Informaatioteknologian tiedekunnan julkaisuja
No. 99/2023

Isokangas, Jyrki (toim.)

Tiedustelun maailma: Kiina
Tiedusteluanalyysi I -kurssin raportteja

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 99/2023

Toimitus: Jyrki Isokangas
Kannen kuva: SeanPavone, www.elements.envato.com

ISBN 978-951-39-9604-8 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2023

Tiedustelun maailma: Kiina
Tiedusteluanalyysi I -kurssin raportteja

Jyrki Isokangas

2023

Sisällys

Esipuhe

Tiedusteluopetus on keskeinen osa Jyväskylän yliopiston Turvallisuus- ja strateginen analyysi -maisteriohjelmaa. Tiedusteluanalyysi I -kurssilla opiskelijat laativat ryhmätyönä raportin tiedusteluun liittyvästä aiheesta. Nämä työt eivät ole vielä varsinaisia tiedusteluanalyysejä, vaan niiden tarkoituksena on tutustuttaa opiskelijat tiedusteluun liittyviin ilmiöihin. Syksyn 2022 kurssilla laadituista ryhmätöistä on toimitettu Jyväskylän yliopiston informaatioteknologian tiedekunnan julkaisusarjaan kaksi eri julkaisua. Toinen julkaisuista käsittelee tiedustelun muutosta. Tämän julkaisun aiheena on Kiina.

Kiina on ollut jo useita vuosia yksi maailman nopeimmin kasvavista talouksista. Maa onkin noussut Yhdysvaltojen ohella toiseksi 2000-luvun suurvalloista, niin taloudellisesti, poliittisesti kuin sotilaallisestikin. Nousulle on luonnollisesti useita syitä. Tässä julkaisussa tarkastellaan Kiinan tiedustelun roolia maan kehityksessä. Tiedustelun merkitys tästä näkökulmasta jää julkisuudessa usein vähälle huomiolle.

Ensimmäinen raportti käsittelee Kiinan tiede- ja teknologiatiedustelua. Länsimainen jako tiedustelun toimijoiden ja kohteiden mukaan on haasteellinen tehtävä, sillä Kiinassa tiedusteluksi luettavaa tiedonhankintaa tekevät useat toimijat läpi yhteiskunnan. Lisäksi Kiinalla on yrityksiä ja kansalaisia yhteistyöhön velvoittava lainsäädäntö. Kiinan tiede- ja teknologiatiedustelu palvelee maan pitkäjänteisiä teknologisia tavoitteita.

Toinen raportti tarkastelee Kiinan Belt and Road Initiative (BRI) -hankkeen käyttöä hybridivaikuttamisen välineenä. Hybridivaikuttaminen on toimintaa, joka kohdistuu valtioiden ja instituutioiden systeemisiä haavoittuvuuksia vastaan. Vuonna 2013 alkanut Kiinan nykyinen BRI-hanke on massiivinen infrastruktuuriprojekti, joka koordinaation, päätöksentekoon vaikuttamisen ja Kiinan etujen ajamisen osalta mahdollistaa hybridivaikuttamisen. Avoimeksi jää, käyttääkö Kiina tätä mahdollisuutta hyväkseen.

Kolmas raportti käsittelee Kiinan tietoverkkotiedustelua ja -vakoilua osana sen strategisten päämäärien tavoittelua. Tietoverkoissa tapahtuvalla tiedonhankinnalla on keskeinen merkitys Kiinan kommunistiselle puolueelle, joka tarvitsee tietoja valtioista, suuryrityksistä, toisinajattelijoista, poliittisista toimijoista, ja jopa omista kansalaisistaan. Tietoverkkoteknologian tutkimus ja tuotekehitys on ollut yksi Kiinan painopisteistä, ja maa onkin noussut maailman johtavaksi toimijaksi. Kiinasta käyty keskustelu painottuu usein taloudelliseen riippuvuuteen ja sen vaikutuksiin maiden turvallisuuteen. Samanlainen keskustelu olisi tarpeen käydä myös Kiinan verkkovakoilusta.

Neljäs raportti tarkastelee Kiinan tiedustelua Pohjoismaissa, missä Kiina nähdään Venäjän ohella keskeisimpänä tiedustelua ja vakoilua tekevänä toimijana. Kiinan yrityksiä ja kansalaisia koskeva velvoittava lainsäädäntö mahdollistaa käytännössä maailmanlaajuisen henkilötiedusteluverkoston luomisen, jopa yritysten ja kansalaisten tahdon vastaisesti. Lainsäädäntö ja yhteiskuntajärjestelmä ohjaavat ihmiset tiedonhankkijoiksi.

Julkaisun tarkoituksena ei ole Kiinan arvostelu. Tavoitteena on nostaa esille tiedustelun rooli suurvallaksi laskettavan maan globaalissa toiminnassa. Tästä näkökulmasta aiheesta on Suomessa kirjoitettu varsin vähän.

Kaikki raportit on julkaistu raportit kirjoittaneiden opiskelijoiden luvalla.

Toivon mielenkiintoisia lukuhetkiä julkaisun parissa!

Jyväskylässä 19.4.2023
Yliopistonopettaja, FM, eversti evp. Jyrki Isokangas

Lyhenteet

1MDB	1Malaysia Development Berhard, Malesialainen strateginen kehitysyhtiö.
2PLA	Kiinan asevoimien (engl. People's Liberation Army, PLA) yleisesikunnan sotilastiedusteluosasto.
3PLA	Kiinan asevoimien signaali- ja kybertiedusteluosasto.
4PLA	Kiinan asevoimien elektronisen sodankäynnin osasto.
5G	engl. fifth generation, viidennen sukupolven datayhteys mobiilitekniikassa.
APT	engl. Advanced Persistent Threat, hyvät resurssit omaava, pitkäjänteisesti toimiva ja kyberturvallisuutta uhkaava toimija.
BRI	engl. Belt and Road Initiative, Kiinan vuonna 2013 käynnistämä kehityshanke, "uusi silkkitie".
CCP	engl. China's Communist Party, Kiinan kommunistinen puolue, myös Communist Party of China's, CPC.
CDSTIC	engl. China Defense Science and Technology Information Center, Kiinan sotilaallisen tieteen ja teknologian tietokeskus.
CIA	engl. Central Intelligence Agency, Yhdysvaltojen keskustiedustelupalvelu.
CICC	engl. China International Commercial Court, Kiinan lainsäädännöllinen ratkaisuelin käsittelemään kansainvälisiä kauppariita-asioita.
CISA	engl. Cybersecurity & Infrastructure Agency, Yhdysvaltojen kyberturvallisuudesta ja infrastruktuurista vastaava viranomainen.
CMC	engl. Central Military Commission, Kiinan keskussotilaskomitea.
EU	Euroopan Unioni
FBI	engl. Federal Bureau of Investigations, Yhdysvaltojen liittovaltion poliisi, joka vastaa mm. vastatiedustelusta.
GSD	engl. General Staff Department, Kiinan kansan vapautusarmeijan (People's Liberation army, PLA) entinen yleisesikunnan osasto.
HLMC	Shanghai Huali Microelectronics Corporation, kiinalainen puolijohteiden valmistaja.
HUMINT	engl. Human intelligence, henkilötiedustelu.
IOT	engl. Internet of Things, esineiden internet.
ISTIC	engl. Institute of Science and Technical Information of China, Kiinan tieteellisen ja teknologisen informaation instituutti.
JHICC	Fujian Jinhua Integrated Circuit Co. Ltd., kiinalainen muistivalmistaja.
JSD	engl. Joint Staff Department, Kiinan kansan vapautusarmeija PLA:n yleisesikunnan osasto.
JSSD	engl. Jiangsu Province Ministry of State Security, valtion turvallisuusministeriön Jiangsun alueen osasto.
MOFCOM	engl. Ministry of Commerce of People's Republic of China, Kiinan kauppaministeriö.
MOST	engl. Ministry of Science and Technology, Kiinan tiede- ja teknologiaministeriö.
MPS	engl. Ministry of Public Security. Ministeriö, joka vastaa Kiinan sisäisestä turvallisuudesta ja järjestyksen ylläpitämisestä.

MSIRC	engl. Military Science Information Research Center, sotilastieteellinen tutkimuskeskus.
MSS	engl. Ministry of State Security, valtion turvallisuusministeriö, vastaa Kiinan sisäisestä ja ulkoisesta tiedustelusta ja turvallisuudesta.
NSA	engl. National Security Agency, Yhdysvaltojen kansallinen turvallisuusvirasto.
NUAA	engl. Nanjing University of Aeronautics and Astronautics, Nanjingin aeronauttinen ja astronauttinen yliopisto.
OBOR	engl. One Belt, One Road -ohjelma.
OECD	engl. Organisation for Economic Co-operation and Development, taloudellisen yhteistyön ja kehityksen järjestö.
PH-LIITTO	mal. Pakatan Harapan, engl. The Alliance of Hope, malesialainen poliittinen koalitio.
PLA	engl. People's Liberation Army, Kiinan kansan vapautusarmeija.
PST	norj. Politiets Sikkerhetstjeneste, Norjan sisäisen turvallisuuden palvelu.
SSF	engl. Stategic Support Force, PLA:n verkkotiedustelun osaamisen keskittymä.
SUPO	Suojelupoliisi, sisäministeriön alainen turvallisuus- ja tiedustelupalvelu.
SÄPÖ	ruots. Säkerhetspolisen, Ruotsin sisäisen turvallisuuden palvelu.
THE FIVE EYES	Tiedusteluyhteistyöjärjestely, johon kuuluvat Australia, Kanada, Uusi-Seelanti, Iso-Britannia ja Yhdysvallat.
TKI-toiminta	Tutkimus-, kehitys- ja innovaatiotoiminta.
TSMC	Taiwan Semiconductor Manufacturing Company, Ltd., taiwanilainen puolijohteiden valmistaja.
TTP	engl. Thousand Talent Program, Kiinan hallituksen ohjelma osaajien houkuttelemiseksi Kiinaan.
UMC	United Microelectronics Corporation, taiwanilainen puolijohteiden valmistaja.
UMNO	engl. United Malays National Organisation, malesialainen poliittinen puolue.
VPS	engl. Virtual Private Server, virtuaalinen palvelin.
WTO	engl. World Trade Organization, Maailman kauppajärjestö.
ZTE	Zhongxing Telecommunication Equipment Corporation, kiinalainen televiestintälaitteiden ja verkkoratkaisujen toimittaja.

KIINAN TIEDE- JA TEKNOLOGIATIEDUSTELU

Suvi Ahonen, Johannes Riska, Harri Sinnelä, Sami Turpeinen

1 Johdanto

Heti 1800-luvun oopiumsotien jälkeen Kiina ryhtyi kehittämään ulkomaankauppaa ja yliopistojärjestelmää sekä rakentamaan omaa teollisuutta. Opiskelijoita lähetettiin eurooppalaisiin yliopistoihin, ja monet Kiinan yliopistoista perustettiin länsimaisen mallin mukaan. Ohjenuoraksi otettiin konfutselaisuudesta ammentava ti-yong-ajattelu, jossa kiinalaisen yhteiskunnan ydin on absoluuttinen, mutta sitä voidaan vahvistaa oppimalla ja ottamalla käyttöön länsimaisia sovelluksia. Yhteistyö, vuorovaikutus ja muilta oppiminen jatkuu edelleen. Osaa toiminnasta voidaan pitää läntisestä näkökulmasta tiedusteluna.

Toiminta on usein keskittynyt tietyille strategisille aloille. Esimerkiksi 1980-luvulta alkaen kiinnostuksen kohteina ovat olleet biologia, avaruusteknologia, tietotekniikka, tuotantoautomaatio, laserteknologia, raaka-aineet ja merentutkimus. Vuoden 2015 Made in China 2025 -strategian painopistealueina ovat puolestaan mikropiirit, tietoliikenne, numeerinen ohjaus, tietojärjestelmät, robotiikka, ilmailuteollisuus, laivanrakennus, rautatieteollisuus, energiatehokkuus ja -teollisuus, maatalouskoneet, metalli- ja materiaalivalmistus, biofarmaseuttinen tutkimus sekä lääkinnälliset laitteet (State Council, 2015).

Tässä raportissa keskitytään kiinalaisten tahojen tekemään tiede- ja teknologiatiedusteluun. Tätä tarkemman rajauksen tekeminen tiedustelun toimijan mukaan on vaikeaa, sillä tiedusteluun rinnastettavaan aktiviteettiin osallistuu useita eri toimijoita. Osa toimijoista on suoraan valtion johdossa. Tiedustelutoiminta voi kohdistua yrityksiin, akateemisiin instituutioihin ja muihin organisaatioihin, joilla on hallussaan Kiinaa kiinnostavaa tietoa. Tarkkaa rajausta ei näin ollen voida tehdä myöskään tiedonhankinnan kohteiden mukaan.

Raportissa käsitellään sellaista tiedustelutoimintaa, jonka tavoitteena on kerätä kiinalaisen tieteen ja teknologian edistämisessä hyödynnettävää tietoa, toimijasta riippumatta. Kiinalaista ajattelutapaa, jossa omavaraisuus yhdistyy tehokkaaseen tiedonhankintaan ulkomailta, voi olla myös vaikeaa hahmottaa länsimaisesta näkökulmasta. Kiinalaista toimintaa leimaa kansallisten kunnianhimoisten suunnitelmien tuoma aikapaine, jonka vuoksi tavoitteita edistetään usein keinoja kaihtamatta.

Luvussa 2 taustoitetaan Kiinan tiede- ja teknologiatiedustelua kuvaamalla maan tiedusteluhistoriaa ja -ajattelua. Luvussa tarkastellaan myös aiheen rajauksen kannalta keskeisimpiä tiedusteluorganisaatioita. Luvun tavoitteena on esitellä lyhyesti kiinalaisen tiedustelun suuria linjoja. Yritystoiminnan tiedustelua käsittelevässä luvussa 3 esitetään eri menetelmiä, joilla Kiina hankkii teknologista osaamista ulkomaisista yrityksistä. Luvun päätteeksi esitellään muutama tapaus, jotka kuvaavat tiede- ja teknologiatiedustelun käytännön toteutusta. Luvussa 4 avataan kiinalaista tiedustelutoimintaa länsimaisissa korkeakouluissa ja tutkimuslaitoksissa. Luku jakautuu taustoittavaan alalukuun, tiedustelutoimintaan erityisesti tekniikan ja luonnontieteiden aloilla sekä Kiinan

pehmeään vaikuttamiseen länsimaisten yliopistojen rinnalla toimineiden Konfutse-instituuttien kautta.

Raportti keskittyy Kiinan tiede- ja teknologiatiedusteluun länsimaissa. Muihin maanosiin ja alueisiin kohdistuvaan kiinalaiseen tiedusteluun viitataan satunnaisesti viitteissä. Luvun 2 taustoittavaa osiota lukuun ottamatta raportissa käytetyt lähteet ja esimerkit ovat ensisijaisesti vuosilta 2010-2022.

2 Taustaa Kiinan tiedusteluajattelusta

2.1 Ulkomaisen teknologian käytön pitkät perinteet

Ti-yong-periaate kiihtyi Kiinan kansantasavaltaa perustettaessa 1940-luvulla. Ajatuksen perustana on varjella kiinalaisen yhteiskunnan ydintä, sekä valikoida länsimaisesta tiedosta omia tarkoitusperiä parhaiten palvelevat käytännön sovellukset. Nuoren kansantasavallan tieteellisteknologiset pyrkimykset olivat painottuneita kiinalais-neuvostoliittolaiseen yhteistyöhön viisivuotissuunnitelmineen. Yliopistojen asema heikkeni, kun teolliset ja teknologiset vaikutteet pyrittiin ohjaamaan yliopistolaitoksen ohi suoraan käytäntöön kansallisen tiedeakatemian kautta. Perustutkimus näivettyi ja huomio kohdistui lähes yksinomaan teolliseen tuotantoon. Samassa yhteydessä neuvostoteknologiaa ja -suunnitelmia kopioitiin tehokkaasti ja sovellettiin edelleen omiin tarpeisiin. (Hannas ym., 2013)

Yhteistyön kariutuminen Neuvostoliiton kanssa 1950-luvun lopulla, puhemies Maon Suuri harppaus sekä kulttuurivallankumous 1960-luvulla aiheuttivat Kiinan tieteellisen ja teknologisen kehityksen lähes täydellisen seisahtumisen. Länsimaiset vaikutteet kiellettiin ja esimerkiksi opiskelijavaihto oli olematonta noin 20 vuoden ajan. Vaikka ulkomaisen teknologian hankkiminen oli jo vakiintunut toimintatapa, tulokset olivat kulttuurivallankumouksen aikana heikkoja. Poliittisia ansioita korostettiin tieteellisteknisen osaamisen kustannuksella. Kiinan kansallista omavaraisuutta korostettiin ja ajatus omavaraisuudesta leimaa edelleen ajattelua. Vuonna 1975 Kiinan kansankongressi julkisti ohjelman, joka tunnetaan nimellä Neljä modernisaatiota. Sen tarkoituksena oli nostaa Kiina maailman johtavien valtioiden joukkoon vuoteen 2000 mennessä. Modernisaation tuli tapahtua neljällä sektorilla: maataloudessa, teollisuudessa, kansallisessa puolustuksessa sekä tieteessä ja teknologiassa. Yhdysvallat nähtiin tavoitteiden kannalta keskeiseksi tiedon ja teknologian lähteeksi. (Hannas ym., 2013)

Vuonna 1986 päätettiin kansallisen tutkimuksen ja tuotekehityksen ohjelmasta, jolla oli tarkoitus vastata maailmanlaajuisiin haasteisiin ja kansainväliseen kilpailuun. Tavoitteeksi asetettiin luoda Kiinasta kilpailukykyinen maailmanluokan toimija valituilla aloilla. Alusta alkaen luotiin tiivis kytkentä asevoimiin Kiinan tiede- ja teknologiaministeriön (MOST, engl. Ministry of Science and Technology) koordinoimana. Tämän jälkeen on käynnistetty keskusjohtoisesti useita ohjelmia korkean teknologian, yliopistouudistuksen sekä perustutkimuksen aloilla. Kaikille näille on yhteistä laaja kansainvälinen yhteistyö ja kiinalaisten opiskelijoiden ja tutkijoiden kautta tapahtuva teknologian siirto Kiinaan. (Hannas ym., 2013)

2.2 Avointen tietolähteiden käyttö tiede- ja teknologiatiedustelussa

Kiinan kansantasavallan alkuvuosina tietopääoma perustui pääosin Neuvostoliitosta saatuihin oppeihin. Muualla ulkomailla opiskelleiden henkilöiden joukko oli pieni. Hankittu osaaminen ei mahdollistanut kehitystä edes jatkotutkimuksen avulla. Kiinan tiede- ja teknologiapyrkimysten edistämiseksi rakennettiin erittäin kehittynyt järjestelmä avointen tietolähteiden käytölle. Tästä tiedonhankinnasta on tullut keskeinen selittäjä Kiinan talouden kehitykselle.

Jo 1950-luvun puolivälistä sovellettu tieteen ja teknologian kehittämisohjelma velvoitti ”raportoimaan kaikista tieteen ja teknologian saavutuksista kaikilta aloilta niiden tehokkaan soveltamisen mahdollistamiseksi ja Kiinan tieteellisteknologisen kehityksen edistämiseksi”. Vuonna 1958 perustettiin Kiinan tieteellisen ja teknologisen informaation instituutti (ISTIC, engl. Institute of Science and Technical Information of China), jonka tehtäväksi määrättiin tieteellis-teknologisen tiedon hankinta, prosessointi ja jakelu. (Hannas ym., 2013)

2.3 Tiedonhankinnan kehittäminen

2.3.1 Teknologisen tietovarannon aktiivinen rakentaminen

Tehokkaan tiedonhankintakoneiston kehittäminen ajoittui osin samaan aikaan Suuren harppauksen kanssa, vaikka ajallinen yhteys vaikuttaa ristiriitaiselta. Tänä aikana kuitenkin perustettiin asevoimiin kyky vieraskielisten materiaalien kääntämiseen. Lisäksi lähes kaikille hallinnonaloille sekä ministeriöille muodostettiin omat tieteellis-teknologisen tiedon hankintatoiminnot. Noin 1960-luvun puoleenväliin mennessä oli rakennettu yhteinen tietovaranto, johon sisältyi miljoonia tieteellisiä tutkimuksia, teknologisia standardeja, patentteja ja materiaalinäytteitä. (Hannas & Chang, 2021)

Avoimesti julkituotuina tavoitteina oli ”parantaa Kiinan kykyä tehdä tutkimusta, kopioida asioita ja valmistaa tuotteita”, sekä ylläpitää ajantasaista käsitystä maailmanlaajuisesta teknologisesta kehityksestä. (Hannas ym., 2013). Tiedonhankinnan kohteena korostui sotilasteknologia. Koko järjestelmää kutsutaan nimellä qingbao. Kielellisesti tai käsitteellisesti termissä ei ole samanlaista eroa tiedonhankinnan ja tiedustelun välillä kuin esimerkiksi suomen kielessä.

2.3.2 Huomion suuntaaminen korkean teknologian aloihin

Noin 1970-luvun lopulta alkaen tiedonhankinta kehittyi modernisaatiopyrkimysten myötä. Kiina elvytti tieteellisen ja teknologisen tiedon seuran, joka oli lähes hävinnyt kulttuurivallankumouksen aikana. Sen toiminta-ajatusta täsmennettiin kattamaan ulkomaisen tieteellisen ja teknisen materiaalin keräämisen kaikenlaisissa tilaisuuksissa ja kaikista lähteistä. ISTIC:n puitteissa aloitettiin uusi kirjastotieteen ja informatiikan oppiaine, jossa keskityttiin pelkästään ulkomaisen tieteellisen tutkimuksen keräämiseen ja hyväksikäyttöön. Jo 1980-luvun puolivälissä ulkomaista tieteellis-teknologista informaatiota keräsi ja analysoi yli 60 000 henkilöä. Kun qingbao korkeimmalla poliittisella taholla kytkettiin talouden kehitystavoitteisiin, voidaan hyvällä syyllä todeta Kiinan kansantasavallan luoneen merkittävän järjestelmän avointen lähteiden tiedonhankintaan valtion strategisten tavoitteiden edistämiseksi. Digitalisaation myötä suurten tietomassojen hallinta on tullut aikaisempaa vaativammaksi, ja 1990-luvun alkupuolelta lähtien tiedonhankintaa on tehty aikaisempaa kohdennetummin. (Hannas ym., 2013)

Kiinan tiede- ja teknologiatiedustelun keskeisimmät mielenkiinnon kohteet ovat määräytyneet 2020-luvulla Kiinan kommunistisen puolueen teollisuus- ja teknologiapolitiikan Made in China 2025 -ohjelman mukaisesti. Sen tavoitteena on siirtää Kiinan tuotannon painopistettä valmistavasta teollisuudesta kohti teknologiaintensiivisempiä aloja. (Eftimiades, 2020)

2.4 Kiinalaiset tiedusteluorganisaatiot

Tiedustelu palvelee Kiinan kommunistisen puolueen ja keskushallinnon tavoitteita. Keskeinen koordinoiva taho on vuonna 1983 perustettu valtion turvallisuusministeriö (MSS, engl. Ministry of State Security), joka voi laajoin toimivaltuuksin velvoittaa minkä tahansa kiinalaisen organisaation myötävaikuttamaan ja tukemaan tiedustelua. Organisaatiomuutosten lisäksi tiedustelun toimintaedellytyksiä on parannettu lainsäädännöllisin keinoin. Yksilöt ja yhteisöt ovat velvollisia avustamaan viranomaisia ankarien rangaistusten uhalla (Eftimiades, 2020).

Kiina on kyennyt luomaan 2000-luvulla vahvan ja maailman ensimmäisen digitaalisen autoritäärisen valtion (Cain, 2022). Tiedustelu-, vakoilu- ja valvontakoneisto kattaa koko yhteiskunnan. Tiede- ja teknologiatiedustelu on tässä tärkeä elementti. Keskeisten organisaatioiden toiminta-ajatus on länsimaisesta näkökulmasta kyseenalainen. Periaatteessa kaikki yritykset, yksittäiset henkilöt, tutkimuslaitokset ja yliopistot tekevät tiedustelua. Siksi länsimainen jako tiedustelupalveluihin ja ei-tiedustelupalveluihin ei ole useinkaan mielekäs. (Eftimiades, 2020)

Kiinan tiede- ja teknologiatiedustelu kattaa koko hallinnon. Kiinan tieteellisen ja teknologisen informaation instituutti ISTIC on keskeisin siviilitiedustelun toimija. Asevoimien puolella keskeisin organisaatio on sotilastieteellinen tutkimuskeskus (MSIRC, engl. Military Science Information Research Center). Toisin kuin valtion turvallisuusministeriö MSS, nämä organisaatiot kertovat toiminnastaan suhteellisen avoimesti. (Eftimiades, 2020)

2.4.1 Kiinan tieteellisen ja teknologisen informaation instituutti (ISTIC)

Oman määritelmänsä mukaan ”ISTIC kerää ja käsittelee ulkomaisia tieteellisiä julkaisuja, tekee niistä analyysejä ja tietokantoja Kiinan tarpeiden ja kansallisten etujen mukaisesti. ISTIC myös ylläpitää tietopalveluita ja kehittää kansainvälistä yhteistyötä tieteen ja teknologian alalla” (Hannas & Chang, 2021). Kiinan tiede- ja teknologiaministeriö MOST:n mukaan ISTIC:llä on teknologian alalla Kiinan suurin ja merkittävin tietovaranto. Tiedon keräys on kohdennettua ja se tukee ”aktiivisesti valtiollisia tutkimus- ja tuotekehitysprojekteja kattavan politiikkalähtöisen strategisen tutkimuksen keinoin kehityksestä ja saavutuksista maailmanlaajuisesti keskeisille valtiollisille toimijoille” (Hannas & Chang, 2021). ISTIC osallistuu myös valtiolliseen tiede- ja teknologiasuunnitteluun ja tukee MOST:in päätöksentekoa ja viisivuotissuunnitelmien valmistelua. Lisäksi se laatii toimintaohjeita ja teknisiä standardeja. Toimintaan kuuluvat myös tieteellisten julkaisujen tarkistus, tutkimusapurahojen myöntäminen, tekijänoikeuksien hallinta sekä asiakirjojen salaustasojen määrittäminen (Hannas & Chang, 2021).

ISTIC valitsee ja kouluttaa ulkomaille lähetettävän tieteen ja teknologia-alan tiedusteluhenkilöstön, sekä raportoi laajasti kommunistisen puolueen keskuskomitealle, kansalliskokoukselle ja valtiojohdolle (Hannas ym., 2013). Kiinan tieteellisen ja teknologisen informaation instituuttia ISTIC:iä voidaan näin hyvällä syyllä luonnehtia

tiedusteluorganisaatioksi. On kuitenkin huomattava, että sen toiminta perustuu avointen lähteiden tiedonhankintaan ja analyysiin. (Hannas & Chang, 2021)

2.4.2 Sotilastieteellinen tutkimuskeskus (MSIRC)

Sotilaallinen avointen lähteiden tiedustelu on keskitetty sotilastieteelliseen tutkimuskeskukseen (MSIRC), jonka rooli tiedonkeräyksessä vastaa ISTIC:iä. Organisaation juuret ovat Kiinan kansan vapautusarmeijan sotatieteellisessä akatemiassa ja Kiinan sotilaallisen tieteen ja teknologian tietokeskuksessa (CDSTIC, engl. China Defense Science and Technology Information Center). (Hannas & Chang, 2021)

MSIRC:n tehtäväksi on määritelty "ulkomaisen tieteellis-teknologisen materiaalin tarjoaminen, tiedonvaihdon järjestäminen, analyysi ja materiaalin laatiminen päätöksentekoa varten" (Hannas & Chang, 2021). MSIRC pitää saavutuksinaan ydinaseen, sekä ballististen ohjusten ja satelliittien kehittämistä. Ehkä yllättäen myös MSIRC on kuitenkin leimallisesti avointen lähteiden tiedusteluun keskittynyt organisaatio. (Hannas & Chang, 2021)

3 Yritystoiminnassa tapahtuva tiedustelu

3.1 Yleisesti Kiinan teknologiatiedustelusta

Viime vuosina julkisuuteen on tullut useita tapauksia, joissa kiinalaistaho on pyrkinyt hankkimaan ulkomaista teknologiaa ja liikesalaisuuksia. (Department of Justice, 2018f; Joske, 2020). Tietoa on hankittu sekä tietomurtojen kautta että henkilötiedustelun avulla. Tietoa ja osaamista on voitu hankkia myös muilla tavoin, kuten yritysjärjestelyjen kautta. Tiedonhankinnan keinot vaihtelevat tilanteen ja tiedonhankkijoiden mukaan. (Department of Justice, 2018a, 2018f; Joske, 2020)

Samoihin kohteisiin on joissakin tapauksissa kohdistettu tiedustelua useita kertoja tai samanaikaisesti eri menetelmillä. Toiminta on vaikuttanut ajoittain hyvin opportunistiselta. Kiinan tiedusteluorganisaatiot pyrkivät hankkimaan ulkomailta eri keinoin teknologiaa ja liikesalaisuuksia. Lisäksi maassa toimivat yritykset palkkaavat itselleen osaajia ulkomailta. Nämä voivat osaamisensa lisäksi tuoda mukanaan kilpailijan yrityssalaisuuksia. Lisäksi Kiinassa kiinnostusta herättävää teknologiaa ja osaamista saatetaan yrittää hankkia ostamalla yrityksiä tai palkkaamalla konsultteja. Järjestelyt voidaan toteuttaa esimerkiksi peiteyrityksiä hyödyntäen tiedonkeräyksen todellisen päämäärän peittämiseksi. (Joske, 2020; O'Connor, 2019; Department of Justice, 2018a, 2018f; Mozur, 2021; United States Attorney's Office, Northern District of California 2020; United States District Court for the Southern District of Ohio, Western Division, 2022)"

3.2 Teknologiatiedustelu henkilötiedustelun avulla

Viime vuosina on tullut julki useita tapauksia, joissa Kiina on hankkinut henkilötiedustelulla yritysten immateriaalioikeuksiin ja liikesalaisuuksiin liittyvää teknologista osaamista. (Department of Justice, 2018f; Joske, 2020). Tapauksille on ollut tyypillistä tietojen kopiointi ja siirtäminen omistajan ulottumattomiin. Tapauksia ei kuitenkaan yhdistä mikään erityinen toimintamalli, mutta tiedustelutoiminnan operaatioturvallisuudessa on lähteiden mukaan ollut toisinaan puutteita. (Brown, 2009; Eftimiades 1994).

Toiminnan peittämiseksi on kuitenkin nähty ajoittain huomattavan paljon vaivaa. Joskus tiedonkeräystä on ohjannut Kiinan tiedusteluhallinnon osa ja ajoittain Kiinassa toimiva yritys. Eräissä tapauksista toiminta vaikuttaa alkaneen tiedot omistavan organisaation työntekijän aloitteesta, työntekijän huomatessa tiedolle olevan kysyntää Kiinassa. Usein työntekijän toimitettua työnantajansa liikesalaisuuksia Kiinassa toimivalle kilpailijalle, hänet on samalla palkattu tiedot vastaanottaneeseen organisaatioon. Usein työntekijällä on ollut aikaisempia sidoksia Kiinaan. Rekrytoinnin kohteeseen on voitu ottaa yhteyttä eri tavoin, esimerkiksi sosiaalisen median kautta (mrkoot 2022) tai kutsumalla kohdehenkilö tapahtumaan, jossa valehenkilöllisyydellä toimiva tiedustelija tapaa hänet ”sattumalta”. Tiedusteluviranomaisten operaatioissa on myös värvätty mukaan kiinalaisen yhteiskunnan muitakin osia, esimerkiksi yliopistoja. (Brown, 2009)

3.3 Teknologiatiedustelu kybertiedustelun avulla

Länsimaiset viranomaiset ja turvallisuusalan yksityiset toimijat ovat edellisten vuosikymmenien aikana tunnistaneet useita kybertiedustelun operaatioita, joiden tekijöiksi on nimetty Kiinaan liitettyjä henkilöitä tai ryhmiä. Kohteina on ollut muun muassa valtioita, yksityisiä yrityksiä, kansainvälisiä järjestöjä sekä muita Kiinaa kiinnostavia organisaatioita. Usein tekijöiksi epäiltyjen ryhmien arvioidaan toimineen valtion turvallisuus- ja tiedustelupalveluiden tuella, vaikkakin itsenäisesti. Ryhmien katsotaan olevaan APT-ryhmiä (engl. Advanced Persistent Threat), ja niille on annettu yleisen tavan mukaan muitakin nimiä. (Department of Justice, 2018b; Department of Justice, 2020a)

Tyypillisessä kybertiedusteluoperaatiossa on käytetty melko kattavasti erilaisia tietomurtoihin käytettäviä menetelmiä. Eri ryhmillä on kuitenkin hieman toisistaan poikkeavia toimintatapoja, joiden perusteella niiden erottaminen toisistaan on mahdollista. Kiinalaisiksi epäiltyjä ryhmiä ja toimijoita on runsaasti. Kaksi tunnettua ryhmää ovat APT10 (tunnetaan myös mm. nimillä Red Apollo, MenuPass, Stone Panda) ja APT41 (Winnti, Barium, Wicked Panda). Molempien ryhmien on arvioitu toimivan yhteistyössä Kiinan tiedustelu- ja turvallisuuspalveluiden kanssa. (Department of Justice, 2018b; Department of Justice, 2020a)

Vaikka ryhmät eivät ole suoraan valtiollisia toimijoita eikä Kiina ole tunnustanut niiden toimivan valtion lukuun, on Kiinaa kuitenkin syytetty ryhmien suojelusta. Ryhmien tunnistaminen ja nimeäminen julkisesti ei myöskään näyttäisi vaikuttavan merkittävästi niiden aktiivisuuteen. Esimerkiksi APT41 tuomittiin tietomurroista Yhdysvalloissa vuonna 2020 ja muutamia siihen liitettyjä ei-kiinalaisia henkilöitä pidätettiin Malesiassa. Kiina ei kuitenkaan pidättänyt omia kansalaisiaan Yhdysvaltojen pyynnöstä huolimatta (Department of Justice, 2020a). Sen sijaan APT41 on jatkanut paljastumisen jälkeen toimintaansa sekä Kiinassa (Chen ym., 2021) että ulkomailla. (Cybereason, 2022)

Kiinassa astui kesällä 2021 voimaan laki, joka velvoittaa raportoimaan tietojärjestelmistä löydetyt haavoittuvuudet valtiolle. Lain perusteluna käytettiin tietoturvan parantamista. Ainakin Microsoft on syyttänyt Kiinaa marraskuussa 2022 siitä, että näitä raportoituja haavoittuvuuksia on hyödynnetty tietomurroissa ja kybertiedustelussa. (Microsoft, 2022)

3.4 Teknologiatiedustelu muilla menetelmillä

3.4.1 Kohdennetut osaajarekrytoinnit

Vuonna 2007 käynnistettiin ”Talent Superpower Strategy” -ohjelma, jonka yhtenä osana oli ohjelma nimeltään ”Thousand Talent Program” (TTP). Ohjelman tavoitteena oli rekrytoida ulkomailla opiskelleita ja menestyneitä kiinalaisia takaisin kotimaahansa (Stoff, 2020) Rekrytointikampanjoita kohdennettiin myös muiden maiden kansalaisiin.

Rekrytointiohjelmien kohteina on ollut niin akateemisen kuin liikemaailman henkilöitä. Monet ohjelmista ovat toimineet vuodesta 2019 lähtien “The High-End Foreign Expert Recruitment Plan” -hankkeen alla. Eri ohjelmilla on myös eri fokus. Esimerkiksi tietty strateginen tieteenala ja kohdehenkilöiden toivotut ominaisuudet vaihtelevat, mutta yhteistä kaikille on meritoituneiden osaajien houkuttelu tukemaan Kiinan sisäistä kehittymistä. Osaajien rekrytoimiseksi on ulkomaille perustettu paikallisia keskuksia, joiden toiminta on tosin usein ulkoistettu jo maassa toimiville Kiinaan liittyville järjestöille. (Joske, 2020; Weinstein, 2020)

Tavoitetta tukeakseen esimerkiksi teknologiayritys Huawei on toistuvasti kohdistanut omia rekrytointipanostuksiaan sellaisiin maantieteellisiin alueisiin, joissa sen kilpailijat toimivat. Huawei rekrytoi ahkerasti esimerkiksi San Diegossa, Tukholmassa ja Ottawassa Ericssonin ja Nortelin irtisanomia työntekijöitä. Tällainen rekrytointi on erityisen tehokasta, sillä irtisanomistilanteissa kilpailukieltosopimukset usein päättyvät välittömästi ja irtisanottujen henkilöiden lojaliteetti entistä työnantajaa kohtaan on koetuksella. (Schaefer, 2020) Huawei on myös tehnyt yhteistyötä länsimaisten yliopistojen kanssa (ks. Tylecote & Clark, 2021).

3.4.2 Liiketoiminnalliset keinot

Kiinalaiset toimijat pyrkivät saamaan pääsyn muiden maiden yritysten teknologioihin myös erilaisten yritysjärjestelyjen kautta. Näiden järjestelyiden tavoitteena on kaupallisin keinoin päästä kiinni kohteiden omistamaan osaamiseen ja teknologiaan. Pääosa toiminnasta on laillista, ja Kiina myös painostaa ulkomaisia yrityksiä lainsäädännöllisin keinoin. Toimintatapana voi olla esimerkiksi vaatimus edellyttää yhteisyrityksen perustamista kiinalaisen osapuolen kanssa. Länsimaiset yritykset saatetaan myös velvoittaa lisensioimaan teknologiaa kiinalaisille. (O’Connor, 2019)

Kiinalaisten toimijoiden on myös epäilty käyttäneen järjestelmällisesti peiteyrityksiä hankkiessaan teknologiaa, johon heillä ei olisi muuten sanktioiden tai vientirajoitusten takia ollut pääsyä. (Allen, 2022) Esimerkiksi Italiassa paljastui vuonna 2021 tapaus, jossa kiinalaisten yritysten väitettiin hankkineen peiteyritysten avulla enemmistöomistuksen paikallisesta drooneja sotilaskäyttöön valmistavasta yrityksestä (Reuters, 2021).

Myös erilaisten konsultointiyritysten toiminta Kiinassa on saanut huomiota viime vuosien aikana vakoiluun tai eturistiriitoihin liitettyjen epäilyjen vuoksi. Vuonna 2014 Kiina kielsi useita yhdysvaltalaisia konsultointiyrityksiä toimimasta Kiinan valtioon liitettyjen yritysten kanssa syyttäen niitä vakoilusta (Anderlini, 2014). Vuonna 2021 puolestaan Yhdysvalloissa heräsi huoli konsultointijätti McKinseyn toiminnasta, sen tarjotessa palveluja niin Yhdysvaltojen puolustushallinnolle kuin Kiinan valtion instituutioille (Luce, 2021). Konsulttien käyttö oman osaamisen kehittämiseksi on kuitenkin normaalia kaikissa maissa, eikä ole erityistä syytä olettaa etteivätkö kiinalaiset yritykset tai toimijat hyödyntäisi konsulttien muualta hankkimaa osaamista omien hankkeidensa

edistämiseen. On myös vaikeaa erotella konsultin omaan ammattitaitoon liittyvää osaamista liikesalaisuuksista.

3.5 Esimerkkejä teknologiaan kohdistuneesta tiedustelutoiminnasta

3.5.1 APT10

APT10-ryhmittymä toteutti vuosina 2014–2017 laajan teknologiaorganisaatioihin kohdistuneen kybertiedusteluoperaation, joka länsimaissa tunnetaan nimellä Cloud Hopper. Cloud Hopper -operaatiossa ensimmäisinä kohteina olivat informaatioteknologiapalveluja tuottavat yritykset, joihin päästiin tyypillisesti sisään hyödyntämällä kohdennettujen sähköpostien avulla levitettyjä haittaohjelmia. Haittaohjelmat olivat yhteydessä APT10:n kontrolloimaan komentopalvelimeen. Tätä kautta ryhmä sai pääsyn yrityksen järjestelmiin ja pystyi jatkamaan tunkeutumistaan järjestelmien sisällä, samalla hyödyntäen niissä olevia erilaisia haavoittuvuuksia. (PwC, 2017)

Seuraavassa vaiheessa ryhmä tunnisti palveluntarjoajan asiakaskunnasta sitä kiinnostavat kohteet. Ryhmä aloitti luottamuksellisen liiketoimintatiedon keräämisen ja kopioimisen järjestelmistä. Kiinnostavia kohteita olivat mm. lääketieteelliset yritykset, energiayritykset, teknologiayritykset, julkishallinto ja teollisen valmistamisen yritykset, erityisesti Pohjois-Amerikassa, Euroopassa ja Etelä-Aasiassa. (PwC, 2017; Department of Justice, 2018b) APT10 on liitetty myös Airbusiin kohdistuneeseen tietomurtoon vuonna 2018. Myös tässä tapauksessa varsinainen pääsy järjestelmiin tehtiin alihankkijan järjestelmän kautta. (Izambard ym., 2020)

3.5.2 APT41

APT41 on ollut aktiivinen ainakin vuodesta 2012 alkaen. Ryhmä aloitti tietomurrot pelialan yrityksistä, mutta on vuodesta 2013 alkaen kohdistanut toimintaansa myös korkean teknologian yrityksiin ja ainakin vuodesta 2017 myös verkkoteknologian yrityksiin. APT41 käyttää useita eri menetelmiä tiedon hankkimiseen, esimerkiksi asentamalla pääsyn mahdollistavan takaoven (engl. backdoor) haittaohjelman sisältämien sähköpostien avulla.

Tietoturvayritys Mandiantin tekemän analyysin perusteella toiminnassa ei ole ollut kyse pelkästä teknologian kopioimisesta, vaan operaatioilla on toteutettu myös taktisemman tason tiedustelutehtäviä. Esimerkkinä APT41 on pyrkinyt saamaan pääsyn Kiinan markkinoille pyrkineen yrityksen puhelutietoihin ja tietojärjestelmiin. (Fraser ym., 2019)

3.5.3 Ilmailuteollisuuteen kohdistuva tiedustelu

Kiinan kansalainen Xu Yanjun tuomittiin Yhdysvalloissa yrityksistä varastaa vuosina 2017–2018 liikesalaisuuksia (Department of Justice, 2018c; Department of Justice, 2021; US District Court for the Southern District of Ohio, Western Division, 2022). Julkaistun syytteen mukaan Xu on Kiinan kansantasavallan tiedustelu-upseeri, valtion turvallisuusministeriö MSS:n Jingsun maakunnan osaston varapäällikkö. (MSS:n haara Jiangsussa tästedes ”JSSD”). Hänen tehtäviinsä on kuulunut ulkomailla toimivien ilmailu- ja avaruusteknologiayhtiöiden liikesalaisuuksien hankkiminen. Toimintatapana oli tunnistaa kiinnostava teknologia ja tämän perusteella maalittaa alan johtavat yritykset ja niiden asiaintuntijat. (Department of Justice, 2018c; US District Court for the Southern District of Ohio, Western Division, 2022)

Syytteen mukaan Xu on ollut esimerkiksi järjestämässä yhdysvaltalaisen GE Aviationin työntekijälle kutsun esiintyä Nanjingin aeronauttisella ja astronauttisella yliopistolla (NUAA; engl. Nanjing University of Aeronautics and Astronautics) ja maksanut tämän matkan. Ilmeisesti Xu on tällöin esitelty valehenkilöllisyydellä GE Aviationin työntekijälle. Syytteen mukaan Xu järjesti työntekijälle rahapalkkion ja kulukorvauksen esityksestä sekä piti yhteyttä työntekijään matkan jälkeen. Työntekijä kutsuttiin seuraavanakin vuonna NUAA:han. (Department of Justice, 2018c; US District Court for the Southern District of Ohio, Western Division, 2022) Yhdysvaltojen oikeusministeriön mukaan oli tyypillistä, että MSS hakkeroi kohdehenkilöiden hotelliinsa jättämät tietokoneet henkilöiden ollessa pois huoneestaan. (Department of Justice, 2022). Xu myös ohjeisti työntekijää, miten GE Aviationin aineistoa saisi välitettyä sen tietojärjestelmistä Kiinaan (Department of Justice, 2018c).

Toisessa tuomioon johtaneessa tapauksessa Xu käsitteli vuosina 2013–2018 Yhdysvaltojen maavoimissa palvelevaa henkilöä. Tehtävänä oli hankkia taustatietoja rekrytointia varten Taiwanissa tai Kiinassa syntyneistä henkilöistä, jotka työskentelivät Yhdysvalloissa esimerkiksi ilmailuteollisuudessa. Ainakin alkuvaiheessa Xu esiintyi valehenkilöllisyydellä, professorina NUAA:ssa. (Department of Justice, 2018c; Department of Justice, 2018d; United States Attorney's Office, Northern District of Illinois, 2022) Xu pidätettiin lopulta Belgiassa. (Department of Justice 2018f; 2021)

Myös toista GE Aviationin työntekijää vastaan nostettiin Yhdysvalloissa syyte yrityssalaisuuksien varastamisesta. Tässä tapauksessa työntekijä kopioi vuosien 2014–2018 aikana työnantajansa tietoja, salasi ne, ja välitti ne steganografiaa (tiedon piilottaminen muun tiedon joukkoon) hyödyntäen eteenpäin. Työntekijän kiinalainen liikekumppani oli korostanut poliittisten virkahenkilöiden olevan kiinnostuneita tiedoista ja yhteistyöstä. (Department of Justice, 2019)

Kiinan valtion turvallisuusministeriön Jiangsun maakunnan osasto (JSSD) on pyrkinyt kerämään aktiivisesti tietoa ilmailuteollisuudesta. JSSD:n työntekijät murtautuivat vuosina 2010–2015 muun muassa ranskalaisen ohivirtausmoottorien valmistajan Safran Aircraft Enginesin ja yhdysvaltalaisen kaasuturbiinien valmistajan Capstone Turbine Corporationin tietojärjestelmiin. Ainakin yhdessä tietomurrossa käytettiin hyväksi myös yrityksen omia työntekijöitä. Heidän avullaan saatiin fyysinen pääsy tietojärjestelmiin ja kyettiin asentamaan haittaohjelma USB-muistista. (Department of Justice, 2017; Department of Justice, 2018a; Department of Justice, 2018e; Department of Justice, 2019; Lynch & Shepardson, 2018; United States District Court for the Northern District of New York, 2018)

3.5.4 Puolijohdeteollisuuteen kohdistuva tiedustelu

Kiina pyrkii kehittämään omaa puolijohdeteollisuutta (Zhong & Li, 2020). Tämän vuoksi tiedustelun kohteena on ollut muun muassa yhdysvaltalainen puolijohdevalmistaja Micron Technology Inc. (tästedes "Micron"), jonka kiinalaisyritys halusi ostaa jo vuonna 2015 (Mozur, 2021).

Yhdysvalloissa ja Taiwanissa on sittemmin nostettu syytteitä kahta yritystä, Kiinan kansantasavallassa toimivaa Fujian Jinhua Integrated Circuitia (JHICC) ja Taiwanissa toimivaa United Microelectronics Corporationia (UMC) vastaan. Lisäksi kolmea entistä Micronin taiwanilaisen tytäryhtiön työntekijää on syytetty yrityksen liikesalaisuuksien varastamisesta. (Wang & Hu, 2018).

Syytteiden mukaan syytetyt varastivat Micronin liikesalaisuuksia vuosien 2015–2016 aikana. Taiwanilainen työntekijä palkattiin Micronin taiwanilaisesta tytäryhtiöstä ensin UMC:hen, ja myöhemmin JHICC:hen. Tällöin hän oli mukana järjestämässä yritysten yhteistyötä muistiteknologian hankkimiseksi. Työntekijä palkkasi UMC:hen lisää työntekijöitä entiseltä työnantajaltaan. Rekrytoidut työntekijät kopioivat lähtiessään Micronilta muun muassa Micronin suunnitelmia ja teknisiä tietoja muistiteknologiasta, ja välittivät tiedot UMC:lle ja JHICC:lle. (Department of Justice, 2018e) UMC on sittemmin tunnustanut osansa varkaudessa (United States Attorney's Office, Northern District of California, 2020). Taiwanissa on langetettu tuomioita tästä tapauksessa (Taipei Times, 2022).

Tiedossa on toinenkin tapaus, jossa Kiinassa toimiva yritys, Shanghai Huali Microelectronics Corporation (HLMC), olisi yrittänyt hankkia toisen puolijohdevalmistajan, Taiwan Semiconductor Manufacturing Company (TSMC), liikesalaisuuksia tämän työntekijän kautta. Taiwanilaisen syytteen ja tuomion mukaan HLMC tarjosi vuonna 2016 työntekijälle esimiestehtävän, johon tämä ei ollut pätevä. Vastineeksi työntekijä kopioi TSMC:n tuotantoprosessiin liittyvää aineistoa, jota olisi ottanut mukaansa HLMC:hen. (Taipei Times, 2017)

4 Tiedustelu yliopistoissa ja tutkimuslaitoksissa

4.1 Yleisesti Kiinan tiedustelusta ja vaikuttamisesta TKI-toiminnassa

TKI-toiminnan (tutkimus-, kehitys- ja innovaatiotoiminta) keskeisiin toimijoihin lukeutuvat yritysten lisäksi yliopistot ja tutkimuslaitokset. Niiden toimintaan kuuluu lähtökohtaisesti neutraaleja tai positiivisia piirteitä, jotka toisaalta muodostavat niistä vaikuttamiselle ja tiedustelutoiminnalle alttiita ympäristöjä. Tutkimustoiminta on useimmilla tieteenaloilla lähtökohtaisesti kansainvälistä. Sekä opiskelijoiden että tutkijoiden kansainvälistä liikkuvuutta ja verkostoitumista pyritään lisäämään osaamisen kehittämiseksi. Kiinalaistaustaiset opiskelijat ovat esimerkiksi muodostaneet osassa Iso-Britannian yliopistoja kolmasosan EU:n ulkopuolelta tulevien opiskelijoiden ryhmästä. Osa Yhdysvaltojen yksityisistä yliopistoista on taloudellisesti riippuvaisia kiinalaisten opiskelijoiden maksamista lukukausimaksuista (Ross, 2021).

Tutkijoille ja opiskelijoille on järjestetty useissa maissa omat viisumijärjestelmänsä, joiden tarkoituksena on helpottaa koulutetun työvoiman liikkuvuutta. Lisäksi kansainvälisenä trendinä tutkimuksen (julkaisujen, aineistojen, tutkimusprosessien) avoimuuden lisääntyminen luo uudenlaisia haasteita. Myös korkeakoulujen ja tutkimuslaitosten yhteydet ensimmäisen, toisen ja kolmannen sektorin toimijoihin ovat ulkomaisten tiedustelutoimijoiden kiinnostuksen kohteina (European Commission, 2022).

4.2 Tiedustelutoiminta korkeakouluissa ja tutkimuslaitoksissa

Kiinassa ei ole länsimaisessa merkityksessä akateemista vapautta. Yliopistot toimivat kommunistisen puolueen ja opetusministeriön ohjauksessa (Ross, 2021). Kiinan valtion näkökulmasta haasteena on ollut lahjakkaiden tutkijoiden ja opiskelijoiden aivovuoto etenkin länsimaisiin yliopistoihin. Tämän estämiseksi perustetun ”Thousand Talent Program” (TTP) -ohjelman kautta onkin onnistuneesti rekrytoitu sekä kiinalaistaustaisia länsimaissa toimineita että johtavia länsimaalaisia tutkijoita.

Tutkijoiden kaksoisaffiliaatiot länsimaisissa ja kiinalaisissa yliopistoissa katsottiin aiemmin ansioiksi. Kiinan aggressiivisen toiminnan, ja etenkin Yhdysvaltojen Kiina-politiikan muutoksen myötä, länsimaisten tutkijoiden tutkimusyhteistyö kiinalaisten ja kiinalaistaustaisten tutkijoiden kanssa on hiipunut vuodesta 2019 lähtien voimakkaasti (Van Noorden, 2022).

Brittiläisen ajatushautomo Civitaksen julkaiseman raportin (Tylecote & Clark, 2021) mukaan useissa brittiläisissä yliopistoissa on tehty kiinalaisten monialayhtiöiden rahoittamaa tutkimusta, jossa länsimaiset tutkijat ovat tukeneet tietämättään kaksoiskäyttötuotteiden kehittämistä. Kaksoiskäyttötuotteella viitataan tuotteisiin tai palveluihin, joilla on siviilikäytön lisäksi mahdollinen sotilaallinen funktio. Rahoittajayrityksillä on ollut yhteyksiä muun muassa joukkotuhoaseiden, mannertenvälisten ballististen ohjusten sekä hypersoonisten ohjusten tuotantoon.

Kiinaa kiinnostavat tutkimusalueet liittyvät muun muassa metalleihin, tekoälyyn, kasvojentunnistusteknologiaan, drooneihin, tutkiin ja robotiikkaan. Myös Suomen opetus- ja kulttuuriministeriön julkaisu vuodelta 2021 Kiinan tiedetiedustelusta mainitsee mahdolliset kaksikäyttötuotteet- ja teknologian Kiina-yhteistyön haasteina.

4.3 Tiedustelu ja vaikuttaminen Konfutse-instituuteissa

Teknologisten innovaatioiden ja kehitystyön lisäksi Kiinan valtio toteuttaa länsimaisissa yliopistoissa humanistis-yhteiskuntatieteellisten alojen ja tiedekuntien kautta tapahtuvaa tiedustelu- ja vaikuttamistoimintaa. Tätä toimintaa on organisoitu vuodesta 2004 lähtien yli 280 eri maassa yliopistojen rinnalla toimivien Konfutse-instituuttien kautta. Instituutit ovat järjestäneet kieli- ja kulttuurikoulutusta, ja niiden toimintaa on kritisoitu Kiinan valtion propagandan levittämisestä ja sen kannalta vaikeista kysymyksistä vaikenemisesta (Lo & Pan, 2014; Luqiu & McCarthy, 2019).

James Ton (2014) mukaan Konfutse-instituuttien tarkoitus on vaikuttaa isäntämaan politiikkaan siten, että se myötäilisi Kiinan valtion päämääriä. Euroopan komission TKI-toiminnan ulkomaista vaikuttamista käsittelevä dokumentti (2022) antaa yhtenä “fiktiivisenä” esimerkkinä ulkomaisesta häirinnästä korkeakoulujen yhteyteen perustetut kieli- ja kulttuuri-instituutit, joiden tehtävänä on levittää propagandaa ja disinformaatiota sekä fasilitoida kohdemaassa tapahtuvaa vakoilua.

Viime vuosina useat yliopistot, mukaan lukien Helsingin yliopisto, ovat irtisanoneet sopimuksensa instituuttien kautta. Konfutse-instituutit ovat noudattaneet totalitaristiselle Kiinalle ominaista ulkopolitiikkaa, jota kuvaavat yhtä lailla esimerkiksi Kiinan sitä kriittisesti tutkiville ajatushautomoille ja tutkijoille asettamat pakotteet. Tutkijoita ja taustaorganisaatioita ohjataan myös rahoituksella ja velvoittavilla yhteistyösopimuksilla itsesensuuriin (Puranen 2021). Esimerkiksi Pohjois-Carolinan valtionyliopisto perui vuonna 2009 Tiibetin johtajan Dalai Laman vierailun poliittisten syiden vuoksi (Edwards, 2021).

Konfutse-instituuttien, samoin kuin muidenkin kiinalaistaustaisten toimijoiden, on esitetty myös etsivän haavoittuvuuksia länsimaisten organisaatioiden ja yhteiskuntien infrastruktuurista (Edwards, 2021; Sharma, 2020). Kiinan tiedustelutoiminta länsimaisissa yliopistoissa ja tutkimuslaitoksissa ei kuitenkaan kohdistu ainoastaan tutkimukseen ja infrastruktuurin haavoittuvuuksiin, vaan tiedustelun kohteena voivat olla myös Kiinan omat kansalaiset. Toisin sanoen tutkimusvakoilu kytkeytyy osittain Kiinan

pakolaisvakoiluun, jonka tarkoituksena on tarkkailla ja kontrolloida Kiinan valtion näkökulmasta haitallisia henkilöitä ja ryhmiä (esimerkiksi toisinajattelijat ja uiguurit). (ks. Dolma, 2021)

4.4 Esimerkkejä Kiinan tiedustelusta ja vaikuttamisesta TKI-ympäristöissä

Suhteellisen harvoissa Yhdysvalloissa julkisuuteen tulleissa Kiinan vakoilutapauksissa on ollut kyse suoranaisesta teknologisten innovaatioiden varastamisesta. Tavanomaisesti kiinalaisen tiedustelun jäljet TKI-ympäristöissä näkyvät esimerkiksi tutkijoiden piilotettuina rahoituslähteinä (engl. double-dipping). Näissä tapauksissa länsimaisessa yliopistossa työskentelevä tutkija on maasta saamansa rahoituksensa lisäksi, ja sen sääntöjen vastaisesti, ottanut vastaan palkkaa tai palkkioita myös kiinalaisilta tahoilta. (Ross 2021)

Yhdysvaltalaisen nanoteknologian professorin Charles M. Lieberin tapaus on tästä hyvä esimerkki. Harvardissa työskennellyt Lieber työskenteli samanaikaisesti Wuhanin teknillisessä yliopistossa, ja hänet oli rekrytoitu Kiinan valtion TTP-ohjelmaan. Tutkinnassa Lieber valehteli ja peitteli Kiina-yhteyksiään. Hänet tuomittiin Yhdysvalloissa vuonna 2020. (Department of Justice, 2020b)

Osassa ilmi tulleista ja rikosseuraamuksiin johtaneista tapauksista kiinalainen tiedustelija on toiminut peiteroolissa tutkijana joko kiinalaisessa tai länsimaisessa yliopistossa. Esimerkiksi edellä esitelty Xun tapaus (Legare, 2022) kuvaa tällaista toimintaa. Xu esiintyi useilla henkilöllisyyksillä useiden kiinalaisten yliopistojen tutkijana. Xun toiminnassa ja sen muutoksissa oli myös yhteys Made in China 2025 -strategiaan. (United States' Sentencing Memorandum, 2022)

Vakoiluepäilyjä on esitetty myös eri maissa toimivien Konfutse-instituuttien työntekijöitä kohtaan. Vuonna 2019 Brysselin vapaan yliopiston yhteydessä toimivan Konfutse-instituutin johtajaa Song Xinningia syytettiin vakoilusta. Häntä syytettiin Belgiassa oleskelevien kiinalaisten opiskelijoiden rekrytoinnista tietolähteiksi ja Kiinan tiedustelun työntekijöiksi. Syytteistä luovuttiin näytön puutteen vuoksi, mutta sekä flaaminkielinen Brysselin vapaa yliopisto että samanniminen ranskankielinen yliopisto lakkauttivat yhteistyösopimuksensa Konfutse-instituuttien kanssa. (Sharma, 2020)

5 Johtopäätökset

Erilaista tiedustelutoimintaa ja tiedonhankintaa harjoittavat Kiinassa useat toimijat läpi yhteiskunnan, joskus yhdessä mutta usein myös erikseen. Eri toimijoiden keskinäiset riippuvuussuhteet eivät ole myöskään aina selvät. Jako valtiollisten ja ei-valtiollisten toimijoiden välillä ei toimi Kiinan yhteydessä samoin kuin länsimaisessa ajattelussa, eikä länsimaista ajattelutapaa voi soveltaa sellaisenaan. Tiedustelutehtävällä ei ole aina selvää alkua tai loppua tai edes tilaajaa, eikä Kiinaan liitetty tiedustelutoiminta ole keskitetysti koordinoitua. Se palvelee kuitenkin laajempia Kiinan valtion yleistavoitteita, jotka ovat teknologian saralla hyvin pitkäjänteisiä. Esimerkiksi Made in China 2025 -strategiassa nostetaan esiin samoja teollisuudenaloja, joita pidettiin strategisina Kiinassa jo 1980-luvulla.

Länsimaiset jäsennystavat eivät sovellu sellaisenaan selittämään kiinalaista mentaliteettia ja rakenteita. Tämä haaste tulee ottaa huomioon myös tätä raporttia luettaessa. Aiheen laajuuden ja siihen vaikuttavien monipuolisten muuttujien määrän vuoksi on varmasti olemassa ulottuvuuksia, joita ei ole käsitelty tässä raportissa.

Kiinalaistahojen tiedonhankinta- ja tiedustelukeinovalikoima on laaja. Samaa tietoa voidaan yrittää kerätä useita erilaisia menetelmiä hyödyntäen. Toiminta voi alkaa esimerkiksi akateemisen yhteistyön tai yrityskauppojen muodossa, mutta jos ne eivät onnistu, tiedon keräys voi jatkua esimerkiksi henkilö- ja kybertiedustelulla. Sama organisaatio voi olla myös usean erilaisen tiedustelutoiminnan kohteena samanaikaisesti.

Kun jostain kiinnostavasta tiedosta on saatu syöte, tieto pyritään saamaan haltuun sopivin keinoin, kunnes tavoite on saavutettu. Julkisuuteen tulleita tapauksia on viime vuosikymmenien ajalta kymmeniä. Tämän raportin yhteydessä ei ole ollut mahdollista arvioida syytä julkisuuteen tulleiden tapausten määrään. Kyse voi olla tiedustelutoiminnan laajuudesta tai sen puutteellisesta operaatioturvallisuudesta. Tiedustelutoiminnan kehittyneisyydessä on merkittäviä eroja.

Kybertoiminnan osalta on merkillepantavaa, että Kiinaan liitettyjä toimijoita liitetään hyvin harvoin sellaiseen toimintaan, jossa pyrittäisiin tuhoamaan kohteen tietoja. Tämä voi viitata joko Kiinan keskittyvän erityisesti kybertiedusteluun suoran vaikuttamisen sijaan, tai vaihtoehtoisesti kyseiset operaatiot ovat pysyneet poissa julkisuudesta. Kybertiedustelussa Kiinaan liitetyt toimijat käyttävät laajasti koko keinovalikoimaa, ja toimintaa on tehokkaasti hajautettu eri toimijoille. Tutkimuksen perusteella ei voida varmasti sanoa, onko tämä kaikilta osin koordinoitua vai orgaanista.

Länsimaisten ajattelumallien ongelmat Kiinan toimintaa selitettäessä koskevat suurelta osin myös tutkimusympäristöjä. Kiinan nousu tieteen uutena suurvaltana haastaa länsimaisen tiedekäsityksen arvopohjaa. Länsimaisissa korkeakouluissa ja tutkimuslaitoksissa ulkomaisen häirinnän vastaisten toimien tulee pohjautua kansainvälisiin periaatelinjauksiin ja peruskirjoihin (European Commission 2022). Vakoilun ja häirinnän ehkäisemiseen kuuluu tutkimuksen vapauden edistäminen, institutionaalinen autonomia (mm. kotimainen rahoituspohja, vrt. Luqiu & McCarthy, 2019) sekä tutkimusetiikan ja tutkimuksen integriteetin korostaminen.

Yksittäiset tapausesimerkit ja kansalliset toimenpidesuositukset Kiinan kanssa tehtävästä tutkimusyhteistyöstä korostavat sitä, että yhteistyöstä on huomattavaa hyötyä Kiinan länsimaisille kumppaneille, mikäli mahdollisia riskejä kyetään riittävässä määrin ennakoimaan ja hallitsemaan. Eurooppalaiset ja kansalliset ohjeistukset TKI-toiminnan kansallisen turvallisuuden riskienhallintaan ovat keskittyneet toistaiseksi erityisesti Kiinaan, mutta myös muiden yhteistyötahojen erityispiirteisiin ja yhteistyön mahdollisiin ristiriitoihin on syytä kiinnittää huomiota.

Tässä raportissa käytetyt lähteet painottuvat vahvasti länsimaihin ja erityisesti Yhdysvaltoihin. Syitä tähän on useita: Yhdysvallat on avoimesti nimennyt Kiinan operaatioiden tekijöiksi, kun taas Euroopassa usein vältetään tekijöiden avointa nimeämistä. Yhdysvallat on myös ollut tiedustelutoiminnan ja tiedonkeräämisen pääkohteena pitkään. Useita tapauksia on myös edennyt Yhdysvalloissa tuomioistuinkäsittelyyn, jolloin niistä on saatavissa helpommin materiaalia. Lisäksi monet kyberturvallisuusraportteja julkaisevista yrityksistä ovat amerikkalaisia. Kielimuuri luo oman haasteensa Kiinaa koskevan lähdemateriaalin hyödyntämiselle. Lähteitä on kuitenkin pyritty hyödyntämään monipuolisesti ja hakemaan useampia toisistaan riippumattomia lähteitä.

Lähteet

Allen G. (2022). Choking Off China's Access to the Future of AI. Center for Strategic & International Studies. 11.10.2022. https://www.csis.org/analysis/choking-chinas-

access-future-ai.

Anderlini, J. (2014). China clamps down on US consulting groups. The Financial Times 25.5.2014. https://www.ft.com/content/310d29ea-e263-11e3-89fd-00144feabdc0.

Brown, A. E. (2009). “Directed or Diffuse? Chinese Human Intelligence Targeting of US Defense Technology”. Edmund A. Walsh School of Foreign Service of Georgetown University. 14.11.2022. https://repository.library.georgetown.edu/bitstream/handle/10822/553457/brownAmy.pdf?sequence=1&isAllowed=y.

Cain, Geoffrey (2022). Totaalinen poliisivaltio: tutkimusmatka Kiinan valvontakoneiston uumeniin. Jyväskylä.

Chen, J., Lu, K., Horejsi, J., Chen, G. (2021). BIOPASS RAT: New Malware Sniffs Victims via Live Streaming. 9.7.2021 https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html.

Cybereason (2022). Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques, 17.3.2023. https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

Department of Justice (2017). United States of America, Plaintiff, v. Zhang Zhang Guj (1), aka "leanov," aka "1eaon," Zha Rong (2), CHai Meng (3), aka "Cobain," Liu Chunliang (4), aka "sxpdlcl," aka "Fangshou" Gao Hong Kun (5), aka "mer4en7y, " Zhuang Xiaowei (6), aka "jpxxav," Ma Zhiqi (7), aka "Le Ma," Li Xiao (B), aka "zhuan86," Gu Gen (9), aka "Sam Gu," Tian Xi (10), Defendants. 15.11.2022. https://www.justice.gov/opa/press-release/file/1106491/download.

Department of Justice (2018a). Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years. 15.11.2022. https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.

Department of Justice (2018b). Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. 20.12.2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Department of Justice (2018c). United States of America, Plaintiff, vs. Yanjun Xu, a/k/a Xu Yanjun, a/k/a Qu Hui, a/k/a Zhang Hui, Defendant. 15.11.2022. https://www.justice.gov/opa/press-release/file/1099876/download.

Department of Justice (2018d). United States of America v. Ji Chaoqun. 15.11.2022. https://www.justice.gov/opa/press-release/file/1096411/download?utm_medium=email&utm_source=govdelivery.

Department of Justice (2018e). United States of America v. United Microelectronics Corporation, et al., Defendant(s). 15.11.2022. https://www.justice.gov/opa/press-release/file/1107251/download.

Department of Justice (2018f). Year in Review for China-Related Cases. 14.11.2022. https://www.justice.gov/archives/opa/page/file/1122681/download.

Department of Justice (2019). United States of America, Plaintiff, v. Zheng Xiaoqing and Zhang Zhaoxi Defendants. 15.11.2022. https://www.justice.gov/opa/press-release/file/1156521/download

Department of Justice (2020a). Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. 16.9.2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

Department of Justice (2020b). Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax. 10.2.2022. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

Department of Justice (2020c). Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases. https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

Department of Justice (2021). Jury Convicts Chinese Intelligence Officer of Espionage Crimes, Attempting to Steal Trade Secrets. 15.11.2022. https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets.

Department of Justice (2022). Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets From Cincinnati Company. 16.11.2022. https://www.justice.gov/opa/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes-attempting.

Dolma, K. (2021). Refugees Are Victims of Chinese Espionage, Not Accomplices. Foreign Policy 5.1.2021. https://foreignpolicy.com/2021/01/05/refugees-chinese-espionage-charges-tibet/

Edwards, L. (2021). Confucius Institutes: China's Trojan Horse. The Heritage Foundation 27.5.2021. https://www.heritage.org/homeland-security/commentary/confucius-institutes-chinas-trojan-horse.

Eftimiades, N. (1994). Chinese Intelligence Operations, Naval Institute Press.

Eftimiades, N. (2020). A Series on Chinese Espionage Vol. I Operations and Tactics. Vitruvian Press.

European Commission (2022). Tackling R&I foreign interference. Staff Working Document. Luxembourg: Publications Office of the European Union. https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1.

Fraser, N., Plan, F., O´Leary, J., Cannon, V., Leong, R., Perez, D. & Shen, C-E. (2019). APT41: A Dual Espionage and Cyber Crime Operation. 7.8.2019. https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation.

Hannas, W. C., Mulvenon, J. & Puglisi, A. B. (2013). Chinese Industrial Espionage:

technology acquisition and military modernisation, (Asian Security Studies), Routledge.

Hannas, W. & Chang, H. (2021). China's STI Operations (Center for Security and Emerging Technology, January 2021). https://doi.org/10.51593/20200049

Izambard, A. & Lamigeon, V. (2020). A400M, M51... Les guerres secrètes du contre-espionnage français. Challenges 10.4.2020. https://www.challenges.fr/entreprise/defense/enquete-sur-les-guerres-secretes-du-contre-espionnage-francais_705487.

Joske, A. (2020). Hunting the Phoenix, The Chinese Communist Party's Global Search for Technology and Talent. Australian Strategic Policy Institute. Policy Brief Report No. 35/2020. 14.11.2022. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Hunting%20the%20phoenix_v2.pdf?TX_kD_pNKlBF_xuSdZO1UMuTK-miNEeAK=.

Legare, R. (2022). Chinese Intelligence Officer Sentenced to 20 Years in Prison in Espionage Case. CBS News 16.11.2022. https://www.cbsnews.com/news/chinese-intelligence-officer-yanjun-xu-sentenced-espionage-stealing-trade-secrets/.

Lo, J. T. & Pan, S. (2014). Confucius Institutes and China's Soft Power: Practices and Paradoxes. Compare, Vol. 46(4), pp. 512-532.

Luce, D. (2021). Advising both Chinese State Companies and the Pentagon, McKinsey & Co. Comes Under Scrutiny. NBC News 13.11.2021 https://www.nbcnews.com/politics/national-security/advising-both-chinese-state-companies-pentagon-mckinsey-co-comes-under-n1283777.

Luqiu, L. R. & McCarthy, J. D. (2019). Confucius Institutes: The Successful Stealth "Soft Power" Penetration of American Universities. The Journal of Higher Education, Vol. 90(4), pp. 620-643.

Lynch, S. N. & Shepardson, D. (2018). U.S. Charges Chinese Intelligence Officers for Jet Engine Data Hack. Reuters 30.10.2018. https://www.reuters.com/article/us-usa-china-hacking-idUSKCN1N42QG.

Microsoft (2022). Microsoft Digital Defense Report 2022. 4.11.2022 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

Mozur, P. (2021). The Failure of China's Microchip Giant Tests Beijing's Tech Ambitions. New York Times 19.7.2021. https://www.nytimes.com/2021/07/19/technology/china-microchips-tsinghua-unigroup.html.

mrkoot (2022). Russian and Chinese services use LinkedIn to target & recruit persons to spy on Dutch companies, says General Intelligence & Security Service (AIVD). 15.11.2022. https://blog.cyberwar.nl/2022/02/russian-and-chinese-services-use-linkedin-to-spy-on-dutch-companies-says-general-intelligence-security-service-aivd/. Käännös: Leupen, J. & van Wijnen, J. F. (2022). Russische en Chinese diensten gebruiken linkedin voor spionage bij nederlandse bedrijven. Het Financieele Dagblad 7.2.2022.

O'connor, S (2019). How Chinese Companies Facilitate Technology Transfer from the

United States. U.S.-China Economic and Security Review Commission. 6.5.2019 https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

Opetus- ja kulttuuriministeriö (2021). Toimintatapasuosituksia akateemiseen yhteistyöhön Kiinan kanssa. Opetus- ja kulttuuriministeriön julkaisuja 2021:51. https://julkaisut.valtioneuvosto.fi/handle/10024/163639.

Puranen, M. (2021). Kiinan EU-pakotteet tähtäävät kriittisen Kiina-tutkimuksen tukahduttamiseen. The Ulkopolitist 11.4.2021. https://ulkopolitist.fi/2021/04/11/kiinan-eu-pakotteet-tahtaavat-kriittisen-kiina-tutkimuksen-tukahduttamiseen/ .

PwC (2017). Operation Cloudhopper - Exposing a Systematic Hacking Operation with an Unprecedented Web of Global Victims. Huhtikuu 2017. https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf.

Reuters (2021). Italy investigating sale of military drones group to Chinese investors - source. Reuters 3.9.2021. https://www.reuters.com/article/italy-china-drones-goldenpowers-idINL8N2Q52GP.

Ross, M. (2021). US-China Higher Education Links in Crisis: Behind the Curtain of Suspicion. Asian Perspective, 45(1), pp. 225-239.

Schaefer, K.J. (2020). Catching up by hiring: The case of Huawei. J Int Bus Stud 51, 1500–1515 (2020). https://doi.org/10.1057/s41267-019-00299-5.

Stoff, J. (2020). Hannas, William C.; Tatlow, Didi Kirsten (eds.), "China's Talent Programs", China’s Quest for Foreign Technology (1 ed.), Abingdon, Oxon: Routledge, pp. 38–54

State Council (2015). Made in China 2025《中国制造 2025》. 14.11.2022. http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf.

Taipei Times (2017). Ex-TSMC engineer stole trade secrets: prosecutors. 15.11.2022. https://www.taipeitimes.com/News/biz/archives/2017/05/03/2003669834.

Taipei Times (2022). UMC fined NT$20m for trade theft. 15.11.2022. https://www.taipeitimes.com/News/biz/archives/2022/01/28/2003772193.

Tylecote, R. & Clark, R. (2021). Inadvertently Arming China? The Chinese Military Complex and its Potential Exploitation of Scientific Research at UK Universities. London: Civitas: Institute for the Study of Civil Society. https://www.civitas.org.uk/content/files/ChinaReport.pdf.

United States Attorney's Office, Northern District of California (2020). Taiwan Company Pleads Guilty To Trade Secret Theft In Criminal Case Involving PRC State-Owned Company. 15.11.2022. https://www.justice.gov/usao-ndca/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned.

United States Attorney’s Office, Northern District of Illinois (2022). Chinese National Convicted of Acting Within the United States as an Unregistered Agent of the People’s Republic of China. 15.11.2022. https://www.justice.gov/usao-

ndil/pr/chinese-national-convicted-acting-within-united-states-unregistered-agent-people-s.

United States District Court for the Southern District of Ohio, Western Division (2022). United States of America v. Xu Yanjun a/k/a Yanjun Xu. https://storage.courtlistener.com/recap/gov.uscourts.ohsd.212371/gov.uscourts.ohsd.212371.209.0.pdf.

United States District Court for the Northern District of New York (2018). United States of America v. Xiaoqing Zheng, d/o/b xx/xx/1963. 15.11.2022. https://storage.courtlistener.com/recap/gov.uscourts.nynd.115346/gov.uscourts.nynd.115346.1.0_1.pdf.

Zhong, R. & Li, C. (2020). With Money, and Waste, China Fights for Chip Independence. New York Times 24.12.2020. https://www.nytimes.com/2020/12/24/technology/china-semiconductors.html.

Van Noorden, R. (2022). Number of Dual US-China Academic Affiliations Falls. Nature, Vol.606 (7913), pp. 235-236.

Wang, Z. & Hu, M. (2018). Fujian facility to lift chip supply. China Daily, 14.7.2018. 15.11.2022. https://www.chinadaily.com.cn/a/201807/14/WS5b49a67ba310796df4df674f.html.

Weinstein, E. (2020). Chinese Talent Program Tracker. Center for Security and Emerging Technology Marraskuu 2020. https://cset.georgetown.edu/publication/chinese-talent-program-tracker/

KIINAN BELT AND ROAD – INITIATIVE (BRI) HYBRIDIVAIKUTTAMISEN VÄLINEENÄ

Esa Alapuranen, Iina Anunti, Marika Kaarnavirta, Heli Laapotti

1 Johdanto

”Kaikkein parasta on vallata vihollisen valtio vahingoittamatta sitä.” – Sunzi

Tämä raportti tarkastelee voiko Kiina hyödyntää vuonna 2013 alkanutta Belt and Road (BRI)-hankettaan hybridivaikuttamisen välineenä. Aihetta lähestytään Euroopan hybridiuhkien torjunnan osaamiskeskuksen hybridivaikuttamisen määritelmän ja käsitteellisen mallin näkökulmasta. Maaliskuussa 2022 BRI-yhteistyösopimuksen oli allekirjoittanut Kiinan kanssa 146 maata ja 32 kansainvälistä järjestöä (Nedopil, 2022).

Raportin laadullinen tiedonhaku toteutettiin ensisijaisesti internetin avoimista suomen-, ruotsin- ja englanninkielisistä lähteistä. Lähteiksi valittiin artikkeleita, julkaisuja, haastatteluja ja podcasteja. Tiedonhaku rajattiin pääosin viimeisen viiden vuoden aikana julkaistuihin lähteisiin, ja lähdekritiikissä huomioitiin sisällön lisäksi myös tiedon julkaisijat. Lähteinä olivat mm. Euroopan Unioni, OECD, Ulkopoliittinen instituutti ja Yleisradio. Kiinalaisista lähteistä käytettiin englanninkielisiä lähteitä ja yliopistolähteitä, joiden osalta tiedostettiin niiden mahdollinen käyttö hybridivaikuttamisen välineenä. Viime vuosina sekä hybridivaikuttamiseen että BRI-hankkeeseen liittyvien tutkimusten ja artikkelien määrä on lisääntynyt.

Raportin luvussa 2 avataan Kiinan historiaa ja nousua Yhdysvaltojen ohella toiseksi 2000-luvun suurvalloista. Luku 3 käsittelee BRI-hankkeen taustaa ja kehittymistä sekä Kiinan mahdollisia tavoitteita hankkeelle. Luvussa 4 avataan hybridivaikuttamista käsitteenä. Luvussa 5 arvioidaan BRI-hankkeen ja hybridivaikuttamisen suhdetta, vertaamalla hybridiuhkien torjunnan osaamiskeskuksen hybridivaikuttamisen määritelmää ja käsitteellistä mallia sekä BRI-hankkeesta julkisesti saatavilla olevia tietoja. Lopuksi esitetään työryhmän pohdinta ja johtopäätökset, sekä annetaan arvio kysymykseen: *”Voiko Kiina hyödyntää BRI-hanketta hybridivaikuttamisen välineenä?”*

2 Kiina valtiona

Kiinan kansantasavalta on maailman väkirikkain valtio, kulttuurisesti monimuotoinen ja monen vielä nykyäänkin käytössä olevan vanhan keksinnön takana. Vielä muutama vuosikymmen sitten Kiina lukeutui maailman köyhimpien maiden joukkoon, mutta on sittemmin noussut yhdeksi tärkeimmistä kauppakumppaneista suurelle osalle maailman maista.

2.1 Maantieteellinen sijainti ja haavoittuvuus

Kiina on Itä-Aasian suurin maa. Kiinan alueesta 69 % koostuu korkeista vuorista ja tasangoista, jotka sijaitsevat pääosin maan länsiosassa (WorldData.info, 2022). Puolet maan

väestöstä ja yli 70 % Kiinan kaupungeista sijaitsevat alueilla, jotka ovat alttiita geologisille, meteorologisille, hydrologisille ja biologisille katastrofeille.

Lähes kaikissa Kiinan maakunnissa on vuosittain erityyppisiä katastrofeja (GFDRR, 2022). Ilmastonmuutoksen vaikutukset näkyvät katastrofien tiheyden ja toistuvuuden kasvuna, eikä tilanteen arvioida muuttuvan tulevina vuosina. Vuosina 1989–2018 katastrofit aiheuttivat lähes 200 000 ihmisen kuoleman ja taloudellisia menetyksiä noin 1700 miljardin dollarin edestä. Vuodesta 2000 lähtien noin 39 miljoonaa hehtaaria on kärsinyt sadon menetyksistä ja katastrofeista.

2.2 Historiasta nykypäivään

Kiinan historiaan kuuluvat niin dynastiat kuin keisaritkin. Kiinasta tuli tasavalta vuoden 1911 vallankumouksen jälkeen. Kiinassa käytiin sisällissota 1920-luvun lopulla. Sodan osapuolet (Kuomintang ja kommunistinen puolue) yhdistivät voimansa toisessa maailmansodassa voittaakseen Japanin, joka oli valloittanut alueita Kiinasta. Toisen maailmansodan jälkeen sisällissota jatkui ja päättyi lopulta kommunistisen puolueen voittoon. Nykyisin Kiinan hallitusmuoto on kansantasavalta ja sitä hallitsee Kiinan kommunistinen puolue. Puolue on ollut vallassa vuodesta 1949 lähtien. (The World Factbook, 2022.)

Kiinan avauduttua ulkomaankaupalle vuonna 1978, maa on keskittynyt markkinasuuntautuneeseen talouskehitykseen. Muutoksen jälkeen Kiina on ollut yksi maailman nopeimmin kasvavista talouksista. Sen todellinen bruttokansantuote on kasvanut keskimäärin yli 9 % vuosittain aina vuoteen 2021 asti. Tämä on nostanut arviolta 800 miljoonaa kiinalaista köyhyydestä ja parantanut yleistä elintasoa. (The World Factbook, 2022.)

Kiinasta tuli maailman suurin vientimaa vuonna 2010 ja suurin kauppamaa vuonna 2013. Viime vuosina Kiina on lisännyt tukea sellaisille valtion omistamille yrityksille ja aloille, joita pidetään tärkeinä "taloudellisen turvallisuuden" kannalta. Tällaisia ovat erityisesti maailmanlaajuisesti kilpailukykyiset teollisuudenalat. (The World Factbook, 2022.) Kiina on noussut Yhdysvaltojen ohella toiseksi 2000-luvun suurvalloista niin taloudellisen, poliittisen kuin sotilaallisen suorituskykynsä osalta. (Ulkoministeriö, 2021).

2.3 Kiinan kommunistisen puolueen politiikka ja propaganda

Kiina on pyrkinyt pysymään syrjässä maailman kriiseistä, keskittyen turvaamaan taloudellisen kasvunsa. Nykyisen johtajansa, Xi Jinpingin johdolla Kiina on ilmoittanut tavoittelevansa sille kuuluvaa suurvalta-asemaa. Nykyään Kiina toteuttaakin suurvaltapolitiikkaa. Tämä näkyy esimerkiksi Kiinan Belt and Road Initiative (BRI) -hankkeena, jota pidetään Kiinan ulkopolitiikan lippulaivana. Kommunistisen puolueen peruskirjaan kirjatut silkkitiehankkeet lisäävät niiden merkitystä, ja onnistuessaan kasvattavat puolueen mainetta. (Kallio, 2022). Kiinan suurvaltapolitiikka näkyy myös Kiinan osallistumisena erilaisiin rauhanturvaamisoperaatioihin. Maa on myös entistä aktiivisempi kansainvälisissä järjestöissä. Kiinan kommunistinen puolue korostaa propagandassaan omaa rooliaan Kiinan vapauttamisessa pitkäaikaisesta ulkovaltojen nöyryytyksen ajasta, sekä Kiinan nostamisessa uuteen kansalliseen kukoistukseen (Manninen, 2019).

Purasen (2021) mukaan Kiinan kommunistinen puolue on äärimmäisen herkkä itseensä kohdistuvalle kritiikille. Puolue haluaa esittää kotimaisessa propagandassaan kuvan maasta, joka on puolueen kanssa samaa mieltä, ja joka tukee puolueen tavoitteita. Sensuuri ja turvallisuuskoneisto kitkevät pois kriittiset äänet. Kiinan rajojen ulkopuolelta

kantautuva kritiikki nähdään uhkana puolueen kertomalle tarinalle ja siten myös puolueen valta-asemalle.

Mannisen (2021) mukaan Kiinan politiikasta ja yhteiskunnasta on keskeistä ymmärtää kommunistisen puolueen asema. Puolueen tärkein tavoite on pitää itsensä vallassa. Kaikki muu on sille alisteista, ja puolueen etu menee kaiken muun ohi. Mikäli Kiinan kansallista ylpeyttä, etua ja puolueen ajamia asioita loukataan, siitä kostetaan silläkin uhalla, että kostosta koituu Kiinalle taloudellista haittaa. Esimerkkinä tästä Manninen (2021) mainitsee Kiinan kauppasotamaiset toimet Australiaa vastaan. Australialaisille viineille määrättiin jopa yli 200 %:n rangaistustullit maan arvosteltua Kiinaa ihmisoikeuksista ja vaadittua Kiinalta kunnollisia tutkimuksia koronaviruksen alkuperästä. Kiina perusteli korotuksia tutkimuksellaan Australian mahdollisesti harjoittamasta polkumyynnistä. (Manninen, 2021.) Lisäksi kiinalaiset viranomaiset ovat arvostelleet negatiivisesti australialaisia tuotteita, minkä vuoksi kiinalaiset kuluttajat eivät uskalla ostaa niitä. Toisena esimerkkinä Manninen (2021) nostaa esiin vuoden 2020 tapahtumat, jolloin Five Eyes-tiedusteluyhteisö arvosteli Kiinan toimia Hongkongissa. Tällöin Kiina uhkasi puhkoa ”viisi silmää” sokeiksi. (Manninen 2021.)

3 Belt and Road Initiative (BRI-Hanke)

Kiinan presidentti Xi Jinping esitteli massiivisen Belt and Road Initiative (BRI) -kehitysohjelman syyskuussa 2013. Kyseessä ei ole mikään uusi hanke, vaan pohjimmiltaan se perustuu aikaisempiin, 1990-luvun alun kehittämishankkeisiin. (Garcia & Guerreiro, 2022.) Kiinan BRI-hankkeessa on kyse massiivisesta infrastruktuuriprojektista, jossa Kiinan toimesta, Kiinan aloitteesta ja usein Kiinan rahoittamana rakennetaan muun muassa maantieverkostoa, rautateitä, satamia, lentokenttiä, voimalinjoja ja tietoliikenneverkkoja. BRI-hanke on alun perin fokusoitunut Euraasiaan, mutta se on myöhemmin laajentunut muihinkin maanosiin (Kohli & Zucker, 2020). Toukokuussa 2019 BRI -hankkeeseen kuului yhteensä 133 maata. Infrastruktuuriyhteyksien lisäksi hanke tukee myös maatalouden ja teollisuuden kehitystä, kauppaa ja investointeja, rahavirtoja ja henkilöitä (Kohli & Zucker, 2020). Infrastruktuurihankkeisiin investoimalla Kiina parantaa yhteyksiä ja helpottaa kaupankäyntiä eri maakuntien, maiden, alueiden ja maanosien välillä.

Kiinan kauppaministeriö (MOFCOM) julkaisi kesäkuussa 2022 tietoja ensimmäisen kuuden kuukauden ajalta Kiinan investoinneista ja yhteistyöstä Belt and Roadin varrella olevissa maissa. Tietojen mukaan kiinalaiset yritykset investoivat näihin maihin noin 89,9 miljardia dollaria, saavuttaen noin 10,2 % kasvun edellisvuoteen verrattuna. Lisäksi vuonna 2022 aloitettiin lähes 1900 uutta projektia, joiden kokonaisarvo on yli 38 miljoonaa dollaria. Kiinan kauppaministeriön tiedot ovat kerätty 55 eri maasta. (Nedopil, 2022.)

3.1 BRI-hankkeen ulottuvuudet

Kiinan Belt and Road -aloitetta (BRI) on kuvattu historian suurimmaksi infrastruktuurihankkeeksi, joka koskee noin 60 prosenttia maailman väestöstä (United Nations Development Programme China, 2017). BRI-hanke koostuu niin kutsutuista talouskäytävistä ja logistisesta verkostosta, jotka sijoittuvat alueille, joille joko on jo rakennettu tai on määrä rakentaa logistista infrastruktuuria. BRI-hankkeesta on julkaistu erilaisia karttoja erilaisista suunnitelmista ja näkökulmista. Paltemaa (2019) on nostanut esiin viisi merkittävää talouskäytävää:

1) ”Uusi Euraasian maasilta”: Junayhteys Länsi-Kiinasta Saksaan.
2) Kiina – Mongolia – Venäjä: Kiina pyrkii sitomaan Mongolian ja Venäjän lähemmäs itseään mm. kaasuputkiston ja muun infrastruktuurin, kuten rautateiden muodossa.
3) Kiina – Keski-Aasia – Lähi-itä: Kiina suunnittelee yhdistävänsä itsensä Euroopan Lähi-idän kautta.
4) Merellinen silkkitie: Kiina rakentaa satamia ja muuta infrastruktuuria Kaakkois-Aasiasta Afrikkaan ja aina Välimerelle saakka.
5) ”Jääsilkkitie”: Arktisen alueen läpi kehitettävät energiahankkeet Venäjän kanssa. Pohjoisnapajäätikön sulaessa avautuu uusi väylä, jonka Kiina liittää osaksi hankettaan.

Edellä mainittujen viiden käytävän lisäksi Kiinan BRI-hankkeeseen kuuluu myös avaruuskäytävä. Osana tätä käytävää on rakennettu muun muassa Beidou-navigointijärjestelmä, satelliittiviestintäjärjestelmä ja satelliittisensorijärjestelmiä (Hui, 2018). BRI-hanke kattaa myös kyberulottuvuuden (Xinhua, 2017).

3.2 Motiivit

3.2.1 Historialliset motiivit

Silkkitie yhdisti vuosituhansien ajan Kiinan, Lähi-idän ja Euroopan. Se oli linkki idän ja lännen välillä, kauppareittien verkosto. Silkkitien kautta kuljetettiin nimensä mukaisesti silkkiä, mutta myös muita kauppatavaroita, kuten mausteita, kultaa, hopeaa ja jalokiviä – unohtamatta myöskään aatteita ja suuria uskontoja.

Silkkitien kukoistuskausi oli Tang-dynastian aikana 700-luvulla. Silkkitie kuihtui lopulta pois 1400-luvulla. Nyt syntymässä oleva silkkitie sitoo lännen jälleen Kiinaan.

3.2.2 Geotaloudelliset motiivit

Kiinalla on vakaa pyrkimys nousta maailmantalouden kärkeen. Vuodesta 2013 alkaen Kiina on investoinut tavoitteensa saavuttamiseksi miljardeja. Kiinan julkituomista motiiveista käy ilmi, että Kiina pyrkii luomaan hankkeillaan Kiina-johtoisen talousalueen Euraasiaan, integroiden kaikki kansalliset alueet itseensä infrastruktuurin kautta. Tällöin Kiinasta tulisi Euraasian alueen talousmahti ja -keskus. (Kohli & Zucker, 2020.)

Kiinan talouskasvu on hidastunut vuosituhannen alun n. 10 % vuosittaisesta kasvusta. Tämä on haaste Kiinan kommunistiselle puolueelle, jonka legitimiteetti nojaa vahvasti jatkuvaan talouskasvuun. Kiinan talouden kasvua on ruokittu Kiinan sisäisillä velkaavusteisilla infrastruktuuri-investoinneilla. Näillä investoinneilla on kasvatettu vientiteollisuutta, jonka voitoilla velat on maksettu pois. Tämä oravanpyörä on kuitenkin johtanut tilanteeseen, jossa vientiteollisuus on kasvanut liian suureksi, eikä tuotteille enää löydy markkinoita kotimaassa tai ulkomailla. Pääoman tuotto jää pääomakustannuksia alhaisemmiksi. (Jones & Hameiri, 2020.) Vientiylijäämä sekä suuret kotimaiset ja ulkomaiset talletukset ovat aiheuttaneet rahoituslaitoksille vaikeuksia löytää pääomalle tuottavia sijoituskohteita. Silkkitien avulla Kiina pyrkii kasvattamaan kiinalaisten tuotteiden, palveluiden ja pääoman kysyntää (Jones & Hameiri, 2020). BRI-hanke mahdollistaa Kiinan ylijäämätuotannon viennin ulkomaille.

Kehittyneen infrastruktuurin myötä Kiina pääsee aikaisempaa paremmin markkinoille alhaisilla kuljetuskustannuksilla. Lisäksi Kiina saa itse paremmin raaka-aineita

käyttöönsä. Tämä on omiaan lisäämään Kiinan kilpailukykyä ja taloudellista vaikutusvaltaa. (Paltemaa, 2019.) Kiina on riippuvainen ulkomailta tuodusta energiasta, koneista, laitteista ja kemikaaleista. Tärkeimmät tuonnin lähteet ovat Japanissa, Taiwanissa, Etelä-Koreassa, Australiassa, EU:n eri maissa ja Yhdysvalloissa (OECD, 2018).

Kiina on tehnyt monivuotisen suunnitelman BRI:n talouskäytävien infrastruktuurin rakentamiseen. Maa on esittänyt BRI-hankkeen infrastruktuurin rakentamisen noudattelevan kestävän kehityksen ja vihreän talouden ajatusmallia. Vuosina 2000–2017 Kiina investoi noin 843 miljardia dollaria 165 maahan ja yli 13 000 projektiin, joista monet liittyivät BRI:hen (Vidal, 2022). Niihin kuuluvat suurnopeusradat, hiili- ja vesivoimalaitokset, satamat, tiet, sillat ja matkailun kehitys. Kiinassa on vuosittain useita luonnonkatastrofeja, jotka hidastavat BRI:tä, mutta joiden vaikutus Kiinan talouteen on rajallinen. Eniten luonnonkatastrofien vaikutukset näkyvät haavoittuviksi arvioitujen alueiden teollisuudessa ja maataloudessa.

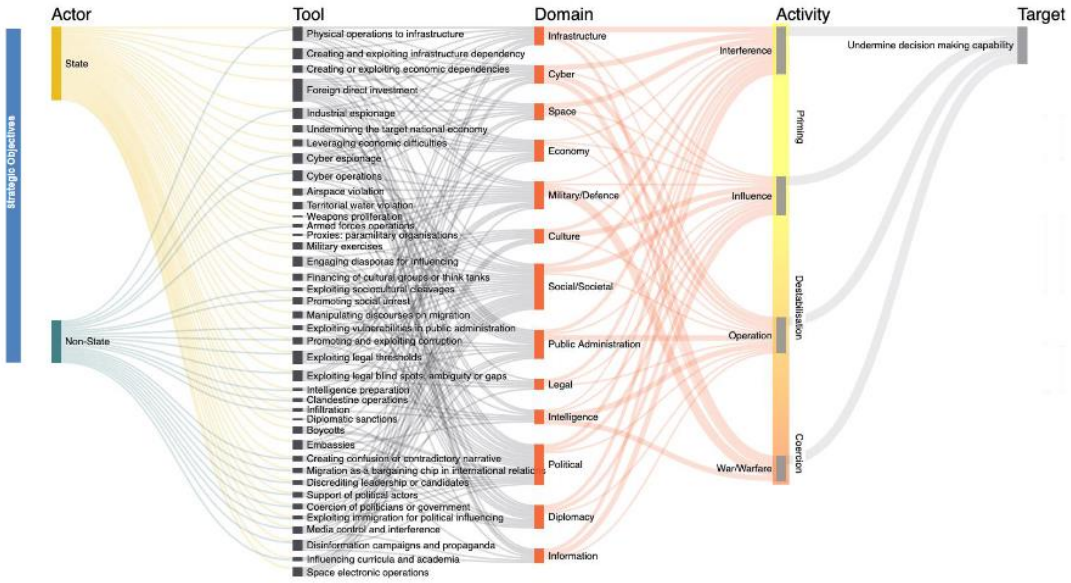
3.2.3 Geopoliittiset motiivit

Kiinan pyrkimyksenä on lisätä vaikutusvaltaansa ja saada johtava rooli maailmassa hyödyntämällä taloutta aikaisempaa voimakkaammin osana diplomaattisuhteita. Kiina itse määrittelee, että kyse on parempien yhteyksien rakentamisesta Kiinan ja hankkeeseen osallistuvien maiden välille, sekä Kiinan talouden integroimisesta lähemmäksi hankkeeseen osallistuvia maita. (Kohli & Zucker, 2020.)

Geopolitiikan tutkijat ovat huomauttaneet BRI-hankkeella olevan huomattava geopoliittinen merkitys. Rakennettavan infrastruktuurin ansiosta Kiina ei ole enää kaukana, vaan se lähentää itseään ja sitoo Euraasiaa tiukemmin oman johtajuuteensa. (Paltemaa, 2019.)

4 Hybridivaikuttaminen

Hybridivaikuttaminen määritellään eri lähteissä eri tavalla. Tässä raportissa hybridivaikuttamista lähestytään Euroopan hybridiuhkien torjunnan osaamiskeskuksen määritelmän ja käsitteellisen mallin näkökulmasta. Hybridivaikuttaminen on synkronoitua ja koordinoitua toimintaa, joka tarkoituksellisesti suuntautuu demokraattisten valtioiden ja instituutioiden systeemisiä haavoittuvuuksia vastaan. Käytössä on laaja keinovalikoima. Toiminnassa hyödynnetään havaittavuuden ja syyksiluettavuuden sekä sodan ja rauhan välistä kynnystä. Tavoitteena on vaikuttaa päätöksentekoon paikallisella, alueellisella, valtiollisella tai institutionaalisella tasolla tekijän etujen mukaisesti ja kohteen etujen vastaisesti. Hybridivaikuttamisen käsitteellisessä mallissa hybridiuhkien torjunnan osaamiskeskus avaa hybridivaikuttamisen eri osa-alueita kuten tekijöitä, kohdealueita, menetelmiä ja vaiheita sekä näiden välisiä suhteita. (KUVIO 1, The European Centre of Excellence for Countering Hybrid Threats, 2021

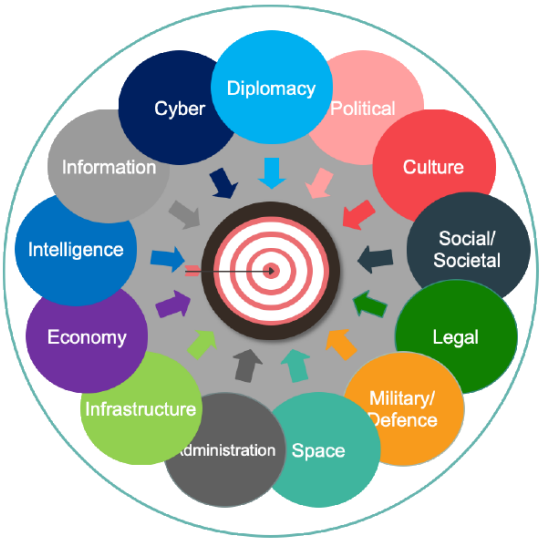


KUVIO 1 The landscape of Hybrid Threats: A conceptual model (The European Centre of Excellence for Countering Hybrid Threats, 2021)

4.1 Hybridivaikuttamisen toimijat, tavoitteet ja menetelmät

Hybridivaikuttamista tekee ja siihen osallistuu laaja kirjo toimijoita, jotka voivat olla valtiollisia tai ei-valtiollisia. Vaikuttamisen tavoitteet voivat olla muitakin kuin sotilaallisia. Hybridivaikuttamiselle on myös tyypillistä, että ei-valtiollinen toimija toimii valtiollisen toimijan sijasta tai puolesta. Hybridivaikuttamisen tavoitteena on hyödyntää kohteen haavoittuvuuksia ja pyrkiä toimimaan mahdollisimman peitellysti. (The European Centre of Excellence for Countering Hybrid Threats, 2021.)

Hybridivaikuttamisen kohteena ovat valtioiden ja instituutioiden systeemiset haavoittuvuudet. Hybridivaikuttamiselle on tyypillistä useiden eri keinojen joko yhtäaikainen tai peräkkäinen käyttäminen ja toiminnan kohdistuminen usealle eri osa-alueelle. Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia. Apuna voidaan käyttää myös teknologiaa ja sosiaalista mediaa. Hybridivaikuttamisen tunnistaminen on vaikeaa. (KUVIO 2, The European Centre of Excellence for Countering Hybrid Threats, 2021.)



KUVIO 2 Hybridivaikuttamisen osa-alueita (EU-Hybnet_network, 2022)

4.2 Hybridivaikuttamisen vaiheet ja niihin liittyvä toiminta

Hybridiuhkien torjunnan osaamiskeskus jakaa hybridivaikuttamisen kolmeen vaiheeseen: valmistelu, horjuttaminen ja pakottaminen. Nämä vaiheet eivät kuitenkaan välttämättä seuraa toisiaan ajallisesti vaan vaiheiden välillä voidaan palata takaisin. Vaiheet voivat seurata toisiaan horisontaalisesti tai vertikaalisesti. Vaiheisiin liittyvä toiminta voi olla esimerkiksi häirintää, vaikuttamista, operointia/kampanjointia, ja sodan uhkaa ja neuvottelua. (The European Centre of Excellence for Countering Hybrid Threats, 2021.) Hybridivaikuttaminen on siis kokonaisuus, joka voi saada erilaisia muotoja ja vaikuttamisen tapoja riippuen esimerkiksi siitä, millaisia vaikutuksia aikaisemmalla toiminnalla on ollut kohteeseen. Taulukossa 1 on esitetty esimerkkejä hybridivaikuttamisesta.

Infrastruktuuriin kohdistuvat fyysiset operaatiot	Maahanmuuttokeskustelun polarisointi
Infrastruktuuririippuvuuksien luominen ja hyväksikäyttö	Korruption hyödyntäminen ja edistäminen
Taloudellisten riippuvuuksien luominen ja hyväksikäyttö	Laissa olevien aukkojen, epäselvyyksien ja kynnysten hyödyntäminen
Suorat ulkomaiset investoinnit	Oikeuskäytännön, prosessien, instituutioiden ja periaatteiden hyödyntäminen
Teollisuusvakoilu	Tiedustelutiedon valmistelu
Vastustajan talouden heikentäminen	Peiteoperaatiot
Kybervakoilu	Soluttautuminen
Kyberoperaatiot	Diplomaattiset sanktiot
Ilmatilaloukkaukset	Boikotit
Merialueloukkaukset	Lähetystöt
Aseiden levittäminen	Hämmennyksen tai ristiriitaisen narratiivin luominen
Asevoimien tavalliset/epätavalliset operaatiot	Maahanmuuton hyödyntäminen neuvotteluvalttina
Puolisotilaalliset organisaatiot (proxyt)	Johdon tai kandidaattien mustamaalaus
Sotaharjoitukset	Poliittisten toimijoiden tukeminen

Hajaannuksen tarkoituksellinen aiheuttaminen	Poliitikkojen tai hallinnon kiristys
Kulttuuriryhmien ja ajatuspajojen rahoitus	Median hallinta ja häirintä
Sosiokulttuuristen ristiriitojen hyödyntäminen (etniset, uskonnolliset, kulttuuriset)	Disinformaatiokampanjat ja propaganda
Sosiaalisen rauhattomuuden edistäminen	Opintosuunnitelmiin ja tieteeseen vaikuttaminen
Julkishallinnon haavoittuvuuksien hyödyntäminen (ml. pelastuspalvelut)	Elektroniset operaatiot

TAULUKKO 1 Esimerkkejä hybridivaikuttamiseen liittyvästä toiminnasta (The European Centre of Excellence for Countering Hybrid Threats, 2021).

5 BRI-hanke ja hybridivaikuttaminen

BRI-hankkeen ja hybridivaikuttamisen suhdetta voidaan arvioida vertaamalla hybridiuhkien torjunnan osaamiskeskuksen hybridivaikuttamisen määritelmää ja käsitteellistä mallia sekä BRI-hankkeesta julkisesti saatavilla olevia tietoja keskenään. Hybridivaikuttamisen tavoitteena on vaikuttaa kohteen päätöksentekoon paikallisella, alueellisella, valtiollisella tai institutionaalisella tasolla, tekijän etujen mukaisesti ja kohteen etujen vastaisesti. Hybridivaikuttamisen toiminta on synkronoitua ja koordinoitua ja siinä hyödynnetään tarkoituksellisesti kohteen systeemisiä haavoittuvuuksia laajaa keinovalikoimaa hyödyntäen.

BRI-hanke on Kiinan kommunistisen puolueen käynnistämää ja ohjaamaa strategista toimintaa. Tältä osin se täyttää hybridivaikuttamisen määritelmän. BRI-hanke pyrkii avoimesti vaikuttamaan kohteen päätöksentekoon, jotta BRI-hankkeen tavoitteet, kuten talouskäytävien avaaminen infrastruktuurihankkeiden ja investointien kautta saadaan toteutetuksi. Näiden hankkeiden ja investointien toteutumisella on jo sinällään itseisarvo Kiinan geotaloudellisten ja geopoliittisten tavoitteiden saavuttamiseksi. Päätöksentekoon vaikuttamisen ja Kiinan etujen ajamisen osalta BRI-hanke siis vastaa hybridivaikuttamisen määritelmän mukaista toimintaa.

Hybridivaikuttamisen määritelmän mukaan vaikuttamisessa toimitaan kohteen etujen vastaisesti ja kohteen systeemisiä haavoittuvuuksia hyödyntäen. Näiltä osin Kiina ei luonnollisestikaan ole avoimesti avannut toimintatapojaan tai -suunnitelmiaan. Näitä näkökulmia arvioidaan alla tarkemmin hybridivaikuttamisen käsitteellisen mallin eri osa-alueiden kautta.

5.1 BRI-hanke ja hybridivaikuttamisen keskeiset komponentit

5.1.1 Toimijat ja niiden strategiset tavoitteet

BRI-hankkeen toimijana on Kiinan valtio eli käytännössä Kiinan kommunistinen puolue. Hybridivaikuttamisen toimijoiksi voidaan katsoa myös kolmannet osapuolet, jotka toimivat varsinaisen toimijan eduksi. BRI-hankkeessa tällaisina osapuolina ovat kiinalaiset rahoituslaitokset, sekä valtio-omisteiset tai -sidonnaiset yritykset. Suoraan tai välillisesti Kiinan valtion omistuksessa tai ohjauksessa olevat yritykset voivat myös hankkia jalansijaa kohdemaasta tai toimialasta esimerkiksi yritysostojen avulla. Ulkopoliittisen instituutin tutkimusprosessori Mikael Mattlinin mukaan yritysostot voivat kohdistua esimerkiksi

yrityksiin, joilla on edistynyttä teknologiaa tai osaamista, jotka omistavat kriittistä infrastruktuuria tai joilla on pääsy arkaluontoiseen tietoon (Mattlin, 2022).

Hybridivaikuttamisen strateginen tavoite muodostuu Kiinan avoimesti kertomista BRI-hankkeen tavoitteista. Taustalla voi olla myös sellaisia tavoitteita, joita Kiina ei ole julkistanut. Kiinalle on tyypillistä hyödyntää epäsuoria strategioita ja epäsuoraa toimintaa. Avoin kanssakäyminen avaa mahdollisuuksia salaisille toimille. Salaiset toimet muokkaavat voimatasapainoa ja mahdollistavat uusia avoimia kanssakäymisen muotoja, mahdollistaen jälleen uusia salaisia toimia. (The European Centre of Excellence for Countering Hybrid Threats, 2021)

Kiinan kansan vapautusarmeija (engl. People's Liberation Army, PLA) jakaa länsimaisia hybridivaikuttamisen keinoja vastaavat Kiinan sodankäynnin operaatiot kolmeen luokkaan. **Psykologinen sodankäynti** kuvaa Kiinan strategisen teorian mukaan operaatioita, jotka saavuttavat poliittiset ja sotilaalliset tavoitteet vaikuttamalla kohteen psyykeeseen ja käyttäytymiseen informaatiota jakamalla. Kohteina ovat esimerkiksi päätöksentekijät. Keinoja voivat olla esimerkiksi pakottaminen, lahjonta, houkuttelu tai pelottelu. **Julkisen mielipiteen sodankäynti** kuvaa operaatioita, joissa vaikutetaan kotimaiseen tai ulkomaiseen tukeen jakamalla informaatiota eri medioissa ja foorumeissa. Tiedolla pyritään muokkaamaan vastaanottajan arvoja Kiinan arvojen, kuten tiukan sosiaalisen kontrollin, mukaiseksi. **Oikeudellinen sodankäynti** nähdään keinona saavuttaa oikeudellisesti vahvempi asema, jota voidaan hyödyntää poliittisesti tai sotilaallisesti. Lakia ja oikeutta ei nähdä rationaalisena päätöksentekomekanismina, vaan sen avulla pyritään saavuttamaan vahvempi asema. Tämän aseman avulla voidaan vaikuttaa kohteisiin ja heidän toimintaansa oikeudellisin keinoin. (The European Centre of Excellence for Countering Hybrid Threats, 2021)

5.1.2 Kohdealueet, menetelmät ja työkalut

Infrastruktuuri lienee näkyvin BRI-hankkeen alue, sillä infrastruktuurin kehittäminen on BRI-hankkeen ytimessä ja myös osa Kiinan virallista BRI-hankkeen kuvausta. Suurilla ulkomaille kohdistuvilla infrastruktuuri-investoinneilla Kiina kykenee avaamaan väyliä muille hybridivaikuttamisen keinoille kuten jäljempänä kuvataan. Kehittämällä ja hankkimalla kriittistä infrastruktuuria, kuten tavaraliikennesatamia ja muita logistiikan hubeja, Kiina toisaalta varmistaa oman logistiikkansa toimivuuden normaali- ja kriisiolosuhteissa, mutta toisaalta voi myös halutessaan vaikeuttaa tai estää muiden toimijoiden logistiikkaa. Suurin osa maailman maista on jo tällä hetkellä riippuvaisia Kiinan vientiteollisuudesta, kuten elektroniikasta, lääkkeistä ja kuluttajatavaroista. Infrastruktuuri-investoinneilla Kiina lisää logistista riippuvuutta. Se voi halutessaan hyödyntää näitä riippuvuuksia muiden hybridivaikuttamisen keinojen ohella.

Kyberulottuvuus on toinen ilmeinen hybridivaikuttamisen alue BRI-hankkeessa. Kiinalaisilla teknologiayrityksillä, kuten Huaweilla ja ZTE:llä, on vahva jalansija globaaleilla markkinoilla. BRI-hankkeessa Kiina on yritysostojen kautta hankkinut teknologista huippuosaamista. Kiinalaisten yritysten on arvioitu asentavan kuituverkkoja 76 maahan ja rakentavan smart city -infrastruktuuria valvontajärjestelmineen 56 maahan (Prasso, 2019, viitattu The National Bureau of Asian Research, 2019). Huawei on rakentanut 5G-verkkoja 12 maahan ja toimii yhteistyössä teleoperaattoreiden kanssa yli 100 maassa. Yli 700 kaupunkia ja yli puolet Fortune 500-yrityksistä käyttää Huawein tuotteita tai palveluita. (Huawei, 2022.)

Omistamiensa, rahoittamiensa ja/tai hallinnoimiensa kuituverkkojen ja langattomien tiedonsiirtoväylien sekä kiinalaisten yritysten valmistamien tuotteiden kautta Kiinalla on ainakin teoriassa pääsy valtaviin tietomassoihin ja toisaalta mahdollisuus myös tiedonsiirron manipulointiin tai estämiseen – kyky erityyppisiin elektronisiin operaatioihin ja informaatiovaikuttamiseen.

BRI:n kautta Kiina voi hyödyntää laajentamiaan **navigointi-, satelliittiviestintä- ja satelliittisensorijärjestelmiä ja -kyvykkyyksiä** myös hybridivaikuttamisen tarkoituksiin. Ilmeisimpänä keinona on tiedustelutiedon kerääminen järjestelmien avulla. Esimerkkinä tästä voidaan mainita Argentiinassa toimiva PLA:n operoima Kiinan avaruuskeskus, jonka valvontaan Argentiinan valtiolla on vain rajalliset mahdollisuudet. Keskusta voidaan ainakin teoriassa käyttää signaalitiedusteluun julkisesti kerrotun tehtävänsä lisäksi. (Garrison, 2019.) Samoin Ruotsin Kiirunassa toimivan Kiinan satelliittiohjauskeskuksen hallinnoimia satelliitteja voidaan hyödyntää myös tiedustelutarkoituksiin ja sotilaallisiin tarkoituksiin (Ruotsin kokonaismaanpuolustuksen tutkimuslaitos, 2019).

Kiina on myös ilmoittanut hyödyntävänsä avaruusjärjestelmiä terrorismin vastaisiin toimiin ja rauhanturvaamiseen (Hui, 2018). Kiinan lainsäädännön määritelmä terrorismista on laaja ja tulkinnanvarainen. Se kattaa esimerkiksi yhteiskuntarauhan häirinnän ja muun vakavan sosiaalisen haitanteon. (United Nations Human Rights Office of the High Commissioner, 2022.) Kiina voi näin ollen käyttää hybridivaikuttamisen keinoja, kuten peiteoperaatioita ja tiedustelua, omasta näkökulmastaan terrorismin vastaisiin toimiin.

Taloudellisten riippuvuuksien luominen tapahtuu luonnollisena osana BRI-hankkeen rahoitusjärjestelyitä, joissa Kiina luotottaa muiden maiden infrastruktuurihankkeita. Kiinaa kohtaan on esitetty syytöksiä näiden riippuvuuksien hyväksikäytöstä ns. velka-ansan muodossa. Toisaalta on esitetty myös näkemyksiä, joiden mukaan Kiinaa kritisoidaan suotta velka-ansan käyttämisestä. Velka-ansasta käytetään usein esimerkkinä Sri Lankan Hambantotan satamaa ja Malesiassa tapahtuneita investointihankkeita, kuten kaasuputki-investointeja. Kummassakin tapauksessa investointiyhteistyö on kuitenkin alun perin käynnistynyt kohdemaan aloitteesta ja aloitteiden taustalla voidaan nähdä olleen Sri Lankan ja Malesian sisäpoliittiset ja taloudelliset intressit. Molemmissa tapauksissa valtiot hakivat rahoitusta avoimesti myös muilta tahoilta, mutta ainoastaan Kiina oli valmis järjestämään rahoituksen. (Jones & Hameiri, 2020.)

Hambantotan syvävesisatama ei ensimmäisen vaiheen valmistuttua kyennyt voitolliseen toimintaan. Tästä huolimatta Sri Lankan hallinto haki ja sai Kiinalta lisärahoituksen sataman laajennukseen. Sri Lankan valtio velkaantui voimakkaasti 2010-luvulla, lainakulut kriisiyttivät maan talouden ja estivät lainamaksut myös Hambantotan sataman osalta. (Jones & Hameiri 2020.) Seurannutta lainan uudelleenjärjestelyä käytetään usein esimerkkinä Kiinan velka-ansan laukeamisesta, jossa Kiinan väitetään saaneen omistukseensa Hambantotan sataman vastineeksi lainan anteeksiannosta. Todellisuudessa Kiina vuokrasi sataman Sri Lankalta 99 vuodeksi. Vuokrauksesta saadulla vastikkeella Sri Lanka kykeni lyhentämään länsimaille kohdistuvaa valtionvelkaansa, joka oli suurempi kuin Kiinalta saatu velka. Sri Lanka oli aloitteellinen sataman vuokrauksessa. Kiina ei käytä satamaa laivastotukikohtana vaan satamassa on sijoitettuna Sri Lankan laivaston henkilöstöä. (Jones & Hameiri 2020.) Kiina on tosin tehnyt laivastovierailuja satamaan (Ni, 2022).

Malesiaa vuosina 1957–2018 hallinnut UMNO-puolue sopi Kiinan kanssa lukuisista suurista infrastruktuuriprojekteista. Vuonna 2018 PH-liitto astui valtaan Malesiassa ja

syytti Kiinaa köyhempien maiden hyväksikäytöstä ja velka-ansan käytöstä Malesiassa. Tämä julkinen ulostulo on synnyttänyt mielikuvan, että Kiina omasta aloitteestaan olisi rahoittanut kriittisiä infrastruktuurihankkeita saadakseen niiden omistajuuden. Todellisuudessa Malesia on ollut aloitteellinen hakiessaan rahoitusta hankkeille. Lisäksi IMF (IMF, 2018, teoksessa Jones & Hameiri, 2020) arvioi Malesian julkisen velan hallittavaksi ja trendiltään pieneneväksi, joten velka-ansan laukeaminen on epätodennäköistä. Kiinan rahoituksen todellinen ongelma liittyi Malesian sisäpoliittisiin ongelmiin ja korruptioon. Suurimmaksi ongelmaksi nousi kahden öljyputken rakentamiseen liittyvä rahoitus, josta suuri osa päätyi 1MDB-rahaston väärinkäytöksen kautta UMNO-puoleen poliittiseen toimintaan. (Jones & Hameiri 2020.)

Sri Lankan ja Malesian esimerkkien perusteella voitaneen todeta, että Kiinan syyllistäminen velka-ansan virittämisestä ja käytöstä on todennäköisesti näiden tapausten osalta virheellistä ja ainakin kovin yksipuolista. Hankkeet ovat olleet ongelmallisia sekä huonosti johdettuja, ja niiden taustalla on ollut kohdemaan korruptio. Toki Kiina pyrkii hyötymään hankkeista kaikin mahdollisin keinoin, myös hybridivaikuttamisen näkökulmasta. Tässä suhteessa velka-ansan käyttö ei ole poissuljettua tulevaisuudessa.

Kiina pyrkii turvaamaan kiinalaisten yritysten ja infrastruktuurin toiminnan myös Kiinan rajojen ulkopuolella. Kiinan talouden kannalta maa- ja merireittien turvallisuus on kriittinen. Reittien ja toiminnan turvaaminen kuuluu PLA:n tehtäviin. Kiinassa on kuitenkin perustettu myös puolisotilaallisia turvallisuusyrityksiä, joilla on läheisiä yhteyksiä PLA:han. Näitä puolisotilaallisia turvallisuusyrityksiä toimii erityisesti Afrikassa. Puolisotilaallisia turvallisuusyrityksiä käyttämällä Kiina välttää PLA:n joukkojen käyttämisen erityisesti Kaakkois-Aasian maissa, joita PLA:n läsnäolo huolestuttaisi. (Russel & Berger, 2020.)

BRI:n puitteissa rakennettava infrastruktuuri noudattaa Kiinan lainsäädäntöä, jonka mukaan siviilirakentamisen projekteissa tulee huomioida myös sotilaalliset vaatimukset. Tämä johtaa esimerkiksi satamahankkeissa kaksikäyttösatamiin, jotka nimellisesti rakennetaan ainoastaan rahtiliikennettä varten, mutta käytännössä voivat toimia myös sotilaskäytössä. Lainsäädännön mukaan PLA:lla on oikeus ottaa hallintaansa siviiliomaisuutta ja -resursseja. Tarvittaessa rakennettavia satamia voidaan siis käyttää myös Kiinan laivaston tarpeisiin. Yhteistyötä satamayhtiöiden ja Kiinan laivaston välillä harjoitellaan Kiinan ulkopuolella säännöllisesti. (Russel & Berger, 2020.)

Kiina haluaa **vahvistaa kulttuurisia siteitään** muiden maiden kanssa. Tästä vahvistamisesta yksi esimerkki on Kiinan kulttuurin symbolisena eläimenä tunnetun pandan lahjoittaminen maihin, joiden Kiina arvioi olevan luotettavia ja turvallisia. Kiinassa pandojen elinympäristöt ovat kutistuneet ja niitä on sijoitettu Kiinan eri suojelukeskuksiin. (Congressional Research Service, 2022.) Kiina on sijoittanut kyseisiä pandoja ystävällisenä eleenä yli kymmeneen eri maahan, joiden kanssa Kiina on myös vahvistanut kauppasuhteitaan (Ballawar, 2022). Kiina kuitenkin perii pandojen sijoittamisesta ja elinkustannuksista vuokraa, joka on useassa maassa osoittautunut ongelmaksi. Kalliiden kustannusten kattamiseen ovat osallistuneet kiinalaiset teknologiajätit, joiden markkinat sijaitsevat samassa maassa. Tällä menettelyllä kiinalaiset yritykset ovat saaneet avattua paremmin markkinoitaan kohdemaassa ja turvattua samalla pandojen elinolot. (Hogenboom, 2013.) Kiina hoitaa ulkosuhteitaan erilaisilla järjestelyillä siten, että maiden välinen luottamus säilyy. Pandojen avulla Kiina voi edistää maiden välistä yhteistyötä (Pacher, 2017).

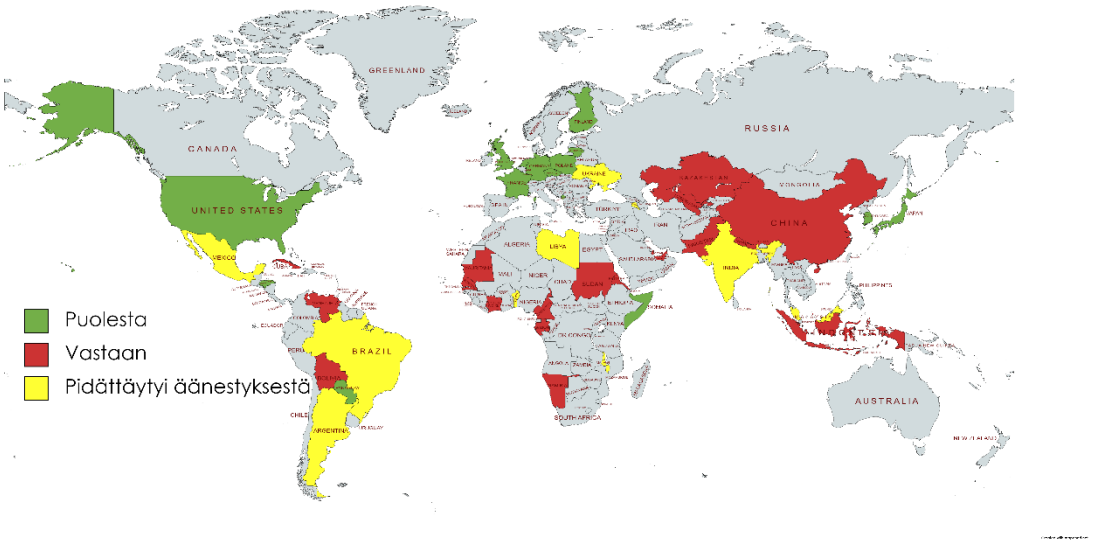
Julkisten hankintojen kilpailutuksissa kiinalaiset yritykset ovat voineet hyödyntää niihin liittyviä systeemisiä haavoittuvuuksia ja näin kasvattaa markkinaosuuttaan julkisella sektorilla. Julkisiin hankintoihin liittyvänä systeemisenä haavoittuvuutena voidaan nähdä esimerkiksi kiinalaisten yritysten saama Kiinan valtion edullinen rahoitus, jonka avulla yhtiö voi hinnoitella tuotteensa tai palvelunsa länsimaisia yhtiöitä edullisemmaksi (Siebold, 2021).

BRI-hankkeeseen liittyvä **oikeudellinen viitekehys** on hyvin hajanainen. BRI:n eri hankkeissa on solmittu erilaisia sopimusehtoja ja BRI-hankkeeseen osallistuvissa maissa on hyvin erilaisia oikeusjärjestelmiä. Riitatilanteiden ratkaisuun ei ole syntynyt yhtenäistä mallia, vaan ratkaisut hoidetaan hankekohtaisesti. Vuonna 2018 kommunistisen puolueen johtava yleisuudistuksen syventämisen komissio (engl. Central Comprehensively Deepening Reforms Commission) ehdotti perustettavaksi keskitettyä mekanismia BRI-hankkeen riitojen ratkaisuun. Nämä sittemmin perustetut Kiinan kansainvälisen kaupan tuomioistuimet (engl. China International Commercial Court, CICC) toimivat BRI-hankkeisiin liittyvien oikeudenkäyntien, sovitteluiden ja neuvotteluiden järjestäjänä yhteistyössä kansainvälisten toimijoiden, kuten Maailman kauppajärjestö WTO:n kanssa. (Dahlan, 2020.) Yhdysvallat suhtautuu kriittisesti Kiinan kommunistisen puolueen alaisuudessa toimivan CICC:n objektiivisuuteen (Whitehouse, 2020).

Neuvoteltaessa BRI-hankkeiden rahoitusehdoista Kiina on rahoituksen tarjoajana etulyöntiasemassa. Se voi vaikuttaa sopimusehtoihin ja sopimuksessa määriteltyihin riidanratkaisumenettelyihin. Näin ollen Kiina kykenee käyttämään hyväkseen PLA:n termein ”oikeudellista sodankäyntiä”, jonka avulla voidaan vaikuttaa kohteisiin ja niiden toimintaansa oikeudellisin menettelyin.

BRI-hanke avaa Kiinalle väyliä eri **tiedustelumenetelmiin**. Aiemmin mainittujen kyber- ja signaalitiedusteluiden lisäksi esimerkiksi geotiedustelun ja mittaus- ja tunnusmerkkitiedustelun mahdollisuudet paranevat BRI:n avaruusulottuvuuden ansiosta. Useisiin BRI-hankkeisiin on liittynyt kohdemaassa tapahtuvaa korruptiota (Jones & Hameiri, 2020). Kiina voi mahdollisesti hyödyntää korruptiota esimerkiksi henkilötiedustelussa joko **lahjomalla** itse tai toisaalta **kiristämällä** lahjontatietoja hyödyntäen kohdemaassa toimivia viranomaisia tai muita henkilöitä.

Kiina kykenee hyödyntämään BRI:n kautta saamaansa taloudellista vipuvartta edistääkseen omia **diplomaattisia** ja poliittisia intressejään. Yhtenä esimerkkinä mahdollisesta diplomaattisesta vaikuttamisesta voidaan nähdä lokakuussa 2022 järjestetty YK:n ihmisoikeusneuvoston äänestys siitä, tuodaanko YK:n ihmisoikeusvaltuutetun raportti Kiinan mahdollisista ihmisoikeusrikkomuksista Xinjiangissa ihmisoikeusneuvoston keskusteluun. Äänestyksessä 17 maata kannatti keskustelua, 19 vastusti ja 11 pidättäytyi äänestämisestä eikä keskustelua näin ollen viety eteenpäin (KUVIO 3) (Taussi, 2022). Käsittelyä vastustaneet ja äänestämisestä pidättyneet maat ovat pitkälti BRI-hankkeeseen osallistuneita maita, ja tämä on voinut vaikuttaa äänestykseen (Dianti, 2022).

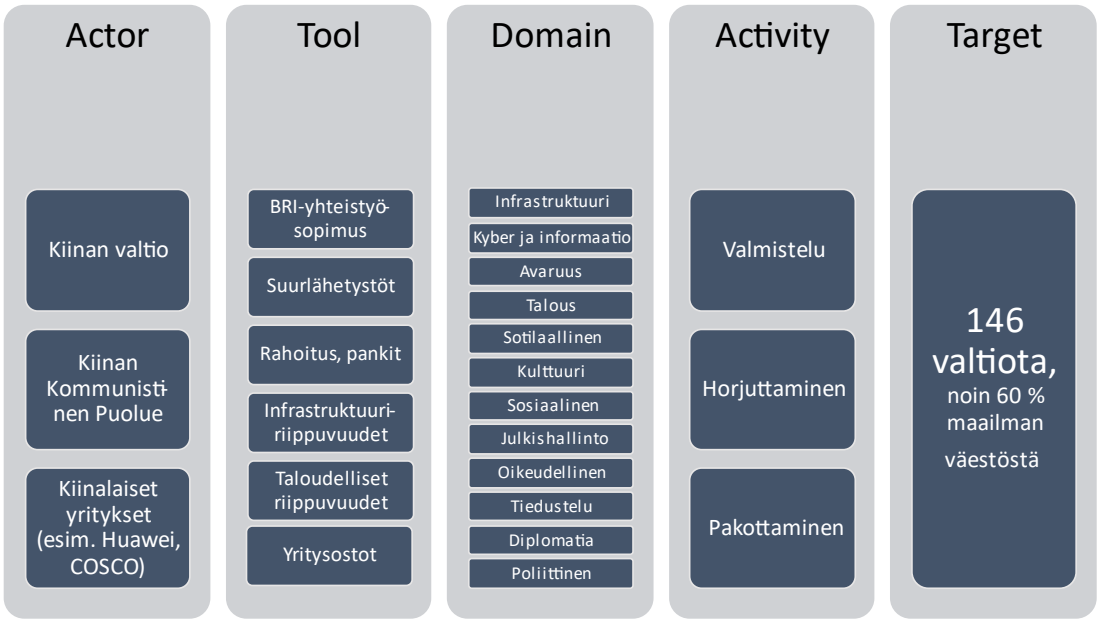


KUVIO 3 Äänestys keskustelusta Kiinan mahdollisista ihmisoikeusrikkomuksista Xinjiangissa (oma kuvio, mukaillen Taussi 2022)

BRI-hankkeita on useissa kohdemaissa käytetty **poliittisen** kamppailun välineinä (Jones & Hameiri, 2020). BRI-hanke saattaa parantaa maan talous- ja työllisyystilannetta ja näin edistää kyseisen hankesopimuksen tehneen hallinnon suosiota. Halutessaan Kiina kykenee BRI-hankkeilla tukemaan itselleen myötämielisen poliittisen liikkeen suosiota kohdemaassa ja siten vaikuttamaan kyseisen maan politiikkaan ja hallintoon.

6 Johtopäätökset

BRI-hankkeen toiminta on Kiinan kommunistisen puolueen käynnistämää ja ohjaamaa strategista toimintaa. BRI-hanke pyrkii avoimesti vaikuttamaan kohteen päätöksentekoon, jotta sen tavoitteet, kuten talouskäytävien ja -teiden avaaminen infrastruktuurihankkeiden ja investointien kautta, saadaan toteutetuksi. Koordinoinnin, päätöksentekoon vaikuttamisen ja Kiinan etujen ajamisen osalta BRI-hanke siis vastaa hybridivaikuttamisen määritelmän mukaista toimintaa. Tulkinnanvaraiseksi jää se käyttääkö Kiina BRI-hanketta hybridivaikuttamisen määritelmän mukaiseen, kohteen etujen vastaiseen, ns. pahansuopaiseen toimintaan. Kuten aikaisemmin todettiin, hybridivaikuttamisen kohdealueen ja menetelmän osalta Kiina kykenee käyttämään BRI-hanketta myös hybridivaikuttamiseen. Monet BRI-hankkeen mahdollistamat hybridivaikuttamisen keinot löytyvät Kiinan työkalupakista mahdollista tulevaa tarvetta varten (KUVIO 4). Osa keinoista on sellaisia, joita Kiinan epäillään hyödyntävän jo tällä hetkellä. Esimerkiksi eri ulottuvuuksissa tapahtuvan tiedustelun ja diplomaattisen vaikuttamisen osalta tällaisesta toiminnasta on jopa vahvoja epäilyjä. Näitä epäilyjä on kuitenkin vaikea todistaa. Tämä todistamisen vaikeus on tyypillinen hybridivaikuttamisen ominaispiirre.



KUVIO 4 Kiinan hybridivaikuttamisen kokonaisuus

BRI-maat joutuvat väistämättä arvioimaan suhdettaan Kiinaan. BRI:n etenemisen myötä lisääntyy maiden välinen integraatio, johon liittyy mahdollisten poliittisten riskien syntyminen ja niiden kautta valtioiden strategisen autonomian vaarantuminen. Kohdemaissa tunnistetut haavoittuvuudet antavat Kiinalle lisäponnen tarjota BRI-hankkeen ratkaisuja. Haavoittuvuuksien tunnistamisessa ja hyödyntämisessä voivat taustalla olla riippuvuussuhteen luominen ja vahvistaminen ja muut hybridivaikuttamisen keinot. Laajat kriisitilanteet voivat kääntyä Kiinan eduksi ja asettaa viennin kohteena olevan maan riippuvaiseksi muun muassa kriittisen infrastruktuurin ylläpitoon tarvittavan materiaalin, terveydenhuollon ja puolustusteollisuuden hankintojen osalta.

Lähteet

Ballawar, N. (6. 5 2022). *Analysing the transition from China's Panda Diplomacy to Wolf-Warrior Diplomacy*. Noudettu osoitteesta Diplomatist: https://diplomatist.com/2022/05/06/analysing-the-transition-from-chinas-panda-diplomacy-to-wolf-warrior-diplomacy/

Congressional Research Service. (2022). *The People's Republic of China's Panda Diplomacy.* Haettu 13. 11 2022 osoitteesta https://crsreports.congress.gov/product/pdf/IF/IF12122/2

Dianti, T. (7. 10 2022). *Indonesia opposes 'politicizing' UN rights body after blocking China-Uyghur debate*. Haettu 11. 11 2022 osoitteesta Radio Free Asia: https://www.rfa.org/english/news/uyghur/un-china-vote-10072022173135.html

EU-Hybnet_network. (13. 11 2022). *A coherent approach focusing on the domains of hybrid threats*. Noudettu osoitteesta Hybrid Threat Domains: https://euhybnet.eu/

Garcia, Z.;& Guerreiro, P. (29. 1 2022). *The Diplomat.* Noudettu osoitteesta https://thediplomat.com/2022/01/chinas-domestic-politics-are-driving-the-belt-and-road-initiative/

GFDRR. (8 2022). *Natural Disaster Challenges in China: Key trends and insights*. Noudettu osoitteesta https://www.gfdrr.org/en/feature-story/natural-disaster-challenges-china-key-trends-and-insights

Hogenboom, M. (25. 9 2013). *China's new phase of panda diplomacy*. Noudettu osoitteesta BBC: https://www.bbc.com/news/science-environment-24161385

Huawei. (2022). *Huawei annual report 2021.* Haettu 8. 11. 2022 osoitteesta https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf

Hui, J. (2018). *The Spatial Information Corridor Contributes to UNISPACE+50.* China National Space Administration. Haettu 11. 11. 2022 osoitteesta https://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf

Jones, L.;& Hameiri, S. (2020). *Debunking the Myth of "Dept-trap Diplomacy" - How Recipient Contries Shape China's Belt and Road Initiative.* Asia-Pacific Programme. Chatham House. Haettu 5. 8. 2022 osoitteesta https://www.chathamhouse.org/sites/default/files/2020-08-25-debunking-myth-debt-trap-diplomacy-jones-hameiri.pdf

Kallio, J. (2022). *China's belt and road initiative - Succesful economic strategy or failed soft-power tool?* Finnish Institute of International Affairs (FIIA).

Kohli, H. S.;& Zucker, L. M. (2020). *An economic perspective on the Belt and Road Initiative: Six yeras after its launch. Teoksessa China's Belt and Road Intiative: Potential Transformation on Central Asia and the South Caucasus.* (H. S. Kohli;J. F. Linn;& L. M. Zucker, Toim.) Sage Publications.

Manninen, M. (2019). Tuntematon Kiina,YLE. (K. Haatanen, Haastattelija) Suomi.

Manninen, M. (2021). *Näin Kiina valloittaa koko maailman.* Helsingin sanomat. HS minidokumentti.

Mattlin, M. (3. 11. 2022). A-Talk. YLE. Helsinki.

Nedopil, C. (2022). *China Belt and Road Initiative (BRI) Investment Report H1 2022*. (G. F. Center, Toim.) Sanghai: FISF Fudan University. Noudettu osoitteesta https://greenfdc.org/wp-content/uploads/2022/07/GFDC-2022_China-Belt-and-Road-Initiative-BRI-Investment-Report-H1-2022.pdf

Ni, V. (16. 8. 2022). *Chinese navy vessel arrives at Sri Lanka port to security concerns from India*. Haettu 12. 11. 2022 osoitteesta The Guardian: https://www.theguardian.com/world/2022/aug/16/chinese-navy-vessel-arrives-at-sri-lanka-port-to-security-concerns-from-india

OECD. (2018). *China´s Belt and Road Initiative in the Global Trade, Investment and Finance Landscape. Business and Finance Outlook 2018.* Paris: OECD, Publishing. doi:https://doi.org/10.1787/bus_fin_out-2018-6-en.

Pacher, A. (2. 11 2017). *China's Panda Diplomacy* . Noudettu osoitteesta The Diplomat: https://thediplomat.com/2017/11/chinas-panda-diplomacy/

Paltemaa, L. (2019). *Turun Eurooppa-foorumi 2019. EU ja Kiina: Uusi silkkitie hinnalla millä hyvänsä?* Turun kaupunki.

Prasso, S. (10. 1. 2019). *China's Digital Silk Road Is Looking More Like an Iron Curtain*. Noudettu osoitteesta Bloomberg.

Puranen, M. (2021). Kiinan EU-pakotteet tähtäävät kriittisen Kiina-tutkimuksen tukahduttamiseen. *The Ulkopolitist.*, https://ulkopolitist.fi/2021/04/11/kiinan-eu-pakotteet-tahtaavat-kriittisen-kiina-tutkimuksen-tukahduttamiseen/.

Ruotsin kokonaismaanpuolustuksen tutkimuslaitos. (2019). *Kinas rymdprogram och rymdförmågor.* Totalförsvarets forskningsinstitut. Haettu 12. 11 2022 osoitteesta https://www.foi.se/rest-api/report/FOI-R--4718--SE

Russel, D. R.;& Berger, B. H. (2020). *Weaponizing the Belt and Road Initiative.* Asia Society Policy Institute. Haettu 11.. 11 2022 osoitteesta https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf

Siebold, S. (5. 5 2021). *With eye on China, EU drafts rules to curb state-backed foreign buyers*. Haettu 9. 11. 2002 osoitteesta Reuters: https://www.reuters.com/world/china/eu-drafts-rules-curb-state-backed-foreign-buyers-2021-05-05/

Taussi, S. (7. 10 2022). *Kiina tukijoineen esti uiguurien vainosta keskustelemisen YK:n ihmisoikeusneuvostossa – äänestystulos oli suuri pettymys länsimaille*. Haettu 11. 11 2022 osoitteesta Yle.fi: https://yle.fi/uutiset/3-12652407

The European Centre of Excellence for Countering Hybrid Threats. (2021). *The Landscape of Hybrid Threats: A Conceptual Model Public Version.* (G. Giannopoulos;H. Smith;& M. Theocharidou, Toim.) European Commission Publications Office. Haettu 5. 11 2022 osoitteesta https://data.europa.eu/doi/10.2760/44985

The World Factbook. (6. 11 2022). Noudettu osoitteesta https://www.cia.gov/the-world-factbook/countries/china/#introduction

Ulkoministeriö. (2021). *Suomen valtionahllinnon Kiina toiminta-ohjelma.* Ulkoministeriö.

United Nations Development Programme China. (2017). *Report on the sustainable development of Chinese enterprises overseas.* Beijing. Haettu 13. 11 2022 osoitteesta https://www.undp.org/china/publications/2017-report-sustainable-development-chinese-enterprises-overseas

United Nations Human Rights Office of the High Commissioner. (2022). *OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous*

Region, People's Republic of China. United Nations. Haettu 11. 11. 2022 osoitteesta https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf

Vidal, J. (2022). *Are China's pledges to green its belt and road initiative the real deal?* Haettu 13. 11 2022 osoitteesta Ensia: https://ensia.com/features/china-belt-road-initiative-infrastructure-sustainable-silk-road/

Whitehouse. (2020). *United States Strategic Approach to the People's Republic of China.* Whitehouse. Haettu 12. 8 2022 osoitteesta https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf

WorldData.info. (8. 11 2022). *WorldData.info*. Noudettu osoitteesta China: https://www.worlddata.info/asia/china/index.php

Xinhua. (14. 5 2017). *Full text of President Xi's speech at opening of Belt and Road forum*. (Yamei, Toimittaja) Haettu 8. 11 2022 osoitteesta XinhuaNet: http://www.xinhuanet.com/english/2017-05/14/c_136282982.htm

TIETOVERKKOTIEDUSTELU JA VERKKOVAKOILU OSANA KIINAN SUORITTAMIA KYBEROPERAATIOITA

Eero Oksala, Mikko Heikkinen, Janne Vulli, Toni Lehtinen

1 Johdanto

Kiinan pitkäaikainen tavoite on nousta maailman suurimmaksi taloudeksi vuoteen 2050 mennessä, jolloin valtio täyttää 100 vuotta. Tähän strategiseen tavoitteeseen pyritään kansallisten konseptien sekä globaalien kehitysohjelmien avulla, joiden tarkoituksena on muun muassa massiivisten infrastruktuuriprojektien kautta luoda maailmankauppaa palveleva teknologiaverkosto, niin sanottu ”digitaalinen silkkitie”. Teknologiaverkosto on osa Kiinan ”Vyö ja tie”-ohjelmaa (engl. Belt and Road Initiative, myöhemmin BRI-ohjelma), minkä mukaisesti valtio rakentaa mittavaa maa- ja meriyhteyksien verkostoa (OECD, 2018).

Kommunikaatioinfrastruktuurin osalta Kiina on linjannut tavoitteekseen edistää rajoja ylittävien verkkoyhteyksien rakentamista ja parantaa kansainvälisiä tietoliikenneyhteyksiä. Samalla Kiinan presidentti Xi Jinping on säätänyt kansallista turvallisuutta vahvistavia lakiuudistuksia, joiden voidaan tulkita edesauttavan Kiinan vaikutusvaltaa lähi- ja ulkomailla, velvoittaen kiinalaiset organisaatiot ja yksilöt avustamaan maan tiedustelutoimijoita (Turunen, 2021). Xin aikakaudella onkin korostunut holistinen turvallisuuskäsitys, jossa perinteiset ja ei-perinteiset uhkat sekä sisäinen ja ulkoinen turvallisuus ovat sekoittuneet (Puranen, 2022).

Moninapaisessa maailmassa korostuvat tutkimus-, kehitys- ja innovaatiotoiminta, jonka johdosta yliotteen saa se valtio, joka hallitsee teknologiaa ja dataa; tekoälyä, kvanttiteknologiaa, robotiikkaa ja televerkkoja (Turunen, 2021). Kiinaa on syytetty teknologiakehityksen dominanssin tukemisesta valtiollisella tietoverkkotiedustelulla, joka länsimaisissa yhteiskunnissa voidaan tulkita verkkovakoiluksi. Verkkovakoilun kautta Kiinan voidaan nähdä pyrkivän hankkimaan osaamista ulkomailta, millä se tukee omaa tuotekehitystään ja siten parantaa markkina-asemaansa. Suojelupoliisi (2021a) onkin varoittanut autoritääristen valtioiden tiedustelupalveluiden käyttävän verkkolaitteita ja palvelimia verkkovakoilussa. Suojelupoliisi myös nimesi ensimmäistä kertaa julkisesti niin kutsutun APT31-ryhmän, jonka ilmoitettiin suorittaneen verkkovakoilua eduskunnan tietojärjestelmissä vuonna 2013 (Suojelupoliisi, 2021b). Suojelupoliisi ei nimennyt tekijävaltiota, mutta APT31 on attribuoitu Kiinan kansanarmeijaan (engl. People’s Liberation Army, myöhemmin PLA) (Itkin & Cohen, 2021).

Tämän raportin tavoitteena on pyrkiä tarkastelemaan Kiinan suorittamaa tietoverkkotiedustelua ja -vakoilua osana sen strategisten intressien tavoittelua. Tarkastelun kohteena ovat Kiinaan attribuoidut APT-ryhmät (engl. Advanced Persistent Threat), PLA:n tietoverkkotiedustelua suorittavat sotilasorganisaatiot, sekä kiinalaiset teknologiahankkeet ja -konsernit. Raportti koostuu neljästä pääluvusta. Luvussa 2 tarkastellaan Kiinan valtiollisten organisaatioiden suorittamaa tietoverkkotiedustelua. Tarkastelu on rajattu PLA:n sotilasorganisaatioihin sekä Kiinan valtioon kytkeytyviin APT-ryhmiin,

joiden suorittamaa tiedonhankintaa pyritään vertaamaan toisiinsa. Koska tiedustelun ja vakoilun attribuoiminen on haastavaa, tarkastellaan APT-ryhmien ja PLA:n tietoverkkotiedustelun tapausesimerkkejä yhtenäisesti. Esimerkeissä on kuitenkin pyritty nimeämään taustaorganisaatio, mikäli se on ollut todennettavissa useasta luotettavasta lähteestä. Luvussa 3 tarkastellaan kiinalaisen globaalin teknologiaverkoston käytön mahdollisuuksia verkkovakoilun viitekehyksessä. Tarkastelun kohteena ovat ”digitaalisen silkkitien” lisäksi kiinalaisten teknologiakonsernien maailmanlaajuinen levittäytyminen. Luvussa 4 esitellään lyhyesti raportin johtopäätökset ja pohditaan aihetta kokonaisuutena.

Raportissa tietoverkkotiedustelulla tarkoitetaan tietoverkossa toteutettavaa suunnitelmallista, peiteltyä tiedonhankintaa, joka jakautuu tietoliikennetiedusteluun ja tietojärjestelmätiedusteluun (Hakonen, 2021). Tietoliikennetiedustelulla tarkoitetaan tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä (Laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019). Tietojärjestelmätiedustelulla tarkoitetaan tietoteknisin menetelmin suoritettavaa tietojen hankintaa tietojärjestelmistä (Laki sotilastiedustelusta 590/2019). Teknologiakonsernien toiminnan tarkastelun sekä sekundäärilähteiden käytön johdosta aihetta käsitellään myös verkkovakoilun näkökulmasta. Raportissa verkkovakoilulla tarkoitetaan tietoteknisin menetelmin suoritettavaa laitonta tietojen hankkimista ja keräämistä (ENISA, 2020).

2 Kiinan valtiollisten toimijoiden suorittama tietoverkkotiedustelu

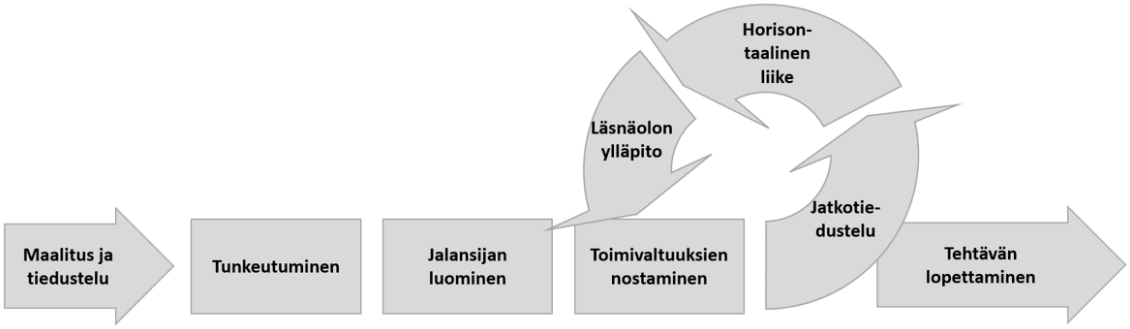
2.1 Yleistä APT-ryhmistä

APT-ryhmillä (engl. Advanced Persistent Threat) tarkoitetaan internetissä toimivia ryhmittymiä, joilla on käytössä edistynyttä osaamista ja resursseja kyberoperaatioiden toteuttamiseksi. Kyberoperaatioiden tavoitteet voivat liittyä tietojen hankkimiseen poliittisista vastustajista, taloudellisen edun tavoitteluun tai teollisuusvakoiluun. Ryhmät pyrkivät tavoitteisiinsa useita eri hyökkäysvektoreita hyödyntämällä, samalla tavoitellen englanninkielisen termin mukaisesti pitkäaikaista läsnäoloa kohdejärjestelmissä. Pitkäaikainen läsnäolo edellyttää kohteen suojaustoimenpiteisiin mukautumista ja kykyä ylläpitää kyberoperaatiota jatkotiedustelulla, takaovilla (engl. backdoor) sekä horisontaalisella liikkeellä kohdejärjestelmässä (National Institute of Standards and Technology, 2011; kts. McWhorter, 2013).

APT-toimijoiksi on tunnistettu valtiollisia toimijoita, järjestäytyneitä rikollisryhmiä ja kyberterroristeja. Toimijoiden attribuointi on kuitenkin haastavaa, sillä toiminta pyritään aina salaamaan ja peittelemään erilaisin teknisin toimenpitein. Valtiolliset toimijat ovat yleensä valtioiden tiedustelupalveluita, sotilasyksiköitä tai valtioiden tukemia ryhmiä. Taustaorganisaatio vaikuttaa APT-ryhmän motivaatiotekijöihin ja kohteisiin. Valtiollisilla toimijoilla kohteena saattaa olla toisen valtion kriittinen infrastruktuuri ja tavoitteena päättäjiin ja päätöksentekoon vaikuttaminen. Tavoitteena voi myös olla toisen valtion tiedustelu ja vakoilu. Järjestäytyneen rikollisuuden APT-ryhmien motiivina on taloudellisen edun tavoittelu, ja kohteina ovat niin yksittäiset kansalaiset kuin yrityksetkin. Sekä valtiollisten, valtiollisiin toimijoihin kytkeytyvien, että järjestäytyneen rikollisuuden APT-ryhmien tavoitteena voi olla myös teollisuusvakoilu, jolla pyritään saamaan haltuun

liiketoimintasuunnitelmia ja liikesalaisuuksia, kuten esimerkiksi tietoja korkean teknologian tutkimus- ja kehitysohjelmista (Secureworks, 2016).

APT-ryhmien toteuttamien kyberoperaatioiden elinkaari ja vaiheet voidaan kuvata kuvion 1 mukaisesti (Mandiant, ei pvm.; McWhorter, 2013). Operaatio alkaa kohteen identifioimisella ja tiedustelulla. Korkean teknologian organisaatiot ja yritykset saattavat joutua APT-ryhmien tiedustelun kohteeksi, mikäli niillä on hallussa kriittisen tiedon liikesalaisuuksia, tai muita immateriaalisia oikeuksia, joita APT-ryhmän taustaorganisaatio kykenisi hyödyntämään. Tiedusteltavalla organisaatiolla saattaa olla myös pääsy hyödyllisiin aineistoihin tai tietokantoihin, tai se saattaa olla osallisena kiinnostavaa tieteellistä tutkimusta. Myös pankit, finanssilaitokset, kriittisen infrastruktuurin toimijat ja poliittiset instituutiot, sekä valtioiden turvallisuuselimet ovat tyypillisiä tiedustelun kohteita (Burita & Le, 2021).



KUVIO 1 APT-ryhmän operaation elinkaari (McWhorter, 2013)

Tiedustelun jälkeen hyökkääjä pyrkii tunkeutumaan maalitetun kohteen tietojärjestelmään. Tyypillisesti APT-ryhmien suorittama tunkeutuminen pyritään toteuttamaan tiedusteluvaiheessa tunnistettuihin henkilöihin kohdistuvan kalastelun kautta (engl. phishing), sekä saastutetun verkkopalvelun tai tiedoston avulla, millä luodaan takaovi uhrin järjestelmään. Takaoven avulla hyökkääjä kykenee kontrolloimaan kohdejärjestelmää, kyeten muodostamaan jalansijan operaation jatkamiselle. Jalansijan luomisen jälkeen hyökkääjä pyrkii nostamaan toimivaltuuksiaan siten, että operaation jatkaminen onnistuu. Kohotettujen toimivaltuuksien avulla hyökkääjä kykenee jatkamaan kohdejärjestelmän tiedustelua, kyeten keräämään kohdeorganisaatiosta tavoiteltua informaatiota. Toimivaltuuksien noston jälkeen hyökkääjä pyrkii liikkumaan horisontaalisesti kohteen tietojärjestelmässä, samalla kohdentaen toimiaan myös muihin käyttäjiin ja järjestelmiin. APT-ryhmät valmistautuvat jatkamaan toimintaansa kohteen tietojärjestelmissä pitkään, kuukausien tai jopa vuosien ajan (McWhorter, 2013).

2.2 Kiinalaiset APT-ryhmät

Kiinalaisia tai Kiinaan kytkeytyviä APT-ryhmiä on tunnistettu noin kolmekymmentä. Näiden ryhmien toiminta on pystytty varmentamaan useasta lähteestä ja niiden tekemät hyökkäykset on dokumentoitu hyvin (Burita & Le, 2021). Taulukossa 1 on esitetty kiinalaisten tai Kiinaan kytkeytyvien APT-ryhmien tunnuksia, nimiä ja päätavoitteita. Kiinalaisten APT-ryhmien tavoitteet voidaan jakaa tietovarkauksiin, vakoiluun ja sabotaasitoimintaan. Esitetty jako on karkea ja todellisuudessa yksittäinen APT-ryhmä saattaa harjoittaa muutakin kuin päätavoitteen mukaista toimintaa. Tietovarkaudella tarkoitetaan laajasti erilaisia aineettomiin oikeuksiin, kuten viestintään, tuotekehitykseen ja henkilötietoihin liittyvää rikollista toimintaa. Vakoilulla tarkoitetaan Kiinan vastustajiksi

katsomiensa tahojen vakoilua, jonka kohteena voivat olla esimerkiksi länsivaltiot, kansalaisjärjestöt, toisinajattelijat ja poliittiset toimijat. Kiinalaisten APT-ryhmien toiminnassa on päätavoitteen lisäksi havaittavissa erikoistumista tiettyjen toimialojen tai maantieteellisen alueen toimijoihin. Esimerkiksi APT21, joka tunnetaan myös nimellä Xhenbao, on erikoistunut Venäjän hallintoa sekä toisaalta kiinalaisia toisinajattelijoita vastaan suuntautuvaan toimintaan. Toisaalta esimerkiksi APT7 on erikoistunut rakennusteollisuuden, ilmailun ja puolustustarviketeollisuuden toimijoihin kohdistuviin operaatioihin (Mandiant, ei pvm).

Ryhmä	Muut nimet	Päätavoite
APT1	PLA Unit 61398, Comment Crew, Comment Panda	Tietovarkaudet
APT2	Putter Panda	Tietovarkaudet
APT3	Gothic Panda, UPS Team	Vakoilu
APT4	Maverick Panda, Sykipot Group, Wisp	Vakoilu
APT6		Tietovarkaudet
APT7		Tietovarkaudet
APT8		Tietovarkaudet
APT10	Red Apollo, MenuPass, POTASSIUM, Stone Panda	Vakoilu
APT12	IXESHE, DunCalc, Numbered Panda	Vakoilu
APT14		Vakoilu
APT15	Ke3chang, Mirage, Vixen Panda	Vakoilu
APT16		Vakoilu
APT17	Debuty Dog	Vakoilu
APT18	TG-0416, Webky, Dynamite Panda	Vakoilu
APT19	Codoso Teamn	Vakoilu
APT20	Twiwy	Vakoilu
APT21	Zhenbao	Vakoilu
APT22	Barista	Sabotaasit
APT23		Vakoilu
APT24	PittyTiger	Vakoilu
APT26		Tietovarkaudet
APT27	IronTiger, Emissary Panda	Tietovarkaudet
APT30	PLA Unit 78020, Naikon	
APT31		Vakoilu
APT40	Leviathan, Periscope Group, TEMP.Jumper	Tietovarkaudet
APT41	Double Dragon	Vakoilu

TAULUKKO 1 Kiinalaisia APT-ryhmiä (Burita & Le, 2021)

APT-ryhmien sisäisestä organisaatiosta, vastuuhenkilöistä ja muista yksityiskohdista tiedetään verrattain vähän, mikä on ymmärrettävää toiminnan luonne huomioon ottaen.

Kuitenkin vuonna 2013 tietoturvayhtiö Mandiant julkaisi yksityiskohtaisen raportin APT1-ryhmästä tutkittuaan ryhmää seitsemän vuoden ajan ja käyden läpi yli 150 ryhmän tekemää kyberoperaatiota. APT1-ryhmä pystyttiin Mandiantin tutkimuksessa kytkemään vahvasti Kiinan kansan vapautusarmeijan yksikköön, joka tunnetaan koodilla 61398. APT1-ryhmän osalta Mandiant pystyi lisäksi selvittämään jopa yksikön fyysisen sijainnin ja yksilöimään kolme ryhmässä toiminutta henkilöä. APT1-ryhmän fyysiseksi sijainniksi paljastettiin Pudongin alue Shanghain kaupungissa Kiinassa ja raportissa henkilöistä käytettiin nimimerkkejä ”UglyGorilla”, ”DOTA” ja ”SuperHard” (McWhorter, 2013). Nimimerkkien taustalla olevien todellisten henkilöiden henkilöllisyyksiä on pystytty selvittämään ja muun muassa FBI on etsintäkuuluttanut sekä APT1-ryhmän jäseniä että muita kyberoperaatioihin liitettyjä kiinalaisia (FBI, ei pvm.).

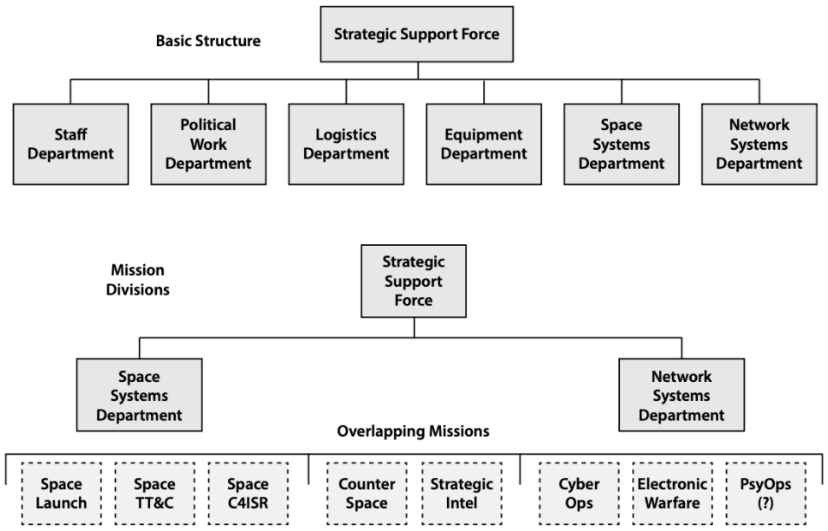
Yhdysvaltalaisviranomaiset ovat varoittaneet Kiinan valtion tukemien APT-ryhmien kasvaneesta kyvykkyydestä kehittyneisiin verkko-operaatioihin. CISA:n (engl. Cybersecurity & Infrastructure Agency) on tunnistanut kolme trendiä Kiinaan kytkeytyvien ryhmien toiminnassa:

1. **Infrastruktuurin ja kyvykkyyksien hankkiminen:** Kiinaan kytkeytyvät ryhmät toimivat ketterästi ja ovat tietoisia tietoturvaan liittyvistä käytännöistä. Ryhmät pyrkivät peittämään toimintansa käyttämällä yksityisiä virtuaalipalvelimia ja kaupallisia tai avoimen lähdekoodin tunkeutumistyökaluja.
2. **Tiedossa olevien haavoittuvuuksien hyödyntäminen**: Kiinalaiset ryhmät skannaavat organisaatioiden tietoverkkoja aktiivisesti ja pystyvät hyödyntämään julkiseksi tulleita haavoittuvuuksia jopa muutamassa päivässä, kun tieto haavoittuvuudesta on julkaistu.
3. **Salattujen monihyppyvälityspalvelimien käyttö (engl. Encrypted Multi-Hop Proxies):** Kiinaan yhdistettävät ryhmät pyrkivät aktiivisesti peittelemään jälkiänsä välityspalvelimia käyttämällä. Niin kutsuttujen SOHO-laitteiden (engl. Small Office and Home Office) heikkoa tietoturvaa hyödynnetään kiinalaisten kyberoperaatioiden salaamisessa ja peittelemisessä (CISA, 2021)

2.3 PLA:n suorittama sotilastiedustelu

Kiinan kansan vapautusarmeijan, PLA:n sotilastiedustelu on Brazilin ja Mattisin (2019) mukaan organisoitu uudelleen vuonna 2015. Tätä ennen tiedustelusta vastasivat yleisesikunnan sotilastiedusteluosasto (2PLA) yhdessä teknisen tiedustelun osaston (3PLA) kanssa. Henkilö- ja signaalitiedustelu kuuluivat aiemmin 2PLA:n tehtäviin, kun taas 3PLA muodosti ilmeisesti henkilöresursseiltaan suurimman kiinalaisen tiedusteluorganisaation (Lowenthal & Clark, 2016). Uudistuksessa verkkotiedustelun osaaminen keskitettiin Stategic Support Forceen (SSF). Samalla aiempi General Staff Department (GSD) nimettiin uudelleen Joint Staff Departmentiksi (JDS), jonka tehtävistä maajoukkojen esikunta eriytettiin ja tiedustelun painoarvoa sen tehtävissä lisättiin (Saunders, 2017). Aiemmat tiedusteluyksiköt 2PLA ja 3 PLA sulautettiin osaksi Strategic Support Forcea, jolloin siitä tehtiin organisaatiokaavioon selkeä sotilastiedustelun osaamiskeskittymä. SSF:n vastuualueelle kuuluu tämän myötä avaruusteknologiaosasto (engl. Space Systems

Department) sekä tietoverkko-osasto (engl. Network Systems Department) (Brazil & Mattis, 2019). SSF:n rakenne on esitetty kuviossa 2.



KUVIO 2 SSF:n hierarkiarakenne (Costello ja McReynolds, 2018)

Nykyisen kiinalaisen määritelmän mukaan kybersodankäynti on osa laajempaa informaatiosodankäyntiä, johon sisältyy myös elektroninen sodankäynti ja psykologinen sodankäynti (Costello & McReynolds, 2018). SSF onkin PLA:n keskeinen organisaatio, joka vastaa informaatiosodankäynnin mukaisista suorituskyvyistä. SSF parantaa PLA:n kykyä suorittaa tietoverkkotiedustelua yhdistämällä sen osaksi informaatiosodankäynnin suorituskykyjä (Costello & McReynolds, 2018). Kiina on lisäksi järjestänyt valtiollisen tiedustelutoimintansa usean muun eri toimijan kautta, joita ovat SSF:n lisäksi Ministry of State Security (MSS) ja Ministry of Public Security (MPS).

Kiinan sotilastiedustelun suorittamat operaatiot mukailevat usein APT-ryhmien hyökkäysten elinkaarta, jossa kiinnostavat kohteet maalitetaan ja tiedustellaan, tekniset haavoittuvuudet tunnistetaan ja niiden hyväksikäyttö suunnitellaan sopivien työkalujen avulla (NSA, 2020). Tunkeutuminen tapahtuu tyypillisesti APT-ryhmien tavoin myös kohdennettujen kalastelusähköpostien avulla, joissa on saastunut haitallinen liitetiedosto (Checkpoint, 2022)

Yhdysvaltojen tiedustelupalveluiden koostaman raportin mukaan Kiinan valtion ja kommunistisen puolueen ohjaaman tiedustelun pääasiallisena tavoitteena on päästä käsiksi Yhdysvaltojen ja sen liittolaisten poliittiseen, taloudelliseen ja puolustukselliseen infrastruktuuriin. On muistettava, että huomattava osa Kiinan verkkotiedustelukyvykkyyksistä löytyy PLA:n sisältä, joten käytännön tiedustelua suorittavat kohteesta riippumatta sotilastiedustelun yksiköt. (NSA; CISA; FBI, 2021) Tietomurron jälkeen tavoitteena on varastaa tuote- tai tuotantoteknologiaan liittyvää materiaalia, Yhdysvaltojen asevoimiin liittyvää informaatiota tai esimerkiksi uusinta tutkimustietoa, mikäli kohteena ovat esimerkiksi yliopistot tai lääketieteellistä tutkimusta tekevät yksiköt (FBI, 2021).

Kiinan sotilastiedustelussa käytetään laajaa keinovalikoimaa asetettujen tavoitteiden saavuttamiseksi, mutta verkkotiedustelun ja -murtojen yhteisinä piirteinä voidaan mainita pyrkimys attribuutio-ongelman luomiseen. Tämän saavuttamiseksi PLA:n toimijat käyttävät VPS:ää (engl. Virtual Private Server) ja vapaasti saatavilla olevia

hyökkäystyökaluja (NSA; CISA; FBI, 2021), joilla kyetään häivyttämään hyökkäysten todellinen tekijä. Myös globaalisti käytössä olevien ohjelmistojen tunnettujen tietosuojahaavoittuvuuksien (engl. Common Vulnerabilities and Exposures, CVE) hyväksikäyttö on kiinalaisille toimijoille tavanomaista (NSA, 2020).

2.4 Esimerkkejä vakoiluhyökkäyksistä

Vuonna 2009 kiinalaiset toimijat onnistuivat tietojärjestelmätiedustelun avulla murtautumaan Yhdysvaltain puolustusministeriön Pentagonin tietojärjestelmiin. Hyökkääjät onnistuvat pääsemään käsiksi Joint Strike Fighter-projektin tiedostoihin, mahdollistaen F35-monitoimihävittäjien suunnitteluun ja elektroniikkaan liittyvän informaation varastamisen (Lehto, 2022).

Vuonna 2015 kiinalaiset toimijat murtautuivat Yhdysvaltojen Office of Personnel Managementin (OPM) tietojärjestelmiin, onnistuen 22 miljoonan valtion virkamiehen henkilötietojen, turvallisuusselvitysten ja biometristen tunnisteiden varastamisessa. Tapaus konkretisoitui korkeimman tason turvallisuusselvitysten tietovuotona, käsittäen muun muassa tiedusteluviranomaisten henkilökohtaiset selvitykset kiristyksille alttiista ihmissuhteista ja elämänkokemuksista. (Anderson, 2020)

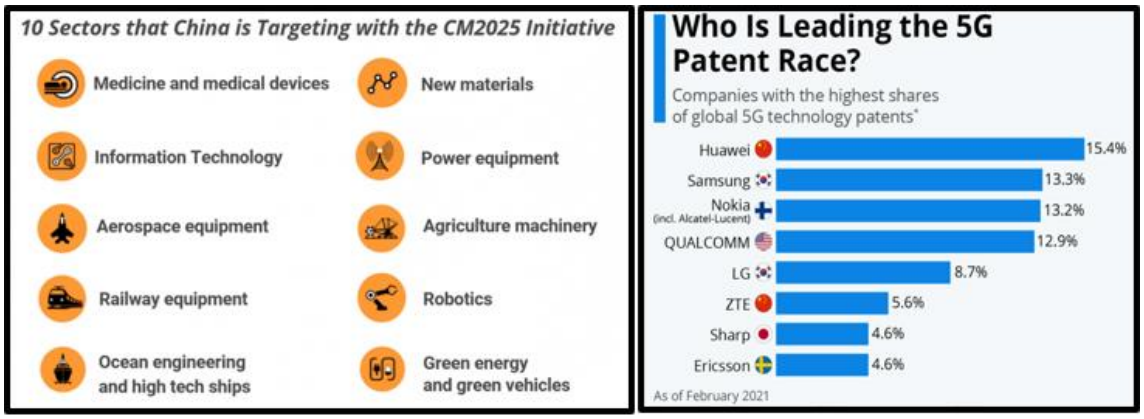
Kiinan asevoimien suorittama tiedustelu ei rajoitu vain sotilaskohteisiin ja kansalliseen turvallisuuteen. Viittä PLA:n upseeria syytettiin vuonna 2019 kuuden yhdysvaltalaisen teknologiateollisuusyrityksen hakkeroinnista. Upseerit toimivat PLA:n yksikössä 61398, joka tunnetaan myös APT1-ryhmänä. Syytetyt olivat ryhmän alaisuudessa suorittaneet kohdistettuja kyberhyökkäyksiä useisiin kaupallisiin yrityksiin, jotka osallistuivat Kiinan valtion omistamien yritysten kauppaneuvotteluihin. Neuvotteluiden aikana upseerit murtautuivat kohdeyritysten tietojärjestelmiin mahdollistaen sähköpostikeskusteluiden sekä yrityssalaisuuksien mukaisten valmistusprosessien ja tuotantokustannusten varastamisen, sekä kohdejärjestelmien haavoittuvuuksien tunnistamisen. Tällä mahdollistettiin Kiinan etulyöntiasema kauppaneuvotteluissa. (FBI, 2019).

3 Verkkovakoilua kommunikaatioinfrastruktuurissa

3.1 Kiinan teknologisen kehityksen strategiat

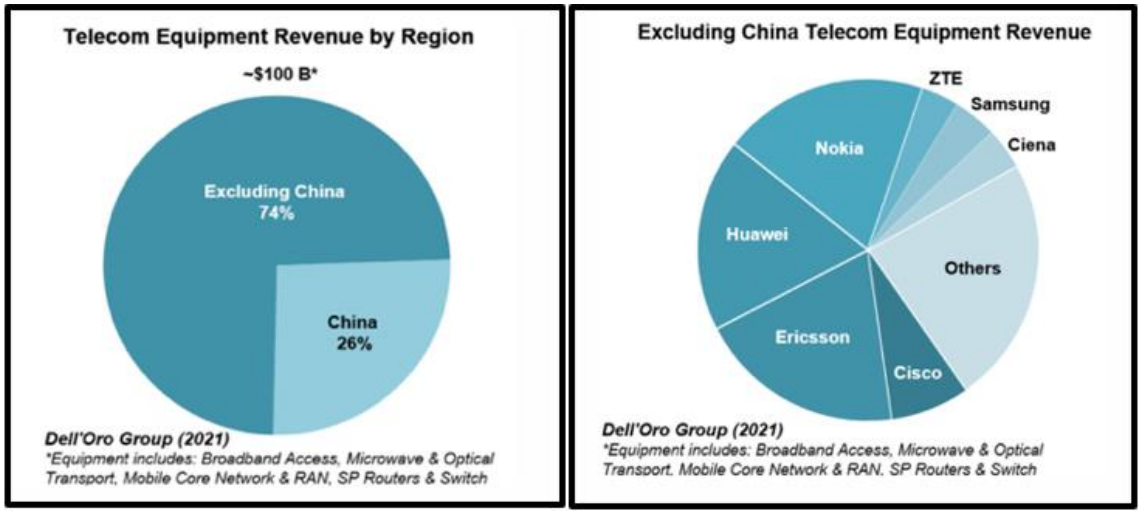
Kiina on teknologisesti kyvykkäimpiä valtioita suorittamaan tietoverkkotiedustelua ja verkkovakoilua osana omien strategisten intressien saavuttamista (NCSC, 2018). Vakoilun tavoitteina arvioidaan olevan vastustajan kriittisen infrastruktuurin ja teknologisten innovaatioiden heikkouksien selvittämisen, kansallisten salaisuuksien varastamisen, sekä demokraattisen yhteiskunnan horjuttamisen (Manfra, 2019). Läntisten valtioiden elintärkeiden toimintojen ja kriittisen infrastruktuurin riippuvuus tieto- ja viestintäjärjestelmistä ja tietoliikenneverkoista on ilmeinen. Kiinan hallitus pitääkin tietoliikenneverkkojen liiketoiminta-aluetta strategisena toimialana, johon se on käyttänyt merkittäviä resursseja uusien toimintamahdollisuuksien edistämiseksi (Portman & Carper, ei pvm; Ceci & Rubin, 2022). Kiina on julkaissut vuonna 2015 niin kutsutun ”*Made in China 2025*”-konseptin (myöhemmin MIC 2025), joka kohdistuu kymmeneen eri teollisuudenalaan, joilla on arvioitu olevan vaikutusta Kiinan taloudelliseen kilpailukyvyn kasvuun sekä korkean teknologian kehitykseen (U.S. Chamber of Commerce, 2017). Konsepti sisältää suunnitelman informaatioteknologian sekä sen mukaisten elektronisten

laitteistojen kehityksestä ja globaalista levityksestä, mihin Kiinan hallinto on sitoutunut erillisillä valtion rahoituksilla, matalakorkoisilla lainoilla ja verohelpotuksilla (McBride & Chatzky, 2019). Tarkkoja rahasummia ei ole ilmoitettu, mutta arvioiden mukaan tuet vastaavat satoja miljardeja Yhdysvaltain dollareita (European Union Chamber of Commerce in China, 2017). Kiina pyrkii asetettuihin tavoitteisiin rajoittamalla ulkomaalaisten teollisuusalojen investointeja Kiinaan, samalla kannustaen kansallisia toimijoita globaalin laajenemiseen. Konseptin mukaiset teollisuudenalat on esitetty kuviossa 3.



KUVIO 3 ”Made in China 2025”-konseptin mukaiset teollisuudenalat (Ruiq, 2015), sekä ”China Standards 2035”-strategian mukaisten SEP -patenttien määrä (Buchholz, 2021).

Kiina on julkaissut vuonna 2020 ”*China Standards 2035*” -strategian (myöhemmin CS 2035), jonka tavoitteena on määrittää globaalit standardit seuraavan sukupolven teknologioille, kuten esineiden internetille (myöhemmin IoT), tekoälylle, pilvilaskennalle sekä 5G- tekniikalle (Wu, 2022). Standardeilla on arvioitu olevan laaja-alaisia vaikutuksia muun muassa tietoliikenneverkkojen ja -laitteistojen käyttöön, sillä standardien mukaisten patenttien on arvioitu luovan teknologista riippuvuutta kiinalaisten teknologiayritysten patenteista (Kharpal, 2020). Standardien avulla Kiinan arvioidaan pyrkivän edistämään kiinalaisten teknologiayhtiöiden protokolliin ja teknisiin spesifikaatioihin perustuvia patentteja, jotka mahdollistavat teknologian yhteistoimivuuden. Etenkin tieto- ja viestintäjärjestelmät sekä televerkot koostuvat SEP-patentoiduista innovaatioista, (engl. Standard-Essential Patents), jotka ovat välttämättömiä standardin täytäntöönpanon kannalta (Euroopan komissio, ei pvm). Kiinalainen verkkolaitevalmistaja Huawei Technologies Co., Ltd (myöhemmin Huawei) onkin jättänyt vuoteen 2022 mennessä yli 13000 5G-teknologiaan liitettyä patenttia, mikä oli eniten kaikista 5G-teknologiayrityksistä vuonna 2020 (GreyB, 2020). Dell’Oron vuoden 2021 raportin mukaan Huawei oli globaalisti suosituin verkkolaitevalmistaja (Pongratz, 2022). Huomionarvoista kuitenkin on, että 26 prosenttia myynnistä kohdistui Kiinaan. Dell’Oron raportin mukainen verkkolaitteiden globaali jakautuminen on esitetty kuviossa 4.



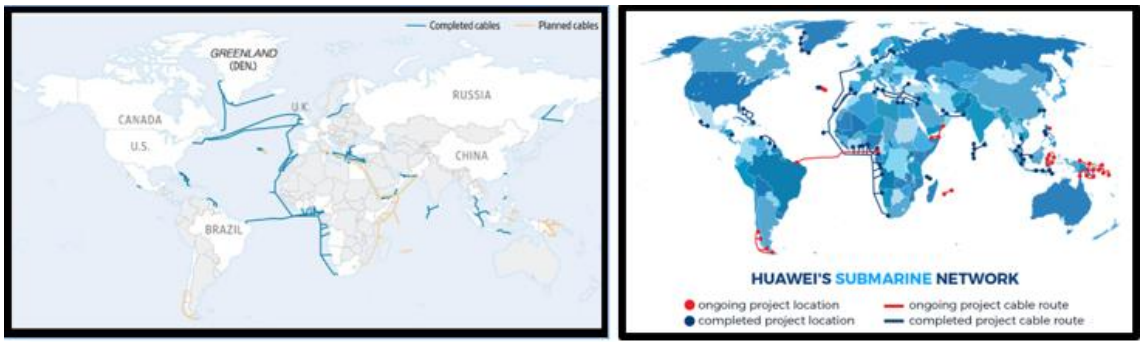
KUVIO 4 Verkkolaitteiden globaali jakautuminen (S. Pongratz, 2022).

Kiinan kansallisten teollisuusalojen ja Huawein kaltaisten teknologiayhtiöiden levittäytyminen maailmalle voidaan nähdä olevan osa digitaalisen silkkitien kehitystä. Puhuttaessa silkkitiestä on syytä avata myös sen historiallista taustaa. Yleinen käsitys silkkitiestä on, että se yhdisti maantieteellisesti kauppareittinä Kiinan ja Euroopan. Usein unohdetaan, että silkkitie ei varsinaisesti ollut vain yksi tie, vaan se muodostui tieverkostojen kokonaisuudesta (Similä, 2020). Silkkitien fundamentaalinen idea on todennäköisesti edelleen säilynyt, Kiinan pyrkiessä hyötymään vähintäänkin taloudellisesti Euroopasta. Digitalisoituneen yhteiskunnan johdosta kehittyneet valtiot ovat riippuvaisia sähköstä ja tietoliikenneyhteyksistä, sekä näihin liittyvästä infrastruktuurista. Ei ole siis mikään ihme, että Kiina on rakentamassa digitaalista silkkitietä 2020-luvulla, minkä tavoitteena on maa- ja meritieyhteyksien lisäksi kehittää myös verkkoliikenneyhteyksiä (Lyytikkä ym., 2018).

Huawei on tiedotteissaan ilmoittanut sitoutuvansa Euroopan digitaalisen infrastruktuurin kehittämiseen, missä sen myötävaikutus korostuu laitteistojen, pilvipalveluiden, tekoälyn ja ohjelmistojen ekosysteemien kehittämisessä (Wang, 2021). Tekoälyn ja IoT-laitteiden on arvioitu rakentuvan 5G-verkkojen ympärille, missä Huaweilla on globaali dominanssi. Suomalainen Nokia ja ruotsalainen Ericsson ovat toistaiseksi ainoat eikiinalaiset kilpailukykyiset vaihtoehdot 5G-teknologialle, mutta niiden tuotteet ovat keskimäärin kalliimpia (Ceci et al., 2022). Lisäksi Kiinan valtion on arvioitu tukevan halvan hinnoittelun tuomaa kilpailuetua MIC 2025 -konseptin mukaisesti, sillä Huawein on todettu vastaanottaneen jo vuonna 2015 yli 100 miljardin dollarin tukipaketin Kiinan valtiolta (FBI, 2015). Huawei kiistää Kiinan valtion rahallisen tuen, ilmoittaen valtion osuuden olleen vuosien 2009 ja 2018 välillä 0,3 prosenttia yrityksen kokonaismyynnistä (Song, ei pvm.).

Koska tietoliikenne on keskittynyt pitkälti kiinteisiin, mannertenvälisiin valokuitukaapeleihin, on Kiinan mukana myös vedenalaisten tietoliikennekaapeleiden rakentajana osana digitaalista silkkitien infrastruktuuria (Griffiths, 2019). Huawei Marine Networks Co. (nykyinen HMN Tech, 2020) onkin rakentanut tai korjannut noin neljänneksen maailman merenalaisista kaapeleista (Zhou, 2021). Konsernin laskemat ja laskettavaksi suunnitellut tietoliikennekaapelit on esitetty kuviossa 5. Huomionarvoista kuitenkin on, että Atlantin valtameren ylittävien tietoliikennekaapelien ilmoitettu omistaja

vaihtelee lähteestä riippuen (Page & Taylor, 2019; Gill, 2020). Vuonna 2021 kolme Kiinan valtionomisteista tietoliikennekonsernia, China Mobile, China Telecom ja China Unicom rahoittivat 31:n vedenalaisen tietoliikennekaapeliin laskun ja asennuksen. Kaapelit laskettiin kaukana Kiinan lähialueelta, minkä voidaan nähdä olevan osa Kiinan BRI-ohjelmaa (Sherman, 2021; kts. TeleGeography). Kiinan kommunistisen puolueen edustajan ilmoitetaan myös sanoneen, kuinka vedenalaisten tietoliikennekaapelien laskeminen mahdollistaa taloudellisen hyödyn lisäksi informaation keräämisen (Federal Communications Commission, 2021).



KUVIO 5 Huawei Marine Netwosk Co. (nykyinen HMN Tech) laskemat ja laskettavaksi suunnitellut merenalaiset tietoliikennekaapelit. Atlantin valtameren alittavien tietoliikennekaapelien ilmoitettu omistaja vaihtelee lähteestä riippuen (Page & Taylor, 2019; Gill, 2020).

3.2 Teknologiakonsernien mahdollisuudet verkkovakoilussa

Länsimaiseen ajattelumaailmaan ja ideologiaan kuuluu tiiviisti ihmisten perusoikeuksien turvaaminen ja valvominen lainsäädännön kautta. Kiinassa länsimaista ajattelumallia ja ihmisten perusoikeuksia ylläpitävää ajattelumallia tukevat henkilöt luokitellaan valtiovallan vastustajiksi, joita myös kohdellaan sen mukaisesti (Bell, 2018). Kiinan lainsäädäntö onkin säädetty tukemaan vallassa olevien vallan lisäämistä ja mahdollisten vastustajien puhdistamista (Puranen, 2022). Kiinan valtiolla on myös erittäin velvoittava lainsäädäntö, joka velvoittaa kansalaiset avustamaan turvallisuus- ja tiedustelupalveluita. Useat länsimaiset tiedustelupalvelut ovat varoittaneet teknologiayrityksiä Kiinan muodostamasta riskistä, mistä myös Suojelupoliisi on varoittanut kansallisen turvallisuuden katsauksessaan (SUPO, 2022c). Katsauksessa Suojelupoliisi on korostanut muun muassa kiinalaisen informaatioteknologian käyttöperiaatteita sekä Kiinan vuonna 2017 voimaantullutta kansallista tiedustelulakia (engl. National Intelligence Law). Kiinan kansallisen tiedustelulain seitsemäs artikla velvoittaa kaikkia kiinalaisia yhtiöitä avustamaan Kiinan turvallisuusviranomaisia tiedustelun suorittamisessa (SUPO, 2022c; CNPCN, 2017).

Lisäksi tiedustelulain 17. artikla pidättää turvallisuusviranomaisille oikeuden kerätä ja vastaanottaa tietoa kansallisten organisaatioiden ja hallinnonalojen tietojärjestelmistä (Kharpal, 2019; CNPCN, 2017). Kansallisen tiedustelulain lisäksi Kiinassa on säädetty muitakin lakeja, joiden voidaan nähdä tukevan Kiinan strategista toimintaa tietoverkoissa. Vuonna 2016 säädetty laki kyberturvallisuudesta (engl. Chinese Cybersecurity Law) velvoittaa 28. artiklassa verkko-operaattoreita antamaan teknistä tukea Kiinan turvallisuusviranomaisille kansallisen turvallisuuden nimissä (Stanford Cyber Policy Center,

2018). Vuoden 2015 kansallisen turvallisuuden lain 77. artikla (engl. National Security Law) velvoittaa vastaavasti kaikkia organisaatioita ja yksilöitä osoittamaan pyydettäessä tukea Kiinan turvallisuusviranomaisille rangaistuksen uhalla (China Law Translate, 2015). Vuoden 2014 vastavakoilulain (engl. Counterespionage Law) 22. artikla velvoittaa kiinalaisia organisaatioita ja yksilöitä raportoimaan totuudenmukaisesti kaikki vastatiedusteluun liittyvät asiakokonaisuudet rangaistuksen uhalla (Law Info China, 2014; Reuters Staff, 2014). Esitetyt lait eivät sisällä maantieteellisiä rajoituksia, ja ne edellyttävät kaikkia maan organisaatioita ja kansalaisia noudattamaan Kiinan turvallisuusviranomaisten pyyntöjä. Kiinan on arvioitu kykenevän käyttämään kansallisia lakejaan kiinalaisten verkkolaitevalmistajien painostamisessa (Walton, 2022; Sacks, 2021).

Kiinalaisilla teknologiakonserneilla on laaja-alainen tarjonta laitteistoista, palveluista ja komponenteista liittyen tietojärjestelmiin, tietoliikenteeseen ja kommunikaatioinfrastruktuuriin (Aaltonen, 2022). Muun muassa Yhdysvallat (Shepardson, 2022), Japani (Denyer, 2018) ja Australia (Huawei, ei pvm.) ovat kokonaisuudessaan kieltäneet kiinalaisen Huawein järjestelmien ja verkkolaitteiden käytön yhteiskunnallisesti kriittisissä tietoverkoissa sekä seuraavan sukupolven 5G-verkkoinfrastuktuurissa. Myös Ruotsin puolustusvoimat ja turvallisuuspoliisi Säpö (ruots. Säkerhetspolisen) ovat arvioineet, että Kiinan valtio ja tiedustelupalvelut voisivat painostaa kiinalaisia yhtiöitä, minkä myötä Ruotsi on ilmoittanut Huawein käyttökiellosta 5G-verkoissa (SVT, 2022). Suomi ei ole kieltänyt laitteiden käyttöä, mutta useat verkko-operaattorit ovat pyrkineet itsenäisesti poistamaan Huawein tuotteita infrastruktuuristaan, korvaten ne suomalaisen Nokian tai ruotsalaisen Ericssonin teknologialla (Hallonblad, 2022). Toistaiseksi Suomessa on kuitenkin osittain käytössä Huawein 5G-teknologiaa Elisan ja DNA:n verkoissa (Pölönen, 2022).

Myös Saksa on arvioinut uudelleen epäluotettavina pidettyjen toimijoiden komponentteja, mutta päätöksiä asian suhteen ei ole toistaiseksi tehty (Kukkonen, 2022). Unkarissa Huaweihin suhtaudutaan kuitenkin vastaanottavasti, sillä maa toivottaa Kiinan tervetulleeksi kauppakumppanina ja sijoittajana pyrkien kahdenvälisten suhteiden kehittämiseen kaikin mahdollisin tavoin (Barabàs, 2022). Huawei hallitsee myös Afrikan tietoliikenneinfrastruktuuria, toimittamalla 70 % mantereen 4G-verkoista, ja tulevaisuudessa myös 5G-verkkoja (Kidera, 2020; Ehl, 2022). Länsimainen lobbaus Huawein sulkemisesta markkinoilta on kuitenkin vaikuttanut yrityksen maailmanlaajuiseen myyntiin kriittisesti, supistaen vuonna 2021 yrityksen liikevaihtoa 30 prosentilla (Yu & Munroe, 2021).

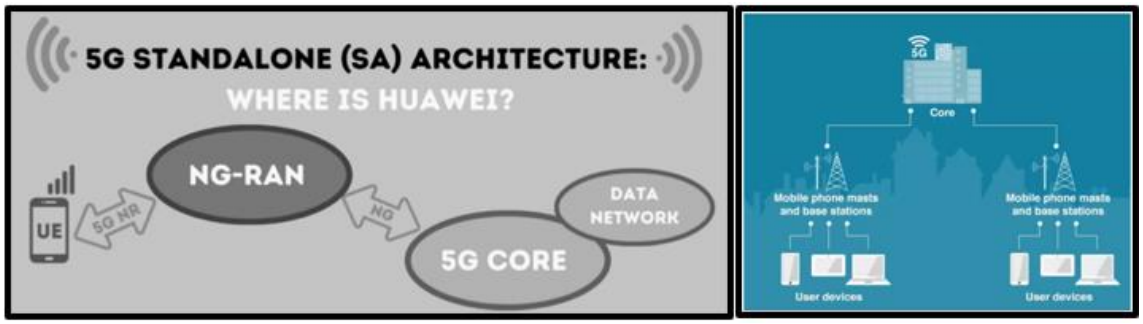
Kiinalainen sosiaalisen median palvelu TikTok on myös ajautunut Yhdysvaltojen kriittisen tarkastelun kohteeksi, sillä sovelluksen kehittäjää ByteDancea on epäilty käyttäjien vakoilusta ja yksityisyydensuojan rikkomisesta. Sovelluksen kerrotaan mahdollistaneen käyttäjien näytöille syötetyn tekstin seuraamisen ja tallentamisen (Krause, 2022). Tämän lisäksi applikaatiota on arvioitu käytettävän yhdysvaltalaisten käyttäjien päätelaitteiden seuraamiseen (Baker-White, 2022).

3.3 Kommunikaatioinfrastruktuurin hyödyntäminen verkkovakoilussa

Kommunikaatioinfrastruktuuri voidaan määritellä verkostoksi, joka muodostuu järjestelmistä, palveluista ja laitteistoista, joita kriittisen infrastruktuurin toimijat ja palvelut tarvitsevat toimintaansa ja palveluiden ylläpitämiseksi. Kommunikaatioinfrastruktuurin ja yhteiskunnan toiminnan kannalta kriittiseksi muodostuvat tietoliikenteen toimivuus

ja siinä liikkuvan tiedon luottamuksellisuus (Longbottom, 2020). Kiina on BRI-ohjelman mukaisesti pyrkinyt järjestelmällisesti rakentamaan globaalia kommunikaatioinfrastruktuuria osana sen digitaalista silkkitietä (Umbach, 2022). Herääkin kysymys siitä, miten Kiina voisi todellisuudessa hyödyntää sen maailmanlaajuista tietoliikenneverkostoaan?

Tietoverkkolaitteiden hyväksikäytön mahdollisuudet voidaan nähdä koostuvan kahdesta menetelmästä (Lewis, 2019). Ensimmäiseksi, useat verkkolaitteet käyttävät julkista internetiä muodostaakseen yhteyden valmistajan palvelimelle, jonka kautta laitteet suorittavat ohjelmistopäivityksiä tai raportoivat vikatilanteista. Teknisesti valmistajan olisikin mahdollista asentaa takaovia tai kerätä arkaluontoista aineistoa käyttäjän huomaamatta (Lewis, 2019). Toiseksi verkkolaitevalmistajan monopoliasemalla kyettäisiin luomaan riippuvuus Kiinan valmistamista tietoverkkolaitteista, jotka implementoidaan osaksi kriittistä infrastruktuuria (Lewis, 2019). Huawein monopoliasema 5G-arkkitehtuurirakenteessa kyettäisiin luomaan useassa portaassa, sillä konserni tuottaa päätelaitteita yksittäisille käyttäjille, antenneja ja vastaanottimia liityntäverkkojen tukiasemille, sekä reitittimiä ja muuta teknologiaa 5G-teknologian ydinverkkoon. Ydinverkko on 5G-verkkoinfrastruktuurin kokonaisuus, joka yhdistää valtiot, maanosat ja eri operaattoreiden verkot. Huawein mahdollinen monopoliasema 5G-verkkoinfrastruktuurissa on esitetty kuviossa 6. Kiina toimiikin Afrikassa keskimäärin joka viidennessä infrastruktuurin kehittämisprojektissa rahoittajana (Tikka, 2021), minkä myötä sen toimintaa on verrattu Troijan puuhevoseen, millä houkutellaan uhri vapaaehtoisesti päästämään vihollinen infrastruktuurinsa sisään (Chatzky et al., 2020). Kommunikaatioinfrastruktuurissa korostuukin hajauttaminen, millä vähennetään riippuvuutta yhdestä laitetoimittajasta, ja sen kautta tietoverkkoyhtiöiden monopoliasemasta.



KUVIO 6 Huawein 5G-arkkitehtuuri perustuu päätelaitteisiin, liityntä- ja siirtoverkojen tukiasemiin, sekä 5G:n ydinverkkoon (Ceci et al., 2022; Kelion, 2020)

Kommunikaatioinfrastruktuurin näkökulmasta Kiinan globaalilla levittäytymisellä voitaisiin nähdä olevan kyse valtion suurvaltapolitiikasta, jossa se pyrkii halvan 5G-teknologian avulla luomaan niin sanottua ”emergenttiä ehdollistamista” (Mattlin & Nojonen, 2015), jossa valtiot joutuisivat riippuvuussuhteeseen kiinalaisesta teknologiasta, mahdollistaen kiinalaisen monopoliaseman valtioiden kommunikaatioinfrastruktuurissa (Vuori, 2022). Tietoliikenteen näkökulmasta vaikutukset konkretisoituisivat tietoverkoissa ja informaatioympäristössä. Tietoverkkojen osalta on tarkasteltava mihin verkkoihin komponentit on implementoitu sekä informaation osalta laitteistojen mahdollisesti keräämän tiedon luottamuksellisuus (Schia et al., 2019). Kiinan kansallisten tiedustelulakien tulkinnan tuloksena on ilmeistä, että Huawei on velvoitettu pyynnöstä

luovuttamaan kerättyä tietoa Kiinan turvallisuusviranomaisille. Vaikka Huawei kiistää kaikenlaisen tiedonvaihdon Kiinan valtion kanssa (Huawei, ei pvm.), on vaikea kuvitella, että globaali supervalta ei käyttäisi tarvittaessa mahdollisuutta hyödyntää sen kansallisia lakeja. Voidaan todeta, että Kiina on tuotteistanut palvelunsa strategisesti, mahdollistaen kokonaisvaltaisen infrastruktuurin tarjoamisen palveluna.

Kommunikaatioinfrastruktuurin mukaisesta tietoverkkovakoilusta on olemassa myös referenssitapauksia. Edward Snowdenin paljastusten myötä kävi ilmi, että Yhdysvaltojen kansallinen turvallisuusvirasto NSA (engl. National Security Agency) suoritti tietoverkkovakoilua yhdysvaltalaisen tietoverkkoyhtiö Ciscon reitittimien ja palvelimien avulla (Menn, 2017; Santos, 2016). Cisco on kiistänyt osallisuutensa tapahtuneeseen, mutta tapaus voidaan nähdä esimerkkinä siitä, kuinka globaali suurvalta saattaa asettaa kansallisen turvallisuuden yksittäisten toimijoiden edelle ilman niiden tietoa. Snowden nosti myös esille TEMPORA-ohjelman, jossa yli 200 transatlanttista tietoliikennekaapelia kuuntelemalla kyettiin keräämään dataa tiedustelun tueksi (Anderson, 2020).

Myös Huawein suorittamasta verkkovakoilusta on jo viitteitä, sillä konserni oli osallisena vuonna 2018 ilmenneessä vakoilutapauksessa, jossa Afrikan unionin päämajan palvelimilta lähetettiin viiden vuoden ajan joka yö aineistoa Kiinan Shanghaissa sijaitsevalle palvelimelle (Vaswani, 2019). Päämajan tieto- ja viestintäjärjestelmät oli toimittanut Huawei. Tapaukset ovatkin esimerkkejä siitä, kuinka valtiot eivät voi ikinä täysin luottaa kommunikaatioinfrastruktuurissaan oleviin toisen valtion tuottamiin laitteistoihin.

4 Johtopäätökset

Kiina on matkalla maailman toiseksi supervallaksi Yhdysvaltojen rinnalle ja se on valjastanut kansakunnan laajat resurssit käyttöönsä tämän tavoitteen saavuttamiseksi. Kiinan kommunistinen puolue on tosiasiallinen vallankäyttäjä Kiinassa ja sen keskeinen turvallisuushuoli on oman legitimiteettinsä säilyttäminen. Saavuttaakseen tavoittelemansa asemansa ja pysyäkseen vallassa, Kiinan kommunistinen puolue tarvitsee tietoa sen vastustajaksi katsomistaan valtioista, suuryrityksistä, toisinajattelijoista, poliittisista toimijoista – ja jopa omista kansalaisistaan. Tiedustelu ja sen tuottama tieto Kiinan päättäjille on kommunistisen puolueen elinehto. Kiinan keskusjohtoinen poliittinen järjestelmä mahdollistaa myös laaja-alaisen ja pitkäjänteisesti tapahtuvan strategisen kehittämisen. Myös länsimaista poikkeavat käsitykset yksilönvapaudesta ja -oikeuksista madaltavat rimaa toteuttaa laajamittaista valvontaa ja vakoilua.

Tässä raportissa on kuvattu Kiinan tietoverkkojen avulla toteuttamaa tiedon hankintaa ja vakoilua sekä käsitelty miten Kiinan strategiset tavoitteet, teknologia ja kybervakoilu ovat kytkeytyneet toisiinsa. Raportissa on käsitelty kyberoperaatioita toteuttavia APT-ryhmiä ja niiden kytkeytymistä Kiinan valtioon sekä Kiinan asevoimien organisoitumista kybertoimintojen osalta. On ilmeistä, että kiinalaisia APT-ryhmiä ja Kiinan asevoimien suorittamia kyberoperaatioita ei voi erottaa täysin toisistaan, vaan toimintaa olisi hyvä tarkastella kokonaisuutena. Kiinan verkkovakoilun tavoitteena on pyrkiä pitkäaikaiseen läsnäoloon kohteen tietoverkoissa ja toiminnan salaamisen. Toiminta on myös sekä teknisesti että toimintatavoiltaan edistynyttä. Kiinan suorittama verkkovakoilu on globaalia, vaikka julkitulleissa esimerkeissä korostuvat länsimaihin kohdistuneet tapaukset.

Kiina pyrkii laajentamaan läsnäoloaan ja vaikutusvaltaansa rajojensa ulkopuolelle investoimalla niin länsimaihin kuin kehittyviin talouksiin. Lisäksi Kiina ja kiinalaiset yritykset investoivat paljon eri toimialojen teknologian kehitykseen. Tietoverkkoteknologian tutkimus ja tuotekehitys on ollut yksi Kiinan painopisteistä, ja Kiina onkin noussut uusien patenttien määrällä mitattuna maailman johtavaksi toimijaksi esimerkiksi 5G-verkkoihin liittyvissä innovaatiossa. Kuten raportissa todetaan, ovat länsimaat heränneet moniulotteiseen riippuvuuteen Kiinasta, minkä vuoksi kiinalaisilla teknologiatoimittajilla on ollut haasteita saada erityisesti tietoverkkotuotteitansa käyttöön useissa läntisissä maissa.

Kiinan käytössä olevat resurssit, keskusjohtoinen poliittinen järjestelmä, strateginen päättäväisyys ja pitkäjänteisyys tekevät siitä verkkotiedustelun suurvallan. Kiina-riippuvuudesta on Ukrainan sodan laajentumisen myötä käyty yhä enemmän julkista keskustelua. Keskustelu on painottunut taloudelliseen riippuvuuteen ja sen vaikutuksiin maiden turvallisuuteen. Samaan keskusteluun olisi hyvä liittää myös Kiinan intressit verkkovakoilussa.

Lähteet

Aaltonen, J. (2022). Olemmeko liian riippuvaisia Kiinasta? Helsingin Sanomat. Haettu 13.11.2022 osoitteesta: https://www.hs.fi/politiikka/art-2000008958596.html

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition. Wiley. ISBN: 978-1-119-64281-7

Baker-White, E. (2022). TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens. Forbes. Haettu 14.11.2022 osoitteesta: https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=388e5c9b6c2d

Baràbas, B. (2022). Free to do Business in Hungary, Huawei Looks for More Speed, Less Energy. Budapest Business Journal. Haettu 7.11.2022 osoitteesta: https://bbj.hu/business/tech/telco/free-to-do-business-in-hungary-huawei-looks-for-more-speed-less-energy

Bell, D (2018). China's political meritocracy versus Western democracy. Economist. Haettu 9.11.2022 osoitteesta: https://www.economist.com/open-future/2018/06/12/chinas-political-meritocracy-versus-western-democracy

Blenkinsop, P (2022). EU seeks united front on China reliance as Germany plans trip. Reuters. Haettu 13.11.2022 osoitteesta: https://www.reuters.com/world/eu-leaders-seek-united-front-china-dependency-2022-10-21/

Buchholz, K. (2021). Who Is Leading the 5G Patent Race?. Statista. Haettu 7.11.2022 osoitteesta: https://www.statista.com/chart/20095/companies-with-most-5g-patent-families-and-patent-families-applications/

Calder, W. (2020). China Will Use Huawei to Spy Because So Would You. Foreign Policy. Haettu 3.11.2022 osoitteesta: https://foreignpolicy.com/2020/07/14/britain-boris-johnson-china-will-use-huawei-to-spy-because-so-would-you/

Cambell, C. (2021). China's People's Liberation Army: Restructuring and Modernization.

Congressional Research Service. Haettu 3.11.2022 osoitteesta: https://crsreports.congress.gov/product/pdf/R/R46808

Chatzky, A & McBride, J. China's Massive Belt and Road Initiative. Council on foreign relations. CFR. Haettu 10.11.2022 osoitteesta: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Checkpoint (2022). Twisted Panda: Chinese APT espionage operation against Russian state-owned defense institutes. CheckPoint Research. Haettu 14.11.2022 osoitteesta: https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/

China Law Translate (2015). National Security Law of the People's Republic of China. Haettu 3.11.2022 osoitteesta: https://www.chinalawtranslate.com/en/2015nsl/

Chrill, G. (2020). Huawei submarine cable unit changes name, identity. Asia Financial. Haettu 19.11.2022 osoitteesta: https://www.asiafinancial.com/huawei-submarine-cable-unit-changes-name-identity

CNPCN; Chinese National People's Congress Network (2017). National Intelligence Law of the People's Republic. Haettu 2.11.2022 osoitteesta: https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

Cordesman, A. H. (2021). Chinese Strategy and Military Forces in 2021. Center for Strategic & International Studies. Haettu 10.11.2022 osoitteesta: https://www.csis.org/analysis/updated-report-chinese-strategy-and-military-forces-2021

Costello, J. & McReynolds, J.(2018). China's Strategic Support Force: A Force for a New Era. Center for the Study of Chinese Military Affairs. Institute for National Strategic Studies. National Defense University

Denyer, S. (2018). Japan effectively bans China's Huawei and ZTE from government contracts, joining U.S.. The Washington Post. Haettu 5.11.2022 osoitteesta: https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html

Ehl D. (2022). Africa embraces Huawei tech despite security concerns. DW News. Haettu 7.11.2022 osoitteesta: https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700

ENISA (2020). ENISA threat landscape 2020 - cyber espionage. European Union Agency for Network and Information Security. Haettu 14.11.2022 osoitteesta: https://www.enisa.europa.eu/publications/enisa-threatlandscape-2020-cyber-espionage

Euroopan komissio (ei pvm). Standard Essential Patents. Euroopan Unioni. Haettu 4.11.2022 osoitteesta: https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/patent-protection-eu/standard-essential-patents_en

European Union Agency for Network and Information Security. Haettu 14.11.2022

osoitteesta: https://www.enisa.europa.eu/publications/enisa-threatlandscape-2020-cyber-espionage

European Union Chamber of Commerce in China, 2017. China manufacturing 2025: Putting Industrial Policy Ahead of Market Forces. Haettu 9.11.2022 osoitteesta: http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf

FBI; Federal Bureau of Investigation (2015). Counterintelligence Strategic Partnership Intelligence Note (Spin) 15-002. Haettu 11.12.2022 osoitteesta: https://info.publicintelligence.net/FBI-SPIN-ProtectingAcademicResearch.pdf

FBI; Federal Bureau of Investigation (2019). China Cyber Thread: Chinese Military Hackers. Federal Bureau of Investgation. Haettu 12.11.2022 osoittesta: https://www.fbi.gov/file-repository/china-case-example-military-hackers-2019.pdf

Federal Communications Commission (2021). Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership. Washington D.C. Haettu 13.11.2022 osoitteesta: https://docs.fcc.gov/public/attachments/FCC-20-133A1.docx

Girard, B. (29. 10 2019). The Real Danger. The Diplomat. Haettu 10.11.2022 osoitteesta: https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/of China's National Intelligence Law:

GreyB (2020). Huawei Holds Maximum Number of 5G Patents. Haettu 4.11.2022 osoitteesta: https://insights.greyb.com/company-with-most-5g-patents/

Griffiths, J (2019). The global internet is powered by vast undersea cables. But they're vulnerable. CNN. Haettu 9.11.2022 osoitteesta: https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html

Grimes, R (2021) Why Isn't the Internet More Secure? Linkedin. Haettu 9.11.2022 osoitteesta: https://www.linkedin.com/pulse/why-isnt-internet-more-secure-roger-grimes

Hakonen, K (2021) Sotilastiedustelun tiedustelulajit sekä siviili- ja sotilastiedustelun tiedustelumenetelmät. Tiedusteluvalvonta. Haettu 12.11.2022 osoitteesta: https://tiedusteluvalvonta.fi/-/sotilastiedustelun-tiedustelulajit-seka-siviili-ja-sotilastiedustelun-tiedustelumenetelmat

Hakonen, K. (2021). Sotilastiedustelun tiedustelulajit sekä siviili- ja soti-lastiedustelun tiedustelumenetelmät. Tiedusteluvalvontavaltuutettu. Haettu 14.11.2022 osoitteesta: https://tiedusteluvalvonta.fi/-/sotilastiedustelun-tiedustelulajit-seka-siviili-ja-sotilastiedustelun-tiedustelumenetelmat

Hallamaa, T (2018). Analyysi: Valtio ohjailee kiinalaishakkereita ja nyt länsimaatkin sanovat sen ääneen. YLE. Haettu 4.11.2022 osoitteesta: https://yle.fi/uutiset/3-10567285

Hallonblad, A. (2022). Huawein 5g-tekniikka pysyy pannassa Ruotsissa. Helsingin Sanomat. Haettu 6.11.2022 osoitteesta: https://www.hs.fi/talous/art-2000008903294.html

Hallonblad, A. (2022). Huawein 5g-tekniikka pysyy pannassa Ruotsissa. Helsingin Sanomat. Haettu 6.11.2022 osoitteesta: https://www.hs.fi/talous/art-2000008903294.html

Halminen, L. (2021). Supoa on sanottu koiraksi, joka ei hauku, mutta Kiinan vakoilusta se osasi älähtää omalla verhotulla tavallaan. Helsingin Sanomat. Haettu 14.11.2022 osoitteesta: https://www.hs.fi/ulkomaat/art-2000007871527.html

Hellgren, R, Jääskeläinen V, Ruutiniemi L, Tuomela E (2021). Valtiollinen tiedustelu osana Kiinan nousua ja valtapyrkimyksiä. Tiedustelun maailma: Tiedusteluanalyysi I-kurssin. Jyväskylän yliopisto.

Hemmilä, I (2022). Tutkija varoittaa nyt Kiina-riskeistä, jotka ovat ”valtavan paljon suurempia” kuin Venäjä-riskit. Iltasanomat. Haettu 12.11.2022 osoitteesta: https://www.is.fi/taloussanomat/art-2000008964616.html

Huawei (ei pvm). Does China’s National Intelligence Law compel Huawei to plant so-called “backdoors” in telecommunications infrastructure?. Haettu 7.11.2022 osoitteesta: https://www.huawei.com/en/facts/question-answer/hw-cooperate-with-chinas-intelligence-community-how-can-we-trust-you

Huawei (ei pvm). What is Huawei’s response to Australia’s ban on Huawei 5G network equipment?. Huawei. Haettu 5.11.2022 osoitteesta: https://www.huawei.com/en/facts/question-answer/whats-huaweis-response-to-australia-ban-hauwei-5g-network

Itkin, E. & Cohen I. (2021). The Story of Jian – How APT31 Stole and Used an Unknown Equation Group 0-Day. Check Point Software Technologies. Haettu 14.11.2022 osoitteesta: https://research.checkpoint.com/2021/the-story-of-jian/

Johansson, M. (2021). Venäjän ja Kiinan sotilastiedusteluorganisaatioiden kybermenetelmien kehitys vuosina 2004-2021. Jyväskylän yliopisto, Informaatioteknologian tiedekunta.

Kelion, L. (2020). Huawei: What is 5G's core and why protect it?. BBC News. Haettu 7.11.2022 osoitteesta: https://www.bbc.com/news/technology-51178376

Kemppi, J (2022). Asiantuntija: ”Suomen tulee varautua merkittävään kyberiskuun”. Iltalehti. Haettu 12.11.2022 osoitteesta: Tutkija varoittaa nyt Kiina-riskeistä, jotka ovat ”valtavan paljon suurempia” kuin Venäjä-riskit - Taloussanomat - Ilta-Sanomat

Kharpal, A. (2019). Huawei says it would never hand data to China’s government. Experts say it wouldn’t have a choice. CNBC. Haettu 2.11.2022 osoitteesta https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

Kharpal, A. (2020) Chinese telecoms giant Huawei sues Verizon for patent infringement. CNBC. Haettu 4.11.2022 osoitteesta https://www.cnbc.com/2020/02/06/huawei-sues-verizon-for-patent-infringement.html

Kidera, M. (2020). Huawei's deep roots put Africa beyond reach of US crackdown. Nikkei Asia. Haettu 7.11.2022 osoitteesta: https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-deep-roots-put-Africa-beyond-reach-of-US-crackdown

Krause, F. (2022). TikTok monitoring all keyboard inputs and taps. ABC News. Haettu 14.11.2022 osoitteesta: https://www.abc.net.au/news/2022-08-23/tiktok-users-warned-of-potential-tracking-system/14029134

Kukkonen, L. (2022). Handelsblatt: Saksa pyrkii eroon ”epäluotettavista” toimijoista, kiinalaisen Huawein teknologia korvattaisiin mahdollisesti Nokian laitteistoilla. Helsingin Sanomat. Haettu 7.11.2022 osoitteesta: https://www.hs.fi/talous/art-2000008967079.html

Law Info China (2014). Counterespionage Law of the People's Republic of China. Haettu 3.11.2022 osoitteesta: http://www.lawinfochina.com/display.aspx?id=18033&lib=law

Lehto, M. (2022). Digitaalisen kybermaailman ilmiöitä ja määrittelyjä. V19.0. Informaatioteknologian Tiedekunta. Jyväskylän Yliopisto.

Lewis J. (2019). 5G: The Impact on National Security, Intellectual Property, and Competition. Statement before the Senate Committee on the Judiciary. Center for Strategic & International Studies. Washington D.C. Haettu 6.11.2022 osoitteesta: https://www.judiciary.senate.gov/imo/media/doc/Lewis%20Testimony1.pdf

Liang J., 2015. 'Made in China 2025' to focus on ten key sectors . People's Daily Online. 7.11.2022 osoitteesta: http://en.people.cn/n/2015/0522/c98649-8895998.html

Lowenthal, M. & Clark, R. M. (2016). The Five Disciplines of Intelligence. Thousand Oaks, California; CQ Press,

Lyytikkä, J. & Hallamaa,T. 2018. Kiina rakentaa verkkoa maailmalle – Googlen ex-toimitusjohtaja ennustaa, että Kiinan vaikutusvallan kasvu jakaa internetin kahtia. YLE. Haettu 10.11.2022 osoitteesta: https://yle.fi/uutiset/3-10442069

Manfra, J. (2019). Role of the United States Government in Securing the Nation’s Internet Architecture. Testimony. U.S. Department of Homeland Security. Washington, DC. Haettu 10.11.2022 osoitteesta: https://www.govinfo.gov/content/pkg/CHRG-116hhrg40505/html/CHRG-116hhrg40505.htm

Mattis, P. & Brazil, M. (2019). Chinese Communist Espionage: An Intelligence Primer. Naval Institute Press.

Mattlin. M & Nojonen ,M. (2015) Conditionality and Path Dependence in Chinese Lending, Journal of Contemporary China, 24:94, 701-720, DOI: 10.1080/10670564.2014.978154

McBride J. and Chatzky A. (2019). Is ‘Made in China 2025’ a Threat to Global Trade?. Council on Foreign Relations. Haettu 6.11.2022 osoitteesta: https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

Menn, J.(2017). A scramble at Cisco exposes uncomfortable truths about U.S. cyber defense. Reuters. Haettu 5.11.2022 osoitteesta: https://www.reuters.com/article/us-usa-cyber-defense-idUSKBN17013U

Michael V. Ceci & Lawrence Rubin (2022). China’s 5G networks: A Tool For Advancing Digital Authoritarianism Abroad. Foreign Policy Research Institute. Elsevier Ltd.

Microsegur. (6.11.2022) Network Infrastructure. Microsegur. Haettu 9.11.2022

osoitteesta: https://microsegur.com/en/what-is-network-infrastructure/

Mills, R (2019). Stop feeding the Chinese ‘Belt and Road’ trojan horse. Mining. Haettu 5.11.2022 osoitteesta: https://www.mining.com/web/stop-feeding-chinese-belt-road-trojan-horse/

Naski, M (2022). Mitä Kiina aikoo? Asiantuntija: Xi ajanut jo läpi "mahdottomia tehtäviä". Iltalehti. Haettu 5.11.2022 osoitteesta: https://www.iltalehti.fi/ulkomaat/a/88fd6265-a920-4be1-af95-df8684621ba7

NCSC; National Counterintelligence And Security Center (2018). Foreign Economic Espionage in Cyberspace. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

NSA, CISA & FBI. (2021). Chinese State-Sponsored Cyber Operations: Observed TTPs. Cybersecurity and Infrastructure Security Agency. Haettu 8.11.2022 osoitteesta: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200b

NSA; National Security Agency (2020). Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities. Cybersecurity and Infrastructure Security Agency. Haettu 8.11.2022 osoitteesta: https://www.cisa.gov/news-events/alerts/2020/10/20/nsa-releases-advisory-chinese-state-sponsored-actors-exploiting

OECD (2018). China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape. Haettu 14.11.2022 osoitteesta: https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf

Page, J. & Taylor, R.(2019). America’s Undersea Battle With China for Control of the Global Internet Grid. The Wall Street Journal. Haettu 13.11.2022 osoitteesta: https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466

Pongratz, S. (2022). Key Takeaways – 2021 Total Telecom Equipment Market. Dell’Oro Group. Haettu 3.11.2022 osoitteesta: https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market/

Portman, R. & Carper, T. (ei pvm). Threats to U.S. Networks: Oversight of Chinese Govermemnt-owned Carriers. Staff Report. United States Senate. Haettu 11.11.2022 osoitteesta: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf

Puolustusvoimat. (2021). Sotilastiedustelu - julkinen katsaus. Pääesikunta. Haettu 11.11.2022 osoitteesta: https://puolustusvoimat.fi/documents/1948673/74055459/PV_sotilastiedustelu_raportti_www_FI_2021.pdf/5a4aea51-64bc-f736-bc70-6b3e4815495c/PV_sotilastiedustelu_raportti_www_FI_2021.pdf?t=1620279050410

Puranen, M. (2022). Kiina, turvallisuus ja ihmiskunnan kohtalonyhteisö -yleisöluento. Jyväskylän Yliopiston yleistöluento. Haettu 10.11.2022 osoitteesta: https://www.jyu.fi/fi/ajankohtaista/arkisto/2022/10/kiina-turvallisuus-ja-

ihmiskunnan-kohtalonyhteiso-yleisoluento

Pölönen, R. (2022). Sodan usvaa; Sodankäynti muutoksessa. Toimittanut Marko Palokangas. Maanpuolustuskorkeakoulu. Sotataidon Laitos. Julkaisusarja 2: Tutkimusselosteita nro 18. ISBN 978-951-25-3286-5.

Rebello, J. (2019). Success of China's Belt & Road Initiative Depends on Deep Policy Reforms, Study Finds. Worldbank. Haettu 12.11.2022 osoitteesta: https://www.worldbank.org/en/news/press-release/2019/06/18/success-of-chinas-belt-road-initiative-depends-on-deep-policy-reforms-study-finds

Reuters Staff (2014). China passes counter-espionage law. Reuters. Haettu 2.11.2022 osoitteesta: https://www.reuters.com/article/us-china-lawmaking-spy-idUSKBN0IL2N520141101

Robertson, J & Riley, M (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg. Haettu 10.11.2022 osoitteesta: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?leadSource=uverify%20wall

Ruiq, Z. (2015). 'Made in China 2025' to focus on ten key sectors. People's Daily Online. Haettu 7.11.2022 osoitteesta: http://en.people.cn/n/2015/0522/c98649-8895998.html

Sacks D. (2021). China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond. Council on Foreign Relations. Haettu 3.11.2022 osoitteesta: https://www.cfr.org/blog/china-huawei-5g.

Santos, O. (2016). The Shadow Brokers EPICBANANA and EXTRABACON Exploits. Cisco Blogs. Haettu 7.11.2022 osoitteesta https://blogs.cisco.com/security/shadow-brokers

Schaer, C (2019). Security: Europe's pushback against Chinese tech has only just begun. ZDNET. Haettu 13.11.2022 osoitteesta: Security: Europe's pushback against Chinese tech has only just begun | ZDNET

Schia, N. & Gjesvik, L. & Friis, K. (2019). Critical Communication Infrastructure and Huawei. Norwegian Institute of International Affairs. SSRN Electronic Journal.

Security Sevice M15. (6.11.2022) Counter-Espionage. MI15. Haettu 7.11.2022 osoitteesta: https://www.mi5.gov.uk/counter-espionage

Shepardson D. (2022). U.S. FCC set to ban approvals of new Huawei, ZTE equipment - document. Reuters. Haettu 5.11.2022 osoitteesta: https://www.reuters.com/technology/us-fcc-set-ban-all-us-sales-huawei-zte-equipment-axios-2022-10-13/

Sherman, J. (2021). Beijing's Growing Influence on the Global Undersea Cable Network – Jamestown. Haettu 13.11.2022 osoitteesta: https://jamestown.org/program/beijings-growing-influence-on-the-global-undersea-cable-network/

Similä, V (2020). Tietä käyden tien on vanki. Mitä Marco Polon matkoista pitäisi tietää nyt, kun Kiina suunnittelee uutta Silkkitietä? Helsingin Sanomat. Haettu 11.11.2022 osoitteesta: https://dynamic.hs.fi/a/2020/marcopolo/

Sinhoe, D (2021) What is a submarine cable? Subsea fiber explained. Data Centry Dynamics. Haettu 10.11.2022 osoitteesta: https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/

Smith, H (2021) Kiinan aggressiivinen käytös herättää kysymyksiä – onko voimistuva ärhentely merkki mahtiuden puutteesta? MTV Uutiset. Haettu 9.11.2022 osoitteesta: https://www.mtvuutiset.fi/artikkeli/kiinan-agressiivinen-kaytos-herattaa-kysymyksia-onko-voimistuva-arhentely-merkki-mahtiuden-puutteesta/8096796#gs.hcm020

Song, K. (ei pvm). No, Huawei isn't built on Chinese state funding. Huawei. Haettu 3.11.2022 osoitteesta: https://www.huawei.com/en/facts/voices-of-huawei/no-huawei-isnt-built-on-chinese-state-funding

Stanford Cyber Policy Center (2018). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Standford University. Haettu 3.11.2022 osoitteesta: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Suojelupoliisi (2021a), Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. Suojelupoliisi. Haettu 14.11.2022 osoitteesta: https://supo.fi/-/ulkomaiset-tiedustelupalvelut-kayttavat-yritysten-ja-yksityishenkiloiden-verkkoreitittimia-kybervakoiluun

Suojelupoliisi (2021b), Suojelupoliisi tunnisti eduskuntaan kohdistuneen ky-bervakoiluoperaation APT31:ksi. Suojelupoliisi. Haettu 14.11.2022 osoitteesta: https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kyberva-koiluoperaation-apt31-ksi

Suojelupoliisi (2022c), Kansallisen turvallisuuden katsaus 2022; Tiedustelu ja vaikuttaminen. Haettu 2.11.2022 osoitteesta: https://supo.fi/tiedustelu-ja-vaikuttaminen

Suojelupoliisi (2022). Foreign intelligence and influence operations. Noudettu 7.11.2022 osoitteesta: https://supo.fi/en/intelligence-and-influence-operations

SUPO. (5. 11 2022). Foreign intelligence and influence operations. Noudettu

SVT Nyheter (2022). Domen: Huawei stoppas i Sverige. Haettu 6.11.2022 osoitteesta: https://www.svt.se/nyheter/ekonomi/huawei-stoppas-i-sverige.

Tarnoff, B (2016). How the internet was invented. The Guardian. Haettu 13.11.2022 osoitteesta: https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf

Tikka, J (2021). Kiinan Silkkitie on rakentanut miljarditeitä ja -siltoja ”ei minnekään. Verkkouutiset. Haettu 12.11.2022 osoitteesta: https://www.verkkouutiset.fi/a/kiinan-silkkitie-on-rakentanut-miljarditeita-ja-siltoja-ei-minnekaan/#78a7b8cb

Turunen, T (2021) Korkeakouluyhteistyö Kiinan kanssa – mahdollisuuksia ja uhkakuvia. Haettu 12.11.2022 osoitteesta: https://supo.fi/-/kolumni-korkeakouluyhteistyo-kiinan-kanssa-mahdollisuuksia-ja-uhkakuvia

Turunen, T. (2021). Kolumni: Korkeakouluyhteistyö Kiinan kanssa – mahdollisuuksia ja uhkakuvia. Suojelupoliisi. Haettu 14.11.2022 osoitteesta: https://supo.fi/-

/kolumni-korkeakouluyhteistyo-kiinan-kanssa-mahdollisuuksia-ja-uhkakuvia

U.S. Chamber of Commerce, 2017. Made in China 2025: Global Ambitions Built on Local Protections. https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf

Umbach, F (2022). Future of China's Belt and Road Initiative. Gisreportsonline. Haettu 4.11.2022 osoitteesta: https://www.gisreportsonline.com/r/belt-road-initiative/

Vaswani, K. (2019). Huawei: The story of a controversial company. BBC News. Haettu 7.11.2022 osoitteesta: https://www.bbc.co.uk/news/resources/idt-sh/Huawei

Vuori, J. (2022). A-Talk: Voiko länsi päästä irti riippuvuudestaan Kiinaan?. A-Studio. Yle Areena. Haettu 3.11.2022 osoitteesta: https://areena.yle.fi/1-50949910

Wang, D. (2021). Huawei: Collaborating on Digital Infrastructure Innovation for an Intelligent World 2030. Huawei. Haettu 3.11.2022 osoitteesta: https://www.huawei.com/en/news/2021/10/eco-connect-europe-2021-david-wang

Wu, Y. (2022). China Standards 2035 Strategy: Recent Developments and Implications for Foreign Companies. Dezan Shira & Associates. Haettu 5.11.2022 osoitteesta: https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/

Wuthnow, J. & Saunders, P. C. (2017). Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications. Center for the Study of Chinese Military Affairs. Institute for National Strategic Studies. National Defense University. Haettu 12.11.2022 osoitteesta: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf

Yu, S. & Munroe, T. (2021). China's Huawei says 2021 revenues down almost 30%, sees challenges ahead. Haettu 7.11.2022 osoitteesta: https://www.reuters.com/technology/chinas-huawei-says-2021-revenues-down-almost-30-sees-challenges-head-2021-12-31/

Zhou, L. (2021). China builds undersea cable bases amid digital infrastruc-ture rivalry. South China Morning Post. Haettu 13.11.2022 osoitteesta: https://www.scmp.com/news/china/diplomacy/article/3159328/china-builds-undersea-cable-bases-amid-digital-infrastructure

KIINAN TIEDUSTELU POHJOISMAISSA

Samuel Alkiomaa, Arttu Siekkinen, Joonas Taskinen, ym.

1 Johdanto

Tämä raportti käsittelee Kiinan tiedustelua Pohjoismaissa. Raportin luvussa 2 käsitellään Kiinan intressejä, sekä avataan intressien taustalla vaikuttavia Kiinan valtiojärjestelmän olennaisia elementtejä tiedustelun näkökulmasta. Tämä johdattaa lukijan raportin lukuun 3, jossa tarkastellaan Pohjoismaiden viranomaisten uhkakuvia Kiinan tiedustelun kohteista ja päämääristä. Ennen loppupäätelmiä raportissa tarkastellaan Kiinan tiedustelun keinoja sekä suoria esimerkkejä paljastuneista Kiinan tiedustelutapauksista Pohjoismaissa. Raportin tavoitteena on tuoda esiin Pohjoismaiden viranomaisten havaintoja Kiinan toteuttamasta tiedustelutoiminnasta ja arvioida Kiinan intressejä Pohjoismaissa.

Kiina tarjoaa tutkijoille mielenkiintoisen tarkastelukohteen sen tiedonhankintakeinojen sekä valtion kiinnostuksen kohteiden vuoksi. Edellä mainitut asiat poikkeavat hieman länsimaisista toimenpiteistä ja intresseistä. Kiinalla on edistyksellinen tietojen keräysmenetelmä, joka on toteutettu yhteiskunnallisen lähestymistavan kautta (Turunen, 2019). Kiina on autoritäärinen valtio ja sitä johtaa Kiinan kommunistinen puolue, jolla on vahva kontrolli ja valvonta yhteiskunnassa (Puranen, 2016). Kiinan autoritäärisyys sekä kommunistisen puolueen tiukka valvonta yhteiskunnasta tarjoavat Kiinalle erilaisia mahdollisuuksia tiedusteluun länsimaihin verrattuna.

Kiina on globaali suurvalta ja se käy kamppailua etenkin talouden ja teknologian osalta Yhdysvaltojen sekä Venäjän kanssa. Kiinalla on suuret intressit taloudellisena vaikuttajana maailmassa, minkä vuoksi se tarvitsee korkean teknologian osaamista. Korkean teknologian hankkimisen ja kehittämisen vuoksi Kiinalla on valtiollinen tarve korkeakoulutettuihin ihmisiin yhteiskunnassaan. Kiinalla on myös halu vaikuttaa kansainvälisesti ihmisten mielipiteeseen Kiinasta sekä ohjata kansainvälisen politiikan päätöksiä Kiinalle edulliseen suuntaan. (Sverige Försvarsmakten, 2021; Ulkoministeriö, 2020; Valtioneuvosto, 2021)

Raportin aihealue muodostui ja rajautui mielenkiinnosta syventää tietoja ja ymmärrystä Kiinan Pohjoismaihin kohdistamasta tiedustelutoiminnasta. Eri viranomaiset Pohjoismaissa näkevät Kiinan Venäjän rinnalla keskeisimpänä ulkoisena uhkana, erityisesti tiedustelun ja vakoilun osalta. Kiinan vuonna 2017 hyväksytty tiedustelulaki velvoittaa kiinalaiset organisaatiot ja yksilöt avustamaan Kiinan tiedustelupalveluita. Tämä herätti osaltaan raportin laatineen työryhmän mielenkiinnon aiheeseen. Kiinan lainsäädäntö poikkeaa tältä osin merkittävästi länsimaista. Lainsäädäntö mahdollistaa käytännössä maailmanlaajuisen henkilötiedusteluverkoston, jossa teoriassa jokainen ulkomailla oleskeleva Kiinan kansalainen ja yritys on osa valtiollista tiedustelujärjestelmää. (Office of the Strategy of Defence , 2020; Turunen, 2021.)

Raportin lähteinä on käytetty ainoastaan avoimia lähteitä, pääosin turvallisuusviranomaisten julkaisuita, aihetta käsittelevää kirjallisuutta sekä aiheeseen liittyvää pohjoismaista tutkimusta.

2 Kiinan tiedustelujärjestelmä ja intressit Pohjoismaissa

2.1 Valtion määrittelemää tiedustelua

Ymmärtääkseen Kiinan tiedustelutoimintaa ja sen päämääriä on ymmärrettävä taustalla vaikuttavasta valtiojärjestelmästä. Kiinassa valtiojärjestelmää hallinnoi käytännössä suvereenisti Kiinan kommunistinen puolue (engl. Communist Party of China, CPC tai engl. China's Communist Party, CCP). Puolueella on ehdoton enemmistö kaikissa valtiollisissa organisaatioissa. Puolueen omat elimet, kuten erilaiset puoluekomiteat ovat virallisia instituutioita ja merkittäviä vallankäyttäjiä. Kiinalaisesta valtiojärjestelmästä löytyy perustuslaki, presidentti, hallitus ministeriöineen sekä lakeja säätävä ja hallituksen toimia valvova parlamentti, eli Kiinan kansankongressi. Nämä organisaatiot toteuttavat kuitenkin lähinnä kommunistisen puolueen tahtoa. (Puranen, 2017)

Kiinalaiseen tiedusteluyhteisöön katsotaan kuuluvaksi Kiinan hallitus, Kansan vapautusarmeija (engl. People's Liberation Army, PLA) sekä Kiinan kommunistisen puolueen eri instituutiot (U.S.-China Economic and Security Review Commission, 2019). Kiinan valtio on puoluevaltio, jossa kommunistinen puolue ja maakuntien sekä kaupunkien hallitukset ovat Kiinan presidentti Xi Jinpingin vaikutusvallan alaisuudessa. Kiinan presidentti toimii samanaikaisesti Kiinan kommunistisen puolueen keskuskomitean ja valtion pääsihteerinä, sekä Kiinan keskussotilaskomission (engl. Central Military Commission, CMC) puheenjohtajana. Presidentin voidaan katsoa olevan koko poliittisen järjestelmän ytimessä. Presidentin alapuolella puoluehierarkiassa ovat keskuskomitean seitsemästä miehestä koostuva pysyvä poliittinen eliitti (politbyroo[1]), jonka valinnasta vastaa puolestaan 25 henkilöstä koostuva laajempi politbyroo. Presidentti Xi Jinping on pysyvän seitsemän hengen politbyroon jäsen. (Lawrence, 2021.)

Keskuskomiteassa on yhteensä 204 äänivaltaista jäsentä, jotka vastaavat kommunistisen puolueen pääsihteerin sekä politbyroon henkilöstövalinnoista. Keskuskomitean äänivaltaiset jäsenet vastaavat Kiinan kommunistisen puolueen keskussotilaskomitean jäsenten ratifioinnista sekä politbyroon ehdotuksista kommunistisen puolueen puoluesihteeristöksi. Puoluesihteeristö valvoo ja ohjaa keskuskomitean byrokratiaa, jotta kommunistisen puoleen kannalta tärkeät henkilöt pysyvät kiinni keskeisissä ministerisalkuissa. Näitä ovat muun muassa turvallisuuspalvelut sekä media- ja kulttuuripalvelut. Puolueen alla toimiva keskussotilaskomitea vastaa Kiinan asevoimien ohjaamisesta ja valvonnasta. (Lawrence, 2021.)

Kiinan kansan vapautusarmeija PLA:n tiedustelu vastaa ulkomaiden sotilaallisesta, poliittisesta ja taloudellisesta tiedustelusta sotilaallisten päämäärien tukemiseksi. PLA ja sen alaiset organisaatiot vastaavat tiedustelutoiminnasta Kiinan keskussotilaskomitealle, joka on maan johtava sotilasviranomainen. Keskussotilaskomitealla on kaksi keskeistä roolia. Sen voidaan katsoa olevan niin Kiinan hallituksen kuin Kiinan kommunistien puoleenkin keskiössä. PLA:n tiedusteluorganisaatiot suorittavat yhtä lailla henkilötiedusteluoperaatioita (HUMINT) kuin teknisen tiedustelutiedon keräämistä, esimerkiksi kyberympäristöstä. (U.S.-China Economic and Security Review Commission, 2019)

Kiina on kehittänyt PLA:n rakennetta ja uudistanut sen toimintamalleja vuoden 2015 lopulta lähtien. Uudistukset ovat koskeneet PLA:n tärkeimpiä

[1] Politbyroo on kommunistisen puolueen korkein johtoelin Kiinassa (Kielitoimisto, 2022).

tiedusteluelementtejä. Tammikuussa 2016 presidentti Xi Jinping ilmoitti PLA:n neljän vanhan osaston (yleisesikunta, poliittinen, logistinen sekä sotavoima) uudelleen organisoimisesta 15 uudeksi virastoksi keskussotilaskomitean alaisuuteen. PLA:n pääesikunnan osasto (engl. General Staff Department, GSD) oli aiemmin vastannut ulkomaisesta tiedustelutietojen keräämisestä, mutta uudelleenorganisoinnin jälkeen on epäselvää vastaako tiedustelutietojen keräämisestä ulkomailta uusi strategisen tuen joukko (engl. Strategic Support Force, SSF) vai pääesikunnan ympärille muodostettu yhteisoperaatio-osasto (engl. Joint Staff Department, JSD) (U.S.-China Economic and Security Review Commission, 2019)

Ulkomaisten tiedustelutietojen keräysvastuussa ennen organisaatiouudistusta olivat toinen (2PLA), kolmas (3PLA) ja neljäs osasto (4PLA). 2PLA:n vastuulla olivat henkilötiedusteluoperaatiot, 3PLA:n vastuulla signaalitiedustelu ja kybertoiminta ja 4PLA vastasi elektronisesta sodankäynnistä. Tehtävä piti sisällään myös elektroniset vastatoimet sekä tietoverkkojen valvomisen. Lisäksi PLA:n maavoimat, laivasto, ilmavoimat sekä ohjusjoukot sisälsivät omia tiedusteluelementtejä. (U.S.-China Economic and Security Review Commission, 2019)

Kiinan yksipuoluejärjestelmän "*koko yhteiskunta*" -lähestymistapa tarkoittaa, että se voi periaatteessa mobilisoida kaikki kiinalaisen yhteiskunnan tasot pyrkimyksissään saavuttaa Kiinan strategiset tavoitteet. Kiina käyttää lukuisia laillisia ja laittomia keinoja ja lähestymistapoja saadakseen tietoa ja tuotteita sekä edistääkseen positiivista narratiivia Kiinasta. (Politiets Efterretningstjeneste, 2021.) Useimmat lait on säädetty lähtökohtaisesti koskemaan Kiinan sisäisiä asioita, mutta ne ovat myös suoraan sovellettavissa Kiinan valtion toimintaan ulkomailla.

Tiedustelutoiminnan kannalta keskeisimpiä lakeja ovat kyberturvallisuuslaki (engl. Cybersecurity Law), vastavakoilulaki (engl. Counter-Espionage Law), kansallisen turvallisuuden laki (engl. National Security Law) sekä vastaterrorismilaki (engl. Counter-Terrorism Law). Näiden lakien tarkoituksena on antaa laajoja toimivaltuuksia ja velvoitteita Kiinan kansallisen turvallisuuden ylläpidolle. Kiinassa *kansallinen turvallisuus* on termi, joka on määritelty hyvin väljästi. (Mulvenon, 2022)

Kyberturvallisuuslaki antaa toimivaltuuksia tietoverkkojen turvallisuuden ja valvonnan toteuttamiseen. Tämä mahdollistaa kiinalaisille tietoverkkoyhtiöille ja valmistajille verkkojen valvonnan ja tiedon keräämisen. (China Law Translate, 2022a.) Vastavakoilulaki velvoittaa jokaisen kansalaisen suojelemaan Kiinan kansantasavallan turvallisuutta, etuja sekä kunniaa. Laki velvoittaa jokaisen järjestön ja yhteisön ylläpitämään kansallista turvallisuutta. (China Law Translate, 2022b.) Kansallista turvallisuutta koskeva laki velvoittaa jokaisen kansalaisen, yrityksen, järjestön, valtiollisen elimen sekä asevoimien edustajan toimimaan valtion turvallisuuden hyväksi. (China Law Translate, 2022c.)

Vuonna 2020 Kiinan hallitus sääti joukon lakeja vahvistamaan sen taloudellisen toiminnan kilpailukykyä tärkeiksi kokemillaan alueilla, sekä vahvistamaan valtion kansallista turvallisuutta (Sutter, 2021). Edellä mainittuja lakeja olivat vientivalvontalaki (engl. Export Control Law), ulkomaisia pakotteita koskeva laki (engl. Anti-Foreign Sanctions Law) sekä tietoturvalaki (engl. Data Security Law). Lakeja muokattiin vastaamaan presidentti Xi Jinpingin linjaa koskien kansallisen turvallisuuden käsitteistöä sekä Kiinan viisivuotissuunnitelman mukaisia painopistealueita. Säädetyt lait ja niiden mukaiset toimenpiteet keskittyvät esimerkiksi sellaisen sisäisen tiedon ja datan valvontaan, jota valtio voisi hyödyntää kilpailussaan muita suurvaltoja vastaan. Säädettyjä lakeja sovelletaan

aktiivisesti Kiinan ulkopuolella, sillä lait koskevat sen kansalaisten ja kansainvälisten organisaatioiden toimintaa. (Sutter, 2021) Lainsäädännön voidaan todeta tarjoavan erilaisia keinoja tiedon keräämiseksi ulkomailta omia kansalaisia hyödyntämällä.

Kiinan toteuttaman tiedustelutoiminnan kannalta keskeisin säädetty laki on vuonna 2017 hyväksytty ja voimaan tullut tiedustelulaki. Lain keskiössä on jokaisen kiinalaisen vastuu valtion turvallisuuden ylläpidossa. (Government of Canada, 2018.)

2.2 Kiinan intressit arktisella alueella

Kiinan intressit arktisella alueella ovat nousseet esille 2010-luvun lopulla. Kiinan ensimmäinen askel arktiselle alueelle tapahtui jo vuonna 1925, kun Kiina solmi Huippuvuorten sopimuksen. Kiina pääsi kuitenkin hyödyntämään sopimusta vasta 90-luvulla kansainvälisen tutkimusyhteistyön kautta. (Kettunen ym., 2022)

Kiina julkaisi vuonna 2018 arktisen politiikansa ja sisällytti polaarisen silkkitien osaksi OBOR[2]-ohjelmaansa. Arktinen alue mainittiin ensimmäisen kerran Kiinan kommunistisen puolueen kahdennessatoista viiden vuoden sopimuksessa vuonna 2011. (Havens & Seland, 2019.) Kiinan intressit polaaritutkimuksessa ovat kohdistuneet taloudellisiin ja poliittisiin tavoitteisiin. (Kettunen ym., 2022; Danish Defence Intelligence Service, 2021). Silkkitie -hanke on yksi esimerkki taloudellisen hyödyn tavoittelusta arktisella alueella ja yksi suurimmista syistä tiedustella Pohjoismaissa.

Kiina ei ole arktinen valtio, koska sillä ei ole maa- tai vesialueita napapiirin pohjoispuolella. Kiina on lanseerannut *”lähes arktinen maa”* -käsitteen arktisen alueen strategiassaan. Käsitteellä se perustelee omaa oikeuttaan olla mukana alueen toiminnassa. Koska arktista aluetta ei hallita kansainvälisillä sopimuksilla, vaan organisaatioilla ja kokoelmalla sopimuksia, on Kiina hyvin riippuvainen arktisten maiden ja kansainvälisten yritysten kanssa tehdystä yhteistoiminnasta.

Kiinan ja Islannin välinen vapaakauppasopimus on esimerkki Kiinan pyrkimyksistä päästä käsiksi arktisen alueen resursseihin. Kiina solmi vuonna 2005 Islannin kanssa yhteisymmärryspöytäkirjan vapaakauppasopimuksen muodostamiseksi. Varsinainen sopimus solmittiin vuonna 2013. Vuonna 2011 kiinalainen sijoitusryhmä yritti ostaa 30 000 hehtaaria maata Grímsstaðirista Islannin pohjoisosista, mutta Islannin valtio esti kaupan arvioidun turvallisuusuhkan takia. (Ping & Lanteigne, 2015)

Kiina alkoi vuodesta 2008 alkaen osallistua ad hoc -tarkkailijana arktisen neuvoston toimintaan. Uusien sääntöjen myötä maa sai virallisen tarkkailijamaan statuksen vuonna 2013 (Kettunen ym., 2022). Kiinan toiminta ei ole ollut aktiivista, mutta sen nojalla maa pääsee seuraamaan arktisen alueen toimintaa ja vaikuttamaan laadittaviin kansainvälisiin yhteistyösääntöihin (Kettunen ym., 2022; Danish Defence Intelligence Service, 2021).

Kiina julisti vuonna 2014 *”sodan ilmastonmuutosta vastaan”* sisäpoliittisten syiden takia. Maan nopea teollistuminen 1990-luvun alusta lähtien on tuonut mukanaan ilmansaasteet, ja kysymys ilmastopolitiikasta on muodostunut sisäpoliittiseksi. Kiina käyttää ilmastonmuutosta enemmänkin legitimoivana tekijänä sen läsnäololle arktisella alueella, eivätkä sen ilmastotoimet heijastu arktiseen strategiaan. (Kettunen ym., 2022)

[2] OBOR; One Belt, One Road -ohjelma.

Arktisella alueella olevien arvioitujen öljy- ja kaasuesiintymien paljastuminen vuonna 2008 kiihdytti Kiinan kiinnostusta alueita kohtaan. Kiinan omien ilmastotavoitteiden mukaan se pyrkii saavuttamaan hiilineutraaliuden vuoteen 2060 mennessä. Tämä voi vähentää Kiinan intressejä arktisen alueen kaasu- ja öljyesiintymiin. Sen sijaan merenpohjasta sekä Grönlannista paljastuneet akkuteollisuuden tarvitsemat maamineraaliesiintymät kiinnostavat Kiinaa todennäköisesti sitäkin enemmän. (Kettunen ym., 2022; Politiets Efterretningstjeneste, 2022.)

Uusiutumattomista energiavaroista, kuten öljystä ja kaasusta irtautuminen sekä kiinnostus ydinvoimaloiden ja uusiutuvan energian rakentamiseen ohjaavat Kiinaa tutkimusyhteistyöhön uusiutuvan energian teknologioiden saralla. Hyvänä esimerkkinä on suomalaisen LUT-yliopiston ja kiinalaisen HEBUT-yliopiston yhteinen kandidaattitutkinto-ohjelma Lahdessa (Rantalainen, 2021). Geotermisen energian hyödyntämisen suhteen yhteistyö Islannin kanssa tulee mahdollisesti kasvamaan (Kettunen ym., 2022).

Arktinen alue tarjoaa Kiinalle mahdollisuuden Koillisväylää lyhyempään merireittiin. Aiemmin mainitun Silkkitie-ohjelman alle onkin lanseerattu ”*Polaarinen silkkitie*”, joka käsittää transpolaarisen merireitin (Kettunen ym., 2022). Tämä mahdollistaisi Kiinan meriliikenteen aiempaa vapaamman toiminnan, koska Koillisväylä kulkee Venäjän aluevesien kautta. Tämän vuoksi Venäjän pystyy vaikuttamaan YK:n merioikeusyleissopimuksen tulkinnalla kauppamerenkulkuun alueellaan (Kettunen ym., 2022).

Kiinalla on taloudellisista ja poliittisista tavoitteista huolimatta tarve tehdä myös tutkimusta arktisella alueella. Maa pyrkii kiihdyttämään hankkeita ja tutkimusta ostamalla pohjolasta infrastruktuuria, sekä toteuttamalla tutkimusyhteistyötä arktisten valtioiden kanssa. Kiinalla on tutkimuskeskuksia tällä hetkellä Islannissa, Huippuvuorilla, Ruotsissa sekä avaruustutkimusyhteistyötä Suomessa. Lisäksi Kiina on ollut kiinnostunut perustamaan tutkimuskeskuksen Grönlantiin. (Kettunen ym., 2022) Infrastruktuurin hankkiminen ei ole kuitenkaan onnistunut suunnitellusti Pohjoismaissa. Kiina on yrittänyt ostaa lentokenttiä Suomesta ja Grönlannista, vanhan laivastotukikohdan Grönlannista sekä aloittaa kaivostoimintaa Islannissa. Lentokentän rakentamista Grönlantiin on ehdotettu, mutta tuloksetta. Valtiot ovat viime vuosina järjestelmällisesti evänneet näitä hankkeita. Kiinan muodostamaan strategiseen uhkaan infrastruktuurin hankintojen ja yrityskauppojen osalta on herätty tosiallisesti vasta viimevuosina. (Kettunen ym., 2022) Yksi osasyy on Kiinan tiedustelun ulottaminen tiedustelulain artiklan 14 mukaan ulkomaille.

Kiina on kiinnostunut erityisesti Grönlannista. Maantieteellisesti Grönlanti ja Färsaaret sijaitsevat strategisesti tärkeällä alueella arktisen ja Pohjois-Atlantin laiva- ja lentoliikenteen näkökulmasta tarkasteltuna (Politiets Efterretningstjeneste, 2022). Tutkimuskeskukset ja -alukset arktisilla vesillä mahdollistavat tiedonkeräämisen moneen tarkoitukseen. Merenpohjan tutkimukset auttavat esimerkiksi sukellusveneiden toimintamahdollisuuksien kartoittamisessa. Kiinan kiinnostus arktista aluetta ja Grönlantia kohtaan on pitkäaikaista. Se jatkaa tutkimus- ja yhteistyömahdollisuuksien etsimistä erityisesti Grönlannissa. (Danish Defence Intelligence Service, 2021.)

3 Kiinan muodostamat uhkat Pohjoismaiden viranomaisten näkökulmasta

3.1 Suomi

Suomelle merkittävimmän tiedustelun ja valtiollisen vaikuttamisen uhkan muodostavat Venäjä ja Kiina (Suojelupoliisi, 2022a). Suojelupoliisin mukaan Suomeen kohdistuu aktiivista, pitkäjänteistä ja laaja-alaista vieraiden valtioiden tiedustelua ja vakoilua. Tätä näkemystä tukevat myös Ruotsissa ja Norjassa julki tulleet tapaukset. (Turunen, 2022).

Suomen kansallista turvallisuutta uhkaavaa tiedustelua toteuttavat erityisesti Venäjän ja Kiinan tiedusteluorganisaatiot. Tiedonhankinnan lisäksi osa Suomea kohtaan toimivista valtioista pyrkii vaikuttamaan suomalaiseen poliittiseen päätöksentekoon ja kansalaismielipiteeseen. Tiedustelu ja vaikuttaminen kohdistuvat järjestöjen, yritysten, yliopistojen ja tutkimuslaitosten tietoon ja toimintaan. (Suojelupoliisi, 2021) Suomessa on runsaasti Kiinan haluamaa teknologista osaamista, ja maalla on kyky hankkia tätä tietoa tiedustelun keinoin (Turunen, 2021). Kiinan asevoimien tai maan kansallisen puolustuksen tieteen, teknologian ja teollisuuden viraston alaisuudessa on Kiinassa kymmeniä yliopistoja. Niistä tulevia tutkijoita on myös Suomessa.

Suomesta ja Suomen kautta pyritään hankkimaan vientivalvonnan alaisia tuotteita, kuten kaksikäyttötuotteita ja joukkotuhoaseohjelmissa käytettävää sensitiivistä teknologiaa. Vientirajoituksia pyritään kiertämään esimerkiksi yritysostoilla, virheellisillä loppukäyttäjätodistuksilla, yksityisten yritysten ja hankintaverkostojen käytöllä sekä tutkimusyhteistyöllä. Kvanttiteknologiassa ja -tietokoneissa tarvittavat komponentit ovat esimerkkejä teknologiasta, joita Suomesta tavoitellaan. (Suojelupoliisi, 2022a.)

Korkea teknologia ja siihen liittyvä osaaminen tulevat poliittisen päätöksenteon ohella säilymään Kiinan kohdistaman tiedustelun keskeisinä kohteina Suomessa tulevaisuudessakin. Kriittiseen infrastruktuuriin kohdistuva tiedustelu ja vaikuttaminen sekä yritysten ja yhteiskunnan keskeisiin toimintoihin liittyvien tuotanto- ja toimitusketjujen häiriöiden uhka pysyy kohonneena lähitulevaisuudessakin. (Suojelupoliisi, 2022a.) Omistusten tai palveluntuottajana toimimisen kautta Kiinan kaltaisesta valtiosta tuleva organisaatio voi saada pääsyn ja vaikutusvaltaa suomalaiseen kriittiseen infrastruktuuriin. (Suojelupoliisi, 2022a.)

Pakolaisvakoilu ei ole Suomessa rikos, mutta se muodostaa uhkan Suomessa asuville kiinalaisille. Autoritäärisillä valtioilla on ajoittain pyrkimys vaikuttaa tai kohdistaa tiedonhankintaa Suomessa oleskeleviin maasta paenneisiin ihmisiin[3] esimerkiksi kontrolloimalla tai vaientamalla heitä, vaikka paenneet olisivat jo asettuneet uuteen kotimaahansa. (Suojelupoliisi, 2021a)

Suojelupoliisin mukaan Suomea koskeva kybervakoilu jakaantuu karkeasti kahteen ryhmään. Suomalaisiin organisaatioihin suoraan kohdistuvalla kybervakoilulla pyritään hankkimaan organisaatioiden tietoa. Infrastruktuuria hyödyntävässä kybervakoilussa pyritään murtautumaan Suomessa sijaitseville verkkolaitteille ja palvelimille ja liittämään ne osaksi kybervakoiluoperaatiossa käytettävää infrastruktuuria (Suojelupoliisi, 2021b). Suojelupoliisin mukaan kiinalaista informaatioteknologiaa hankittaessa tulisi riskiarviossa huomioida laitteilla käsiteltävän tiedon luottamuksellisuus. Kiinalaisilla

[3] Näitä ovat esimerkiksi toisinajattelijat ja poliittiseen oppositioon kuuluvat henkilöt.

laitevalmistajilla on velvoite avustaa tarvittaessa maan tiedustelupalveluita, joiden tehtäviin kuuluu myös länsimaihin kohdistuva kybervakoilu. (Suojelupoliisi, 2022a.)

3.2 Ruotsi

Ruotsin tiedustelu- ja turvallisuuspalvelu SÄPO:n (ruots. Säkerhetspolisen) mukaan Venäjä, Kiina ja Iran ovat maan suurimmat ulkoiset uhkat (Säkerhetspolisen, 2021). Kiinan Ruotsia vastaan kohdistamat tiedustelukeinot ovat laaja-alaisia (Säkerhetspolisen, 2021). Vaikka Ruotsi on maantieteellisesti kaukana Kiinasta se ei estä Kiinan toimintaa sen pyrkiessä saavuttamaan pitkän aikavälin sotilaallisia, taloudellisia ja poliittisia tavoitteitaan (Säkerhetspolisen, 2021).

Kiinan muodostama tiedustelu-uhka on lisääntynyt, ja se voi sisältää muun muassa kybervakoilua, strategisia yritysostoja sekä ruotsalaisiin poliittisiin päättäjiin, tutkijoihin ja julkisuuden henkilöihin kohdistuvaa painostusta tai uhkailua (Säkerhetspolisen, 2021). SÄPO:n mukaan vieraiden valtioiden Ruotsiin kohdistama aktiivinen toiminta tietoverkoissa ilmenee pääasiassa vakoiluna ja kohteiden kartoittamisena, mutta myös suoria hyökkäysyrityksiä on havaittu. SÄPO:n havaintojen perusteella Ruotsin alueelta on toteutettu kyberhyökkäyksiä muita valtioita vastaan. (Säkerhetspolisen, 2021)

Ruotsin asema huipputeknologian, tutkimuksen ja innovaatioiden kärkipäässä houkuttelee Kiinan kaltaisten valtioiden tiedustelua. Kiinan tiedustelua Ruotsissa kiinnostavat esimerkiksi korkea teknologia, raaka-aineet ja innovaatiot. (Säkerhetspolisen, 2021) Ruotsalaisissa korkeakouluissa ja yliopistoissa opiskelevia Kiinan kansalaisia käytetään lain velvoittamana hankkimaan korkeaa teknologiaa ja osaamista, joka hyödyttää Kiinaa sen kehittäessä esimerkiksi omaa sotilas- ja avaruusteknologiaansa (Säkerhetspolisen, 2021). Kiinan pakolaisvakoilu kohdistuu pääasiassa toisinajattelijoihin ja poliittiseen oppositioon. Vakoilu kohdistuu erityisesti Ruotsissa asuviin tiibetiläisiin ja uiguureihin. (Säkerhetspolisen, 2021)

3.3 Norja

Norjan tiedustelu- ja turvallisuuspalvelun PST:n (norj. Politiets Sikkerhetstjeneste) mukaan maan alueella toimii useiden maiden tiedustelupalveluita, mutta suurimman uhkan muodostavat Venäjän ja Kiinan tiedustelupalvelut. Norjan tekemät uudistukset ja hankkeet puolustusteollisuuden, varautumisen, päätöksenteon ja korkean teknologian aloilla ovat PST:n mukaan erityisen alttiita tiedustelulle ja vakoilulle. (Politiets Sikkerhetstjeneste, 2022)

PST:n arvion mukaan ulkovaltojen tiedustelu muodostaa uhkan norjalaisille liikeelämän ja teollisuuden asiantuntijaryhmille, jotka toimivat modernin puolustus- ja aseteollisuuden parissa. Arvion mukaan on todennäköistä, että tällaisia ryhmiä vastaan kohdistuu peiteltyä tiedonhankintaa. Valtiolliset toimijat tulevat myös tulevaisuudessa tarkkailemaan Norjassa asuvia ulkomaiden kansalaisia, eli toteuttamaan pakolaisvakoilua. Vakoilun tavoitteena on pyrkiä estämään tai tukahduttamaan Norjasta käsin toteutettava poliittinen vastarinta. (Politiets Sikkerhetstjeneste, 2022)

Tietoverkoissa tapahtuvasta toiminnasta on tullut olennainen osa ulkomaisten tiedustelupalvelujen toimintaa Norjassa. Norjan parlamenttiin vuosina 2020 ja 2021 kohdistetut kyberhyökkäykset ovat esimerkkejä erittäin vakavista välikohtauksista. Norjan kansallisen turvallisuusviranomaisen NSM:n (norj. Nasjonal Sikkerhetsmyndighet) havaintojen perusteella julkisen ja yksityisen sektorin yrityksiin kohdistuvat vakavat

kyberturvallisuuspoikkeamat ovat jopa kolminkertaistuneet viime vuosina. Osa näistä on toteutettu ulkomaisten tiedustelupalveluiden laskuun, yleisimmin Kiinan ja Venäjän tiedusteluille. Vuonna 2021 vihamieliset toimijat onnistuivat soluttautumaan Norjan viranomaisille ja yksityisille yrityksille kuuluviin verkkoihin, ja on odotettavissa, että esimerkiksi Kiina jatkaa vastaavanlaista aktiivista toimintaa Norjaa vastaan myös tulevaisuudessa. (Politiets Sikkerhetstjeneste, 2022)

Kybervakoilun osalta ulkomaiset tiedustelupalvelut ovat todennäköisesti kiinnostuneita Norjan päätöksentekoprosessista saatavasta tiedosta. Kybervakoilun uhka koskettaa keskeisesti sellaisia yrityksiä ja tutkimusryhmiä, jotka ovat tekemisissä maan ulko-, puolustus- ja turvallisuuspolitiikan kanssa. Myös terveys- puolustus- ja meriteknologiaa sekä öljyntuotantoa ja avaruutta käsittävät alat ovat todennäköisiä kohteita. (Politiets Sikkerhetstjeneste, 2022)

Norjan ja Kiinan kahdenvälisten suhteiden normalisoitumisen jälkeen PST on havainnut, että Kiinan toiminta tietoverkoissa on keskittynyt enemmän Norjan poliittisiin kysymyksiin. PST:n mukaan tämä on selkeä muutos aikaisempaan, jolloin toiminta suuntautui enemmän teknologiayrityksiin. Vihamielisten kiinalaisten kybertoimijoiden tehtävänä on pyrkiä tunnistamaan norjalaisia poliitikkoja ja muita Kiinaa arvostelevia henkilöitä. (Politiets Sikkerhetstjeneste, 2022)

Muiden autoritääristen valtioiden tavoin Kiinan käyttää tiedustelupalveluaan kitkeäkseen poliittisten toisinajattelijoiden toimintaa maan rajojensa ulkopuolella. Kiinan kaltaisten maiden viranomaiset haluavat varmistaa, että niiden poliittiset vastustajat eivät tunne oloaan turvalliseksi puhuakseen julkisesti. Pakolaisiin ja poliittisiin toisinajattelijoihin kohdistuvaa vakoilua toteutetaan esimerkiksi pakolaisryhmien tapahtumissa ja yhdistyksissä, mutta myös uskonnollisissa kohtaamispaikoissa ja internetissä. Vakoiluun voi kuulua myös sosiaalisen median seurantaa ja elektronisiin laitteisiin murtautumista yksilöiden tai ryhmien seuraamiseksi. (Politiets Sikkerhetstjeneste, 2022)

3.4 Tanska

Tanskaan ja sen etuihin kohdistuvan tiedustelun ja vakoilun uhka aiheuttaa sille merkittäviä poliittisia, turvallisuuteen liittyviä ja taloudellisia haasteita. Tällaiseen toimintaan kuuluvat vakoilu, ulkomainen sekaantuminen maan sisäisiin asioihin, häirintä, tuotteiden, teknologian ja tiedon laittoman hankinnan yritykset sekä erityistapauksissa salamurhat. Uhka koskee Tanskan valtakunnan kaikkia kolmea osaa: Tanskaa, Grönlantia, Färsaaria. (Danish Defence Intelligence Service, 2021)

Kiinan tiedustelupalveluiden muodostama uhka koskee etenkin vaikuttamista ja vakoilua. Sen kohteita ovat poliitikot, julkishallinnon virkamiehet, yritykset ja organisaatiot, jotka työskentelevät ulko-, turvallisuus- ja puolustuspolitiikan aloilla, energiaa, raaka-aineita ja kaupallista merenkulkua koskevilla aloilla, tai joiden toiminta arktisella alueella liittyy näihin teemoihin. (Danish Defence Intelligence Service, 2021; Politiets Efterretningstjeneste, 2021; Politiets Efterretningstjeneste, 2022a.)

Useat vieraat valtiot osallistuvat vientivalvonnan ja pakotteiden alaisten tuotteiden ja teknologian laittomaan hankintaan Tanskasta. Laittomasta hankinnasta on kyse silloin, kun yritykset vievät tavaroita tai antavat teknistä tukea, joka välittäjien kautta päätyy vääriin käsiin. Tällainen laittomien hankintojen uhka kohdistuu pääasiassa yrityksiin ja tutkimuslaitoksiin. (Politiets Efterretningstjeneste, 2022c.)

Ulkomaiset tiedustelupalvelut pyrkivät jatkuvasti luomaan yhteyksiä opiskelijoihin, tutkijoihin ja yrityksiin, jotka pystyvät tarjoamaan tietoa uusimmasta tanskalaisesta teknologiasta ja tutkimuksesta. Tämä koskee erityisesti energia-, bio- ja kvanttiteknologian, robotiikan, puolustusteollisuuden sekä vientivalvonnan piiriin kuuluvien tuotteiden aloja. (Politiets Efterretningstjeneste, 2021)

Kiinan kaltaisten valtioiden osalta kansainvälinen yhteistyö, investoinnit ja kauppa voivat sisältää sellaisia geostrategisia tai turvallisuuspoliittisia tavoitteita, jotka ylittävät näiden maiden yhteistyön viralliset tavoitteet. Kansainvälinen yhteistyö, laajat investoinnit ja kauppa Kiinan kanssa voi sisältää riskejä, koska tällaiset toimet voivat altistaa Färsaaret ja Grönlannin vakoilulle ja vaikuttamistoiminnalle. (Politiets Efterretningstjeneste, 2021) Kiinalaisten yritysten ja sen poliittisen järjestelmän välisten yhteyksien seurauksena sen investointeihin Grönlantiin liittyy riskejä. Suurilla investoinneilla voi olla vaikutus Grönlannin talouteen. Mahdollisen poliittisen vaikuttamisen ja painostuksen riski kasvaa silloin, kun investoinnit suunnataan strategisiin resursseihin tai kriittiseen infrastruktuuriin. (Danish Defence Intelligence Service, 2021)

Kyberympäristössä tapahtuva toiminta on yksi keskeisistä ja merkittävistä Tanskaan kohdistuvista uhkista. Sitä tapahtuu niin valtiollisten kuin rikollistenkin toimijoiden toteuttamana. Kybertoimintaa ovat esimerkiksi kiristysohjelmahyökkäykset, joita erityisesti rikolliset hakkerit suosivat. (Danish Defence Intelligence Service, 2021) Vihamielisten valtioiden ja niiden tukemien hakkereiden kybervakoilu muodostaa erittäin suuren uhkan etenkin kriittisten alojen yrityksille, mutta myös viranomaisille (Centre for Cyber Security, 2022). Kybervakoilun aiheuttaman vakavan uhkan taustalla ovat ulkomaisten valtioiden, erityisesti Venäjän ja Kiinan intressit saada tietoa ulko-, turvallisuus- ja puolustuspoliittisista kysymyksistä (Centre for Cyber Security, 2022).

Merenkulku-, energia- ja puolustusteollisuuden viranomaiset ja yksityiset yritykset ovat jo useiden vuosien ajan olleet erittäin suuren kybervakoilun uhkan alla. Vieraat valtiot, mukaan lukien Kiina, ovat tyypillisesti kiinnostuneita laitteista ja tekniikasta, joita voidaan käyttää sekä siviili- että sotilastarkoituksiin. (Centre for Cyber Security, 2022) Kybervakoilun kautta saatavaa tietoa voidaan hyödyntää Tanskan etujen tai tanskalaisten yritysten vahingoittamiseen (Danish Defence Intelligence Service, 2021). Kiina kykenee laajan mittakaavan kybervakoiluun sekä käynnistämään kohdennettuja kyberoperaatioita länsimaisia viranomaisia, yrityksiä ja organisaatioita vastaan (Danish Defence Intelligence Service, 2021).

4 Kiinan tiedonkeräys Pohjoismaissa

4.1 Kiinalaiset korkeakouluopiskelijat teknologiavakoilun mahdollisuutena

Kiina on viimeisten vuosien aikana panostanut erityisesti yliopistotasoiseen koulutukseen. Vuonna 2021 Kiinan yliopistoista kymmenen (ml. Hong Kong) oli noussut The Times Higher Educationin World University Ranking -listalle top 100:n joukkoon. Tämä on merkittävä suoritus, sillä listattuna on noin 1600 yliopistoa ympäri maailman. (The Times Higer Education, 2022.)

Kiina ei ole päässyt listalle helposti, sillä se on käyttänyt korkeakouluopiskelijoihin vuonna 2019 yli 170 miljardia euroa (Ministry of education, The Peoples's Republic of China, 2020). Kiinasta ulkomaille lähteneiden opiskelijoiden määrät ovat olleet tasaisessa kasvussa ennen COVID-19 pandemiaa. Vuonna 2019 maailmalla opiskeli yli 700

000 kiinalaista korkeakouluopiskelijaa. COVID-19 pandemian takia vuonna 2020 opiskelijoiden määrä laski 350 000:een. (Statista, 2022.)

EU:n korkeakouluissa opiskeli vuonna 2019 noin 200 000 kiinalaista. Näistä noin 15 000 oli tohtoriopiskelijoita (Eurostat, 2022). Kiinalaiset opiskelijat muodostavat noin 20 % kaikista kansainvälisistä tohtoriopiskelijoista. Kiinalaisten korkeakouluopiskelijoiden määrä ulkomailla kasvoi Kiinan keventäessä byrokratiaa. Pohjoismaista Norja on houkuttanut paljon kiinalaisia opetuksen korkean tason ja ilmaisen opetuksensa takia. (Yujing, 2013) Vuoden 2023 aikana Norja on kuitenkin suunnitellut opiskelumaksuja EU/EEA:n ja Sveitsin ulkopuolisille opiskelijoille (Norwegian directorate for higher education and skills, 2022). Tämä tulee todennäköisesti laskemaan jonkin verran ulkomaalaisten opiskelijoiden määrää.

Ruotsissa kiinalaisten korkeakouluopiskelijoiden määrät ovat vaihdelleet vuodesta 2012 vuoteen 2019 asti 1500–2200 opiskelijan välillä (Eurostat, 2022; Statiska centralbyrån, 2017). Suomessa vastaavat määrät ovat vaihdelleet 1000–1600 opiskelijan välillä (Eurostat, 2022). Suomessa on käynnistetty viimevuosina yhteistyökursseja tekniikan opintoihin liittyen, esimerkiksi kiinalaisen HEBUT-yliopiston ja suomalaisen LUT-yliopiston välillä. Opinnot sisältävät energiateknologian ja ohjelmoinnin kandidaatin tutkinnot. LUT:n mukaan kiinalaisia opiskelijoita haluttaisiin saada jäämään töihin Suomeen. (Rantalainen, 2021.)

Tällä hetkellä ei ole havaittavissa erityistä kiinalaisten opiskelijoiden uudelleenhakeutumista Pohjoismaisiin yliopistoihin, mutta COVID-19 pandemian laantuminen voi palauttaa ulkomailla opiskelevien kiinalaisten määrän vuoden 2019 tasolle. Toisaalta Kiinan omat yliopistot ovat saavuttamassa länsimaisten huippuyliopistojen tasoa (The Times Higer Education, 2022), joten Kiinaan opiskelemaan jäävien opiskelijoiden määrät todennäköisesi kasvavat.

Kiinalaisten korkeakouluopiskelijoiden määrä on hyvä huomata teollisuusvakoilusta puhuttaessa. Esimerkiksi Yhdysvaltojen liittovaltion poliisi FBI (engl. Federal Bureau of Investigation) ilmoittaa, etteivät Kiinan kansalaiset ole itsessään turvallisuusongelma länsimaisille valtioille. Ongelmana on Kiinan autoritäärisen hallinnon toteuttama teollisuus- ja teknologiavakoilu, käyttämällä maan kansalaisia hyväksi tiedustelulain artikla 14 mukaisesti. (Federal Bureau of Investigation, 2022.)

Suomessa asui vuonna 2021 yhteensä 11 405 kiinalaista (Tilastokeskus, 2022), ja on epätodennäköistä, että heistä kaikki toimittaisivat jollakin tavalla merkityksellistä tietoa Kiinan kansantasavallalle. Eräässä kandidaatin opinnäytetyössä on selvitetty kiinalaisten kandidaatintutkinnon suorittaneiden opiskelijoiden tavoitteita kurssin jälkeen. Tutkimuksen mukaan suurin osa kiinalaisista jatkaa maisteriopintoja Suomessa tai jatkaa muuhun ulkomaiseen yliopistoon jatkamaan opintojaan. Kiinalaisten työllistyminen Suomessa on kuitenkin hankalaa kulttuurierojen, kielimuurin ja Suomen taloudellisen taantuman vuoksi. Tämä lisää kiinalaisten paluumuuttoa kotimaahansa. (Yingying & Yiping, 2021)

Opintojen kautta kiinalaisten työllistyminen suomalaiseen teollisuuteen ja teknologian yrityksiin on haastavaa ja vain murto-osa kiinalaisista päätyy tällöin sellaiselle teknologian tai teollisuuden alalle töihin, josta olisi tiedonhankintamielessä hyötyä Kiinalle. Suuremman uhkan muodostavat korkeakouluopinnoissa korkealle tähtäävät kiinalaiset, jotka kykenevät pääsemään käsiksi tai osaksi uusia teknologisia innovaatioita. Esimerkiksi Yhdysvalloissa Duken yliopistosta vuonna 2006 kiinalainen tohtoriopiskelija Ruopeng Liu kopioi Smith’s Labin näkymättömyysviitan piirustukset ja valmisti tuotteen.

Hän toimitti tuotteen Kiinaan ilman tutkimuslaboratorion myöntämää lupaa. (McFadden; Nadi & McGee, 2018.)

Tämän kaltainen teollisuus- tai teknologiavakoilu voi olla mahdollista myös Pohjoismaissa, vaikka tapauksia ei ole tullut julkisuuteen. Kiinan asevoimien tai maan kansallisen puolustuksen tieteen, teknologian ja teollisuuden viraston alaisuudessa toimii Kiinassa kymmeniä yliopistoja, joista saapuu tutkijoita myös Suomeen. Näillä on mahdollisuus hankkia vientivalvonnan alaista teknologista osaamista Kiinaan. (Suojelupoliisi, 2022b.)

Ensimmäisessä pääluvussa mainitut Kiinan intressit arktisella alueella sekä kiinnostus energiateknologiaan voi ohjata kiinalaisia opiskelijoita suuntautumaan kyseisiin aiheisiin. Kiinan tiedusteluviranomaiset seuraavat todennäköisesti opinnoissa pitkälle eteneviä henkilöitä tarkasti. He muodostavat Kiinan tiedusteluviranomaisille todennäköisesti mielenkiintoisen tietolähteen, maan tavoitellessa tieteellistä ja teknologista ylivoimaa suurvalta-asemansa parantamiseksi arktisella alueella.

4.2 Organisoitua vakoilua ja vaikuttamista yhteisöjen kautta

Kiinalla on useita valtiollisia organisaatioita, jotka ovat erikoistuneet vaikutustoimintaan. Vaikuttaminen on maailmanlaajuista ja myös Pohjoismaat ovat sen kohteena. Erityisesti teknologia-alan yritykset sekä akateemisen maailman edustajat ovat Kiinan vaikuttamiselle kiinnostavia kohteita. (Liski, 2020.) Suojelupoliisin mukaan kiinalaiseen vaikuttamistoimintaan voidaan käyttää tiedustelumaailmasta tuttuja peiteorganisaatioita, kuten tiede- ja teknologiayrityksiä. Näillä aloilla toimivat opiskelijat ja tutkijat ovat Kiinan kannalta houkuttelevia kohteita. Tutkimustoiminnan varjolla toteutettava tiedustelutoiminta saadaan näyttäytymään avoimena tieteellisenä tutkimuksena, eikä sitä toteuttava välttämättä tiedosta tuottavansa tiedustelutietoa Kiinan valtapuolueelle. (Liski, 2020.)

Kiinalaiset yritykset ovat tehneet investointeja strategisiksi luokitelluille aloille ja kriittiseen infrastruktuuriin myös Pohjoismaissa (Puranen, 2020). Strategisia riippuvuuksia sisältävät alat liittyvät raaka-aineisiin, puolijohteisiin, energiavaltaisiin teollisuusaloihin sekä lääketuotantoon (Euroopan komissio, 2020). Kiinalaisten yritysten suoranaista yhteyttä Kiinan valtioon ei voida poissulkea (Puranen, 2020).

Suomessa keskustelua on herättänyt Konfutse-instituutti. Se on akateeminen koulutus- ja tutkimusinstituutti, jonka toiminnan ytimessä ovat kiinan kieli, kiinalainen kulttuuri sekä Kiina-tutkimus. Instituutti järjestää esimerkiksi kieli- ja kulttuurikursseja, virallisia kiinan kielen tasokokeita sekä Kiina-aiheisia luentoja ja tutkimusprojekteja. (Confucius Institute, 2022.)[4] Instituuttien on pelätty murentavan yliopistojen akateemista vapautta välttelemällä järjestämissään tilaisuuksissa Kiinan kannalta epäedullisia aiheita (Puranen, 2020). Kesällä 2022 on uutisoitu Helsingin yliopiston alla toimivan Konfutse-instituutin lakkauttamisesta mainehaittojen ja vaikutusepäilyjen vuoksi. Instituutti toimi yliopistolla vuodesta 2007 alkaen. (Kangasluoma, 2022.)

Suomessa toimii Kiinan kommunistisen puolueen Yhteisrintaman työosasto (engl. United Front Work Department, jatkossa Yhteisrintama), joka on Kiinalle uniikki tiedustelua ja vaikuttamista yhdistävä organisaatio. Yhteisrintama toimii kaikkialla maailmassa tiedustelu- ja vaikuttamistehtävissä. Suomessa organisaation toimintamenetelmät ovat

[4] 2023 alkuvuodesta Konfutse Instituutin (Confucius Institute) blogi Helsingin yliopiston nettisivuilla oli ajettu alas osana kesällä 2022 tehtyä lakkauttamispäätöstä.

hienovaraisia eivätkä herätä suurta huomiota. Kiinan kommunistisen puolueen Yhteisrintama on suorassa yhteydessä keskuskomiteaan toimiva puolueen osa. Organisaationa Yhteisrintama on yhtä vanha itse puolueen kanssa, mutta sen toiminnan merkitys on lisääntynyt presidentti Xi Jinpingin kaudella vuodesta 2012 alkaen. Xi Jinping on asettanut Yhteisrintaman kehittämisen ja toiminnan uudistamisen yhdeksi keskeiseksi tavoitteeksi. (Puranen, 2020.)

Kiinan ulkopuolella Yhteisrintaman pääkohteina ovat ulkokiinalaiset yhteisöt, joihin kuuluu maailmanlaajuisesti yli 50 miljoonaa kiinalaista. Yhteisrintaman tavoitteena on torjua Kiinan ulkopuolella asuvien kansalaisten muodostama uhka kommunistiselle puolueelle sekä mobilisoida isänmaallisia ja puolueen tavoitteille myötämielisiä kiinalaisia. Isänmaalliset kiinalaiset tarjoavat Yhteisrintamalle väylän tiedustelutoimintaan sekä poliittisen ja taloudellisen vaikutusvallan levittämiseen. Yhteisrintama toimii sellaisella alueella, joka esimerkiksi Venäjän toiminnassa mielletään hybridivaikuttamiseksi. (Puranen, 2020.)

Yhteisrintama perustaa uusia ulkokiinalaisia järjestöjä ja soluttautuu jo olemassa oleviin järjestöihin sekä yhdistyksiin. Järjestö- ja yhdistystoiminnan kautta Yhteisrintama kykenee valvomaan kokonaisvaltaisesti etenkin ulkokiinalaisia opiskelijoita ja tutkijoita, mutta yhtä lailla se kykenee muodostamaan yhteyksiä keskeisissä asemissa oleviin ulkokiinalaisiin. Kiinan toimintatapamalliin kuuluu käyttää erilaisia järjestöjä ja yhdistyksiä peiteorganisaatioina toteuttamalleen tiedustelu- ja vaikutustoiminnalle. Hyvin harva ulkokiinalainen yhteisö kykenee jättäytymään nykypäivänä Yhteisrintaman vaikutusvallan ulkopuolelle. (Puranen, 2020.)

Järjestöjen valvonnan ja niiden kautta vaikuttamisen lisäksi Yhteisrintama käyttää päämääriensä saavuttamiseksi myös perinteisiä diplomatian keinoja. Uudessa-Seelannissa toimivaa Yhteisrintamaa tutkineen professorin Anne-Marie Bradyn mukaan jokaisessa kiinalaisessa suurlähetystössä on Yhteisrintamalle työskentelevä henkilö peiteroolissa. Niin järjestötyön kuin diplomaattisen vaikuttamisen tavoitteena on Bradyn mukaan luoda läheisiä kontakteja kohdevaltion poliittiseen, taloudelliseen ja akateemiseen eliittiin sekä keskeisiin vaikuttajiin. Erilaisilla lahjoituksilla ja rahoituksilla Kiina ulottaa omaa vaikutusvaltaansa kohdemaihinsa. (Puranen, 2020.)

Ruotsissa Kiinan suurlähetystö ajaa agendaansa Suomea voimakkaammin. Tästä esimerkkinä ovat Ruotsin suurimpien uutistoimitusten saamat yhteydenotot Kiinan suurlähetystöstä. (Rognerud, 2020.) Yhteydenottojen tarkoituksena on ollut arvostella uutisointia sekä vaikuttaa ruotsalaisten tiedotusvälineiden toimintaan (Kokkonen, 2020). Ruotsin puolustusministeriö on arvioinut, että valtiollisten toimijoiden sponsoroima disinformaatio ja hybridivaikuttaminen ovat osa uutta normaalia. EU-maat ovat syyttäneet Kiinaa teollisuusvakoilusta, ja kiinalaista tiedeyhteisöä pidetään tutkimuksellisesti epäeettisenä. Useat EU-maat ovat kieltäneet kiinalaisten 5G-laitteiden käytön, koska Kiinan tiedustelulaki velvoittaa yritykset tekemään yhteistyötä maan tiedustelun kanssa. (Bazarkina, 2020.)

Kiinan vaikutusvalta on voimistunut myös Suomessa. Keväästä 2020 alkaen on havaittu merkkejä normaalista vuorovaikutuksesta eroavasta tiedustelu- ja vakoilutoiminasta. Toiminta on vaihdellut tyypillisistä Yhteisrintaman toteuttamista järjestöjä hyödyntävistä operaatioista aina erilaisiin tiedotusoperaatioihin sekä Suomessa olevien pakolaisten häirintään. (Puranen & Aukia, 2022.) Erillistapauksina voidaan mainita esimerkiksi kiinalaisen PLA:n kenraalin kutsuminen yksityisesti Suomen eduskuntaan ja samalle ajalle ajoittunut kyberhyökkäys eduskuntaa vastaan. Kutsu kenraalille oli järjestynyt

suomalaisen kansanedustajan yhteyksistä yritykseen, joka toimii kiinalaisella rahoituksella. Lisäksi tutkimukset osoittivat kyberhyökkäyksen olevan kiinalaista alkuperää. (Puranen & Aukia, 2022.) Tämä toiminta on osa kiinalaisten vallan ja läsnäolon näyttöä.

5 Johtopäätökset ja lähdekritiikki

5.1 Johtopäätökset

Kiina on noussut haastamaan Yhdysvaltojen suurvalta-asemaa. Suurvalta-aseman saavuttaminen ja ylläpitäminen vaatii vahvaa taloudellista pohjaa, tieteellisiä saavutuksia ja teknologista ylivoimaa sekä näkyvyyttä ympäri maailman. Kiina on turvautunut laajaan tiedonhankinnan malliin vuoden 2017 tiedustelulain avulla. Tiedustelulaki tuo uusia mahdollisuuksia Kiinan valtiolle tiedon hankkimiseen kansalaisiltaan ja yrityksiltään. Kiina kykenee keräämään tietoa nykyään lähes kaikkialta, missä sen kansalaiset liikkuvat.

Pohjoismaista houkuttelevan kohteen Kiinan yliopisto-opiskelijoille tekee korkea koulutuksen taso sekä edullinen tai jopa ilmainen opiskeluoikeus. Kiinan tiedustelulaki mahdollistaa tiedonkeräämisen kaikilta kiinalaisilta korkeakouluopiskelijoita, vaikkakaan kaikki maailmalla olevat 350 000 opiskelijaa eivät ole Kiinan tiedustelun mielenkiinnon kohteena. Tiedon kerääminen kohdennetaan todennäköisesti vain tietyn tason tai tiettyjen alojen opiskelijoihin. Ulkomailla olevat 15 000 tohtoriopiskelijaa ovat Kiinan tiedonhankinnan kannalta merkittävä resurssi tieteisiin ja erityisesti teknologiaan liittyvässä vakoilussa. Kiinan tiedustelujärjestelmä pyrkii muiden suurvaltojen tavoin tunnistamaan ja löytämään kansalaisistaan ne henkilöt, joilla on Kiinan valtiolle eniten tarjottavaa tiedustelun saralla.

Tiedustelutietoa kerätään yksittäisiltä kansalaisilta ja organisaatioilta. Kiinalaiset ovat käyttäneet tiedusteluun myös teknisiä- ja kybertiedustelukeinoja. Kyberhyökkäykset tietomurtoineen ovat mahdollisia esimerkiksi valtioiden hallintojärjestelmiin sekä datakeskuksiin. Hyökkäysten jäljittäminen on haastavaa valtioiden käyttäessä erillisiä hakkeriryhmiä tai kohdentamalla hyökkäykset kolmansien maiden kautta. Yhteisen maarajan puuttuessa, Kiinan kyberkyvyt luovat uhkan pohjoismaiselle kyberympäristölle.

Kiinan tiedustelun toimintaa on pidetty hyvin organisoituna ja osittain salaperäisinä. Moni asia osoittaa kuitenkin tiedustelun salaperäisyyden ja organisoinnin olevan luultua heikommalla tasolla. Kiinan tiedustelu perustuu etenkin henkilötiedustelun osalta enemmän laajaan massaan, kuin yksittäisten henkilöiden osaamiseen. Pohjoismaissa Kiina muodostaa Venäjän rinnalla suurimman uhkan tiedustelun näkökulmasta. Pohjoismaisten viranomaisten julkaisujen perusteella Kiinan uhka nähdään pitkälti samanlaisena kaikissa Pohjoismaissa. Kolme neljästä maasta, joiden viranomaisten julkaisuja tarkasteltiin, nimesi Kiinan yhdeksi sen merkittävimmistä ulkoisista uhkista. Keskeinen havainto oli, että Kiinan tiedustelua Pohjoismaissa pidetään pitkäjänteisenä sekä laaja-alaisena, ja sillä pyritään ensisijaisesti strategisen tason tiedonhankintaan.

Kiinalaisten muualla asuviin kansalaisiinsa kohdistama pakolaisvakoilu on yksi sen tiedustelun ja vaikuttamisen keskeisistä päämääristä Pohjoismaissa. Kiina pyrkii pakolaisvakoilulla estämään maan ulkopuolella asuvien kiinalaisten negatiiviset viestit Kiinasta ja näin vaikuttamaan kansainvälisesti ihmisten mielipiteeseen. Kiinalla on ulkomailla omia järjestöjä, kuten Yhteisrintama, joiden tehtävänä on hankkia tietoa ihmisten mielipiteistä sekä pyrkiä vaikuttamaan yleiseen mielipiteeseen.

Kiinalla, kuten muillakin suurvalloilla, on erityisiä intressejä arktisella alueella, vaikka se ei olekaan arktinen valtio. Kiinan intressit arktisella alueella ovat puhtaasti valtion omien etujen ajamista tulevaisuudessa tarjolla olevilla resursseilla, sekä pyrkimystä laajentaa omaa toimintavapautta arktisella alueella. Pohjoismaista hankittavalla tiedolla pyritään todennäköisesti saavuttamaan etulyöntiasema arktisen alueen strategisten tavoitteiden saavuttamisessa osana suurvaltakamppailua.

Kiinan sotilastiedustelun intressit Pohjoismaissa kohdistuvat aseteollisuuteen sekä sotilaallisiin innovaatioihin. Kerätystä tiedostaan Kiina välittää sotilaallisia asioita koskevat tiedot, kuten tiedot kaksoiskäyttötuotteista ja sotilasteknologisista innovaatioista, niistä vastaaville organisaatioille. Kiinalla on kyky ja resurssit laadukkaaseen ja länsimaista tuttuihin tiedonhankintakeinoihin. Näitä ovat esimerkiksi diplomaatit, tiedustelu-upseerit, värvätyt agentit sekä tekninen tiedustelu.

Kiina on siirtämässä tiedonhankinnan painopistettä teknologia-alalta poliittiseen päätöksentekoon. Tähän vaikuttaa Kiinan menestys teknologian alalla, sekä maan mahdollinen seuraava päämäärä edistää Kiinan intressejä sille suotuisilla kansainvälisillä ja kansallisilla poliittisilla päätöksillä.

Kiinan kansalaisten tekemä tiedustelu ja vakoilu ei lähtökohtaisesti ole kansalaisista itsestään lähtöistä, vaan valtion valvontakeinot ja yhteiskuntajärjestelmä ohjaavat ihmiset tiedonhankkijoiksi. Kiinan tiedustelun tavoitteena on hankkia teknologista osaamista, tietoa poliittisista päätöksistä ja aikeista. Näillä tiedoilla Kiina pyrkii vaikuttamaan kansainväliseen mielipiteeseen, valtioiden poliittiseen päätöksentekoon ja hankkimaan itselleen taloudellisia etuja. Kaiken takana vaikuttaa Kiinan intressi vankistaa valtaansa maailman suurvaltojen joukossa.

5.2 Lähdekritiikki

Tiedustelu- ja turvallisuuspalveluiden lähteet ovat luotettavia ja niiden takana on todennäköisesti laadukasta analyysiä ja ammattimaisia tiedonhankintakeinoja. Analyysin näkökulmasta ne ovat hyvin samansuuntaisia eivätkä tuo maantieteellisten erojen lisäksi uutta tietoa tai kilpailevia näkemyksiä. Moni raportin lähteistä on Yhdysvalloista, mutta niistä voidaan tehdä johtopäätöksiä myös Pohjoismaihin. Johtopäätöksien avulla tuotetut ajatukset Pohjoismaissa tapahtuvaan tiedusteluun sisältävät kirjoittajien näkemyksiä. Raportin teossa käytetyt lähteet eivät mahdollistaneet pääsyä käsiksi primäärilähteisiin.

Käytetyissä lähteissä näkyy niiden tekijöiden käsitys käsiteltävästä aiheesta. Taustalla voivat vaikuttaa kirjoittajien omat ennakkokäsitykset tutkittavasta ilmiöstä. Ilman läpinäkyvää tutkimusprosessia on mahdotonta arvioida lopputulosta täysin kriittisesti. Raportissa käytettyjen tutkimusten tekijät selviävät teksteistä ja heidän koulutustasonsa voidaan sen kautta varmentaa. Lähteiden taustalla olevat organisaatiot ovat luotettavia, mutta eivät kovin läpinäkyviä. Organisaatioiden luottamus perustuu pitkälti niiden asemaan yhteiskunnassa. Lähteiden ollessa länsimaisia myös länsimaiset narratiivit voivat heijastua lähteisiin ja niiden tulkintaan.

Lähdeaineiston perusteella Kiinassa vuonna 2015 toteutettu organisaatiouudistus on osin jättänyt avoimia kysymyksiä siitä, miten tiedustelu on organisoitu uudessa rakenteessa. Täten tarkkaa kuvaa Kiinan tiedustelun toiminta-ajatuksesta ei kyetä vielä muodostamaan. Pääosa lähteistä on peräisin vuosilta 2010–2022, jolloin tietoa voidaan pitää edelleen relevanttina.

Lähteet

Politiets Efterretningstjeneste (2022): Illegal procurement. https://pet.dk/en/illegal-procurement, luettu 24.11.2022.

Bazarkina, D. Yu (2020): Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States. PubMed Central. [https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9492455/], luettu 24.11.2022.

Bazarkina, D. Yu (2020): Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States. PubMed Central. [https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9492455/], luettu 24.11.2022.

Centre for Cyber Security (2022): Threat Assessment: The cyber threat against Denmark 2022. [https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/CFCS-the-cyber-threat-against-denmark-2022.pdf], luettu 24.11.2022

China Law Translate (2022a): Cybersecurity Law. [https://www.chinalawtranslate.com/en/2016-cybersecurity-law/], luettu 28.11.2022.

China Law Translate (2022b): Counter-Espionage Law. [https://www.chinalawtranslate.com/anti-espionage/?lang=en], luettu 28.11.2022.

China Law Translate (2022c): National Security Law. [https://www.chinalawtranslate.com/2015nsl/?lang=en], luettu 28.11.2022.

Confucius Institute (2022): Konfutse-instituutti. Helsingin yliopisto. [https://blogs.helsinki.fi/confucius-institute/confucius-institute/konfutse-instituutti/], luettu 24.11.2022.

Danish Defence Intelligence Service (2021): Intelligence outlook 2021. Copenhagen December 2021. [https://www.fe-ddis.dk/globalassets/fe/dokumenter/2021/udsyn/-fe-udsyn-uk_final_samlet_fredag-.pdf]

Euroopan komissio (2020): Euroopan teollisuusstrategia. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_fi], luettu 24.11.2022.

Eurostat (2022): Education and training database. [https://ec.europa.eu/eurostat/web/education-and-training/data/database], luettu 23.11.2022.

Federal Bureau of Investigation (2022): What we investigate. [https://www.fbi.gov/investigate/counterintelligence/the-china-threat], luettu 23.11.2022.

Government of Canada (2018): China's intelligence law and the country's future intelligence competitions. [https://www.canada.ca/en/security-intelligence-

service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html], luettu 22.11.2022.

Havens Heljar & Seland Johan Martin (2019): The increasing security focus in china's arctic policy. The Arctic Institute. [https://www.thearcticinstitute.org/increasing-security-focus-china-arctic-policy/], luettu 25.11.2022.

Kangasluoma, Emilia (2022): Kiinan rahoittama Konfutse-instituutti lopettaa Helsingin yliopistossa. Helsingin Sanomat, kesäkuu 2022. [https://www.hs.fi/kaupunki/art-2000008893823.html], luettu 28.11.2022.

Kettunen, Ossi (toim.) (2022); Iloniemi Jaakko, Koivurova Timo, Kopa Sanna, Lassenius Oscar, Rautala Ari, Sirviö Heikki, Toveri Pekka, Tynkkynen Veli-Pekka, Väätänen Vesa & Ylärinne Hannu: Arktisen alueen geoplitiikka 2000-luvulla. Maanpuolustuskorkeakoulu, Sotataidonlaitos, Julkaisusarja 2: Tutkimusselosteita NRO 17, 2022 Helsnki.

Kielitoimiston (2022): Politbyroo. [https://www.kielitoimistonsanakirja.fi/#/politbyroo], luettu 25.11.2022.

Kokkonen, Yrjö (2020): Kiina painostaa voimakkaasti Ruotsin tiedotusvälineitä. YLE Uutiset, 2020. [https://yle.fi/a/3-11164777], luettu 24.11.2022.

Lawrence, Susan (2021): China's Political System in Charts: A Snapshot Before the 20th Party Congress. Congressional Research Service, R46977, Marraskuu 2021. [https://crsreports.congress.gov/product/pdf/R/R46977], luettu 25.11.2022.

Liski, Jarno (2020): Suojelupoliisi Kiinan tiedustelusta Suomessa: Vieraanvaraisia kutsuja seminaareihin, tutkimusrahoitusta, investointeja. Suomen Kuvalehti, Helmikuu 2020, [https://suomenkuvalehti.fi/kotimaa/suojelupoliisi-kiinan-tiedustelusta-suomessa-vieraanvaraisia-kutsuja-seminaareihin-tutkimusrahoitusta-investointeja/?shared=1112477-9c8a8801-999], luettu 24.11.2022.

McFadden Cynthia; Aliza Nadi & N.C. Courtney McGee (2018): Education or espiongae? A Chinese student take his homework home to China. NBCNews, 2018. [https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881], luettu 24.11.2022.

Ministry of education, The Peoples's Republic of China (2020): China's education spending for 2019. [http://en.moe.gov.cn/news/press_releases/202006/t20200622_467671.html], luettu 23.11.2022.

Mulvenon, James (2022): Threats to US National Security: Countering PRC's Economic and Technological Plan for Dominance. Senate Select Committee on Intelligence, Maaliskuu 2022. [https://www.intelligence.senate.gov/sites/default/files/documents/os-jmulvenon-051122.pdf], luettu 28.11.2022.

Norwegian directorate for higher education an skills (2022): Study in Norway - Tuition fees for students outside EU/EEA and Switzerland. [https://studyinnorway.no/node/2724], luettu 24.11.2022.

Office of the Strategy of Defence (2020): Military and Security Developments Involving the People's Republic of China 2020. [https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF], luettu 22.11.2022.

Osipova, Elsa (2021): Supo: Eduskuntaan kohdistunut vakoilu viittaa Kiinaan – poliisin mukaan verkkovakoilulla on yritetty kalastella tietoja vieraalle valtiolle. Yle Uutiset, 2021. [https://yle.fi/a/3-11843261], luettu 25.11.2022.

Ping Su, Lanteigne Marc (2015): China's developing arctic policies: Myths and misconceptions. Aalborg University Press.

Politiets Efterretningstjeneste (2021): Assessment of the espionage threat to Denmark. [https://pet.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vsd_uk.pdf], luettu 24.11.2022.

Politiets Efterretningstjeneste (2022): Illegal procurement. https://pet.dk/en/illegal-procurement, luettu 24.11.2022.

Politiets Efterretningstjeneste (2022a): Espionage. [https://pet.dk/en/espionage], luettu 24.11.2022.

Politiets Efterretningstjeneste (2022b): Illegal foreign interference. [https://pet.dk/en/illegal-foreign-interference], luettu 24.11.2022.

Politiets Sikkerhetstjeneste (2022): National Threat Assessment for 2022. [https://pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-engelsk.pdf]

Puranen, Matti & Jukka Aukia (2022): Finland's China Shift. The Diplomat, 2022. [https://thediplomat.com/2022/02/finlands-china-shift/], luettu 24.11.2022.

Puranen, Matti (2016): Kiinan ulko- ja sotilaspolitiikka muutoksessa. Maanpuolustuskorkeakoulu, Sotataidonlaitos, Helsinki 2016. (https://www.doria.fi/bitstream/handle/10024/123580/Puranen2%28net%29.pdf?sequence=2&isAllowed=y), luettu 25.11.2022.

Puranen, Matti (2017): Kansanvaltaa kiinalaisittain: maailman suurin parlamentti kokoontuu parhaillaan Pekingissä. The Ulkopolitist. [https://ulkopolitist.fi/2017/03/10/kansanvaltaa-kiinalaisittain-maailman-suurin-parlamentti-kiinan-kansankongerssi-kokoontuu-parhaillaan-pekingissa/], luettu 25.11.2022.

Puranen, Matti (2020): Kiinan vaikutusoperaatioiden "taika-ase" toimii myös Suomessa. The Ulkopolitist. [https://ulkopolitist.fi/2020/02/23/kiinan-vaikutusoperaatioiden-taika-ase-toimii-myos-suomessa/], luettu 24.11.2022.

Rantalainen, Elina (2021): Valtaosa Lahden ensimmäisistä kandiopiskelijoista tulee Kiinasta – tavoite on houkutella huippuosaajia myös jäämään Suomeen. Yle Uutiset, 2021. [https://yle.fi/a/3-12091209], luettu 23.11.2022.

Rognerud, Knut (2020): Omfattande påtryckningsarbete mot svenska medier från Kina. SVT Nyheter, 2020. [https://www.svt.se/nyheter/utrikes/omfattande-patryckningsarbete-mot-svenska-medier-fran-kina], luettu 24.11.2022.

Statista (2022): Number of students from China going abroad for study from 2010 to 2020. [https://www.statista.com/statistics/227240/number-of-chinese-students-that-study-abroad/], luettu 24.11.2022.

Statistiska centralbyrån (2017): Universitet och högskolor: Internaltionell studentmobilitet i högskolan 2016/17. [https://www.uka.se/download/18.25e0981c160509744a21334/1513614099676/SM1703-internationell-studentmobilitet-2016-17.pdf].

Suojelupoliisi (2021a): Vuosikirja 2021. SUPO, Helsinki 2021a.

Suojelupoliisi (2021b): Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. SUPO, Helsinki. [https://supo.fi/-/ulkomaiset-tiedustelupalvelut-kayttavat-yritysten-ja-yksityishenkiloiden-verkkoreitittimia-kybervakoiluun], luettu 25.11.2022.

Suojelupoliisi (2022a): Kansallisen turvallisuuden katsaus: Tiedustelu ja vaikuttaminen. SUPO, Helsinki. [https://supo.fi/tiedustelu-ja-vaikuttaminen], luettu 25.11.2022.

Suojelupoliisi (2022b): Tiedustelu ja vaikuttaminen. SUPO, Helsinki. [https://supo.fi/tiedustelu-ja-vaikuttaminen]. Luettu 23.11.2022.

Suojelupoliisi (2022c): Suojelupoliisi tunnisti eduskuntaan kohdistuneen kybervakoiluoperaation APT31:ksi. SUPO, Helsinki. [https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi], luettu 25.11.2022.

Sutter, Karen (2021): China's Recent Trade Measures and Countermeasures: Issues for Congress. Congressional Research Service, R46915, 2021. [https://crsreports.congress.gov/product/pdf/R/R46915], luettu 28.11.2022.

Sverige Forsvarsmakten (2021): MUST Årsöversikt 2021 - Militära underrättelse- och säkerhetstjänsten. (https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/musts-arsoversikt-2021-.pdf) Luettu 23.11.2022.

Säkerhetspolisen (2021): Årsbok 2021. [https://www.sakerhetspolisen.se/download/18.650ed51617f9c29b552287/1649683389251/Sakerhetspolisen_arsbok%202021.pdf], luettu 24.11.2022.

The Times Higer Education (2022): World University Ranking 2022. [https://www.timeshighereducation.com/world-university-rankings/2022/world-

ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats], luettu 23.11.2022.

Tilastokeskus (2022): Väestönrakenne. [https://www.tilastokeskus.fi/tup/suoluk/suoluk_vaesto.html#V%C3%A4est%C3%B6%20syntyper%C3%A4n,%20syntym%C3%A4maan%20ja%20kielen%20mukaan], luettu 23.11.2022.

Turunen, Ilkka (2019): Challenges and possibilities in networking in the US. Team Finland Konowledge -webinaarit 26.11.2019, seminaariesitys. [https://www.oph.fi/sites/default/files/documents/ilkka-turunen_washington.pdf], luettu 22.11.2022.

Turunen, Teemu (2021): Korkeakouluyhteistyö Kiinan kanssa - mahdollisuuksia ja uhkakuvia. SUPO, 2021. [https://supo.fi/-/kolumni-korkeakouluyhteistyo-kiinan-kanssa-mahdollisuuksia-ja-uhkakuvia], luettu 25.11.2022.

Turunen, Teemu (2022): Vakoilutapaukset kuohuttavat Pohjoismaissa - tapahtuuko vastaavaa Suomessa? SUPO, 2022. [https://supo.fi/-/vakoilutapaukset-kuohuttavat-pohjoismaissa-tapahtuuko-vastaavaa-suomessa-], luettu 25.11.2022.

U.S.-China Economic and Security Review Commission (2019): Chinese Intelligence Services and Espionage Threats to The United States. [https://www.uscc.gov/sites/default/files/2019-11/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf], luettu 25.11.2022.

Ulkoministeriö (2020): Ulko- ja turvallisuuspoliittinen selonteko. Valtioneuvoston julkaisuja, Helsinki 2020. (https://julkaisut.valtioneuvosto.fi/bitstream/hadle/10024/162513/VN_2020_30.pdf?sequence=1&isAllowed=y). Luettu 25.11.2022.

Valtioneuvos (2021): Puolustusselonteko. Valtioneuvoston julkaisuja, Helsinki 2021. (Valtioneuvoston puolustusselonteko). Luettu 25.11.2022.

Yingying Liu & Hou Yiping (2021): Chinese students in Finland: A qualitative study of employment and further studies afrer graduation. LAB University of Applied Siciences LTD, Bachelor of Business Admistration, 2021.

Yujing Yu (2013): Chinese in Norway - Motivation of transnational chinese students to study aboard in Norway. University of Oslo, Department of culture studies and oriental languages, Master Thesis. Oslo 2013.

Informaatioteknologian tiedekunnan julkaisuja
No. 99/2023

ISBN 978-951-39-9604-8 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO