee Yhdysvalloissa (The Diplomat 21.11.2015). Yhdysvallat ilmoitti luopuvansa internetin domain-nimien ja IP-osoitteista vastaavasta Internet Corporation for Assigned Names and Numbersista (ICANN), tehden organisaatiosta ensimmäistä kertaa autonomisen. Tämän hetken tavoitteena siirtymälle on vuosi 2016 (Wall Street Journal 18.8.2015), johon mennessä ICANN pyrkisi luomaan uuden organisaatiojohtomallin, jolla turvattaisiin läntisten arvojen, kuten sananvapauden keskeisyys ICANN:n toiminnassa. Lopullisia ratkaisuja ICANN:n suhteen ei kuitenkaan ole vielä tehty ja keskustelu muun muassa Yhdysvaltojen roolista suhteessa organisaatioon jatkuu yhä (Washington Post 28.9.2015). Viimeisin muutos tilanteeseen nähtiin maaliskuussa 2016, kun ICANN julisti virallisesti käynnistäneensä prosessiin internetin hallinnon osa-alueiden siirtämisestä kansainvälisen yhteisön hallintaan (IANACG.org).

Samalla diskurssia kybervalvonnasta käydään aiempaa aktiivisemmin myös Euroopassa ja ihmisten yksityisyyden ja valtion oikeuksien rajoja määritellään uudelleen. Muutosten keskellä Kiinalla on siis teoriassa aiempaa parempi mahdollisuus ajaa toivomaansa kansainvälisen kybernormiston muutosta ja selkeästi voimistuneet kansainväliset pyrkimykset kielivät sekä vaikutusvaltansa kasvun tunnistavasta että tilaisuuttaan hakevasta Kiinan valtiosta. Euroopasta käsin kyse ei ole niinkään uhkasta Euroopan sisäiselle internetnormistolle, mutta internetin vapauden ajatellun universaalisuuden tilalle voi syntyä rinnakkaisia arvojärjestelmiä.

4. KYBERPOLITIIKAN KÄYTÄNNÖN VAIKUTUKSIA

Tässä luvussa käyn läpi Kiinan internetpolitiikan vaikutuksia ja retoriikan implikaatioita. Tarkastelen tietoturvallisuuteen ja kansalliseen turvallisuuteen luotujen lakien sanallista sisältöä suhteessa turvallistamiseen ja Vuoren turvallistamistyyppeihin. Analyysi kohdistuu kolmeen synergiseen osatekijään, joilla turvallistaminen ja kontrolli Kiinan internetpolitiikassa tapahtuu: fyysinen järjestelmien hallinta, turvallistamisen seurauksena tapahtuva itsesensuuri sekä kansainvälinen kontrollin validointi.

Fyysinen kontrolli ja itsesensuuri kulkevat analyysissani limittäin, sillä Kiinan käyttämät merkittävät resurssit fyysiseen informaation rajaamiseen ja valvomiseen ovat suorassa yhteydessä itsesensuuriin. Tarkoitukseni on samalla argumentoida, miksi itsesensuuri sekä mittaa turvallistamisen onnistumista että osoittaa turvallistamisen teorian empirian mittaamisen ongelmia. Kansainvälisessä validoinnissa käyn läpi Kiinan kampanjoimaa internetin suvereniteetin konseptia sekä internetin rajoitusten ja kansainvälisen kaupan, sekä sen myötä Kiinan kasvupyrkimysten, välisiä jännitteitä.

Ennen varsinaiseen analyysiin siirtymistä käyn läpi tutkimuksessa käytettävän teoriaohjaavan sisällönanalyysin metodiikkaa.

4.1. Metodina teoriaohjaava sisällönanalyysi

Tämän tutkimuksen aineiston analyysiin on käytetty tutkimusmetodina teoriaohjaavaa sisällönanalyysia. Sisällönanalyysi tutkimusmuotona sai virallisesti alkunsa 1960-luvulla, jolloin termi määriteltiin tarkoittamaan tutkimuskohteensa ekplsiittien ja latenttien analyysia (Krippendorff 2006, 1). Krippendorff kuitenkin huomauttaa metodin olleen tavalla tai toisella läsnä koko ihmiskunnan kielellisen ja symbolisen historian ajan, sillä kielellä ja symboliikalla on aina ollut vaikutusta havainnoitsijansa tulkintaan. Nykyisin symboliikka, jota sisällön analyysilla tutkitaan, on erottamaton osa taidetta, kirjallisuutta, viihdeteollisuutta ja politiikkaa.

Tutkimusmetodina sisällönanalyysin erottaa muista metodeista kolme keskeistä piirrettä (Krippendorff 2006, xvii-xxiii):

1) Sisällönanalyysi on empiriaan pohjaava tutkimusmetodi, jonka prosessi on löydöksiin perustuvaa ja pyrkimyksiltään päättelyyn pohjaava. Metodin pohjalla on kielen ja merkitysten muodostuminen psykologian pohjalta, pelkän täyden

rationaalisuuden sijaan. Muista empiirisistä menetelmistä sisällönanalyysin erottaa sen pyrkimys tutkia, mitä sen tutkimuksen kohde merkitsee ihmisille, mitä kohde mahdollistaa tai estää ja mitä vaikutusta tutkimuskohteen informaatiolla on.

2) Sisällönanalyysi ylittää perinteiset symboliikan ja sisällön määritelmät, mikä on tapahtunut toistaiseksi viidessä kehitysvaiheessa. Ensin identifioitiin *viestin* merkitys, minkä seurauksena intentioita alettiin välittää kirjallisessa, muuttumattomassa muodossa. Viesti on pikemmin intention säilytys ja kuljetusmekanismi, kuin sisällöllinen viitekehys. Toisena käsitteenä nousi ajatus *kanavista*, joiden avulla kommunikaatio tapahtuu. Tämä koskee niin kirjallisen ilmaisun rajoittumista aakkosiin, kuin esimerkiksi lähihistoriaan saakka puheluiden rajoittumiseen äänelliseen viestintään. Kolmantena nousi ajatus *kommunikaatiosta* vuorovaikutuksen tilana lähettäjän ja vastaanottajan välillä, missä kahdenkeskeisiä ja yhteiskunnallisia suhteita muovataan. Ajatus oli pitkälti seurausta massamedian syntymisestä ja sen tuomista informaation levittämisen mahdollisuuksista. Neljäs vaihe oli tunnistaa *järjestelmät*, joiden luonteeseen kuuluu globaalius ja interaktiivisuus. Erona globaaliin yksisuuntaiseen massamediaan on vuorovaikutteisuus ja keskinäisriippuvaisuus sekä teknologian mahdollistama lähes universaali mahdollisuus osallistua. Viides, käynnissä oleva vaihe, on hahmottaa kognitiivisten ja sosiaalisten prosessien algoritminen luonne. Tämä *ohjelmoinnin* ymmärtäminen mahdollistaa uudenlaista tutkimusta ja vaikuttamista.
3) Sisällönanalyysi on luonut itselleen omat metodologiset ratkaisut. Syinä tähän voidaan katsoa olevan ensinnäkin sisällönanalyysin kontekstuaalisen ympäristön laajeneminen, muun muassa elektronisen aineiston myötä. Toiseksi edellä mainittuun liittyy myös paine luoda uusia automatisoituja keinoja käsitellä aiempaa suurempia määriä dataa.

Koska tutkimuksessa on lähdetty tarkastelemaan aineistoa erityisesti turvallistamisen kulmasta, toimii tutkimusmetodina nimenomaan teorialähtöinen sisällönanalyysi. Tällöin analyysin viitekehyksenä ja tutkimusta ohjaavana termistönä toimii olemassa oleva teoria (Tuomi & Sarajärvi 2002, 109-116). Metodissa teoria ja aiemmat tutkimukset ohjaavat vahvasti analyysia ja tavoitteena on tutkimuksen avulla kehittää teorian käsitystä tai mallia tutkittavasta asiasta (Vilkka 2017). Teoriaohjaavaan sisällönanalyysiin liitetään usein kvantitatiivisia piirteitä. Tällöin tutkimuksessa määritellään kategorioita, joiden esiintymisten määrää tutkitaan valitussa aineistossa. Tämä kategorioiden luominen

ja kvantitatiivisen kulman sisällyttämään tähän tutkimukseen ei kuitenkaan olisi aineiston ja teorian huomioiden oleellisesti palvellut tutkimuksen tavoitteita. Tutkimuksen kohteena oleva aineisto on suhteellisen eklektinen kokoelma lähteitä, eikä pelkkä turvallisuussanaston toistumisen arviointi olisi avannut kuvaa Kiinan internetpolitiikan tilasta. Siksi tämä tutkimus painottuu pikemmin sisällön kvalitatiiviseen analysointiin kuin sisällön erittelyyn, joka voidaan karkeasti erotella kvantitatiiviseksi versioksi sisällönanalyysista.

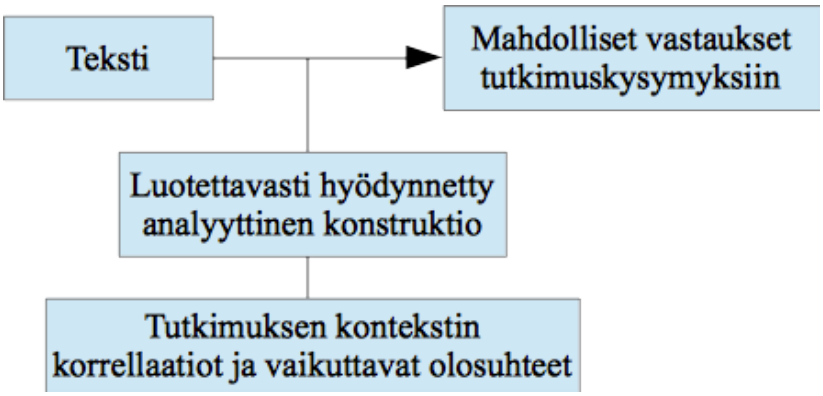
Turvallistamisella ja propagandalla on retorisia yhtäläisyyksiä, eikä näiden kahden termin väliviiva ole aina objektiivisesti erotettavissa. Sisällönanalyysi on kyennyt tunnistamaan propagandasta piirteitä ja säännönmukaisuuksia aiemmissa tutkimuksissa (Krippendorff 2006, 27-28). Sisältö ei ole kommunikaation ominaisuus, sillä kommunikoijan ja yleisön tulkinta sisällöstä voi erota merkittävästi ja ennalta arvaamattomasti. Sisällöntutkija joutuu ennustamaan ja tulkitsemaan ilmiöitä, joita hän ei pysty suoraan havainnoimaan. Yksilön ja yhteisön tasolla ei pystytä välttämättä havainnoimaan esimerkiksi turvallistamisentoimen vaikutusta ajatuksiin ja asenteisiin. Koska tutkija tekee tulkintoja tekstin ulkopuolelta on tutkimusten johtopäätösten toisintaminen ongelmallista. Sisällönanalyysin tulee pystyä määrittämään kontekstit missä kommunikaatio tapahtuu, tai miksi tietyissä konteksteissa ei kommunikoida. Sosiaalisten ja poliittisten ilmiöiden tutkiminen pelkkänä kvantitatiivisena datana on usein pinnallista ja sisällönanalyysi pyrkii antamaan työkalut, joilla kvalitatiivinen tulkinta on systemaattista ja luotettavaa.

Sisällönanalyysin tarkoitus tarkastella aineistoa siten, että luodaan informatiivisia ja tulkintaa selkeyttäviä kokonaisuuksia. Hajanainenkin aineisto pyritään tiivistämään muotoon, jossa aineistojen ja todellisuuden suhteet saatetaan koheesiin muotoon (Tuomi & Sarajärvi 2002). Tämä voidaan tehdä aineiston väljällä tai tiukan strukturoidulla käsittelyllä.

Sisällönanalyysin avulla tehdyssä tutkimuksessa tutkijan täyty tehdä valinta tutkitaanko ainoastaan manifestia sisältöä vai myös latenttia, eli piilossa olevaa viestintää (Tuomi & Sarajärvi 2002). Turvallistamisen teorian kannalta on olennaista pyrkiä purkamaan retoriikkaa myös kirjaimellisen viestinnän taakse, sillä esimerkiksi viholliskuvien luonti voi yhtälailla tapahtua konkreettisesti sanavalinnoilla kuin implikaatiolla. Näin ollen tämä tutkimus ei rajoitu vain manifestiin sisältöön vaan pyrkii ottamaan huomioon myös aineistonsa latentin sisällön.

Sisällönanalyysin taustalla on abduktiivinen päättely (Krippendorff 2006, 38-39). Tällöin datasta (D) tehdään johtopäätös (C), jonka toteutumiseen on tiettyjä edellytyksiä (W). Edellytykset ovat loogisen

päättelyn ketju, joka johtaa datasta päätelmään. Näitä edellytyksiä voivat lisäksi tukea perusteet (B) edellytykseltä. Sisällönanalyysin osalta asian voi havainnoida Krippendorffin tapaan seuraavasti:



Tämän tutkimuksen kannalta datana siis toimivat erilliset lehtiartikkelit sekä valtion poliittiset linjaukset ja asiakirjat. Analyyttinen konstruktio jonka läpi ilmiötä tarkastellaan on turvallistamisen teoria ja Vuoren (2008) turvallistamisen tyypit. Huomio kiinnittyy erityisesti turvallistamisen lajeista kontrollin tyyppiin ja tämä turvallistamistyyppi toimii sisällönanalyysini teoreettisena ankkurina, jonka kautta arvioin aineistoa.

4.2. Analyysi

Turvallistaminen pohjaa ajatukseen siitä, että uudet turvallisuuslinjaukset ja uhat määritellään onnistuneesti yleisölle, jota uhan torjunnan tuomat rajoitukset koskevat. Samalla turvallistamista tehdään myös esimerkiksi hallituksen sisäisissä rakenteissa. Tietyissä tilanteissa pyritään turvallistamistoimet legitimoimaan myös kansainvälisesti. Näin ollen voidaan puhua erillisistä yleisöistä ja erillisistä valtion oman statuksen mahdollistamista onnistuneen turvallistamisen erilaisista priorisoinneista.

Internetin ja informaation vahva sensurointi itsessään lisää turvallistamista ja turvallistamistoimien onnistumisen todennäköisyyttä. Kiinan tapauksessa on syytä huomioida, ettei turvallistamiseen yleensä liitettävä poikkeustila ole saumattomasti sovellettavissa sensuuriin. Ei niinkään etteikö Kiinan sensuuri olisi globaalilla tasolla turvallisuudellisesti poikkeuksellisesta tai että perustelut sen takana eivät olisi turvallisuuspuhetta, vaan ongelma on pikemminkin se että poikkeustilasta on tullut valtion järjestelmän normaali olotila.

Turvallistaminen siis pyrkii siirtämään kohdettaan avoimen politiikan ulkopuolelle ja luomaan uhan torjumiseksi poikkeustilaa, joka oikeuttaa normaaleista olosuhteista poikkeavia vapauksien rajoituksia. Tällöin turvallistamisen onnistumiseen, järjestelmästä riippumatta, vaikuttaa olennaisesti myös turvallistamisen ympärillä oletettujen uhkien ja vaikutusten ymmärtäminen. Mitä vähemmän turvallistamisen yleisö tietää ja ymmärtää turvallistamisen kohteesta, sitä vähemmän se kykenee arvioimaan turvallistamisen sisältöä kriittisesti. Informaation turvallistaminen on tässä mielessä erityisen ongelmallista. Prosessin alku voi olla vaikea perustella, mutta mitä hallitumpaa saavutettava informaatio yleisölle on, sitä helpommin yleisölle pystytään ajan kuluessa konstruoimaan lisätoimia vaativia uhkia.

Kiina ei ole kuitenkaan turvautunut vain ulkopuolisten informaatiolähteiden rajaamiseen. Internet ja sen suhteellisen notkeat estojen kiertomahdollisuudet ovat vaatineet hienovaraisempaa otetta. Samalla kun kansainvälistä informaatiota ja käyttökanavia on kansallisen turvallisuuden nimissä suljettu kansalaisten ulottumattomiin, hallitus on tukenut yrityksiä, jotka ovat luoneet vaihtoehtoisia sivustoja, jotka toiminnaltaan vastaavat globaaleja sivustoja. Ei ole perusteetonta kyseenalaistaa, mihin kiinalainen nuori tarvitsee pääsyä esimerkiksi länsimaiseen sosiaaliseen mediaan, jos hänelle on pääsy maailman suurimpaan valtion sisäiseen sosiaalisen median verkkoon. Sama asia nousi esille myös keskusteluissani Suomessa kiinalaisten vaihto-opiskelijoiden kanssa, jotka totesivat etteivät sinänsä kaipaa länsimaisia sivustoja. Heidän koko tuttavapiiri oli heidän kanssaan samoilla sivustoilla. [34]

Kiinan internetsensuuri sekä poikkeukselliset järjestelyt ja resurssit, jotka siihen on sidottu, on kohdennettu rajaamaan nimenomaan informaatiota. Se takaa verrattain vahvan monopolin hallitukselle määrittää mitä informaatiota väestö kykenee tavoittamaan. Tuottamalla globaaleista palveluista kansalliset versiot, joiden sisältöä Kiina pystyy tehokkaasti moderoimaan, Xi:n hallinto on kiristänyt ideologista otettaan. Samalla turvallistamisen näkökulmasta turvallistamisen yleisönä väestön kyky arvioida turvallistamisen argumenttia heikkenee. Äärimmäisenä versiona vastaavasta voidaan pitää Pohjois-Koreaa, missä rajojen ulkopuolelta saatava informaatio on vielä rajoitetumpaa ja väestön hallinta tiukempaa.

Retoriikka Kiinan taholta on kohdistunut nimenomaan ideologiseen uhkaan, joka vaarantaisi koko Kiinan valtion olemassaoloa, mikäli läntisten vaikutteiden annettaisiin turmella kiinalaisen

[34] Keskustelut käyty Tampereella marraskuussa 2015.

kommunismin ihanteita. Samalla kun ideologinen ohjaus nuorten koulutuksessa vahvistuu, rajoitetaan internetin tuomia kansainvälistymisen mahdollisuuksia. Kun katsotaan esimerkiksi Hong Kongin sateenvarjovallankumousta, ei ole yllättävää että nimenomaan nuoret aikuiset ovat tehostetusti hallinnan kohteena. Internetin käyttäjistä merkittävä osa on nuoria aikuisia, joiden internetissä käyttämä aika ohjataan nyt voimakkaasti Kiinan verkon sisäisiin, hallittaviin sisältöihin. Opiskelijat ja nuoriso on myös retorisesti asetettu läntisten vaikutteiden uhan keskeisiksi uhreiksi. Juuri nuoriso on myös turvallistamisen ja nimenomaan kyberinformaation turvallistamisen kontrollin kannalta haasteellisin ryhmä. Sukupolvi on tottunut olemaan keskenään laajamittaisesti yhteydessä viiveettömästi. Taloudellisten insentiivien lisäksi tämä tottumus on myös korostanut Kiinan informaatiohallinnan tarvetta luoda rinnakkaisia sivustoja ja ohjelmia länsimaisille, vaikeammin hallinnoitaville sivustoille. Levottomuuksien yhteydessä myös Turkissa, missä urbaaneissa keskuksissa nuoriso oli keskeinen osa viime vuosien levottomuuksia, internetin katkokset kohdistuivat nimenomaan nuorten aikuisten suosimiin sosiaalisiin medioihin (Freedom House raportti 2016).

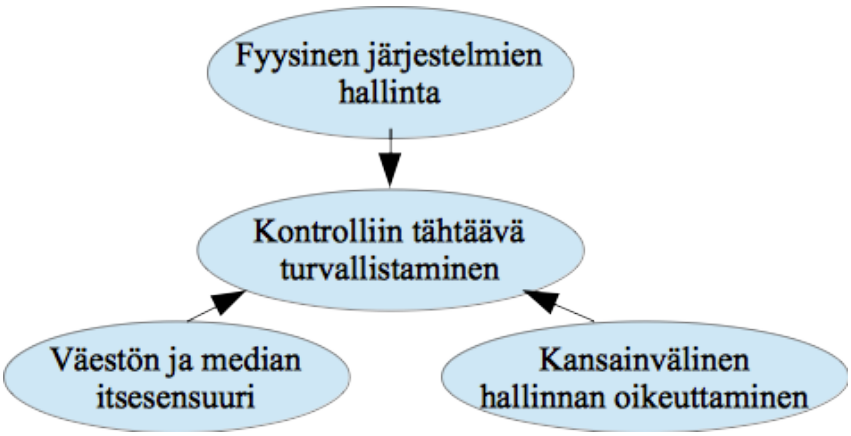
Sensuuripolitiikan juuret sijoittuvat vuosiin 1996 ja 1997, jolloin Kiinassa tehtiin ensimmäiset muodolliset säädökset internetin hallinnoimisesta (Qiu 1999). Kansallinen turvallisuutta ja yhtenäisyyttä vaarantavan informaation jakaminen ja käyttö on näissä säädöksissä[35] todettu rikolliseksi toiminnaksi, mikä sisälsi myös juorujen levittämisen. 2005 kirjattiin lakiin lisäyksiä, jotka rajoittivat uutismaista informaatiota jakavien henkilöiden tai ryhmien sivustojen toimintaa. Kaikkien vastaavien sivustojen tuli olla rekisteröity valtiolle uutisorganisaatioina. Uutisorganisaatioita vuorostaan velvoitetaan sisältämään kokenutta henkilökuntaa, omistamaan viralliset toimitilat ja pääomaa (Lum 2006). Nykyisessä kontekstissaan nämä linjaukset tekee turvallistamisen kannalta oleelliseksi nimenomaan kyberturvallisuuden liittäminen osaksi kansallista turvallisuutta, minkä Presidentti Xi eksplisiitisti siis oli tehnyt todettuaan, että kansallista turvallisuutta ei ole ilman kyberturvallisuutta. Tämä on tarkoittanut samalla ettei ainoastaan tietoverkkojen toiminta ja turvallisuus ole kansallista turvallisuutta, vaan myös puolueen ja valtion vakautta uhkaava digitaalinen informaatio on osa kansallista turvallisuutta. Tällöin lakipykälät mahdollistavat hallitsevalle taholle helpon keinon

[35] Englannin kielen käännös lain artikloista 4-6 (Lum 2006): ”Individuals are prohibited from using the Internet to: harm national security; disclose state secrets; or injure the interests of the state or society. Users are prohibited from using the Internet to create, replicate, retrieve, or transmit information that incites resistance to the PRC Constitution, laws, or administrative regulations; promotes the overthrow of the government or socialist system; undermines national unification; distorts the truth, spreads rumors, or destroys social order; or provides sexually suggestive material or encourages gambling, violence, or murder. Users are prohibited from engaging in activities that harm the security of computer information networks and from using networks or changing network resources without prior approval.”

muovata tailnteen mukaan määritelmät levitettävistä juoruista, eli tarvittaessa määrittää minkä tahansa ei valtion virallista linjaa edustavan informaation uhkaksi kansalliselle turvallisuudelle. Turvallisuuden takaamiseksi on silloin perusteltua ylläpitää poikkeuksellisia turvallisuuslinjauksia myös informaatiosisällöistä internetissä.

Tilannekartoituksessa (luku 3) esille nostettu CAC on ensimmäinen organisaatiotasolla muodollisesti ja virallisesti nimenomaan internetpolitiikan hallintaan erikoistunut valtion elin. CAC:n perustaminen ei kuitenkaan tapahtunut vähin äänin. Ajallisesti yhdessä Wuzhenissa järjestetyn internetkonferenssin kanssa perustettu CAC sai mediahuomiota ja sen tehtävä esitettiin kiinalaisissa viestimissä selkein kansallista turvallisuutta, kansan eettisiä hyveitä ja yhteiskunnan tasapainoa varjelevana toimijana.

Internetistä ei siis niinkään ole tehty turvallisuusuhkaa fyysisessä mielessä, vaan valtion näkökulmasta internetin muodostama eksistentiaalinen uhka kumpuaa internetin kyvystä levittää informaation laaja-alaisesti ja hallitsemattoman nopeasti. Kontrolliin tähtäävän turvallistamisen näkökulmasta tämä aiheuttaa merkittävän haasteen. Kiinassa kontrollin turvallistamista on toteutettu kolmella osa-alueella:



Kommunistinen puolue on viime vuosina tehnyt näyttäviä esimerkkejä liian vaikutusvaltaisista internetpersoonista ja sulkemisten lisäksi aktiivisesti rangaissut (China Digital Times 1.3.2016) sosiaalisessa mediassa isoja seuraajamääriä saaneita, epäsopivaa sisältöä julkaisseita henkilöitä. Kun myös mediaan on kohdistettu tiukkaa valvontaa, ja tarvittaessa sanktioita, internetissä levitettävien uutisointien osalta, on hallitus onnistunut varsin tehokkaasti luomaan kansalaistensa piirissä itsesensuurin kulttuurin. Itsesensuurin suhde turvallistamiseen on problemaattinen, koska turvallistamisen yleisön hyväksyntä ja itsesensuuri eivät varsinaisesti ole sama asia. Periaatteessa tutkijan pitäisi pystyä arvioimaan onko itsesensuurin syynä onnistunut turvallistamistoimi, jonka seurauksena yksilö sensuroi itseään, koska yleinen turvallisuus edellyttää sitä, vai onko tapahtuuko

itsesensuuri rangaistuksen pelossa.[36] Jälkimmäisen suorat vaikutukset ovat toki verrattavissa turvallistamiseen siinä mielessä, että myös uhkailu on kontrollin muoto, mutta tähän tiivistyy yksi autoritääristen järjestelmien turvallistamisen tutkimuksen keskeisimmistä ongelmista. Eroa on äärimmäisen vaikea mitata empiirisesti, mutta nimenomaan tuo erottelu määrittää onnistunutta turvallistamista.

4.1.1. Kansallinen turvallistaminen

Merkittävin muodollinen internetin hallinnoinnin dokumentti on ollut 2016 vuoden kyberturvallisuuslaki. Lain ensimmäisessä artiklassa todetaan, että lain tarkoituksena on turvata *internetin kansallista autonomiaa*, edistää *kansallista turvallisuutta*, suojata yhteiskunnallisia intressejä ja edistää *terveellistä ekonomista ja sosiaalista informatisaatiota.* Laissa rinnastetaan alusta alkaen kansallinen turvallisuus ja yhteiskunnallinen järjestys, jota internetin informaatio omalta osaltaan uhkaisi. Artikla 6 on lain pohjustavista pykälistä selkeimmin osoitettu kansalaisiin ja näiden internetissä jakaman tietoon: ”Valtio ajaa vilpitöntä, rehellistä, tervehenkistä ja sivistynyttä verkkokäyttäytymistä; kannustaen sosialististen arvojen levittämistä.” Samaan retoriikkaan yhdistyy myös 2015 vuoden kansallinen turvallisuuslaki, jossa nostetaan tarve edistää sosialististen arvojen levittämistä ja turvautua haitallisilta moraalistandardeilta. Molemmissa dokumenteissa informaatio, ja tarkemmin internetissä levitetty tieto ja mielipiteet, on sidottu kiinteästi osaksi kansallista turvallisuutta. Epäsuotuisa tai sopimaton sisältö on suorassa ristiriidassa valtion turvallisuuden ja kommunististen arvojen kanssa.

Kahden yllämainitun pykälän lisäksi informaatiota ja internetkäyttäytymistä määrittää kyberturvallisuuslaissa artikla 12 (korostukset lisätty):

> Jokaisen verkkoa käyttävän yksilön ja organisaation tulee noudattaa perustuslakia ja muita lakeja, *ylläpitää yleistä järjestystä ja kunnioittaa sosiaalista moraalia*. He eivät saa toimia vaarantaen kansallista turvallisuutta, *kansallista kunniaa* ja intressejä, kiihottaa kansallisen itsemääräämisoikeuden heikentämistä, *sosialistisen järjestelmän kumoamista,* kiihottaa separatismiin, *heikentää kansallista yhtenäisyyttä* […] luoda tai jakaa valheellista

[36] Turvallistamisen ja pelon konseptuaalisesta suhteesta katso Williams (2011), joka argumentoi pelon olevan osa turvallistamisen ajatusta, muttei synonyymi tämän kanssa. Williams on myös huomauttaa pelon voivan kohdistua niin ulkoisiin uhkiin kuin omaan valtioon, mikä voi toimia itsesensuurin insentiivinä.

> informaatiota, joka häiritsee taloudellista tai *yhteiskunnallista järjestystä* sekä *toisten mainetta*, yksityisyyttä, immateriaalioikeuksia tai muita laillisia intressejä rikkovaa informaatiota.

Artiklassa korostuu kommunistisen puolueen korostama kiinalainen turvallisuuden määritelmä, joka korostaa pikemmin järjestystä ja harmoniaa kuin pelkkää konkreettista turvallisuutta. Poliittista nykytilaa varjelevat ja ylläpitävät turvallisuusintressit on saumattomasti yhdistetty konkreettisiin turvallisuusintresseihin.

Artiklan 12 vakautta turvaava termistö on määrittelyltään suhteellisen tulkinnanvarainen. Laki antaa suhteellisen vapaat kädet lainvalvojille tulkita informaatiota haitalliseksi ja lain piiriin kuuluvaksi. Artikla ilmaisee eksplisiitisti sosiaalisen moraalin, kansallisen kunnian, sosialistisen järjestelmän ja kansallisen yhtenäisyyden osaksi kyberturvallisuutta ja kansallista turvallisuutta. Käytännön tasolla nämä kaikki ovat kansalaisiin kohdistuvia jaetun informaation säännöstöjä. Turvallistamisen kannalta lain mainitussa artikloissa on kaksi kiinnostavaa ominaisuutta: 1) artiklat kohdistuvat informaation ja kansalaisten kontrolliin vastaten suoraan Vuoren kategorioiden kontrolli-turvallistamista, missä kansalaisia ohjataan toimimaan tai pitäytymään toimimasta tietyllä tavalla. 2) Artikloiden kontrollin kohteen kieli on määrittelyiltään hyvin tulkinnanvaraista ja väljää. Tämä mahdollistaa kontrollin hyvin tapauskohtaisten ja intressien mukaan muuttuvien kriteerien perusteella.

Sekä kyberturvallisuus- että kansallisessa turvallisuuslaissa on eritelty kielletyksi niin kansallista turvallisuutta ja yhtenäisyyttä vaarantava sisältö kuin myös juorut. Itsesensuurin kannalta näiden säädösten tulkinnanvaraisuus tekee säännöistä ennalta arvaamattomia, sillä varsinkin autoritäärisessä järjestelmässä lain tulkinta on altis poliittisille intresseille. Julkiset kampanjat internetin järjestykseen saattamiseksi itsessään luovat ilmapiiriä, missä hallinta ei vaadi konkreettisia interventioita vaan yhteiskunnan tietoisuus rangaistusten ja valvonnan olemassaolosta pystyy merkittävistä rajaamaan millaisista asioista internetissä koetaan turvalliseksi jakaa. Samalla järjestelmä pystyy sallimaan sen asettamien rajojen puitteissa tapahtuvaa sääntöjen rikkomista, pidättäen samalla keinot puuttua, mikäli vapaudet ylitetään (Vuori 2011, 238). Esimerkiksi juorujen kohdalla tämä mahdollistaa intressejä ja päämääriä palvelevien spekulaatioiden sallimista, mutta hallintoa uhkaavien kirjoitusten ja sisältöjen poistamisen sekä julkaisijan rankaisemisen.

Yllä mainitun lisäksi artiklan 58 nojalla pidetään oikeus tarpeen vaatiessa rajoittaa verkkokommunikaatiota väliaikaisesti. Lain muotoilu on kiinnostava siinä mielessä, että osa

kommunikaatioon kohdistuvista rajoitteista ovat käytännössä olleet jatkuvia. Esimerkiksi Googleen ja sosiaalisen median sivustoihin sekä tiettyihin avainsanoihin kohdistuvat estot ja automaattiset sensuroinnit ovat olleet yhtäjaksoisesti voimassa ilman suoria perusteita kyberturvallisuuslaista. Sosiaalisen median ja läntisten uutislähteiden sulkeminen palomuurin taakse on tosin myös retoriikan tasolla yhteydessä *haitallisten vaikutteiden* torjunnan retoriikkaan (esim. China Digital Times 07.05.2015).

Xu (2007, 143) toteaa keskimääräisen kiinalaisen internetin käyttäjän olevan kokonaisväestöön vertailtaessa keskivertoa koulutetumpi, internetin käyttäjien keski-ikä on Euroopan vastaavia lukuja selkeästi alhaisempi ja painottuu voimakkaasti kaupunkeihin. Viime vuosikymmeninä juuri kaupunkien opiskeleva nuoriso on ollut yhtenä laukaisevana tekijänä yhteiskunnallisissa muutoksissa. Kiinalla on tämän osalta myös omaa historiansa Tiananmenin aukion välikohtauksesta 1989. Suoraan yhteydessä tähän on myös näiden pysyvien *haitallisten vaikutteiden* torjumiseen asetettujen estojen kohdistuminen nimenomaan nuorison suosimiin sosiaalisen median sivustoihin. Siinä missä läntiset sivustot on suljettu kokokaan pois, toimii kiinalaisissa korvikkeissa, kuten Weibo, aktiivinen avainsanojen haravointi (China Digital Times 2014). Näin tietyt arkaluontoiset avainsanat saadaan poistettua nopeasti ja kattavasti erinäisiltä Kiinan sisäisiltä sivustoilta. Koska sensuuri on suhteellisen aktiivista ja muun muassa tunnettuihin sosiaalisen median henkilöihin kohdistuneet sanktiot ovat olleet näkyviä, on tämän avulla pystytty tehokkaasti valjastamaan internetkäyttäjien itsesensuuria. Toisaalta kiinan kielen runsaat homonyymit ovat luoneet erilaisia sijaissanoja ja koodikieli-ilmaisuja, joilla estetyt sanat ja aiheet korvataan automaattisten haravointien välttämiseksi (ibid.).

Itsesensuuri ei rajoitu ainoastaan yksityishenkilöihin, vaan myös uutislähteet joutuvat arvioimaan miten ja mitä he uutisoivat. China Digital Times on kuluneen kolmen vuoden aikana julkaissut lukuisia viestintäministeriön uutislähteille toimittamia määräyksiä kielletyistä aiheista tai uutisointien sävyjen ohjeistuksesta. Näiden määräysten uhmaaminen on johtanut sakkoihin ja muihin sanktioihin. Internetissä julkaiseviin uutislähteisiin kohdistuva kontrolli on kiristynyt entisestään vuoden 2017 aikana (BBC 3.5.2017). Lehdistön ja uutisten julkaisujen rajoittamisessa valtio käyttää samoja retorisia ilmauksia vakauden varmistamisesta ja *terveellisen* internetin luomisesta.

Turvallistaminen ja kontrolli kohdistuu siis erityisesti yhteiskunnallisiin, kommunistista järjestelmää uhkaaviin ajatuksiin. Tässä suhteessa turvallistamisen näkökulmasta Kiinan hallitus on haastavassa asemassa, sillä sen täytyy kyetä riittävän uskottavasti turvallistamaan ajatus itsestään vakauden ja nykyisen vaurauden takaajana epäjärjestyksen ja poliittisen levottomuuden uhkaa vastaan. Vaikka

yhteiskuntajärjestyksen muutos on pikemmin uhka hallitukselle kuin valtiolle, on kommunistisen puolueen toistaiseksi onnistunut luomaan olosuhteet, missä sen linjauksia vähintään siedetään. Eräs Suomessa opiskellut kiinalainen opiskelija kiteytti omasta näkökulmasta jännitteen sanoen: ”en näe itselleni tarvetta käyttää Facebookin kaltaisia länsimaisia sivustoja tai länsimaisia uutisia, mutta minusta meillä tulisi olla vapaus valita.”

Onnistuminen tässä hallinnan turvallistamisen ylläpitämisessä ei kuitenkaan ole taattua. Presidentti Xin on onnistunut luomaan puolueineen riittävä turvallistamisen tai vaihtoehtoisesti pelon tila, missä sen toimet aiheuttavat vain vaimeaa vastarintaa. Vaikka hallitus on ajoittain saanut kritiikkiä toimintatavoistaan vakauden ylläpito ja talouskasvu ollut riittävä turvallistamisen kohde.

Kiinan pyrkimys tiukentaa ideologista otetta internetin kaltaisen avoimen datalähteen puitteissa on vaatinut infrastruktuurisesti kaksi toimintalinjaa, millä hallituksen on onnistunut oleellisesti vähentää turvallistamisen perusteluihin kohdistuvia paineita. Tietojärjestelmätasolla Kiina on pakon edessä luonut maailman mahdollisesti sofistikoituneimman palomuurin ja datan eristysjärjestelmän, joka kuitenkin vaatii resursseja jatkuvaan edelleen kehittämiseen. VPN-servereiden kaltaisten vaihtoehtoisten yhteyskeinojen rajoittamisen on vaatinut lisää kohdennettuja toimia. Välillisenä negatiivisena seurauksena Kiinan tiukalle ideologilisille vakauden tavoittelulle on ollut merkittäviä heikennyksiä kiinalaisten verkkojen yhteysnopeuksissa, millä on seurauksia niin kaupallisesti kuin tieteellisestikin. Toisaalta Kiina on edesauttanut kansallisten vaihtoehtoisten sovellusten nousun ilman kansainvälisiä kilpailijoita. Tästä on turvallistamisen ja Kiinan tavoitteiden kannalta kaksi keskeistä etua: 1) Kiina on pystynyt luomaan vaihtoehtoiset palvelut kansalaisilleen, eli turvallistamisen yleisölle. Vaihtoehtoisten palveluiden takia on pystytty liennyttämään painetta ja tarvetta aktiivisesti turvallistaa, miksi kansainvälisiin sosiaalisen median sivustoihin pääsy on rajattu. 2) Kiina on niin valtava sisämarkkina-alue, että sen on ollut mahdollista luoda kasvua ohjelmistoyrityksilleen sekä luomaan tarpeeksi kattavan palvelutarjonnan, ettei turvallistamisen kohteella ole välttämättä omalähtöistä tarvetta kansainvälisiin palveluihin.

Kiinan internetin ja informaation hallinnoinnin politiikassa korostuu valtion sisäisten tavoitteiden ristiriitaisuus. Ideologinen ja yhden puolueen järjestelmän asema pyritään pitää tiukkana, mutta pragmaattinen suhtautuminen kehitykseen ja talouskasvuun luovat paineita kehittää ja tehostaa myös internetin infrastruktuuria. Nykyinen keskitettyjen ulkomailta ja ulkomaille dataa suodattavien muutaman valvotun serverin malli, ei toimintanopeudeltaan ja rajoitteiltaan vaikeuttaa varsinkin monikansallisten yritysten ja yliopistojen toimintaa. Internetin yhteysnopeudet metropoleissakaan eivät

yllä lähellekään Euroopan tai Yhdysvaltojen keskitasoja, mikä vaikeuttaa yritysten arkista toimintaa ja tiedonsiirtoa merkittävästi. Samalla esimerkiksi Googlen ajoittainen kokonaisvaltainen blokkaaminen vaikeuttaa ulkomaisten yritysten sisäistä informaatiokulkua. Toki tämä omalta osaltaan myös vahvistaa kiinalaisten yritysten etulyöntiasemaa Kiinan omilla markkinoilla.

Ongelma ei kosketa ainoastaan yritysmaailmaa, vaan myös tieteellisen tutkimuksen ja teknologisen kehityksen potentiaalia jää Kiinassa käyttämättä merkittävän paljon. Kiinalaisten tutkijoiden ja opiskelijoiden on paikoin vaikeaa tavoittaa länsimaisia tutkimuslähteitä. Tämä koskee niin ympäristöteknologiaa kuin yhteiskunnallisia aineita. Esimerkiksi *smog* on terminä blokattujen sanojen listalla Kiinan datansiirrossa, mutta kytkeytyy olennaisesti moneen ilmanlaatu- ja ilmastotutkimukseen. Kun Kiina samalla yhtäältä pyrkii toimimaan ympäristöteknologian johtavana maana Yhdysvaltojen ympäristöpolitiikan täyskäännöksen jälkeen ja toisaalta rajoittamaan suurkaupunkiensa äärimmäisiä ilmanlaatuongelmia, on tutkimuksen edistämiseen vaadittavan tiedon saatavuuden ja tavoitteiden välillä merkittävä ristiriita.

Tätä kilpailukyvyn haittaa on kommentoitu myös Kiinan parlamentin sisällä, joskin tämä kritiikki oli vuorostaan sensuroitu Kiinan sisäisistä internetlähteistä (South China Morning Post 13.03.2017). Kiinassa ainoan sallitun ei kommunistisen puolueen (Kiinan demokratiaa edustava yhdistys) edustaja Luo Fuhe oli nostanut esille miten kohtuutonta vaivaa kiinalaiset tutkijat joutuivat näkemään hyödyntääkseen kansainvälistä tutkimusdataa (ibid.). Esimerkkinä hän oli nostanut ulkomaisten yliopiston sivustojen ajoittain vaativan lähes puolen tunnin mittaisen latausajan, sensuurijärjestelmän suodattaessa sivuston dataa.

Jos internetsensuuri aiheuttaa merkittävää taloudellista haittaa, vaarantaa se samalla Kiinan hallituksen turvallistamistoimien onnistumista. Kiinan tasainen talouskasvu ja internetin tuoma suhteellinen läpinäkyvyyden parantaminen suhteessa aikaan ennen internetiä ovat antaneet hallitukselle liikkumavaraa informaatiohallinnan turvallistamisessa (China Digital Times 25.3.2015). Mikäli kuitenkin kritiikki Kiinan talouskasvun hidastuessa alkaa aiempaa voimakkaan kohdistua internetinfrastruktuuriin ja sen tuomiin haasteisiin, joutuu kommunistisen puolueen kyky turvallistaa hallintaa uudenlaisen haasteen eteen. Turvallistamisen vuorovaikutteisuus edellyttää uskottavia argumentteja turvallistamisen onnistumiseksi ja tämä sisältää myös varsinaisen informaatiohallinnan ulkopuoliset tekijät.

4.2.2. Kansainväliset turvallistamisen perustelut

Kiina on viimeisten vuosien aikana pyrkinyt CAC:n perustamisen myötä koheesiin kokonaisvaltaiseen kyberpolitiikkaan, joka sisältää sen kansallisen turvallisuuden turvaavia informaatiohallintatoimia ja verkkoturvallisuustoimia. Johdonmukaisesti muunn kansainvälisen kritiikin kanssa, Kiina on reagoinut myös internetsensuuriaan kohtaan esitettyyn kritiikkiin kansallisen suvereniteetin argumentein.

Keskeinen instrumentti Kiinan kansainvälisessä informaatiohallinnan turvallistamisessa on ollut sen luoma *internetsuvereniteetin* käsite. Turvallistamisen teorian näkökulmasta sanavalinta on ilmeisen harkittu. Ensinnäkin suvereniteetin erottamaton osa valtioiden poliittisessa käyttäytymisessä ja kansainvälistä lakia tulkittaessa se tekee termistä Kiinan toimintavapauden kannalta erittäin hyödyllisen. Toisaalta suvereeniuden käsite ja sen sisältämä uhmakkuus Kiinaa kohtaan esitettyyn ihmisoikeuskritiikkiin luo edellytyksiä muiden autoritääristen tai autoritäärisyyden rajoilla operoivien valtioiden hallintojen elimille. Kiinaa pienempien valtioiden päättäjille tämä konsepti tullessaan normiksi, antaisi toimintavapauksia turvallistaa ja hallita näiden maiden omien internetverkkojen informaatiota.

Kiinan armeijan strategisen komitean Ye Zheng julkaisi artikkelin heinäkuussa 2015, missä hän toteaa internetsuvereniteetin olevan kiinalainen innovaatio kansallisen suvereniteetin konseptin rinnalle. Tämä innovaatio on Yen mukaan myös Kiinan valtion ulkopoliittinen missio (China Digital Times 9.10.2015). China Digital Times lainaa myös People's Dailyn artikkelia, jossa todetaan Kiinan läntisten vihamielisten voimien käyttävän verkostoja vihamielisen vaikutteiden levittämiseen. Näiden universaalien arvojen on artikkelin mukaan tarkoitus tuhota kommunistisen puolueen luoma Kiinan valtion järjestelmä. Internetin suvereniteetin konsepti saattaakin olla oletettua tärkeämpi sisäpoliittinen turvallistamisen työkalu hallinnon ja armeijan vuorovaikutuksessa.

Nämä pyrkimykset saivat muodollisen alkunsa loppuvuodesta 2013. Tuolloin valtion internetinformaation ministerinä toiminut Lu Wei piti puheen Iso-Britanniassa, Kiinan ja Iso-Britannian välisessä internettapaamisessa (Xinhua 29.9.2013). Kyseisessä puheessa ministeri Lu esitteli Kiinan tulkintaa internetsuvereniteetista ja internetin hallinnoinnin tulevaisuudesta 6 keskeisellä teesillä:

1) Tasapuolinen mahdollisuus vaikuttaa internetin kehittämisen tulevaisuuteen ja internetsuvereniteetin tunnustaminen.
2) Internetin informaation globaali tasapainottaminen siten, että kaikilla valtioilla olisi yhtäläisempi pääsy informaation, jonka tulisi kulkea globaalisti tehokkaasti, vapaasti ja hallitusti.
3) *Positiivisen energian* levittäminen.
4) Nuoria tulisi suojella internetissä haitalliselta informaatiolta näiden terveen ja tasapainoisen kasvamisen takaamiseksi.
5) Luoda yksityisyyttä ja internetturvallisuutta parantavaa yhteistyötä, jolla varmistetaan ettei yksikään valtio joudu vahingollisen hakkeroinnin kohteeksi.
6) Internetin lain puitteista tehtävä hallinnointi. ”Internet on vapaa ja avoin alusta. Jokaisella on oikeus puhua. Kellään ei kuitenkaan ole oikeutta rikkoa lakeja. Viime vuonna britannialainen uimari Tom Daley sai Twitterin kautta tappouhkauksen jäätyään mitaleitta. Käyttäjä pidätettiin tämän seurauksena […] Kyberväkivalta, internetin juorut ja internethuijaukset ovat internetin kasvaimia. Meidän tulee pitää kiinni periaatteista ja hallinnoida internetiä lain puitteissa. Haluamme luoda yhteistyössä muiden valtioiden kanssa internetin hallintaa YK:n puitteissa, mikä toimisi multilateraalisti, demokraattisesti ja läpinäkyvästi. Tämä tekisi internetistä järjestelmällisempää ja edesauttaisi koko ihmiskunnan hyvinvointia.”

Lu:n esittämistä ajatuksissa on havaittavissa kaksi eri suuntaa. Ensinnäkin kohdat 1 ja 2 ovat sisällöltään kohdistettu selkeästi muille vahvaa internetin itsemääräämisoikeutta toivoville valtioille, joita Kiina on pyrkinyt aktiivisesti saamaan aloitteensa taakse (kts. Luku 3.4). Kiinan intressi tähän on sekä oman vaikutusvallan lisääminen että sen sisäpolitiikkaa kohdistuvan kritiikin rajoittaminen. Kiinan aloitteet internetsuvereniteetin ympärillä eivät toistaiseksi kuitenkaan ole edistyneet kovin merkittävästi muualla kuin pitkälti autoritääristen valtioiden piirissä (China Digital Times 16.9.2016). Yhteistyötä muun muassa Venäjän kanssa on tiivistetty tarjoamalla Venäjän hallinnolle työkaluja luoda Kiinan palomuuria vastaavia esto- ja suodatusjärjestelmiä, minkä seurauksena myös Venäjä on velvoittanut maassa käytettävien internetpalveluiden palvelinten sijoittamisen Venäjälle (China Digital Times 27.4.2016).

Kuten kansallisessa informaation turvallistamisessaan, presidentti Xi ja ministeri Lu ovat nostaneet internetin informaatiohallinnan rinnakkain muun kansallisen turvallisuuden kanssa tekemällä siitä kiinteän osan kansallista suvereniteettia. Kiinan vaikutusvallan kasvaessa sen pyrkimykset kansallisen suvereniteetin laajentamiseen kyberulottuvuuteen on otettava vakavasti. Kiinan suvereniteettimallin ja EU:n edustamien vapaan globaalin internetin mallin taustalla toimii kaksi erilaista logiikkaa, jotka heijastelevat ajatusmaailmoja globaalista järjestyksestä ja valtajakaumasta. Liberaaleissa ympäristöissä internet on kasvanut käyttäjiensä vahvassa valtiohallintovastaisessa eetoksessa, missä valtioita ja niiden puuttumista kritisoidaan voimakkaasti. Kiinassa tätä vastaavaa valtiovaltaa rajoittavaa kokemusta ei internetin nousun yhteydessä ole. EU:ssa ja Yhdysvalloissa voi tuntua käsittämättömältä, että valtiot dominoisivat internetin hallintoa, on Kiinan näkökulmasta yhtä käsittämätöntä, että valtiot eivät olisi hallintoa dominoiva osapuoli (China-US Focus 27.4.2016). Viime vuosikymmenten odotukset, että Kiina muuttuisi kansainvälisten avautumisensa myötä myös sisältä avoimemmaksi ei välttämättä ole toteutumassa myöskään kyberulottuvuuden osalta. Sen sijaan Kiina saattaa kyetä toisaalta avautumaan ja integroitumaan aiempaa voimakkaammin ympäröivään maailmaan, mutta samalla pysymään sisältä tiukasti poliittista toisinajattelua tukehduttavana yksipuoluejärjestelmänä (Mann 2017, 102-104).

Kiinnostavaa Iso-Britannian tapaamisessa on myös Kiinan suora hyökkäys osakseen saamaansa kritiikkiä vastaan. Lun toteamukset 3, 4 ja 6 ovat suoria viittauksia internetin sisällön hallintaan. Lun esille nostama *positiivinen energia* oli yhä keskeinen maan sisäinen hallituksen lausuntojen teema asuessani Kiinassa 2014 lopussa. Käytännössä tämä tarkoitti, että epäkohtiin takertumisen sijaan kansalaisilta toivottiin positiivisessa hengessä tehtyä internetkommentointia, mikä tarkoitti kansallisten menestysten juhlistamista ja kritiikiltä pidättäytymistä. Kohta 4 on suhteellisen ongelmaton myös eurooppalaisesta viitekehyksestä, sillä puheessaan Lu painottaa tällä nimenomaan lasten ja nuorten turvaamista pornografiselta ja väkivaltaiselta materiaalilta.

Keskeisin huomio Kiinan kansallisen suvereniteetin puolustamisen osalta Lun puheessa on kuitenkin kohta 6. Puheessa tehdään kansallisen turvallisuuden tapaan retorinen assimilaatio perinteisen fyysisen turvallisuuden sekä poliittisen hallinnon vakauden välillä. Lu aloittaa pohjustamalla, että internetin sisällön hallinnointi tulisi toteuttaa siten, että jokaisella on oikeus puhua vapaasti (kansallisen) lain puitteissa. Tätä seuraa relativistinen siirto, missä Iso-Britanniassa tappouhkauksien pohjalta tehdyt pidätykset verrataan suoraan Kiinan informaation hallintaan ja lakien rikkomisen seurauksiin.

Argumentti päättyy avoimeen ilmaisuun pyrkiä YK:n puitteissa luomaan kansalliseen suvereniteettiin perustavia internetin hallinnointiin puuttuvia säädöksiä.

Lun puhe on toki vain yksittäinen esimerkki, mutta se kertoo Kiinan ja Euroopan tulkinnallisista eroista, kun puhutaan internetin sisällöstä ja valtioiden roolista. On China-US Focus oikeassa tai ei todetessaan Kiinalle olevan käsittämätöntä ajatella internet ilman valtion vahvaa sisältöä hallinnoivaa roolia, ovat Kiinan nykyiset pyrkimykset vahvasti valtiollisen itsemääräämisoikeuden ja sisäpoliittisen koskemattomuuden linjassa.

Tämän tutkimuksen toteuttamisen kuluessa on datan valvonnan ja datan rajoittamisen kiristämiseksi tehty aloitteita myös muissa maissa. Venäjä on tehnyt suoraa yhteistyötä Kiinan kanssa luodakseen tehokkaampaa palomuuria ja hallintaa rajojen ulkopuolelle. Turkissa on levottomuuksien yhteydessä rajoitettu pääsyä sosiaaliseen mediaan ja viimeisimpänä Turkin valtion epäillään olleen Wikipedian palvelukatkoksen takana. Suomessa datan valvonta on noussut esille tiedustelulain valmistelussa, missä rajojen yli tulevan datan valvontaan luotaisiin uutta järjestelmää. Datan valvonnasta datan hallintaan on intention tasolla merkittävä hyppy, mutta datan valvonnan työkalut ovat ensinnäkin indikaattori datalle annetun merkityksen korostumisesta ja toisaalta luovat teknologisen pohjan myös informaation hallintaan pienemmillä lisäpanostuksilla.

Samaan aikaan Suomi harkitsee vakavasti yhteistä datakaapeliprojektia nimenomaan Venäjän ja Kiinan kanssa, ilman varmuutta muiden läntisten demokratioiden osallistumisesta. Liikenneministeriön hanke ei ensikädessä aiheuttaisi käytännön uhkia suomalaisille internetin käyttäjille, mutta yhteistyö kahden internetin itsemääräämisoikeuden ja sen tuoman informaatiohallinnan kannattajan kanssa loisi ulkopoliittisen imago-ongelman.

5. JOHTOPÄÄTÖKSET JA REFLEKTIOTA

Kiina ei suinkaan ole ainoa valtio joka luo suhdettaan internetiin ja sen käyttäjien vapauksiin. Suomessa, Euroopassa yleensä ja muun muassa Yhdysvalloissa käydään debattia eri tietoteknisten sovellusten yksityisyydestä ja kyberulottuvuuden toiminnan vapaudesta. Kansalliset ja ei-kansalliset uhat ja internetin rooli kommunikaation mahdollistajana ovat johtaneet erinäisiin pyrkimyksiin valvonnan laajentamiseksi ja syventämiseksi.

Kiina on monin tavoin esimerkki miten yhtäältä tehokkaasti informaatiota pystytään rajaamaan, vaikka samaan aikaan Kiinan informaatiohallinnan ongelmat osoittavat, miten vaikeaa internetin kaltaisen järjestelmän täydellinen rajaus on ilman haittavaikutuksia. Samalla VPN-yhteydet ja muut kiertokeinot kertovat siitä, että pääosa uusista esteistä on osaavalle henkilölle kuitenkin ohitettavissa. Eurooppalaisesta sananvapausperinteestä käsin katsottaessa ongelmallisin ja mahdollisesti seurauksiltaan kauaskantoisin vaikutus Kiinan internetpolitiikasta on kansainvälien informaatiohallinnan ja internetin kansallisen suvereniteetin konseptilla. Jos oletetaan Kiinan vankistavan vaikutusvaltaansa Aasiassa, Lähi-idässä ja Afrikassa, on täysin mahdollista että sen toimintatapoja omaksutaan laajemmin muissakin valtioissa.

Kiinan lisääntynyt kansainvälinen vaikutusvalta on myös mahdollistanut maan internetin turvallistamistoimien tiukentamista ilman akuutteja tarpeita onnistuneesti laajentaa internetin kansallista politiikkaansa rajojensa ulkopuolella. Toisin sanoen Kiinan ei tarvitse välttämättä kyetä uskottavasti perustelemaan internetsensuurinsa tiukentamista muille valtioille tai järjestöille jatkossakaan, vaan keskittyä avautumaan kaupallisesti ulospäin pysyen poliittisesti sisäisesti yhä tiukasti hallittuna.

Tutkimuksen kirjoittamisen aikana globaali poliittinen ilmapiiri on muuttunut ja kylmän sodan jälkeinen demokraattinen ja liberaali kehitys vaikuttaisi olevan ongelmissa ainakin väliaikaisesti. Kun kansallisten intressien painoarvo korostuu kosmopoliittisten intressien edelle, helpottuu myös informaatiohallinnan turvallistaminen. Samaan aikaan Yhdysvalloissa tulevan presidentin Donald J. Trumpin hallinnon alaisuuden on arvioitu NSA:n toimivaltuuksien lisäämistä myös internetin valvonnassa. Toistaiseksi fokus Yhdysvalloissa ja Euroopassa on pikemminkin valvoa ja seurata kuin rajata informaatioa, mutta valvonnan infrastruktuuri mahdollistaa nopean siirtymisen informaation

hallintaan. Samalla valvonnan normalisoituessa kynnys hallinnan turvallistamiselle madaltuu, mahdollistaen turvallisuustoimien edelleen voimistamisen.

Nykyisellään Kiinan yhteiskunnan kilpailuhenkisyys itsessään tukee sen internethallinnan turvallistamista. Toistaiseksi valtion talouskasvu on turvannut laajassa kuvassa yhteiskunnallista vakautta. Talouskasvun tärkeys yhteiskunnan tyytyväisyydelle ja poikkeukselliselle tiukalle hallinnoimiselle sisältää kuitenkin myös turvallistamisen onnistumisen suurimman ongelman. Internetin käytön ja sisällön rajoittamisesta aiheutuva haitta kaupalliselle ja tieteelliselle toiminnalle on merkittävää, joskaan ei yksinään ratkaisevaa. Kiinan valtio joutuukin joko kehittämään voimakkaasti sensuurista infrastruktuuriaan entistä nyansoidummaksi ja samalla internetin yhteysnopeuksia tukevaksi tai ennen pitkään höllentämään sisällön hallinnoinnin otetta.

Tutkimukseni tutkimuskysymyksiin palatakseni, voidaan Presidentti Xi Jinpingin valtakaudella havainnoida internetin valvonnan osalta kaksi keskeistä muutosta: kyber- ja informaatioturvallisuuden nouseminen keskeiseen asemaan kansallisen turvallisuuden määritelmässä sekä poliittisen ohjauksen voimistuminen. Tutkimuksessani eritellyistä muutosten osa-alueista keskeisiä tekijöitä on ollut CAC:n perustaminen informaatiohallinnan viralliseksi organisaatioksi. Vaikka Kiina on toisaalta pyrkinyt aktiiviseen vuorovaikutukseen ulkomaailman kanssa, ohjaa Kiinan internetiä aiempaa tiukempi ideologinen kuri, missä poliittisesti ongelmallisten sisältöjen leviäminen laajaan tietoisuuteen pyritään ehkäisemään mahdollisimman tehokkaasti. Perinteiset kommunistiset ja hyveelliset arvot ovat toimineet Xin hallinnon vastapainona aiempaa laajempaan vuorovaikutukseen ulkomaailman kanssa. Tutkimuksen pohjalta voidaan todeta Kiinan internetpolitiikassa kolme keskeistä muutosta: 1) Kiina on kiristänyt ideologista kontrolliaan ja tiukentanut valvontaansa niin uutisoinnin kuin yksityishenkilöiden internetissä jakaman sisällön osalta. 2) Hallitus on tehnyt kyber- ja informaatioturvallisuuden osaksi kansallista turvallisuutta. 3) Kiina pyrkii aktiivisesti muovaamaan kansainvälistä internetsäännöstöä ja luomaan uutta kansallisen internetsuvereniteetin normia.

Toinen tutkimuskysymyksistäni oli määrittää miten Kiinan hallitus on turvallistanut ja perustellut muutoksia internetpolitiikassaan. Kiinan retoriikkaa kansainvälisissä aloitteissaan on painottunut pikemminkin suvereniteetin konseptin ja globaalin valtatasapainon perusteluille kuin sinänsä turvallisuusperiaatteilla. Pyrkimyksenä on lähinnä ollut varmistaa, että hallituksella on mahdollisuus tehdä turvallisuuttaan edesauttavat toimet ilman rajojen ulkopuolelta tulevaa painostusta. Aloitteiden tueksi on toistaiseksi asettunut vasta muita autoritäärisin piirtein johdettuja valtioita. Omien rajojensa sisäpuolella taas Kiinan informaatiohallinnon retoriikka on selkeämmin hahmotettavissa

turvallistamisen konseptin kautta. Arvioidessa asiakirjoja ja lehtiartikkeleiden lainausten retoriikkaa hahmottuu Kiinan internetpolitiikan turvallistaminen Vuoren (2008) turvallistamistyyppien kontrollin kautta. Aineiston pohjalta voidaan arvioida presidentti Xin hallinnon harjoittavan kontrolliin tähtäävää turvallistamista, missä kansalaisille luodaan selkeitä vapauden rajoitteita, jotka perustellaan ideologisten vaikutteiden eksistentiaalisella uhalla. Retorisesti hallitus tekee selkeitä retorisia rinnastuksia kommunistisen järjestelmän ja mallin säilymisen sekä Kiinan valtion jatkuvuuden välille. Mikä tekee Kiinan internetpolitiikan turvallistamisesta nimenomaan kontrolliin tähtäävää turvallistamista, on sen perustelemien rajoitusten suhteellisesti pysyvä luonne ja kansalaisten toiminnanvapauteen tähtäävät toimet.

Turvallistamisen näkökulmasta Kiinan internethallinnan kontrollin turvallistaminen ei ole vielä joutunut ison koetuksen eteen. Ihmisten taloudellisen hyvinvoinnin parantuessa poliittinen tyytymättömyys on rajallista ja pääosalle väestöä sensuuri on varsin pieni murhe. Mikäli talouskasvu tyrehtyy ja yleinen tyytyväisyys hallintoon laskee, joutuu myös informaation hallinnan turvallistaminen uuteen testiin. Tällöin olisi mielenkiintoista arvioida uudestaan turvallistamisen teorian selitysvoimaa yksipuoluejärjestelmässä, missä tyytymättömyys heikentäisi mahdollisesti merkittävästi turvallistamisen onnistumisehtojen täyttymistä. Nykyisessä tilanteessa voidaan lähinnä todeta, että Kiina tekee retorisia turvallistamistoimia tekemällä informaation hallinnasta osan kansallista turvallisuutta ja näin informaation hallinta edistää ja ylläpitää valtion vakautta ja kasvua. Tämän turvallistamisen aspektin laajempi analyysi yskäpuoluejärjestelmissä voisi mielestäni täydentää osaa turvallistamisen teorian puutteista.

Turvallistamisen teoria kohtaa autoritäärisessä järjestelmässä tulkinnallisia ongelmia. Turvallistamisen toteutumisen olosuhteet ovat varsin erilaiset, sillä itsesensuurin ei voida automaattisesti katsoa olevan osoitus turvallistamisen onnistumisesta. Pikemmin kyse voi Williamsin (2011) esiin nostamasta turvallistamisen konseptiin linkittyvästä omaan valtioon kohdistuvasta pelosta. Toisaalta tämä pelko voidaan tulkita turvallistamisen onnistumista edistäväksi olosuhteeksi, joka tyytymättömyyden lisääntyessä menettää merkitystään. Tällöin kriittisen pisteen ylittäessä turvallistaminen voi epäonnistua mahdollisesta pelon vaikutuksesta huolimatta. Sen lisäksi vaihtoehtoiset keinot tavoittaa informaatio palomuurin takaa kielivät siitä, etteivät turvallistamisen perusteet ole välttämättä hyväksyttyjä, vaikka kontrollia ei vastusta avoimesti.

Tutkimukseni tavoitteena oli selvittää Kiinan internethallinnan muutoksia ja hallintaan kytkettyä retoriikkaa. Taustalla oleva motivaationi oli selvittää miten Kiinan valtion toimet perustellaan ja

millaisia esimerkkejä tämä saattaa antaa muille valtioille. Kiina on nykyisessä maailmanpoliittisessa ja kansainvälisen talouden tilanteessa monelle valtio tärkeä sopimuskumppani, mikä voisi varsinkin IT-alalle johtaa tilanteisiin, missä myös EU-kansalaisiin kohdistuu Kiinan kyberpoliittisten linjausten seurauksia. Suomessa tehtävän tutkimuksen ja politiikan analyysin kannalta liikenneministeriön kaapelihankkeen kaltaisten projektien implikaatiot internetin käytölle ja Suomen poliittiselle statukselle eivät ole vähäpätöisiä.

On syytä myös reflektoida tutkimuksen rakenteen ja toteutuksen ongelmia ja puutteita. Ensimmäisenä on syytä todeta, että tutkimuksen edetessä alkoi käymään yhä selvemmäksi, että tutkimukseni aineisto ei täysin soveltunut tarkastelemaan ilmiötä akateemis-teoreettisesta näkökulmasta. Olin aloittanut prosessin merkittävällä kiinnostuksella internetsensuurin turvallisuuspoliittisiin retorisiin perusteluihin ja käytännön vaikutuksiin, joihin olin jo alustavasti ehtinyt tutustua toimiessani harjoittelijana Pekingissä. Harjoittelun ja luonteeltaan journalistisempiin selvityksiin painottunut tutkimuskokemukseni myös myötävaikutti tutkimuksen yleisiin tavoitteisiin, joihin turvallistamisen teoreettinen viitekehys ei täysin pystynyt vastaamaan. Akateemisessa mielessä tutkimukseni kärsikin nähdäkseni toteutukseltaan pikemminkin ulkoministeriön selvityksen tai poliittisen journalistisen artikkelin asettelusta, minkä takia teoriaosuus ja aineisto eivät tukeneet toisiaan riittävän vahvasti luodakseen teoriaohjaavan sisältöanalyysin mukaista dataa teorian kehittämiseksi.

Tulosten selitysvoima on tämän tutkimuksen pohjalta teoreettisesta näkökulmasta rajallinen. Jälkikäteen arvioituna tutkimusmetodi ja teoriaratkaisut eivät välttämättä mahdollista pro gradun mittakaavassa tehtävälle tutkimukselle selkeitä päätelmiä. Turvallistamisen teorian kokonaisvaltainen hyödyntäminen retoriikkaa arvioidessa on rajallista lähdemateriaalien ollessa riippuvaisia siitä, mitä dokumentteja ja lausuntoja on käännetty englanniksi tai muulle tutkijan hallitsemalle kielelle. Nyt tutkimus onnistuu kyllä kartoittamaan ja kuvaamaan Kiinan internetin hallinnan nykytilannetta, mutta turvallistamisen näkökulmasta sen perusteluiden ja yleisösuhteen arviointi on rajallista. Tämä johtuu osittain tutkimuskysymysten muotoilusta, mutta myös turvallistamisen teoriaan sisäisistä ristiriidoista ja ongelmista objektiivisesti mitattavien tulosten tuottamiseen. Toisaalta tutkimus voi toimia poliittisen tilanteen kartoituksellaan sekä identifioimalla joitain turvallistamisen yleisön ja turvallistajan välisen kontrollisuhteen ongelmia, lähtöpisteenä syvemmälle selvitykselle.

Uskon kuitenkin että Kiinan rooli internetin ja informaation määrittelijänä on relevantti tutkimusaihe myös turvallistamisen näkökulmasta. Ottaen huomioon että Kiina on tehnyt yhteistyötä muiden autokratiaan taipuvaisten valtioiden kanssa internetin informaation hallitsemiseksi, sekä arviot

esimerkiksi Venäjän informaatiovaikuttamisesta ovat kansainvälispoliittisesti merkittäviä tulevaisuuden tekijöitä. Riippuen Kiinan lähitulevaisuuden muusta poliittisesta painoarvosta, sillä voi olla merkittävä rooli kansainvälisen säännöstön muovaamisessa, jolloin Kiinan argumentoinnin ja turvallisuusajattelun logiikkaa on tärkeää ymmärtää.

LÄHTEET

MONOGRAFIA

Austin, J.L. (1962), How To Do Things With Words. UK: Oxford University Press

Balzacq, Thierry (2010), Securitization Theory: How Security Problems Emerge and Dissolve. London: Routledge.

Buzan, Barry ja Hansen, Lene (2009), The Evolution of International Security Studies. UK: Cambridge University Press.

Buzan, Barry, Wæver, Ole ja de Wilde, Jaap (1998), Security: A New Framework for Analysis. UK: Lynne Rienner Publishers, Inc.

China Digital Times (2014), Decoding the Chinese Internet: a Glossary of Political Slang. China Digital Times

Hakovirta, H. (2012). Maailmanpolitiikka: Teoria ja todellisuus (2. uud. laitos.). [Tampere]: Kustannus 54.

Harari, Yuval Noah (2016), Homo Deus. UK: Vintage Publishing.

Haukkala, Hiski teoksessa, Forsberg, Tuomas ja Raunio, Tapio (toim.) (2014), Politiikan muutos. Tampere: Vastapaino.

Krippendorff, Klaus (2004), Content Analysis: An Introduction to its Methodology. Sage Publications, Inc.

Mann, James (2017), The China Fantasy: How Our Leaders Explain Away Chinese Repression. Viking Adult.

Searle, John R. (1969), Speech Acts. UK: Cambridge University Press.

Tuomi, Jouni & Sarajärvi, Anneli (2004), Laadullinen tutkimus ja sisällönanalyysi. Jyväskylä: Gummerus Kirjapaino Oy.

Vilkka, Hanna (2017), Tutki ja Kehitä. PS-kustannus

Vuori, Juha A. (2011), How To Do Security with Words - A Grammar of Securitisation in the People's Republic of China. Turku: Uniprint – Turku

Wittgenstein, Ludwig. (1999 [1953]), Filosofisia tutkimuksia. Trans. Heikki Nyman. Juva: WSOY.

Xu, Wu (2007), Chinese Cyber Nationalism: evolution, characteristics and implications. UK: Lexington Books.

ARTIKKELI

Balzacq, Thierry (2005), The three faces of securitization: Political agency, audience and context. *European Journal of International Relations* 11, (4): 171-201.

Balzacq, Thierry (2015), The 'Essence' of securitization: Theory, ideal type, and a sociological science of security. *International Relations* 29(1), 103-113

Bourbeau, Philippe (2014), Moving Forward Together: Logics of the Securitisation Process. *Millennium: Journal of International Studies* Vol. 43(1) 187–206

Demchak, Chris ja Dombrowski, Peter (2011), Rise of Cybered Westhphalian Age. *Strategic Studies Quarterly*. Volume 5, Spring 2011. Air University Press, 31-61.

Gierow, Hauke (2014), Cyber Security in China: New Political Leadership Focuses on Boosting National Security. *China Monitor*. Number 20. Mercator Institute for China Studies. 1-9.

Huysmans, Jef (2011), What's in an act? On security speech acts and little security nothings. *Security Dialogue* 42(4-5) 371-383.

Liang, Bin ja Lu, Hong (2010), Internet Development, Censorship and Cyber Crimes in China. *Journal of Contemporary Criminal Justice* 26(1), Sage Publications, 103-120.

Neumann, Iver B. (2002), Returning Practice to the Linguistic Turn: The Case of Diplomacy. *Millennium: Journal of International Studies* Vol. 31, No. 3, pp. 627-651

Patomäki, Heikki (2015), Absenting the absence of future dangers and structural transformations in securitization theory. *International Relations* 29(1), 128-136

Qiu, Jack L. (1999), Virtual Censorship in China: Keeping the Gate Between the Cyberspaces. *International Journal of Communications Law and Policy*. 4.

Searle, John R. (1975), "A Taxonomy of Illocutionary Acts", in: Günderson, K. (ed.), *Language, Mind, and Knowledge*, (*Minneapolis Studies in the Philosophy of Science*, vol. 7), University of Minneapolis Press, 344-69.

Stritzel, Holger (2007), Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations* Vol. 13(3): 357–383

Stritzel, Holger (2011), Security, the translation. *Security Dialogue* 42(4-5) 343–355

Swaine, Michael D. (2013), Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor*. Fall 2013 Issue 42 Hoover Publications, 1-27.

Vuori, Juha A. (2008), Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders. *European Journal of International Relations* Vol. 14(1) 65–99

Watson, Scott D. (2012), 'Framing' the Copenhagen School: Integrating the Literature on Threat Construction. *Millennium: Journal of International Studies* 40(2) 279-301.

Williams, Michael C. (2011), Securitization and the liberalism of fear. *Security Dialogue* 42(4-5) 453-463

Wæver, Ole (2011), Politics, security, theory. *Security Dialogue* 42(4-5) 465-480.

Wæver, Ole (2015), The theory act: Responsibility and exactitude as seen from securitization. *International Relations* 29(1), 121-127.

INTERNET

Internetsivut:

China Internet Watch <https://www.chinainternetwatch.com/whitepaper/china-internet-statistics/> (Avattu 25.6.2017)

China Law Translate <http://www.chinalawtranslate.com > (Avattu 25.6.2017)

Committee to Protect Journalists <https://www.cpj.org> (Avattu 21.5.2017)

IANA Stewardship Transition Coordination Group <https://www.ianacg.org/plan-to-transition-stewardship-of-key-internet-functions-sent-to-the-u-s-government/> (Avattu 25.6.2017)

Freedom House Report on Internet Freedom <https://freedomhouse.org/report/freedom-net> (avattu 21.5.2017)

YouTube videot*:*

Jenkins, Simon videossa IqSquared "Don't give them what they want: Terrorists should be starved of the oxygen of publicity" <https://www.youtube.com/watch?v=aKTyWXVvp_0> (Avattu 21.5.2017)

Vox "Castro hates the internet, so Cubans created their own" <https://www.youtube.com/watch?v=FFPjJM6yYS8> (Avattu 21.5.2017)

AINEISTO

Asiakirjat:

A/68/50 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24.6.2013). <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf> (Avattu 26.11.2015)

China Intenrnet Network Information Centre: CNNIC 36th Report on Internet Development in China <http://www1.cnnic.cn/AU/MediaC/rdxw/2015n/201507/t20150727_52663.htm> (Avattu 26.11.2015)

Congressional Research Service RL33167: Internet Development and Information Control in the People's Republic of China. (10.2.2006)

European Chamber of Commerce in China (12.2.2015) Press release: Internet Restrictions Increasingly Harmful to Business, say European Companies in China. <http://www.europeanchamber.com.cn/en/press-releases/2235/internet_restrictions_increasingly_harmful_to_business_say_european_companies_in_china> (Avattu 25.11.2015)

Information Office of the State Council of the People's Republic of China. (2010). White Paper: The Internet in China. http://www.china.org.cn/government/whitepaper/node_7093508.htm (Avattu 25.11.2015)

Kiinan, Venäjän, Kirgsisian, Tajikistanin, Uzbekistanin ja Kasakhstanin edustajien kirje YK:n pääsihteerille (9.1.2015) Code of Conduct in Cyberspace. <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf> (Avattu 26.11.2015)

Liikenne- ja viestintäministeriön Selvitys Koillisväylän tietoliikennekaapelihankkeesta (25.11.2016). <https://www.lvm.fi/documents/20181/880507/Raportit+ja+selvitykset+2-2016.pdf/16cc0f68-5fd7-4262-a288-db0647284ce0> (Avattu 8.1.2017)

Liikenne- ja viestintäministeriön tiedote (14.01.2015) < https://www.lvm.fi/-/lvm-vaatii-lisaa-keskustelua-verkkovalvonnan-tehokkuudesta-ja-vaikutuksista-796311> (Avattu 26.6.2017)

U.S.-China Economic and Security Review Commission Staff Report (6.5.2014). China and International Law in Cyberspace. <http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf> (Avattu 26.11.2015)

Uutisartikkeli:

BBC (19.11.2014), China we conference opens amid internet freedom criticism. <http://www.bbc.com/news/world-asia-china-30110430> (Avattu 25.11.2015)

BBC (03.05.2017), China announces tighter regulations for online news. <http://www.bbc.com/news/technology-39791781> (Avattu 10.05.2017)

Bloomberg (21.11.2014), Scarves and declarations unravels at World Internet Conference. <http://www.bloomberg.com/news/2014-11-21/declarations-and-scarves-unravel-at-world-internet-conference.html> (Avattu 25.11.2015)

Business Insider UK (24.9.2015), Microsoft Threw Bing and MSN Under the Bus to Promote Windows 10 in China. <http://uk.businessinsider.com/microsoft-baidu-deal-in-china-2015-9?r=US&IR=T> (Avattu 25.11.2015)

CCTV (11.9.2015), Lu Wei delivers keynote speech to China-Arab States Expo Online Silk Road Forum. <http://english.cntv.cn/2015/09/11/ARTI1441925703537251.shtml> (Avattu 26.11.2015)

China Daily (30.1.2015), China to hold 2nd World Internet Conference in October. <http://www.chinadaily.com.cn/business/tech/2015-01/30/content_19449819.htm> (Avattu 25.11.2015)

China Digital Times (25.3.2015), China: No need for an open internet? <http://chinadigitaltimes.net/2015/03/china-no-need-for-open-internet/> (Avattu 24.11.2015)

China Digital Times (7.5.2015), Analysts voice concern over draft national security law. <http://chinadigitaltimes.net/2015/05/analysts-voice-concern-over-draft-national-security-law/> (Avattu 26.11.2015)

China Digital Times (11.5.2015), China and Russia support cyber sovereignty. <http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/> (Avattu 25.11.2015)

China Digital Times (1.7.2015), China approves sweeping national security law <http://chinadigitaltimes.net/2015/07/china-approves-sweeping-security-law-bolstering-communist-rule/> (Avattu 26.11.2015)

China Digital Times (9.10.2015), Re-Defining Cyberspace <http://chinadigitaltimes.net/2015/10/re-defining-cyberspace/> (Avattu 14.12.2015)

China Digital Times (1.3.2016), Social Media Purge Goes Far Beyond Ren Zhiqiang <http://chinadigitaltimes.net/2016/03/social-media-purge-goes-far-beyond-ren-zhiqiang/>

China Digital Times (27.4.2016), Chinese Cyberchiefs Preach Net Sovereignty in Moscow <http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-internet-sovereignty-moscow/> (Avattu 1.5.2017)

China Digital Times (16.9.2016), How China's Cyberspace Administration Works. <http://chinadigitaltimes.net/2016/09/chinas-cyberspace-administration-works-doesnt/> (Avattu 2.5.2017)

China Internet Watch (24.11.2014), Renren had 219 million MAU's, less login users in Q3 2014. <http://www.chinainternetwatch.com/10928/renren-q3-2014/> (Avattu: 25.11.2015)

China Internet Watch (16.11.2015), Tencent in Q3 2015: QQ MAUs 850M, WeChat MAUs 650M. <http://www.chinainternetwatch.com/15592/tencent-q3-2015/> (Avattu 25.11.2015)

China Internet Watch (20.11.2015), Weibo MAU's reached 222 million in Q3 2015. <http://www.chinainternetwatch.com/15740/weibo-q3-2015/> (Avattu 25.11.2015)

China-US Focus (27.04.2016), Recognizing China's Internet Governance Despite Its Foundational Opposition to Western Values. <http://www.chinausfocus.com/political-social-

development/recognizing-chinas-internet-governance-despite-its-foundational-opposition-to-western-values/>

Cnet (22.9.2014), Search engine DuckDuckGo blocked in China. < https://www.cnet.com/news/search-engine-duckduckgo-now-blocked-in-china> (Avattu 10.10.2016)

Committee to Protect Journalists (30.10.2015), In China, harsh penalties for 'false news' make it harder for reporters to work. <https://cpj.org/blog/2015/10/in-china-harsh-penalties-for-false-news-make-it-ha.php> (Avattu 25.112015)

The Diplomat (22.1.2015), China and Internet Sovereignty Revisited. <http://thediplomat.com/2015/01/china-and-internet-sovereignty-revisited/> (Avattu 25.11.2015)

The Diplomat (21.8.2015), Have Russia and China signed a cyber nonaggression pact? >http://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/> (Avattu 25.11.2015)

The Guardian (11.2.2014), Bing censoring Chinese language search results for users in the US. <http://www.theguardian.com/technology/2014/feb/11/bing-censors-chinese-language-search-results> (Avattu 25.11.2015)

The Independent (30.1.2015), China's great firewall gets higher: tools to evade surveillance and site bans are blocked as Chinese internet censors tighten grip. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/chinas-great-firewall-gets-higher-tools-to-evade-surveillance-and-site-bans-are-blocked-as-chinese-10013537.html> (Avattu 25.11.2015)

The New York Times (2.6.2014), China Escalating Attack on Google. <http://www.nytimes.com/2014/06/03/business/chinas-battle-against-google-heats-up.html> (Avattu 25.11.2015)

The New York Times (1.12.2014), Gregarious and Direct: China's Web Doorkeeper. <http://www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper.html?_r=1> (Avattu 25.11.2015)

Reuters (20.3.2015), Reuters Becomes Inaccessible in China. <http://www.reuters.com/article/2015/03/20/us-china-reuters-idUSKBN0MG0CV20150320#4I5HpWoZuMd0obsb.97> (Avattu 25.11.2015)

South China Morning Post (8.7.2015), Why China's draft cybersecurity law has chilling implications for the internet and multinationals. <http://www.scmp.com/news/china/policies-politics/article/1834506/chinas-publishes-draft-cybersecurity-law-implications> (Avattu 25.11.2015)

South China Morning Post (13.3.2017), China's internet censorship under fire – but proposal against controls gets ... censored. <http://www.scmp.com/news/china/policies-politics/article/2078350/chinas-internet-censorship-under-fire-two-sessions> (Avattu 21.5.2017)

Vice (28.1.2017), The Data That Turned the World Upside Down.

< https://motherboard.vice.com/en_us/article/big-data-cambridge-analytica-brexit-trump> (Avattu 13.4.2017)

The Wall Street Journal (7.8.2014), China Tightens Grip on Messaging Apps. <http://www.wsj.com/articles/china-issues-new-restrictions-on-messaging-apps-1407405666> (Avattu 25.11.2015)

The Wall Street Journal (30.1.2015), China's great firewall gets taller. <http://www.wsj.com/articles/chinas-great-firewall-gets-taller-1422607143> (Avattu 26.11.2015)

The Wall Street Journal (10.6.2015), China's slow internet a drag on businesses, European chamber says. <http://blogs.wsj.com/chinarealtime/2015/06/10/chinas-slow-internet-a-drag-on-businesses-european-chamber-says/> (Avattu 25.11.2015)

The Wall Street Journal (18.8.2015), U.S. Delays Giving Up Oversight of Internet Administrator ICANN. <http://www.wsj.com/articles/u-s-delays-giving-up-oversight-of-internet-administrator-icann-1439851721> (Avattu 25.11.2015)

The Wall Street Journal (22.9.2015), Full Transcript: Interview with Chinese President Xi Jinping. <http://www.wsj.com/articles/full-transcript-interview-with-chinese-president-xi-jinping-1442894700> (Avattu 26.11.2015)

Xinhua (9.9.2013), Lu Wei: Liberty and Order in Cyberspace (Full Text). <http://news.xinhuanet.com/english/china/2013-09/09/c_132705681.htm> (Avattu 25.11.2015)

Xinhua (20.11.2014), China holds first World Internet Conference, urges better governance. <http://news.xinhuanet.com/english/china/2014-11/20/c_127230940.htm> (Avattu 25.11.2015)