VALTIONEUVOSTON SELONTEKO SISÄISESTÄ TURVALLISUUDESTA

VNS 6/2025 VP

Asiantuntijalausunto eduskunnan talousvaliokunnalle

Teija Tiilikainen, johtaja

Euroopan hybridiuhkien torjunnan osaamiskeskus

Yleistä

Valtioneuvoston sisäisen turvallisuuden selonteko koskee Suomen sisäisen turvallisuuden toimintaympäristöä ja siihen liittyviä keskeisiä turvallisuusriskejä ja uhkia. Ulkoisen uhkakuvatilanteen osalta selonteko nojaa aiemmin hyväksyttyihin ulko- ja turvallisuuspoliittiseen sekä puolustuspoliittiseen selontekoon. Tässä lausunnossa keskityn valiokunnan pyynnöstä sisäisen turvallisuuden selonteon osaan, joka koskee kriittiseen infrastruktuuriin liittyviä turvallisuusuhkia.

Yhteiskuntien kriittiseen infrastruktuuriin kohdistetut uhat kuten erilaiset sabotaasiteot, häirintätoimet, kyberiskut tai muut suunnitelmalliset vihamieliset toimet ovat lisääntyneet merkittävästi viime vuosina. Ne muodostavat tärkeän kokonaisuuden läntisiä demokratioita heikentämään pyrkivien autoritääristen valtioiden välinevalikoimassa.

Kun näitä hybridiuhiksi kutsuttuja uhkia torjutaan, on hyvä muistaa niiden monimuotoiset tavoitteet vihamielisten toimijoiden tavoitteenasettelussa. Kriittisiin infrastruktuureihin kohdistetuilla häiriöillä tai vahingonteoilla tavoitellaan yhtäältä yhteiskuntien normaalien toimintojen estämistä ja lamauttamista, minkä erityisesti vakavan turvallisuuspoliittisen konfliktin tilanteessa voi katsoa olennaisesti heikentävän kohdevaltion kykyä vastata yleisestä turvallisuudestaan tai puolustuksestaan. Rauhan aikana infrastruktuuri-iskuilla voidaan testata kohdevaltion varautumista ja reaktioita. Niillä voidaan myös heikentää olennaisesti kohdemaan kansalaisten turvallisuudentunnetta taikka sitoa sen hallituksen huomiota ja voimavaroja, jolloin aiheuttajavaltion kannalta keskeisemmän agendan hoitamiselle jää vähemmän mahdollisuuksia.

Nykyisessä turvallisuusympäristössä voi katsoa Venäjän kohdistavan uhkia EU- ja NATO-maiden kriittiseen infrastruktuuriin ruokkiakseen pelkoa ja lietsoakseen epävarmuutta, joka tukee sen tavoitteenasettelua huomion kohdistamiseksi pois Ukrainan tukemisesta.

Kriittisen infrastruktuurin suojaaminen Suomen sisäisen turvallisuuden selonteossa

Sisäisen turvallisuuden selonteossa kriittisen infrastruktuurin suojaamisen tarve liitetään lähinnä merenalaiseen infrastruktuuriin, Ahvenanmaan turvallisuuteen sekä kyberturvallisuuden haasteisiin. Uhan nykyisen relevanssin ja kriittisen infrastruktuurin merkittävien haavoittuvuuksien näkökulmasta huomattavasti laajempi näkökulma olisi ollut suositeltava.

Suomen olisi ensinnäkin arvioitava kriittisen infrastruktuurin haavoittuvuuksia täydentämällä CER-direktiivin vaatimia prosesseja kansallisin toimin. Sektorikohtaisia haavoittuvuusarviointeja tulisi suorittaa yhteistyössä alan yksityisten toimijoiden kanssa. Vain omaa tilannekuvaa ylläpitämällä voidaan varmistua kriittisten infrastruktuurien riittävästä resilienssistä ja kriisinkestävyydestä. Harjoitusten ja koulutusten lisääminen on keskeinen osa resilienssin rakentamista. Yhteiskunnan kannalta kriittiset infrastruktuurit muodostavat myös hyvin monimuotoisen kokonaisuuden ja haavoittuvuusarviointien suunnittelussa on myös hyvä varmistua siitä, ettei mikään keskeinen kokonaisuus putoa esimerkiksi hallinnonalojen väliin sen haavoittuvuuksia tai resilienssin kehittämistä arvioitaessa. Vihamieliset epävakauttamistoimet voivat kaikkein tyypillisimpien infrastruktuurikohteiden lisäksi kohdistua esimerkiksi rahoitusalan infrastruktuuriin kuten pankki- ja maksujärjestelmiin yhtä hyvin kuin esimerkiksi julkisen tiedonvälityksen kannalta merkittävään viestintävälineistöön.

Selonteossa jäävät katveeseen myös suomalaisen kriittisen infrastruktuurin kansalliset keskinäisriippuvuudet samoin kuin riippuvuudet ja rooli osana kansainvälistä järjestelmää erityisesti EU:ta tai NATOa. Suomen kriittiseen infrastruktuuriin voi kohdistua laajoja häiriöitä myös Suomen ulkopuolella tapahtuvan vihamielisen iskun tai häirinnän seurauksena. Myös nämä keskeiset haavoittuvuudet ja riippuvuudet on hyvä tunnistaa etukäteen kansallisten toimintojen turvaamiseksi kriisitilanteessa.

Kolmas merkittävä katveeseen jäävä yksityiskohta koskee sitä hybridiuhkiin liittyvää keskeistä toimintamallia, jossa vihamielisiin operaatioihin haetaan tehoa erilaisten uhkavälineiden samanaikaisesta hyödyntämisestä. Yhteiskuntien kriittisiin infrastruktuureihin kohdistettujen iskujen tai häirintätoimien rinnalla toteutetut informaatio-operaatiot voivat antaa niille huomattavaa lisätehoa esimerkiksi johtamalla kansalaisyhteiskuntaa ja yleistä mielipidettä harhaan koskien iskujen luonnetta tai tarkoitusperiä. Esimerkiksi pankki- tai rahoitusjärjestelmään kohdistuvien kyberiskujen tai muiden häirintätoimien yhteydessä toteutetut tehokkaat informaatio-operaatiot voivat saada aikaan tallettajien tai sijoittajien massiivisen varainsiirron tai nk. pankkipaon. Tällaiset operaatiot luonnollisesti johtavat huomattavaan yhteiskunnalliseen ja poliittiseen epävakauteen tai jopa paniikkiin.

Yhteenveto

Nykyisessä jännitteisessä ja konfliktiherkässä geopoliittisessa ympäristössä läntisten demokratioiden kriittisen infrastruktuurin haavoittuvuuksia on jo monessa yhteydessä käytetty onnistuneesti hyödyksi kohdemaan heikentämis- tai epävakauttamistarkoituksessa. Demokratioiden avoimessa informaatioympäristössä haavoittuvuuksia on mahdotonta kokonaan suojata tai piilottaa. On hyvin todennäköistä, että ne ovat yksi keskeinen kohde vihamielisten valtioiden strategisessa suunnittelussa myös vakavampien konfliktitilanteiden yhteydessä käytettäviksi.

Suomen tulisi varautua suojaamaan kriittisiä infrastruktuurejaan huomioimalla ja kartoittamalla niiden keskeisiä haavoittuvuuksia, jotka juontavat juurensa yhtä hyvin kansallisiin kuin kansainvälisiin olosuhteisiin ja kytköksiin. Hybridiuhkaympäristössä erilaisten uhkavälineiden yhteiskäytön potentiaalia ja seurauksia Suomen turvallisuuden ja yhteiskunnallisen vakauden kannalta tulisi myös huolellisesti kartoittaa ja varautumista tällaisiin uhkatilanteisiin vahvistaa niin erilaisin varautumissuunnitelmin kuin harjoituksinkin.