Kyberturvallisuuden skenaariot 2035 – johdon yhteenveto

Esipuhe

Kyberturvallisuuden skenaariot 2035 kuvaavat neljä vaihtoehtoista tulevaisuuden maailmaa, joissa kiihtyvä teknologinen kehitys, keskinäisriippuvuudet, suuryritysten valta ja sääntelyn onnistuminen muovaavat tulevaisuuden kyberympäristöä hyvin eri tavoin.

Skenaariotyön tarkoituksena on tarjota väline ymmärtää vaihtoehtoisia kehityspolkuja ja niiden seurauksia eri organisaatioille ja toimijoille. Työ heijastaa poikkeuksellisen laajaa asiantuntijanäkemystä: yli 200 asiantuntijaa julkiselta ja yksityiseltä sektorilta, akatemiasta, kansainvälisistä kumppaniverkostoista sekä kansalaisyhteiskunnasta.

Kriittisimmät riskit voivat syntyä silloin, kun teknologinen riippuvuus, heikko hallinta, identiteetin mureneminen ja fyysisen sekä digitaalisen maailman integraatio keskittyvät ja kasautuvat. Kyberturvallisuuden tulevaisuus ratkaistaneen yhä enemmän riippuvuuksien, luottamuksen ja vallan rakenteissa. Kaikissa skenaarioissa tekoäly, toimitusketjut, informaatioympäristön luotettavuus ja kriittisen infrastruktuurin kytkeytyneisyys nousevat ratkaiseviksi kysymyksiksi.

Kyberturvallisuuden skenaariot tukevat varautumista, päätöksentekoa ja strategista keskustelua tilanteessa, jossa tulevaisuuden digitaalisen yhteiskunnan turvallisuus rakentuu yhä monimutkaisempien riippuvuuksien varaan.

Kyberturvallisuuden skenaariot 2035 ovat osa Suomen kyberturvallisuusstrategian toimeenpanoa. Tulevaisuuteen varautuminen ja siihen liittyvä strateginen ennakointi on myös yksi Liikenne- ja viestintäviraston strategian painopisteistä.

Kirsi Karlamaa
Teknologia- ja strategiajohtaja

TRAFICOM
Liikenne- ja viestintävirasto

Keskeiset löydökset

1. Tekoälyn kasvava integroituminen yhteiskuntaan voi muuttaa kyberturvallisuuden luonteen infrastruktuurikysymykseksi. Keskiössä ovat data, laskenta, hallintakerrokset ja agenttiekosysteemit sekä niiden kytkökset kriittisiin prosesseihin.

2. Informaatioympäristön luotettavuus on kyberturvallisuuden ytimessä kaikissa skenaarioissa.

3. Tulevaisuuden uhkatoimijat voivat olla pitkälti samoja kuin tällä hetkellä. Niiden vaikutusvalta riippuu resursseista ja kyvykkyyksistä toimia eri teknologisissa ympäristöissä.

4. Teknologioiden keskittäminen tai pirstaloituminen voivat tuottaa erilaisia riskiprofiileja.

5. 6G-, avaruus- ja kvanttiteknologiat voivat muuttaa kyberympäristön rakennetta. Ne lisäävät sekä resilienssiä että systeemisten häiriöiden riskiä.

6. Suurimmat tulevaisuuden riskit voivat syntyä epävarmuuksien keskittymisessä ja kasautuessa. Vakavimmat tilanteet voivat syntyä, kun autonomia, keskitetty infrastruktuuri, fyysisen ja digitaalisen maailman yhdentyminen, identiteetin mureneminen ja hallinnan puute kietoutuvat yhteen.

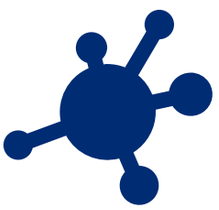
Neljä tulevaisuuden maailmaa

Tulenkantaja
Tulenkantajassa maailma on edelleen geopoliittisesti jännitteinen ja toimitusketjut ovat osin alueellistuneet. EU toimii teknologian ja kyberturvallisuuden sääntelyn sekä standardien määrittäjänä ja rakentaa demokratiaa ja yksityisyydensuojaa korostavaa "kolmatta tietä" Yhdysvaltojen ja Kiinan mallien väliin. Vahva tunnistautuminen, EU-pilvi ja sääntelynmukaiset dataratkaisut muodostavat turvallisuuden minimitason.

Tässä skenaariossa informaatioympäristön hajautumista pyritään estämään. Alustoilta vaaditaan läpinäkyvyyttä, synteettisen ja orgaanisen sisällön erottamista ja kansalaisille rakennetaan vahvan tunnistautumisen taakse todennetun tiedon ympäristöjä. Samalla mallin varjopuoli on se, että osa toimijoista kokee tämän sensuurina tai liian ohjaavana "EU-todellisuutena".

Teknologian kehitys ei pysähdy, mutta sen käyttöönotto muuttuu maltillisemmaksi. Suurten tekoälyn kielimallien ylikuumentunut hypetys on hiipunut. EU onnistuu parantamaan omavaraisuuttaan pilvessä, tekoälyssä, kvantti-, 6G- ja avaruusteknologiassa. Tämä ei poista uhkia, mutta tekee niistä hallittavampia.

Pirstaloituminen
Pirstaloitumisessa maailma ajautuu blokkeihin, toimitusketjut alueellistuvat ja EU menettää kykynsä muodostaa yhteistä digi- ja infralinjaa. Jäsenmaat jakautuvat eri leireihin, suuryritykset jarruttavat sääntelyä ja teknologinen kehitys etenee epätasaisesti. Lopputuloksena on tilkkutäkkimäinen infrastruktuuri, jossa yhteentoimivuus, hallinta ja luottamus heikkenevät.



Tämän skenaarion ytimessä on luottamuksen romahdus. Julkinen internet muuttuu synteettisen sisällön, manipulaation ja huijausten kyllästämäksi ympäristöksi, josta ihmiset ja organisaatiot vetäytyvät suljetumpiin ratkaisuihin. Eri alustoilla syntyy erilaisia totuuspohjia, ja yhteinen tiedollinen perusta haurastuu. Samalla kansalaiset alkavat vastustaa järjestelmiä myös aktiivisesti, esimerkiksi sensorien ja älyominaisuuksien myrkyttämisen kaltaisilla vastakeinoilla.

Tekoälyn käyttöönotto on tässä maailmassa ollut liian nopeaa ja liian huonosti hallittua. "AI-katastrofit" ovat johtaneet arkaluonteisten tietojen vuotoihin, manipulointiin ja takaisinmallinnukseen, minkä seurauksena luottamus datan luovuttamiseen heikkenee ja käyttöönotto hidastuu. Teknologiaa kyllä käytetään, mutta varovaisemmin, kapeammin ja epäluuloisemmin. Samalla uhkatoimijat jatkavat tekoälyn hyödyntämistä aggressiivisesti.

Epäluottamuksesta huolimatta riippuvuudet eivät vähene vaan syvenevät. Teknologiajätit ja suuret toimittajat jäävät käytännössä ainoiksi toimijoiksi, jotka pystyvät takaamaan digitaalisen jatkuvuuden, vaikka niiden valta ja hyväksyttävyys samalla murenevat.

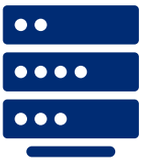
Kaksi valtakuntaa

Kaksi valtakuntaa kuvaa maailman, jossa globaali digitaalinen infrastruktuuri on jakautunut kahteen suurvaltavetoiseen blokkiin. Yhdysvallat yrittää irrottautua Kiinasta riippuvaisista toimitusketjuista, Kiina on teknologisesti erittäin vahva ja EU jää turvallisuuspoliittisesti Yhdysvaltojen teknologioiden ja valvonnan varaan. EU:n suvereeniteettihankkeet jäävät vajaiksi, vaikka turvallisuussääntely kiristyy.

Tässä tulevaisuudessa turvallisuus menee yksityisyyden edelle. Digitaalisen infrastruktuurin valvonta lisääntyy, tietosuoja heikkenee ja suuret palveluntarjoajat saavat myös valvontatehtäviä. Informaatioympäristö muuttuu ohjatuksi, suodatetuksi ja ideologisesti kontrolloiduksi. Sisäisen ja ulkoisen turvallisuuden nimissä myös toisinajattelun tila kapenee.

Teknologian logiikka on tässä maailmassa kilpavarustelun logiikka. Autonominen hyökkäys ja puolustus lyhentävät vasteajat minimiin, huoltovarmuuskriittiset toiminnot siirtyvät tekoälyohjauksen varaan, ja 6G, satelliittilaajakaistat sekä kvanttiteknologia kytkeytyvät osaksi turvallisuusarkkitehtuuria. Kyberturvallisuus on osa suurvaltapoliittista voimapeliä.

Dataimperiumit



Dataimperiumeissa globaali kasvu perustuu liikkuvuuteen, dataan ja yritysvetoiseen teknologiseen integraatioon. Suuret teknologiayritykset onnistuvat pitämään arvoketjut vakaina, lieventämään protektionismia ja säilyttämään yhteydet myös Kiinasta riippuvaiseen maailmankauppaan. Valtiot jakautuvat käytännössä yritysten etupiireihin, ja EU:n rooli muuttuu aktiivisesta sääntelijästä asiakkaaksi.

Tämän skenaarion ydin on vallansiirtymä. Julkinen sääntely ei pysy teknologisen abstraktiotason ja monimutkaisuuden perässä, joten dataimperiumit alkavat täyttää päätöksentekorakenteita, vaikuttaa politiikkaan ja tarjota myös hallinnolle omat AI-työkalunsa. Demokratian muodot säilyvät, mutta käytännön ohjaus siirtyy yhä enemmän yritysvetoisiin mustiin laatikoihin.

Kansalaisten arki rakentuu tässä maailmassa suljettujen ympäristöjen varaan. Biometrinen data toimii porttina parempiin palveluihin, kriittinen ajattelu heikentyy ja koetut todellisuudet hajautuvat tulotason ja käytetyn ekosysteemin mukaan. Yksityisyydestä tulee luksustuote: parhaan suojan saa maksamalla, ei automaattisena oikeutena.

Kyberturvallisuuden logiikka on valikoiva. Dataimperiumit suojaavat vahvimmin omat tietovarastonsa ja maksukykyiset asiakkaansa, mutta muille perustaso voi jäädä heikoksi.