Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

LAUSUNTO EDUSKUNNAN TALOUSVALIOKUNNALLE 26.02.2025

HE 205/2024 vp Hallituksen esitys eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi

Lainsäädäntöhankkeen tausta:

Meneillään on globaali kilpailu, jossa tavoitellaan maailmanjärjestyksen muutosta ja demokratia-arvojen heikkouksien esilletuomista globaalissa kontekstissa. Kilpailua käydään monilla aloilla, kuten geopolitiikka, geoekonomia, ideologiat, taloudellis- tekninen kehitys ja kulttuurinäkemykset. Tavoitteena on demokratia-arvot jakavien valtioiden (Euro-atlanttinen liittokunta ja vakiintuneet demokraattiset markkinataloudet muualla maailmassa) heikentäminen ja siirtyminen uudenlaiseen alueellisiin hegemonioihin perustuvaan voimapolitiikkaan. Lännen haastajat hakevat poliittista ja taloudellista kasvuvoimaa ns. Globaalin etelän maista ja väestöistä, joiden keskuudessa Kiinan ja Venäjän maakuva on nyt voittopuolisesti myönteinen. Sotia voidaan käyttää kilpailun välineenä, kuten Venäjän sota Ukrainaa vastaan osoittaa. Ukrainan sodan lisäksi on havaittavissa useita sellaisia jännitteitä, jotka voivat johtaa muiden sotien käynnistymiseen varsinkin Aasian-Tyynenmeren alueella. Näilläkin sodilla voi olla suoria yhtymäkohtia Euroopan vakauteen. Suomi on selkeästi osa tällaista laajaa kokonaisuutta, jossa turvallisuuden kannalta sekä oman toimintakyvyn, että liittolaisten tuen varmistaminen on tärkeää.

Hybridiuhkaoperaatioita ja -sodankäyntiä käytetään lisääntyvässä määrin demokratioita vastaan perinteistä sotaa alemman asteisten vaikutusten aikaansaamiseksi. EU:n ja NATO:n alueella on havaittu Venäjän ja Kiinan keräävän tietoa kriittisestä infrastruktuurista ja tämän on arvioitu merkitsevän järjestelmiä vahingoittavien iskujen valmistelua. Sabotaasitekoja on myös jo havaittu, mm asevarastoja, rautateitä ja lentoliikennettä kohtaan. Merenalaisen infrastruktuurin haavoittuvuudet nousevat esille toistuvien sabotaasiepäilyjen yhteydessä. Rahoituslaitoksiin kohdistuvat kyberiskut puolestaan korostavat tarvetta vahvistaa pankki- ja rahoitusjärjestelmien resilienssiä.

Hybridiosaamiskeskus on toimintansa aikana perehtynyt laajasti kriittisen infrastruktuurin rakenteisiin ja niiden haavoittuvuuksiin. Keskus on toteuttanut useita riskien arviointiin liittyviä harjoituksia ja laati yhdessä komission tutkimuskeskuksen kanssa vuonna 2023 Suomessakin toteutetun energiajärjestelmien stressitestistön.

Hybrid CoE
Fabianinkatu 21
FIN-00130
HELSINKI

Työn puitteissa on käynyt ilmi, että modernin yhteiskunnan järjestelmät ovat monimukaisesti verkottuneita ja keskinäisriippuvaisia. Riippuvuudet eivät myöskään rajoitu maantieteellisesti valtioiden rajojen mukaan. Länsimaissa järjestelmät ovat tätä nykyä valtaosin yksityisomistuksessa, eli niitä hoidetaan liiketoimintaperiaatteella ja sama yritys voi tarjota palveluja usean eri valtion alueella. Lisäksi lähes kaikkien järjestelmien tietojen hallinta ja toiminnan ohjaus on digitalisoitu, eli tietoverkon kautta voidaan paitsi ohjata järjestelmiä, myös hyökätä niitä vastaan.

Ukrainan sota on osaltaan parantanut ymmärrystä siitä, kuinka kriittisen infrastruktuuriin vaikutetaan sotilaallisen kriisin alkaessa ja sen aikana. Toiminnassa käytetään sekä fyysistä vahingoittamista että verkkosodankäyntiä. Myös EU:n jäsenvaltioissa on varauduttava näihin molempiin. Avoimissa yhteiskunnissa kriittisistäkin järjestelmistä on saatavilla vapaasti tietoa jopa internetissä. Sen lisäksi vapaa liikkuvuus mahdollistaa kohteiden lähestymiset ilman, että se herättäisi epäilyksiä. Fyysinen uhka kohteita vastaan onkin kohtuullisen helppoa toteuttaa käyttämällä erikoisoperaatioita.

Kuvailtua uhkaympäristöä vasten hallituksen esittämää EU:n CER-direktiivin täytäntöönpanoa voi pitää ensiarvoisen tärkeänä lainsäädäntöhankkeena. Sen myötä Suomelle saadaan lainsäädäntökehys, joka tarjoaa valtiolle paremman näkymän yhteiskunnan kriittisten toimijoiden varautumisen tilaan ja sen kehittämistarpeisiin. CER-direktiivi tarjoaa myös EU:lle välineen suojata kriittisen infrastruktuurin muodostamia keskinäisriippuvuuksia.

Tämä lainsäädäntökokonaisuus on hybridiuhkaympäristössä erittäin tärkeää kehitystä. Esitetty yleislaki ja toiminnan yhteensovittamisesta ja yleisohjauksesta vastaavan ministeriön nimeäminen (Sisäministeriö) ovat riittävän selkä lähtökohta toiminnalle. Lisäksi nimetään valvontaviranomaiset sektorikohtaisesti ja niille annetaan mahdollisuus määrätä laiminlyönneistä aiheutuva seuraamusmaksu, sekä nimetään Valtioneuvoston tilannekeskus tilannekuvan kokoajaksi ja kansainväliseksi yhteyspisteeksi. Nämä toimenpiteet ovat perusteltuja.

Erityisiä huomioita:

CER-direktiivillä asetetaan EU:n jäsenvaltioille velvoitteita välttämättömien yhteiskunnan toimintojen tai taloudellisen toiminnan ylläpitämisen kannalta keskeisten

palveluiden häiriöttömän toiminnan varmistamiseksi. Tämän tavoitteen saavuttamiseksi määritellään yksitoista kriittistä toimialaa, joiden toimijoita koskien määritellään yhdenmukaiset vähimmäissäännöt menettelyille ja vaatimuksille, joilla voidaan turvata keskeisten palveluiden tarjonta, vahvistaa kriittisten toimijoiden häiriönsietokykyä ja parantaa viranomaisten rajat ylittävää yhteistyötä.

Direktiivin toimeenpano edellyttää jäsenvaltioilta ensinnäkin kriittisten toimijoiden määrittelyä sen käsittämillä toimialoilla ja alasektoreilla. Toimijoita on informoitava niiden roolista ja varmistettava, että ne täyttävät direktiivin niihin kohdistamat uudet velvoitteet. Toimijoiden kriisinsietokyvyn arvioimiseksi perustetaan mekanismeja ja indikaattoreita, jotka systemaattisuudessaan tuovat tärkeän lisän olemassaolevaan suomalaiseen järjestelmään. Tällaista kriittisten toimijoiden yksilöintiä voi pitää hyödyllisenä toimenpiteenä jo kansallistakin kriisinkestokykyä ajatellen samoin kuin niiden kansallisten viranomaistahojen määrittelyä, joilla on jatkossa vastuu direktiivin soveltamisesta ja täytäntöönpanosta. Myös kansallisten yhteyspisteiden keskinäinen verkosto ja EU-komission tuki mahdollisimman yhdenmukaisen järjestelmän luomiseksi muodostavat jatkossa tärkeän kokonaisuuden EU-tason resilienssin luomisessa.

Pankkiala ja rahoituslaitokset muodostavat tärkeän osan yhteiskuntien kriittistä infrastruktuuria ja niihin on kohdistettu erimuotoisia häirintäoperaatioita viime aikoina. Laajamittaiset operaatiot voivat onnistuessaan lamauttaa pankki- ja maksupalvelut ja niihin kohdistetuilla häirintätoimilla on myös laajempia valtioiden rajat ylittäviä vaikutuksia. Tämän toimialan liittäminen CER-direktiivin puitteisiin vaikuttaa perustellulta ja tuon selkeän lisän kansallisten järjestelmien puitteissa sovellettaviin häiriönsieto- ja riskienhallintamekanismeihin.

26.2.2025

Euroopan Hybridiuhkien torjunnan
Osaamiskeskuksen johtaja

Teija Tiilikainen

Haavoittuvuudet ja resilienssiverkoston
johtaja, Kommodori evp.

Jukka Savolainen

Hybrid CoE
Fabianinkatu 21
FIN-00130
HELSINKI

Hybrid CoE
The European Centre of Excellence
for Countering Hybrid Threats

Hybrid CoE
Fabianinkatu 21
FIN-00130
HELSINKI