Eduskunta
Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

30.1.2019

Viite: Liikenne- ja viestintävaliokunnan lausuntopyyntö E 39/2018 vp

E 39/2018 vp VALTIONEUVOSTON SELVITYS: EUROOPPALAINEN LÄHESTYMISTAPA DISINFORMAATION TORJUNTAAN VERKOSSA

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Euroopan hybridiuhkien torjunnan osaamiskeskukselta lausuntoa E 39/2018 vp valtioneuvoston selvityksestä Eurooppalainen lähestymistapa disinformaation torjuntaan verkossa. Euroopan hybridiuhkien torjunnan osaamiskeskus lausuu asiassa seuraavaa:

Yleistä hybridiuhkista:

Euroopan turvallisuusympäristö on viime vuosina ollut merkittävien muutosten kohteena. Turvallisuusympäristön muutosta sekä uusia uhkakuvia käsittelevissä keskusteluissa hybridiuhan käsite nousee usein esille.

Hybridiuhkien lisääntyminen onkin osa Euroopan turvallisuusympäristön muutosta. Kyse ei ole vain hybriditaktiikan hyödyntämisestä osana sotilaallista konfliktia, vaan hybridikeinoja käytetään laajemmin osana voimapolitiikkaa. Hybridivaikuttamisella ymmärretään suunnitelmallista toimintaa, jossa valtiollinen tai ei-valtiollinen toimija voi hyödyntää samanaikaisesti erilaisia keinoja vaikuttaakseen kohteena olevan valtion heikkouksiin ja saavuttaakseen omat tavoitteensa. Kyseeseen voivat tulla esimerkiksi sotilaalliset, taloudelliset tai teknologiaan perustuvat painostuskeinot sekä erilaiset informaatio-operaatiot, mukaan lukien sosiaalisen median hyödyntäminen.

Turvallisuusympäristön muutokseen vaikuttavat muutokset useilla eri toimintasektorilla. Muutoksiin maailmanpolitiikan toimintakentässä ovat vaikuttaneet muun muassa suurvaltojen ja kansainvälisten instituutioiden uudet valtasuhteet sekä pyrkimys niiden uudelleen järjestelyyn. Useat valtiot hakevat itselleen joko alueellisen suurvallan tai globaalin suurvallan statusta.

Median toimintakentällä internet, tiedon tuottamisen ja hankkimisen reaaliaikaisuus sekä sosiaalinen media ovat nousseet merkittävään rooliin. Riippuvuus digitaalisesta ympäristöstä sekä siellä tuotetusta informaatiosta on kasvanut. Tämä on johtanut myös uusien ja epäluotettavien lähteiden nopeaan lisääntymiseen sekä luonut tilaa informaatiovaikuttamiselle, sisällönmanipulaatiolle sekä tehokkaalle mielipiteen muokkaukselle. Hybriditoiminnasta puhuttaessa esillä on usein informaatiovaikuttaminen. Se on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä edelleen yhteiskunnan toimintakykyyn. Informaatiovaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen levittäminen sekä painostaminen, mutta myös sinänsä paikkaansa pitävän tiedon tarkoitushakuinen käyttö. Kyseessä on strateginen toiminta, jonka tavoitteena

on saada kohde tekemään itselleen haitallisia päätöksiä tai toimimaan omaa etuaan vastaan. Informaatiovaikuttamista on vaikea havaita ja torjua, mikä tekee siitä tehokkaan menetelmän demokraattisia prosesseja vastaan käytettäväksi.

Globalisaatio ja keskinäisriippuvuus ovat edenneet yhä pidemmälle, tehden maailmasta yhä monitasoisemman ja moninaisemmin verkottuneen. Linkki sisäisen ja ulkoisen turvallisuuden välillä vahvistuu edelleen, eikä niitä voi erottaa toisistaan. Uhkat ovat usein luonteeltaan rajat ylittäviä, laajalle levinneitä sekä kompleksisia. Usein ne ovat ennalta arvaamattomia, mikä tarkoittaa, että niihin on vaikea varautua. Keskinäisriippuvuuksien myötä myös haavoittuvuudet lisääntyvät. Valtiollisten ja ei-valtiollisten toimijoiden verkottuminen antaa varjopuolenaan mahdollisuuksia myös hybridivaikuttamiselle, kun erinäisten toimintojen takana olevia tahoja sekä syy-seuraussuhteita on vaikea tunnistaa.

Sodan ja konfliktin kuvat ovat olleet voimakkaan muutoksen kohteena. Siinä missä perinteinen sotilaallinen turvallisuus on edelleen relevantti, on yhtä ilmeistä, että monet asiat ovat muuttuneet. Perinteinen raja sodan ja rauhan sekä kansalaisen ja sotilaan välillä on hämärtynyt. Pienet vihreät tunnuksettomat miehet ovat ylittäneet rajoja, kyberhyökkäyksiä toteutetaan enenevässä määrin, trollijoukkoja valjastetaan informaatiovaikuttamiseen sekä pakolaisvirtoja ohjataan rajojen yli.

Toimintakentillä tapahtuneet muutokset sekä sisäisen ja ulkoisen turvallisuuden entistä tiiviimpi yhteen kietoutuminen ovat mahdollistaneet hybridiuhkilla vaikuttamisen, niiden luomisen ja käytön. Verrattuna aiempaan, myös Suomen turvallisuus kytkeytyy entistä selkeämmin globalisaation muokkaamaan toimintakenttään. Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin. Siten myös ulkomaista alkuperää olevan ja siellä syntyvän uhkan seuraukset näkyvät Suomessa aiempaa herkemmin. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhkille on yhteistä se, että taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa.

Kansalliseen turvallisuuteen kohdistuvina uhkina voidaan pitää muun muassa kansainvälistä terrorismia, ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilua, joukkotuhoaseiden ja kaksikäyttötuotteiden levittämispyrkimyksiä sekä sellaista kansainvälistä järjestäytynyttä rikollisuutta, joka pyrkii vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Viime vuosina erityisesti tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhkaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille. Tietoverkoissa tapahtuva sabotaasi ja tiedon vääristäminen ovat myös merkittäviä uhkia.

Lisäksi valtiolliset toimijat voivat käyttää ohjauksessaan olevia ns. liiketaloudellisia toimijoita Suomea tai muita valtioita vahingoittaviin tarkoituksiin muun muassa liiketoimintaperusteisilla hankinnoilla, joilla ei ole kuitenkaan havaittavaa tuottoa suurille investoinneille. Myös ei-valtiolliset toimijat voivat haluta päästä kohteisiin tai anastaa tietoja. Näin ollen kriittisen infrastruktuurin määritteleminen on erityisen tärkeää. Esimerkiksi merkittävät turvallisuuteen linkittyvät liikenteen-valvontajärjestelmät, olisi turvallisinta pitää omassa hallinnassa. Erilaisissa yhtiöittämisprosesseissa hallinnan menetys on mahdollinen. Lisäksi avainhenkilöstön kansalaisuus- ja lojaliteettiasioiden tarkastelut ja menettelyt ovat olennaisen tärkeitä ennalta estävässä työssä.

Nykyisessä turvallisuusympäristössä uhkien ymmärtäminen sekä oman järjestelmän haavoittuvuuksien tunteminen korostuvat. Haavoittuvuuksien käsittelemiseksi ja uhkaan vastaamiseksi on ohjattava resursseja sekä muodostettava luotettava, yhteiskunnan kaikki toimialueet kattava tilannetietoisuus. Ilman tilannetietoisuutta päätöksentekijöiden on mahdotonta tunnistaa todellista muutosta sekä tehdä oikeita johtopäätöksiä tarvittavista toimenpiteistä. Uhkiin vastaaminen ja niiden torjuminen edellyttää valtioilta strategista valmiutta, joka koostuu kattavasta uhkaympäristön tilannekuvasta, ennakoinnin mahdollistavista elementeistä sekä välineistä poliittisten suositusten ja toimintasuunnitelmien laatimiseen.

Erityishuomiot esityksestä:

Hybridivaikuttaminen ja disinformaatio

Tiedonannossa on mainittu hybridivaikuttaminen sekä Suomessa toimiva Euroopan hybridiuhkien torjunnan osaamiskeskus. Tieto hybriditoiminnasta ja siihen liittyvä osaaminen ovat keskeisiä, kun luodaan vahvenpia toimia disinformaation analysoimiseksi ja torjumiseksi. Euroopan hybridiuhkien torjunnan osaamiskeskus järjestää kuluvana vuonna jäsenmaille vaaleihin liittyvän disinformaation torjuntaan keskittyviä koulutuksia sekä harjoituksia. Toimittajille järjestetään erikseen harjoituksia, joiden tarkoituksena on parantaa median resilienssiä. Tämä toiminta tukee EU:n ulkosuhdehallinnon StratCom-toimintaa.

Disinformaation leviäminen on ongelma, joka ei ratkea yhdellä toimenpiteellä, vaan vaatii paljon erilaisia torjutatoimia. Selvitys korostaa kiirreellisten, koordinoitujen ja pitkäkestoisten toimien merkitystä ja tarjoaa laaja-alaisesti toimenpide-ehdotuksia, mikä on kannatettava lähestysmistapa ongelman ratkaisemiseksi.

Disinformaation käyttäminen hybridivaikuttamisen osana tähtää usein epäluottamuksen kylvämiseen kohdemaan yhteiskunnassa. Tästä syystä toimet, joiden tavoitteena on vahvistaa kansalaisten luottamusta viranomaisiin, hallintoon ja vapaaseen mediaan ovat avainasemassa hybridivaikuttamisen torjunnassa ja resilienssin kasvattamisessa. Erityistä huomiota tulee kohdistaa tuleviin Euroopan parlamenttivaaleihin ja informaatiovaikuttamisen ennaltaehkäisyyn sekä nopeaan yhteiseen reagointiin. Tästä syystä selvityksessä mainitut toimet, jotka tähtäävät reaaliaikaisen tiedonvaihdon (Rapid Alert System -verkosto) parantamiseen ja kehittämiseen, laadukkaan journalismin tukemiseen, medialukutaidon parantamiseen ja moniarvoisen ja vaihtoehtoisen mediaympäristön tukemiseen parantavat jäsenmaiden valmiuksia valmistatua, ennaltaehkäistä sekä reagoida informaatiovaikuttamiseen. Samalla on mahdollista parantaa kansalaisten kykyä toimia muuttuneessa informaatioympäristössä ja saada luotettavaa tietoa ja analysoida sitä kriittisesti. Myös toimilla jotka edistävät kyberturvallisuutta on olennainen rooli ongelman ennaltaehkäisemisessä, sillä hack/leak -toiminta on ollut olennaisena osana vaalivaikuttamista Ranskassa ja Yhdysvalloissa. Tärkeää on myös turvata riittävät resurssit EU:n ulkosuhdehallinnon StratCom-toiminnalle.

Lopuksi: Edellä mainittujen turvallisuusympäristön muutoksiin liittyvien syiden perusteella Euroopan hybridiuhkien torjunnan osaamiskeskus katsoo otsikossa mainitun esityksen olevan omalta osaltaan kannatettava ja perusteltu.

.