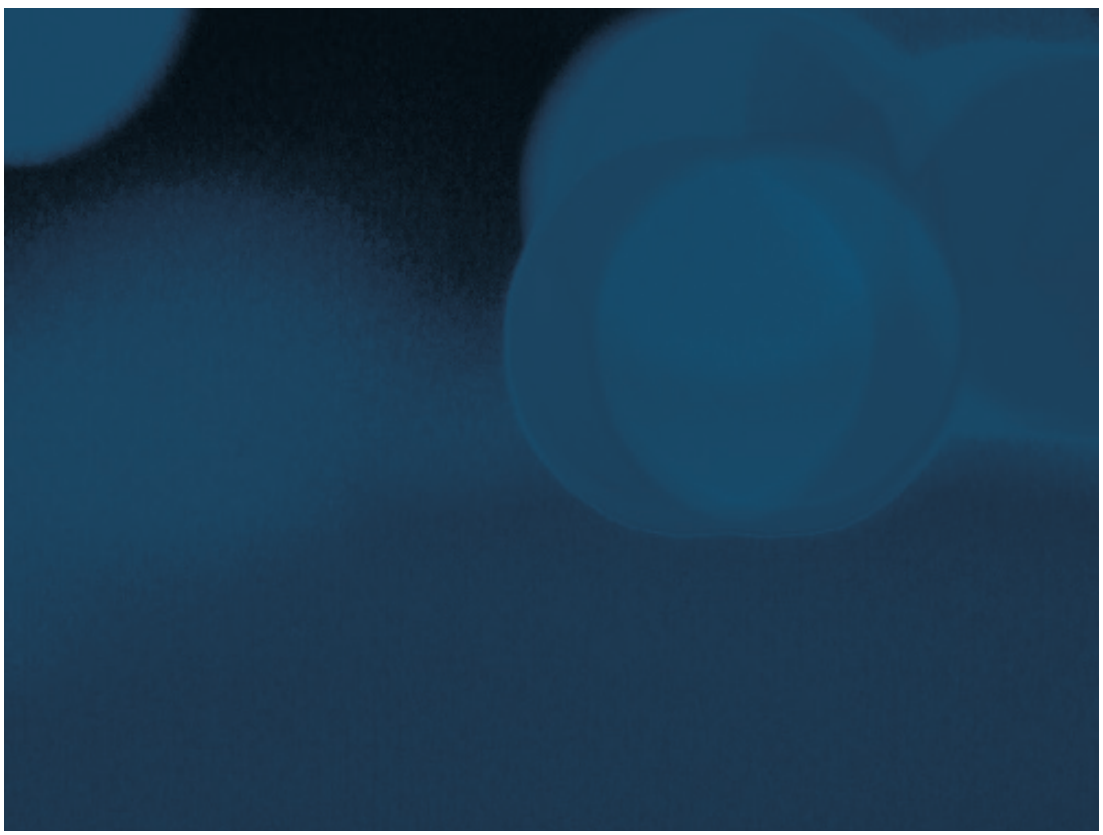
SUPO

Kansallisen turvallisuuden katsaus 2025



GLOBAALI TURVALLISUUS-YMPÄRISTÖ JA SUOMI

2
Synkkä turvallisuustilanne toi tiedustelun ulko- ja turvallisuuspolitiikan ytimeen

6
Kiina vahvistaa läsnäoloaan arktisella alueella

10
Venäjä asemoi itseään uudelleen maailmalla

12
Venäjä yrittää kiertää pakotteita yhä useammin EU:n sisäisillä hankintaketjuilla

17
Dataa voidaan hyödyntää myös Suomea uhkaaviin tarkoituksiin

VAKOILU JA VAIKUTTAMINEN

20
Valtiollisen vakoilun ja vaikuttamisen tilannekatsaus

24
Venäjä pyrkii vaikuttamaan sabotaasilla Euroopan maihin

27
Autoritaaristen valtioiden kyberekosysteemit uhkaavat kansainvälistä vakautta

34
Kiina hyödyntää sosiaalisen median alustoja tiedustelussaan

TERRORISMI

38
Kansallinen terrorismin uhka-arvio 2025

42
Alaikäisten radikalisoitumisesta on tullut vakiintunut ongelma Euroopassa

44
Radikaaliin äärioikeistoon liittyvät havainnot ovat kasvaneet turvallisuusselvityksissä

SUPON VUOSI

46
Vuosi 2024 kuuden supolaisen silmin

Synkkä turvallisuustilanne toi tiedustelun ulko- ja turvallisuuspolitiikan ytimeen

Juha Martelius
Suojelupoliisin päällikkö

Valtio ja kansallinen turvallisuus ovat palanneet politiikan keskiöön. Synkkäsävyinen suurvaltakilpailun ja valtioiden välisen vastakkainasettelun aika on nostanut turvallisuus- ja tiedustelupalvelut entistä suurempaan rooliin ulko- ja turvallisuuspolitiikassa.

Suomessakin tiedustelutiedon yhä kasvava merkitys on tunnistettu viime kesänä julkistetussa valtioneuvoston ulko- ja turvallisuuspoliittisessa selonteossa. Valtiojohdon on tärkeää tietää, mitä vastapuoli suunnittelee ja ymmärtää turvallisuusympäristön kehitys. Samaan aikaan on myös tiedettävä, mikä ei ole vastapuolen vaikuttamista vaan esimerkiksi julkisessa keskustelussa syntyneitä vääriä oletuksia ja spekulaatiota. Tätä tietoa ei voi yleensä julkisista lähteistä saada. Suojelupoliisi käyttää täysimääräisesti tiedustelulainsäädännön sallimia keinoja hankkia tietoa kansallista turvallisuuttamme uhkaavista kehityskuluista.

Sekä tiedustelun että laaja-alaisen vaikuttamisen tilannekuvassa entistä suurempaan rooliin ovat nousseet eri valtioiden käyttämät sijaistoimijat. Valtiollinen toimija pyrkii häivyttämään jälkensä välikäsien kautta, oli kyse sitten Venäjän, Kiinan tai Iranin toiminnasta. Sijaistoimijoiden avulla itsevaltaisten maiden voimaviranomaiset haluavat hämärtää todellisuutta, helpottaa tekojen kiistettävyyttä ja luoda uudenlaista epävarmuutta. Rekrytointi voidaan hoitaa sosiaalisessa mediassa ja maksu kryptovaluutoilla. Tehtävän suorittaja ei aina välttämättä itsekään tiedä, kenen lukuun toimii.

Yksi esimerkki sijaistoimijoiden käytöstä on Venäjän sabotaasitoiminta Euroopassa. Se on saanut entistä vaarallisempia muotoja ja osoittaa välinpitämättömyyttä sivullisista uhreista. Skaala on laaja erittäin monimutkaisista kyberhyökkäyksistä yksinkertaisiin tuhotöihin. Päätavoite on horjuttaa länsimaiden tukea Ukrainalle.

Suomi ei toistaiseksi ole ollut Venäjän voimakkaan vaikuttamisen kohteena vaan se on kohdistunut ennen kaikkea suuriin EU-maihin ja toisaalta maihin, joissa on esimerkiksi suuri venäläisvähemmistö tai venäjämyönteisiä puolueita.

Mediassa ja sitä myötä kansalaisten mielissä kuva Venäjän vaikuttamisesta ei aina vastaa todellisuutta vaan Venäjän tekemäksi luetaan esimerkiksi tavallista kotoperäistä ilkivaltaa. Tämä sopii Venäjälle hyvin, koska se kasvattaa sen pelotetta ja luo kuvaa Venäjän kaikkivoipaisuudesta.

Vaikuttamistoiminnallaan Venäjä jatkuvasti testaa länttä ja Natoa, seuraa niiden reaktioita ja sietokykyä. Venäjä ymmärtää länttä ja Suomea huonosti, esimerkiksi Suomen liittyminen Natoon yllätti Venäjän johdon. Mahdollisesti edelleen heikkenevä ymmärrys Suomen toiminnan logiikasta – ja toisaalta haluttomuus viedä ylimmälle johdolle epätoivottuja uutisia – saattavat aiheuttaa väärinkäsitysten riskin, jolloin Venäjä voi reagoida asioihin omien väärintulkintojensa perusteella.

Yhä harmaammalla alueella tapahtuva vaikuttaminen vaatii yhä enemmän myös tiedustelulta. Suojelupoliisin tavoite on antaa valtiojohdolle ennakkovaroitus Venäjän ei-sotilaallisesta vaikuttamisesta. Myös viranomaiset käyttävät Suojelupoliisin tuottamaa tiedustelutietoa kaikkein vakavimpien uhkien, kuten terrorismin, tehokkaaseen torjuntaan.

Tiedustelumaailman säännöt edellyttävät äärimmäistä luottamuksellisuutta, ja siksi kansainväliseen tiedonvaihtoon voivat osallistua vain samanmieliset tiedustelupalvelut. Tässä mielessä tiedustelupalvelut ovat kansallisvaltioille korvaamattomia työkaluja. Jos Suojelupoliisilla ja sotilastiedustelulla ei ole riittäviä resursseja osallistua yhteistyöhön ulkomaisten kumppaniensa kanssa, nämä ovet on Suomelta kokonaan suljettu.

Selvää on, että erityisesti Venäjä on muuttanut merkittävällä tavalla turvallisuusympäristöämme. Kehitystä parempaan ei ole näköpiirissä. Venäjä on aggressiivinen, laajentumishaluinen valtio, joka on valmis käyttämään kaikkia keinoja poliittisten tavoitteidensa saavuttamiseksi. Venäjän imperialistisen luonteen korostuminen, tosiasioihin perustumattomat historiatulkinnat ja jo vuosikymmeniä jatkunut kansakunnan manipulointi uskomaan Venäjän historiallinen missio edellyttävät Suomessa osaavaa ja vahvaa tiedustelua, joka pystyy antamaan ensivaroituksen mahdollisista maahamme kohdistuvista toimista. ■

Globaali turvallisuus-ympäristö ja Suomi

Kiina vahvistaa läsnäoloaan arktisella alueella

Hyökkäyssota on tehnyt Venäjästä riippuvaisemman Kiinasta. Kiina ja Venäjä ovat tiivistäneet yhteistyötään suurvaltakilpailun kannalta oleellisella arktisella alueella.

Jääpeite elokuussa 2024

VENÄJÄ

MONGOLIA

KIINA

KAZAKSTAN

GRÖNLANTI

HUIPPUVUORET

Kiinan tutkimus asema

Venäjän tutkimus asema

Kiinan ja Islannin yhteinen tutkimusasema

Venäjällä on yli 50 jäänmurtajaa

Kiinalla on 5 jäänmurtajaa

Napapiiri

Koillisväylä

Ukrainaan kohdistuvasta hyökkäyssodasta johtuvien pakotteiden seurauksena Venäjästä on tullut entistä riippuvaisempi Kiinasta. Uusi tilanne luo edellytyksiä entistä tiiviimmälle Venäjän ja Kiinan väliselle yhteistyölle arktisella alueella. Kiina on päässyt vahvistamaan hiljalleen läsnäoloaan arktisella alueella Venäjän kanssa tehtävän yhteistyön kautta. Venäjästä onkin tullut Kiinalle ensisijainen reitti arktiselle alueelle.

Kiinan ja Venäjän tiivistyvä yhteistyö pohjoisessa näkyy monella tapaa. Venäjän ja Kiinan rannikkovartiostot partioivat ensimmäistä kertaa yhdessä arktisella alueella syksyllä 2024. Maat ovat järjestäneet yhteisiä sotilaallisia harjoituksia myös Suomenlahdella.

Venäjä saa Kiinalta myös teknologista tukea ja investointeja arktisen alueen energiahankkeisiin. Maiden alueeseen liittyvä tutkimusyhteistyö on tiivistynyt.

Kiihtyvä suurvaltakilpailu arktisella alueella heijastuu Suomeen

Arktinen alue on yksi keskeisistä suurvaltakilpailun näyttämöistä. Kiinan kasvava läsnäolo arktisella alueella kiihdyttää todennäköisesti kilpailua entisestään. Suomi on arktinen valtio, joten on selvää, että voimatasapaino alueella vaikuttaa myös Suomeen.

Tiedustelupalveluna Suojelupoliisin tehtävä on hankkia tietoa tällaisista Suomen kansalliseen turvallisuuteen merkittävällä tavalla vaikuttavista kehityskuluista.

Kiinan ja Venäjän suhteiden tiivistymisen vaikutukset Suomelle ovat moninaiset. Venäjä pitää Natoa suorana uhkana itselleen. Myös Kiina vastustaa kaikkia sotilaallisia liittoumia, joissa Yhdysvallat on mukana. Arktinen alue on tärkeä strategiseen tasapainoon liittyvien ydinaseiden ja niitä kuljettavien ohjusten kehittämisessä, käyttämisessä, havaitsemisessa ja torjunnassa.

Myös riski siitä, että osaamistamme ja teknologiaamme päätyy Kiinan kautta myös Venäjälle, on kasvanut. Suomella on monenlaista arktista osaamista, joka kiinnostaa Kiinaa ja Venäjää. Jäänmurtajien ja muiden jäävahvisteisten alusten rakennus on tästä vain yksi esimerkki.

Arktinen alue on keskeinen esimerkiksi satelliittiteknologian kannalta

Arktinen alue on sijainniltaan olennainen turvallisuuteen, kauppaan ja teknologiaan liittyvistä syistä. Jo pitkään on ollut tiedossa, että jääpeitteiden sulaminen avaa uusia merireittejä ja vapauttaa hyödynnettäväksi luonnonvaroja, kuten mineraaleja, kaasua ja öljyä. Kiina haluaa suurvaltana olla hyödyntämässä näitä mahdollisuuksia.

Arktinen alue on tärkeä myös satelliittiteknologian kannalta, sillä napa-alueet ovat sijainniltaan ihanteellisia satelliittimaa-asemille. Monet sotilas- ja siviilikäytössä olevat paikannus- ja viestintäjärjestelmät ovat riippuvaisia satelliittiteknologiasta.

Kiina on tavoitellut satelliittimaa-asemien perustamista Pohjoismaihin. Suomi ja muut Pohjoismaat ovat suhtautuneet näihin hankkeisiin kriittisesti. Suomi on puuttunut tilanteeseen tekemällä maa- ja tutka-asemista luvanvaraisia. Lupia punnitaan nykylainsäädännön mukaan myös kansallisen turvallisuuden näkökulmasta.

Kiina ajattelee myös, että suurvallalla pitää olla laivasto, jonka on kyettävä operoimaan missä tahansa, myös arktisissa olosuhteissa. Kiina pyrkii pitkällä aikavälillä hankkimaan itsenäisen operointikyvyn alueella. Siksi Kiina on panostanut muun muassa jäänmurtajakalustonsa kehittämiseen.

Venäjä tarvitsee Kiinaa

Venäjän hyökkäyssota on vaikuttanut merkittävällä tavalla arktisen alueen dynamiikkaan. Sodan vuoksi Arktisen neuvoston työ on pysähtynyt. Keskeisin muutos on tapahtunut kuitenkin Kiinan ja Venäjän suhteessa.

Vielä vuosikymmen sitten Venäjä suhtautui paljon nykyistä epäilevämmin Kiinan kanssa tehtävään arktiseen yhteistyöhön, koska se halusi säilyttää oman valta-asemansa alueella. Vaikka Kiinalla ja Venäjällä on yhteneviä tavoitteita ja yhteistyö on viime vuosina tiivistynyt, suhteisiin liittyy edelleen myös epäluottamusta.

Kiinalla on nyt aiempaa parempi neuvotteluasema keskusteluissa arktisesta yhteistyöstä Venäjän kanssa kuin ennen hyökkäyssotaa. Venäjän sotateollisuus on hyvin riippuvainen Kiinasta tuotavasta teknologiasta. Venäjä saa Kiinasta muun muassa sotateollisuuden tarvitsemia mikrosiruja ja erilaisia komponentteja. Myös Venäjän taloudellinen riippuvuus Kiinasta on kasvanut. Kiinan tuen ansiosta Venäjä voi jatkaa aggressiivista toimintaansa Euroopassa.

Toisaalta Venäjää ei pidä myöskään liiaksi aliarvioida. Arktisella alueella Venäjä on yhä vahvempi toimija pitkän historiansa vuoksi, vaikka se joutuukin sietämään Kiinalta enemmän kuin aiemmin. Kuvaavaa on, että Venäjällä on yli 50 jäänmurtajaa, kun Kiinalla on niitä viisi.

Arktisen läsnäolon vahvistaminen on osa Kiinan laajempia tavoitteita

Kokonaisuudessa Kiina tavoittelee globaalia sotilaallista läsnäoloa, joten sen kiinnostus arktiseen on osa laajempia tavoitteita. Kiinalle keskeisintä on suurvaltakilpailu Yhdysvaltojen kanssa.

Kiina hyötyy siitä, että se on saanut Venäjästä aiempaa läheisemmän kumppanin Yhdysvaltain vastaisessa rintamassa. Kiina pyrkii vahvistamaan länsimaista riippumattomia kansainvälisiä rakenteita, joista Brics-maiden tiivistyvä yhteistyö on esimerkki.

Venäjä hyötyy itsekin länsimaista riippumattomien kansainvälisten rakenteiden vahvistumisesta, vaikka ne ovat selvästi Kiina-vetoisia.

Kiinalla ei ole halukkuutta painostaa voimakkaasti Venäjää ja vaarantaa hyvää kahdenvälistä suhdetta. Vakaa Venäjä vapauttaa Kiinan resursseja tärkeimpään eli suurvaltakilpailuun Yhdysvaltojen kanssa. Kiina voikin antaa asioiden edetä painollaan ja odottaa, että Venäjä joutuu pyytämään siltä apua. ■

Venäjä asemoi itseään uudelleen maailmalla

Venäjä esiintyy Euroopan suuntaan uhoavasti, mutta haluaisi palauttaa kauppasuhteet Euroopan maiden kanssa. Ukrainalle annettavan tuen heikentäminen ja pakotteiden lieventäminen ovat Venäjän keskeisiä tavoitteita maailmalla. Samaan aikaan Venäjä tähyää uusiin ilmansuuntiin.

Kolme vuotta kestänyt sota Ukrainassa on pakottanut Venäjää asemoimaan itseään kansainvälisesti merkittävästi uudelleen. Venäjä esiintyy ulkopolitiikassaan itsevarmasti, mutta samaan aikaan on selvää, että maan painoarvo on laskenut globaalisti.

Muutos on ollut dramaattisin Venäjän ja länsimaiden suhteissa, jotka ovat aallonpohjassa. Venäjä on omalla toiminnallaan heikentänyt merkittävästi mahdollisuuksiaan vaikuttaa länsimaihin.

Kun tavanomaiset vaikuttamisen keinot ovat heikentyneet, Venäjän toiminta Euroopassa on muuttunut aggressiivisemmaksi. Toisaalta myös lännen mahdollisuudet vaikuttaa Venäjään ovat vähäisemmät, sillä länsi on tällä hetkellä entistä etäisempi venäläisille.

Asetelma kasvattaa huomattavasti väärinymmärrysten ja ylilyöntien mahdollisuutta. Kun perinteiset viranomaisyhteydet ovat lähes poikki, keskustelua käydään yhä enemmän julkisuuden kautta. Tiedustelutiedon tarve puolin ja toisin kasvaa, kun tietoa on tarjolla kehnosti tavanomaisia kanavia pitkin.

Venäjä tähyää itään ja etelään

Venäjä ei kuitenkaan ole niin eristyksissä maailmasta kuin lännestä katsottuna voisi näyttää. Olennaisin suunta, johon Venäjä nyt tähyää, on Kiina. Venäjä on sitonut itsensä yhä voimakkaammin Kiinaan ja sen ulkopoliittisiin tavoitteisiin. Selvää on, että Kiina on Venäjää vahvempi osapuoli. Venäjä ja Kiina pyrkivät vahvistamaan kansainvälisiä rakenteita, joissa länsimaat eivät ole mukana.

Venäjä katsoo globaalin etelän suuntaan eli Afrikkaan, Aasiaan ja Etelä-Amerikkaan. Yksi areena tälle on Brics-maiden yhteistyö. Venäjä pyrkii kartoittamaan globaalissa etelässä kauppahankkeita, mutta lisäämään myös poliittista painoarvoaan, mikä näkyy esimerkiksi diplomaattipanostuksissa.

On selvää, ettei globaali etelä korvaa Eurooppaa, jonne suuri osa Venäjän kaupasta aiemmin suuntautui. Siihen vaikuttaa logistiikkakin – kaasuputkia ei rakenneta hetkessä uusiin suuntiin.

Globaalissa etelässäkään Venäjän toimintakenttä ei ole yksinkertainen. Palkkasotilasyhtiö Wagner toimi aiemmin yhtenä Venäjän vaikuttamisen kanavana useissa Afrikan maissa. Kesän 2023 vallankaappausyrityksen jälkeen Venäjän puolustusministeriö on purkanut Wagneria. Jäykkä virkakoneisto ei ole kyennyt korvaamaan ketterämpänä vaikuttamiskanavana toiminutta yhtiötä. Venäjä on siis tätä kautta myös menettänyt vaikutusvaltaansa Afrikassa.

Venäjä uhoaa, mutta haluaisi palauttaa kauppasuhteet Euroopan kanssa

Venäjän presidentti **Vladimir Putin** on ollut vallassa pidempään kuin yksikään eurooppalainen johtaja, mikä tuo hänelle tiettyä itsevarmuutta. Venäjän johto ei joudu ajattelemaan ratkaisujaan vaalisyklien mukaisesti, joten se ajattelee monessa asiassa voivansa väsyttää vastapuolen.

Venäjälle keskeinen vaikuttamisen tavoite on tuen heikentäminen Ukrainalle. Venäjän voi sanoa onnistuneen tässä osittain, sillä maa on kyennyt luomaan pidäkkeitä lännen antamalle sotilaalliselle tuelle. Toisaalta länsimaiden Ukrainalle annettava tuki on jatkunut ja syventynyt sodan pitkittyessä.

Vaikka Venäjä esiintyy itsevarmasti ja hyökkäävästi puheissaan, se haluaisi palauttaa kauppasuhteet Euroopan maiden kanssa. Venäjän toinen keskeinen tavoite onkin pakotteiden purkaminen tai vähintään lieventäminen.

Venäjä pyrkii kohdentamaan Euroopassa viestiään niille, jotka haluaisivat palauttaa normaalit kauppasuhteet. Suomessa Ukrainan tuki on ollut hyvin yksimielistä, mutta monessa muussa Euroopan maassa tilanne ei ole yhtä selvä. Talouteen liittyvät argumentit ovat keskiössä, kun Venäjän kohdistaa vaikuttamistaan.

Venäjän johdon maailmankuvassa länsimaat eivät ole absoluuttisen pahoja, vaan jakautuvat hyvään ja pahaan länteen. Länsimaiden johtajat edustavat niin sanottua pahaa länttä, joka pyrkii eristämään Venäjän. Hyvää länttä edustavat tavallinen kansa ja tahot, jotka olisivat valmiita jatkamaan kauppaa Venäjän kanssa. Venäjä ei arvosta demokratiaa eikä ymmärrä, että Euroopan maissa poliittinen johto heijastelee kansan mielipiteitä.

Selvää on, ettei paluuta vanhaan ole Euroopan ja Venäjän kauppasuhteissa kummankaan näkökulmasta. Euroopasta katsottuna luottamuksen palautuminen vaatisi radikaalin ja epätodennäköisen muutoksen Venäjällä. Venäjä puolestaan ei halua tulla uudelleen yhtä riippuvaiseksi lännestä kuin se oli ennen sotaa.

Pienet valtiot eivät ole Venäjän vaikuttamisen keskiössä

Euroopassa Venäjän vaikuttaminen kohdentuu etenkin suuriin maihin ja tietysti Ukrainaan. Venäjä ei ole kaikkivoipa vaikuttaja, vaan sotaa käyvä maa, joka joutuu priorisoimaan tekemisiään. Suomen kaltaiset pienet maat eivät ole Venäjän näkökulmasta merkittävimpiä vaikuttamisen kohteita.

Venäjä näkee itsensä suurvaltana, jonka päävastustaja on Yhdysvallat. Toisaalta Venäjä kokee olevansa myös uhattuna – ja toimivansa vastavuoroisesti silloinkin, kun se länsimaiden näkökulmasta eskaloi tilannetta. Venäjän keskeinen tavoite on ylläpitää omaa sisäistä vakauttaan.

Venäjä on Suomelle suurin uhka, mutta Venäjän näkökulmasta Suomi ei ole yhtä olennainen kuin toisinpäin. Venäjän näkökulmasta Suomen kaltaiset pienet maat ovat toimintakenttää suurten valtioiden intresseille. Venäjä näkee maailman, jossa pienistä valtioista tulisi suurempien valtioiden satelliittimaita, joista piittaamatta muutama suuri maa voisi sopia asioista keskenään.

Samaan aikaan Itämerellä on iso merkitys Venäjälle. Itämerellä seilaava varjolaivasto on tällä hetkellä taloudellisesti ja logistisesti kannattavin vaihtoehto Venäjälle kuljettaa öljyä meriteitse. Varjolaivaston käyttämisellä raakaöljyyn kohdistuvien pakotteiden kiertämisessä on suuri merkitys Venäjän talouden kannalta.

Venäjän ja Suomen suhde on muuttunut perustavanlaatuisesti. Venäjä suhtautuu Suomeen epäystävällisenä maana muun muassa Nato-jäsenyyden myötä. Se kokee, että Suomi on pettänyt sen luottamuksen ryhtymällä liittolaiseksi Yhdysvalloille.

Venäjä valmistautuu edelleen syvenevään vastakkainasetteluun länsimaiden kanssa ja pyrkii ylläpitämään työkaluja, joihin se voi tarpeen tullen turvautua. Se varustautuu monenlaiseen vihamieliseen toimintaan länsimaita ja myös Suomea vastaan. Varautuminen ei kuitenkaan ole osoitus päätöksestä ryhtyä tällaisiin toimiin välittömästi. ■

Venäjä yrittää kiertää pakotteita yhä useammin EU:n sisäisillä hankintaketjuilla

Venäjän keinot kiertää sille asetettuja pakotteita ja vientirajoituksia ovat yhä vaikeammin tunnistettavissa. Hankintareittien mutkistuessa yritykset voivat olla tietämättään osallisina niiden kiertämisessä.

Venäjä etsii koko ajan uusia ja hienovaraisempia keinoja kiertääkseen sille asetettuja pakotteita ja vientirajoituksia. Yhä useammin Venäjä ketjuttaa hankintojaan myös Euroopan unionin sisämarkkinoilla.

Venäjä pyrkii kätkemään entistä tehokkaammin hankintaketjuja, koska länsimaiset viranomaiset ovat tietoisempia sen tavoista kiertää pakotteita ja vientirajoituksia. Kun hankintaketjuissa on mukana yhä enemmän välikäsiä, viranomaisten ja yritysten on entistä vaikeampi tietää kenen kanssa ne kauppaa lopulta käyvät.

Hankintaketjujen ulottaminen Euroopan unionin sisämarkkinoille tarkoittaa, että yhteydenotto suomalaiselle yritykselle voi tulla Suomesta tai jostakin muusta EU-maasta. Yhteydenotossa ei välttämättä näy selkeää kytkentää Venäjälle tai EU:n ulkopuoliseen maahan.

Hankintojen ketjuttamisessa käytetään peitteenä sekä yksittäisiä yrityksiä että laajempia hankintaverkostoja, joiden kautta Venäjä voi ohjata tarvittavaa materiaalia maahan.

EU:n sisämarkkinoilla alkavat ketjut jatkuvat usein pitkää välitysketjua hyödyntäen EU:n ulkopuolisissa kolmansissa maissa.

Pakotteiden vaikutus näkyy Venäjällä

Venäjä pyrkii pakotteita ja vientirajoituksia kiertämällä hankkimaan itselleen tarpeellisia tuotteita ja teknologiaa.

Suomalaisilla yrityksillä, yliopistoilla ja tutkimuslaitoksilla on runsaasti kansainvälisesti arvostettua osaamista ja edistynyttä teknologiaa. Venäjän hankintapyrkimysten kohteena voi olla niin huipputeknologia kuin tavanomaiset komponentit, kuten piirilevyt. Sitä kiinnostavat esimerkiksi erilaiset elektroniset komponentit, mittauslaitteet, työstökoneet, materiaalitekniikka, optiikka, meriteknologia ja kvanttiosaaminen.

Venäjän hankinnan kohteina ovat myös EU:n asetuksella vientivalvotut kaksikäyttötuotteet. Kaksikäyttötuotteilla tarkoitetaan teknologiaa tai tuotteita, jotka soveltuvat sekä siviili- että sotilaskäyttöön tai joukkotuhoaseiden kehittämiseen.

Venäjälle asetetut pakotteet ja vientirajoitukset hankaloittavat ja hidastavat niiden alaisten tuotteiden hankkimista maahan sekä tekevät niistä kalliimpia. Venäjä tarvitsee hankintoja ennen kaikkea ylläpitääkseen sotilaallista kyvykkyyttään.

Poikkeaviin yhteydenottoihin syytä kiinnittää huomiota

Venäjän hankintareittien mutkistuessa ja kytkeytyessä entistä enemmän EU:n sisämarkkinoille, yritykset voivat olla tietämättään osallisina pakotteiden ja vientirajoitusten kiertämisessä.

Yritysten on syytä kiinnittää huomiota tavanomaisesta poikkeaviin hankintapyrkimyksiin tai yhteydenottoihin. Yhteydenotto voi tulla esimerkiksi hiljattain perustetulta yritykseltä tai yritys voi sijaita maassa, jonka toimintaympäristö ei ole entuudestaan tuttu. Yrityksellä voi olla pitkä historia kaupankäynnistä Venäjän kanssa tai se on voinut muuttaa toimintaansa merkittävästi aikaisemmasta esimerkiksi viennin, tuonnin ja hankintojen maksujärjestelyjen osalta.

Yritysten on myös syytä kiinnittää huomiota sellaisiin liikekumppaneihin, joiden viestintä tapahtuu vain erilaisten välikäsien kautta tai valtakirjalla yritystä edustavien kanssa. On hyvä suhtautua varauksellisesti myös epätavallisiin maksujärjestelyihin, joissa ostaja esimerkiksi haluaa maksaa hankinnan kolmannen osapuolen avulla tai veroparatiiseissa sijaitsevien pankkitilien kautta.

Tehokkaalla sopimushallinnalla ja hyvällä asiakkaiden tuntemisella yritykset voivat vähentää riskiä joutua tahtomattaan osaksi pakotteiden tai vientirajoitusten kiertämisverkostoa.

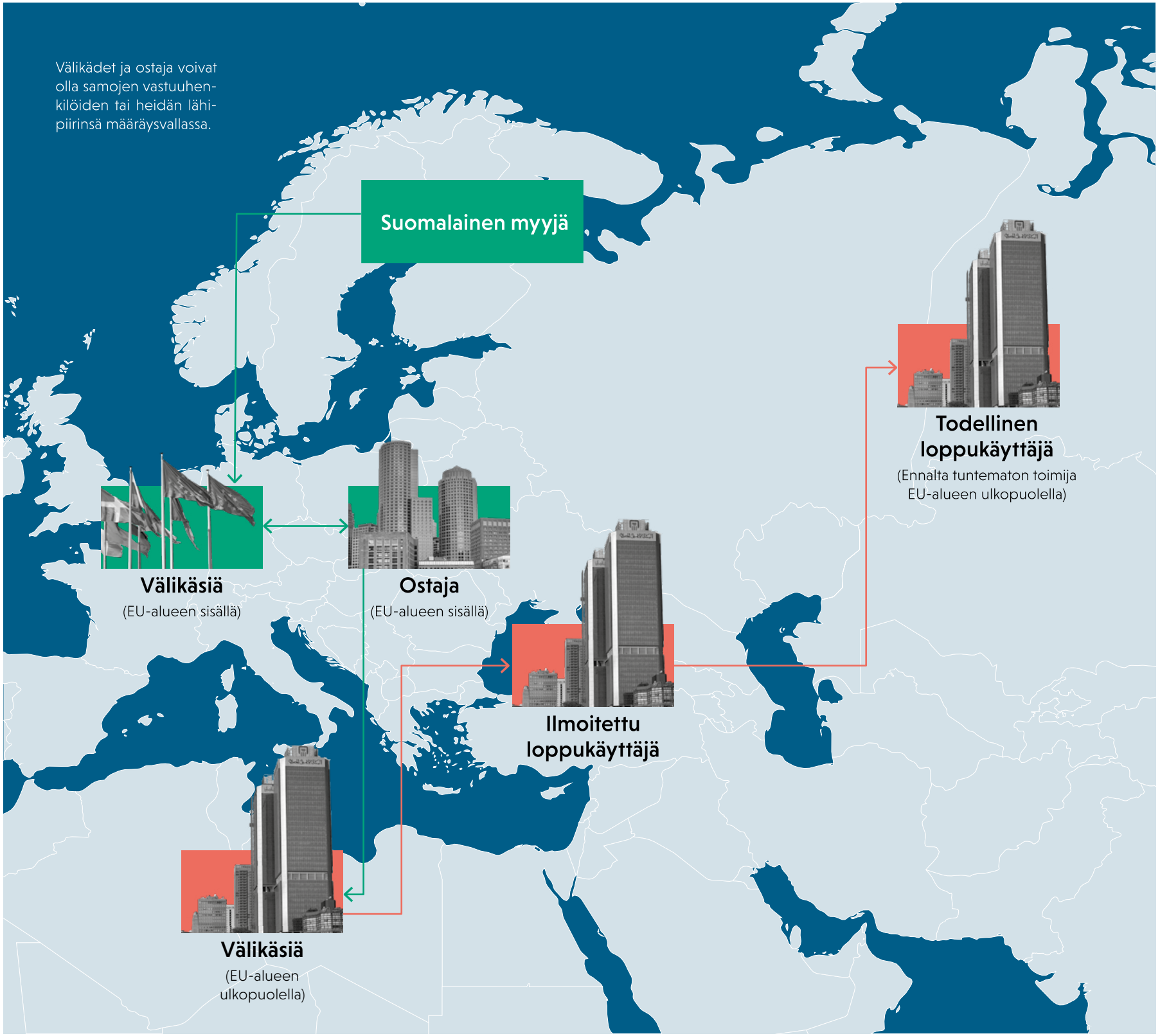
Yrityksillä vastuu pakotteiden ja vientirajoitusten noudattamisesta

Yritysten on tiedettävä, kenen kanssa ne käyvät kauppaa. Niillä on viime kädessä vastuu varmistaa, mihin myytävät tuotteet lopulta päätyvät.

Venäjä kiertää pakotteita mahdollistaakseen sodankäynnin

Euroopan unioni ja muut länsimaat ovat asettaneet pakotteita vastauksena Venäjän aloittamaan hyökkäyssotaan. Pakotteet ovat ulkopoliittisia toimenpiteitä, joiden yhtenä tavoitteena on heikentää Venäjän kykyä jatkaa hyökkäystään Ukrainaa vastaan. Pakotteet koskevat esimerkiksi energia-, kuljetus-, teknologia- ja puolustussektoreita. Viime aikoina toimenpiteitä on kohdistettu myös pakotteiden kiertämisen estämiseen.

Venäjä pyrkii kiertämään erityisesti teknologian tuontiin ja energian vientiin kohdistettuja pakotteita, koska ne vaikuttavat sen mahdollisuuksiin käydä sotaa Ukrainassa. Lisäksi se todennäköisesti pyrkii jatkossakin vaikuttamaan EU-maiden päätöksentekoon uusista pakotteista sekä kohdistamaan vastatoimia EU:n ja muiden länsimaiden asettamille pakotteille.



Yritysten ja muiden yksityisten toimijoiden on hyvä tiedostaa pakotteiden ja vientirajoitusten kiertämiseen liittyvät riskit. Yritysten johdolla on EU:n pakotteiden ja vientirajoitusten noudattamisessa rikosoikeudellinen vastuu. Liiketoimet pakotteiden alaisten toimijoiden kanssa voivat vaikuttaa kielteisesti myös yrityksen omaan liiketoimintaan sekä maksu- tai rahoitusyhteyksiin.

Rikosoikeudellisten seuraamusten lisäksi pakotteiden ja vientirajoitusten kiertämiseen osallistuminen on yritykselle merkittävä mainehaitta. Haitta ei välttämättä koske vain yrityksen omaa mainetta. Sitä voi seurata myös pakotteita tai vientirajoituksia kiertävän yrityksen sidosryhmille ja asiakkaille.

Yleisiä tullimenettelyjä ja tullirikoksia koskevissa asioissa yritykset voivat olla yhteydessä Tulliin. Pakotteisiin ja niiden tulkintaan sekä kaksikäyttötuotteiden vientirajoituksiin ja viennin luvanvaraisuuteen liittyvissä asioissa neuvoo ulkoministeriö.

Suojelupoliisin tehtävänä on valvoa yhdessä muiden viranomaisten kanssa, ettei Suomesta tai Suomen kautta viedä teknologiaa tai tuotteita, joihin kohdistuu vientirajoituksia. Jos yritys tai organisaatio joutuu epäilyttävän lähestymisen kohteeksi, asiasta voi olla yhteydessä Suojelupoliisiin verkkosivujen yhteydenottolomakkeen kautta. →

Varjolaivastolla on keskeinen rooli pakotteiden kiertämisessä

Suomenlahti on Venäjälle tärkeä öljyn ja kaasun kuljetusreitti, jonka toiminnan se haluaa turvata.

Itämerellä kulkee viikoittain kymmeniä niin sanottuun varjolaivastoon kuuluvia aluksia, joita Venäjä käyttää öljylle asetetun hintakaton ja muiden energianvientiin kohdistettujen pakotteiden kiertämiseen. Kaikkiaan Venäjän varjolaivastoon kuuluu satoja aluksia. Ne eivät kuitenkaan muodosta yhtenäistä laivastoa, sillä aluksilla on erilaisia peiteltyjä ja muuttuvia omistajuus- ja vakuutusjärjestelyjä ja ne pur jehtivat useiden valtioiden lippujen alla.

Energiaan ja sen kuljettamiseen kohdistuvien pakotteiden kiertämi sellä on suuri merkitys Venäjän talouden kannalta. Öljy- ja kaasutulot muodostavat noin kolmasosan federaatiobudjetin tuloista.

Varjolaivasto aiheuttaa merkittävän ympäristöriskin Itämerellä esi merkiksi alusten heikkokuntoisuuden, puutteellisten vakuutusten, miehistön mahdollisen epäpätevyyden ja haasteellisten navigoin tiolosuhteiden takia. Öljyonnettomuudella olisi pitkäaikaisia ympäris tövaikutuksia Itämeren rantavaltioille, todennäköisesti myös Venäjälle.

Jos läntiset rantavaltiot asettavat uusia pakotteita tai muita rajoituksia Suomenlahden käytölle, Venäjä reagoi todennäköisesti vastatoi milla. Se voi esimerkiksi informaatiovaikuttamisessaan yrittää luoda uhkakuvia sotilaallisesta eskalaatiosta, jos se tulkitsee EU-maiden rajoittavan meriliikennettään Itämerellä. Venäjän riippuvuus Suomen lahden liikenteestä kuitenkin todennäköisesti rajoittaa sen valmiutta vastatoimiin. ■

Dataa voidaan hyödyntää myös Suomea uhkaaviin tarkoituksiin

Geopolitiikka uusine riskeineen koskettaa myös datanhallintaa. Tiedon jakamista joudutaan arvioimaan yhä useammin suhteessa mahdollisiin uhkiin.

Euroopassa vallitsevana tavoitteena on ollut edistää pääsyä julkisin varoin tuotettuun dataan. Se, että joku käyttäisi dataa väärin on ollut jäännösriski – hyväksyttävissä oleva hinta siitä, että kuka tahansa voi tuottaa datan avulla näppäriä sovelluksia helpottamaan arkea.

Akateemisessa tutkimuksessa avoimen datan perinne on ollut toiminnan perusta. Se on kiistatta palvellut sekä perus- että soveltavaa tutkimusta erittäin menestyksellisesti.

Muuttuvassa turvallisuusympäristössä joudutaan enenevässä määrin huomioimaan, että dataa voidaan hyödyntää myös tarkoituksiin, jotka voivat vaarantaa vakavasti Suomen tai suomalaisten turvallisuuden.

Laskentakapasiteetin kasvaessa ja tekoälyalgoritmien kehittyessä autoritääristen valtioiden keinot hyödyntää ja yhdistää harmittomilta näyttäviä datamassoja ovat ottaneet suuren kehitysloikan.

Suomessa ymmärretään jo tarvetta suojella viestintää laitevalmistajariskiltä. Myös kriittisen infrastruktuurin sijaintitietojen avoimeen saatavuuteen on jo konkreettisesti reagoitu. Yhä useammin myös muun tiedon jakamista joudutaan arvioimaan suhteessa uhkiin, joita tiedon käyttö voi aiheuttaa. Kyse on nimenomaan riskiarviosta. On edelleen paljon tietoa, jonka avoimuuteen ei liity riskiä.

Biodataa voidaan hyödyntää sairauksien parantamiseen, mutta myös niiden luomiseen

Yksi esimerkki avoimesta datapolitiikasta on biodata eli terveys- ja geenitiedot. Suomi on kattavien, hyvin organisoitujen terveystietorekisterien maa, jossa data on ollut melko avoimesti hyödynnettävissä tutkimuskäyttöön. Tutkimusta tehdään usein kansainvälisessä akateemisessa ja kaupallisessa yhteistyössä, joten dataa on totuttu jakamaan.

Biodatan jakaminen on mahdollistanut tehokkaita tapoja kehittää lääketiedettä, mutta siihen liittyy mahdollisuus datan väärinkäyttöön. Nykyisessä geopoliittisessa tilanteessa väärinkäytön riski on kasvanut aiemmasta valtavasti.

Tällä hetkellä esimerkiksi Kiina kerää aktiivisesti eri maista biodataa, muttei jaa omaansa. Myös Venäjällä on pitkät perinteet sotilaslääketieteessä.

Vakavimmissa skenaarioissa biodataa voidaan väärinkäyttää taudinaiheuttajien kehittämiseen ja niiden leviämisvaikutusten arviointiin tietyssä kohderyhmässä. Biodataa tarjoamalla Suomi voi tahattomasti edesauttaa tällaisten sovellusten kehittämistä. Tekoälyä ja bioinformatiikkaa yhdistämällä kaikki tutkimus nopeutuu hyvässä ja pahassa. ■

Vakoilu ja vaikuttaminen

Valtiollisen vakoilun ja vaikuttamisen tilannekatsaus

Venäjä ja Kiina muodostavat merkittävimmän tiedustelullisen uhkan Suomelle. Venäjän henkilötiedustelu Suomessa on vaikeutunut, mutta sen Suomeen kohdistama kybertoiminta on lisääntynyt. Kiinan tiedustelullinen kiinnostus Suomea kohtaan on pitkäaikaista ja jatkuvaa. Suomi kiinnostaa tiedustelullisesti myös joitain kolmansia maita, kuten Irania.

Venäjä suhtautuu Suomeen epäystävällisenä maana

Venäjä on Suomelle keskeisin tiedustelun ja vaikuttamisen uhka lyhyellä ja pitkällä aikavälillä. Venäjän tiedustelua kiinnostaa Suomessa erityisesti ulko- ja turvallisuuspoliittinen päätöksenteko, kuten Suomen Nato-politiikka, ja kriittinen infrastruktuuri, sotilaallinen puolustuskyky ja puolustusteollisuus. Venäjä yrittää hankkia Suomesta tietoa niin henkilö- kuin kybertiedustelun keinoin.

Vaikuttaminen on aina kuulunut Venäjän tiedustelu- ja turvallisuuspalveluiden toimintaan, mutta sen kohteet ja aktiivisuus ovat vaihdelleet maailmanpoliittisesta tilanteesta riippuen. Natoon kuuluvat Venäjän rajanaapurit ovat sen tiedustelun erityisen mielenkiinnon kohteena. Venäjän ja länsimaiden välien viilennyttyä Venäjän vaikuttaminen on muuttunut astetta vakavampaan suuntaan, josta esimerkkinä voidaan pitää Venäjän sabotaasitoimintaa Euroopassa.

Suomessa Venäjän tiedustelupalvelut ovat hyödyntäneet perinteisiä vaikuttamisen keinoja, kuten informaatiovaikuttamista tai yhteydenpitoa poliittisiin päättäjiin ja toimittajiin. Venäjä hyödyntää erilaisia informaatiovaikuttajia länsimaiden ja Suomen vastaisten narratiivien vahvistamiseen ja historian vääristelyyn.

Venäjä pyrkii vaikuttamaan ulkomailla asuviin venäjänkielisiin muun muassa maanmiespolitiikalla sekä esimerkiksi venäjänkielisen väestön seuraaman perinteisen ja sosiaalisen median sekä pikaviestimien kautta. Tällaiset pyrkimykset eivät ole poissuljettuja Suomessakaan, mutta Venäjän vaikutusmahdollisuudet Suomen venäjänkieliseen väestöön ovat rajalliset.

Tällä hetkellä Venäjä suhtautuu Suomeen epäystävällisenä maana, joten myös suomalaisten on varauduttava aiempaa aktiivisempaan ja vihamielisempään vaikuttamiseen. Venäjä on kuitenkin sotaa käyvä maa, jonka päähuomio on muualla kuin Suomessa.

Venäjän kybertiedustelu on lisääntynyt ja tarkentunut Suomessa

Venäjän tiedustelupalveluiden Suomeen kohdistama toiminta kyberympäristössä on ollut jo vuosien ajan erittäin aktiivista, mutta se on lisääntynyt ja tarkentunut viime aikoina entisestään. Venäjän tiedustelupalveluiden Suomeen kohdistama kybertoiminta keskittyy pääosin valtionhallintoon sekä ulko- ja turvallisuuspoliittisiin kohteisiin.

Kybervakoilu tarjoaa kustannustehokkaan, monistuvan sekä ajasta ja paikasta riippumattoman väylän tiedonhankinnalle. Venäjä hyödyntää Suomea myös kyberkauttakulkumaana eli venäläiset tiedustelupalvelut käyttävät säännöllisesti Suomessa sijaitsevaa tietoverkkoinfrastruktuuria kolmansiin maihin kohdistuvissa kyberoperaatioissa.

Venäjän kybertoiminnan suorien ja epäsuorien vaikutusten riskit ovat kohonneet. Venäjä käyttää sodassaan Ukrainaa vastaan aktiivisesti kybervaikuttamista, jolla se pyrkii häiritsemään ja lamauttamaan ukrainalaisen yhteiskunnan toimintaa. Digitalisoituneessa maailmassa kybervaikuttamisen kohdistaminen ei kuitenkaan ole yksinkertaista. Siksi kyberhyökkäysten sekä informaatio-operaatioiden tahaton kohdistuminen Suomeen tai muihin ulkopuolisiin valtioihin on aiempaa todennäköisempää.

Näkyvänä ilmiönä kuluneen vuoden aikana ovat olleet venäjämielisten kyberhaktivistiryhmittymien Suomeen ja muihin länsimaihin kohdistamat palvelunestohyökkäykset. Kyberhaktivistitoiminta mukailee Venäjän etujen mukaista kybervaikuttamista ja on vähintään Venäjän valtion hyväksymää tai jopa ohjaamaa.

Venäjä on jo vuosia tarjonnut kyberrikollis- ja haktivistiryhmittymien toiminnalle suotuisat edellytykset tietyin rajoin, mutta viime vuosien aikana näihin liittyvä koordinaatio ja yhteistyö on mahdollisesti lisääntynyt. Hyödyntämällä sijaistoimijoita kybervaikuttamisessa Venäjän on mahdollista kiistää oma osallisuutensa.

Viimeaikaiset palvelunestohyökkäykset voidaan nähdä erityisesti kansalaisille suunnattuna viestinä. Niiden tavoitteena on ennen kaikkea epäluottamuksen ja pelotteen synnyttäminen.

Venäjän henkilötiedustelu on vaikeutunut Suomessa

Venäjän turvallisuus- ja tiedustelupalveluilla on perinteisesti ollut pysyvää läsnäoloa niin Suomessa kuin muissa maissa. Tiedustelupalvelujen edustajat ovat toimineet pääosin diplomaattisen peitteen suojassa.

Venäjän tiedustelun läsnäolo Suomessa ja muualla Euroopassa on kuitenkin merkittävästi vähentynyt hyökkäyssodan vastineena toteutettujen diplomaattipeitteellä toimineiden tiedustelu-upseerien karkotusten myötä. Tilanteeseen vaikuttavat myös matkustukseen kohdistuvat rajoitukset ja se, että yhä harvempi Suomessa haluaa sodan vuoksi olla tekemisissä venäläisten toimijoiden kanssa.

Venäjän henkilötiedustelun uhka ei kuitenkaan ole pitkällä aikavälillä vähentynyt, sillä Venäjän tiedontarpeet eivät ole kadonneet minnekään.

Muuttunut toimintaympäristö on ajanut myös Venäjän tiedustelu- ja turvallisuuspalvelut muuttamaan toimintaansa. Venäjä pyrkii aikaisempaa enemmän hyödyntämään välikäsiä sekä muita peitteitä kuin diplomaattipeitettä. Ne eivät tule korvaamaan laajamittaisesti tai nopeasti diplomaattipeitteen hyödyllisyyttä. Venäjä yrittää myös edelleen sijoittaa tiedustelu-upseereitaan diplomaatin tehtäviin.

Venäjän tiedustelutoimijat joutuvat enenevässä määrin toimimaan Venäjältä käsin. Tiedustelua voi kohdistua Venäjällä oleviin tai matkustaviin, Suomessa asuviin henkilöihin. Myös epäasiallisten keinojen käyttö on mahdollista Venäjällä.

Suomeen kohdistuu Kiinan vaikuttamista ja tiedustelua

Kiinan tiedustelullinen kiinnostus Suomea kohtaan on jatkuvaa ja pitkäaikaista. Kiina kohdistaa Suomeen henkilötiedustelua ja kybervakoilua. Suurvaltakilpailu, länsimaiden lisääntyvä Kiina-kriittisyys, vientirajoitteet sekä Kiinan sisäinen tilanne vaikuttavat Kiinan kiinnostuksen kohteisiin.

Kiinan tiedustelu kohdistuu ulko- ja turvallisuuspoliittiseen päätöksentekoon, arktisiin kysymyksiin, huipputeknologiaan sekä Kiinan hallinnon uhkaksi katsomiin ryhmiin. Myös Nato-jäsenyys ja sen vaikutukset Suomen suhtautumiseen Kiinaan ovat lisänneet Suomeen kohdistuvaa kiinnostusta.

Kiinan vaikuttaminen on globaalia ja myös Suomi on sen kohteena. Sitä harjoittavat useat Kiinan valtioon ja kommunistiseen puolueeseen yhdistyvät organisaatiot. Kiinan vaikuttaminen ja tiedustelu kytkeytyvät usein läheisesti toisiinsa, ja myös vaikuttamista pyritään tekemään peitellysti.

Vaikuttamisen tavoitteena on Suomessakin muun muassa ohjata poliittista päätöksentekoa ja Kiinasta käytävää keskustelua Kiinan päämäärien mukaiseen suuntaan ja välttää Kiinan näkökulmasta epätoivottavien aiheiden käsittelyä. Vaikuttamista kohdistetaan esimerkiksi poliittisiin päättäjiin, julkiseen mielipiteeseen ja Suomessa asuvaan kiinalaistaustaiseen väestöön.

Kiina harjoittaa Suomessa myös pakolaisvakoilua eli kerää tietoa, valvoo ja pyrkii kontrolloimaan Suomessa asuvia entisiä ja nykyisiä kansalaisiaan. Tyypillisesti pakolaisvakoilun kohteena ovat henkilöt, jotka edustavat jotain Kiinan hallinnon uhkaksi itselleen katsomaa ryhmää. Kiinan viranomaiset voivat kohdistaa tällaisiin henkilöihin tai heidän Kiinassa asuviin läheisiinsä häirintää.

Kiinan kyberoperaatioissa korostuvat kriittisen infrastruktuurin kohteet ja kuluttajaverkkolaitteiden hyödyntäminen

Kiina kohdistaa Suomeen kyberoperaatioitaan sekä hyödyntää aktiivisesti suomalaista tietoverkkoinfrastruktuuria kolmansiin maihin kohdistuvissa kyberoperaatioissaan. Kiinan kyberoperaatioiden kyvykkyydet ja kohdistaminen ovat viime aikoina keskittyneet lisääntyvästi länsimaiseen kriittiseen infrastruktuuriin. Kiina pyrkii luomaan mahdollisuuden länsimaihin kohdistuvaan kybervaikuttamiseen.

Kybervaikuttamiseen ja kriittiseen infrastruktuuriin kohdistuvan tiedustelu-uhkan lisääntyminen länsimaissa kasvattaa Suomen kansalliseen turvallisuuteen kohdistuvaa uhkaa.

Kiinalaiset kyberuhkatoimijat hyödyntävät operaatioissaan enenevissä määrin heikosti suojattuja kuluttajaverkkolaitteita. Näihin laitteisiin liittyvässä systemaattisessa tunkeutumisessa ja toimintainfrastruktuurin rakentamisessa hyödynnetään laajalti myös kiinalaisia it-alan yksityisiä yrityksiä. Muutoksen taustalla on sekä pienempi kiinnijäämisen riski että haavoittuvien laitteiden merkittävän suuri määrä. Yhä useammassa kuluttajalaitteessa on internetyhteys, ja erityisesti suojaamattomat ja päivittämättömät kotireitittimet muodostavat tällä hetkellä merkittävän riskin kansalliselle turvallisuudelle.

Kiina havittelee huippuosaamista ja -teknologiaa ulkomailta

Kiina tavoittelee kansainvälistä johtoasemaa keskeisissä murrosteknologioissa, joihin kuuluvat muun muassa tekoäly ja kvanttiteknologia. Kiina pyrkii hankkimaan ulkomailta teknologiaa oman taloudellisen kehityksensä tueksi muun muassa investointeja, muuta kaupallista yhteistyötä ja tutkimusyhteistyötä hyödyntäen.

Kiina hankkii ulkomailta osaamista ja teknologiaa myös sotilaallisiin tarkoituksiin. Kiinan asevoimiin linkittyy Kiinassa useita kymmeniä yliopistoja, ja Kiinan tarvitsemaa osaamista pyritään siirtämään Kiinaan myös akateemisen yhteistyön avulla.

Yhdysvaltojen Kiinalle asettamat puolijohteiden ja niiden valmistusteknologian vientirajoitteet kasvattavat Kiinan tarvetta hankkia tietoa myös tiedustelun keinoin. Myös Suomessa on runsaasti sellaista teknologista osaamista, josta Kiina on kiinnostunut.

Myös eräät muut maat kohdistavat Suomeen vakoilua

Suomi kiinnostaa tiedustelullisesti erityisesti Venäjää ja Kiinaa, mutta myös joitain muita maita, kuten Irania. Autoritaariset valtiot kohdistavat vakoilua ja vaikuttamista usein henkilöihin, jotka kuuluvat lähtömaassaan poliittiseen oppositioon tai muuhun vallanpitäjien uhkaksi katsomaan ryhmään. ■

Venäjä pyrkii vaikuttamaan sabotaasilla Euroopan maihin

Venäjän sabotaasityöt kytkeytyvät useimmiten sotilastiedustelupalvelu GRU:hun. Tuhotöiden tarkoitus on lietsoa pelkoa ja heikentää länsimaiden tukea Ukrainalle.

Useissa Euroopan maissa on nähty Venäjän tiedusteluun kytkeytyvää sabotaasia viimeisen kahden vuoden aikana. Tuhotyöt ovat yksi Venäjän vaikuttamisen muodoista Euroopassa. Toiminta on kohdistunut Euroopan isoihin maihin ja muutamaan muuhun valtioon.

Venäjän vaikuttamisen mahdollisuudet Euroopassa heikkenivät merkittävästi sen aloitettua laajamittaisen hyökkäyksen Ukrainassa vuonna 2022. Venäjä on perinteisesti hyödyntänyt diplomaattipeitettä tiedustelussaan, mutta sodan alettua länsimaat ovat karkottaneet merkittävän määrän tiedustelu-upseereja suurlähetystöistä.

Venäjän tiedustelu on joutunut muuttamaan toimintamallejaan sopeutuakseen muuttuneeseen tilanteeseen. Venäjä elää sotayhteiskunnassa, mikä on heijastunut sen tapoihin toimia myös Ukrainan ulkopuolella.

Aiempaa aktiivisempi sabotaasitoiminta on seurausta tästä kehityksestä. Toiminta kytkeytyy pääosin Venäjän sotilastiedustelupalveluun GRU:hun. Se on osa Venäjän asevoimia, joten suorempi toiminta on sille tyypillisempää kuin toiselle ulkomaantiedustelun keskeiselle toimijalle, siviilitiedustelupalvelu SVR:lle. Venäjän liittovaltion turvallisuuspalvelu FSB toimii puolestaan enimmäkseen Venäjän rajojen sisällä, vaikka silläkin on toimivaltuudet ja myös historiaa ulkomailla toimimisesta.

Sabotaasi on saanut vakavampia muotoja

Aiemmin Venäjän tiedustelun ulkomailla toteuttamalle sabotaasille oli tyypillistä, että sen toteuttamisesta vastasivat Venäjän omat koulutetut tiedustelu-upseerit. Operaatioita oli harvemmin, mutta ne olivat huolellisemmin suunniteltuja ja kohdennetumpia strategisiin kohteisiin. Tästä esimerkkejä ovat GRU:n sotilasyksikkö 29155:n toteuttamat Skripalien salamurhayritys Britanniassa ja ammusvaraston räjäyttäminen Tshekissä vuonna 2014.

Tällä hetkellä Venäjä hyödyntää tuhotöiden toteuttamisessa välikäsiä, kuten rikollisia tai muita taloudellisesta hyödystä kiinnostuneita. He saattavat toteuttaa esimerkiksi tuhopolttoja pientäkin rahaa vastaan tietämättä, kuka alkuperäinen toimeksiantaja todellisuudessa on. Sijaistoimijat rekrytoidaan tyypillisesti sosiaalisessa mediassa, eivätkä he ole kovin ammattimaisia.

Tuhotyöt ovat kohdistuneet yksinkertaisiin ja helposti lähestyttäviin symbolisiin tai varsinaisen Ukrainalle annettavan tuen kannalta toisarvoisiin kohteisiin, kuten kauppakeskuksiin tai muihin heikommin suojattuihin kohteisiin. Mahdollinen kohde on Ukrainalle annettava sotilaallinen tuki, esimerkiksi sen valmistus, kuljetus tai varastointi.

Venäjän sabotaasitoiminta Euroopassa on kuitenkin saanut entistä vaarallisempia muotoja. Venäjä osoittaa toiminnallaan välinpitämättömyyttä jopa sivullisista uhreista. Sitä kuvaavat uutiset rahtiliikenteessä kuljetetuista itsesyttyvistä paketeista, joista Saksan ja Britannian viranomaiset kertoivat vuonna 2024 julkisuuteen.

Venäjä pyrkii luomaan pelkoa

Venäjä pyrkii sabotaasilla vaikuttamaan yleiseen mielipiteeseen, kansalaisten turvallisuuden tunteeseen sekä kuormittamaan viranomaisia. Kohteilla ei itsessään ole kovinkaan suurta strategisen tason merkitystä. Esimerkiksi yksittäiset sotilaalliseen tukeen kohdistuvat tuhotyöt eivät vaikuttaisi merkittävällä tavalla rintamatilanteeseen Ukrainassa.

Haettu vaikutus on enemmän psykologinen. Venäjä haluaa luoda uhkatilan, jolla se yrittää vaikuttaa päätöksiin länsimaissa. Koska toiminnan taustalla on GRU, ovat myös tavoitteet sotilaalliset.

Varsinainen päätavoite on, että yleinen mielipide lännessä kääntyisi Ukrainan tukemista vastaan.

Venäjä pyrkii osoittamaan kykyään toimia myös lännessä sekä hakemaan neuvotteluasemia tulevaisuutta ajatellen. Vaikka toiminnan kohteet eivät ole strategisesti yhtä merkittäviä kuin aiemmin, niiden vaikutus on kasvanut.

Venäjän tiedustelupalveluiden toiminnassa voidaan hyvinkin nähdä muutoksia tulevaisuudessa. Kun sabotaasitapauksia tulee julkisuuteen, Venäjä voi keksiä uusia vaikuttamisen keinoja. Venäjä toimii usein opportunistisesti eli kokeilee erilaisia toimintatapoja, joista se kerää saatavilla olevat hyödyt.

Muutokset Venäjän ja lännen suhteissa vaikuttavat myös Venäjän toimintatapoihin. Jos esimerkiksi Venäjän tiedustelun toimintaedellytykset lännessä paranevat, Venäjä voi hyvinkin painottaa jälleen klassisempia tiedustelukeinoja toiminnassaan. Vasta pidemmällä aikavälillä nähdään, vakiintuuko nykyinen sabotaasitoiminta Venäjän tavaksi toimia.

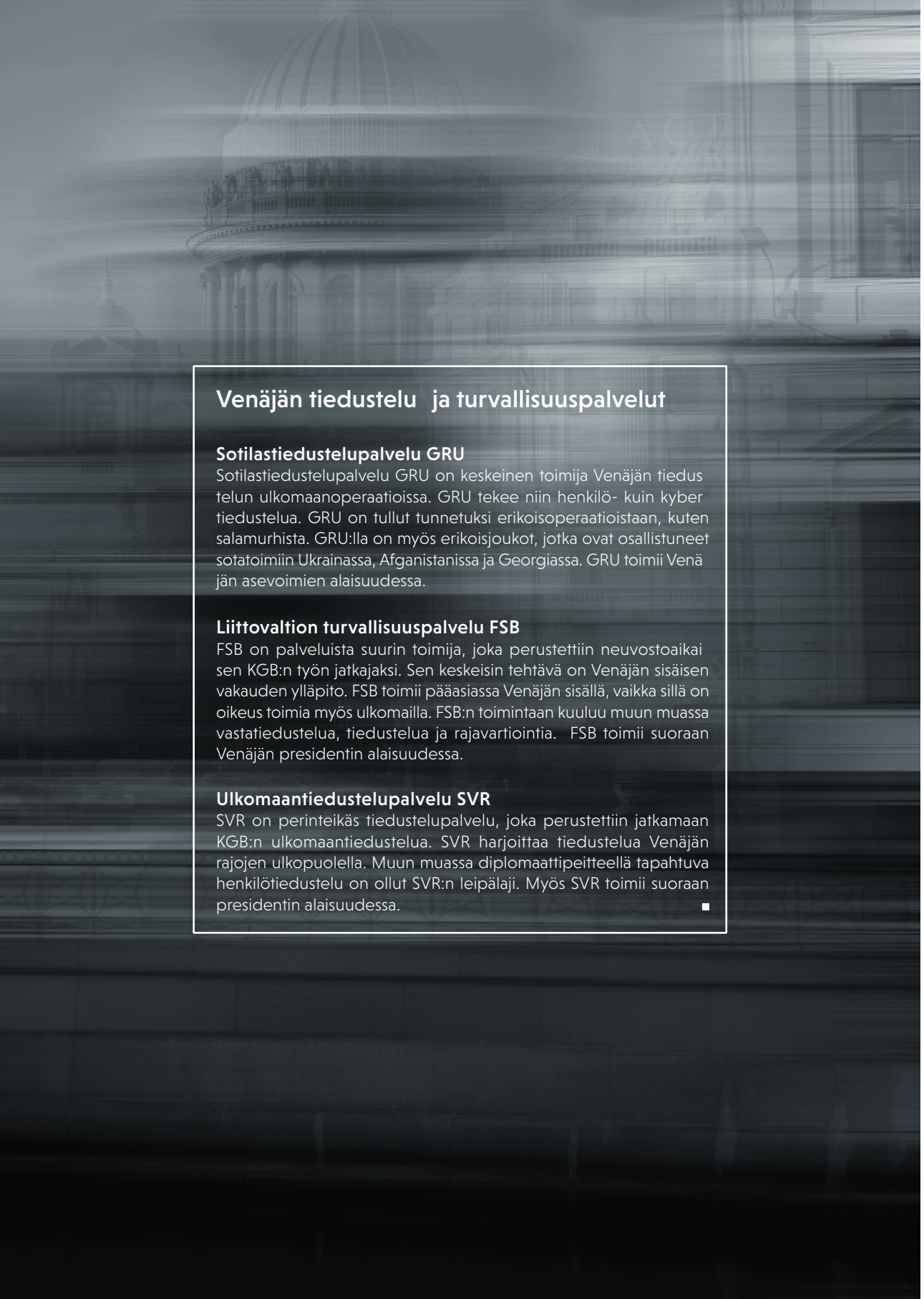
Suomi ei ole keskeisin kohde, mutta sabotaasia ei voida poissulkea

Suomi ei ole todennäköisesti vaikuttavuuden ja huomioarvon kannalta erityisen keskeinen kohde Venäjän toiminnalle. Suomi ei ole Venäjän näkökulmasta keskeinen toimija, joka voisi vaikuttaa länsirintaman päätöksentekoon.

Sabotaasin uhka on silti todellinen ja otettava vakavasti täälläkin. Suomi on muuttunut Venäjän näkökulmasta epäystävälliseksi maaksi ja tiukentanut kannanottojaan Venäjää kohtaan. Suojelupoliisi on huomioinut sabotaasiuhkan arvioissaan jo jonkin aikaa.

Myös Suomessa Venäjän tukeman sabotaasitoiminnan todennäköisin kohde olisivat Ukrainan materiaalitukeen liittyvät toimijat, kuten puolustusteollisuus. Venäjän sabotaasitoiminta ei tällä hetkellä uhkaa kriittisten palveluiden toimintaa.

→



Venäjän tiedustelu ja turvallisuuspalvelut

Sotilastiedustelupalvelu GRU
Sotilastiedustelupalvelu GRU on keskeinen toimija Venäjän tiedus telun ulkomaanoperaatioissa. GRU tekee niin henkilö- kuin kyber tiedustelua. GRU on tullut tunnetuksi erikoisoperaatioistaan, kuten salamurhista. GRU:lla on myös erikoisjoukot, jotka ovat osallistuneet sotatoimiin Ukrainassa, Afganistanissa ja Georgiassa. GRU toimii Venä jän asevoimien alaisuudessa.

Liittovaltion turvallisuuspalvelu FSB
FSB on palveluista suurin toimija, joka perustettiin neuvostoaikai sen KGB:n työn jatkajaksi. Sen keskeisin tehtävä on Venäjän sisäisen vakauden ylläpito. FSB toimii pääasiassa Venäjän sisällä, vaikka sillä on oikeus toimia myös ulkomailla. FSB:n toimintaan kuuluu muun muassa vastatiedustelua, tiedustelua ja rajavartiointia. FSB toimii suoraan Venäjän presidentin alaisuudessa.

Ulkomaantiedustelupalvelu SVR
SVR on perinteikäs tiedustelupalvelu, joka perustettiin jatkamaan KGB:n ulkomaantiedustelua. SVR harjoittaa tiedustelua Venäjän rajojen ulkopuolella. Muun muassa diplomaattipeitteellä tapahtuva henkilötiedustelu on ollut SVR:n leipälaji. Myös SVR toimii suoraan presidentin alaisuudessa. ■

Autoritaaristen valtioiden kyberekosysteemit uhkaavat kansainvälistä vakautta

Pärjätäkseen jatkuvasti kehittyvässä kybermaailmassa valtiot tarvitsevat viranomaisten ohella akateemisten instituutioiden, yksityisten yritysten ja asiantuntijoiden osaamista. Eri toimijoiden kykyjen ja valmiuksien yhdistymistä monimutkaisissa verkostoissa kutsutaan kyberekosysteemeiksi. Autoritaarisissa maissa, kuten Venäjällä ja Kiinassa, kyberalan yritykset ja tutkijat voivat joutua myös osaksi valtiollisen vakoilun ja vaikuttamisen koneistoa.

Kybermaailmasta on tullut geopoliittisen voimannäytön pelikenttä. Nopeasti digitalisoituneessa maailmassa valtiot ovat joutuneet keskittämään resursseja torjunnallisiin kybersuorituskykyihin. Vahvat kyberekosysteemit edistävät valtioiden kansallista turvallisuutta ja resilienssiä kyberuhkiin kokonaisvaltaisemmin. Geopoliittisten jännitteiden kasvaessa rajat torjunnallisten ja hyökkäyksellisten suorituskykyjen ja tavoitteiden välillä ovat kuitenkin hämärtyneet. Erityisesti autoritaarisissa valtioissa kyberalan kehitystyö on keskittynyt kansallisten kyberturvallisuusresurssien valjastamiseen osaksi valtiollisten intressien mukaista tiedustelua ja vaikuttamista. Samoja suorituskykyjä käytetään autoritaarisissa valtioissa myös sisäiseen kontrollointiin.

Sekä Venäjällä että Kiinassa valtionhallinnot ovat pyrkineet saamaan kyberalan yritysten ja asiantuntijoiden tietotaidon osaksi vakoilu- ja vaikuttamiskoneistoaan. Tätä molemmat valtiot ovat edistäneet muun muassa kiristämällä lainsäädäntöä, panostamalla kyberalan tutkimukseen ja koulutukseen sekä lisäämällä yksityisen sektorin osuutta palveluntuotannossa. Erityisesti Kiina on vienyt kyberekosysteeminsä ennennäkemättömään laajuuteen.

Mikä kyberekosysteemi?

Kukaan ei voi yksin puolustaa valtiota kyberympäristössä, vaan siihen tarvitaan eri toimijoiden yhteistoimintaa. Kyberekosysteemit muodostuvat kyberympäristön turvaamiseen tai palveluntuotantoon osallistuvista yrityksistä, tiedustelu- ja turvallisuusviranomaisista, asevoimista, tutkimuslaitoksista, mediasta ja muista organisaatioista, joita tarvitaan kansallisen turvallisuuden suojaamiseen kyberympäristössä. Kyberekosysteemit yhdistävät näiden eri toimijoiden resurssit ja valmiudet palvelemaan valtioiden kansallista kyberturvallisuutta kokonaisvaltaisemmin.

Koulutus- ja tutkimussektori

Julkinen sektori

Yksityinen sektori

Velvoitteet

Kannustimet

Ohjaus

VENÄJÄ, KIINA
Seikkaperäinen lainsäädäntö
Lait, säädökset ja teknologiset standardit ohjaavat kyberturvallisuusalan tutkimusta, tiedonhallintaa ja koulutusta, palvelu-, ohjelmisto- ja laitekehitystä sekä rajat ylittävää tietoliikennettä.

KIINA
Tiedonjaon rajoittaminen
Kyberturvallisuuteen liittyvää julkista, erityisesti kansainvälistä tiedonjakoa rajoitetaan muun muassa ilmaisukielloin sekä estämällä kyberasiantuntijoiden osallistuminen kansainvälisiin tietoturvatapahtumiin.

KIINA
Haavoittuvuuksien pakkokeräys
Yritykset, tietoturvatutkijat ja asiantuntijat on velvoitettu viipymättä ilmoittamaan kaikki ohjelmisto- ja laitehaavoittuvuudet valtiolle. Ilmoitusvelvollisuuteen on sidottu myös ilmaisukielto ja korjaustoimien rajoitus.

VENÄJÄ, KIINA
Velvollisuus luovuttaa tietoa ja pääsyoikeuksia viranomaisille
Kiinassa toimivat laite- ja palveluntarjoajat ovat velvoitettuja avustamaan tiedusteluviranomaisia muun muassa tietoja ja pääsyjä luovuttamalla.

VENÄJÄ, KIINA
Rahoitus
Valtio rahoittaa kansallista tietoturvahaavoittuvuuksiin ja kybersodankäyntiin liittyvää tutkimusta.

KIINA, OSIN VENÄJÄ
Palveluostot alihankkijoilta
Freelance-toimijat toteuttavat itsenäistä kybervakoilua ja tunkeutumisia palvelumuotoisesti.

KIINA, OSIN VENÄJÄ
Yritysten osallistaminen tiedusteluun
Yksityiset yritykset tuottavat Kiinan tiedustelupalveluille työkaluja ja infrastruktuuria alihankintana.

VENÄJÄ, KIINA
Koulutusohjelmat
Kiina on lisännyt kansallisia kyberturvallisuuteen keskittyviä koulutusohjelmia ja -linjoja, sekä kansallisia akkreditointi- ja sertifiointiohjelmia.

VENÄJÄ, KIINA
Kybertapahtumat
Kansalliset kyberturvallisuus-alan tapahtumat toimivat tiedonhankinta- ja rekrytointi-alustoina turvallisuus- ja tiedustelupalveluille.

KIINA
Haavoittuvuus-tietokanta
Kansallinen haavoittuvuus-tietokanta mahdollistaa tiedusteluviranomaisille jatkuvan pääsyn uusimpiin hyökkäysvektoreihin.

VENÄJÄ, KIINA
Autoritaarinen hallinto
Teollisuuteen, informaatioteknologiaan ja kansalliseen turvallisuuteen keskittyvien ministeriöiden sekä näiden alaisten elinten ja yhdistysten toiminta on vahvasti valtion ylimmän johdon alaisuudessa.

KIINA, OSIN VENÄJÄ
Yritykset viranomaispeitteenä
Kiinan tiedusteluviranomaiset käyttävät tietoturva-alan toimijoiksi naamioituja peiteyrityksiä kybervakoilussaan.

Analyysi

Venäjälle kyberympäristö on modernien konfliktien pelikenttä

Venäjän kyberekosysteemi yhdistää perinteistä propagandaa ja nykyaikaista teknologiaa.

Venäjän suhtautuminen kyberympäristöön on kaksijakoinen. Toisaalta kyberympäristö on Venäjälle valtion sisäistä vakautta, kulttuuria, arvoja ja kansallista identiteettiä uhkaava vaikuttamisalusta, minkä vuoksi maa tavoittelee riippuvuuden vähentämistä länsimaisesta teknologiasta. Venäjä haluaa rajoittaa kansalaistensa pääsyä vapaaseen internetiin, mutta myös rajoittaa länsimaiden edellytyksiä vakoilla tai vaikuttaa Venäjän järjestelmiin. Samanaikaisesti Venäjä aktiivisesti käyttää kyberympäristöä välineenä valtiollisten intressien saavuttamisessa ja vaalii Venäjän ulkopuolelle kohdistuvan kyberrikollisuuden kukoistamista maassa.

Venäjä näkee informaatioympäristön konfliktien pelikenttänä. Tämä ajatus on luotsannut Venäjää määrätietoisesti organisoimaan maahan kyberekosysteemiä, jossa valtio saa kybertoimintoihinsa tukea muulta yhteiskunnalta. Venäjän kyberekosysteemin ytimessä on ylin valtiojohto sekä turvallisuus- ja tiedustelupalvelut, jotka vastaavat kansallisten kyberresurssien strategisesta suunnittelusta, priorisoinnista sekä jalkauttamisesta. Venäjä onkin onnistunut luomaan järjestelmän, joka yhdistää perinteisen propagandan ja nykyaikaisen teknologian.

Muuntautumiskykyistä kyberekosysteemiä on koeteltu käytännössä

Venäjä on rakentanut kyberekosysteemiään monella saralla. Se on panostanut kyberturvallisuusalan asiantuntijoiden kouluttamiseen niin korkeakouluissa kuin turvallisuusviranomaisten omissa koulutusohjelmissa. Akateemiset instituutiot tukevat valtiollista kybertoimintaa myös kehitystyöllä ja asiantuntemuksella.

Venäjä on myös investoinut kansalliseen kyberturvallisuus-, informaatio-, viestintä- ja teknologia-alaan, sekä lainsäädännön keinoin vahvistanut mahdollisuuksiaan hyödyntää yksityisen sektorin toimijoiden hallussa olevaa tietoa tiedustelussa ja vaikuttamisessa. Valtiolliset ja valtion tukemat mediaorganisaatiot levittävät Venäjän intressien mukaisia narratiiveja. Myös tarkasti säännellyt kansalliset teknologia- ja viestintäalustat tarjoavat mahdollisuuksia informaatiovirtojen valvonnalle ja kontrolloinnille.

Näiden eri suorituskykyjen yhdistäminen tekee Venäjän kyberekosysteemistä muuntautumiskykyisen kokonaisuuden, jota maan turvallisuusviranomaiset ovat konkreettisesti hyödyntäneet sekä Ukrainaan kohdistuvissa sotatoimissa että länsimaihin kohdistuvassa vaikuttamisessa ja vakoilussa. Ulko- ja turvallisuuspoliittisen tiedon lisäksi Venäjä on kybertoiminnallaan pyrkinyt hankkimaan tietoa, jota on myöhemmin hyödynnetty vaikuttamisen välineenä.

Lisäksi Venäjän tiedusteluviranomaiset ovat toteuttaneet lukuisia kybersabotaasioperaatioita, joilla on pyritty häiritsemään Ukrainan yhteiskunnan toimintaa. Yhteistä toiminnalle on ollut pelon, epävarmuuden ja epäluottamuksen aiheuttaminen ja siten kansallisen ja kansainvälisen yhtenäisyyden heikentäminen Venäjän näkökulmasta "epäystävällisiksi" luokitelluissa maissa ja eri liittoumissa.

Venäjä pyrkii eristäytymään länsimaisesta internetistä

Venäjä näkee informaation jatkuvan hallinnan tärkeänä osana digitaalisen suvereniteettinsa säilyttämistä. Maan hallinto kokee, että kansallista informaatiotilaa tulisi suojata ulkopuoliselta vaikuttamiselta. Virallisesti Venäjä on asettanut tavoitteekseen vihamielisen ulkomaisen toiminnan torjunnan sekä Venäjän kulttuurin ja arvojen edistämisen, mutta tosiasiassa myös tiedon vapaa saatavuus on merkittävä uhka autoritaariselle hallintojärjestelmälle.

Venäjä on pyrkinyt estämään länsimaisille uutissivustoille pääsyn tavallisilta venäläisiltä ja samalla se on sulkenut useiden venäläisten viranomaisten verkkosivustot länsimaisilta käyttäjiltä. Venäjä on myös määrätietoisesti pyrkinyt irrottautumaan länsimaisten tietoverkkojen suunnitteluperiaatteista, kuten tietoturvallisesti toteutetuista salausjärjestelmistä.

Osana tavoitteitaan saada internet laajemmin valtion kontrolliin, Venäjä on myös pitkäjänteisesti kehittänyt kansallisia vaihtoehtoja tietoliikenneverkoille, tiedontallennukseen ja viestintään. Korvaamalla ulkomailla tuotettuja palveluita kansallisesti tuotetuilla ratkaisuilla Venäjä pyrkii kontrolloimaan sitä internetin osaa, joka sijaitsee fyysisesti Venäjän valtion rajojen sisäpuolella tai Venäjän oikeudellisen vallan alla.

Venäjä mahdollistaa kyberrikollisuuden tarkoituksella

Venäjä on myös jo vuosia tarjonnut suotuisat edellytykset rikolliselle kybertoiminnalle, edellyttäen että toiminta kohdistuu Venäjän ulkopuolelle eikä toiminta ole ristiriidassa Venäjän kansallisten tai ulkopoliittisten intressien kanssa. Kyberrikollisten toimintatapoihin ovat kuuluneet esimerkiksi kiristyshaittaohjelmien avulla toteutetut hyökkäykset, joista Suomikin on saanut osansa.

Tämä hallinnon ja kyberrikollisten sekä haktivistiryhmien yhteiselo on saanut uusia muotoja geopoliittisten jännitteiden lisäännyttyä etenkin Venäjän käynnistämän hyökkäyssodan jälkeen. Niin kutsuttujen venäjämielisten haktivistien toteuttamat palvelunestohyökkäykset ovat säännöllisesti kohdistuneet länsimaihin – Suomi mukaan luettuna. Lisääntynyt haktivismi ja kyberrikollisuus mukailevat Venäjän intressejä heikentää länsimaiden kansalaisten luottamusta yhteiskunnan toimintaan, vaikka ne eivät kaikissa tapauksissa olisikaan valtiollisten tahojen ohjaamia. Sijaistoimijoiden kautta tapahtuva vaikuttaminen antaa Venäjälle mahdollisuuden kiistää oma osallisuutensa.

Analyysi

Kiina tavoittelee kybersuurvalta-asemaa

Kiinan mittakaavaltaan poikkeuksellinen kyberekosysteemi aiheuttaa merkittävän haasteen länsimaille.

Kiinan kyberekosysteemiä määrittää sen poikkeuksellinen laajuus. Maa on kehittänyt kybersuorituskykynsä tasolle, jolla sen kyberresurssit ovat moninkertaiset useimpiin länsimaihin verrattuna. Tilanne on seurausta jo vuosikymmenen ajan jatkuneesta pitkäjänteisestä työstä, jossa maan informaatioteknologia- ja kyberturvallisuusalat on valjastettu valtion kybersuorituskykyjen maksimoimiseen keskitetyn ohjauksen ja lainsäädännön keinoin.

Kiinan pyrkimys saavuttaa teknologinen suurvalta-asema on toiminut maan kyberekosysteemin kehityksen tavoitteena. Kiina hyödyntää suorituskykyjään poliittisen ja taloudellisen vaikuttamisen sekä tiedonhankinnan lisäksi sisäisen ja ulkoisen kontrollin välineenä. Taloudellisen vaikuttamisen avulla Kiina myös parantaa omia kybertoiminnan edellytyksiään ulkomailla, mutta yhtä lailla parantaa taloudellisen vaikuttamisen edellytyksiään kybertoiminnallaan.

Kiinan kybervakoilun mittakaava on kasvanut viime aikoina merkittävästi ja johtanut mittaviin poliittisesti ja taloudellisesti merkittävien tietojen anastuksiin. Kiinan kyberoperaatiot kehittyvät jatkuvasti, ja ne hyödyntävät alati edistyneempiä menetelmiä. Valtion kyberoperaatiot eivät enää keskity pelkkään tiedonhankintaan vaan tähtäävät aktiivisesti luomaan mahdollisuuksia kybervaikuttamiselle muun muassa länsimaiseen kriittiseen infrastruktuuriin tunkeutumalla.

Kiinan panostukset kyberekosysteemiinsä ovat muovanneet kyberturvallisuuskenttää perustavanlaatuisesti ja aiheuttavat nyt merkittävän uhan Suomen ja muiden länsimaiden kansalliselle turvallisuudelle ja vakaudelle. Länsimaat kohtaavat aiempaa monimutkaisemman haasteen, jossa Kiinan on niin halutessaan mahdollista hyödyntää laaja-alaisesti ja joustavasti kaikkia kyberturvallisuussektorin resursseja taloudellisten, poliittisten että sotilaallisten tavoitteidensa saavuttamiseen.

Kiinan kommunistinen puolue ja tiedusteluviranomaiset kyberekosysteemin ytimessä

Venäjän ja monen muun maan tavoin myös Kiina on keskittänyt kyberalan sääntelyä ja koordinointia suoraan valtiojohdon alaisuuteen. Kiinassa tämä tarkoittaa kommunistisen puolueen merkittävää roolia kyberalan ohjauksessa. Kyberhallintoon keskittyvät elimet johtavat kansallisia kyberstrategioita ja pyrkivät perinteisen diplomatian keinoin muovaamaan kansainvälisen yhteisön kybertoiminnan normeja ja standardeja mukailemaan Kiinan kansallisia intressejä. Tiedusteluviranomaisten hyökkäyksellisiä kyberoperaatioita voidaan ohjata suoraan valtion johdosta.

Lisäksi lait, säädökset ja teknologiset standardit ohjaavat laajasti kyberturvallisuusalan koulutusta, tutkimusta ja tiedonhallintaa, mutta myös velvoittavat kyberalan organisaatiot ja yksityishenkilöt tukemaan Kiinan intressien mukaista tiedustelu- ja vakoilutoimintaa. Kaiken tämän ohella viranomaiset suuntaavat taloudellisin kannustimin yksityisten yritysten palvelu-, ohjelmisto- ja laitekehitystä vastaamaan tiedustelutoiminnan tarpeita.

Keskitetyn ohjauksen ja lainsäädännön keinoin Kiinan on ollut mahdollista valjastaa maan eri toimijat ainutlaatuiseksi kyberekosysteemiksi virastojen ja tiedustelupalveluiden ympärille. Esimerkiksi yksityinen sektori edistää Kiinan tiedustelutoimintaa alihankintaroolissa tuottamalla maan turvallisuus- ja tiedustelupalveluille soveltuvaa kyberinfrastruktuuria ja -työkaluja.

Kiina on lisäksi onnistunut luomaan kannustimia haitallisen kybertoiminnan toteuttamiselle: yksityiset alihankkijat toteuttavat tunkeutumisia ja kybervakoilua itsenäisesti tiedusteluviranomaisten intressejä mukaillen. Myös tietoturva-alan toimijoiksi naamioidut peiteyritykset korostuvat Kiinan kansainvälisissä kybervakoiluoperaatioissa.

Kiinan kyberekosysteemi antaa sille potentiaalisen etulyöntiaseman myös mahdollisissa konfliktitilanteissa – monipuolinen kyberalan toimijoista koostuva verkosto pystyy nopeasti tuottamaan kybersuorituskykyjä kulloistenkin tarpeiden mukaan, mutta myös tarjoamaan ennalta estävää tai pelotetta luovaa suojaa Kiinan vastaiselle toiminnalle.

Kiina integroi koulutus-, tutkimus- ja yrityssektorin osaksi kybertoimintaa

Kiinan kyberekosysteemi ulottuu vahvasti koulutus- ja tutkimussektorille. Kiinan valtio rahoittaa kiinalaisten korkeakoulujen ja tutkimusorganisaatioiden tietoturvahaavoittuvuuksiin ja kybersodankäyntiin liittyvää tutkimusta. Kiina kerää tietoja haavoittuvuuksista kansalliseen haavoittuvuustietokantaan, josta ne ovat välittömästi turvallisuus- ja tiedustelupalveluiden käytettävissä.

Kiina tukee avokätisesti ulkomaisiin yliopistoihin lähteviä opiskelijoita rahoituksella, joka velvoittaa heidät palaamaan opintojen jälkeen määräajaksi Kiinaan. Samanaikaisesti Kiina kuitenkin rajoittaa kiinalaisten tietoturvatutkijoiden mahdollisuuksia osallistua kansainvälisiin tietoturva-alan tapahtumiin ja kilpailuihin, joissa nämä voisivat tuoda esiin löytämiään haavoittuvuuksia laajoille yleisöille. Sen sijaan Kiina on panostanut vahvasti valtiollisten instituutioiden ja yksityisen sektorin toimijoiden yhteistyössä järjestämiin kansallisiin tietoturvatapahtumiin, jotka palvelevat teknologisten kykyjen kartoittamisfoorumeina.

Kiina hyödyntää koulutussektoria paikkaamaan kyberturvallisuusstrategiassa tunnistettua kyberosaamisvajetta lisäämällä kyberturvallisuuteen keskittyviä koulutusohjelmia ja -linjoja. Yksittäiset kiinalaiset korkeakoulut ovat myös tukeneet suoraan Kiinan tiedusteluviranomaisten kybervakoilutoimintaa kansainvälisen kohde- ja haavoittuvuuskartoituksen sekä kybermenetelmien innovaatioiden, kehitystyön ja asiantuntemuksen kautta. Sekä kansalliset tietoturvatapahtumat että korkeakoulut toimivat työntekijöiden rekrytointialustana turvallisuus- ja tiedustelupalveluille. ■

Kiina hyödyntää sosiaalisen median alustoja tiedustelussaan

Sosiaalisen median kautta tapahtuvassa etävärväyksessä kiinnijäämisen riski on tiedustelutoimijalle kasvokkaista kohtaamista pienempi. Somealustoilla tapahtuvia yhteydenottoja voi olla vaikea tunnistaa Kiinan tiedusteluun liittyviksi.

Kiinalaiset tiedustelutoimijat

Kiinalla on useita tiedusteluun ja vaikuttamiseen erikoistuneita valtiollisia organisaatioita.

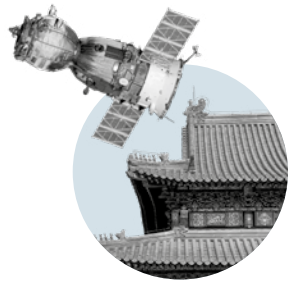
Kiinan siviilitiedustelupalvelu MSS harjoittaa vastatiedustelu- ja tiedustelutoimintaa, muun muassa ulkomaille suuntautuvaa henkilö- ja kybertiedustelua.

Kiinan sotilastiedustelupalvelu MID

Kiinan yleisen turvallisuuden ministeriö MPS on keskeisessä vastuussa muun muassa Kiinan poliisivoimista, rikostutkinnasta, terrorismintorjunnasta, rajavalvonnasta ja maahanmuutosta, mutta se suorittaa myös vastatiedustelua ja ulkomaanoperaatioita.

Kiinan kommunistisen puolueen kansainvälinen osasto ylläpitää Kiinan kommunistisen puolueen (KKP) suhteita muiden maiden poliittisiin puolueisiin, mutta kerää myös tietoa muiden maiden poliittisista tilanteista sekä pyrkii edistämään positiivista kuvaa Kiinasta muiden maiden päätöksentekijöiden keskuudessa.

Yhdistynyt työrintamaosasto UFWD on Kiinan kommunistisen puolueen alainen elin, joka on pääkoordinaatiovastuussa yhteisrintamatyöstä. Yhteisrintamatyön tavoitteena on edistää Kiinan kommunistisen puolueen etuja niin Kiinassa kuin sen ulkopuolella muun muassa osallistamalla Kiinan ulkopuolella asuvia kiinalaistaustaisia henkilöitä KKP:n etujen mukaiseen vaikuttamistoimintaan.



Kiinan tiedustelupalvelut käyttävät aktiivisesti henkilötietolähteiden värväämiseen eri sosiaalisen median alustoja, kuten LinkedIniä. Myös suomalaiset ovat kiinnostavia kohteita Kiinan tiedustelulle.

Kiinan tiedustelupalveluille henkilötietolähteiden värvääminen tai tähän pyrkiminen sosiaalisen median alustoilla on tehokasta ja taloudellista toteuttaa. LinkedInin kaltaisilla alustoilla sopivia kohteita on helppo valikoida ja lähestyä.

Sosiaalisen median alustojen käyttöön sisältyy pienempi kiinnijäämisen riski verrattuna kasvokkain tapahtuvaan henkilötiedusteluun, koska toimijan ei tarvitse fyysisesti poistua kotimaastaan. Yhteydenottoja voi olla vaikea todentaa etenkin aluksi Kiinan tiedustelutoimintaan liittyviksi.

Värväystoiminnan lisäksi tiedustelupalvelut keräävät sosiaalisen median alustoilta aktiivisesti tietoa eri käyttötarkoituksiin.

Lähestymisyritys vaikeasti tunnistettavissa

Värväysprosessi LinkedInissä alkaa tyypillisesti siten, että tiedustelu-upseeri tai hänen laskuunsa toimiva henkilö lähestyy kohdehenkilöä jonkin yrityksen nimissä. Hän saattaa pyytää kohdetta kirjoittamaan raportin tai käymään hänen kanssaan konsultaatiokeskustelun jostakin Kiinaa kiinnostavasta aiheesta, kuten esimerkiksi poliittisesta päätöksenteosta tai huipputeknologian osaamisesta.

Palvelun pyytäjä ei välttämättä ole suoraan yhdistettävissä Kiinaan. Hän voi esiintyä esimerkiksi kuvitteellisen tai todellisen, Kiinaan näennäisesti kytkeytymättömän rekrytointi- tai konsultointiyrityksen edustajana.

Alkuvaiheessa pyydetty tieto on usein saatavilla julkisista lähteistä. Pyyntöön voi sisältyä myös jokin palkkio. Jos kohde suostuu pyyntöön, häneltä voidaan myöhemmin pyytää tietoa salaisemmasta aineistosta. Kohde voidaan yrittää myös houkutella matkustamaan Kiinaan.

Jos alkuperäinen yhteydenottaja ei ole itse tiedustelu-upseeri, hän pyrkii jossain vaiheessa siirtämään yhteydenpidon varsinaiselle tiedustelu-upseerille.

Epäilyttävistä yhteydenotoista yhteys Suojelupoliisiin

Tiedustelu ja värväysyritykset muun muassa LinkedInissä ovat Kiinan tiedustelun vakiintunut toimintatapa. Epätavallisiin ja odottamattomiin yhteydenottoihin kannattaa suhtautua epäilevästi. Niistä on hyvä kertoa ensisijaisesti oman organisaation turvallisuudesta vastaavalle taholle.

Epäillyistä värväysyrityksistä voi olla yhteydessä myös Suojelupoliisiin. Yhteydenotto kannattaa, vaikka mahdollinen värväysprosessi olisi edennyt jo pidemmälle.

Kiinan tiedustelupalvelut jatkavat erittäin todennäköisesti sosiaalisen median alustoilla toimimista myös tulevaisuudessa. Todennäköisesti Kiinan tiedustelupalvelut pyrkivät kehittämään toimintatapojaan entistä hienostuneemmiksi siten, että yhteydenottoa on yhä vaikeampaa yhdistää Kiinaan. Yhteydenotot saatetaan jatkossa naamioida esimerkiksi työpaikan rekrytointiprosessin taakse. Myös tekoälyn hyödyntäminen tuo toimintatapaan uusia mahdollisuuksia.

Jos yhteydenottaja pyytää enenevissä määrin arkaluontoista tietoa tai kutsuu Kiinaan, kyse voi olla Kiinan tiedustelupalveluihin liittyvästä yhteydenotosta. ■

Terrorismi

Kansallinen terrorismin uhka-arvio 2025

Suojelupoliisi on ottanut käyttöön uuden viisiportaisen terrorismin uhkatasoasteikon. Uudella asteikolla äärioikeistolaisen ja radikaali-islamistisen terrorismin uhka on tasolla kolme, kohonnut. Todennäköisimmän isku-uhkan muodostavat edelleen yksittäiset äärioikeistolaisen tai radikaali-islamistisen ideologian kannattajat tai pienryhmät.

Uudella asteikolla äärioikeistolaisen ja radikaali-islamistisen terrorismin uhka on tasolla kolme, *kohonnut*. Tämä on lievä nousu verrattuna aiempaan uhkatasoon. Viime vuosien aikana Suomen turvallisuusympäristössä on havaittu useita kehityskulkuja, jotka kohottavat terrorismin uhkaa.

Todennäköisimmän isku-uhkan muodostavat edelleen äärioikeistolaista tai radikaali-islamistista ideologiaa kannattavat yksittäiset henkilöt tai pienryhmät. Suomessa on henkilöitä, joilla on motivaatio ja kyky terrori-iskujen tekemiseen. Muun terrorismin uhka on matala.

Terrori-iskuilla länsimaissa on todennäköisesti inspiraatiovaikutusta myös Suomessa. Ääritoimijoiden propagandassa korostuvat kansainvälisesti yksittäiset väestöryhmät, kuten etniset, uskonnolliset ja seksuaalivähemmistöt sekä viranomaiset ja poliittiset päättäjät. Lähi-idän konfliktien eskaloituminen on aktivoinut eri ääri-ideologioiden edustajia Euroopassa, mikä vaikuttaa terrorismin uhkatasoon myös Suomessa.

Nuorten verkkoon painottuva radikalisoituminen on keskeinen kansainvälinen trendi. Se näkyy myös Suomessa sekä radikaali-islamistisessa että äärioikeistolaisessa toimintaympäristössä. Nuorten radikalisoituminen näkyy lähitulevaisuudessa todennäköisesti myös terrorismin torjunnan kohdehenkilöiden joukossa. Nuorten radikalisoitumisessa on havaittu yleisen väkivaltakiinnostuksen korostumista, ja nuorten on havaittu radikalisoituvan aiempaa nopeammin.

Verkko on keskeinen äärioikeistolaisessa toiminnassa

Äärioikeistolaisten terrorismin torjunnan kohdehenkilöiden määrä Suomessa on kasvanut 2020-luvulla. Äärioikeistolaiset terroristit ovat kiinnostuneita ampuma-aseista ja räjähteistä, mutta myös yksinkertaisia tekovälineitä kuten teräaseita hyödynnetään. Todennäköisimpiä iskukohteita ovat etniset, uskonnolliset ja seksuaalivähemmistöt sekä ideologisiksi vastustajiksi katsotut tahot, kuten poliitikot tai viranomaiset.

Järjestäytynyt äärioikeistoliikehdintä ei muodosta suoraa terroristista uhkaa Suomessa, mutta se voi toimia alustana yksilöiden ja pienryhmien radikalisoitumiselle ja ideologialla perustellulle väkivaltaiselle toiminnalle. Suomen äärioikeiston keskuudessa on kiinnostusta ampuma-aseiden ja räjähteiden hankkimiseen ja näiden käyttöön liittyvään kouluttautumiseen. Kiinnostusta aseisiin selittää osittain aatemaailmasta kumpuava ajatus varautumisesta yhteiskunnan romahtamiseen.

Äärioikeistolaiset terrorismin torjunnan kohdehenkilöt ovat tyypillisesti väkivallasta kiinnostuneita nuoria miehiä, joista osalla on mielenterveyteen ja elämänhallintaan liittyviä ongelmia. Äärioikeistolaisessa retoriikassa korostuvat valkoisen väestönosan kokemat uhkat, varautuminen yhteiskunnallista epävakautta ja sodan kaltaista tilaa varten, suurta medianäkyvyyttä saaneista iskuista haettu inspiraatio sekä terrorismin ihannointi verkossa.

Verkko on keskeinen äärioikeistolaisessa toiminnassa. Suomalaisia osallistuu aktiivisesti väkivaltaa ihannoiviin keskusteluihin. Osallistujissa on myös alaikäisiä. Sekä Suomessa että kansainvälisesti useat iskuhankkeet ovat liittyneet verkkopainotteiseen Siege-kulttuuriin, jonka tukijat kannattavat nykyisen yhteiskuntajärjestelmän kaatamista poliittisen väkivallan keinoin.

Kansainväliset kehityskulut kohottavat radikaali-islamistisen terrorismin uhkaa Suomessa

Todennäköisin radikaali-islamistinen terrori-isku on yksinkertaisin tekovälinein julkisella paikalla tehty isku. Kansainvälinen radikaali-islamistinen propaganda kehottaa väkivaltaan etenkin islamille vihamieliseksi tulkittuja tahoja kohtaan. Iskukehotukset kohdistuvat kristinuskoa, Israelia ja juutalaisuutta edustaviin kohteisiin sekä seksuaalivähemmistöihin. Konfliktialueilla toimivat terroristijärjestöt pyrkivät edelleen toteuttamaan ja edistämään iskuja länsimaissa, mutta laajamittaisen iskun toteutus Suomessa on epätodennäköistä.

Radikaali-islamistinen toiminta keskittyy Suomessa edelleen pääosin kansainvälisen terrorismin tukitoimintaan, kuten propagandan levittämiseen

Miksi uhkatasoasteikko muuttui?

Suojelupoliisi seurasi vuosina 2017–2024 terrorismin uhkatasoa neliportaisella asteikolla. Vuonna 2025 otettiin käyttöön viisiportainen asteikko. Uhkatasoasteikolla arvioidaan ja viestitään Suomessa toteutettavan tai Suomen intresseihin ulkomailla kohdistuvan terrori-iskun uhkaa. Kansallinen terrorismin uhkataso määräytyy korkeimman uhkan mukaan.

Viisiportainen asteikko soveltuu neliportaista joustavammin uhkan arviointiin ja siitä viestimiseen.

”Viime vuosien aikana Suomen turvallisuusympäristössä on tapahtunut useita kehityskulkuja, jotka kohottavat terrorismin uhkaa. Tästä syystä uudella viisiportaisella asteikolla uhka yltää tasolle 3, *kohonnut*. Meille on tärkeää pystyä entistä tarkemmin kuvaamaan myös tällaista uhkan nousua”, kertoo Suojelupoliisin erikoistutkija **Anna Santaholma**.

Myös muut Pohjoismaat käyttävät terrorismin uhkatason arviointiin viisiportaista järjestelmää.

Suojelupoliisi tarkastelee uhkatasoa jatkuvasti ja julkaisee uhka-arvion vähintään kerran vuodessa.

ja tuottamiseen, terrorismin rahoittamiseen, sekä tukiverkostojen kasvattamiseen. Viimeisen kahden vuoden aikana on nähty kansainvälisiä kehityskulkuja, jotka ovat kohottaneet myös Suomeen ja Suomen intresseihin kohdistuvaa radikaali-islamistisen terrorismin uhkaa.

Koraanien häpäisy ja etenkin laajentuneet Lähi-idän konfliktit ovat toimineet radikalisoivina ja mobilisoivina tekijöinä Euroopan radikaali-islamistisessa toimintaympäristössä. Muutokset ovat näkyneet muun muassa terrori-iskujen sekä keskeytettyjen iskuhankkeiden määrän kasvuna.

Terroristijärjestö "Islamilaisen valtion" (Isil) ja sen Afganistanin provinssin (ISKP) verkostot Euroopassa ja sen lähialueilla ovat aktivoituneet. Ryhmän kansainvälisessä toiminnassa korostuvat etenkin keski-aasialais- ja kaukasialaistaustaiset radikaali-islamistit.

Keskusrikospoliisi (KRP) aloitti viime syksynä Isiliin liittyvän esitutkinnan terroristiryhmän toimintaan osallistumisesta. KRP pääsi epäiltyjen jäljille Suojelupoliisin tiedonhankinnan ansiosta ja Suojelupoliisi tukee myös tutkintaa omalla asiantuntemuksellaan.

Maailmanlaajuisesti merkittävimmän terrori-uhkan muodostavat edelleen Isil ja al-Qaida sekä niille uskollisuutta vannovat ryhmittymät. Ne ovat hyödyntäneet symbolisesti merkittäviä tapahtumia propagandassaan ja lisänneet länsimaihin kohdistuvia iskukehotuksia. Terroristijärjestöjen muodostama uhka keskittyy pääosin epävakaille alueille Afrikassa, Lähi-idässä ja Etelä-Aasiassa, jonne järjestöt pyrkivät myös houkuttelemaan vierastaistelijoita.

Irakin ja Syyrian konfliktialueella Isil on jatkanut terroristista toimintaansa ja pyrkinyt inspiroimaan, tukemaan ja toteuttamaan terrori-iskuja Euroopassa. Radikaali-islamistisen Hayat Tahrir al-Shamin (HTS) valtaannousu Syyriassa ja sen luoma epävakaus todennäköisesti laajentaa Isilin toimintavapautta alueella. Muutoksen laajemmat vaikutukset Syyriassa ja sen ulkopuolella näkyvät vasta pitemmän ajan kuluessa.

Vuonna 2024 Suomeen palasi yksi Suomesta Syyrian ja Irakin konfliktialueelle lähtenyt henkilö. Alueella on edelleen noin 50 Suomesta lähtenyttä henkilöä, joista suurin osa on todennäköisesti kuollut, mutta alueella vallitsevien olosuhteiden vuoksi kuolemia ei ole voitu vahvistaa.

Muun terrorismin uhka on matala

Muun terrorismin osalta Suomeen kohdistuva uhka on matala. Äärivasemmiston toiminta Suomessa on pääosin väkivallatonta ja keskittyy kurditoimijoiden tukemiseen sekä radikaaliin antifasismiin. Äärivasemmiston joukossa on kuitenkin yksittäisiä, väkivaltaiseen toimintaan valmiita henkilöitä. Väkivalta ilmenee erityisesti yhteenotoissa äärioikeistolaisten mielenosoittajien kanssa. Terroristi-järjestö Kurdistanin työväenpuolueen (PKK) toiminta Suomessa keskittyy pääasiassa tukitoimintaan.

Muissa Euroopan maissa tapahtuneissa äärivasemmistolaisissa iskuissa kohteina ovat olleet yritykset ja julkinen sektori. Äärivasemmiston terrori-iskujen tyypillinen toimintatapa on infrastruktuuriin kohdistettu sabotaasi. Mielenosoituksissa kuitenkin esiintyy väkivaltaa, joka kohdistuu ensisijaisesti vihollisiksi miellettyihin tahoihin, kuten poliittisiin vastustajiin ja viranomaisiin. ■

Alaikäisten radikalisoitumisesta on tullut vakiintunut ongelma Euroopassa

Lasten ja nuorten radikalisoituminen koskee sekä radikaali-islamistista että äärioikeistolaista terrorismia. Ilmiö on nähtävissä myös Suomessa.

Alaikäisten kiinnostus väkivaltaisia ääriliikkeitä kohtaan ja osallistuminen terroristiseen toimintaan on viime vuosina ollut kasvava trendi Euroopassa. Osallistuminen on kasvanut sekä radikaali-islamistista että äärioikeistolaista ideologiaa kannattavien nuorten keskuudessa.

Verkolla on keskeinen rooli alaikäisten radikalisoitumisessa ideologiasta riippumatta. Radikaalin materiaalin tuottaminen, kääntäminen ja jakaminen ovat tavanomaisia osallistumisen tapoja alaikäisille.

Myös väkivaltaiseen toimintaan osallistuminen on aiempaa yleisempää. Eurooppalaiset viranomaiset ovat viime vuosina keskeyttäneet useita epäiltyjä iskuhankkeita, joihin on osallistunut alaikäisiä. Euroopassa on viime vuonna tapahtunut myös yksi alaikäisen toteuttama radikaali-islamistinen terrori-isku.

Useat Euroopan maat ovat ilmaisseet huolensa lasten ja nuorten radikalisoitumisesta. Selvää on, että ilmiöstä on tullut pidempiaikainen kehityskulku, joka koskettaa myös Suomea. Suomessa nuoret aikuiset korostuvat tässä kontekstissa, mutta ääriaatteiden on havaittu vetoavan myös alaikäisiin. Ilmiöstä on tehty kasvavassa määrin havaintoja viime vuosien aikana.

Lasten ja nuorten radikalisoitumisen torjunnassa viranomaisten välinen yhteistyö on olennaista. Suojelupoliisi on järjestänyt aiheesta koulutusta esimerkiksi kunnissa kasvatuksen toimialalla työskenteleville.

Verkkoyhteisöjen merkitys on keskeinen

Sosiaalisen median alustat ovat tuoneet radikaalit ideologiat sekä niitä edustavat toimijat ja yhteisöt aiempaa helpommin ja riskittömämmin nuorten ulottuville. Virtuaaliset yhteisöt muodostavat ääri-ideologioita kannattaville tai niistä kiinnostuneille tärkeän vertaisryhmän, jonka osana omia näkemyksiä voi voimistaa ja saada niille hyväksyntää.

Toiminnassa hyödynnetään suljettuja viestisovelluksia ja keskustelualustoja, joilla voidaan levittää propagandaa, kehottaa iskuihin ja ohjata iskujen tekemiseen. Virtuaaliympäristön ulkopuoliseen toimintaan kehotetaan ja rohkaistaan etenkin jäsenmäärältään suurista yhteisöistä irtaantuneissa suljetuissa pienryhmissä.

Sekä radikaali-islamistiset että äärioikeistolaiset verkkoyhteisöt ovat luonteeltaan kansainvälisiä, mutta on olemassa myös paikallisempia tai tietyn kieliryhmän edustajia yhdistäviä yhteisöjä. Myös suomalaisia nuoria osallistuu näihin yhteisöihin.

Verkko ei yleensä ole ainoa syy radikalisoitumiselle, vaan taustalla on monia altistavia tekijöitä. Verkkoyhteisöjen ja -ryhmien tarjoama yhteisöllisyys voi kuitenkin olla merkittävässä osassa radikalisoitumisessa. Niistä saatetaan hakea sosiaalista hyväksyntää tai merkityksellisyyden tunnetta.

Verkkotoiminnan merkityksen kasvun on havaittu lyhentäneen yksilökohtaista radikalisoitumisprosessia. Huolestuttavimmissa tapauksissa valmius väkivaltaiseen toimintaan saavutetaan aikaisempaa nopeammin.

Oma lukunsa ovat lähipiirissään ääriajattelulle altistuneet lapset ja nuoret. He ovat keskimääräistä alttiimpia radikalisoitumiselle. Ylisukupolvista radikalisoitumista on myös Suomessa sekä äärioikeiston että radikaali-islamistisen toiminnan piirissä.

Propagandassa hyödynnetään populaarikulttuuria

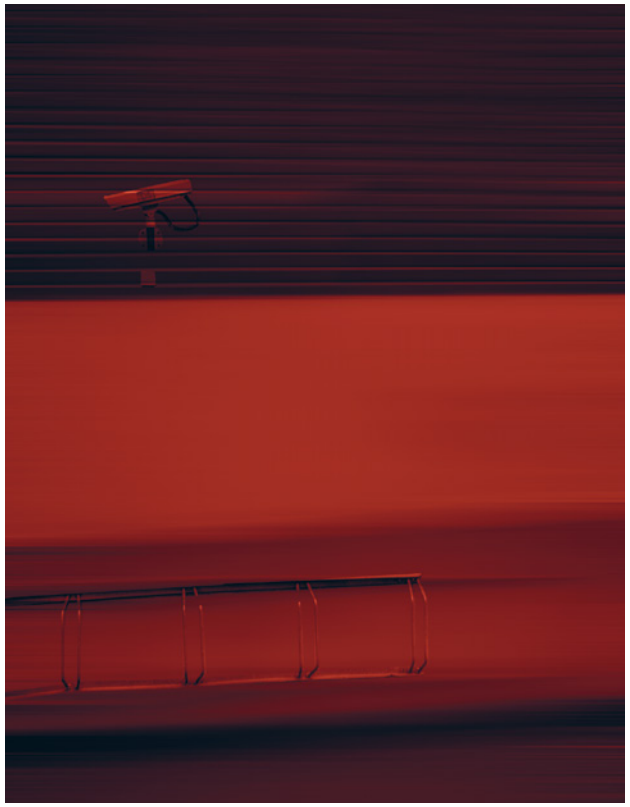
Radikaalit toimijat kohdistavat propagandaa lapsille ja nuorille, mutta alaikäiset voivat myös itse tuottaa aktiivisesti sisältöä toisilleen ja aikuisille. Radikaaleissa verkkoyhteisöissä lapset saattavat esiintyä itseään vanhempana ja omaksua samanlaisia rooleja kuin aikuiset.

Propagandan tuottajat ammentavat sisältöä nuorten keskuudessa suosituista peleistä ja populaarikulttuurista. Sekä radikaali-islamistisessa että äärioikeistolaisessa propagandassa hyödynnetään nykyään taitavasti lyhytvideoita, meemejä ja pelillistettyjä sisältöjä. Yksittäisten itsenäisten toimijoiden merkitys propagandantuotannossa on korostunut viime vuosina.

Maailmankuvaa rakennetaan usein yksilöllisesti, yhdistelemällä ajatuksia erilaisista ideologioista. ■

Radikaaliin äärioikeistoon liittyvät havainnot ovat kasvaneet turvallisuusselvityksissä

Havaintojen kasvun taustalla on monia syitä. Äärioikeistolaisten toimijoiden järjestelmällisestä hakeutumisesta tietyille aloille ei ole selkeitä viitteitä.



Suojelupoliisin tekemien turvallisuusselvitysten määrä on kasvanut merkittävästi. Vuonna 2019 turvallisuusselvityksiä tehtiin vajaat 70 000. Vuonna 2024 selvitysten määrä nousi ensimmäistä kertaa yli sadan tuhannen.

Järjestäytyneeseen tai terrorismiin kytkeytyvään äärioikeistoon, kuten oikeuden päätöksellä lakkautettuun Pohjoismaiseen Vastarintaliikkeeseen, liittyvien havaintojen määrä on noussut selvästi Suojelupoliisin tekemissä turvallisuusselvityksissä viime vuosina. Havaintojen määrä on kuusinkertaistunut sitten vuoden 2019. Havaintojen määrän kasvu ei kerro suoraan äärioikeiston aktiivisuuden kasvusta, vaikka se onkin yksi selittävistä tekijöistä. Taustalla vaikuttaa valvontaan suunnattujen resurssien kasvu.

Suojelupoliisin terrorismin torjunnan uhka-arviossa on todettu useamman vuoden ajan, että radikaali-islamismi ja äärioikeisto muodostavat merkittävimmän terrorismin uhkan Suomessa. Ääriliikehdintä pitää sisällään monenlaisia vakavuusasteita, joista terroristinen toiminta on vakavin ja harvinaisin muoto.

Todennäköisimmän terroristisen isku-uhkan muodostavat yksittäiset toimijat ja pienryhmät. Järjestäytynyt äärioikeisto voi toimia alustana yksittäisten henkilöiden ja pienryhmien radikalisoitumiselle ja kohottaa heidän väkivaltaisen toimintansa uhkaa.

Turvallisuusselvityksissä havaittujen äärioikeistoon liittyvien kytkösten voimakkuus vaihtelee. Joukossa on kasvavassa määrin ajallisesti tuoreita havaintoja. Valtaosa vakavista havainnoista liittyy järjestäytyneeseen äärioikeistoon tai äärioikeistolaiseen terrorismiin. Vakavimmillaan kyse on ollut siitä, että vahvoja yhteyksiä järjestäytyneeseen äärioikeistoon omaava henkilö on hakeutunut turvallisuuskriittiseen tehtävään tai organisaatioon.

Äärioikeisto ei ole pyrkinyt järjestelmällisesti tietyille aloille

Suojelupoliisi ei ole havainnut viitteitä siitä, että järjestäytyneeseen äärioikeistoon kytkeytyvät henkilöt olisivat pyrkineet laajamittaisemmin tietyille työnantajille tai tiettyihin tehtäviin. Havaintoja tehdään sitä enemmän, mitä suuremmasta organisaatiosta on kyse, sillä niille tehdään enemmän turvallisuusselvityksiä. Eniten havaintoja tehdään rakennus- ja it-alan turvallisuusselvityksissä.

Kaikista turvallisuusselvityksistä noin 2–4 prosentista löytyy työnantajalle ilmoitettavaa tietoa. Tällaisissa tapauksissa Supo antaa työnantajalle kirjallisen ilmoituksen.

Yleisimmin kirjalliset ilmoitukset liittyvät mainintoihin poliisin rekistereissä tai talousvaikeuksiin – nämä kattavat noin 90 prosenttia tapauksista. Äärioikeistoon liittyvien havaintojen osuus kaikesta työnantajille ilmoitettavasta tiedosta ei ole suuri, vaikka havaintojen määrä onkin noussut.

Suojelupoliisi käyttää aina tapauskohtaista harkintaa päättäessään, onko jokin asia olennaista ilmoittaa mahdolliselle työnantajalle. Kaikki tehdyt havainnot eivät siis päädy automaattisesti työnantajan tietoon. ■

Turvallisuusselvityksessä arvioidaan luotettavuutta

Turvallisuusselvityksillä on tärkeä rooli ennaltaehkäisevässä turvallisuustyössä. Selvitysten tarkoitus on ennalta estää Suomen turvallisuudelle tärkeiden tietojen päätyminen esimerkiksi vieraiden valtioiden tai ääriliikkeiden käsiin.

Turvallisuusselvityksessä tutkitaan sellaisia asioita, jotka voivat tehdä ihmisestä alttiin vaikuttamiselle tai painostukselle tai jotka voisivat vaikuttaa henkilön luotettavuuteen tietyssä tehtävässä.

Supo harkitsee aina tapauskohtaisesti ja suhteessa työtehtäviin, ovatko selvityksen yhteydessä esiin tulleet tiedot sellaisia, että ne on välttämätöntä ilmoittaa työnantajalle. Esimerkiksi vakavat talousvaikeudet voivat altistaa henkilön vaikuttamisyrityksille.

Turvallisuusselvitys ei sido työnantajaa. Työnantaja päättää aina itse, vaikuttaako Supon ilmoittama tieto esimerkiksi rekrytointiin.

Supon vuosi

Suojelupoliisi on turvallisuus- ja tiedustelupalvelu, joka hankkii, analysoi ja raportoi valtiojohdolle ennakoivaa ja ainutlaatuista tiedustelutietoa kansallisen turvallisuuden uhkista. Supo myös torjuu terrorismia, estää vakoilua ja tekee turvallisuusselvityksiä.

Kansallista turvallisuutta on suojattava vuoden jokaisena päivänä, kellon ympäri. Tätä työtä tehdään yli 580 supolaisen voimin toimistoilla, kentällä ja verkossa – kaikkialla Suomessa ja myös ulkomailla. Vuosikoosteessa kuusi Supon työntekijää kokoaa ajatuksiaan kiireisestä työvuodestaan.

Turvallisuusselvitysosaston päällikkö Ilkka Hanski: "Selvitysten laatua on pyritty kehittämään"

Tämäkin vuosi on ollut kiireinen turvallisuusselvitysosastolla, sillä selvitysten määrä on noussut merkittävästi. Kasvua on tapahtunut pidemmällä aikavälillä, mutta tänä vuonna selvitysten määrä nousi ensimmäistä kertaa yli sadan tuhannen. Selvityksiä tehtiin kaikkiaan noin 115 000.

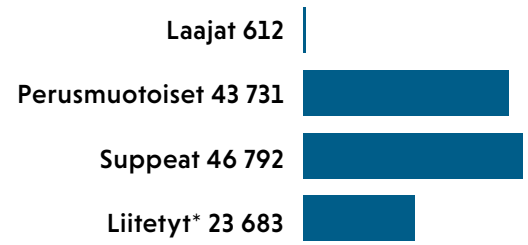
Selvitysten määrän kasvuun ovat vaikuttaneet viime vuosina tehdyt lakimuutokset, mutta olemme myös Suojelupoliisissa tehneet johdonmukaista työtä, jotta kaikki keskeiset toimijat olisivat turvallisuusselvitysten piirissä. Menettelyssä jo mukana olevien organisaatioiden kanssa on käyty keskustelua, jotta myös kaikki oikeat tehtävät olisivat turvallisuusselvitettyjä.

Myös selvitysten laatua on pyritty kehittämään. Perusmuotoisten turvallissuuselvitysten yhteydessä selvitetään yhä useammin nykyään ulkomaansidonnaisuudet. Turvallisuusselvitysten yhteydessä tehdään myös enemmän haastatteluja.

Turvallisuusselvitysten kesto on lyhentynyt keskimäärin, sillä olemme kehittäneet omia prosessejamme. Nopeus vaikuttaa siihen, miten matala kynnys organisaatioilla on hyödyntää turvallisuusselvityksiä. Työ näkyy, sillä viime vuonna toteuttamassamme asiakaskyselyssä 95 prosenttia vastanneista oli tyytyväisiä palveluihimme. Asiakkaista 97 prosenttia piti turvallisuusselvityksiä tärkeinä organisaatiolleen.

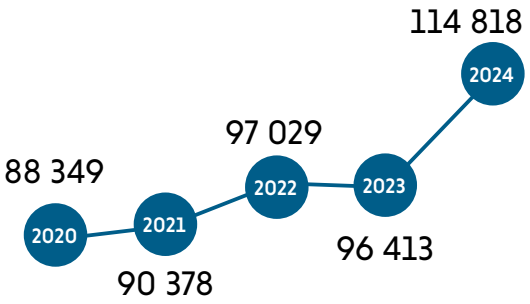
Supon turvallisuusselvitysosasto antaa lausuntoja myös oleskelulupiin, kansalaisuus- ja viisumihakemuksiin. Myös näiden lausuntojen määrä on noussut. Lausunnoilla voimme vaikuttaa siihen, ettei Suomeen päätyisi ihmisiä, jotka ovat vaaraksi kansalliselle turvallisuudelle.

Turvallisuusselvitykset 2024



*Henkilöstä ei tarvitse aina tehdä uutta selvitystä hänen työtehtäviensä vaihtuessa.

Turvallisuusselvitykset yhteensä



Tarkkailutehtävissä työskentelevä supolainen: "Olemme paljon ulkona läsnä siellä, missä ihmisetkin ovat"

Olen työskennellyt vuosia Suojelupoliisin tarkkailutehtävissä eli Supon oman tiedonhankinnan ytimessä. Tiedustelumenetelmänä tarkkailulla tarkoitetaan havaintojen tekemistä henkilöstä tai henkilöryhmästä salassa, kun se on tarpeen tärkeiden tietojen saamiseksi ja kansallisen turvallisuuden suojaamiseksi.

Supon tehtävä on hankkia kansallista turvallisuutta koskevaa ainutlaatuista tietoa, jota ei muualta saa. Supon oma ja itsenäisesti suorittama tiedonhankinta on siinä olennaista.

Olemme paljon ulkona läsnä siellä, missä ihmisetkin ovat. Meidän tiedonhankinnan kohteemme pyrkivät toimimaan ammattimaisesti salassa, joten myös meidän on toimittava samoin, mutta paremmin. Vaikka verkossa tapahtuva tiedonhankinta on kasvattanut merkitystään, on paljon tietoa, joka pitää edelleen hankkia reaalimaailmassa.

Työmme on haastavaa ja vaatii pitkäjänteisyyttä. Operaatioissa saatetaan kerätä tietoa hyvin pitkään, mutta varsinaiset tulokset näkyvät vasta vuosien päästä. Tiedostamme myös, että työpanoksemme tuottaa vain yhden palan siviilitiedustelun suureen palapeliin, jossa pelaajia on useita.

Kulunut vuosi on ollut myös meille poikkeuksellisen kiireinen. Olemme käyttäneet tiedustelumenetelmiä monipuolisesti ja saaneet hankittua merkittävää tietoa kansallisen turvallisuuden kannalta.

Vuosi on ollut myös kuormittava henkilöstölle, kun ison työmäärän yhdistää epävarmaan taloustilanteeseen. Henkilöstön keskuudessa on ollut huolta siitä, voimmeko ohenevilla resursseilla jatkaa työtämme tässä muodossa. Supon läsnäolo turvaamassa yhteiskuntaa vaatii ihmisiä.

Vastatiedustelun päällikkö Teemu Liikkanen: "Meidän pitää etsiä uusia keinoja torjua vakoilua"

Aloitin vastatiedustelun päällikkönä syyskuun 2024 alussa. Oletin etukäteen tehtävän olevan haastava, mutta silti kiire, asioiden ja tiedon määrä ovat yllättäneet.

Tässä tehtävässä on todella isojen asioiden ja vastuun äärellä koko ajan. Kun puhutaan Suomeen kohdistuvasta vakoilusta ja vaikuttamisesta, ei puhuta vain Supoa vaan koko Suomea koskevista asioista. Se tekee työstä myös mielenkiintoista ja palkitsevaa erityisesti silloin, kun tulee onnistumisia.

Työn merkityksellisyyttä ei tarvitse tässä tehtävässä miettiä, vaikkei tämä työ pelkkää glamouria ole. Kuten muuhunkin asiantuntijatyöhön tähänkin kuuluu paljon palavereissa istumista, lukemista, perehtymistä ja kirjoittamista.

Vastatiedustelun päällikkönä pyrin kehittämään työtämme entistä enemmän ennakoivaan suuntaan. Venäjä on perinteisesti hyödyntänyt henkilötiedustelussaan diplomaattipeitettä, mutta nyt se on vaikeutunut merkittävästi. Koska vastapuoli on pakotettu etsimään uusia keinoja hankkia tietoa, myös meidän pitää etsiä uusia keinoja torjua vakoilua. Parhaassa tapauksessa pääsemme kiinni vastapuolen suunnitelmiin jo ennen kuin niitä ehditään toteuttaa.

Koska toimintaympäristö muuttuu ja uhkat ovat monisäikeisiä, pitää meidän kehittää toimintaamme. Haluan olla osaltani helpottamassa esimerkiksi osastojen välistä yhteistyötä eli rikkoa raja-aitoja.

Vastatiedustelu kuuluu Supon perinteikkäisiin ydintehtäviin. Uudistamista onkin tehtävä historiaa kunnioittaen – hyvät asiat on syytäkin säilyttää.

Tietoverkkotiedustelija: "Hullulta kuulostava ratkaisuehdotus saattaa johtaa oikeille jäljille"

Työnkuvani on kerätä tietoa erilaisista tietoverkoista. Tiimimme toimii eräänlaisena konsernipalveluna, joka on erikoistunut käyttämään erilaisia tiedonhankinta- ja tiedustelumenetelmiä internetissä.

Päivämme vaihtelevat paljon tiedonhankinnan tarpeiden mukaan. Saatamme tehdä yhtenä päivänä Venäjään liittyvää tiedonhankintaa, seuraavana terrorismintorjuntaan. Koska tiimimme toimii Suojelupoliisin koko toimialan laajuudella, en voi sanoa minkään yhden teeman hallinneen viime vuotta. Toki kaikki kaiut idästä työllistävät. Työtä tehdään aina kun tarvitsee – internet ei nuku!

Avoimet lähteet ovat tärkeä lähtöpiste lähes kaikkiin työtehtäviini. Avoimista lähteistä löytyvää tietoa voidaan verrata muilla menetelmillä kerättyyn tiedustelutietoon tai vaikkapa muihin viranomaisrekistereihin. Avointen lähteiden tiedustelu on erinomainen väline suuntaamaan varsinaisten tiedustelumenetelmien käyttöä. Tiettyjä tiedustelumenetelmiä käytämme itse, toisissa tuemme muita yksiköitä heidän osaamisalueillaan.

Tiimimme muodostuu karkeasti kuvattuna kolmenlaisesta osaamisesta. Mukana on poliisitaustaisia dekkariaivoja, jotka ovat niin sanotusti hyviä palapelin kokoajia. Toisaalta tarvitsemme erilaisten kielten osaajia (mainittakoon erikseen vaikkapa kiina, venäjä ja arabia), minkä lisäksi tietysti it-osaajat ovat tärkeitä. Harvoin on yhtä ihmistä, joka olisi kaikkea tätä yhtä aikaa.

Teemme tiivistä yhteistyötä substanssiasiantuntijoiden kanssa ja koulutamme myös heitä avointen lähteiden käytössä. Esimerkiksi Kiinaan erikoistunut tutkija saattaa katsella kerättyä tietoa hyvin eri silmin kuin me.

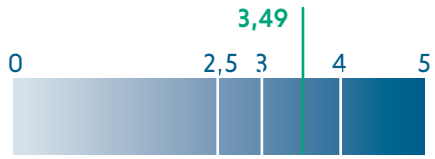
Työni on luonteeltaan varsin itsenäistä. Kukaan ei tule neuvomaan, miten keikka pitäisi hoitaa, sillä hyvään tulokseen voi päästä niin monia eri reittejä pitkin. Toisaalta tiimin tuoma tuki on tärkeä voimavara, jos esimerkiksi takoo pitkään päätään seinään jonkun ongelman kanssa. Työkaveri saattaa tuoreemmilla silmillä nähdä jotain, mitä ei itse huomaa. On yllättävää, kuinka usein työkaverin mielikuvituksen ja huumorintajun värittämä, hullulta kuulostava ratkaisuehdotus omaan ongelmaan saattaa lopulta auttaa oikeille jäljille.

Tiedustelutyöhön liittyy aina erilaisia ajattelun vinoumia, jotka tiedustelutyön ammattilaisen on hyvä tiedostaa. Perinteinen internet-tiedustelijan ajattelun vinouma on ajatus siitä, että kyllähän tämän asian joku jo varmasti tietää, joten siitä ei kannata raportoida. Arki on kuitenkin opettanut, että aina kannattaa avata suunsa, kun epäilee löytäneensä jotain Suojelupoliisin toimialaan kuuluvaa. Parasta työssäni onkin, että meidän tiimin hankkima pienikin tiedon murunen voi toimia herätteenä muulle tiedonhankinnalle.

Joskus internet-tiedonhankinta tuntuu siltä, kuin etsisi neulaa heinäsuovasta. Tai kuten meillä sanotaan: Kuin yrittäisi löytää tuntematonta järvenrantamökkiä maailman kartalta. Lähes aina löytyy!

Luottamus ja maine

Supon luottamusta ja mainetta kansalaisten keskuudessa selvitettiin vuonna 2024 T-Median tutkimuksella. Mainetta kuvaava luku kokoaa yhteen kansalaisten arvion Supon työstä, hallinnosta, taloudesta, johdosta, vastuullisuudesta, työantajakuvasta, vuorovaikutuksesta ja uudistumiskyvystä.



0–2,5 Erittäin heikko
2,5–3 Heikko
3–3,5 Kohtalainen
3,5–4 Hyvä
4–5 Erinomainen

Kansainvälisten asioiden päällikkö: "Kansainvälinen yhteistyö on yksi Suojelupoliisin keskeisimmistä kyvykkyyksistä"

Suomeen vaikuttavat uhkat ovat monimutkaistuneet viime vuosina ja kaukaisemmillakin kriiseillä voi olla heijastevaikutuksia. Kansainvälinen tiedonvaihto ja vertailu auttavat analysoimaan uhkatekijöiden toimintamalleja, keskinäisriippuvuuksia ja kehityskulkuja. Siksi tiedustelun näkökulmasta kansainväliset verkostot ja yhteistyö kasvattavat merkitystään työssämme entisestään.

Kansainvälinen yhteistyö on yksi Suojelupoliisin keskeisimmistä kyvykkyyksistä. Se on keino vaihtaa ainutlaatuista tietoa puolin ja toisin. Kansainvälisen yhteistyön kautta hankittu tieto on olennainen osa esimerkiksi laadukasta raportointia valtiojohdollemme.

Suojelupoliisin kansainvälinen yhteistyö onkin vilkastunut, mikä näkyy myös alati kasvavana kirjeenvaihdon määränä. Kansainvälinen yhteistyö on supolaisille päivittäistä, ja sitä tehdään laajasti eri osastoilla.

Kahdenvälisen tiedonvaihdon rinnalla yhteistyötä tehdään osana monenkeskisiä foorumeja, joista esimerkiksi Nato on tuonut kansainväliseen yhteistyöhömme vaikuttavan lisän. Suojelupoliisin osalta Nato-yhteistyö onkin entisestään vakiintunut ja vahvistunut kuluvan vuoden aikana. Liittokunnassa yhteistyö ei ole ainoastaan mahdollisuus vaan myös velvollisuus ja Suojelupoliisi vastaa liittokunnassa toimialansa mukaisesti Suomen osalta siviilitiedusteluun liittyviin kysymyksiin.

Ei-sotilaallinen vaikuttaminen ja uhkat ovat moninaistuneet viime vuosina, mikä näkyy myös Nato-yhteistyössä.

Suojelupoliisin kansainvälisen yhteistyön arki on hektistä ja päivittäin muuttuvaa, sillä turvallisuusympäristön ja ulko- ja turvallisuuspolitiikan muuttujat eivät yleensä noudata tarkkoja maantieteellisiä tai aikavyöhykkeiden rajoja.

Kansainvälinen kirjeenvaihto

21 000

kansainvälistä viestiä
(lähetettyä ja vastaanotettua)

Henkilöstö

Keski-ikä **42,9**

Henkilöstöä yhteensä **584**

Korkeakoulututkinnon suorittaneet **72,6 %**

Järjestelmäpäällikkö Susanna Kallonen: "ICT-väkemme ei pääse helpolla"

ICT-alalla työskentely on tyypillisesti luonteeltaan vaikeiden ja monimutkaisten teknisten sekä prosesseihin liittyvien ongelmien ratkomista yhteistyössä eri sidosryhmien kanssa. Sitä se on myös meillä Supossa vuonna 2025.

Lisämausteensa tekemiseen juuri viime aikoina on tuonut haastava taloustilanteemme. Tästä huolimatta olemme pystyneet viemään eteenpäin merkittäviä järjestelmäkehityskokonaisuuksia muun muassa EU-rahoituksen turvin käynnistetyssä Inter-hankkeessa, jossa tuotamme tiedon analysointia tukevia moderneja työkaluja ja tekoälyominaisuuksia Supon keskeisiin tietojärjestelmiin.

Hankkeessa tavoitellaan työn tehostamista ja työprosessien laadun parantamista. Tämän tyyppisten kehittämiskokonaisuuksien avulla Supo haluaa entisestään parantaa analyysikyvykkyyksiään. Työ tukee Suojelupoliisin muuntumista tiedustelupalveluksi ja auttaa varautumaan käsiteltävän tiedon määrän kasvuun.

Hanke on suunnilleen puolivälissä. Tähän mennessä hankkeessa mitattavat välitavoitteet on suurimmaksi osaksi saavutettu ja hanke etenee aikataulussa. Hankkeessa on jo toteutettu muun muassa tutkijoiden yhteistyötä tehostava työalusta. Seuraavaksi siirrytään tekoälyä hyödyntävien työkalujen toteutukseen.

Myös Suojelupoliisin uuden toimitalon edellyttämät laajamittaiset it-infrastruktuurityöt ovat edellyttäneet merkittävää ponnistusta ICT-väeltämme, kun vuonna 2025 siintää muutto uuteen osoitteeseen. Kaiken pitää olla kohdillaan muuttoa varten, jotta järjestelmät toimivat ja arki voi jatkua sujuvasti muuton jälkeen. Tässäkin valtavassa projektissa väkemme on osoittanut erinomaisen ammattitaitonsa.

Toimialamme erityispiirteiden vuoksi myös tietojärjestelmäkehittämiseemme liittyy erityisiä vaatimuksia, jotka tuovat tekemiseen omat mutkansa. ICT-väkemme ei pääse helpolla kehittäessään ja ylläpitäessään lukuisia järjestelmiä ja taustalla olevaa infrastruktuuria sekä laitteistoja. Työtä tehdään kovalla tarmolla tavoitteena pysyä yleisen ICT-kehityksen vauhdikkaassa kelkassa mukana.

Kaikista näistä onnistumisista kiitos kuuluu huippuosaavalle ja sinnikkäälle ICT-henkilöstöllemme, jotka päivästä toiseen ratkovat niitä aiemmin mainittuja monimutkaisia ongelmia ja mahdollistavat omalta osaltaan organisaatiomme ydintoiminnan jatkuvuuden. ■

Käytetty rahoitus tilivuosittain

(miljoonaa euroa)