Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Valtioneuvoston selonteko tiedustelulainsäädännöstä (VNS 11/2021 vp)
Lausunto : Euroopan hybridiuhkien torjunnan osaamiskeskus

Valtioneuvoston selonteossa tiedustelulainsäädännöstä (VNS 11/2021 vp) arvioidaan tiedustelutoiminnan luonnetta muuttuneessa toimintaympäristössä ja Suomen tiedustelulainsäädännön toimivuutta ja kehittämistarpeita tästä näkökulmasta.

Selonteossa todetaan, että ”Suomen turvallisuusympäristö on tiedustelulainsäädännön hyväksymisen jälkeen ollut jatkuvassa muutoksessa. Muutokset muodostavat yhteiskunnalle, sen toiminnoille ja jäsenille uusia uhkia ja uhkien yhdistelmiä.” Nämä muutokset ja niiden sisältämät monihäiriötilanteiden mahdollisuudet sekä monimuotoiset ja -ulotteiset hybridiuhat puoltavat lainsäädännön perusteellista arviointia.

Selonteon mukaan Suomeen kohdistetaan hybridivaikuttamista, jota ”voidaan toteuttaa poliittisilla, taloudellisilla sekä sotilaallisilla sektoreilla, jolloin käytetään muun muassa infrastruktuuriin, informaatioon ja kyberturvallisuuteen kohdistuvia toimenpiteitä.” Tämänkaltainen vaikuttaminen alleviivaa tarvetta käsitellä tiedustelun kokonaisuutta aiempaa laajemmasta näkökulmasta. Pelkän siviili-sotilas-jakolinjan sijasta uhkia tulee lähestyä kokonaisvaltaisesta näkökulmasta, jolla on seurauksensa sekä tiedon hankintaa että sen jakoa koskeville periaatteille.

Tiedustelutiedon oikea-aikainen tavoitettavuus tulisi varmistaa kaikille kansallisen turvallisuuden suojaamiseen osallistuville toimijoille. Näitä toimijoita ovat yhä useammin perinteisen kovan turvallisuuden toimijoiden ohella myös muut hallinnonalat, kuten liikenne- ja viestintäministeriön hallinnonala ja valtiovarainministeriön hallinnonala. Tiedonjaon kannalta keskeisiä toimijoita tulisikin tarkastella aiempaa laajemmin, huomioiden tiedon salassapitoon liittyvät vaatimukset.

Samalla myös tiedonhankintaa tulisi ajatella aiempaa laajemmasta näkökulmasta. Esimerkiksi taloudellisia indikaattoreita tai kybertoimintaympäristöön liittyviä riskejä tulisi tarkastella aiempaa kokonaisvaltaisemmin turvallisuuspolitiikan näkökulmasta ja tarvittaessa kehittää näitä koskevia tiedonhankintamekanismeja.

Kansallinen turvallisuus ja puolustus kuuluvat Euroopan unionissa jäsenvaltion vastuulle. Sekä EU-lainsäädännölle että muulla EU:ssa toteutettavalla yhteistyölle on kuitenkin kauaskantoisia ja merkittäviä seurauksia kansalliselle turvallisuudelle ja puolustukselle. Sekä tiivistyvä puolustusyhteistyö että esimerkiksi jäsenmaiden kriittisen infrastruktuurin suojaamiseen tähtäävät CER- ja NIS2-direktiivit luovat sekä mahdollisuuksia että vaateita kansallisten painopisteiden ja prosessien yhteensovittamiselle myös tiedusteluyhteistyön osalta. Kuten valtioneuvoston selonteossa EU-politiikasta (VNS 7/2020 vp) perustellusti

Hybrid CoE
Fabianinkatu 21
FIN-00130
Helsinki, Finland

todetaan, EU-tason tiedusteluyhteistyön merkitys korostuu muun muassa hybridiuhkien torjunnassa.

Kokonaisvaltaisena toimijana EU:n tehokas päätöksenteko edellyttää laajaa tilannekuvaa, jonka vain jäsenvaltiot voivat tarjota. Tilannekuvan merkitys korostuu esimerkiksi valmisteilla olevan EU:n hybridityökalupakin mahdollistamista toimista päätettäessä. Siksi kansallisen tiedon jakamista EU:lle on syytä pyrkiä lisäämään. Erityisesti EU:n tiedusteluanalyysikeskuksen (EU INTCEN) riittävä ja oikea-aikainen tukeminen nousee keskeiseen asemaan. Myös muun kahdenvälisen ja monenvälisen tiedustelutiedon vaihdon merkitys korostuu verkottuneessa maailmassa ja hybridiuhkien leimaamassa turvallisuusympäristössä. Suomen Nato-jäsenyys tulee osaltaan luomaan uusia mahdollisuuksia tehostetulle tiedonvaihdolle.

Siviili- ja sotilastiedustelun painopisteiden tulee olla yhteensovitettuja. Tiedustelun ja tilannekuvan koordinaatioryhmän rooli on tässä keskeinen, mutta yhteensovittaminen tulee varmistaa myös valmistelun muilla tasoilla ja muissa vaiheessa.

Selonteossa todetun mukaisesti lainsäädännön määrittämissä tapauksissa tiedusteluviranomaiset voivat luovuttaa yrityksille ja yksityisille yhteisöille tietoa uhkista, mikä hyödyttää toimijoiden omaa toimintaa ja laajemmin yhteiskuntaa. Tämä on keskeisen tärkeää huomioiden myös yksityisen sektorin roolin kriittisen infrastruktuurin ylläpidossa ja suojaamisessa ja yhteiskunnan kokonaisvarautumisessa. (Samalla tulee huomioida myös kansalliseen turvallisuuteen läheisesti kytkeytyvät kansainväliset toimijat.)

Tiedustelun tiedonhankintajärjestelmiä tulee kehittää kaikissa toimintaympäristöissä, mutta erityisesti avaruus- ja kybertoimintaympäristöissä. Avaruuteen liittyvissä järjestelmissä EU-tason ja muu kansainvälinen yhteistyö korostuu jo järjestelmien korkean hinnan johdosta. Myös esimerkiksi ilmatilaa hyödyntävässä tiedustelussa tulisi harkita resurssien poolaamista sensoreiden saatavuuden varmistamiseksi.

Johtopäätökset

Suomen kansainvälinen toimintaympäristö tulee olemaan vuosikausia poliittisten ja ideologisten vastakkainasettelujen värittämä. Suomeen kohdistuu erimuotoisia vihamielisiä vaikuttamisyrityksiä, joiden muodot ja aikaperspektiivit vaihtelevat. Mitä kattavampi ja ennakoivampi käsitys suomalaisten päätöksentekijöiden keskuudessa vallitsee näistä toimista ja niiden muodostamasta kokonaisuudesta, sitä tehokkaammin Suomi voi suojautua vaikuttamisyrityksiltä ja torjua niitä.

Tiedustelutoiminnan painopisteet tulee asettaa Suomeen kohdistuvien uhkien ja vaikuttamisyritysten kokonaisuus huomioimalla siten, että tiedon tuottaminen ja jakamineen tukee omalta osaltaan poikkihallinnollista yhteistyötä ja edistää näin ollen Suomen

kokonaisturvallisuuden lähestymistapoja. Vihamieliset toimijat pyrkivät kaikin tavoin hyödyntämään tilannetietoisuuteen syntyviä aukkoja ja katvealueita, mikä on syytä ottaa huomioon tiedustelutoiminnan suunnittelussa. Tehokkaalla tiedustelutoiminnalla ja -yhteistyöllä kyetään toisaalta myös aktiivisesti torjumaan informaatioympäristön manipuloinnilla tavoiteltua päätöksenteon ohjailua.

Hybrid CoE
Fabianinkatu 21
FIN-00130
Helsinki, Finland