



TRAFICOM

Liikenne- ja viestintävirasto

Tulevaisuuteen varautuminen

Kyberturvallisuuden skenaariot 2035

Kirsi Karlamaa

Teknologia- ja strategiajohtaja



Kyberturvallisuusstrategia osaava, innovatiivinen ja kokeileva kyberekosysteemi 2035

- ▶ Olemme käynnistäneet poikkihallinnollisen kyberturvallisuuden tulevaisuus- ja ennakointimallin.
- ▶ Tavoitteena ymmärtää uusien teknologioiden ja ilmiöiden vaikutuksia kyberturvallisuuteen.
- ▶ Käynnistynyt jatkuva työ on edellytys kyberturvallisuuden uhka-arvion laatimiselle.

”Hyödynnämme teknologiset mahdollisuudet ja ymmärrämme niihin liittyvät uhkat kybertoimintaympäristölle ja yhteiskunnalle. Kehitämme osaamista laaja-alaisesti.”

Kyberturvallisuuden muutostekijät

- ▶ Geopoliittinen kehitys
- ▶ Digitaalinen infrastruktuuri
- ▶ Tulevaisuuden kyberuhat ml. Rikollisuus
- ▶ Toimitusketjut
- ▶ EU:n yhtenäisyys ja asema
- ▶ Satelliitti- ja avaruusteknologia
- ▶ Teknologiset riippuvuudet
- ▶ Organisaatioiden varautumISRatkaisut
- ▶ Tekoälyn kehitys
- ▶ Kybersäätely
- ▶ Informaatioympäristö ja yhteiskunta
- ▶ Kvanttitekhnologia
- ▶ Teknologiajättien asema
- ▶ Osaamisen kehitys
- ▶ Haavoittuvuudet ja solmukohdat
- ▶ Standardit ja luottamus
- ▶ Disinformaatio ja hybridivaikuttaminen

"Nimeä korkeintaan kolme mielestäsi merkittävintä toimintaympäristön tekijää, ilmiötä / tapahtumaa, jotka vaikuttavat tai voivat vaikuttaa kyberturvallisuuteen vuoteen 2035 mennessä."

Geopolitiikka	Teknologia	Luottamus
Yhdysvaltojen kanssa tehtävien diilien aikakausi Kiinan kilpailukyyn pysytellessä rinnalla. Yhdysvallat säilyttänyt johtoasemansa. Venäjä tekee EU:ssa operaatioita sodankäynnin kynnyksen alapuolella.	AI:n rajattujen mallien "luomuaikakausi" . EU rakentaa digitaalista suvereniteettia ja omia pilviratkaisuja ollen kuitenkin avainteknologioissa riippuvainen Yhdysvalloista ja epäileväinen Kiinan tekemisistä.	Vahvan EU-tunnistautumisen informaatioympäristöt suojelevat kansalaisia disinformaatiolta. AI-assistentit ja informaatioympäristöt vahvistavat demokratia-maailmankuvaa.
SOIHUNKANTAJA		
Kyberympäristö		
Valtiotoimijat tiedustelevat, miinoittavat ja sabotoivat länsimaisia järjestelmiä konflikteja ennakoiden. Länsimaiden ja EU:n yhtenäisyyttä pyritään hajottamaan.	Kyberrikolliset pyrkivät pääsemään kiinni arvokkaaseen toimialadataan, jota on kerrytetty mm. EU-sisämarkkinayritysten yhteisiin datajärviin.	EU:n kytkeytyneet smart city-rajapinnat, kyberfyysiset ympäristöt sekä vahvan tunnistautumisen identiteetit kytköksineen hyökkäyskohteina.

Geopolitiikka	Teknologia	Luottamus
Kiinan ja Yhdysvaltojen geopoliittinen kamppailu lakipisteessä. EU kantaa Naton tiedusteluella kortensa kekoon Venäjän patoamisessa Baltiassa, Kiina aggressiivinen Itä-Aasiassa uhaten toimitusketjuja.	Länsimaat linnoittaneet yhteiskunnan kytkeytyneet järjestelmät AI-valvottavien, digitaalisten suojamuurien sisään, joita Big Tech-yritykset ylläpitävät vastaten puolustusviranomaisille. Kvanttikilpajuoksu.	Käyttäjien toiminnan viranomaisvalvontaa sisäisten uhkien paljastamiseksi. Arkea ohjataan voimakkaasti AI-avusteisesti ja internet on voimakkaasti sensuroitu versio. Mukautumista ja kaninamieliä.
KAKSI VALTAKUNTAA		
Kyberympäristö		
Demokratioiden ja autokratioiden tekoälymallien hyökkäys- ja puolustusagentit kamppailevat pyrkien vaikuttamaan toistensa ohjelmointiin.	Puolustusjärjestelmien iskunkestävyyden ja kytkeytymisen myötä digitaalinen turvallisuus korostuu puolustus-AI:n infrassa ja ihmiskäyttäjissä.	Huoltovarmuuskriittiset toimialat logistiikasta ruokahuoltoon ja peruspalvelut energiasta veteen yhteiskuntien kyberjärkyttämisen väyliä valtiotoimijoille.

Geopolitiikka	Teknologia	Luottamus
Moninapaisen pirstaloitumisen aika, Kiina ja Venäjä liikkuvat sisäisesti epävakaaan USA:n jättämiin valtatyhjiöihin. EU-maat jakautuvat autokratioita myötäileviin ja vastustaviin, EU menettää toimintakykynsä.	Hallitsemattoman AI-vallankumouksen myötä tietovuodot, disinformaatio ja manipulaatio ovat johtaneet demokratioiden vaikutusvallan siirtymiseen valtiotoimijoille ja yrityksille. Teknologioiden käyttöönotto vaarallista.	Internetin kuolema sisältötulvaan, digitaalisen elämän vastoinkäymiset ja uhat saavat yhdet heimoutumaan turvaan suuryritysten alustoille, toiset aktiiviseen vastarintaan teknologia-elämäntapaa vastaan.
PIRSTALOITUMINEN		
Kyberympäristö		
Autokratiat pyrkivät kaatamaan demokraattiset yhteiskunnat info-operaatioilla ja sabotaasilla ampumatta laukaustakaan. Kyberrikollisten imperiumit kasvavat valtatyhjiöissä.	Ennennäkemättömän laaja käyttäjien sensitiivisten tietojen paljastuminen AI-sovellusten kautta avaa ovet pitkälle erikoistuneille ja kohdennetuille AI-avusteisille huijauksille.	Tilkkutäkkimäiset järjestelmäratkaisut ja tuntemattomat solmukohdat vaikeuttavat jatkuvuudenhallintaa, mutta myös pahantahtoista toimintaa.

Geopolitiikka	Teknologia	Luottamus
Dataimperiumit hillitsevät poliittisesti geopoliittista vastakkainasettelua taatakseen itselleen suotuisan toimintaympäristön. Vakaa kansainvälinen tilanne takaa niille lähes rajatonta kasvua.	Dataimperiumien varaan rakentuneet superekosysteemit yhteiskuntien digitaalisen infrastruktuurin elinehtoina. Maailma jaettu niiden palveluntarjonnan ja etuihin perustuvien kiihtyvien voimien välillä.	Käyttäjät AI-muotoilluissa henkilökohtaisissa informaatiopeilisaleissa dataimperiumien massiiviseen datankeruuseen perustuvien, reaaliaikaisten Mind ² -tietovarantojen avulla avusteisesti kiihtyvien voimien äämiä.
DATAIMPERIUMIT		
Kyberympäristö		
Dataimperiumien muurit antavat turvaa maksukykyisille ja dataa luovuttaville. Kyberrikolliset vaanivat siellä, minne ne eivät ulota lonkeroitaan.	Käyttäjistä kerrytetty monipuoliset ja reaaliaikaiset tietovarannot alttiita AI-injektio- tietomurroille, mahdollistaen virtuaalisen henkilöllisyyden rikollisen kloonaamisen.	Teknologian hyötyjen kasautuminen harvoille on lisännyt sisäpiiriläisyyttä ja radikalismia teknologisen elämäntavan mahdollistajina toimivia dataimperiumeja vastaan.

Maailma vuonna 2035

Skenaariot kuvaavat vaihtoehtoisen geopoliittisen ja teknologisen muutoksen värittämää yhteiskuntaa järjestelmineen, sekä tulevaisuuden maailmoissa mahdollisesti nousevia kyberuhkia ja haavoittuvuuksia.



Toistuvat ilmiöt vastaavat kohtalonkysymyksiin

AI-kehitys 2035

Kehityskulku 1:
Rajatut sovellutus-
mahdollisuudet
korostavat laadukasta
dataa

Kehityskulku 2:
Tietoturvakatastrofi
romahduttaa
luottamuksen

Kehityskulku 3:
Hyökkäyksen ja
puolustuksen
kilpavarustelu

Kehityskulku 4:
Laaja käyttöönotto
johtaa vallan
uusjakoon

Infrastruktuuri ja toimitusketjut 2035

Kehityskulku 1:
Demokraattinen
omavaraisuus

Kehityskulku 2:
Tilkkutäkki
tuuliajolla

Kehityskulku 3:
Kyberfysiset
linnoitukset

Kehityskulku 4:
Kytkeytyminen
ylikerroksilla

Geopoliittinen kehitys 2035

Kehityskulku 1:
EU jättiläisten
välissä

Kehityskulku 2:
Moninapainen
pirstaloituminen

Kehityskulku 3:
Hegemoninen
kamppailu

Kehityskulku 4:
Suuryritysdiplomatia

Kyberuhat ja haavoittuvuudet 2035

Kehityskulku 1:
Sodan kynnyksen
alittavia operaatioita
kytkeytyneessä
Euroopassa

Kehityskulku 2:
Pirstaloituminen
paljastaa
heikkoudet

Kehityskulku 3:
Valtiotoimijat iskevät
kriittiseen
infrastruktuuriin

Kehityskulku 4:
AI-dataifikaatio johtaa
rikollisuuden
uusiin muotoihin

Tekoäly ei ole vain teknologiahanke. Se on yhteiskunnallinen valinta, joka määrittää, kuinka haavoittuvia tai kestäviä olemme vuonna 2030.

"Yksi virhe – koko yhteiskunta sekaisin."

Keskittymisriski. Yksi virhe tai häiriö leviää useille sektoreille samanaikaisesti.

"Kone tekee oikein – mutta väärää asiaa."

Tekoälyagentit saavat yhä enemmän oikeuksia: ne tilaavat palveluja, muuttavat asetuksia ja tekevät päätöksiä.

"Totuus hajoaa – kehen voi enää luottaa?"

Deepfaket, tekoälyllä tuotettu sisältö ja uskottavat huijausviestit murentavat perinteiset luottamuksen mekanismit.

6G-teknologian suurin uhka ei ole yksittäinen hyökkäys – vaan se, ettemme enää näe kokonaisuutta.

"Hyökkäys ei riko yhteyttä – se muuttaa todellisuutta."

Sensorit, paikannus ja digitaaliset kaksoset ovat osa verkkoa. Kyse ei ole enää vain datasta, vaan ympäristön tulkinnasta.

"Yksi haavoittuvuus ei kaada verkkoa – se kaataa ekosysteemin."

6G on järjestelmien järjestelmä, haavoittuvuudet kasaantuvat. Pilvi, satelliitit, ohjelmistot ja tekoäly ovat kaikki riippuvaisia toisistaan.

"Miljoonien porttien hyökkäys."

6G yhdistää valtavan määrän laitteita ja IoT-sensoreita, lisäten hyökkäyspintaa.



Kilpailu teknologiasta, datasta ja infrastruktuurin hallinnasta määrittää valtioiden vaikutusvaltaa, taloudellista autonomiaa ja yhteiskunnallista vakautta.



Kvanttiuhkaan varautuminen on pitkän aikavälin turvallisuuspäätös.

- *"Kun dataa keskitetään, siitä tulee strateginen maali."*
- *"Kuka hallitsee pilveä, hallitsee toimintakykyä."*
- *"Tieto voidaan varastaa tänään ja murtaa huomenna."*
 - *"Emme suojautuneet ajoissa kvanttikestävillä ratkaisuilla ilman pakkoa."*
- *"Valtiollinen kybertoiminta – epävarmuuden strategia."*
- *"Vaikuttaminen ei kohdistu valtioihin – vaan ihmisiin."*



***Tämän päivän valinnat ja
strategiset toimet
vaikuttavat
tulevaisuuteemme.
Voimme vaikuttaa
epävarmuuksiin ja
kohtalonkysymyksiimme
itse.***

Kiitos!

