Cyberwatch Finland

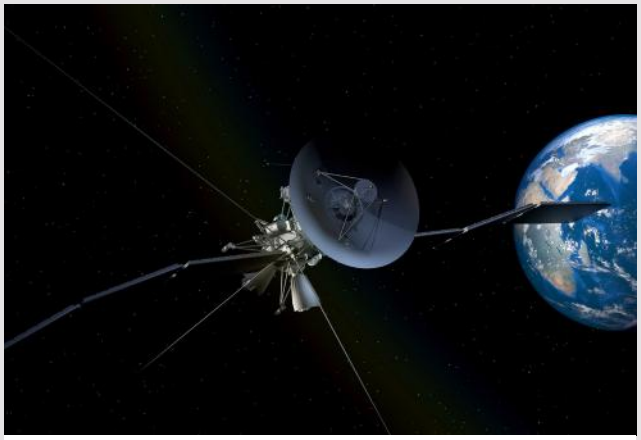
2024

MODERNIN DIGITAALISEN YHTEISKUNNAN HAASTEET JA RESILIENSSI

WHITE PAPER
CYBERWATCH FINLAND

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLLYS



5 EI-KINEETTINEN VAIKUTTAMINEN JA OPERAATIOT

5.1 Hybridivaikuttaminen/operaatiot
5.2 Kybervaikuttaminen/operaatiot
5.3 Informaatiovaikuttaminen/operaatiot
5.4 Elektroninen vaikuttaminen ja operaatiot
5.5 Kognitiivinen vaikuttaminen ja sodankäynti

6 KYBERTURVALLINEN YHTEISKUNTA

6.1 Kansallinen turvallisuus
6.2 Yhteiskunnan resilienssi
6.3 Kokonaisturvallisuuden johtamisen nykytila
6.4 Kokonaisturvallisuuden mallin ja huoltovarmuuden kehittäminen
6.5 Kyberhuoltovarmuus
6.6 Huoltovarmuuden kehittäminen

7 VIRANOMAISTEN JA ELINKEINOELÄMÄN YHTEISTYÖ

8 JOHTOPÄÄTÖKSET

9 KESKEISET LÄHTEET

1. JOHDANTO

EU:n mukaan sähköverkko, liikenneverkko sekä tieto- ja viestintäjärjestelmät ovat kriittisiä infrastruktuureja, jotka ovat välttämättömiä elintärkeiden yhteiskunnallisten toimintojen ylläpitämiseksi. Tällä hetkellä kriittisen infrastruktuurin geopoliittinen toimintaympäristö on erittäin epävakaa, jota selittää erityisesti Venäjän Ukrainaa vastaan käymä hyökkäyssota. Venäjä katsoo käyvänsä kineettistä (perinteistä) sotaa Ukrainassa ja hybridisotaa länsimaista sivilisaatiota vastaan. Tämä näyttäytyy erilaisina kybersabotaasi-iskuina, hybridi- ja informaatiovaikuttamisena sekä dominanssin tavoittelemisena kognitiivisessa toimintaympäristössä. Suomessa ja koko Euroopassa.

Euroopan komissio on käynnistänyt eurooppalaisen kriittisten infrastruktuurien suojaamisohjelman (EPCIP), jonka tarkoituksena on nimensä mukaisesti parantaa kriittisen infrastruktuurin suojaa Euroopassa. Nousevat uhat sekä epätavanomaiset hyökkäykset kriittisiin infrastruktuureihin ovat paljastaneet perinteisen riskinarvioinnin ja riskinhallintatoimien puutteet. Kaikkia uhkia ei voida perinteisin menetelmin ennakoida, ja siksi vaaditaan tehokkaampaa riskianalyysiä ja järjestelmien resilienssiä. Suomalainen kokonaisturvallisuuden malli, jossa huolehtiminen kriittisestä infrastruktuurista on jaettu eri ministeriöiden vastuulle, on nerokas, mutta osin haasteellinen toteuttaa erityisestinopeaa reagointia vaativissa kriisitilanteissa.

Ukrainan sota on muuttanut turvallisuusympäristöämme pysyvästi. Kriittinen infrastruktuuri on ollut kineettisten ja ei-kineettisten iskujen pääkohde. Tämä korostaa kansallista johtamisen koordinointia, uusien kyberturvallisuutta edistävien ohjelmien luomista ja tehokasta kriisijohtamista. Kybersodankäynti Ukrainassa on ollut vaikutuksiltaan odotettua vähäisempää. Venäjä näyttääkin käyttävän Ukrainassa mieluummin perinteistä sotavoimaa, jolla on suurempi tuho ja pelotevaikutus, kuin älykkäitä kyberoperaatioita, joita niiden paljastumisen jälkeen on vaikea käyttää uudestaan. Näyttääkin siltä, että älykkäimmät kyberoperaatiot säästetään hybridivaikuttamisen välineiksi länsimaita vastaan. Näin pystytään operoimaan perinteisen sodan kynnyksen alapuolella ja saadaan aikaan informaatio-psykologisia pelotevaikutuksia. Kognitiivinen sodankäynti on tullut vahvasti osaksi epäsymmetristä sodankäyntiä. Kansalaisten henkistä kriisinkestävyyttä pyritään horjuttamaan pitkäkestoisella hybridioperoinnilla.

Cyberwatchin analyysitiimi on seurannut Ukrainan sodan tapahtumia ja vaikutuksia sen alkamisesta saakka osana kybertilannekatsauksiamme. Tässä selvityksessä käymme läpi Ukrainan sodan ja kansainvälisen toimintaympäristön muutoksen esiin nostamia uusia haasteita ja kehittämistarpeita sekä teemme konkreettisia esityksiä käytännön toimista, joilla modernin digitaalisen yhteiskunnan resilienssiä voidaan parantaa.

2. SOTA UKRAINASSA TUONUT KRIITTISEN INFRASTRUKTUURIN KESKIÖÖN

2.1 KYBERHYÖKKÄYKSIÄ UKRAINAN KRIITTISTÄ INFRASTRUKTUURIA VASTAAN

Venäjä on jatkanut sotatoimia Ukrainassa vuodesta 2014 lähtien Krimin laittoman valtauksen jälkeen. Venäjä aloitti 24.2.2022 YK:n peruskirjaa ja kansainvälistä oikeutta rikkovan sotilaallisen hyökkäyksen Ukrainaan. Ukrainan Kyberturvallisuusviraston johtaja Yuriy Schygol ilmoitti tammikuussa 2023, että vuonna 2022 Ukrainaa kohtaan tehtiin 2 194 kyberhyökkäystä, joista 1 655 Venäjän sotilaallisen suurhyökkäyksen (24.2.) jälkeen. Genevessä päämajaansa pitävän riippumattoman CyberPeace Instituten mukaan Ukrainan siviilikohteisiin on tehty joulukuuhun 2023 mennessä 666 hyökkäystä, Venäjän kohteisiin 331 hyökkäystä ja muihin maihin 2258. Kyberhyökkäyksillä on CyberPeace Instituten arvion mukaan yhteys Venäjän hyökkäyssotaan. Venäjän hyökkäyskohteita sodan aikana ovat olleet:

- Ukrainan hallinto
- Energia
- Tietoliikennesektori
    - Triolan Internet Service Provider
    - Vinasterisk Internet Service Provider
    - Ukrtelecom
- Media
- Kuljetus ja logistiikka
- Vapaaehtoisjärjestöt, NGO:t

Hyökkäyksistä valtaosa on ollut hajautettuja palvelunestohyökkäyksiä (DDoS), joita CyberPeace Instituten tilastoinnin mukaan oli tammikuun 2022 - joulukuu 2023 oli 493. Vastaavana aikana tiedusteluhyökkäyksiä oli 26, kalasteluhyökkäyksiä 23, verkkosivujen manipulointia 22 ja tiedostojen tuhoamiseen tähtääviä hyökkäyksiä (Wiper-haittaohjelmat)18. Kyberhyökkäysten ohella Venäjä toteuttaa laajamittaista informaatiovaikuttamista. Se tuottaa keskimäärin 166 miljoonaa huijausviestiä viikossa, samalla kun yli 50 000 sosiaalisen median valetiliä tuottaa jatkuvasti valeuutisia.

Venäjän turvallisuuselimet GRU, SVR ja FSB ovat toimineet aktiivisesti Ukrainassa ennen sodan alkamista ja sen aikana. Ne kaikki ovat toteuttaneet tietojenkalastelua, mutta GRU on ollut päävastuussa tietoa tuhoavista operaatioista. GRU:hun liitettyjä uhkatoimijoita on myös yhdistetty moniin kyber- ja informaatio-operaatioihin. Venäjä tehosti tietojenkalasteluaan noin vuosi ennen hyökkäyssodan aloittamista, tavoitteena todennäköisesti kerätä tietoa Ukrainan valtionhallinnosta, asevoimista, kriittisestä infrastruktuurista ja kriittisestä informaatioinfrastruktuurista. Lisäksi Venäjä oli kiinnostunut Ukrainaa tukevien maiden poliittisesta päätöksenteosta ja maiden suhteista Ukrainaan. Venäjän informaatio- ja kyberoperaatiot ovat liittyneet tiiviisti toisiinsa läpi sodan. Esimerkiksi ukrainalaisten henkilötietoja on vuodettu osana informaatio-operaatiota, palvelunestohyökkäyksille on annettu avoimesti poliittisia motiiveja ja tietojärjestelmistä hakkeroituja sähköpostiosoitteita on käytetty informaatio-operaatioiden kohdelistoina.

2.2 HAVAINTOJA UKRAINASTA

Ukrainan armeijan pääesikunnan kyberturvallisuusosaston johtaja, eversti Maksym Pavljuk on analysoinut Venäjän hybridioperaatioita. Hänen mukaansa Venäjä testaa jatkuvasti sähkö- ja tietoverkkojenkyberturvallisuuden sietokykyä. Julkisuudesta tunnetut Black Energy (2015), Viasat (2022) ja Kyivstar (2023) ovat olleet tehokkaimpia kyberiskuja. Venäjä suosii kineettisiä iskuja sähköverkkoa ja kriittistä infrastruktuuria vastaan, ja tämän vuoksi Ukrainassa on päivittäisiä katkoksia. Perinteisten iskujen lisäksi pyrkii tekemään hyökkäyksiä sähköverkkoon myös kyberavaruudessa.

ICT-järjestelmissä kyberhyökkäysten vaikutus on monimutkaisempi ja dynaamisempi. Hybridioperaatioissaan Venäjä on kohdistanut hyökkäyksiä siviili-infrastruktuurin lisäksi Ukrainan sotilasjärjestelmiin, datakeskuksiin, ja jopa armeijan henkilöstönhenkilökohtaisiin laitteisiin. Venäjän suurhyökkäyksen jälkeen Ukrainan puolustusvoimien vahvuus nelinkertaistui mobilisoinnin ansiosta. Heti alusta alkaen käyttöön otettiin BYOD-politiikka (engl. Bring your own device). Tämä omien laitteiden käyttö on edellyttänyt tehokasta kyberhygieniaa, jota on toteutettu pakollisen verkkokurssin avulla. Koulutuksessa mm. kuvataan vihollisen tietojenkalastelumetodeja, neuvotaan henkilökohtaisten laitteiden huoltamista sekä annetaan ohjeita laillisista ohjelmistoista ja virustorjunnan päivityksistä. Saadun palautteen mukaan järjestelmä toimii varsin hyvin.

Ukrainassa Venäjän kyberhyökkäysten painopisteitä ovat olleet puolustusvoimien johtamisjärjestelmä, tilannetietoisuus, logistiikka, terveydenhuolto, tykistö, elektroninen sodankäynti ja muut asejärjestelmien tietojärjestelmät. Venäläiset kohdistavat hyökkäyksiä sekä tietoverkoissa sijaitseviin palvelimiin että loppukäyttäjiin. Kyberpuolustusta Ukraina toteuttaa mahdollisimman tehokkaasti kumppanimaiden tuella, jonka vuoksi toistaiseksi em. järjestelmiin ei ole aiheutunut katastrofaalisia vaikutuksia. Tästä huolimatta kyberpuolustuksen suorituskykyä on vahvistettava.

Yhteenvetona Pavljuk toteaa, että sen vastustajat (ei vain Venäjä, vaan muutkin roistovaltiot) eivät ole diletantteja operaatioissa sodan kynnyksen alapuolella, vaikka ohjukset ja pommit olisivatkin käytännössä parempia. Tämä johtaa kahteen päähavaintoon ja suositukseen:

1 Nykyisellä digitaalisella aikakaudella konfliktit eivät ole poissuljettuja ja kybertoimintaympäristö on muiden perinteisten asevoimien toiminta-alueiden ohella merkittävässä roolissa. Siksi tehokas kyberturvallisuus koko kriittisen infrastruktuurin alueella on keskeistä sen resilienssin ja vakaan toiminnan kannalta.

2 Sota Ukrainassa osoittaa, että kyberpuolustuksen kannalta erittäin suojatutkin kohteet ovat saavutettavissa kineettisellä voimalla. NATO-sateenvarjo on hieno asia, mutta Venäjän naapureille Pavljuk suosittelee harkitsemaan tärkeiden kohteiden fyysistä suojaamista. Sähköverkkojen puolustamiseen tarvitaan ilmapuolustus- ja elso-järjestelmiä. Palvelinkeskusten on mahdollisuuksien mukaan oltava siirrettäviä tai sijoitettu maan alle.

2.3 MAALINA KOMMUNIKAATIOJÄRJESTELMÄT

Ukrainassa on sodasta ja Venäjän tuholaistoiminnasta huolimatta onnistuttu pitämään telekommunikaatioverkko (4G) suhteellisen hyvin toiminnassa. Se on vaatinut teleoperaattoreiden ja verkkolaitetoimittajien yhteisponnistuksia. Saumattoman yhteistyön merkitys on koettu kriisinkestävyyden perusedellytykseksi. Ensimmäinen oppi on, että häiriötilanteiden ja poikkeusolojen järjestelyt tulee suunnitella ja harjoitella etukäteen ja niiden tulee olla osa normaalioloissa laadittavia kaupallisia sopimuksia. Varautumisvelvoitteita määriteltäessä tulee ottaa huomioon tarve nopeaan valmiuden kohottamiseen sekä hybridisodankäynnin fyysiset ja epäsymmetriset operaatiot. Ukrainalaiset korostavat toimittajien luotettavuuden merkitystä ja sen arvioimisen vaikeutta sopimuksia tehtäessä. Arvioinnissa tulisi voida käyttää selkeitä kriteereitä, kuten luotettavuus, maturiteettitaso, auditointi ja palautumiskyky häiriötilanteissa. Pelkät lupaukset eivät riitä, vaan operaattoreiden ja verkkolaitetoimittajien kyvykkyys ja luotettavuus pitäisi pystyä todentamaan riittävällä varmuudella.

Ukrainan sota on nostanut esiin telekommunikaation merkityksen kansakunnan henkisen kriisinkestävyyden ylläpitämisessä ja kriittisen infrastruktuurin toiminnan varmistamisessa. Kapasiteettiä on pystyttävä nopeasti kasvattamaan ja verkot pitää pystyä pitämään toiminnassa häiriötilanteista huolimatta. Tämä edellyttää esimerkiksi lisenssien vapauttamista ja kaikkien verkkojen yhteiskäytön mahdollistamista sekä optimointia. Operaattorit ovat olleet tässä koordinaattorin roolissa ja avainasemassa. Verkkolaitetoimittajien varaosien varastointi alueelle ja toimituskyky ovat vaurioiden nopean korjaamisen perusedellytyksiä.

Sodan aikana on opittu monia pieniä yksityiskohtia, kuten verkkojen nopean testauksen järjestelyt, merkkivalojen poistaminen mastoista ja sähkön saannin varmistaminen eri tavoin, myös maan rajojen ulkopuolelta. Edelleen verkkoja on priorisoitu esimerkiksi maksuliikenteen ja sähköverkon toiminnan turvaamiseksi. On myös havaittu, että logistiikan ja varastoinnin järjestelyjen pitää noudattaa samaa logiikkaa kuin ammusten osalta, mikä tarkoittaa varastointia lähelle kohteita ja logististen ketjujen luotettavuuden varmistamista. Myös kahdennetut runkoverkot ovat osoittautuneet välttämättömäksi.

Kommunikaatiojärjestelmät ovat olleet sodan alun kyberiskuista alkaen yksi Venäjä tuholaistoiminnan pääkohteista. Ukrainassa on koettu yhteiskunnan resilienssin kannalta tärkeäksi, että maassa on toiminut useampi operaattori ja verkkolaitetoimittaja. Normaaliajan toimiva markkina luo pohjan kriisitilanteiden kriisinkestävyydelle. Kokonaisvaltainen riskianalyysi helpottaa hahmottamaan yhteiskunnan kriittisten toimintojen, kuten sähköverkon ja telekommunikaatiojärjestelmien keskinäisriippuvuudet; kumpikaan ei toimi ilman toista.

2.4 KYBERTURVALLISUUDEN JOHTAMINEN KOROSTUU

Strategisella tasolla valtioiden tulee perustaa kyberturvallisuuden johtaminen tietoperusteiseen päätöksentekoon. Kerätyn datan perusteella muodostuvan tilannekuvan merkitys on aivan keskeinen. Tarvittavat nopeat strategiset päätökset perustuvat käytettävissä olevaan reaaliaikaiseen tietoon, useisiin vaihtoehtoisiin ratkaisuihin, teknologian mahdollisuuksiin ja asiantuntijoiden tukeen. Strateginen johtamisen avulla voidaan yhteensovittaa, osallistaa ja koordinoida eri kansallisten toimijoiden yhteistyötä kyberturvallisuuteen liittyvässä toiminnassa ja varautumisessa. Lisäksi strateginen johtaminen luo edellytykset niin poliittiselle päätöksenteolle kuin operatiiviselle toiminnalle. Strategisen johtamisjärjestelmän tulee olla kiinteässä vuorovaikutuksessa poliittisten päätöksentekijöiden kanssa. Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista. Kyberturvallisuuden strategisen johtaminen on valtion kyvykkyyksien ja elintärkeiden toimintojen turvaamista, koska tätä kautta myös yksityinen sektori ja kolmas sektori pystyvät rakentamaan toimintaansa toimivien ja turvallisten tietoverkkojen varaan.

Operatiivis-taktisella tasolla kyberturvallisuuden johtamiseen kuuluu joukko oikeudellisia, tiedonhallintaan ja -jakamiseen, organisaation toimintojen johtamiseen ja päätöksentekoon sekä teknologiaan liittyviä toimenpiteitä, joita tarvitaan kyberuhkien- ja -riskienhallinnassa sekä kyberresilienssin toteuttamisessa.

Kyberturvallisuuden (KT) hallintaan on kehitetty erilaisia malleja, jotka painottavat erilaisia asioita sen mukaisesti, mihin tarkoitukseen malli on kehitetty. Oheinen malli koostuu johtamisen seitsemästä osakokonaisuudesta:

1. KT-resurssien johtaminen: tietoisuus systeemien turvallisuusrakenteista, -ratkaisuista niiden haavoittuvuuksista ja heikoista kohdista.

2. KT-organisaation johtaminen: toiminnan johtaminen kyberhyökkäysten ennaltaehkäisyssä, varautumisessa ja häiriötilanteiden hallinnan suunnittelussa.

3. KT-teknologian johtaminen: määritellään käytettävien ohjelmistojen, tietoliikenteen ja tietoverkkojen kyberturvallisuusratkaisut. Määritellään käytettävien ohjelmistojen, tietoliikenteen ja tietoverkkojen kyberturvallisuusratkaisut.

4. KT-kulttuurin johtaminen: johdetaan organisaation henkilöstöä toimimaan kyberturvallisesti, johdetaan kyberturvallisuusosaamisen hallintaa sekä lisätään tietoisuutta yksilön vastuusta kyberturvallisuudessa.

5. KT-juridiikan johtaminen: hallitaan kyberturvallisuuteen liittyvää kansallista ja kansainvälistä lainsäädäntöä ja erityisesti sen vaikutusta organisaation toimintaan.

6. KT-häiriötilanteiden johtaminen: johdetaan kyberonnettomuustilanteita laaditun häiriötilanteiden ja jatkuvuudenhallinnan suunnitelmien ja ohjeiden mukaisesti.

7. KT-strategian johtaminen: johdetaan organisaation kyberturvallisuuden strategiaprosessia sen laadinnasta implementaatioon ja päivityksiin.

Vakavia kyberhäiriötilanteita voi esiintyä sekä normaali- että poikkeusoloissa. Normaaliolojen häiriötilanteet hallitaan viranomaisten tavanomaisin toimivaltuuksin ja organisaatioiden voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä tulee voida hyödyntää normaaliolojen häiriötilanteiden hallinnassa. On ennakoitu, että perinteiset teollisen aikakauden johtamismallit korvautuvat digitaalisen maailman malleilla yllättävän nopeasti.

3. YHTEISKUNNAN KRIITTISET RAKENTEET

3.1 KRIITTINEN INFRASTRUKTUURI

Kriittistä infrastruktuuria ei ole yksiselitteisesti määritelty. Saksan ulkopoliittisen seuran (Deutsche Gesellschaft für Auswärtige Politik, DGAP) raportin (2023) mukaan YK:n 193 jäsenvaltiolla ja Taiwanilla ei ole yhteistä määritelmää kriittiselle infrastruktuurille. Aiheesta on olemassa ainakin sata erilaista kansallista määritelmää. Monilta mailta puuttuu luettelo kriittisen infrastruktuurin tai kriittisten informaatioinfrastruktuurin sektoreista. Sata maata 194:stä on julkaissut kriittisiksi sektoreiksi katsomansa toimialat. Useimmin raporteissa mainitut alat ovat energia (96 %), tieto- ja viestintätekniikka (95 %), liikenne (93 %), talous ja rahoitus (89 %), julkiset palvelut (84 %) sekä terveydenhuoltoala (83 %).

3.1.1 KOKONAISVALTAINEN LÄHESTYMISTAPA JA MÄÄRITTELY

Kyberhyökkäysten merkittävimpänä kohteena on kriittinen infrastruktuuri (engl. Critical Infrastructure, CI), joka käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. Näiden turvaaminen tarkoittaa yksittäisten kriittisten kohtien löytämistä ja turvaamista. Määritelmä on yleensä syntynyt uuden, sisäistä turvallisuutta koskevan lainsäädännön yhteydessä. Kriittisen infrastruktuurin turvaamisessa on kolme ulottuvuutta: poliittinen, taloudellinen ja tekninen.

Poliittiseen ulottuvuuteen kuuluu kansallinen lainsäädäntö ja kansalliset turvallisuustarpeet sekä kansainvälinen yhteistyö näiden ympärillä. Kansainvälisellä yhteistyöllä pyritään samankaltaisiin ratkaisuihin maissa, joiden tarpeet ovat samanlaisia. Yhtenäinen lainsäädäntö ja turvallisuuspolitiikka mahdollistavat teknisen yhteistyön etenkin tilanteissa, joissa infrastruktuurit ovat usean maan yhteiset.

Taloudellinen ulottuvuus käsittää kaikki ne yritykset ja muut taloudelliset toimijat, jotka rakentavat, omistavat ja hallinnoivat infrastruktuurijärjestelmiä ja -laitoksia ja jotka toimivat taloudellisten intressien mukaisesti. Taloudelliseen ulottuvuuteen kuuluu myös turvaamiskustannusten oikeudenmukainen jakaminen eri toimijoiden kesken. Monissa maissa vastuu kriittisen infrastruktuurin toimivuudesta on yksityisillä yrityksillä.

Tekninen ulottuvuus käsittää tekniikan ja sen hyödyntämisen sekä kaikki ne käytännön ratkaisut ja toimenpiteet, joita valtiot ja yritykset tekevät turvatakseen kriittisen infrastruktuurinsa toimivuutta mahdollisten häiriöiden varalta. Nämä verkostot eivät ole erillisiä entiteettejä, vaan muodostavat kansallisen kriittisen infrastruktuuriverkoston, jossa on erittäin paljon keskinäisriippuvuuksia. Yhden systeemin lamaantuminen tai romahtaminen vaikuttaa verkoston muihin osiin.

Kriittinen infrastruktuuri muodostuu siis välineistä ja laitteista, palveluista ja tietojärjestelmistä, jotka ovat kansakunnille niin elintärkeitä, että niiden toimintakyvyttömyydellä tai tuhoutumisella olisi heikentävä vaikutus kansalliseen turvallisuuteen, kansantalouteen, yleiseen terveyteen ja turvallisuuteen sekä valtionhallinnon tehokkaaseen toimintaan.

3.1.2 EU TEHOSTAA KRIITTISEN INFRASTRUKTUURIN SUOJAAMISTA

EU pyrkii regulaatiollaan vahvistamaan jäsenvaltioiden resilienssiä. Kriittisten yksiköiden sietokykyä koskeva direktiivi (engl. Directive on the Resilience of Critical Entities, CER) tuli voimaan 16.1.2023. Jäsenvaltioiden tulee 17.10.2024 mennessä antaa kansallinen lainsäädäntö direktiivin toimeenpanemiseksi. Direktiivin tavoitteena on vahvistaa kriittisten yksiköiden sietokykyä monenlaisia uhkia vastaan.

EU hyväksyi vuonna 2022 kyberturvallisuusdirektiivin (engl. Directive on Security of Network and Information Systems, NIS 2), jolla korvattiin vuoden 2016 verkko- ja tietoturvadirektiivi. Uudella sääntelyllä pyritään varmistamaan yhteinen, korkea kyberturvataso koko unionissa, reagoida muuttuvaan uhkaympäristöön ja ottaa huomioon digitalisaatio, jota koronapandemia on vauhdittanut. Suomessa kansallinen toimeenpano toteutetaan uutena kyberturvallisuuslakina vuoden 2024 loppuun mennessä. Sen tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan kriittisten sektoreiden osalta. NIS2-direktiivissä sen soveltamisen piiriin kuuluvat toimijat on jaoteltu keskeisiin (essential) ja tärkeisiin (muihin) (important, other) toimijoihin. Keskeisiä toimialoja ovat mm. digitaalinen infrastruktuuri, ICT-palvelun hallinta ja energia-ala.

Koska toimialojen (ja toimijoiden) kriittisyyden tason kuvaaminen on toisistaan poikkeavien vaatimusten ja haasteiden kannalta erityisen merkityksellistä, puhutaan tässä selvityksessä näiden osalta kriittisistä toimijoista ja kuvataan kriittisen infrastruktuusin ydin.

3.2 KRIITTISEN INFRASTRUKTUURIN YDIN

NIS2-direktiivin soveltamisalaan kuuluvien toimijoiden tulee toteuttaa asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu sekä estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin. Kriittisestä infrastruktuurista voisi rakentaa kolmitasoisen mallin esimerkiksi keskinäisriippuvuuksien merkittävyyden mukaisesti. Kriittisen infrastruktuurin ytimen muodostavat yhteiskuntien kannalta kriittisimmät toiminnot, joita ovat sähköverkko ja digitaalinen infrastruktuuri sekä paikkatiedon ja tarkan ajan tuottamiseksi tarvittavat satelliittijärjestelmät.

3.2.1 SÄHKÖVERKKO

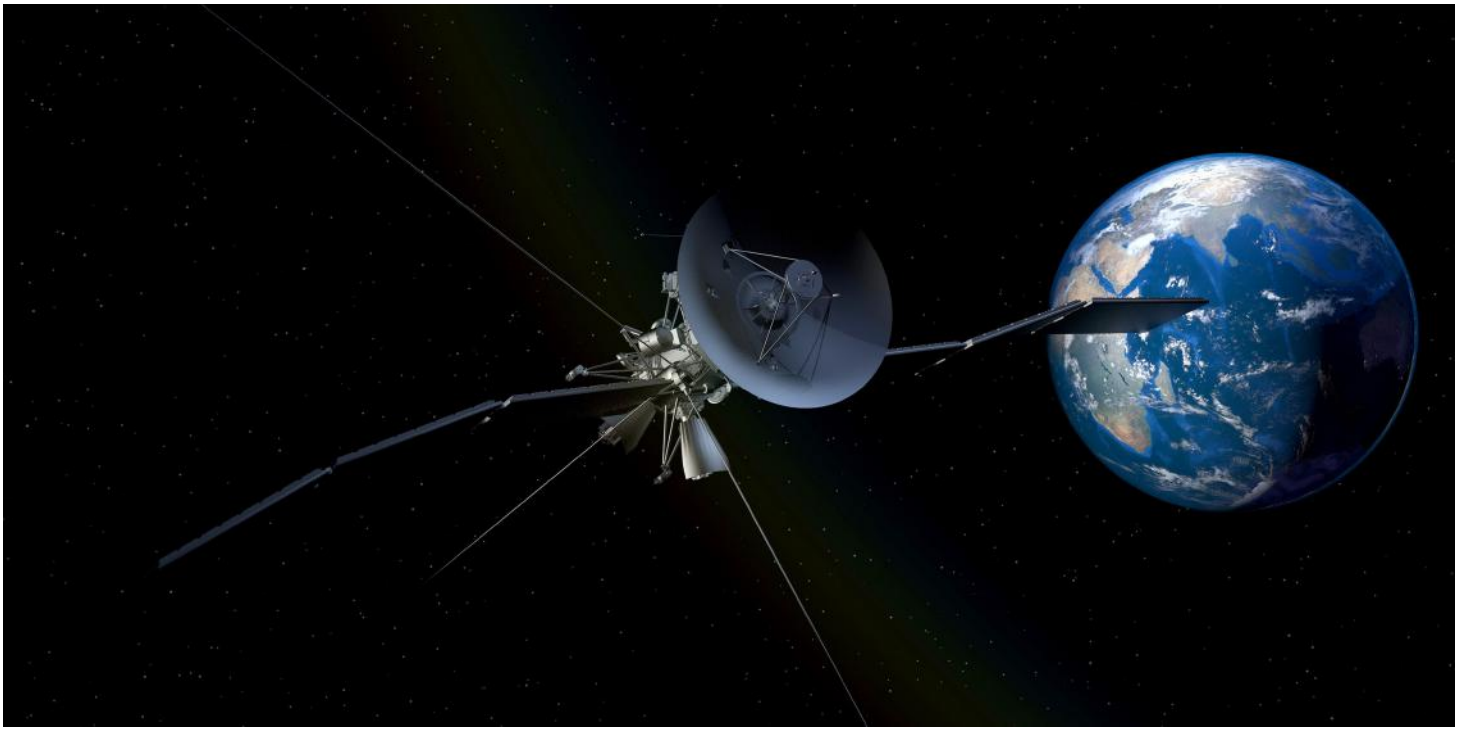
Suomen sähköjärjestelmä koostuu voimalaitoksista, kantaverkosta, suurjännitteisistä jakeluverkoista ja sähkön kuluttajista. Sähköverkkoon kuuluu lukuisia sähköasemia ja jakelumuuntamoita. Sähköasemat ovat verkon solmupisteitä, joissa erijännitteiset voimajohdot yhtyvät. Asemilla voidaan muuntaa, jakaa ja keskittää sähkön siirtoa ja jakelua. Sähköverkon ohjausta varten on teollisuusautomaatioverkko, jolla hallitaan sähköjärjestelmän komponentteja. Energiantoimittajien tulee turvata sekä toiminta- että tietojärjestelmät (OT ja IT) ja varmistaa, että ne toimivat toimitusketjuissaan luotettujen kumppaneiden kanssa. Haasteena on, että Euroopan sähköverkkojen käyttämät käyttöjärjestelmät ovat jopa 40 vuotta vanhoja, mikä tarkoittaa, että niitä on erittäin vaikea tehdä kyberturvallisiksi.

Kriittisten infrastruktuurin elementtejä ovat teollinen ohjausjärjestelmä (ICS), valvonta- ja tiedonkeruujärjestelmä (SCADA), hajautettu ohjausjärjestelmä (DCS) ja käyttötekniikka (OT). Nämä järjestelmät ovat infrastruktuurin avainkomponentteja. Industrial Control System (ICS) on kattotermi, joka sisältää sekä SCADA:n että DCS:n. ICS:t ovat rajapintoja, joissa virtuaalikomennot luovat fyysistä todellisuutta teollisuusympäristöissä. SCADA-järjestelmät ovat näiden ICS:iden ohjelmistopohjaisia elementtejä. ICS- ja SCADA-järjestelmät tarjoavat reaaliaikaista, kaksisuuntaista tiedonkulkua anturien, työasemien ja muiden verkkoon kytkettyjen laitteiden välillä koko järjestelmässä. Ne mahdollistavat jatkuvan ja hajautetun seurannan ja ohjauksen.

3.2.2 DIGITAALINEN INFRASTRUKTUURI

Verkko- ja tietojärjestelmät ovat kehittyneet arjen keskeiseksi osaksi yhteiskuntien digitalisaation ja verkottumisen edetessä nopeasti, myös rajat ylittävässä yhteydenpidossa. Kyberhyökkäysten määrä, laajuus, kehittyneisyys, esiintymistiheys ja vaikutukset lisääntyvät, ja ne muodostavat merkittävän uhkan verkko- ja tietojärjestelmien toiminnalle. Nopeat, toimivat ja turvalliset viestintäverkot ovat modernin yhteiskunnan perusta ja digitalisaation edellytys. Internet on maailmanlaajuinen toisiinsa kytkettyjen tietoverkkojen järjestelmä, joka käyttää internet-protokollaa (TCP/IP) yhdistämään tietoteknisiä laitteita toisiinsa. Se on tietoverkkojen tietoverkko, joka koostuu eri kokoisista miljoonista yksityisistä, julkisista, akateemisista, liike-elämän ja valtiohallintojen tietoverkoista, jotka kytkeytyvät toisiinsa erilaisten teknisten laitteistojen avulla (esim. langattomat ja optiset verkkoteknologiat). Internetissä on laaja valikoima erilaisia tietovarantoja ja -palveluita, kuten esimerkiksi web-sivut, sähköposti, puhelinpalvelut, verkkopankit ja tiedostojen jakamiseen käytetyt vertaisverkot.

Toimivat tietoliikenneyhteydet ovat monella tapaa digitaalisen yhteiskunnan ”verenkierto” ja resilienssin selkäranka. Sähköverkko ja tietoliikenneyhteydet mahdollistavat muiden kriittisten palveluiden ja infrastruktuurin toimivuuden. Lisäksi ne ovat keskinäisriippuvaisia; toinen ei toimi ilman toista. Nämä muodostavat digitaalisen yhteiskunnan toimivuuden kannalta kriittisen infrastruktuurin kriittisen ytimen.



3.2.3 SATELLIITTIJÄRJESTELMÄT

Avaruudesta on tullut elintärkeä ihmiskunnalle ja kriittinen erityisesti maailmantaloudelle ja sitä tukevalle televiestintäverkolle. Suurin osa satelliiteista on tietoliikennesatelliitteja. Kaukokartoitussatelliittien avulla maata ja sen pinnalla olevia kohteita kuvataan, mitataan ja havainnoidaan erilaisilla tavoilla erilaisia tarkoituksia varten. Sääsatelliitteja käytetään säähavaintojen tekemiseen. Tiedustelusatelliiteilla pyritään tarkkailemaan toimintaa toisten valtioiden alueella (esim. joukkojen sijoituksia ja liikkeitä tai ohjustukikohtien ja teollisuuslaitosten rakentamista). Tutkimussatelliittien avulla tutkitaan avaruutta ja siellä olevia kohteita.

Satelliittipaikannus tarkoittaa paikanmääritystä paikallisen tai maailmanlaajuisesti kattavan satelliittijärjestelmän avulla. Maailmanlaajuisesta satelliittipaikannusjärjestelmästä käytetään lyhennettä GNSS (Global Navigation Satellite System). Yhdysvalloilla on GPS, Venäjällä Glonass, Euroopalla Galileo ja Kiinalla BeiDou.

Modernit yhteiskunnat ovat entistä riippuvaisempia satelliittipohjaisista sijainti-,navigointi- ja aikapalveluista (engl. Positioning, Navigation and Timing, PNT). PNT-signaaleista erityisesti tarkka aikapalvelu tukee myös kriittistä infrastruktuuria. Ilman tarkkaa aikaa esimerkiksi rahoituslaitokset eivät pystyisi luomaan aikaleimoja liiketoimille, mikä vaikuttaisi pankkiautomaattien ja luottokorttien käyttöön. Myöskään sähköyhtiöt eivät pystyisi siirtämään sähköä tehokkaasti.

PNT-signaali tukee meri-, maa-, ja lentoliikennettä esimerkiksi reittien suunnittelussa ja ruuhkien hallinnassa. Sotilaille nämä tiedot mahdollistavat ohjusten ja ammusten tarkan kohdistamisen sekä ilma-alusten, maavoimien yksiköiden ja alusten navigoinnin. Lisäksi pelastus- ja poliisitoiminnot tarvitsevat luotettavaa sijaintitietoa. Tämä on tullut selkeästi esille Ukrainan sodan aikana. GNSS-häirintä on siitä hyvä esimerkki. Tulevaisuudessa tulee myös pystyä havaitsemaan yritykset aika- ja paikkatiedon manipulaatiolle, minkä seuraukset olisivat todella kohtalokkaat yhteiskunnan kriittisille palveluille.

Häiriöiltä, häirinnältä ja harhautukselta suojattu julkisesti säännelty satelliittipalvelu (engl. Public Regulated Service, PRS) pyrkii turvaamaan sijainti- ja aikatiedon saatavuuden ja luotettavuuden viranomaisille ja kriittisen infrastruktuurin toimijoille. Paikannuspalveluista ja aikatiedosta on muodostunut yhteiskunnan erittäin kriittinen osa-alue, jota muut kriittiset toiminnot tarvitsevat toimiakseen. Satelliittipalvelun merkitys korostuu myös modernien asejärjestelmien osalta, mikä kasvattaa palvelun kriittisyyttä kansallisessa puolustuksessa.

Satelliittien merkitys osana tietoliikenteen runkoverkkoja kasvaa merkittävästi lähitulevaisuudessa. Langattoman tietoliikenteen 5G NTN (5G Non-terrestrial Networks) -konsepti on lähellä käyttöönottoa ja se tulee käyttämään tiedonsiirron tukiasemina matalan kiertoradan LEO-satelliitteja (Low Earth Orbit) ja muita miehittämättömiä lentolaitteita. 5G NTN -kehityksen tavoitteena on yhdistää tällä hetkellä erikseen toimivat maanpäälliset ja satelliittipohjaiset tietoliikenneverkot.

Lähivuosina kuluttajien kännykät käyttävät sujuvasti rinnakkain sekä maanpäällisiä tukiasemia että satelliitteja. IoT-sensoreita voidaan asentaa keskellä erämaata tai valtamerta sijaitseviin tuotantolaitoksiin, kun niitä voidaan ohjata 5G NTN -verkkojen avulla. Satelliittijärjestelmistä tulee samalla olennainen osa energian ja sähköntuotannon toimivuutta sekä osa digitaalista infrastruktuuria, ja samalla sen painoarvo kriittisen infrastruktuurin ytimessä kasvaa.

4 TOIMINTAYMPÄRISTÖN MUUTOSTEKIJÄT

4.1 DIGITALISAATIO

Yhteiskuntien digitalisoituminen jatkuu vauhdilla. Digitaaliset palvelut perustuvat ihmisten, innovatiivisten toimijoiden ja älykkäiden koneiden ekosysteemiin. Tavoitteena on tehdä palveluista toimivampia ja joustavampia sekä kustannustehokkaita. Digitalisaatiossa tulee mahdollistaa entistä paremmat ja luotettavammat palveluketjut ja järjestelmät kansalaisten, julkisen sektorin ja yritysten tarpeisiin. Digitalisaation seurauksena syntyy myös uudenlaisia uhkia. Digitaalinen maailma houkuttelee rikollisia, jotka etsivät uusia mahdollisuuksia anastaa, hyödyntää ja myydä tietoa. Tiedon ja informaation siirtyminen verkkoon on tuonut sinne myös tiedusteluorganisaatiot. Terroristeille kybermaailma on yhteydenpidon, viestinnän ja vaikuttamisen toimintaympäristö, minkä lisäksi se on heille houkutteleva hyökkäyskohde. Asevoimien digitalisaatio on luonut sotilaallisen kybermaailman, jossa vaikuttavat verkottuneiden sotilaiden lisäksi älykkäät ja yhä itsenäisemmät asejärjestelmät. Näistä syistä digitalisaation vahvistuessa ja laajentuessa keskiöön tulisi nostaa informaatio- ja kyberturvallisuus.

4.2 DIGIYHTEISKUNNAN MILITARISOITUMINEN

Elektronisen sodankäynnin, informaatiosodankäynnin ja kybersodankäynnin operaatiot muodostavat viitekehyksenä kyberajan ei-kineettisten verkkoperusteisten operaatioiden kokonaisuuden. Sodankäynnissä nämä operaatiot muodostavat verkottuneen kokonaisuuden, jossa eri operaatiomuotojen avulla pyritään saavuttamaan sodankäynnille asetetut tavoitteet usein osana hybridivaikuttamista. Kyberympäristöstä on tullut erottamaton osa niin nykyajan sodankäyntiä kuin kansallista kybertoimintaympäristöä. Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia toteuttaa yhä kehittyneempiä kyberoperaatioita, joilla on sotilaallisia, poliittisia ja taloudellisia tavoitteita. Äärimmillään yhteiskunnan haavoittuvuuksia hyödynnetään kyberoperaatioissa kriittisen infrastruktuurin sabotoimiseen, lamauttamiseen ja tuhoamiseen. Tämä on tullut selkeästi esiin Ukrainan sodassa.

4.3 SODANKÄYNNIN PARADIGMAN MUUTOS

Perinteinen rauha-sota-asetelma on digitalisaatiokehityksen myötä muuttunut perinteisestä clausewitzilaisesta tarkkarajaisesta mallista epämääräiseksi, ennustamattomaksi ja epävakaaksi ulko- ja turvallisuuspolitiikan toimintaympäristöksi. Sodankäynti on kahden itsenäisen toimijan välistä organisoitua, vihamielistä vaikuttamista, jossa keskeinen ja perinteinen keino on fyysinen väkivalta. Sen tavoitteena on vastapuolen taivuttaminen omaan tahtoon. Clausewitzin mukaan sota jatkaa valtion politiikkaa toisin keinoin. Tämän perinteisen jaottelun rinnalle on muodostunut osapuolten ulko- ja turvallisuuspolitiikan kriisiytymisvaihe, jota kutsutaan harmaaksi vaiheeksi rauhan ja sodan välissä. Sitä voidaan kuvata valmistelevaksi vaiheeksi, joka kuvaa sodan aloittamista edeltävää toimintaa. Harmaa vaihe käsittää laajan skaalan erilaisia toimia, jotka nykyisin määritellään hybridivaikuttamisena tai hybridisodankäyntinä.

Kuva 1. Perinteinen rauha-sota-asetelma.

Venäjä on omassa retoriikassaan todennut olevansa sodassa lännen kanssa. Tämä ajattelutapa muuttaa edellä kuvattua näkökulmaa. Siinä sotatila on keskeinen olotila, jonka intensiivisyysasteet vaihtelevat. Alla olevassa kuvassa 3 on esitetty uuden kylmän sodan rauhan-sodan-ajan asetelma.

Kuva 2. Uuden kylmän sodan ajan rauha-sota-asetelma.

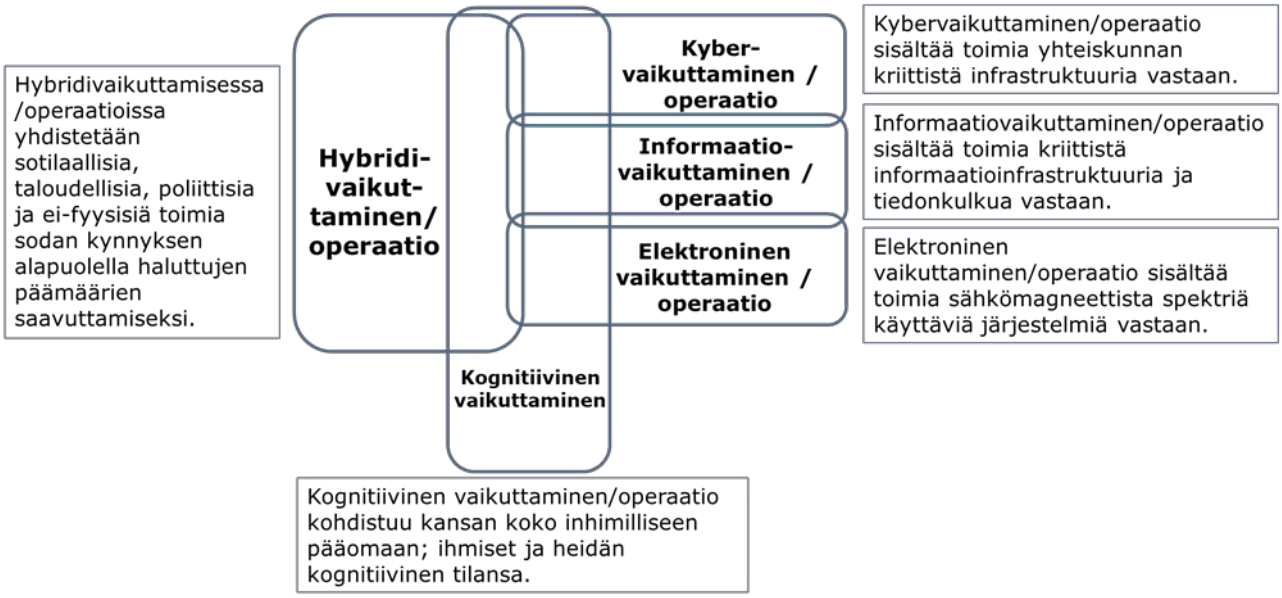
Uusi sodankäynnin paradigma on syrjäyttämässä perinteisen mallin sodan julistamisesta rauhan sopimiseen luomalla tilan, jossa sotaa ei julisteta eikä rauhaa solmita. Tämä asetelma yhdessä yhteiskunnan digitalisaation kanssa mahdollistaa tilan, jossa erilaista ei-kineettistä vaikuttamista voidaan toteuttaa eri vaiheissa ennen aktiivista sotaa pysyen sodan kynnyksen alapuolella ja toimijoiden attribuution ulottumattomissa. Avoimen sodan aikana ei-kineettisiä operaatioita toteutetaan maa-, meri, ilma- ja avaruusoperaatioiden rinnalla ja niiden tukena ja mahdollistajana.

Tässä asetelmassa sodankäynnin käsite ja siihen liittyvät operaatiot edellyttävät toimijoiden välistä avointa sotaa, joten sen ulkopuolella tapahtuvat toiminnat tulee määritelmällisesti erottaa avoimen sodan toiminnoista. Ei-kineettiset toiminnot voidaan määritellä rauhan ja konfliktin aikana vaikuttamiseksi ja aktiivisen sodan aikana operaatioiksi. Korkealla abstraktiotasolla vaikuttaminen ja operaatiot ovat toiminnallisesti samankaltaisia; eroja ilmenee maalittamisessa ja toiminnan intensiteetissä.

Ei-kineettisten operaatioiden avulla erityisesti suurvallat voivat perustella läsnäoloaan sekä vaikuttaa ja luoda sekasortoa haluamillaan alueilla. Toimintaa voidaan perustella rauhanturvaamisella, tasapainon säilyttämisellä, omien etujen ja kansalaisten suojaamisella tai liittolaisten tukemisella, ylipäätään kaikella näennäisesti hyväksyttävällä toiminnalla. Digitaalinen toimintaympäristö on luonut uuden tilan vaikuttaa toisen valtion alueella käyttämällä hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi. Digitaalinen toimintaympäristö soveltuu hyvin hybridisodankäyntiin ja sen eri muotoihin, erityisesti kun operaatiot voidaan toteuttaa yllätyksellisesti ja ilman, että tekijä paljastuu.

5 EI-KINEETTINEN VAIKUTTAMINEN JA OPERAATIOT

Tässä selvityksessä tarkastellaan erityisesti ei-kineettistä toimintaa korkealla abstraktiotasolla, joten rauhan ajan vaikuttaminen ja sotilaalliset operaatiot käsitellään yhtenä kokonaisuutena. Digitaalisessa toimintaympäristössä hybridi-, informaatio- ja kybervaikuttaminen ja operaatiot sekä elektroninen ja kognitiivinen vaikuttaminen muodostavat monitasoisen, kompleksisen ja yhteen sulautuneen kokonaisuuden, jossa ilmiöt eivät ole määritelmällisesti tai toiminnallisesti tarkkarajaisia. Hybridisodankäynnin, elektronisen sodankäynnin, informaatiosodankäynnin, kybersodankäynnin ja kognitiivisen sodankäynnin operaatiot muodostavat kyberajan ei-kineettisten verkkoperusteisten operaatioiden kokonaisuuden.



Kuva 3. Ei-kineettinen toimintaympäristö, (lähde Dr Martti Lehto)

5.1 HYBRIDIVAIKUTTAMINEN JA OPERAATIOT

Hybridivaikuttaminen sisältää sotilaallisten, poliittisten, taloudellisten, siviili- ja tiedotusvälineiden systemaattisen integroinnin, ja se ilmentyy usein ns. harmaalla alueella, tavanomaisen sodan kynnyksen alapuolella. Tällä alueella hybridioperaatioita käytetään epätavanomaisesti ja innovatiivisesti, jotta vältetään attribuutio eli operaation toteuttajan tunnistaminen ja vastuun kohdentaminen. Hybridivaikuttamisen keinovalikoimaan kuuluvat mm. diplomaattiset, taloudelliset ja sotilaalliset keinot sekä informaatio- ja kybervaikuttaminen. Hybridioperaatioita toteuttavat ensisijaisesti valtiolliset toimijat. Hybridioperaatioiden eri menetelmiä on äärimmäisen houkuttelevaa kokeilla, koska niissä on suhteellisen pieni kiinnijäämis- ja eskalaationriski verrattuna perinteisiin sotilaallisiin operaatioihin tai muihin vaikuttamismenetelmiin.

Hybridisodankäynnissä vihamielinen valtio voi käyttää valtiollisia (asevoimat/turvallisuuspalvelu) tai ei-valtiollisia toimijoita (erilaiset rikollis- tai aktivistiryhmät) sodankäynnin ei-näkyvässä osassa kieltääkseen osallisuutensa usein siviilikohteisiin kohdistuviin iskuihin, mutta tavoitteenaan saavuttaa strategisia tavoitteitaan. Hybridisodankäynti sijoittuu sodan ja rauhan välimaastoon. Hybridioperaatioiden havaitseminen ja estäminen olisi tehtävä varhaisessa vaiheessa, ennen kuin hyökkääjä ottaa käyttöönsä koko hybridimenetelmien arsenaalin. Hybridioperaatioiden havaitsemiskykyä (ennakkovaroitus) on parannettava, jotta vastustajan toiminta ja vaikuttamisyritykset voidaan lopettaa ennen kuin ne ovat kunnolla alkaneetkaan.

5.2 KYBERVAIKUTTAMINEN JA OPERAATIOT

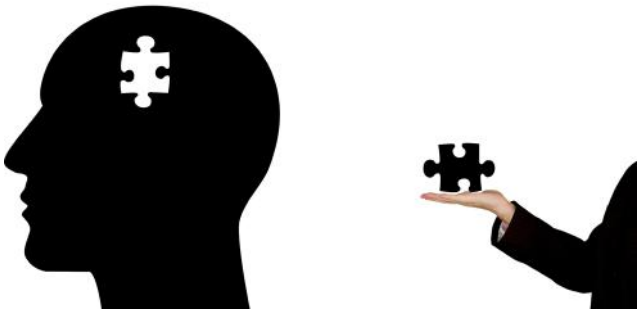
Normaaliaikoina **kybervaikuttaminen** on erilaisten kybersabotaasioperaatioiden toteuttamista, jossa hyökkääjä pyrkii pysymään sodan kynnyksen alapuolella. Tavoitteina voivat olla epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäyskykyjen testaaminen sekä hybridioperaatioiden tai sodan valmistelu. Kybersabotaasin aikakausi alkoi Stuxnet-verkkomadon myötä vuonna 2010. Se oli ensimmäinen virus, joka kohdisti hyökkäyksen toiminnan ohjausjärjestelmään (SCADA) kohteenaan Iranin ydinrikastuslaitos.

Kybersodankäynnissä hyökkäysten kohteena eivät ole vain asevoimat, vaan yhteiskunnan kriittinen infrastruktuuri ja sen elintärkeät toiminnot, aivan kuten kybersabotaasissa. Kybersodankäynti on myös yksi tekijä fyysisen sotilaallisen voiman käytön mahdollistajana, kuten Ukrainan sodan yhteydessä on voitu nähdä.Yhteiskunnan elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja siksi kyberhyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

5.3 INFORMAATIOVAIKUTTAMINEN JA OPERAATIOT

Normaalioloissa informaatiovaikuttamisella pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn eri kampanjoiden avulla. Informaatiotilaa halutaan hallita erityisesti sosiaalisen median alustojen avulla. Informaatio-operaatioilla voidaan tuottaa ja jakaa vääristeltyä tietoa näillä alustoilla ja siten mobilisoida suuria ihmisjoukkoja ja lisätä yleistä levottomuutta sekä vastakkainasettelua yhteiskunnassa. Eri toimijat yhteiskunnassa pyrkivät omilla vastuualueillaan torjumaan disinformaatiota sekä aggressiivista ja anonyymia vaikuttamista Internetissä. Tässä riippumaton, itsenäinen media ja kansalaisten koulutustaso ovat avainasemassa ja osa yhteiskunnan informaatiopuolustusta.

Informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista eli informaatioylivoiman hankkimista. Informaatiopuolustuksen päämäärä on suojata maanpuolustuksen toimintoja ulkoa ohjatun ja muun vahingoittamistarkoituksessa tehdyn viestinnän vaikutuksilta. Erityisen tärkeää on tunnistaa tarpeet yhteensovittaa eri toimintatavat viranomaisten, elinkeinoelämän ja muiden toimijoiden kesken. Lisäksi suorituskykyjen kehittämisessä tarvitaan yhteistoimintaa kaikkien viranomaisten ja kansainvälisten kumppanien kanssa.



5.4 ELEKTRONINEN VAIKUTTAMINEN JA OPERAATIOT

Kaikkia sähkömagneettisen spektrin alueita käytetään tutkimuksessa, viranomaispalveluissa, sotilaallisissa sovelluksissa ja myös monissa arkipäivän sovelluksissa. Yksi kehityssuunta on jatkuva siirtyminen yhä suurempien taajuuksien käyttöön, jotta yhä suurempien tietomäärien siirtäminen olisi mahdollista. Keskeinen sovellusalue on kommunikaatio (satelliitti, mobiili, radio).

Elektronisen vaikuttamisen keinoilla hyökkääjä operoi sotaa alemmalla tasolla. Näillä operaatioilla suojataan omia järjestelmiä ja tuotetaan häiriöitä kohteen sähkömagneettisen spektrin alueen laitteissa ja järjestelmissä. Tästä hyvä esimerkki on Venäjän GPS-häirintä, jota se on toteuttanut pitkään erityisesti NATO:n sotaharjoitusten aikana. Ukrainan sodan aikana toiminta on laajentunut.

Elektronisen sodankäynnin keinoilla hyökkääjä pyrkii vaikuttamaan informaation kulkuun siten, että johtamisen ja tulenkäyttöjärjestelmien luotettavuus alenee ja informaatiorakenteiden käytettävyys pienenee. Elektronisen sodankäynnin operaatioilla on yhteys informaatio- ja kyberoperaatioihin. Elektronisilla offensiivisilla operaatioilla pyritään estämään, hidastamaan tai vähentämään vihollisen sähkömagneettista säteilyä hyödyntävien tai elektroniikasta riippuvien järjestelmien käyttöä taikka suuntaamaan käyttö oman toiminnan kannalta edulliselle alueelle.

5.5 KOGNITIIVINEN VAIKUTTAMINEN JA SODANKÄYNTI

Kyber- ja informaatioajan teknologinen kehitys on ottanut seuraavan askeleen kohti kognitiivista vaikuttamista ja sodankäyntiä. Kehitys tuottaa vaikeasti hallittavan haasteen. Siinä ymmärryksemme maailmasta ja reaktiomme sen tapahtumiin häiriintyvät asteittain pitkän ajan kuluessa ja hienovaraisesti tuottaen ajan mittaan merkittäviä haitallisia vaikutuksia. Kognitiivinen vaikuttaminen ja sodankäynti kohdistuu yksilöistä valtioihin ja monikansallisiin organisaatioihin. Se ruokkii disinformaation ja propagandan tekniikoita, joiden tarkoituksena on kyllästää ja lamaannuttaa tiedon vastaanottajat psykologisesti. Olemme kaikki osa tätä vaikuttamista tietoisesti tai alitajuisesti, ja erityisesti avoimet yhteiskunnat ovat haavoittuvia.

Kognitiivinen vaikuttaminen ja sodankäynti tuo uuden merkittävän uuden ulottuvuuden digitaaliseen yhteiskuntaan ja taistelukentälle sekä haastaa kokonaisturvallisuuden mallimme. Maa-, meri-, ilma- ja informaatioulottuvuuden, sekä kyberneettisen, spatiaalisen ja sähkömagneettisen ulottuvuuksien rinnalle on tullut kognitiivinen ulottuvuus. Modernien teknologioiden avulla voidaan kognitiivista taistelutilaa hallinta globaalisti. Tämän mahdollistaa yhteiskuntien ja yksilöiden globaali verkostoituminen (engl. hyper-connectivity).

Toiminnan tarkoituksena on muuttaa vastustajan kognitiivisia prosesseja, hyödyntää ennakkoluuloja ja mentaalisia toimintatapoja sekä vääristää havaintoja, jotta saadaan aikaan ajattelun vääristymiä, muutoksia päätöksentekoon ja toimintaamme aiheuttaen jopa tuhoisia seurauksia sekä yksilötasolla että kollektiivisella tasolla. Kehityksen mahdollistaa NBIC (Nanotechnology/Biotechnology/Information Technology and Cognitive Science) kehitys. NBIC:ta voidaan myös hyödyntää johtajien ja taistelijoiden kognitiivisten valmiuksien parantamiseen, ihmisen ja koneen välisten rajapintojen kehittämiseen sekä robotiikan ja kognitiivisten teknologioiden (AI/ML) yhteistoiminnan hyödyntämiseen.

Kognitiivisessa vaikuttamisessa tekoälyä voidaan käyttää vastustajan päättäjien pelotteluun ja yleisen mielipiteen manipulointiin. Yleisen mielipiteen suoran manipuloinnin käsitteleminen vaatii monimutkaista toimintaa. Eri toimenpitein vaikutetaan, suojellaan ja/tai häiritään yksilön ja ryhmän kognitiivisia tuntemuksia. Toiminnot vaihtelevat suuresti toimintaympäristöistä ja kulttuureista riippuen. Kognitiivisessa vaikuttamisessa ihmismielestä tulee taistelukenttä. Tavoitteena ei ole muuttaa vain sitä, mitä ihmiset ajattelevat, vaan myös sitä, miten he toimivat ja vaikuttavat osana digitaalista yhteiskuntaa. Kognitiivisessa vaikuttamisessa tekoäly tuodaan eri muodoissaan yhteiskunnan eri tasoille. Geneerisellä tekoälyllä voidaan tuottaa tekstiä, ääntä ja kuvaa disinformaation, valeuutisten ja parjauskampanjoiden tuottamiseen. Jatkuva kehitys tekoälyssä, kognitiivisissa tieteissä, neuroteknologiassa ja muilla niihin liittyvillä aloilla lisää entisestään joukkomanipulaatioriskiä ja mahdollistaa mielen militarisoitumisen. Tämä on jatkossa otettava huomioon kansalaisten henkisen kriisinsietokyvyn ylläpitäviä toimia mietittäessä.

Kognitiivinen sodankäynti edustaa paradigman muutosta myös sotilaallisten operaatioiden suorittamisessa. Se on tekoälyn ja koneoppimisen strategista käyttöä, jolla vaikutetaan vastustajien kognitiivisiin prosesseihin. Tavoitteena on manipuloida päätöksentekoprosessia, luoda hämmennystä ja lopulta saada strateginen etu. Tämä lähestymistapa tunnustetaan yhä useammin tehokkaaksi työkaluksi nykyaikaisessa sodankäynnissä, koska se hyödyntää tekoälyn tehoa ihmisen kykyjen lisäämiseen. Kognitiivisessa sodankäynnissä yhdistyy ja synkronoituu perinteisten kineettisten ja ei-kineettisten sodankäyntimuotojen elementtejä, joilla vaikutetaan toimijoiden (sotilaat ja poliitikot) asenteisiin ja käyttäytymiseen. Sillä pyritään vaikuttamaan vastustajien mieliin ja muokkaamaan heidän päätöksiään ja luomaan näin strategisesti suotuisa ympäristö tai alistamaan heidät ilman taistelua.

6. KYBERTURVALLINEN YHTEISKUNTA

6.1 KANSALLINEN TURVALLISUUS

Kansallisessa turvallisuudessa on kyse koko suomalaisen yhteiskunnan yhteisestä turvallisuudesta ja Suomen suvereniteetista. Käsitteenä kansallinen turvallisuus on dynaaminen ja määrittyy sekä ajassa että suhteessa Suomen muuttuvaan uhka- ja toimintaympäristöön.

Uudessa digitaalisen maailman normaali- ja poikkeusolojen ei-kineettisessä uhkaympäristössä on mielekästä tarkastella kansallista turvallisuutta kahden käsitteen avulla: kokonaisturvallisuus ja kokonaismaanpuolustus. Kokonaisturvallisuus on suomalaisen varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä. Sen toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa. Kokonaisturvallisuuden yleiset periaatteet linjataan Yhteiskunnan turvallisuusstrategiassa, jota ollaan uudistamassa. Kokonaismaanpuolustus tarkoittaa siviili- ja sotilasalojen toimintaa, jolla turvataan kansalaisten elinmahdollisuudet ja turvallisuus ulkoista, muiden valtioiden aiheuttamaa tai muuta uhkaa vastaan sekä viime kädessä valtiollinen itsenäisyys. Kokonaismaanpuolustuksen järjestelyillä mahdollistetaan koko yhteiskunnan tuki sotilaalliselle puolustukselle poikkeusoloissa. Näiden käsitteiden sisältöä on jatkossa tarkasteltava entistä enemmän ei-kineettisten uhkien näkökulmasta, ottaen huomioon digitaalisen yhteiskunnan resilienssi ja siinä tapahtuvat muutokset.

6.2 YHTEISKUNNAN RESILIENSSI

Yhteiskunnan resilienssi ilmentää uutta hallintamentaliteettia, jossa turvallisuus kytketään varautumiseen, ennustamattomien riskien kohtaamiseen sekä epävarmuuden kanssa elämiseen. Resilienssin määritelmät ja käsitteen merkitys vaihtelevat käyttöyhteydestä ja toimintakulttuurista riippuen. Suomen turvallisuus, hyvinvointi ja huoltovarmuus ovat aiempaa riippuvaisempia yhteiskunnan keskeisten, useasti rajat ylittävien ja kansallisen toimivallan ulottumattomissa olevien toimintojen jatkuvuudesta. Huoltovarmuusajattelussa onkin ryhdytty painottamaan organisaatioiden toimintaprosessien jatkuvuuden varmistamista ja kriittisen infrastruktuurin turvaamista jo normaalioloissa. Globaalit logistiset ketjut ja kumppanuudet ja niiden kyberturvallisuus korostuvat jatkossa.

Kaikkiin kuviteltavissa oleviin uhkiin on haastavaa varautua tehokkaasti. Siksi on luotava suotuisat olosuhteet resilienssiin perustuvalle lähestymiselle kansallisen turvallisuuden edistämiseksi erityisesti kriittisen infrastruktuurin suojaamisessa. Resilienssi-käsite kuvaa kykyä kestää äkillisiä iskuja ja toipua tai palautua takaisin niistä. Turvallisuus ja siihen liittyvä resilienssi on keskeinen tekijä yhteiskunnan elintärkeiden toimintojen jatkuvuuden sekä erityisesti sen kriittisen infrastruktuurin toimivuuden varmistamisessa. Ennakoivan tilannekuvan ja hyvä riskitietoisuus ovat entistä tärkeämpiä.

Eurooppalaisen Galileon PRS-palvelun tarkoitus on tuottaa vuodesta 2026 alkaen varmennettua ja häiriöitä, häirintää sekä manipulointia paremmin kestävää aika- ja paikkatietoa EU:n jäsenvaltioiden eri viranomaisille ja kriittisen infrastruktuurin toimijoille. Se vähentää riippuvuutta muista satelliittijärjestelmistä. Palvelu parantaa selkeästi Suomen turvallisuutta ja huoltovarmuutta. Suomen maantieteellinen asema asettaa erityisiä haasteita ja siksi on hyvä, että PRS-palvelu otetaan käyttöön heti, kun se on käytettävissä. PRS-palvelu tulee tuottamaan avoimiin satelliittiperusteisiin aika- ja paikkapalveluihin verrattuna merkittävästi turvatumpaa aika- ja paikkatietoa. PRS-palvelu tukee Suomessa kokonaisturvallisuutta ja on osa Suomen kansallisen kyberturvallisuuden varmistamista. Palvelun käyttöönotto vaikuttaa myönteisesti myös Suomen huoltovarmuuteen vähentämällä suomalaisten toimijoiden riippuvuutta Euroopan ulkopuolisista aika- ja paikkajärjestelmistä. Suomessa PRS-palvelun suunniteltuja käyttäjiä ovat sisäministeriön ja sosiaali- ja terveysministeriön viranomaiskäyttäjät, Puolustusvoimat, Tulli sekä kriittisen infrastruktuurin toimijat, kuten teleoperaattorit ja energia-, finanssi- ja logistiikka-alan toimijat.

6.3 KOKONAISTURVALLISUUDEN JOHTAMISEN NYKYTILA

Suomen kokonaisturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa. Kokonaisturvallisuuden strateginen johtaminen on kansallisten turvallisuus- ja puolustusselontekojen, strategioiden ja pitkän tähtäimen suunnittelun toimeenpanoa. Strateginen johtaminen vie yhteiskuntaa kohti asetettua tavoitetilaa. Strategisen johtajuuden toimeenpanotehtävän perustana on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistaminen ja asettaminen.

Kansallinen kokonaisturvallisuuden strategisen tason johtaminen muodostuu kolmesta osakokonaisuudesta:

1. Normaaliolojen turvallisuusjohtaminen
2. Normaali- ja poikkeusolojen häiriötilanteiden hallinnan johtaminen
3. Varautumisen ja huoltovarmuuden johtaminen

Vakavia häiriötilanteita voi esiintyä sekä normaali- että poikkeusoloissa. Normaaliolojen häiriötilanteet hallitaan viranomaisten tavanomaisin toimivaltuuksin ja organisaatioiden voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliolojen häiriötilanteiden hallinnassa. Varautumisessa yhdistyy huoltovarmuus ja omavaraisuudesta huolehtiminen. Tämä tarkoittaa väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen ja niihin liittyvien teknisten järjestelmien turvaamista poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta. Varautumista ohjaa eri elintärkeille toiminnoille asetetut velvoitteet ja organisaatioiden omat tavoitteet erityisesti toiminnan jatkuvuuden hallinnan kannalta.

6.4 KOKONAISTURVALLISUUDEN MALLIN JA HUOLTOVARMUUDEN KEHITTÄMINEN

Ukrainan sodasta on saatu hyödyllisiä kokemuksia Suomen kokonaisturvallisuuden mallin kehittämiseksi. Strategisen johtamisen näkökulmasta, ja erityisesti digitalisaation lisääntyessä, on välttämätöntä, että yllättäen ja yhteiskunnassa nopeasti syntyvien laaja-alaisten kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti. Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on myös välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta. Kybertoimintaympäristön ja sähkömagneettisen spektrin alueen häiriötilanteiden sekä hybridi-, informaatio- ja kognitiivisenvaikuttamisen hallinta yhdessä näihin varautumisen kanssa edellyttävät nykyistä vahvempaa johtamista. Kokonaisturvallisuuden toimintamalli on sisällään erittäin toimiva, mutta mentäessä operatiivisen toiminnan tasolle, tulee olla kyky nopeasti reagoida nopeasti muuttuviin uhkakuviin.

Mallia voitaisiin ottaa esimerkiksi Yhdysvaltojen kyberturvallisuuden strategisesta johtamisesta, josta vastaa Kansallinen kyberjohtajan toimisto (The Office of the National Cyber Director, ONCD) sijoitettuna presidentin kansliaan (White House). Sen tehtävä on:

- Varmistaa liittovaltiotason kyberturvallisuusstrategian ja toimintaohjeiden toimeenpano
- Parantaa julkista ja yksityistä yhteistyötä (engl. Public-Private Partnership, PPP)
- Allokoida resursseja liittovaltion tavoitteiden mukaisesti
- Lisätä olemassa olevaa ja tulevaisuudessa tarvittavaa kyberresilienssiä

Suomessakin tulisi selkeyttää kyberturvallisuuden johtamismallia ja johtovastuita. Kyberiskut tulevat aina yllättäen ja etenevät entistä nopeammin, mikä haastaa kokonaisturvallisuuden johtamismallimme. ”Kansallinen kybernyrkki” tarvittaisiin, jotta pystytään ylläpitämään yhteiskunnan elintärkeitä toimintoja ja kriittistä infrastruktuuria toiminnassa yllättävissä häiriötilanteissa. Viranomaisten ja yritysten yhteistyön kehittäminen pitää olla jatkuva prosessi.

Sotilaallisen puolustuksen toimintakyky ja järjestelmät perustuvat yhä enemmän digitalisaatioon, informaatioon ja avaruuden hyödyntämiseen. Puolustusjärjestelmällä on kyettävä entistä kattavammin valvomaan eri toimintaympäristöjä, ymmärtämään ristikkäisvaikutuksia niiden välillä sekä tarvittaessa käynnistämään puolustukselliset toimenpiteet eri ympäristöissä. Kyberuhkat on kyettävä havaitsemaan ajoissa, ja kyberympäristön muutoksia on kyettävä seuraamaan reaaliajassa. Toimivan kyberpuolustuksen valvonta- ja tilannekuvan avulla havaitaan ja tunnistetaan valtiolliset ja muut uhkatoimijat sekä estetään niiden pääsy puolustusjärjestelmän kannalta keskeisiin järjestelmiin ja tietoihin. Sotilaallinen kyber-

puolustus on entistä riippuvaisempi koko yhteiskunnan kyberresiliteetistä. Suomalainen asevelvollisuusjärjestelmä on arvokas menestystekijä ja sen merkitys korostuu erityisesti kriittisten osa-alueiden osaamisen kehittämisessä ja yhteistoiminnan järjestelyissä.

6.5 KYBERHUOLTOVARMUUS

Huoltovarmuus on yhteiskunnan kokonaisturvallisuuden yksi peruspilareista. Kyberhuoltovarmuuden turvaamisen toimintalogiikka poikkeaa perinteisestä huoltovarmuuden turvaamisesta. Kybertoimintaympäristössä korostuvat erityisesti prosessit sekä tuotanto- ja toimitusketjut. Kyberturvallisuudessa useat kansalliset kriittiset prosessit ovat integroituneet erilaisiin globaaleihin toimintaprosesseihin ja logistisiin ketjuihin. Käytännön esimerkkeinä toiminnasta ovat ulkomailla sijaitsevat palvelimet, pilvipalvelut ja finanssialan varmennusketjut. Toimitusverkoston huoltovarmuutta on mahdotonta ylläpitää tai hallita pelkästään kansallisin toimin. Toiminta edellyttää rajat ylittävää verkostokyvykkyyttä sekä kansainvälistä yhteistyötä ja kumppaneita. Kyberturvallisuuden varmistamista ja kyberhuoltovarmuuden turvaamista haastavat lisäksi toimintaympäristön hajanaisuus, muutosten nopeus ja vaikeasti ennustettava poliittinen kehitys.

Toimivat kansalliset ja kansainväliset markkinat, monipuolinen teollinen ja muu tuotannollinen pohja sekä kilpailukykyinen vakaa julkinen talous ovat huoltovarmuuden perusta. Keskeinen osa varautumista on aktiivinen viranomaisten ja yritysten välinen yhteistyö ja sopimukset. Markkinatoimijoiden kyky sopeutua häiriöihin ja toimintansa jatkuvuuden turvaaminen määrittää kriittisen tuotannon ja palveluiden kriisinsietokyvyn.

Huoltovarmuus rakentuu kriittisillä sektoreilla toimivien yritysten kyvystä reagoida normaali- poikkeusolojen häiriötilanteisiin sekä palautua niistä nopeasti. Yhteiskunnan kriisitilanteissakin lähtökohtana on markkinaehtoinen toiminta. Jos markkinat eivät pysty ylläpitämään yhteiskunnan taloudellisia ja teknisiä perustoimintoja häiriötilanteissa ja poikkeusoloissa, tarvitaan koko yhteiskunnan turvaavia toimia. Yritysten jatkuvuuden hallinnan suunnittelu ja varautuminen luo perustan poikkeusolojen toimintakyvylle. Ukrainan sota on osoittanut kansainvälisten kumppanuuksien ja toimivien logististen ketjujen merkityksen, tämä on otettava huomioon jo normaaliolojen järjestelyitä tarkasteltaessa.

6.6 HUOLTOVARMUUDEN KEHITTÄMINEN

Kansallisesti tulee varmistaa, että markkinat toimivat mahdollisimman tehokkaasti kansantalouden, kuluttajien ja maan turvallisuuden eduksi. Kun kilpailu markkinoilla toimii hyvin, se kannustaa yrityksiä kehittämään tuotteita ja palveluita, jotka ovat käyttäjän kannalta edullisia ja vastaavat entistä paremmin heidän erilaisiin tarpeisiinsa. Laaja markkina tarjoaa kyberturvallisuustuotteiden ja -palveluiden käyttäjille riittävästi vaihtoehtoja, joista he voivat valita itselleen sopivimman. Kybermarkkinassa tämä tarkoittaa myös kaksikäyttötuotteiden kehittämistä. Kaksikäyttötuote on tuote, joka soveltuu normaalin siviilikäytön lisäksi myös sotilaallisiin tarkoituksiin. Huoltovarmuustoimenpiteiden toteutuksessa merkittävässä asemassa on julkisen ja yksityisen sektorin kumppanuus sekä logistiikan toimintavarmuus. Huoltovarmuutta turvataan eräillä toimialoilla myös velvoittavilla säädöksillä. Lainsäädäntöä tulee kehittää, jotta viranomaiset voivat kehittää huoltovarmuutta tukevia rakenteita ja toimintamalleja sellaisia tilanteita varten, joissa markkinat eivät yksin riitä ylläpitämään tarvittavaa huoltovarmuuden tasoa.

Voimassa olevan hallitusohjelman mukaan huoltovarmuuden näkökulma otetaan huomioon kaikessa päätöksenteossa kaikilla hallinnonaloilla. Hallitus varmistaa riittävän huoltovarmuuden tason, jotta väestön toimeentulon, talouselämän ja maanpuolustuksen kannalta välttämätön tuotanto, palvelut ja infrastruktuuri voidaan turvata normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa. Lisäksi hallitus varmistaa valtioneuvoston huoltovarmuuspäätöksellä, että huoltovarmuuden taso vastaa muuttuneen turvallisuusympäristön vaatimuksia ja selvittää geopoliittisten riskien ja riippuvuuksien vaikutukset huoltovarmuuteen. Ohjelman mukaan huoltovarmuutta vahvistetaan kehittämällä kansainvälistä yhteistyötä EU:n ja NATO:n kautta sekä kahdenvälisesti eri valtioiden kanssa. Edelleen hallitus selvittää tarpeen ja mahdollisuudet uudistaa yleistä julkisten hankintojen sääntelyä EU-sääntelyn puitteissa siten, että huoltovarmuustarpeet tulevat riittävästi huomioiduiksi. Toivottavasti nämä toimenpiteet saadaan toteutettua ja vaikuttamaan yhteiskuntamme kriittisten toimintojen resiliteetin kehittämistä. Toiminta edellyttää aina rajat ylittävää verkostokyvykkyyttä sekä kansainvälistä yhteistyötä ja kumppaneita

7. VIRANOMAISTEN JA ELINKEINOELÄMÄN YHTEISTYÖ

Julkisen ja yksityisen sektorin kumppanuusmallissa (engl. Public-Private Partnership, PPP) julkinen ja yksityinen sektori tekevät yhteistyötä saavuttaakseen asetetut yhteiset tavoitteet. Yksityisen ja julkisen sektorin kumppanuus luo mahdollisuuden yhdistää eri tahojen osaaminen sekä synnyttää uusia ratkaisuja ja palveluita. PPP-mallissa huomio tulee kiinnittää yksityisen ja julkisen sektorin välisen yhteistyön tuottamiin molemminpuolisiin hyötyihin. Kansallinen kyberturvallisuus edellyttää laajaa ja tiivistä yhteistyötä viranomaisten, kolmannen sektorin järjestöjen ja elinkeinoelämän kesken. Yhteistyö tarkoittaa hyvin erilaisia toimintatapoja ja se voi olla pitkäkestoista tai projektiluonteista. Yhteistyön selkeät rakenteet ja pitkäjänteinen toiminnanohjaus tukevat kyberturvallisuuden kehittämistä ja eri hallinnonaloilla toimivien viranomaisten yhteistyötä. Kansallisten viranomaisten ja yritysten keskinäistä luottamusta tulee vahvistaa, mikä antaa yrityksille näköalan kilpailukykyisestä toimintaympäristöstä ja varmuutta investoida.

Voimassa olevassa hallitusohjelmassa todetaan, vahva teollisuuspolitiikka tukee koko yhteiskunnan resilienssiä ja huoltovarmuuden kehittymistä. Investoinnit digiteknologiaan ja sen tehokas soveltaminen ovat yritysten kilpailu¬kyvyn ja kasvun keskiössä. Tämä tarkoittaa valtion ja yksityisten toimijoiden välisen kyberturvallisuusalan kehittämistä, johon kuuluvat keskinäisen luottamuksen lisääminen, strategioiden tehokas toimeenpano, kriittisen infrastruktuurin kokonaisturvallisuus, standardointi sekä yhteistyö kumppaneiden kanssa. Erityisesti kyberturvallisuudessa tarvitaan vahvaa ja pitkäjänteistä teollisuuspolitiikkaa, jotta Suomen ja Euroopan strategista kilpailukykyä, omavaraisuutta ja huoltovarmuutta voidaan kehittää. Digitalisaation laajentuminen edellyttää kyberturvallisuuden vahvistamista, jossa erityisiä teemoja ovat kvanttilaskenta, nopeat langattomat verkot ja tekoäly. Tähän tarvitaan erityinen eri toimijat huomioon ottava kyberteollisuuden strategia/teknologiaohjelma, jossa:

1. Yhteistyöstä on välitöntä hyötyä viranomaisille ja yrityksille.
2. Yhteistyö aikaansaa pysyvää verkostoitumista yritysten ja viranomaisten välillä.
3. Yhteistyöhön kytketään mukaan julkinen ja yksityinen koulutus- ja tutkimussektori.
4. Yhteistyö linkittää yhteistyön eri tasot (valtakunnallinen – alueellinen – paikallinen).
5. Yhteistyössä kaikilla osapuolilla on tosiasiallinen mahdollisuus vaikuttaa toimintaan.

Kyberturvallisuuteen liittyvä PPP-kumppanuus tulee kuvata selkeästi kansallisessa politiikassa ja/tai lainsäädännössä. Tämä edellyttää julkisen ja yksityisen sektorin välisten järjestelyjen merkityksen tunnustamista kansallisessa kyberturvallisuuspolitiikassa ja -strategioissa. Jatkossa tarvitaan entistä enemmän avointa yksityisen sektorin kuulemista siihen vaikuttavissa poliittisissa, lainsäädännöllisissä ja sääntelyyn liittyvissä päätöksissä.

8. JOHTOPÄÄTÖKSET

Tämä selvitys on keskittynyt Ukrainan sodasta saatujen kokemusten analysointiin ja modernin digitaalisen yhteiskunnan haasteiden tarkastelussa neljään osa-alueeseen:

1 Kriittisen infrastruktuurin ydin

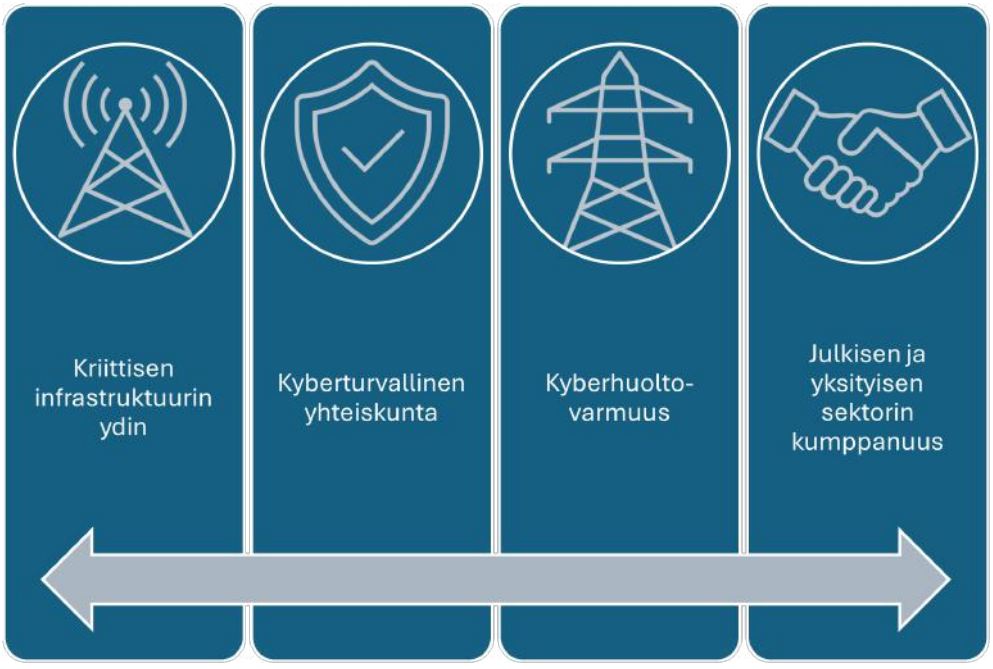
2 Kyberturvallinen yhteiskunta

3 Kyberhuoltovarmuus

4 Julkisen ja yksityisen sektorin kumppanuus

Kansallisen turvallisuuden strategisena tavoitteena tulee olla yhteiskunnan kriittisten palveluiden ja infrastruktuurin toiminnan turvaaminen kaikissa olosuhteissa. Se tulee tapahtua kriittisen infrastruktuurin, erityisesti kriittisen infrastruktuurin ytimen, resilienssin vahvistamisella osana kyberturvallista yhteiskuntaa, jossa erityinen huomio on kohdistettu kyberhuoltovarmuuteen sekä julkisen ja yksityisen sektorin tiiviiseen yhteistoimintaan. Kriittisen infrastruktuurin määrittelyä tulee tarkentaa, ottaen huomioon monimutkaiset keskinäisriippuvuudet ja laajat epäsymmetriset vaikuttamisen keinot. Kriisijohtamisvalmiutta tulee kehittää niin kansallisella kuin yksittäisten yritystenkin tasolla. Huoltovarmuuden varautumisen ja jatkuvuuden hallinnan merkitys korostuu entisestään.

ALLA OLEVASSA KUVASSA ON ESITETTY TÄMÄN SELVITYKSEN NELJÄ PILARIA.



Kuva 4. Kehittämisen neljä pilaria

KRIITTISEN INFRASTRUKTUURIN YDIN:

- Määritellään kansallisen kriittisen infrastruktuurin ydin osana kansallista kriittistä infrastruktuuria ja palveluja.
- Laaditaan tälle kriittiselle infrastruktuurille oma erityinen kyberturvallisuusohjelma, jossa otetaan huomioon sekä ei-kineettinen ja kineettinen vaikuttaminen eri valmiustiloissa ja häiriötilanteissa.
- Tehostetaan toimenpiteitä EU-regulaation vaatimusten toimeenpanossa kriittisen infrastruktuurin ytimen osalta, tavoitteena mahdollisimman suuri kotimaisuusaste ja toimivat kansainväliset kumppanuudet.
- Selkeytetään kriittisen infrastruktuurin määrittelyä, koordinaatiota ja kriisijohtamisjärjestelyjä.
- Parannetaan kriittisen infrastruktuurin toimijoiden uhka- ja riskitietoisuutta.

KYBERTURVALLINEN YHTEISKUNTA:

- Laaditaan kattava toimintaohjelma, jossa otetaan huomioon koko ei-kineettisen vaikuttamisen ja operoinnin kirjo (hybridi-informaatio-kyber-elektroninen-kognitiivinen).
- Kehitetään kansallista kyberriskianalyysiä, ottaen huomioon Ukrainan sodan opetukset ja toimintaympäristön muutos.
- Määritellään selkeä kansallinen ei-kineettisen turvallisuuden johtovastuu ja johtamisen rakenteet - ”kybernyrkki”.
- Vahvistetaan myös ei-kineettisen sodankäynnin johtamista perustamalla sille oma johtoporras (National Cyber and Information Command).
- Kehitetään kyberturvallisuuden toimenpiteitä, jolla vahvistetaan Suomen digitaalista itsenäisyyttä ja strategista autonomiaa osana Euroopan unionia.
- Kehitetään kyberuhkatiedustelun kapasiteettia ja kansallista kybertilannekuvaa.

KYBERHUOLTOVARMUUS:

- Muodostetaan kattava ja pitkäaikainen teknologia/huoltovarmuusohjelma ei-kineettiseen toimintaympäristöön.
- Määritellään EU:n viitekehyksessä keskeiset periaatteet, jolla vahvistetaan kotimaista kyberturvallisuusalan tuotteiden ja palveluiden tuottamista.
- Vahvistetaan kansallista kyberturvallisuuden huoltovarmuusekosysteemiä ja kansainvälistä kumppanuusverkostoa sekä logistisia järjestelyjä.

JULKISEN JA YKSITYISEN SEKTORIN KUMPPANUUS:

- Kehitetään julkisen ja yksityisen sektorin tiiviimpää ja luottamusta vahvistavaa yhteistoimintamallia ja siihen liittyviä käytännön toimenpiteitä.
- Kehitetään ja tarjotaan yhdessä julkisen sektorin ja yksityisen sektorin kanssa keskitettyjä, toimintavarmoja ja kustannustehokkaita kyberturvallisuuspalveluja.
- Kehitetään yhdessä entistä tehokkaampia tiedon, riskianalyysien ja tilannekuvan vaihto- sekä -analysointimekanismeja.
- Laaditaan yhteinen varautumissuunnitelma kyberhuoltovarmuuden ylläpitämiseksi, joka kattaen normaaliolot ja erilaiset häiriötilanteet aina poikkeusoloihin asti.

Ukrainan sota tarjoaa paljon hyödyllistä tietoa yhteiskuntamme kokonaisturvallisuuden kehittämiseksi. Toimintaympäristömme radikaali muutos vaatii selkeitä toimenpiteitä ja uutta ajattelua, innovaatiota ja johtamista. Muutostekijät ovat usein yllättäviä ja tapahtuvat nopeasti. Yrityksissä riskianalyysi on jatkuva prosessi. Jatkossa näin tulisi olla kansallisella tasolla. Koko yhteiskunnan kattavan tilannekuvatoiminnan kehittäminen nousee keskiöön ja sen tulisi luoda selkeämpi pohja kansalliselle riskianalyysille. Yritykset voisivat jakaa omaa uhka- ja riskitietojaan täydentämään viranomaisten toimintaa. Samoin tulisi kiinnittää huomiota siihen, ettei kriittisen tiedon jakaminen jää hallinnonalojen ”raja-aitojen” takia jakamatta. Kokonaisuuden hallinta korostuu ja erityishuomiota tulee kiinnittää yhteiskunnan kaikkein kriittisimmän infrastruktuurin ytimen riskiarvion ylläpitämiseen ja uhkaympäristön seurantaan sekä havainnointikyvyn parantamiseen.

Kyberturvallisuus on aina organisaation johdon vastuulla. Organisaatioiden johdon tulee tarkastella säännöllisesti muuttuneiden kyberturvallisuuden uhkakuvien vaikutuksia omaan toimintaansa ottaen huomioon lainsäädännön muutokset, jotka osaltaan antavat vaatimuksia kyberturvallisuuden toteuttamiselle.

Jatkuvasti muuttuva ja laajentuva kyberturvallisuusympäristö edellyttää organisaatioita varaamaan riittävät resurssit kyberturvallisuuden varmistamiseksi ja tarvittavien toimenpiteiden toteuttamiseksi, missä erityisesti korostuu toiminnan johtaminen ja kyberriskien hallinta.

Kyberturvallisuuteen liittyvillä julkisen ja yksityisen sektorin toimenpiteillä ja muilla järjestelyillä on oltava selkeämmät tavoitteet ja toimintamallit. Tämä edellyttää ekosysteemiyhteistyön tiivistämistä, selkeää käsitystä kansallisesta kyberturvallisuuden tilasta, keskeisten alojen tunnistamista, joilla yhteistyö olisi kaikkien tehokkaita sekä keskinäisen sitoutumisen vahvistamista. Tähän tarvitaan tehokasta kansallisen kyberturvallisuuden strategista johtamista sekä varautumisessa että normaali- ja poikkeusolojen häiriötilanteiden johtamisessa ja hallinnassa. Kriisijohtamiskyvyn kehittämiseen tulee kiinnittää erityistä huomiota hallinnon eri tasoilla ja yhteiskunnan kannalta kriittisten yritysten varautumisessa.

KESKEISET LÄHTEET:

Cyberwatch Finland katsaukset 2022–2024

du Cluzel Francois. 2023. Cognitive Warfare, a Battle for the Brain, ACT Norfolk, Virginia

Huoltovarmuuskeskus. 2024. Kotisivut, https://www.huoltovarmuuskeskus.fi/

Koichiro Takagi. 2022. New Tech, New Concepts: China's Plans for AI and Cognitive Warfare, War on the Rocks, April 13, 2022.

Kosola Jyrki & Jokinen Janne. 2004. Elektroninen sodankäynti, osa 1 – taistelun viides dimensio. Tekniikan laitos, julkaisusarja 5, No 2/2004, Helsinki: Maanpuolustuskorkeakoulu.

Lehto Martti & Limnéll Jarno. 2017. Kybersodankäynnin kehityksestä ja tulevaisuudesta, kirjassa Silvasti M (Edit.) Tiede- ja Ase, 2017, sivut 179–212.

Lehto Martti, Limnéll Jarno, Kokkomäki Tuomas, Pöyhönen Jouni, Salminen Mirva. 2018. Kyber-turvallisuuden strateginen johtaminen Suomessa, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, maaliskuu 2018.

Lehto Martti, Neittaanmäki Pekka. 2016. Digitalisaatio muuttaa yhteiskunnan ja yksilöiden tapaa toimia, Tiedepolitiikka 1/2016, s. 56–64.

Park Jin. 2023. AI in Warfare: The Dawn of Cognitive Combat, 31. May 2023.

Pohjankoski Merja. 2023. Kyberhyökkäyksistä Ukrainassa 2022, pro gradu tutkielma, Jyväskylän yliopisto.

Pye Graeme and Warren Matthew. 2011. Analysis and Modelling of Critical Infrastructure Systems, Proceedings of the 10th European Conference on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 7-8 July 2011, s. 194-201.

Pöyhönen, Jouni. 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, JYU Dissertations 270, 67–70.

Tvaronavičienė M., Plėta T., Della Casa S. 2021. Cyber Security Management Model for Critical Infrastructure Protection, International Scientific Conference, 13–14 May 2021, Vilnius, Lithuania.

Valtioneuvoston kanslia. 2017. Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 5:2017.

Valtioneuvoston kanslia. 2018. Valtioneuvoston päätös huoltovarmuuden tavoitteista, Valtioneuvoston päätös 1048/2018.

Valtioneuvoston kanslia. 2020. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko, Valtioneuvoston kanslian julkaisusarja 30:2020.

Valtioneuvoston kanslia. 2021. Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 28:2021.

Valtioneuvoston kanslia. 2022. Valtioneuvoston huoltovarmuusselonteko, Valtioneuvoston julkaisuja 8:2022.

Valtioneuvoston kanslia. 2023. Vahva ja välittävä Suomi - Pääministeri Petteri Orpon hallituksen ohjelma, Valtioneuvoston julkaisuja 58:2023

Cyberwatch Finland

JULKAISIJA
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

SISÄLTÖ
Toimitusjohtaja
Aapo Cederberg
aapo@cyberwatchfinland.fi

Toimitussihteeri
Elina Turunen
elina@cyberwatchfinland.fi

ULKOASU JA TAITTO
Elina Turunen
elina@cyberwatchfinland.fi

KUVITUS
Gencraft
Pixabay
Shutterstock

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

PAINO
Scanseri Oy, Helsinki

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Ota yhteyttä

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi