SUPO

Kansallisen turvallisuuden katsaus 2023

Suomeen kohdistuu tiedustelua ja vaikuttamista

Suomeen ja suomalaisiin kohdistuvaa tiedustelua tekevät erityisesti Venäjä ja Kiina. Venäjän tiedustelua kiinnostavat ensisijaisesti länsimaiden turvallisuuspolitiikkaan, erityisesti Ukrainan tilanteeseen ja tukemiseen liittyvät kysymykset ja keinot pakotteiden kiertämiseen. Kiinan tiedustelu kohdistuu muun muassa ulko- ja turvallisuuspoliittiseen päätöksentekoon ja huipputeknologiaan.

Venäjä siirtää tiedonhankintansa painopistettä kyberympäristöön

Venäjän hyökkäyssodan aiheuttama jännitteinen turvallisuustilanne Euroopassa vaikuttaa Venäjän tiedustelun suuntaamiseen. Ajankohtaisina mielenkiinnon kohteina korostuvat Suomen Nato-jäsenyyden konkreettiset seuraukset, Ukrainalle osoitettava materiaalituki sekä keinot pakotteiden kiertämiseen Suomen kautta.

Venäjän henkilötiedustelun toimintaedellytykset Suomessa ovat heikentyneet Venäjän hyökättyä Ukrainaan sekä diplomaattien karkotusten vuoksi. Venäjä joutuu erittäin todennäköisesti siirtämään tiedonhankintansa painopistettä kyberympäristöön.

Venäjän vaikuttamisen keskeisenä tavoitteena on heikentää Naton ja EU:n yhtenäisyyttä sekä vähentää länsimaiden tukea Ukrainalle. Suomen liittyminen Natoon, sodan jatkuminen Ukrainassa, syvenevä vastakkainasettelu länsimaiden ja Venäjän välillä sekä lisääntyvät pakotteet todennäköisesti voimistavat Venäjän vastatoimia Suomea kohtaan. Kuitenkin juuri Nato-jäsenyys antaa suojaa vaikuttamisen väkivaltaisimpia muotoja vastaan.

VENÄJÄ MUUNTELEE TODELLISIA TIETOJA INFORMAATIO-VAIKUTTAMISESSAAN

Venäjä käyttää verkkoalustoja tavoitteellisesti länsimaihin suunnattuun informaatiovaikuttamiseen. Se hyödyntää todellisia uutisia ja tietoja, mutta muuttaa niiden sävyä, yksityiskohtia tai kehystä siten, että uutinen näyttää tukevan Venäjää. Viestit on kirjoitettu kunkin median viestintäkulttuurin mukaisesti, eikä niitä ole aina helppoa tunnistaa propagandaksi. Venäjä käyttää myös palvelunestohyökkäyksiä informaatiovaikuttamisen välineenä.

Kiinalle asetetut vientirajoitteet ja maan sisäinen tilanne kasvattavat tiedustelun tarvetta

Kiina kohdistaa Suomeen henkilötiedustelua ja kybervakoilua. Kiinan kybervakoilun tavoitteena on hankkia tietoa muiden valtioiden ulkopoliittisista näkemyksistä sekä teknologista tuotekehitystietoa. Esimerkiksi Yhdysvaltojen Kiinalle asettamat puolijohteiden ja niiden valmistusteknologian vientirajoitteet kasvattavat Kiinan tarvetta hankkia tietoa kybervakoilulla.

Kiina korostaa kansallisen turvallisuuden varmistamisen olevan kaikkien kiinalaisten velvollisuus. Tämä yhdessä Kiinan lainsäädäntömuutosten kanssa todennäköisesti vaikeuttaa monien Kiinassa oleskelevien ulkomaalaisten, kuten diplomaattien, toimittajien ja tutkijoiden toimintaa entisestään sekä todennäköisesti kasvattaa Suomessa asuviin kiinalaistaustaisiin henkilöihin kohdistettua valvontaa.

Kansallisen turvallisuuden uhkat ovat jatkuvassa muutoksessa

Yhteiskunnan digitalisaation ja teknologisen kehityksen myötä myös kansallisen turvallisuuden uhat muuttuvat. Yhteiskunnan kriittiset palvelut ovat yhä enemmän riippuvaisia avaruuteen sijoitetusta infrastruktuurista. Kehittyvien teknologioiden kaksikäyttöisyys, vientivalvontakysymykset sekä kotimaisen tutkimuksen ja kehityksen suojaaminen ovat nousevia teemoja.

Kybervakoilu hyödyntää suojaamattomia kuluttajalaitteita

Suurin osa suomalaisista ei ole Venäjän tai Kiinan kybervakoilun kohteena, mutta kuka tahansa verkkoon kiinteästi kytketyn suojaamattoman laitteen, kuten kotireitittimen, haltija voi olla sen mahdollistaja. Yhä useammassa kuluttajalaitteessa on internetyhteys, joka sallii laitteen etäohjauksen. Samalla se tarjoaa mahdollisuuden oikeudettomalle etäkäytölle valtiollisille toimijoille, jotka pyrkivät tunkeutumaan Suomen tai kumppanimaidemme tietojärjestelmiin. Euroopan unionin uusien kuluttajalaitteiden tietoturvavaatimuksia koskeva kyberkestävyyssäädös (Cyber Resilience Act) parantaa tilannetta, mutta sen vaikutus näkyy vasta viiveellä.

Erityisesti suojaamattomat ja päivittämättömät kotireitittimet muodostavat tällä hetkellä merkittävän riskin kansalliselle turvallisuudelle. Tietomurto kotireitittimeen aiheuttaa riskin myös laitteen haltijalle, sillä tunkeutuja voi esiintyä laitteen kautta liittymän haltijan identiteetillä. Teleyritykset huolehtivat tarjoamiensa laitteiden turvallisista asetuksista ja ylläpidosta, mutta kuluttajien kaupasta hankkimissa laitteissa vastuu turvallisista asetuksista ja ylläpidosta on kuluttajalla itsellään.

Kriittisen infrastruktuurin riippuvuus avaruudesta kasvaa

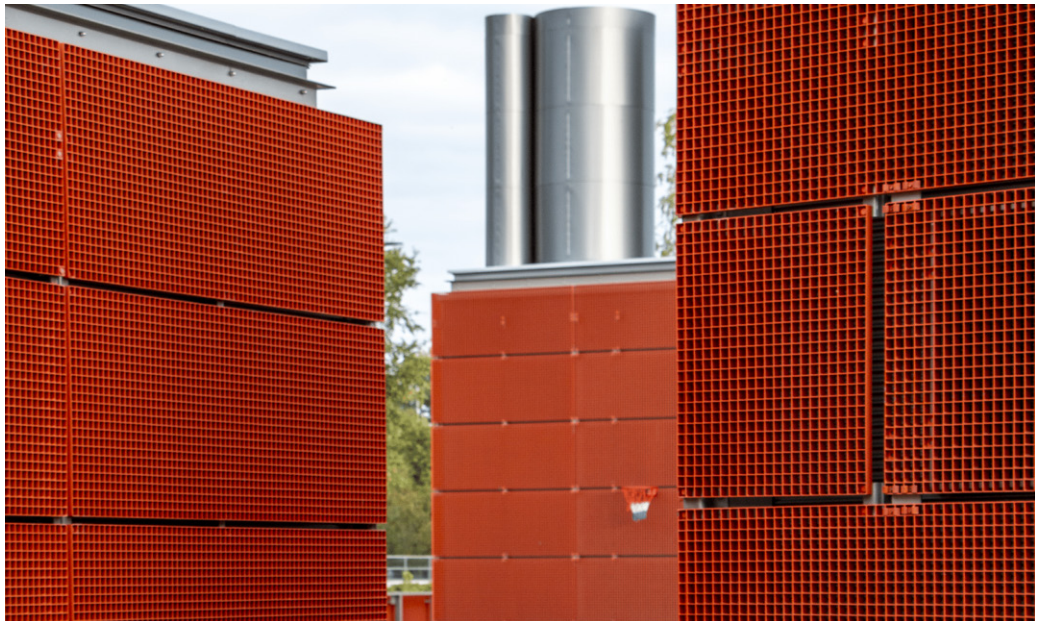
Yhteiskunnan kriittiset palvelut sekä tietyt viranomaispalvelut tarvitsevat toimiakseen satelliittien kautta välitettävää aika- ja paikkatietoa. Esimerkiksi logistiikkasektorin toiminta hidastuu ilman satelliittipaikkatietoa, ja viikkoja kestävät satelliittiaikatiedon häiriöt voivat vaikuttaa tietoliikenneinfrastruktuurin toimintaan sekä esimerkiksi finanssialaan. Pitkällä aikavälillä yhteiskunnan riippuvuus satelliittipalveluista lisääntyy. Yksityisen sektorin kasvava osuus palveluiden tuottajana lisää niiden saatavuuteen liittyviä riskejä, kun palveluntuotantoon eivät aina vaikuta yksinomaan kaupalliset tekijät, vaan mahdollisissa poikkeustilanteissa yrityksen oma tai jonkin valtion etu.

Kriittisen infrastruktuurin ohjausjärjestelmät ovat verkossa. Ne ovat yleensä huolellisesti suojattuja, ja Suomen Nato-jäsenyys on kasvattanut kynnystä Suomeen kohdistuvaan vihamieliseen vaikuttamiseen. Kyberhyökkäyksinä uutisoidut tapahtumat ovat useimmiten hajautettuja palvelunestohyökkäyksiä, jotka ruuhkauttavat hetkellisesti yksittäisen julkisen verkkosivuston, mutta eivät yleensä vaaranna kansallista turvallisuutta.

Venäjä kiertää vientirajoituksia kolmansien maiden kautta

Länsimaiden asettamat vientirajoitukset vaikeuttavat Venäjän teknologiasektorin ja teollisuuden toimintaa merkittävästi. Tämän vuoksi Venäjä pyrkii kiertämään rajoituksia esimerkiksi häivyttämällä hankintaketjuista tiedon todellisesta ostajasta sekä hankkimalla tuotteita kolmansien maiden kautta. Kaikkea tarvittavaa teknologiatuontia se ei pysty kuitenkaan kattavasti korvaamaan.

Nousevien teknologioiden kaksikäyttösovellutusten ja vientivalvonnan aukkojen hyödyntäminen tulevat todennäköisesti lisääntymään. Esimerkiksi kvanttiteknologia ei ole yleisesti vientivalvonnan piirissä, vaikka sillä on kaksikäyttömahdollisuuksia ja jotkut laitteet tai niiden komponentit ovat vientivalvottuja.



Terrorismin uhka on tasolla kohonnut

Terrorismin uhka on edelleen neliportaisen asteikon tasolla kaksi eli kohonnut. Terrorismin torjunnan kohdehenkilöitä on Suomessa noin 350. Todennäköisimmän isku-uhkan aiheuttavat äärioikeistolaista tai radikaali-islamistista ideologiaa kannattavat yksittäiset henkilöt tai pienryhmät. Suurin osa terrorismiin kytkeytyvästä toiminnasta Suomessa on tukitoimia, kuten varainkeruuta ja ideologian levittämistä verkossa.

4. Erittäin korkea

3. Korkea

2. Kohonnut

1. Matala

Väkivallan uhkaa aiheuttaa äärioikeistolainen terrorismi

Äärioikeistolaisen terrorismin kannattajat ovat saaneet vaikutteita esimerkiksi yhteiskuntajärjestyksen väkivaltaiseen romahduttamiseen tähtäävästä Siege-kulttuurista. He näkevät aseelliset iskut keskeisenä keinona yhteiskunnan romahduttamisen kiihdyttämisessä. He kuuluvat verkkoyhteisöihin, joissa ihannoidaan äärioikeistolaisia joukkoampujia, kannustetaan iskujen toteuttamiseen ja jaetaan materiaalia iskujen suunnitteluun.

Rahoitus on keskeinen radikaali-islamistisen terrorismin tukimuoto Suomessa

Terrorismin rahoituksesta on kyse silloin, kun hankittua tai kerättyä rahaa välitetään henkilöille, jotka kytkeytyvät terroristiseen toimintaan. Rahoitus on keskeinen radikaali-islamistisen terrorismin tukimuoto Suomessa. Varoja voidaan hankkia esimerkiksi lahjoituksina. Omaisuusrikoksilla, laittomalla kaupalla ja suojelurahojen keräämisellä hankittuja varoja pyritään usein pesemään laillista liiketoimintaa hyödyntämällä: varat siirretään virallisesti rekisteröidyn yrityksen tilille jollakin liiketoiminnalta näyttävällä syyllä ja edelleen yrityksen tililtä maahan, jossa on joko löyhempi pankkivalvontajärjestelmä tai suoraa terroristista toimintaa.

Digitaalisen rahansiirron käyttö ja virtuaalivaluuttojen yleistyminen ovat vaikuttaneet epävirallisen pankki- ja rahansiirtopalvelusektorin vahvistumiseen. Terroristisen toiminnan rahoitus on kansainvälinen ja talousalueiden rajat ylittävä ilmiö. Terroristiset toimijat voivat kerätä yksittäisessä maassa merkittäviäkin määriä rahoitusta ilman, että kyseisen maan terrorismiuhka kohoaa.

Terrorismin rahoituksessa hyödynnetään myös kolmatta sektoria. Rahaa voidaan lähettää esimerkiksi nimellisesti voittoa tavoittelemattoman säätiön kautta suoraan terroristiselle toimijalle. Varoja voidaan siirtää myös ulkomailla olevalle ihmiselle, joka välittää ne terroristiselle toimijalle suoraan, liiketoiminnan kautta tai kolmannen sektorin välityksellä.

Moniviranomaisyhteistyö on keskeisessä asemassa terrorismirahoituksen jäljittämisessä. Suojelupoliisi tekee asiassa yhteistyötä niin kansainvälisesti kuin kotimaassa, muun muassa Keskusrikospoliisin ja Tullin kanssa.

SUPO

TODENNÄKÖISYYTTÄ KUVAAVAT TERMIT

Erittäin epätodennäköinen	5 %
Epätodennäköinen	20 %
Todennäköinen	75 %
Erittäin todennäköinen	90 %

RAPORTISSA KÄYTETYT AIKAMÄÄREITÄ KUVAAVAT TERMIT

Lähitulevaisuudessa	0–6 kk
Lyhyt aikaväli	6 kk–2 v
Keskipitkä aikaväli	2–5 v
Pitkä aikaväli	yli 5 v