Liikenteenohjausyhtiöt hybridivaikuttamisen kohteena

17. Turvallisuusjohdon koulutusohjelma

Kehitysprojektin raportti

Jorma Timonen

Finntraffic Meriliikenteenohjaus Oy

Kirkkonummi 10.5.2022

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Hybridivaikuttaminen (laaja-alainen vaikuttaminen, yhdistelmävaikuttaminen) on toimintamalli, jossa yleensä valtiollinen toimija pyrkii vaikuttamaan kohteeksi valitsemaansa organisaatioon tai valtioon saadakseen sen toimimaan vaikuttajatahon pyrkimyksiä edistävästi. Määritelmällisesti hybridivaikuttaminen on sen kohteeksi joutuvan näkökulmasta negatiivinen ilmiö, jossa kohde yritetään saada toimimaan omien etujensa vastaisesti vaikuttajatahon hyväksi.

Laaja-alaisessa vaikuttamisessa käytetään monipuolisesti erilaisia keinoja, joilla kohteen sisäistä yhtenäisyyttä ja päätöksentekokykyä pyritään heikentämään. Käytettäviä keinoja ovat muun muassa informaatiovaikuttaminen, kyberoperaatiot, taloudellinen vaikuttaminen ja vaalivaikuttaminen. Vaikuttajatahon pyrkimyksenä on toimia salassa ja paljastumatta uutiskynnystä ylittämättä. Tyypillistä vaikuttamiselle on kohteen, usein länsimaisen demokratian, vahvuuksien kääntäminen sitä itseään vastaan, jolloin vaikuttamiseen reagointi on vaikeaa.

Suomessa laaja-alainen vaikuttaminen on jo arkipäivää ja sille altistumisen todennäköisyys kasvaa koko ajan Euroopan turvallisuuspoliittisen tilanteen heikentymisen myötä. Osana julkista sektoria ja suomalaista yhteiskuntaa Fintraffic-konsernikaan ei ole turvassa vaikuttamiselta ja myös sen tulisi huomioida erilaiset vaikuttamisen tavat uhka-analyyseissä ja varautumisen kehitystyössä.

Abstract

Hybrid influencing (wide-ranging influence, combined influence) is an operating model in which a state actor usually seeks to influence the organisation or state of its choice in order to make it act in a way that promotes the aspirations of the influencer. By definition, hybrid influence is a negative phenomenon from the point of view of the object being targeted, in which the target is attempted to act against its own interests in favour of the influencer.

Wide-ranging influence uses a wide range of means to reduce the internal coherence and decision-making capacity of the target. The means used include information influence, cyber operations, financial influence and election interference. The aim of the influencer is to operate in secret and without revealing the news threshold. Typical of influencing is the reversal of the strengths of the target, often western democracy, against itself, making it difficult to react to influence.

In Finland, wide-ranging influence is already commonplace, and the likelihood of exposure to it is constantly increasing as the security policy situation in Europe deteriorates. As part of the public sector and Finnish society, the Fintraffic Group is not safe from influencing either, and it should also take into account different ways of influencing threat analyses and preparedness development.

Sisältö

1 Johdanto

Turvallisuusjohdon koulutusohjelman alkaessa syksyllä 2020 tuli ajankohtaiseksi päättää opintoihin kuuluvan kehitysprojektin aihe. Otin yhteyttä turvallisuuden tehtävissä toimiviin kollegoihini Fintraffic-konsernissa ja pyysin ideoita sopivista aiheista. Tavoitteena oli löytää sellainen ajankohtainen aihe, josta olisi hyötyä koko konsernille ja mahdollistaisi toiminnan kehittämistä tukevien tulosten syntymistä. Konsernin silloinen Chief Information Security Officer (CISO) Anne Hännikäinen ehdotti hybridisotaan liittyvää otsikkoa ja kun vähän aikaa olimme aihetta pallotelleet, päädyin lopulliseen aiheeseen: ”Liikenteenohjausyhtiöt hybridivaikuttamisen kohteena”. Sain myös muita erinomaisia ehdotuksia aiheiksi, mutta tämä sopi parhaiten yhteen myös omien mielenkiinnon kohteideni kanssa. Lisäksi aihe oli koko konsernia koskettava eikä yhteen liikennemuotoon sidottu.

Aloittaessani perehtymisen hybridivaikuttamiseen mieleen hiipi monta kertaa epäilys siitä, että onkohan aihe sittenkään sopiva. Epäilyksiä herätti lähinnä aiheeseen liittynyt keskustelu esimerkiksi mediassa, jossa hybridivaikuttamista kuvailtiin usein lähinnä agenttielokuvista tutuilla keinoilla. Olinko valinnut aiheen, jossa yritän väkisin nähdä sellaisia uhkia, joita muut eivät näe ja jotka voidaan helposti leimata mielikuvituksen tuotteeksi? Venäjän hyökkäys Itä-Ukrainaan ja miehitettyä Krimin vuonna 2014 sekä vuoden 2015 pakolaiskriisi olivat tuossa vaiheessa jo haalistuneet suuren yleisön muistijälkinä taka-alalle.

Vuoden 2021 aikana turvallisuuspolittiinen tilanne Euroopassa kuitenkin muuttui ja kehitysprojektin kirjoitusvaiheessa alkoikin jo vaikuttaa siltä, että olen jo myöhässä aiheeni kanssa. Tammikuussa 2022 uutisoitiin lähes päivittäin Euroopan olevan lähempänä sotilaallista konfliktia kuin kertaakaan 30 vuoden aikana ja talven edetessä hybridivaikuttamiseen viittaavia tapahtumia uutisoitiin viikoittain eri puolilta Eurooppaa. Helmikuussa Suomen ja koko Euroopan turvallisuuspoliittinen toimintaympäristö muuttui yhdessä yössä

Venäjän aloitettua sodan Ukrainaa vastaan. Samalla alkoi aktiivinen keskustelu Suomen ja Ruotsin mahdollisesta jäsenyydestä puolustusliitto NATO:ssa. Maaliskuussa sosiaalisen median kanavissa ja uutisissa asiantuntijoiden voimin pohditaan jatkuvasti sitä, minkälaisia hybridivaikuttamisen keinoja Suomi tulee osakseen saamaan. Enää ei ole syytä pohtia, että saatamme joutua vaikuttamisen kohteeksi, vaan enemmänkin milloin ja minkälaisella intensiteetillä se tapahtuu.

Kehitysprojektin tekemisen aikana perehdyin aiheesta julkaistuihin artikkeleihin, uutisiin ja tutkimuksiin sekä kävin erinomaisia keskusteluita eri alojen asiantuntijoiden kanssa. Aivan alkumetreiltä lähtien tiesin, että haluan keskustella aiheesta ainakin suomalaisten turvallisuusviranomaisten kanssa ja lisäksi oman organisaationi ja liikenteenohjauskonsernia ohjaavien viranomaisten turvallisuudesta vastaavien kanssa. Näiden lisäksi lukemieni artikkeleiden lähdeluetteloiden perusteella tunnistin muutaman asiantuntijan lisää ja onnistuin löytämään aikaa keskusteluille myös heidän kanssaan. Tässä vaiheessa esitän lämpimät kiitokseni kaikille keskusteluissa mukana olleille.

Haastattelut suoritettiin osin kasvotusten mutta vallinneen pandemiatilanteen vuoksi suurimmaksi osaksi etäyhteyksin. Lähetin laatimani kysymykset ja keskustelunaiheet keskustelukumppaneilleni ennakolta luettavaksi ja keskusteluiden yhteydessä tein muistiinpanoja eikä keskusteluita tallennettu muilla tavoin. Haastatteluprosessin aikana pyysin jokaiselta keskustelukumppanilta erikseen luvan nimen käyttämiseen lähdeluettelossa ja lähes kaikki siihen suostuivat. Käytyjen keskusteluiden luonteen ja muutaman haastatellun toiveen mukaisesti vuoksi päätin kuitenkin noudattaa Chatham House Rule -periaatetta ja jättää tekstistä viittaukset haastateltavaan pois. Lähdeluettelossa on siis mainittu lähes kaikki keskustelukumppanit, mutta heihin ei viitata tekstissä.

Tiettyyn organisaatioon kohdistuva hybridivaikuttaminen on aihe, josta kirjoittaessa täytyy olla tarkkana, ettei vahingossa paljasta kyseessä olevan organisaation mahdollisia heikkouksia ja siten anna mahdollisesti vihamieliselle lukijalle mahdollisuutta toimia organisaatiota vastaan. Tämän vuoksi kehitysprojektini loppuraportin julkisessa versiossa ei mennä sellaisiin yksityiskohtiin, joilla voitaisiin toimia Fintraffic-konsernia vastaan. Konsernille toimitettavassa versiossa on mukana sisältöä, joissa käsitellään yksityiskohtaisempia tietoja. Uhkana tällaisessa ratkaisussa on se, että lopputulos on

mauton ja hajuton, diplomaatista jargonia tai muuten niin liukas ettei siitä saa otetta. Tavoitteeni kuin kuitenkin ollut kirjoittaa loppuraportti sillä tavalla, että lukija voisi korvata liikenteenohjausyhtiön millä tahansa muulla organisaatiolla. Liikenteenohjauskonserni toimii siis esimerkkiorganisaationa, mutta olen jokseenkin varma, että samanlaisia havaintoja ja ilmiöitä on muissakin organisaatiossa toimialasta riippumatta huomioiden tietenkin niiden turvallisuuden kypsyystaso. Jos lukijalla herää ajatuksia oman organisaationsa toiminnan kehittämiseksi, olen onnistunut.

Johdannon jälkeen kerron mikä liikenteenohjauskonserni Fintraffic on ja miksi se on olemassa. Sen jälkeen kuvailen lyhyesti mistä hybridivaikuttamisessa on kysymys. Neljäs luku sisältää keskusteluissa esille tulleita ajatuksia ja näkemyksiä Fintrafficista mahdollisena hybridivaikuttamisen kohteena ja sen tähänastista varautumista niihin. Viidenteen lukuun olen koonnut keskusteluista tehtyjä johtopäätöksiä ja kirjannut muistiin ajatuksia Fintrafficin hybridiuhkiin varautumisen kehittämiseksi.

2 Fintraffic-konserni

Fintraffic-konserni on Suomen valtion kokonaan omistama erityistehtäväkonserni, jonka tehtävä on tuottaa liikenteenohjauksen ja -hallinnan palveluita valtakunnallisesti. Konsernin emoyhtiö on Liikenteenohjausyhtiö Fintraffic Oy, joka omistaa kokonaan kaikki neljä tytäryhtiötä: lennonvarmistuksen palveluiden tuottamisesta vastaa Fintraffic Lennonvarmistus Oy, meriliikenteenohjauksen palveluita tuottaa Fintraffic Meriliikenteenohjaus Oy, rautatieliikenteenohjauksen ja -hallinnan palveluita Fintraffic Raide Oy ja tieliikenteen ohjauksen ja -hallinnan palveluita Fintraffic Tie Oy. Emoyhtiön tehtävä on tuottaa yhteiskunnalle liikenteen ekosysteemipalveluita ja yhteisiä tukipalveluita konserniyhtiöiden käyttöön (Fintraffic, 2022).

Konsernille annettu erityistehtävä tarkoittaa käytännössä yhteiskunnan, viranomaisten ja elinkeinoelämän tarvitsemien välttämättömien liikenteenohjauspalveluiden tuottamista. Lisäksi erityistehtäväroolilla varmistetaan liikennejärjestelmässä tarvittavien liikenteenohjauspalveluiden tuottaminen normaaliolojen häiriötilanteissa ja poikkeusoloissa. Erityisenä tehtävänä yhtiöllä on tarjota, ylläpitää ja kehittää liikenteenohjaus- ja hallintapalveluita puolustus- ja turvallisuusviranomaisten tarpeita varten siinä laajuudessa kuin se on näiden lakisääteisten virkatehtävien hoitamiseksi perusteltua. Fintraffic vastaa myös liikenteeseen liittyvän tiedon keruusta, hallinnasta, hyödyntämisestä ja tarjoamisesta tasapuolisesti muille toimijoille uuden liiketoiminnan mahdollistamiseksi. Yhtiöllä on siis valtion määrittelemä yhteiskunta-, elinkeino-, turvallisuus- ja liikennepoliittinen tehtävä (Fintraffic, 2022).

Fintraffic -konserni toimii Liikenne- ja viestintäministeriön omistajaohjauksessa ja sen palveluksessa on noin 1100 henkilöä. Liikenteenohjaustyötä tehdään kaikissa liikennemuodoissa ympäri vuorokauden vuoden jokaisen päivänä, joten suurin osa henkilövahvuudesta on liikennekeskusten operatiivista henkilökuntaa (Fintraffic vuosikatsaus, 2021, s. 43).

Fintraffic-konserni aloitti toimintansa 1.1.2019 kun Väyläviraston (aikaisemmin Liikennevirasto) tuottamat meri-, tie- ja rautatieliikenteen ohjaus- ja hallintapalvelut yhtiöitettiin osaksi valtion kokonaan omistamaa liikenteenohjauskonsernia. Väylävirastosta siirtyneiden osien lisäksi uuteen yhtiöön siirrettiin jo aikaisemmin perustetut ja valtion omistamat rautatieliikenteenohjaus- ja lennonvarmistuspalveluita tuottavat yhtiöt (silloisilta nimiltään Finrail Oy ja Air Navigation Services Finland Oy) (Fintraffic toimintakertomus ja tilinpäätös 2020, 2021, s. 3). Yhtiöittäminen perustui lakiin Liikenneviraston liikenteenohjaus- ja hallintapalveluiden muuttamisesta osakeyhtiöksi 574/2018 ja hallituksen esitykseen HE 34/2018 (Finlex 574/ 2018, 2018).

Fintraffic toimii tiiviissä yhteistyössä laajan asiakas- ja yhteistyökumppaniverkoston kanssa. Yhtiön liikenteenohjauspalveluita hankkivat Väylävirasto (tie-, meri- ja rautatie), Finavia ja lentoyhtiöt (lennonvarmistus). Muita keskeisiä sidosryhmiä ovat Liikenne- ja viestintävirasto Traficom, puolustus- ja turvallisuusviranomaiset, kaupungit, julkisen liikenteen toimijat, tutkimuslaitokset ja eri alojen yritykset. Konsernilla oli 31.12.2021 toimintaa Helsingin, Vantaan, Tampereen, Turun ja Oulun lisäksi 24 muulla paikkakunnalla. Konsernin liikevaihto oli vuonna 2021 209,7 miljoonaa euroa ja liikevoitto 6,1 miljoonaa euroa (Fintraffic, 2022).

Liikenteenohjaustehtävien yhtiöittämisen tärkeimpiä tavoitteita oli kustannustehokkuuden jatkuva parantaminen ja tämä onkin nostettu konsernin strategiseksi tavoitteeksi. Fintraffic on sitoutunut parantamaan palvelutasoaan, yhteiskunnallista vaikuttavuuttaan ja tehostamaan liikenteen ohjauksen palveluntuotantoa operatiivista toimintamallia kehittämällä kumulatiivisesti 30 miljoonaa euroa tulevien vuosien aikana (Fintraffic, 2022).

3 Hybridivaikuttaminen

Hybridivaikuttaminen (josta käytetään myös suomenkielisiä termejä yhdistelmävaikuttaminen ja laaja-alainen vaikuttaminen) on jonkin tahon toteuttamaa tietoista vaikuttamista, joka hyödyntää useampaa kuin yhtä vaikuttamiskeinoa saavuttaakseen tavoitteensa. Hybridivaikuttamisen käsite on laaja ja se kattaa suuren määrän erilaisia vaikuttamisen keinoja, joita ovat esimerkiksi informaatiovaikuttaminen, taloudellinen vaikuttaminen, vaalivaikuttaminen, tieto- ja kyberturvallisuuteen liittyvät operaatiot, sabotaasit infrastruktuuria vastaan ja viime kädessä myös sotilaallisten keinojen käyttö. Leimallista yhdistelmävaikuttamiselle on toimijuuden, keinojen ja tavoitteiden välisen yhteyden hämärtäminen. Uhkan kohteen on vaikea erottaa yhdistelmävaikuttamisen rajoja tai tunnistaa vastuussa olevia tahoja. Toiminnan on tarkoitus olla aluksi ei-tunnistettavaa ja jos toiminta huomataan ja/tai tunnistetaan, sitä ei myönnetä. Toiminta pyritään toteuttamaan niin sanotusti sodan ja rauhan välimaastossa, jotta vastatoimet olisivat mahdollisimman hankalia. Varsin laaja yhteisymmärrys vallitsee siitä, että hybridivaikuttaminen on lähtökohtaisesti valtiollisten toimijoiden harjoittamaa toimintaa, jonka kohteena on sellainen toinen valtio, jonka toimintaan halutaan vaikuttaa. Hybridivaikuttaminen on käsitteenä otettu käyttöön hybridisodankäynnin sijaan silloin kun halutaan painottaa ei-sotilaallisia, piilotettuja toimia. Hybridivaikuttamiselle on tyypillistä, että toimija pyrkii pysymään havaitsemis- ja reagointikynnyksen alapuolella ja toiminnassa luotetaan informaatioaikakaudelle tyypillisesti kaikkialla läsnä olevan digitaaliteknologian mahdollistamaan nopeuteen ja volyymiin (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 5; Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, s. 24; Cullen & Reichborn-Kjennerud, 2017, s. 9).

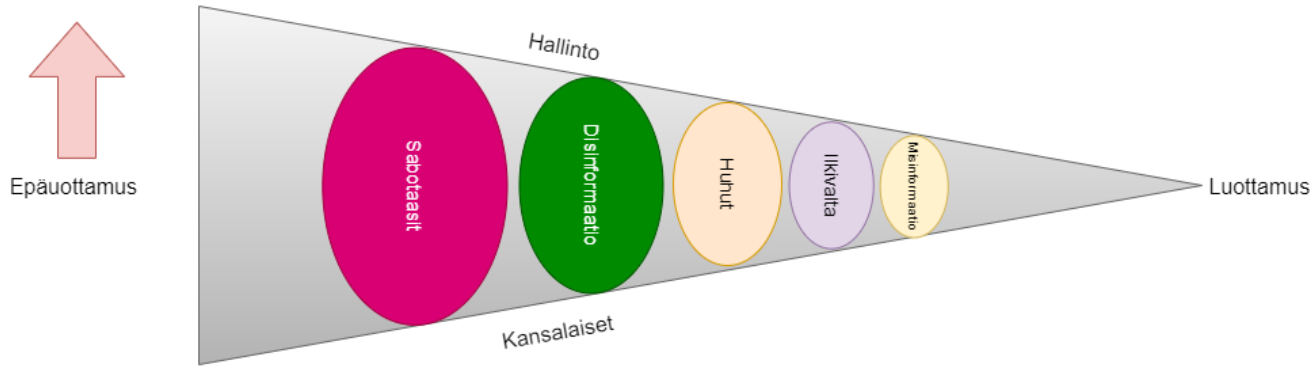
Hybridivaikuttaminen politiikan välineenä viittaa manipuloivaan, ei-toivottuun häirintään, jossa käytetään laajaa keinovalikoimaa; esimerkiksi vääristellyn tai virheellisen tiedon tai vahvojen (mutta väärien tai osittain väärien) historiallisten kertomusten tahalliseen levittämiseen. Tämä tarkoittaa sitä,

että poliittisena konseptina hybridiuhkia voidaan pitää mahdottomina hyväksyä ajatellen suvereenien valtioiden sisäisten asioiden ja tilan loukkaamattomuutta (Giannopoulos;Smith;& Theocharidou, 2021, s. 9).

3.1 Tavoitteet

Mikkolan et. al. mukaan hybridihäirintä voidaan määritellä usean häirintämetodin synkronoiduksi yhteiskäytöksi, jonka tavoitteena on vahvistaa kohdeyhteisöjen sisäisiä jakolinjoja ja yleistä epävakautta. Hybridihäirinnässä on kyse useimmiten piilotetusta kohdevaltioiden strategisten intressien haitallisesta ja vihamielisestä manipuloinnista. Toiminnan ideaalisena tavoitteena on muokata kohdeyhteisön näkemyksiä siten, että se taipuu vapaaehtoisesti ottamaan askelia, jotka edistävät hybriditoimijan agendaa tai vaihtoehtoisesti halvaannuttaa kohdeyhteisön omaa päätöksentekokykyä. Hybridihäirintä ei hyödynnä ”yksi koko sopii kaikille”-lähtökohtaa, vaan se käyttää hyväkseen kohdeyhteisön spesifejä haavoittuvuuksia heikentääkseen kohteen yhtenäisyyttä ja kykyä yhteistoimintaan. Tämän strategian taustalla oleva perusajatus on se, että piilotettu häirintä voi altistaa ja pahentaa kohdeyhteisön omien strategisten intressien ja prioriteettien muodostamiseen liittyviä jakolinjoja ja kiihdyttää kohdeyhteisön erimielisyyksiä suhteessa yleiseen poliittiseen linjaan (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, ss. 25-26).

Yhteiskunnan kriittiset toiminnot voivat olla houkutteleva häirinnän kohde, jos toimija haluaa kiilastrategian (Kuva 1) menettelytapoja noudattaen heikentää luottamusta viranomaisten ja yhteiskunnan toimivuuteen (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, s. 10). Onnistunut vaikuttaminen voi vaikeuttaa poliittisen järjestelmän toimintaa ja sotilaallisen maanpuolustuksen toimintakykyä. Painostuskeinoina voidaan käyttää esimerkiksi poliittisia, taloudellisia tai sotilaallisia keinoja kyberoperaatioita ja informaatiovaikuttamista unohtamatta. Vaikuttamisen tavoitteena ei välttämättä ole suurten aineellisten tuhojen aikaansaaminen, vaan häiriöiden ja levottomuuden aiheuttaminen voi riittää (Savolainen, Working paper on Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?, 2019, s. 16).



Kuva 1: Kiilastrategian periaate, kun tavoitteena on epäluottamuksen lisääminen yhteiskunnassa. Ilmiöt eivät ole tärkeysjärjestyksessä.

Tärkeä vaikuttamisen kohde voivat olla myös turvallisuusviranomaiset, joiden toiminnan luotettavuutta ja toiminnan laillisuutta voidaan kyseenalaistaa. Luottamusta heikentämällä luodaan epävakautta ja hankaloitetaan poliittista päätöksentekoa. Hybridivaikuttamisen keinot muuttuvat nopeasti ja ovat innovatiivisia, uusia työkaluja ja teknologioita hyödynnetään aktiivisesti. Hyökkäystä vastaan puolustautuvan tahon on osattava ennakoida ja pyrkiä näkemään vaikuttamispyrkimysten seuraavat aallot ennalta (Limnéll, 2019).

3.2 Keinovalikoima

Kuten edellä jo todettiin, niin hybridivaikuttamisen keinovalikoima on laaja. Tässä yhteydessä muutamaan yhteiskunnan toimintaan vaikuttamiseen pyrkivään keinoon; informaatiovaikuttamiseen ja taloudelliseen vaikuttamiseen. Kyberoperaatioiota ja vaalivaikuttamista ei kuitenkaan täysin voida sivuuttaa, koska kyberympäristössä tapahtuva vaikuttaminen on niin ilmeinen keino tietoverkkojen toimintaan perustuvassa yhteiskunnassa, ettei sitä voi sivuuttaa. Liikenteenohjausyhtiö Fintraffic puolestaan osana valtiokonsernia elää ja toimii aina kulloinkin vallassa olevan poliittisen suuntauksen perusteella tehtyjen päätösten mukaisesti, joten vaalien tuloksilla on sillekin merkitystä.

Julkisessa keskustelussa ja mediassa näkee toisinaan, että hybridivaikuttamista ja kybervaikuttamista ja -operaatioita käsitellään synonyymeinä. Kyberoperaatiot ovat kuitenkin vain yksi hybridivaikuttamisen keino. Hybridivaikuttamisen yhteydessä puhutaan kiilastrategiasta (Kuva 1), joka tarkoittaa toimintaperiaatetta, jonka tarkoitus on rikkoa kohdevaltiota tai -koalitioita, ja sen kautta heikentää kohteen kykyä vastatoimiin. Hybridivaikuttamista harjoittava taho ei kohtaa kohdettaan ”silmästä silmään” perinteisen sodankäyn-

nin tapaan, vaan toiminnassa hyödynnetään hienovaraisempia häirinnän keinoja. Keinovalikoima voi sisältää esimerkiksi kyberoperaatioita, disinformaation[1] ja misinformaation[2] levittämistä, ääriliikkeiden toiminnan tukemista eri keinoin, vaikuttaja-agenttien värväämistä, poliittisten päättäjien korruptoimista tai taloudellisten houkuttimien tarjoamista (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, s. 26).

Yritys tai muu organisaatio voi olla lopullinen kohde, mutta todennäköisempää on, että sitä käytetään reittinä tai välikappaleena lopulliseen strategiseen tavoitteeseen pyrittäessä. Esimerkiksi liikeyritykseen voi kohdistua vain informaatiovaikuttamista, siihen jonkinlaisessa suhteessa olevaan kohteeseen kybervaikuttamista ja kolmanteen kohteeseen fyysistä vaikuttamista. Se että organisaatio tunnistaa itseensä kohdistuvan vain yhdenlaista vaikuttamista ei sulje pois mahdollisuutta, että yritys on osana laajempaa hybridivaikuttamisoperaatiota (Vesterinen;Fogle;& Eronen, 2018, s. 4).

3.2.1 Operaatiot kyberympäristössä

Kansallisen turvallisuuden kannalta kyberuhat ovat tyypillisesti kriittiseen infrastruktuuriin, valtion päätöksentekoon, maanpuolustukseen tai yhteiskunnan toiminnan häiritsemiseen tähtääviä toimia, joissa hyödynnetään tietoverkkoja. Tyypillisiä piirteitä ovat muun muassa pyrkimys laittomia keinoja käyttäen hankkia tietoa valtionhallinnon päätöksenteosta tai valtion toimintakyvyn kannalta kriittisistä haavoittuvuuksista. Yhtä lailla vaikuttaminen ja tiedonhankinta voi kohdistua myös yrityksiin ja tutkimuslaitoksiin (Sisäministeriö, 2022).

Kybervaikuttamisen keinovalikoimaan kuuluvat myös tietojärjestelmien kaataminen, tietomurrot ja tietojen varastaminen, kriittisen infrastruktuurin häirintä ja lamauttaminen sekä palveluiden ruuhkauttaminen (Harjanne;Muilu;Pääkkönen;& Smith, 2018). Myös näillä keinoilla tavoitellaan epävarmuuden luomista yhteiskuntaan ja luottamuksen rapauttamista

[1] Disinformaatio on tietoisesti jaettua väärää tietoa, jonka motiivina voi olla muun muassa: poliittinen ja yhteiskunnallinen vaikuttaminen, taloudellinen hyöty (klikkaukset, kuluttajan harhauttaminen), ilkivalta, pilailu

[2] Misinformaatio on puutteellista tai väärää tietoa, jota annetaan epähuomiossa eikä tarkoitus ole tahallisesti johtaa harhaan.

julkiseen sektoriin ja poliittisiin päättäjiin. Sen lisäksi tavoitteena voi olla tietojen kerääminen myöhempiä operaatioita varten tai taloudellisen hyödyn saamiseksi.

Kiristyshaittaohjelmia käytetään organisaation tai yksityishenkilöiden tietokoneiden kaappaamiseen tai tietojen varastamiseen. Onnistuneen kaappauksen jälkeen vaaditaan maksua laitteiden hallinnan tai tietojen palauttamiseksi oikealle omistajalleen. Kiristyshaittaohjelmien toteutuksessa hyödynnetään ohjelmistoissa ja käyttöjärjestelmissä olevia haavoittuvuuksia ja ihmisten vakiintuneita toimintamalleja. Kiristyshaittaohjelmia pidetään tällä hetkellä kaikkein huomattavimpina kyberuhkina. Kiristysten taloudelliset kustannukset vaihtelevat organisaation koon ja tietovuodon vakavuuden mukaan, mutta kustannukset saattavat helposti nousta miljoonaluokkaan (F-Secure, 2022).

3.2.2 Informaatiovaikuttaminen

Historiallisina aikoina tieto levisi suusta suuhun ja myöhemmin kirjapainotaidon leviämisen jälkeen myös kirjallisena. Suullisen tiedon leviäminen vaati ihmisten kohtaamisia kasvotusten tai myöhemmin esimerkiksi puhelimitse. Joka tapauksessa viesti kulki ihmisjoukossa ja mukana olleet ns. tolkun ihmiset karsivat hurjimmat huhut, esimerkiksi kirkossa pappi saattoi toimia tiedonvälittäjänä ja vaikutti siihen millä tavalla tieto tuotiin julki. Tietotekniikan myötä erityisesti tiedonkulun nopeus ja henkilökohtaiset mahdollisuudet valita käytettävät kanavat ja mediat on muuttanut viestintää. Internetin aikakaudella tieto liikkuu valon nopeudella ja vastaanottajana voi olla kuka tahansa, jolla on käytössään tarvittavat työkalut, esimerkiksi älypuhelin. Vastuu tiedon tulkinnasta on siirtynyt sen vastaanottajalle eikä vastaavia suodattimia tai tulkitsijoita entisaikojen tapaan enää ole.

Tiedonkulun nopeutuminen ja moderni viestintäteknologia ovat mahdollistaneet tavallisten kansalaisten aikaisempaa aktiivisemman osallistumisen ja osallistaminen tiedon jakamiseen. Samalla tavalliset kansalaiset ovat myös tulleet vaikuttamiseen pyrkivälle taholle (viholliselle) näkyviksi kohteiksi ja potentiaalisiksi maalittamisen kohteiksi. Aikaisemmin maalittamisen kohteeksi joutuivat yleensä avainhenkilöt, mutta nyttemmin maalikirjo on laajentunut suureen yleisöön. Enää suureen yleisöön ei tarvitse vaikuttaa vain epäsuorasti esimerkiksi median tai poliitikkojen kautta (Jantunen, 2015, s. 31).

Suomessa lehdistönvapaus on edelleen hyvä ja Toimittajat ilman rajoja järjestön vuosittaisessa lehdistönvapausindeksissä Suomi oli vuonna 2020 toisella sijalla (Suomen journalistiliitto, 2021). Vaikka lehdistönvapauden tilanne on hyvä, niin toimittajiin kohdistuva häirintä saattaa vaikuttaa siihen mitä kirjoitetaan, miten kirjoitetaan tai jätetään kirjoittamatta. Toistuvat määrätietoiset ja kampanjamaiset häirintätoimet voivat johtaa siihen, että toimittajat tai tutkijat alkavat välttämään tietyistä aiheista kirjoittamista (Niemi, 2021).

Sosiaalisen median kanavia voidaan hyödyntää myös toimijan maineen tai osaamisen mustamaalaamiseen. Sen lisäksi huolimattomuudella tai tarkoituksellisesti julkaistuja kuvia esimerkiksi henkilön kulkuluvista tai muista tunnisteista voidaan hyödyntää, kun tarkoituksena on tunkeutuminen organisaation fyysisiin toimitiloihin (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 8).

Onnistuessaan informaatiovaikuttaminen heikentää luottamusta viranomaisiin tai muihin julkisiin toimijoihin ja sen myötä tasoittaa tietä muiden vaikuttamiskeinojen käytölle. Sosiaalinen media on voimistanut samanmielisten ”kuplautumista” ja siten ollut edesauttamassa keskustelun polarisoitumista, joka myös ruokkii epäluottamusta. Vaikutelma siitä, että jossakin asiassa olisi vain kaksi ääripäätä voi vahvistaa ulkopuolisen vaikuttajan toimintaa tai olla seurausta siitä. Informaatiovaikuttaminen kestää kauan ja sen vaikutukset saatetaan nähdä vasta pitkän ajan kuluttua (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 16).

3.2.3 Taloudellinen vaikuttaminen

Taloudellisen vaikuttamisen tavoitteena on saada kohde toimimaan tavalla, jolla se ei muuten toimisi. Pakotteet (keppi) ja toisaalta rahoituksen tarjoaminen kehityshankkeille (porkkana) ovat keinoja, kun vaikuttamiseen pyrkivä taho edistää tavoitteitaan (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, s. 39).

Taloudellisen vaikuttamisen keinot voivat olla suuria, mittakaavaltaan massiivisia investointihankkeita tai pienempiä yhteiskunnan arjen toimintaan liittyviä. Esimerkiksi Kiinan silkkitiehanketta (Belt and Road Initiative), voidaan hyödyntää ulkoisen vaikutusvallan lisäämisessä tavalla, joka tekee kohdeval-

tiosta riippuvaisen hybriditoimijan kyvystä hallita syntynyttä infrastruktuuria. Tämä puolestaan voi johtaa kohdevaltion suvereniteetin alenemiseen (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, s. 29).

Julkisen sektorin organisaatiot tukeutuvat toiminnassaan yhä vahvemmin alihankkijoihin ja ulkoistettuihin palveluihin. Markkinaehtoisesti toimivat organisaatiot julkisen sektorin palveluiden tuottajina ja pitkien alihankintaketjujen aiheuttama epävarmuus huoltovarmuudelle on nykyajan ilmiö, jonka hallitseminen on vaikeaa. Palvelun tilaajan tulisi olla perillä alihankkijana toimivan yrityksen taustoista, tilanteesta (esim. taloudellinen asema, mahdolliset riippuvuussuhteet) ja alihankintaketjuista. Joskus voi olla tarpeen sopimuksellisesti rajoittaa alihankintaketjun pituutta. Tämä korostuu kriittisen infrastruktuurin kohteissa, esimerkiksi logistiikassa (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018, ss. 47-48).

3.2.4 Vaalivaikuttaminen

Viime vuosien tunnetuimpia tapauksia vaalivalittamisen saralla ovat vuoden 2016 presidentinvaalit Yhdysvalloissa, Ison-Britannian Brexit-äänestys ja vuoden 2017 vaalit Ranskassa. Vaalivaikuttamisessa keinona käytetään tyypillisesti informaatiovaikuttamista, kun kohdevaltion vaalitulokseen pyritään vaikuttamaan ja saamaan tavoitteiden mukainen ehdokas menestymään.

Yhdysvaltain vaalien aikaista vaikuttamista on tutkittu analysoimalla suuria Twitter- ja Facebook-aineistoja. Tulosten perusteella valeuutisia ja disinformaatiota kohdistettiin Twitterissä erityisesti avainosavaltioihin. Facebookin ja Twitterin kautta kohdennettiin valeuutisia ja salaliittoteorioita varsinkin sotaveteraaneihin (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018).

Yhdysvaltain vuoden 2016 vaalien aikaan venäläiset sosiaalisen median tilit organisoivat maahanmuutto- ja muslimivastaisia tilaisuuksia, jotka toistivat tehokkaasti Donald Trumpin vaaliteemoja. Facebookista ostettiin mainostilaa, Twitterissä levitettiin disinformaatiota ja Hillary Clintonia mustamaalaavia videoita tilattiin vloggareilta ja julkaistiin Youtubessa. Kaikki nämä on jälkeenpäin yhdistetty venäläisiin toimijoihin (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018).

Ranskassa EU-myönteisen presidentti Emmanuel Macronin kampanjaa häirittiin julkaisemalla hänen yksityiselämäänsä koskevia perättömiä väitteitä ja

hänen sanottiin olevan vieraan vallan agentti. Lisäksi Macronin sähköposti hakkeroitiin ja viestejä vuodettiin julkisuteen. Vaikuttamisen tulokset olivat heikompia kuin Yhdysvalloissa, koska kampanja oli osannut varautua vaikuttamiseen.

3.3 Demokratiaa uhataan sen omilla vahvuuksilla

Hybridivaikuttamisen yhteydessä oleellisen tärkeää on ymmärtää se, että vaikuttamisen kohteeksi joutuvaa liberaalia länsimaista demokratiaa uhataan sen omilla vahvuuksilla; esimerkiksi vapaalla tiedonvälityksellä, laajoilla yksilönvapauksilla ja mielipiteen ilmaisulla sekä vapaalla markkinataloudella. Näitä ominaisuuksia hyödyntävää vihamielistä tahoa on vaikea pysäyttää, koska demokratian oma lainsäädäntö estää sen. Sen vuoksi demokratian näkökulmasta resilienssin kehittäminen näitä vaikutuskanavia vastaan on tullut ajankohtaiseksi niin valtion kuin organisaatioidenkin tasolla (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018).

Omanlaisensa kyberkeino on myös lainsäädännön tuomien oikeuksien väärinkäyttö. Esimerkiksi EU:n yleinen tietosuoja-asetus mahdollistaa ihmisille itseään koskevien tietojen pyytämisen niitä säilyttäviltä organisaatioilta. Asetusta voisi hyödyntää palvelunestohyökkäyksessä ruuhkauttamalla kohteena oleva organisaatio tuhansilla yhtäaikaisilla tietopyynnöillä. Organisaatio on lain edessä velvollinen reagoimaan jokaiseen pyyntöön. Tällainen tilanne voidaan aiheuttaa informaatiovaikuttamisoperaatiolla: vihamielinen toimija syöttää disinformaatiota, joka ylittää uutiskynnyksen ja käyttää sosiaalista mediaa tiedon tuottajana ja generoijana. Kuvitteellisessa esimerkissä organisaation väitetään käsittelevän henkilötietoja väärin. Toimija voisi vedota tunteisiin, jotta saisi mahdollisimman paljon ihmisiä pyytämään tietojaan organisaatiolta lyhyen ajan sisällä. Voitaisiin virheellisesti väittää esimerkiksi, että lapsia koskevia tietoja käytetään organisaatiossa jollain tavalla väärin tai arveluttavasti. Jos tai kun organisaatio ei pysty kaikkiin pyyntöihin vastaamaan, voidaan asiasta kannella laillisuusvalvojille ja saada sieltä langettava päätös, joka heikentää organisaation mainetta ja antaa lisää mahdollisuuksia vaikuttamiselle. Vastaavia altistavia velvoitteita voi syntyä erilaisia palvelulupauksia linjattaessa (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 13).

3.4 Hybridivaikuttamisen konsepti

Teoksessa The Landscape of Hybrid Threats: A Conceptual Model (Giannopoulos;Smith;& Theocharidou, 2021) esitellään hybridivaikuttamisen analyyttinen viitekehys ja sen elementit. Viitekehykseen kuuluu neljä osa-aluetta, joiden välisten suhteiden ja vuorovaikutuksen ymmärtäminen auttaa hahmottamaan hybridivaikuttamisen käsitettä. Nämä osa-alueet ovat toimijat (actor) ja niiden strategiset tavoitteet, toimijan käyttämät työkalut (tools), toimijoiden kohteet (domains) ja toiminnan vaiheet (phases) mukaan lukien eri vaiheissa havaittavat toimet (activity). Viitekehys on koottu havainnolliseksi kuvaksi (Kuva 2), jota voidaan yhdessä organisaation hankkiman tiedon kanssa hyödyntää riskienarvioinnin ja resilienssin kehittämisen työkaluna. Kuvassa on huomioitu myös ajallinen ulottuvuus strategisen vaikuttamisen valmistelusta (priming), epävakauden (destabilization) luomisen kautta pakottamiseen (coercion).

On syytä pitää mielessä, että kukin toimija valitsee sellaisen työkaluvalikoiman, joka parhaiten tukee sen tavoitteiden saavuttamista. Tavoitteena kuitenkin loppujen lopuksi on kohteen päätöksentekokyvyn heikentäminen. Työkalujen käyttö voidaan kohdistaa yhteen tai useampaan kohteeseen tai niiden välisiin rajapintoihin. Tavoite voidaan saavuttaa joko valittujen työkalujen suoralla käytöllä tai luomalla kasautumisvaikutuksia.

4 Asiantuntijanäkemyksiä

Keskusteluissa asiantuntijoiden kanssa kävi selväksi, että laaja-alainen vaikuttaminen on Suomessa jo arkipäivää ja Liikenteenohjausyhtiö Fintraffic tulee väistämättä saamaan osansa siitä viimeistään sitten, kun turvallisuuspoliittinen tilanne Suomen lähialueilla muuttuu. Haastattelut tehtiin kesän ja alkusyksyn 2021 aikana, jolloin elettiin vielä jokseenkin rauhallista aikaa. Asiantuntijoiden kanssa käydyissä keskusteluissa oli kuitenkin havaittavissa, että pinnan alla kuplii jo – oli tavallaan tyyntä myrskyn edellä. He osasivat osoittaa uutisvirrasta sellaisia signaaleja, joiden perusteella myöhemmin realisoitunut sota Ukrainassa oli looginen jatkumo aikaisemmille tapahtumille.

Keskusteluissa keskityimme pohtimaan hybridivaikuttamista ilmiönä yleisellä tasolla, käsittelemään erilaisia havaintoja käytetyistä metodeista ja arvioimaan Fintraffic -konsernin asemaa suomalaisessa yhteiskunnassa hybridivaikuttamisen näkökulmasta. Monessa kohdin keskusteluita viitattiin edellä kuvattuihin kirjallisuudesta ja tutkimusjulkaisuissa kuvattuihin ilmiöihin.

4.1 Toimintamalleja ja uhkia

Hybridivaikuttaminen ei ole uusi ilmiö, samankaltaisia keinoja on käytetty valtioiden välisissä konflikteissa jo vuosisatoja (Giannopoulos;Smith;& Theocharidou, 2021). Iso muutos on kuitenkin tapahtunut tieto- ja viestintätekniikan muutoksen myötä, kun yhä pienemmällä panoksella on mahdollista saavuttaa yhä suurempi yleisö. Suomella on naapurimaanaan Venäjä, jolla on kolmensadan vuoden kokemus hybridivaikuttamisesta ja sen sanotaankin olevan maailman paras tällä alalla. Venäläiseen strategiseen ajatteluun kuuluu vahvasti refleksiivisen kontrollin käsite, jonka tavoite on vaikuttaa kohteen päätöksentekoon ja saada se toimimaan (hyvässä uskossa) oma etunsa vastaisesti. Kylmän sodan aikainen suomettumisilmiö ja YYA-sopimus ovat esimerkkejä tästä.

Suomi on Neuvostoliiton hajoamisen jälkeen viimeisten kolmenkymmenen vuoden ajan asemoitunut yhä kiinteämmin läntiseen arvoyhteisöön ja läntiset demokratiat ovat jo pidemmän aikaa olleet aktiivisen hybridivaikuttamisen kohteena. Vaikuttamista harjoittavat valtiot ja muut ideologisesti tai uskonnollisesti yhtenäiset, mutta länsimaisten demokratioiden kanssa vastakkaiset ryhmät. Läntisiin demokratioihin kohdistuvaa vaikuttamista harjoittavilla tahoilla on paljon yhteistä: ne ovat tyypillisesti diktatuureja tai muuten ei-demokraattisia järjestelmiä, joissa vallanpitäjien ei tarvitse miellyttää äänestäjiä pysyäkseen vallassa. Lisäksi ne eivät jaa ja kunnioita läntisiä arvoja kuten tasa-arvoa, humanismia, sananvapautta tai vapaata lehdistöä. Arvojen erilaisuuden vuoksi vaikuttamisessa on mahdollista käyttää keinoja, joita länsimaisissa demokratioissa pidetään ei-toivottuina. Tällaisia ovat esimerkiksi harhaanjohtavien väitteiden keksiminen ja levittäminen tosina sekä valehtelu niin omalle kansalle kuin ulkomaillekin ilman pelkoa äänestäjien reaktioista tai rikosoikeudellisista seuraamuksista. Hybridivaikuttamisessa sananvapautta käytetään väärin julkaisemalla omia tavoitteita edistävää aineistoa ilman sanavapauden kanssa käsi kädessä kulkevaa vastuuta.

Kun Suomessa tai jossain muussa läntisessä demokratiassa julkaistaan uutta lainsäädäntöä, niin muiden valtioiden edustustojen kiinnostus on suurta. Edustuston asiantuntijat perehtyvät lakiin syvällisesti ja etsivät siitä omiin tarkoitusperiinsä sopivia mahdollisia vaikuttamiskanavia, heikkoja kohtia ja viranomaisten toimivaltuuksien rajoja ja rajapintoja. Tätä tietoa hyödynnetään, kun on tarve jollain tavalla vaikuttaa kohdemaassa, kiinalaiset käyttävät menettelytavasta termiä ”legal warfare”.

Yleisesti länsimaissa ja erityisesti Suomessa viranomaiset noudattavat lakia ja pitävät kiinni toimivaltuuksiensa rajoista. Kun vaikuttajataho on hyvin selvillä toimivaltuuksien rajapinnoista, voidaan toimet kohdistaa niihin. Viranomaisten aikaa kuluu toimivaltarajojen selvittämiseen, jolloin reagointi varsinaiseen toimintaan viivästyy. Samalla viranomainen voi suurelle yleisölle näyttäytyä tehottomana, valmistautumattomana ja osaamattomana, mikä luo uusia mahdollisuuksia negatiiviseen ja valheelliseen uutisointiin (ja toimii syötteenä informaatiovaikuttamiselle). Tästä saatiin runsaasti esimerkkejä vuosina 2020 ja 2021 COVID19 -pandemian yhteydessä, kun suomalaiset viranomaiset joutuivat kokonaan uuteen tilanteeseen ja toimivallan rajoja koeteltiin eri sektoreilla. Erilaisiin viranomaisten virheisiin, kömmähdyksiin ja ristiriitaisuuksiin tartuttiin hanakasti ja etenkin sosiaalisessa mediassa tietoa

levitettiin laajasti. Samaan aikaan myös ahkerasti levitetyillä ”rokotekriittisillä” näkemyksillä pyrittiin nakertamaan viranomaisten asiantuntemusta ja näitä ajatuksia levittivät erityisesti yhteiskuntaan muutenkin kriittisesti suhtautuvat tahot, kuten populistiset ja äärioikeistolaiset toimijat. Näiden toimien uutisoinnin ja analysoinnin yhteydessä on esitetty arveluja siitä, että niitä masinoitiin ja voimistettiin tarkoituksellisesti Suomen ulkopuolelta tavoitteena Suomen sisäisten jakolinjojen vahvistaminen kiilastrategian mukaisesti.

4.2 Kohteena Fintraffic

Lähes kaikki haastatellut totesivat, että liikenteenohjausyhtiöitä voidaan varmuudella pitää hybridivaikuttamisen kohteina. Kohteeksi ei päädytä niinkään siksi, että kysymys on Fintrafficista yhtiönä vaan houkuttelevuus syntyy sen roolista osana valtiokonsernia ja tehtävien luonteesta. Julkisen sektorin organisaationa, osana yhteiskuntaa ja sen kriittiseksi katsottuja toimintoja konserni tekee oman osansa Suomen kokonaisturvallisuuden hyväksi. Kun jokin vieras Suomen ulkopuolinen taho haluaa vaikuttaa yhteiskuntamme toimintaan ovat kohteena laajasti organisaatiot yhteiskunnan kaikilta sektoreilta eikä Fintraffic tässä suhteessa muodosta poikkeusta.

Liikenteenohjaukseen vaikuttamalla ulkopuolinen toimija saavuttaa hyvän hyötysuhteen, koska jo varsin pienillä toimilla voidaan saada isoja vaikutuksia. Suomessa liikenne on lähtökohtaisesti sujuvaa ja tehokasta, joten pienetkin häiriöt saavat kansalaisten arjessa aikaan helposti näkyviä vaikutuksia. Liikenteen ongelmista myös uutisoidaan herkästi ja kansalaiset ovat hanakoita jakamaan sosiaalisessa mediassa negatiivisia kokemuksiaan erityisesti julkisen liikenteen ongelmista ja toki myös autoliikennettä häiritsevistä ilmiöistä ja tapahtumista. Negatiiviseen uutisointiin on vaikuttajatahon helpompi tarttua ja ryhtyä levittämään sanomaa, jolla pyritään lisäämään ristiriitoja ja heikentämään luottamusta yhteiskuntaan. Yksittäinenkin päivitys sosiaalisessa mediassa voi nousta hetkellisesti ilmiöksi, kun se saa tarpeeksi näkyvyyttä esimerkiksi bottien avustuksella.

Kun Suomi seuraavan kerran joutuu sotilaallisen hyökkäyksen kohteeksi, niin liikennejärjestelmä on yksi vaikuttamisen kohteista, koska tavoitteena on yhteiskunnan toiminnan lamauttaminen ja sen puolustamisen vaikeuttaminen. Silloin liikenteenohjaus on yksi kohteista, koska siihen vaikuttamalla pystytään liikennejärjestelmän kapasiteettia pienentämään niin paljon, että yhteiskunnan toiminnan kannalta välttämätön logistiikka ei enää toimi. Varmana

pidetään sitä, että jo ennen kuin poliittinen tilanne on eskaloitunut sotilaallisten iskujen asteelle, niin liikenteenohjausyhtiöihin vaikutetaan aktiivisesti muilla keinoilla. Kysymykseen voivat tulla ainakin informaatiovaikuttaminen ja taloudellinen vaikuttaminen eikä fyysistäkään vaikuttamista voida sulkea pois.

Asiantuntijoiden näkemyksissä tuli toistuvasti esille, että tärkeimpiä tavoitteita suomalaiseen yhteiskuntaan kohdistuvassa vaikuttamisessa on kansalaisten turvallisuudentunteen horjuttaminen. Koettua turvallisuudentunnetta voidaan horjuttaa kyseenalaistamalla julkisen sektorin, viranomaisten ja esimerkiksi Fintrafficin kaltaisten yhtiöiden luotettavuus, toiminnan tarkoitusperät ja toimintakyky. Vaikuttajan tavoitteena on lyödä kiilaa julkisen sektorin ja kansalaisten väliin ja aiheuttaa epäluottamusta hallintoa kohtaan. Epäluottamus aiheuttaa hajaannusta ja vaikeuttaa yhteiskunnan toimintaa, jolloin varautuminen esimerkiksi sotilaallisiin uhkiin heikkenee.

Uhka organisaatioon ei välttämättä tule ulkopuolelta. Pettynyt yhteistyökumppani, entinen tai nykyinen työntekijä tai muu läheisessä suhteessa organisaatioon ollut voi olla mukana aiheuttamassa ongelmia tahallaan tai vahingossa. ”Sisäpiirin” henkilö on vaikuttamiseen pyrkivälle toimijalle oivallinen apulainen, koska häntä voidaan käyttää lisäämään sanoman uskottavuutta ja tuomaan ”silminnäkijälausuntoja”. Työntekijöillä saattaa olla tiedossaan julkisuudelta piilossa pysyneitä tapahtumia tai muita tietoja, jotka saattaisivat julkaistuna vaarantaa organisaation maineen tai jopa toimintakyvyn. Epämiellyttävät asiat eivät lähtökohtaisesti vaaranna organisaation olemassaoloa tai toimintamahdollisuuksia, koska vahinkoja, erehdyksiä ja väärinkäytöksiäkin tapahtuu toisinaan kaikille. Mutta tarkoitushakuisesti uutisoituna ja organisaation kannalta hallitsemattomasti viestittynä niistä tulee ainakin ylimääräistä työtä tai mainehaittaa, joka voidaan kääntää organisaatiota vastaan. Hyvän henkilöstöpolitiikan noudattaminen rekrytoinnista työsuhteen päättymiseen on avainasemassa, kun tavoitellaan lojaalia ja luotettavaa henkilökuntaa. Yhtä lailla yhteistyökumppanien kanssa kannattaa tavoitella sopimuksia ja ratkaisuja, joihin molemmat osapuolet voivat olla tyytyväisiä.

Avoimuus on suomalaisen yhteiskunnan vahvuus ja ominaisuus, joka voidaan helposti kääntää myös sitä itseään vastaan. Julkista sektoria koskee laki viranomaisen toiminnan julkisuudesta, jonka perusajatus on se, että tiedot ovat julkisia, ellei ole erityisiä syitä salassapidolle. Viranomaisten ja muiden

toimijoiden keräämiä tietoaineistoja on avattu aktiivisesti kansalaisten ja elinkeinoelämän käyttöön. Tavoitteena tietojen avaamiselle on verorahoilla kerättyjen tietojen saaminen koko yhteiskuntaa hyödyttävään käyttöön ja esimerkiksi tietoihin perustuvan uuden liiketoiminnan synnyttäminen ja sen myötä taloudellisen toimeliaisuuden ja verokertymän lisääminen. Avoimen datan kääntöpuolena voi olla yhteiskunnan kriittisten toimintojen toimintaperiaatteiden paljastuminen, jos tiedot ovat niin kattavia, että niiden perusteella voidaan tällaisia arvioita tehdä. Merkittävä osa valtioiden sotilasorganisaatioiden harjoittamasta tiedustelusta perustuu kaikkien ulottuvilla oleviin avoimiin lähteisiin, joten lähtökohtaisesti yhteiskunnan hyväksi tarkoitettuja aineistoja voidaan helposti käyttää myös sitä vastaan. Sama pätee myös esimerkiksi organisaation yhteystietoihin ja avainhenkilöiden tietoihin. On syytä huomioida myös kasautumisvaikutus, jossa suuresta määrästä lähtökohtaisesti vaaratonta tietoa voidaan eri lähteiden tietoja yhdistelemällä muodostaa turvallisuusuhan muodostava kokonaisuus.

Taloudellisen vaikuttamisen sektorilla alihankintaketjujen merkitys korostuu. Tyypillisesti organisaatioilla on suuri määrä erilaisia palveluita tuottavia kumppaneita, joilla on jonkinlainen pääsy organisaation tiloihin tai tietoihin. Vastaavasti alihankkijoilla on omat alihankkijansa, joilla on samalla tavalla pääsyoikeuksia ja -mahdollisuuksia. Alihankintaketjujen hallitseminen ja kumppanien luotettavuuden arvioiminen on oleellista, kun suojaudutaan haitallista vaikuttamista vastaan ja vähennetään yhteistyösuhteiden kautta tulevien uhkien toteutumisen todennäköisyyksiä. Tiloihin ja tietoihin tulisi olla pääsy vain sellaisilla tahoilla, joilla on tehtävänsä suorittamisen vuoksi siihen tarve ja organisaation tulee olla perillä siitä ketkä sen tiloissa liikkuvat ja miksi. Yrityskauppojen myötä alihankintaverkostossa voi tapahtua muutoksia, joiden tuloksena toimijoiden omistus voi siirtyä epäluotettavalle taholle. Ei-toivottujen tilanteiden välttämiseksi alihankinta- ja palvelusopimuksiin olisi syytä kirjata ehtoja myös omistajanvaihdostilanteita varten.

Merkittävä osa varautumista on valmiussuunnitelmien laatiminen ja niiden käytön harjoittelu. Organisaation joutuessa eri tavoin tapahtuvan vaikuttamisen kohteeksi tarvitaan henkilökuntaa ja palveluntuottajia, joilla on osaaminen ja valmius hoitaa tilannetta ja minimoida aiheutuvat vahingot. Pelkkä suunnittelu ei riitä vaan suunnitelmien käyttöä on myös harjoiteltava säännöllisesti, jotta syntyy valmius toimia tositilanteessa.

4.3 Varautuminen Fintrafficissa

Keskusteluiden perusteella Fintraffic-konsernissa on tunnistettu hybridivaikuttamisen olemassaolo, mutta varautumisen toimet ovat painottuneet vahvasti tieto- ja kyberturvallisuuden parantamiseen. Tämä on ymmärrettävää ajatellen toimivan tietotekniikan ja tietoliikenteen merkitystä konsernin ydintehtäville. Tieto- ja kyberturvallisuuden kehityshankkeita on aloitettu ja niihin on panostettu merkittäviä resursseja tilannekuvan ja reagointikyvyn parantamiseksi. Henkilökunnan kouluttaminen ja perehdyttäminen esimerkiksi tietoturvan ja -suojan sektorilla on ollut aktiivista.

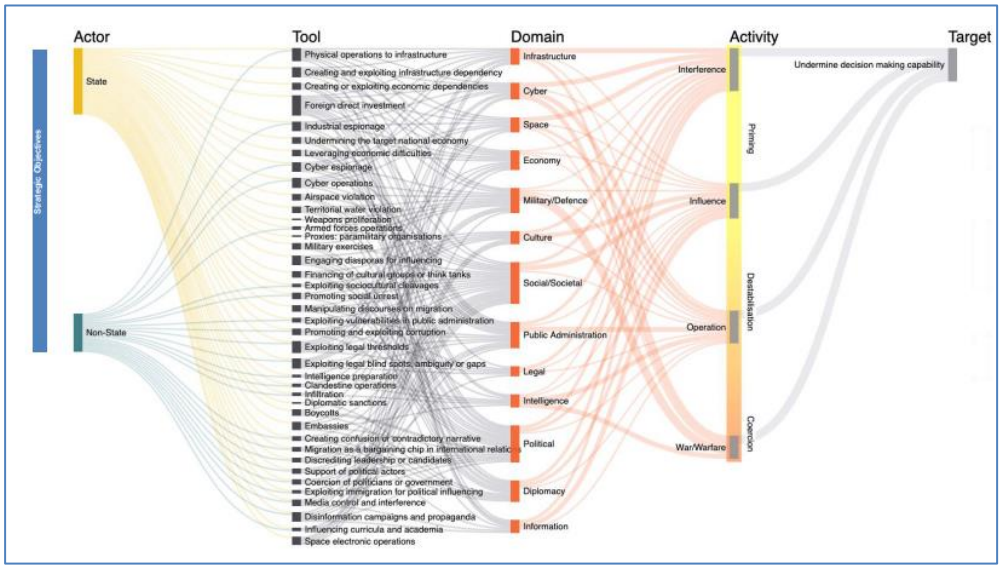
Tieto- ja kyberturvallisuuden lisäksi viestinnän sektorilla on tunnistettu tarve henkilökunnan kouluttamiselle ja esimerkiksi kriisiviestintäsuunnitelmien ja -harjoitusten laatimiselle ja järjestämiselle. Tehokkaan ja toimivan viestinnän keinoin voidaan vastata mahdollisiin konserniin kohdistuviin dis- tai misinformaatiokampanjoihin ja lieventää konserniin kohdistuvia vahinkoja.

Huomiota on kuitenkin syytä kiinnittää siihen, että konsernilla ei ole ollut järjestelmällistä tilannekuvan kokoamiseen ja seurantaan tarkoitettua toimintoa. Liikennemuotokohtaiset tytäryhtiöt tekevät tiivistä yhteistyötä kumppaniensa kanssa ja toimivat valtakunnallisesti vuorokauden ympäri. Niiden yhteistyön tai oman työskentelyn kautta saamaa tilannetietoa ei ole koottu yhteiseksi tilannekuvaksi, jonka myötä saataisiin yhteinen liikennemuodot ylittävä ja kattava kuva siitä, mitä konsernissa ja sen lähipiirissä tapahtuu.

Julkisen sektorin toimijana, jonka rahoituksesta merkittävä osa tulee valtion budjetista, Fintraffic on velvollinen noudattamaan lakia julkisista hankinnoista. Julkisten hankintojen kilpailutuksissa julkaistaan pääsääntöisesti tarjouspyyntö, johon mikä tahansa tarjoaja voi vastata ja tarjota hankinnan kohteena olevaa palvelua tai tuotetta. Kilpailutuksen voittaja voidaan valita joko pelkän hinnan tai laatutekijöistä ja hinnasta laaditun pisteytyksen perusteella. Tietojärjestelmiin liittyvissä hankinnoissa kiinnitetään huomiota myös valittavan toimittajan taustoihin ja erityisesti tietoturvaan. Tavoitteena on välttää sellaisten tuotteiden hankkimista, jotka voisivat altistaa hankintayksikön esimerkiksi tuotteeseen jätetyn takaportin kautta tapahtuvalle tiedustelulle. Tuotteen valmistusmaahan liittyviä kriteerien käyttäminen on kuitenkin hankalaa, koska ne tulkitaan syrjiviksi ja avointa kilpailua estäviksi ja sen vuoksi tuotteen laadullisten oinaisuuksien merkitys korostuu hinnan ohella. Tilanne

on muuttunut viime vuosien aikana hankalammaksi, kun esimerkiksi kiinalaisten tuotteiden laatu on parantunut. Kiinalaisten valmistajien tuotteet täyttävät laadulle asetetut vaatimukset ja hinta on silti edullinen. Tuotteet täyttävät vaaditut eurooppalaiset tai globaalit standardit, joita käytetään valintakriteereinä, mutta siitä huolimatta niiden turvallisuudesta ei voida olla varmoja. Hinnaltaan edullinen vaatimukset täyttävä tuote on vaikeasti voitettava kilpakumppani julkisessa hankinnassa. Samaan aikaan on kuitenkin tiedossa, että esimerkiksi kiinalaisissa tuotteissa on tarkoituksellisia tietoturva-aukkoja, joita voidaan hyödyntää vakoiluun, tietojen varastamiseen tai manipulointiin.

Fintraffic-konsernilla on paljon erilaisia palveluita tuottavia yhteistyökumppaneita sekä julkisella että yksityisellä sektorilla. Vastaavasti myös konsernin yhtiöt tuottavat palveluita muille organisaatioille, eli toimii alihankkijana jollekin muulle organisaatiolle. Alihankintaverkostot on tunnistettu mahdolliseksi hybridivaikuttamisen kanavaksi esimerkiksi taloudellisen vaikuttamisen keinoja hyödyntäen. Alihankkijoiden luotettavuuden arviointi perustuu pääsääntöisesti osana hankintaprosessia suoritettavaan vastuullisuuden arviointiin (esim. luotettava kumppani -merkintä). Sopimuksissa ei aina rajoiteta sopimuskumppaniksi valittavalta toimittajalta alihankinnan käyttämistä, jolloin alihankintaketju voi kasvaa pitkäksi. Samalla toimitusketjun hallinta vaikeutuu ja mahdollisuudet puuttua esimerkiksi muutaman alihankintaportaan takana olevaan toimittajaan on vähintäänkin hankalaa. Mitä pidemmäksi alihankintaketju kasvaa sen suuremmaksi kasvaa myös vaara, että ketjun kautta päästään vaikuttamaan varsinaiseen hankintayksikköön, tässä tapauksessa Fintraffic-konserniin tai sen yhteistyökumppaneihin. Vaikuttaminen ei välttämättä ole esimerkiksi tietojenhankintaa vaan se voi ilmetä myös esimerkiksi palvelukatkoksina, jotka vaikeuttavat Fintrafficin tehtävien hoitamista.



Kuva 2: Hybridivaikuttamisen käsitemalli (Giannopoulos;Smith;& Theocharidou, 2021).

4.4 Suomi hybridivaikuttamisen kohteena

2000-luvulla Suomea ei välttämättä ole pidetty vaikuttamisen kannalta mielenkiintoisena tai ensisijaisena kohteena kansalaisten keskuudessa. Kansainvälisessä politiikassa vallitsee kuitenkin vahva arvojen vastakkainasettelu ja länsimaiset arvot omaksuneena Suomi on osa länttä, jonka vuoksi se on mukana pelissä halusi tai ei (Auvinen & Brännare, 2020). Toisaalta Suomikin on jo muiden länsimaiden ohella ollut Venäjän kohdennettujen informaatiokampanjoiden kohteena esimerkiksi niin kutsutuissa lapsikiistoissa. Lapsikiistoissa esitetään tarina paitsi läntisten viranomaisten russofobiasta, myös läntisen liberalismin moraalisesta rappiosta, jossa ydinperhe on uhanalainen malli ja jopa lapset riistetään äideiltään (Mikkola;Aaltola;Wigell;Juntunen;& Vihma, 2018). Venäjän hyökkäys Ukrainaan helmikuussa 2022 muutti tilannetta radikaalisti ja Suomeen kohdistuva hybridivaikuttaminen tuli vahvasti näkyväksi julkisessa keskustelussa. Aikaisemmin laaja-alaisen vaikuttamisen mahdollisuudesta ja todennäköisyyksistä keskusteltiin lähinnä asiantuntijapiireissä ja aihe ei saanut kovin paljon palstatilaa medioissa ja jos sai, niin uutiset leimatiin helposti pelotteluksi. Siinä missä vaikuttamista aikaisemmin pidettiin mahdollisena, puhutaan asiasta nyt varmana ja kysymys on lähinnä siitä, milloin ja missä muodossa vaikuttamista ilmenee. Informaatiovaikuttamisen sektorilla erityisesti Suomen ja Ruotsin NATO-jäsenyyteen liittyviin kysymyksiin vaikuttamista pidetään jokseenkin varmana.

Ukrainan sodan myötä on herännyt myös keskustelua siitä, missä määrin Suomi on jo ollut hybridivaikuttamisen kohteena. Jyväskylän yliopistossa tiedusteluanalyysia opettavan eversti evp. Martti J. Karin Venäjän strategista kulttuuria käsittelevä luento vuodelta 2018 on tässä yhteydessä saanut paljon julkisuutta ja linkkiä siihen on ahkerasti jaettu monissa kanavissa. Luennossaan Kari toteaa, että Suomi on koko 2000-luvun ollut vahvasti erityisesti Venäjän hybridivaikuttamisen kohteena. Tästä esimerkkeinä hän mainitsee politiikasta poistuneiden entisten pääministerien uudet työt venäläisten yhtiöiden hallituksissa, venäläistä teknologiaa hyödyntävän ja venäläisellä pääomalla osittain rahoitettavan ydinvoimalan rakennushankkeen sekä venäläisellä rahalla toimivan suomalaisen jääkiekkojoukkueen pelaamisen Venäjän KHL-liigassa (Kari, 2018).

Euroopan parlamentin julkaisemassa tutkimuksessa Best Practices in the whole-of-society approach in countering hybrid threats (Wigell;Mikkola;& Juntunen, 2021) mainitaan esimerkkinä laajasta hybridioperaatiosta vuonna 2018 julkisuutta saanut Airiston Helmi -tapaus. Kysymys oli venäläistaustaisten toimijoiden kiinteistöomistuksista eri puolilla Lounais-Suomen rannikkoa lähellä strategisesti tärkeitä kohteita. Toiminta oli naamioitu vapaa-ajan asuntotoimintaa pyörittäväksi yhtiöksi, mutta yrityksillä ei suurista sijoituksista huolimatta ollut lainkaan tuloja ja se teki suuria tappioita vuodesta toiseen. Lopulta viranomaiset tekivät osana veropetostutkintaa laajoja kotietsintöjä kohteisiin

4.5 Varautuminen hybridivaikuttamiseen

Sini Korpinen ja Sara Lindström toteavat teoksessaan Mainekriisi, että organisaatiota kohtaava mainekriisi syntyy harvoin aivan sattumalta. Sen sijaan sen syntymiseen vaikuttavia tekijöitä on pystytty näkemään ainakin organisaation sisällä jo hyvissä ajoin ennen tilanteen eskaloitumista (Korpinen & Lindström, 2020, s. 18).

Korpinen ja Lindström puhuvat mainekriisin kohdalla ydinongelmasta, joka on kohun juurisyy. Siinä missä poikkeustilanne on yleensä tapahtuma, johon organisaatio ei itse omilla toimillaan olisi pystynyt vaikuttamaan (esim. sähkönjakeluhäiriö valtakunnanverkossa), niin mainekriisin siemenet on useimmiten kylvetty sen oman toiminnan tuloksena. Suojellakseen organisaatiota mainekriiseiltä olisi sen johdon siis syytä rehellisesti arvioida löytyykö organisaation historiasta ja toimintatavoista sellaisia asioita ja tapahtumia, jotka

voitaisiin kääntää sitä vastaan. Ydinongelma voi olla esimerkiksi ristiriita organisaation ja sen sidosryhmien odotusten välillä tai moraalinen haaste, joka liittyy organisaation tai jonkun sen toimijan tekemisiin (taloudellinen väärinkäytös, kiusaaminen jne.) (Korpinen & Lindström, 2020, ss. 43-44). Organisaation pienetkin maineongelmat voidaan hybridivaikuttamisen keinoja hyödyntäen kääntää sitä vastaan ja niitä voidaan tehokkaasti voimistaa sosiaalisen median avulla. Luomalla mainekriisi ja voimistamalla sitä luottamusta organisaatioon heikennetään ainakin hetkellisesti. Kun mainekriisejä tapahtuu riittävän paljon esimerkiksi julkisen sektorin organisaatioille, voi yleinen luottamus niihin rapautua kansalaisten silmissä. Varautuminen mainekriisiin voisi olla esimerkiksi skenaarioiden laatimista erilaisia negatiivisia uutistapahtumia varten ja näihin reagoimisen harjoittelua.

Euroopan hybridiuhkien torjunnan osaamiskeskuksen (Hybrid CoE) haavoittuvuudet ja resilienssi -verkoston johtaja Jukka Savolaisen mukaan ulkopuoliseen hybridivaikuttamiseen voi varautua tiedostamalla, että uhkia on ylipäätään olemassa:

- Hybridivaikuttamisessa joku tulee tahallaan tekemään odottamattomia asioita. Siihen on varauduttava yhdessä ja riski täytyy ymmärtää. Koko hallinnon on toimittava yhdessä samoin kuin eri yhteiskunnallisten toimijoiden. Kenttää pitää arvioida koko ajan uudelleen. Omiin reviireihin ei ole varaa jäädä kiinni.

- Hyvin tärkeää on myös yksityisen sektorin osallistuminen. On yhteinen etu, että uhka tehdään tarpeeksi näkyväksi, painottaa Savolainen (Tanhuanpää, 2019).

Helsingin kaupungin vuonna 2018 julkaistua ”Helsinki yhdistelmäuhkien aikakaudella – Yhdistelmävaikuttaminen ja kaupunki” -raporttia varten tekijät haastattelivat useita hybridivaikuttamisen asiantuntijoita. Usea haastateltava totesi, että yhdistelmävaikuttamisen ehkäisemiseksi tarvitaan vahvempaa johtamista. Osan kokemus oli, ettei yhdistelmävaikuttamisen teema ole kenenkään vastuulla, vaan se on ripoteltu eri organisaatioiden työlistoille. Näin ollen mahdollisia vaikutuskeinoja ei välttämättä pystytä yhdistämään toisiinsa kokonaisuudeksi (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 14).

Raportissa todetaan, että yhdistelmäuhkien kohde voi olla yhtä lailla ”kova”, kuten satama tai voimalaitos, kuin ”pehmeä”, kuten yhteiskunnan koheesio,

eivätkä nämä sulje toisiaan pois. Suomalaisella yhteiskunnalla on sinänsä hyvät valmiudet suojautua yhdistelmävaikuttamiselta, sillä pitkä kokonaisturvallisuuden ja varautumisen kulttuuri ja korkea yhteiskunnallinen luottamus ovat tässä valtteja, mutta on tärkeää huolehtia siitä, että paikallistasolla toiminta nivoutuu osaksi kokonaiskuvaa (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 23). Raportissa esitettyä päätelmää voidaan soveltaa myös osakeyhtiömuodossa toimiviin organisaatioihin.

On myös syytä todeta, ettei kaiken ikävän taustalla ole pahantahtoista yhdistelmävaikuttamista. Osaamme luoda ongelmia itsellemme myös ilman ulkopuolista apua. Jos yhdistelmävaikuttamista pelätään joka käänteessä, voi epäluulo itsessään romuttaa luottamusta ja provosoida eri tahoja. Ylikorostamista viisaampaa on suhtautua niin, että ymmärtää ja tiedostaa yhdistelmävaikuttamisen luonteen ja eri tahojen mahdolliset intressit. Yhdistelmäuhkilta suojautumista edesauttavat teot tuovat usein myös muita hyötyjä. Yhdistelmävaikuttamiselle altistavia kehityskulkuja, esimerkiksi yhteiskunnallisia jännitteitä ja keskinäistä epäluuloa, kannattaa pyrkiä hillitsemään joka tapauksessa (Harjanne;Muilu;Pääkkönen;& Smith, 2018, s. 23).

Helsingin seudun kauppakamari selvitti vuonna 2018 yritysten käsityksiä organisaatioihin kohdistuvista hybridiuhista ja varautumisesta niihin. Yleisimpänä syynä, jonka vuoksi yritykseen kohdistuisi hybridivaikuttamista mainittiin aktiiviset työntekijät (11 %), jotka toimivat sosiaalisessa mediassa ja joilla on paljon seuraajia. Julkisuudessa on käsitelty paljon eri maiden vaaleihin vaikuttamista ja siitä toiminnasta päivänvaloon on noussut lähes ainoastaan sosiaalisen median kautta tapahtunut vaikuttaminen. Yleisesti ottaen yritykset eivät vielä tunnista miten monin eri syin ne voivat päätyä hybridivaikuttamisen kohteeksi. Sosiaalinen vaikuttaminen voi olla vain osasyy, jolla yritys tai sen työntekijä valikoituu kohteeksi. Aktiivisuus sosiaalisessa mediassa voi toisaalta nostaa pienenkin yrityksen kohteeksi. Jos sosiaalisessa mediassa julkaistaan sellaista materiaalia, joka paljastaa yrityksen toiminnasta ja suhteista viranomaisiin tai poliitikkoihin sellaista tietoa, voi tämä olla kohteeksi määrittävä tekijä (Vesterinen;Fogle;& Eronen, 2018, s. 6).

Kyselyyn osallistuneiden yritysten mukaan hybridivaikuttamisesta ja vakoilusta ei ole tarpeeksi tietoa tarjolla. Avoimuus, sinisilmäisyys, tietoisuuden puute, valppauden puute tai kyvyttömyys tunnistaa uhkia ovat kaikki asioita,

jotka enemmän tai vähemmän voidaan korjata tiedon jakamisella ja koulutuksella siinä määrin, kun niiden korjaaminen on mahdollista. Hybridivaikuttajan kannalta ihmisten hyödyntämisen rooli informaatio- ja kybervaikuttamisen rinnalla voi olla yllättävän suuri, eritoten koska Suomi on hyvin verkottunut ja pieni yhteiskunta (Vesterinen;Fogle;& Eronen, 2018, s. 8).

Kyselyssä selvitettiin myös yritysten yhteistyötä turvallisuusviranomaisten kanssa. Mitä pienemmästä yrityksestä oli kysymys sen vähemmän yhteistyötä tehtiin ja organisaation koon kasvaessa yhteistyö lisääntyi. Viranomaisten suuntaan aktiivinen yrityskenttä kuitenkin vaikeuttaa hybridivaikuttajan työtä, sillä hybridivaikuttajan valikoidessa yrityksiä kohteekseen, sen on huomioitava se riski siitä, että yritys voi tehdä varoituksen toiminnasta ja itse hybridivaikutusoperaatio voi päätyä tarkkailun alle. Tältä osin voidaan puhua eräänlaisesta yhteiskunnan kokonaisvarautumisesta, jossa elinkeinoelämällä on oma roolinsa (Vesterinen;Fogle;& Eronen, 2018, s. 22).

Elinkeinoelämälle paras ja tehokkain tapa varautua hybridivaikuttamisen varalle on koulutus ja tieto. Viranomaisilla on keskeinen rooli neutraalin ja luotettavan materiaalin tuottamisessa. Uhkana hybridivaikuttaminen on monimuotoinen ja epäsäännönmukainen ja sen vuoksi sen varalle ei voi tehdä kovin yksityiskohtaisia ohjeita tai toimintamalleja. Yleinen tietämys, osaaminen ja havainnointikyky nousevat ratkaisevaan asemaan. Tunnistamisen tai epäilyn synnyttyä on myös tiedettävä kehen tai mihin otetaan yhteyttä ja se vaatii hyvää yhteistyötä ja aktiivisuutta viranomaisten suunnalta (Vesterinen;Fogle;& Eronen, 2018, s. 21).

Hybridivaikuttamiseen varautumisessa on aivan ensimmäiseksi omasta organisaatiosta tunnistettava ja määriteltävä kriittiset toiminnot ja niiden haavoittuvuudet. Sen jälkeen tulee määritellä kynnysarvot, jotta toiminnan tilaa ja siinä tapahtuvia muutoksia voidaan seurata. Ennalta määritellyt kynnysarvot (esimerkiksi normaalitilanne, kriisitilanne, hätätilanne) auttavat tunnistamaan ja arvioimaan tapahtuneen tai epäillyn hyökkäyksen vakavuuden. Lisäksi on syytä määritellä vaiheesta toiseen siirtymisen kriteerit esimerkiksi tapahtumien intensiteetin tai laajuuden perusteella (Cullen & Reichborn-Kjennerud, 2017, s. 20).

Hybridivaikuttamista harjoittavan tahon toiminta voi olla häiritsevää ja aiheuttaa fyysisiä vahinkoja, mutta niiden laajuus voi olla myös sellainen, että

tilannetta on vaikea erottaa normaaleista aika ajoin tapahtuvista sattumuksista. Jos tapahtumia ilmenee usein tai useilla sektoreilla samaan aikaan, voi hälytyskynnys ylittyä, koska synkronoitu toiminta voi johtaa kumuloituviin ja epälineaarisiin vaikutuksiin (Cullen & Reichborn-Kjennerud, 2017, s. 20).

Hybridisota ja hybridivaikuttaminen eivät istu kovin hyvin perinteiseen hyökkäysvaihe -käsitykseen, koska tilanne ei välttämättä kehity lineaarisesti kohti strategisesti määriteltyä lopputilannetta. Sen sijaan operatiivisissa vaiheissa tilanne vaihtelee nopeasti eskaloitumisesta vetäytymiseen ja takaisin ja eri kohteissa samaan aikaan. Hyökkääjä käyttää joustavasti hyväkseen eri puolilla aikaan saatuja vaikutuksia sitä mukaa kun niitä ilmenee. Tämän johdosta hybridivaikuttamiseen varautuminen vaatii jatkuvaa omien tunnistettujen haavoittuvuuksien seurantaa ja niihin kohdistuvien toimien mahdollisten vaikutusten arviointia (Cullen & Reichborn-Kjennerud, 2017, ss. 20-21).

5 Fintrafficin varautumisen kehittäminen

Fintrafficin varautuminen hybridivaikuttamiseen on käytyjen keskusteluiden ja arjessa tehtyjen havaintojen perusteella hyvässä vauhdissa, mutta on muutamia osa-alueita, joihin panostamalla varautumista voitaisiin vielä kehittää. Olen koonnut havaintoni neljän kohdan luetteloksi, joka seuraavissa kappaleissa avataan yksityiskohtaisemmin:

1. Tilannekuvatoiminto
2. Hyvä henkilöstöpolitiikka
3. Turvatoimet
4. Harjoittelu

Saatuani kaikki haastattelut tehdyksi syksyllä 2021 oli listalla ensimmäisenä kohtana valmiuspäällikkö -tyyppisen roolin perustaminen konsernille. Ajatuksena oli ehdottaa sellaista tehtävänkuvaa, joka mahdollistaisi yhtiörajat ylittävän tilannekuvan muodostamisen ja varautumisen koordinoinnin. Tämä kehitysajatus tuli mahdollisesti jo täytetyksi marraskuussa, kun konsernin aiempi kyber- ja tietoturvallisuusjohtajan tehtävänkuva laajennettiin valmius- ja kyberturvallisuusjohtajaksi. Aika näyttää miten uusi rooli vastaa tarpeeseen.

Joka tapauksessa on todettava, että nuorena organisaationa Fintrafficilla on ollut mahdollisuus rakentaa monia asioita alusta alkaen ja sen ansiosta monella sektorilla on pystytty aloittamaan ns. puhtaalta pöydältä. Emoyhtiö on kuitenkin ainoa kokonaan uusi organisaatio ja se onkin vielä etsinyt paikkaansa ja rooliaan kokonaisuudessa. Liikennemuotokohtaiset yhtiöt ovat tulleet aikaisemmista organisaatioista ja tuoneet mukanaan omat toimintamallinsa ja kulttuurinsa ja niiden sovittaminen yhteen emoyhtiön ja toistensa kanssa on vielä kesken.

5.1 Tilannekuvatoiminto

Asiantuntijoiden kanssa käydyissä keskusteluissa tuli selväksi, että organisaation on rakennettava oma tilannekuvansa itse, sitä ei kukaan tai mikään muu voi sen puolesta tehdä. Viranomaiset eivät välttämättä ole halukkaita eivätkä aina edes pysty jakamaan omia tietojaan muille, joten tilannekuvan tuottamiseksi tarvitaan omaa aktiivisuutta. Tilannekuvan rakentamisen edellytys on hyvien ja luottamuksellisten yhteistyösuhteiden luominen kumppanien kanssa.

Tilannekuva voisi koostua esimerkiksi neljästä osa-alueesta: toimintaympäristössä tapahtuneiden muutosten kuvauksesta, oman organisaation tilanteesta ja siinä tapahtuneista muutoksista, tulevaisuuksia koskevasta ennusteesta ja niiden vaatimista toimista sekä arviosta oman organisaation kyvystä suoriutua edellä kuvatuista toimenpiteistä (Kuva 3).

Kuva 3: Esimerkki tilannekuvan muodostamisesta.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tuottama Kybersää on hyvä esimerkki tuotteistetusta tilannekuvasta. Kybersää julkaistaan säännöllisesti kerran kuukaudessa ja siinä käydään läpi ajankohtaiset asiat ja tapahtumat kyberturvallisuuden näkökulmasta sekä annetaan suosituksia uhkilta suojautumiseksi. Tilannekuvan yhteenvetosivulla (Kuva 4) on ajankohtaisia nostoja kuudelta aihealueelta ja sisäsivuilla kuvataan tarkemmin mistä on kysymys, minkälaisia case-esimerkkejä aiheesta on olemassa ja miten olisi syytä toimia.

Kuva 4: Kyberturvallisuuskeskuksen Kybersää helmikuu 2022 (Traficom, 2022).

Toimintaympäristön tunteminen on varautumisen lähtökohta. Täytyy tuntea paitsi oma toiminta, sen vahvuudet ja heikkoudet niin myös yhteistyökumppanien toimintaympäristö. Fintrafficin tulisi olla selvillä siitä mitä omassa organisaatiossa tapahtuu eri sektoreilla ja myös siitä mitä sen yhteistyökumppanien arjessa tapahtuu. Tietoa havainnoista ja varsinkin poikkeavista tapahtumista tulisi jakaa aktiivisesti konserniyhtiöiden kesken ja tarvittaessa myös yhteistyökumppaneille, erityisesti turvallisuusviranomaisille.

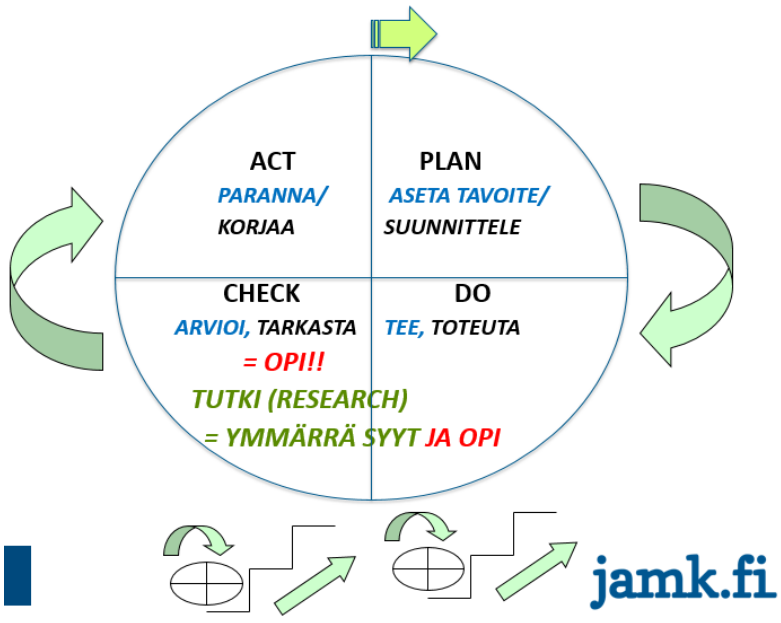
Eri puolilla konsernia tuotetaan ja käsitellään suuria määriä erilaista informaatiota, jota olisi mahdollista hyödyntää tilannekuvan rakentamisessa. Turvallisuuspoikkeamaraportit, erilaiset valvontaraportit, kulunvalvonnan ja rikosilmoittimien tai tietoturvajärjestelmien tuottama lokitieto on sellaista aineistoa, jota kertyy paljon ja suurelta osin automatisoidusti. Tällaisten suurten aineistomäärien käsittely ei ihmisvoimin ole kannattavaa, mutta tekoälyn ja koneoppimisen myötä datasta saattaisi olla löydettävissä apuväline tilannekuvan tuottamisen tarpeisiin. Tekoälyn ja koneoppimisen valjastaminen operatiivisen työn ja tukitehtävien eri vaiheissa syntyvän datan analysointiin on aihe, jota kannattaisi tutkia lisää.

Tieto- ja kyberturvallisuuden tavoitteiden asettaminen ja niiden saavuttamista tukevien palveluiden hankkiminen ovat korostuneet emoyhtiön toimissa Fintrafficin ensimmäisten toimintavuosien aikana. Tällaisia palveluita ovat esim. SOC- ja SIEM-palvelut, joita konserniyhtiöiden käyttöön on hankittu.

Näiden palveluiden avulla saadaan tietoturvallisuuden tilannekuvaa parannettua ja se onkin merkittävä osa-alue, kun konsernin turvallisuuden tilannekuvaa rakennetaan.

Konserni saa aika ajoin erilaisia tietopyyntöjä sen toimintaa ohjaavilta virastoilta tai ministeriöiltä. Tiedot näihin pyyntöihin kootaan yleensä liikennemuotokohtaisista tiedoista, joita mahdollisesti täydennetään emoyhtiön tiedoilla. Samaan tapaan liikennemuotokohtaiset yhtiöt raportoivat säännöllisesti emoyhtiölle esimerkiksi turvallisuussektorin tilanteesta ja ajankohtaisista tapahtumista. Nämä tiedot kuitenkin jäävät sille tielleen, eivätkä tytäryhtiöt saa paluupostissa yhteenvetoa, analyysiä tai muuta koostetta yhteisestä koko konsernin tilanteesta. Sama pätee myös ulos konsernista lähtevään raportointiin, siitä ei tytäryhtiöille saakka tule palautetta tai yhteenvetoa ns. suuremmasta kuvasta. Tämäntapainen yksisuuntainen raportointi ei tue aktiivisen tietojen vaihtamisen kulttuuria ja ennen pitkää motivaatio raportoinnin suorittamiseen laskee, kun yhteiseen käyttöön annetuista tiedoista ei saada raportoijalle itselleen minkäänlaista hyötyä ainakaan kovin nopeasti. Raportoidun tiedon perusteella saattaa toki myöhemmin tulla uusia toimeksiantoja ja tavoitteita, mutta niitä ei välttämättä osata enää silloin osata kytkeä aikaisemman raportoinnin tuloksiksi. Jatkuvan kehittämisen periaatteen (Kuva 5) mukainen tiedonkulun kehä suunnittele – toteuta – arvioi – paranna jää vajaaksi arvioinnin kohdalta. Sen vuoksi palautekanavan rakentaminen raportointiin olisi tutkimisen arvoinen kehityskohde.

Kuva 5: Jatkuvan parantamisen kehä (JAMK, 2020).



Fintraffic -konsernin ensimmäisten vuosien aikana en ole tunnistanut yhteisen tilannekuvan rakentamiseen tähtäävää toimintaa nimenomaan turvatoimisektorilla. Liikennemuotokohtaiset yhtiöt tekevät tiivistä yhteistyötä kumppaniensa ja verkostojensa kanssa, mutta näistä yhteistyösuhteista saatuja tietoja ei jaeta konsernissa Fintrafficin toimintaympäristön tilannekuvan luomiseksi. Olisi syytä harkita tilannekuvan rakentamisen ja ylläpidon mekanismien luomista osaksi konsernin turvallisuusjohtamista mukaan lukien myös tilannekuvatoiminnon tuottamiseksi tarvittavat tietojärjestelmät.

5.2 Hyvä henkilöstöpolitiikka

Hyvällä henkilöstöpolitiikalla vähennetään organisaation sisältä tulevien uhkien toteutumisen todennäköisyyttä, koska tyytyväinen henkilökunta on todennäköisesti lojaalimpaa työnantajalleen ja siksi haluttomampaa toimimaan työnantajansa etujen vastaisesti. Fintrafficissa HR-toiminnot tuotetaan keskitetysti emoyhtiön toimesta eikä operatiivisesta toiminnasta vastaavissa tytäryhtiöissä ole omia HR-palveluita. Järjestelyn ansiosta resurssit henkilöstöasioiden hoitamiseen ovat hyvät ja laaja-alaista asiantuntemusta on tarvittaessa aina käytettävissä. Yhtiöissä on käytössä useita erilaisia työehtosopimuksia, joten täysin samasta muotista ei palveluita voida kaikille tuottaa. Työehtosopimusten mahdollisesti aiheuttamat ongelma- ja riitatilanteet ovatkin sellaisia tapahtumia, jotka voivat kärjistää työnantaja- ja tekijäpuolten suhteita.

Fintrafficin olemassaolon aikana HR-sektorin resursseja ja toimintamallia on määrätietoisesti kehitetty vastaamaan paremmin konserniyhtiöiden tarpeita. Samaan aikaan myös henkilöstön työssä jaksamista on tuettu monipuolisesti niin työterveydenhuollon toimin kuin esimerkiksi tarjoamalla henkilökuntaetuna liikunta- ja kulttuurietuja. Pandemia-aikana on erityisesti kiinnitetty huomiota henkiseen hyvinvointiin ja jaksamiseen epävarmassa tilanteessa ja sama toimintamalli on jatkunut Venäjän Ukrainaa vastaan aloittaman sodan alkamisen jälkeen.

Työtyytyväisyyskyselyn tulokset ovat epävarmasta ajasta huolimatta olleet hyviä ja niiden perusteella henkilöstöpolitiikka on ollut onnistunutta. Viimeisimpänä toimena matkalla vieläkin paremmaksi työnantajaksi on ollut liittyminen Oikotien vastuullinen työnantaja -kampanjaan, jossa noudatetaan kuutta periaatetta: syrjimättömyyttä, työelämän tasapainoa ja hyvinvointia, esihenkilötyöhön panostamista, työn merkityksellisyyttä ja työssä kehittymistä, tehtävän mukaista palkkausta ja hyvää hakijakokemusta. Fintrafficin

HR-sektorin aktiiviset toimet tukevat osaltaan myös varautumista konserniin kohdistuviin vaikuttamisyrityksiin.

5.3 Turvatoimet

Turvatoimilla (security) tarkoitetaan tässä yhteydessä kaikkia niitä toimia, joiden tavoitteena on suojata Fintraffic-konsernia ja sen henkilökuntaa tahallisilta vahingoittamispyrkimyksiltä. Näin ollen turvatoimien skaala on laaja ja se kattaa aktiiviset toimet teknisestä tietoturvallisuudesta ja toimitilojen fyysisestä suojaamisesta hallinnollisen turvallisuuden piiriin kuuluviin henkilökunnan ja palveluntuottajien henkilöturvallisuusselvityksiin ja salassapitositoumusten tekemiseen. Hyvätkään tekniset ratkaisut eivät kuitenkaan riitä, jos organisaation turvallisuuskulttuurissa on puutteita. Hyvässä turvallisuuskulttuurissa kaikki ovat kiinnostuneita ja motivoituneita ylläpitämään hyvää turvallisuustasoa ja valmiita puuttumaan havaitsemiinsa ongelmiin. Virheistä otetaan opiksi eikä niistä rangaista tai etsitä syyllisiä ja tavoitteena on jatkuva parantaminen. Fintrafficin turvatoimet koostuvat emoyhtiön tuottamista politiikka- ja tavoite -tyyppisestä dokumentaatiosta sekä tytäryhtiöiden toteuttamista käytännön toimista, jotka suurelta osin ovat niiden oman harkinnan ja päätösten mukaisia.

Lähtökohtaisesti oma henkilökunta saa vapaan pääsyn työpaikkansa tiloihin ja joissain tapauksissa myös luottamuksellisiin ja salassa pidettäviin tietoihin. Monilla palveluntuottajilla alihankkijoineen on tehtävien hoitamiseksi kulkuoikeudet Fintrafficin yleisöltä suljettuihin tiloihin. Tiloihin pääsyä valvotaan teknisillä järjestelmillä, jotka yleensä ovat kiinteistökohtaisia ja siten useimmiten Fintrafficin ulkopuolisen toimijan hallinnassa. Pääsyoikeuksien myöntämisen perusteena on työtehtävään perustuva tarve ja salassapitositoumuksen tekeminen. Emoyhtiön vastuulla on henkilöturvallisuusselvitysten hankkiminen suurimmalle osalle konsernia ja niille palveluntuottajille, joille lain mukaan voidaan selvityksiä hankkia. Työssä olevien henkilöiden ja palveluntuottajien luotettavuuden ja nuhteettomuuden selvittäminen ja seuranta on viimeinen varmistus turvatoimien ketjussa.

Kuten edellä jo todettiin, niin toimitilojen fyysiset turvallisuusratkaisut ovat pääsääntöisesti kiinteistökohtaisia, ja sen vuoksi niihin liittyvät sopimukset on hoidettu suurimmaksi osaksi tytäryhtiöiden toimesta. Fintrafficilla ei pääsääntöisesti ole pääsyä kulunvalvontajärjestelmiin tai muihin turvatoimien teknisiin toteutuksiin ja sen vuoksi konsernilla ei ole täysin kattavaa tietoa

siitä, miten järjestelmät on toteutettu tai minkälaisille henkilöryhmille on myönnetty pääsyoikeuksia konsernin käytössä oleviin tiloihin. Parhaan ymmärryksen konsernin tilojen käytöstä ja käyttäjistä saisi, jos kulunvalvonta ja muu turvallisuustekniikka olisi Fintrafficin hallinnassa ja valvonnassa. Fyysisten turvatoimien järjestäminen voisikin tulevaisuudessa olla yksi konsernin yhtiöilleen tarjoamista tukipalveluista.

5.4 Harjoittelu

Kriisitilanteita varten Fintraffic-yhtiöissä on olemassa toimintamalleja ja erityisesti viestintäohjeita, mutta hyvätkään ohjeet ja suunnitelmat eivät ole hyödyllisiä, ellei niiden käyttöä harjoitella. Fintraffic-konsernissa ei ole sen olemassaolon aikana vielä syntynyt aktiivista yhteistä harjoittelukulttuuria. Liikennemuotokohtaiset yhtiöt ovat olleet aktiivisesti mukana yhteistyökumppanien kanssa toteutetuissa harjoituksissa, mutta sisäisiä oman organisaation toimintaan liittyviä ja liikennemuotorajat ylittäviä poikkeustilanne- ja kriisiharjoituksia ei vielä ole ollut. Muutamia konserniyhtiöiden sisäisiä harjoituksia on järjestetty ja konsernin henkilökuntaa on osallistunut valtionhallinnon isompiin harjoituksiin. Keväällä 2020 alkanut pandemia-aika on joka tapauksessa hankaloittanut kaikenlaisten fyysisiä kokoontumisia vaativien harjoitusten toteuttamista ja siten osaltaan hidastanut harjoittelutoiminnan käynnistämistä. Toisaalta pandemia-aikana on myös saatu hyviä kokemuksia monipaikkaisista etätyömenetelmin toteutetuista harjoitustapahtumista.

Harjoittelu voidaan toteuttaa monella tavalla ja monen tasoisena. Harjoituksen ei aina tarvitse olla monipäiväinen ja laajan skenaarion sisältävä useamman toimijan yhteinen harjoitus. Myös pieniä ja lyhyitä esimerkiksi vain tiettyä yksikköä tai toimintoa koskevia harjoituksia voidaan ottaa osaksi harjoitusohjelmaa. Harjoitusten suunnittelussa ja toteutuksessa voidaan turvautua alkuvaiheessa ulkopuoliseen asiantuntija-apuun ja oleellisinta olisikin harjoittelukulttuurin ja niihin liittyvien rutiinien luominen – harjoittelemaan oppiminen.

Harjoitusten suunnittelua varten voitaisiin laatia kokoelma erilaisia uhka-arvioiden ja riskianalyysien perusteella laadittuja skenaarioita, joissa keskityttäisiin tapahtumiin, joihin on vastattava yhdessä. Tällaisia voisivat olla esimerkiksi mainekriiseihin liittyvät aktiivista viestintää tai laajasti muiden yhteisten tukipalveluiden resursseja vaativat aiheet. Fintrafficin asema julkisen sektorin ja kansalaisten rajapinnassa aiheuttaa sen, häiriötilanteissa joudutaan

herkästi arvioimaan toimivaltuuksien ja tehtävien rajapintoja. Organisaatiorajat ylittävät harjoitukset, joissa Fintrafficin kaltaiset erityistehtäväyhtiöt pääsisivät harjoittelemaan häiriötilanteiden ja poikkeusolojen yhteistoimintaa yhdessä viranomaisten kanssa, olisivat erittäin hyödyllisiä rajapinnoissa olevien ongelmien löytämiseksi.

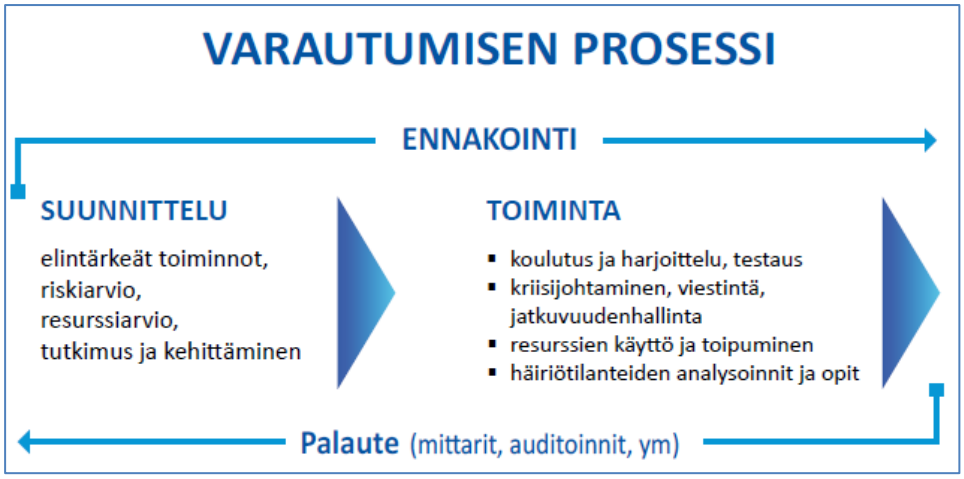
Häiriö- ja poikkeustilanteissa viestinnällä on suuri merkitys ja viestinnän ammattilaisille onkin aina tarvetta riippumatta siitä mitä harjoitellaan. Nykyaikaisessa informaatioyhteiskunnassa tieto liikkuu valon nopeudella ja hetkessä tavoitetaan potentiaalisesti vähintään tuhansia ja pahimmassa tapauksessa miljoonia ihmisiä. Vaikka sosiaalisen median tai uutismedioiden kanssa ei kannatakaan ryhtyä kilpailemaan nopeudessa, niin oman viestintäkyvykkyyden merkitys kasvaa koko ajan ja organisaatiolla tulisi olla valmius reagoida nopeasti paitsi itseään koskevaan uutisointiin, niin erityisesti huhuihin ja virheelliseen tietoon. Viestinnän ammattilainen ei aina välttämättä heti ole paikalla, kun tapahtuu, joten myös operatiivisella johdolla on oltava tarpeelliset valmiudet reagoida, kun sille on tarvetta. Nopeaa ja oikeanlaista reagointia helpottaa, jos mahdollisia skenaarioita on mietitty ennakolta ja harjoiteltu niissä toimimista.

Tunkeutumistestaus on organisaation turvallisuuskulttuuria harjoittava ja kehittävä harjoittelun muoto, joka voidaan kohdistaa fyysisiin turvatoimiin tai tietojärjestelmiin. Fyysisessä tunkeutumistestauksessa organisaation ulkopuolinen asiantuntija pyrkii löytämään keinot päästäkseen sisälle organisaation toimitiloihin. Tehdyistä havainnoista ja saaduista kokemuksista laaditaan raportti, jonka perusteella organisaatio voi ryhtyä kehittämään turvatoimiaan ja turvallisuuskulttuuriaan. Tunkeutumistestaus tukee tieto- ja kyberturvallisuuden kehittämistä, koska usein vakavien kyberhyökkäysten valmisteluun liittyy myös paikan päällä hyökkäyksen kohteen toimitiloissa tapahtuvaa tiedustelua ja valmistelua.

5.5 YTS kiteyttää varautumisen periaatteet

Yhteiskunnan turvallisuusstrategia (YTS) on valtioneuvoston periaatepäätös, joka yhtenäistää varautumisen kansallisia periaatteita ja ohjaa varautumista (Turvallisuuskomitea, 2017). YTS kuvaa varautumisen prosessin, joka ohjaa hallintoa ennakoimaan reagoinnin sijaan. Ennakointi edellyttää hiljaisten sig-

naalien tunnistamista sekä muun muassa tutkimustiedon, tieto- ja paikkatietoanalyysien hyödyntämistä ja toimintaympäristön muutostrendien havaitsemista ja skenaarioiden läpikäymistä harjoituksissa.



Kuva 6: Varautumisen prosessi Turvallisuuskomitean (2017) mukaan.

YTS:n mukainen prosessi voidaan skaalata yhteiskuntaan, hallinnonalaan, yksittäiseen organisaatioon tai organisaation osaan. Jokaisella mainituista toimijoista on omat elintärkeät toimintonsa, jotka tunnistamalla suunnittelu voidaan aloittaa. Toimintojen tunnistamisen jälkeen edetään vaihe vaiheelta kohti toteutuksia ja harjoittelua. YTS:n mukaista varautumisen mallia voisi hyödyntää myös Fintraffic-konsernin hybridivaikuttamiseen varautumisessa.

Suomeen kohdistuvan laaja-alaisen vaikuttamisen voimistuessa sabotaaseiksi tai muutoin fyysiseksi toiminnaksi olisi liikennejärjestelmään vaikuttaminen todennäköistä viimeistään sitten, kun toiminnalla on tarkoitus vaikuttaa yhteiskunnan strategisiin toimintoihin. Toimiva liikenteenohjaus mahdollistaa yhteiskunnan turvallisen ja sujuvan arjen ja sen vuoksi siihen vaikuttamalla on mahdollista häiritä kansalaisten ja elinkeinoelämän toimintaa.

Hybridivaikuttamiseen varautumisen tulisi olla osa myös Fintrafficin toimintaa aina ja kaikissa tilanteissa riippumatta siitä miten todennäköisenä uhkana sitä pidetään. Hybridivaikuttamisen luonteeseen kuuluu pitkä aikajänne, joten vaikuttaminen alkaa jo kauan ennen kuin kohteeseen vaikutetaan konkreettisesti esimerkiksi fyysisiä rakenteita tuhoamalla. Tyypillisesti aikajänne on ainakin kuukausia, mutta voi olla myös vuosia tai jopa vuosikymmeniä. Sen vuoksi rauhallisessa arjessa, ns. syvässä rauhan tilassa, varautuminen hybri-

divaikuttamisen kaltaiseen lähes näkymättömän uhkaan voi tuntua liioittelulta. Hankalaksi asian tekee paitsi vaikuttajan toiminta omien silmien alla demokratian toimintatapoja noudattaen ilman, että hälytysraja ylittyy, niin myös nimenomaan aikajänne; sitten kun vaikuttaminen on jo ilmiselvää ja konkreettista on jo liian myöhäistä reagoida. Fintrafficin varautuminen laaja-alaiseen vaikuttamiseen on jo lähtenyt liikkeelle, mutta vallitsevassa tilanteessa toimia ei ole syytä ainakaan vähentää.

6 Lähdeluettelo

Aaltonen, M. (9.. syyskuu 2021). Johtava asiantuntija, Liikenne- ja viestintävirasto.

Auvinen, P.;& Brännare, S. (2020). *YLE*. Haettu 1. 5 2021 osoitteesta https://yle.fi/uutiset/3-11563746

Cullen, P.;& Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare.* Multinational Capability Development Campaign (MCDC) 2016-17. Noudettu osoitteesta https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Finlex 574/ 2018. (2018). *Laki Liikenneviraston liikenteenohjaus- ja hallintapalveluiden muuttamisesta osakeyhtiöksi*. Haettu 29. 5 2021 osoitteesta https://www.finlex.fi/fi/laki/alkup/2018/20180574

Fintraffic. (4. 3 2022). *Toimintakertomus ja tilinpäätös 2021*. Haettu 29. 3 2022 osoitteesta https://www.fintraffic.fi/sites/default/files/2022-03/Fintraffic_Toimintakertomus_ja_tilinp%C3%A4%C3%A4t%C3%B6s_2021.pdf

Fintraffic toimintakertomus ja tilinpäätös 2020. (2021). *Fintraffic toimintakertomus ja tilinpäätös 2020.* Haettu 29. 5 2021 osoitteesta https://www.fintraffic.fi/sites/default/files/2021-03/Hallituksen_toimintakertomus_ja_Tilinpaatos_2020.pdf

Fintraffic vuosikatsaus. (2021). *Fintraffic vuosikertomus 2020.* Haettu 29. 5 2021 osoitteesta https://www.fintraffic.fi/sites/default/files/2021-03/Fintraffic_Vuosikatsaus_2020.pdf

F-Secure. (2022). *Kiristyshaittaohjelmasuojaus*. Haettu 28. 3 2022 osoitteesta https://www.f-secure.com/fi/business/resources/ransomware-protection

Giannopoulos, G.;Smith, H.;& Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A conceptual model.* Luxembourg: Publications Office of the European Union.

Harjanne, A.;Muilu, E.;Pääkkönen, J.;& Smith, H. (2018). *Helsinki yhdistelmäuhkien aikakaudella.* Helsinki: Helsingin kaupunki. Haettu 18. 5 2021 osoitteesta https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_fin_020818_netti.pdf

Holmström, L. (10. kesäkuu 2021). Suojelupoliisi.

Huhtakallio, J. (8.. syyskuu 2021). Cyber Security Architect, Liikentenohjausyhtiö Fintraffic Oy.

Hytönen, T. (23.. syyskuu 2021). Turvallisuusjohtaja, Fintraffic Raide Oy.

Hännikäinen, A. (20.. elokuu 2021). CISO, Liikenteenohjausyhtiö Fintraffic Oy.

Hätinen, T. (15.. syyskuu 2021). Turvallisuusjohtaja Fintraffic Lennonvarmistus Oy.

JAMK. (2020). *Näkökulmia jatkuvaan parantamiseen.* Haettu 31. 3 2022 osoitteesta https://blogit.jamk.fi/techtothefuture/2020/07/06/nakokulmia-jatkuvaan-parantamiseen/

Jantunen, S. (2015). *Infosota* (1 p.). Keuruu: Otava.

Juutinen, J.-P. (9.. syyskuu 2021). Johtaja, Liikenne- ja viestintävirasto.

Kangas, T. (24.. elokuu 2021). Apulaisjohtaja, Väylävirasto.

Kari, M. J. (2018). *Venäläinen strateginen kulttuuri - miksi Venäjä toimii niin kuin se toimii?* Haettu 13. 3 2022 osoitteesta https://m3.jyu.fi/jyumv/ohjelmat/it/panu/kyber/hybridivaikuttaminen-ja-turvallisuus/031218

Korpinen, S.;& Lindström, S. (2020). *Mainekriisi.* Alma Talent.

Kossila, T. (13.. syyskuu 2021). SQE-johtaja, Liikenteenohjausyhtiö Fintraffic Oy.

Krok, S. (13.. syyskuu 2021). Yritysturvallisuuspäällikkö, Liikenteenohjausyhtiö Fintraffic Oy.

Limnéll, J. (2019). *Hybridivaikuttaminen haastaa turvallisuuttamme*. Haettu 1. 5 2021 osoitteesta https://www.spjl.fi/viestinta/julkaisut/blogit/turvaamme_selustasi_-blogi/hybridivaikuttaminen_haastaa_turvallisuuttamme.4435.blog

Lohela, T. (17.. kesäkuu 2021). Hybrid CoE.

Mikkola, H.;Aaltola, M.;Wigell, M.;Juntunen, T.;& Vihma, A. (2018). *Hybridivaikuttaminen ja demokratian resilienssi.* Helsinki: Ulkopoliittinen instituutti. Haettu 8.1.2021. 1 2021 osoitteesta https://www.researchgate.net/publication/326033234_Hybridivaikuttaminen_ja_demokratian_resilienssi_Ulkoisen_hairinnan_mahdollisuudet_ja_torjuntakyky_liberaaleissa_demokratioissa

Muikku, J.-M. (8. 10 2021). Turvallisuuspäällikkö, Fintraffic Tie Oy.

Muukkonen, A. (24.. elokuu 2021). Valmiuspäällikkö, Väylävirasto.

Niemi, K. (2021). *Helsingin Sanomat*. Haettu 1. 5 2021 osoitteesta https://www.hs.fi/ulkomaat/art-2000007949235.html?share=9decc0bea11f452157a5e6a00749dbc5

Niemimuukko, H. (24.. elokuu 2021). Turvallisuusjohtaja, Väylävirasto.

Patrakka, J. (29. 9 2021). Johtaja, Järjestelmät ja palvelut, Fintraffic Meriliikenteenohjaus Oy.

Saarelainen, M. (10.. kesäkuu 2021). Suojelupoliisi.

Saariaho, M. (21.. syyskuu 2021). Vaikuttavuusjohtaja, Liikenteenohjausyhtiö Fintraffic Oy.

Salpakari, J. (9.. syyskuu 2021). Riskienhallintapäällikkö, Liikenne- ja viestintävirasto.

Savolainen, J. (2019). *Working paper on Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* The European Centre of Excellence for Countering Hybrid Threats.

Savolainen, J. (17.. kesäkuu 2021). COI Director, Vulnerabilities and Resilience, Hybrid CoE. Hybridiuhkien osaamiskeskus.

Sisäministeriö. (2022). *Kyberturvallisuus osana kansallista turvallisuutta*. Haettu 26. 3 2022 osoitteesta https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Suomen journalistiliitto. (2021). *Lehdistönvapausindeksi: Suomi edelleen toisena, lehdistönvapauden tila heikkenee*. Haettu 30. 1 2022 osoitteesta https://journalistiliitto.fi/fi/lehdistonvapausindeksi-suomi-edelleen-toisena-lehdistonvapauden-tila-heikkenee/

Tanhuanpää, A. (2019). *Rauhanturvaaja*. Haettu 11. 4 2021 osoitteesta http://www.rauhanturvaajalehti.fi/1243-hybrivaikuttamista-on-myos-kriha-operaatioissa/

Traficom. (2022). *Kybersää*. Haettu 31. 3 2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202022

Turvallisuuskomitea. (2017). *Yhteiskunnan turvallisuusstrategia*. Haettu 26. 3 2022 osoitteesta https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Vesterinen, P.;Fogle, C.;& Eronen, P. (2018). *Elinkeinoelämä ja hybridivaikuttaminen.* Helsinki: Helsingin seudun kauppakamari. Noudettu osoitteesta https://view.24mags.com/sites/all/files/public_files/documents/helsinki.chamber/18713054e05eb566fb18616b9c9458ea/document.pdf

Wigell, M.;Mikkola, H.;& Juntunen, T. (2021). *Best Practices in the whole-of-society approach in countering hybrid threats.* Euroopan Parlamentti.

Ylitalo, J. (9.. syyskuu 2021). Turvallisuusjohtaja, Liikenne- ja viestintävirasto.