Tietopolitiikan ja tekoälyn selonteko, taustapaperi

Turvallisuus jatkuvuudenhallinnan takeena

PLM, SM, UM

Toim. Aulikki Pakanen

15.6.2018

Turvallisuus: tila, jossa uhkat ja riskit ovat hallittavissa

Jatkuvuudenhallinta: huoltovarmuutta parantava organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle

> Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla.
> Jatkuvuudenhallinnan painopiste on *normaaliolojen* häiriöissä, mutta prosessiin voi sisältyä myös *poikkeusoloihin varautumista*.
> Jatkuvuudenhallinta on yleensä omaehtoista toimintaa, mutta joillakin aloilla organisaatiot ovat myös lailla velvoitettuja varmistamaan toimintansa jatkuvuuden eri olosuhteissa.
> Jatkuvuudenhallinnan käsite on peräisin elinkeinoelämästä, mutta se on yleistymässä myös muiden organisaatioiden toiminnassa.

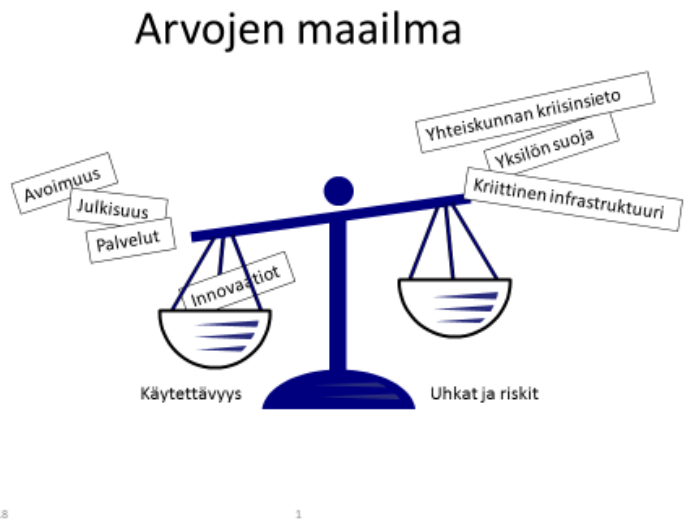
(Kokonaisturvallisuuden sanasto, 2. laitos, 2017)

Sisällys

1. Yhteenveto/keskeiset teesit

1) Mahdollisuuksien ja uhkien, avoimuuden ja turvallisuuden tasapainon hakeminen muuttuvassa toimintaympäristössä
2) Turvallisuuskriittisen tiedon tunnistaminen ja riskien arviointi
3) Valmiuden ja varautumisen huomioiminen osaamisessa
4) Tiedon luovuttamisen hallinta

2. Tietopolitiikka – mahdollisuuksien ja uhkien, avoimuuden ja turvallisuuden tasapainon hakeminen muuttuvassa toimintaympäristössä



Kuva 1. Turvallisuus arvojen maailman mahdollistajana.

2.1. Tulevaisuuden digitaalinen toimintaympäristö kokonaisturvallisuuden näkökulmasta

Digitaalinen maailma ja yhteiskunta on kokonaisturvallisuuden näkökulmasta monia tutkimuskysymyksiä herättävä ja yhteiskunnalle haasteita mutta myös mahdollisuuksia tarjoava ilmiö. Keskeisiä teemoja:

- Tiedon eheys ja keinot tiedon eheyden takaamiseksi.
- Jatkuvuuden turvaaminen: digitaalisen tiedon tallentaminen/varmentaminen häiriötilanteita varten - yhteiskunnan toiminta ja kansalaisten kriisinsietoa nostaa varmuus siitä, että viranomais- ja yksityisen sektorin palvelut toimivat.

- Käytössä olevan tiedon fyysinen paikka ja alkuperän luotettavuus sekä tiedon avoimuus/julkisuus ja saatavuus. Tiedon julkistamisen ja avoimen tiedon lisäarvo - kenelle on lisäarvoa eri tiedon julkistamisesta/tarvitseeko kaikkien tietää kaikkea.
- Sensorifuusio ja verkossa jatkuvasti kiinni olevat sensorit/laitteet mahdollistavat tiedon keräämisen 24/7. Jatkuvan sensoroinnin tuottama tieto saattaa muodostua arvokkaaksi/ongelmalliseksi ja mahdollistaa esim. yllättävän ja kohtuullisen laajamittaisen ei helposti ”uhkaksi” havaittavan infran häirinnän.
- Tiedon yhdistämisen mukanaan tuoma kokonaisuuden hallinta/arviointi sen osalta, että muodostaako kokonaisuus uhan tai isoja riskejä kansalliselle turvallisuudelle: riskiarvioit - mikä on hyväksyttävä riskitaso.
- Tulee varautua siihen, että Suomeen kohdistuva vihamielinen hybridivaikuttaminen lisääntyy. Kyber ja informaatio-operaatiot ovat tällä hetkellä eniten käytetyt keinot vihamielisessä hybridivaikuttamisessa.
- Positiivisen avoimen tiedon käyttö eli turvallisuustoimijoiden kannalta olennaisen kriittisen tiedon lisäksi luotettavan tiedon ja luotettavien tietolähteiden kautta tulleen tiedon analysointi tiedon hyödynnettävyyden ja jaettavuuden kehittämiseksi turvallisuustoimijoiden kesken.
- Tiedon louhinnan, lohkoketjujen ym. hyödyntäminen merkitsee sähkönkulutuksen kasvua, millä on vaikutuksia ja riippuvuuksia yli Suomen rajojen. Merkitsee myös ympäristökysymysten esille nousua.

2.2. Kyberiä ja tekoälyä koskevia ulko- ja turvallisuuspoliittisia näkökohtia hallituksen tieto- ja tekoälypolitiikkaa koskevaan selontekoon

Elämme tällä hetkellä kybertoimintaympäristössä eli maailmassa, joka pohjautuu yhteiskuntiemme vahvaan digitalisoituneisuuteen. Siirtyessämme kybertoimintaympäristön maailmasta kohti yhä vahvempaa tekoälyyn pohjautuvaa yhteiskuntaa, tulee tässä muutosprosessissa kiinnittää huomiota myös ulko-, turvallisuus-, ja puolustuspoliittisiin näkökohtiin.

Tämän hetken kybermaailmassa teknisen turvallisuuden lisäämiseen tähtäävät toimet ovat oleellisia sietokyvyn (resilienssi) kasvattamisessa niin kansallisesti kuin kansainvälisesti. Samalla tarvitaan laajaa monitoimija-yhteistyötä.

Kansainvälinen yhteisö on vasta hiljattain havahtunut panostamaan strategiseen, poliittisen tason yhteistyöhön pelisääntöjen luomiseksi kybertoimintaympäristöön eli kyberdiplomatiaan. Kansainvälisen yhteistyön tavoitteena on vastuullisen valtiokäyttäytymisen edistäminen. Tämän avulla pyritään universaalin, vapaan ja vakaan internetin säilyttämiseen, mikä puolestaan edesauttaa takaamaan yhteiskuntiemme taloudellisen ja sosiaalisen hyvinvoinnin sekä vahvistamaan turvallisuutta. Siksi kybermaailman ulko-, turvallisuus- ja puolustuspoliittisten näkökohtien tarkastelu on keskeistä. Kyberulottuvuudella on vaikutusta niin kansainväliseen oikeuteen ml. ihmisoikeuksiin, kehityskysymyksiin, luottamusta lisäävien toimien toimeenpanoon, kyber-rikollisuuden säätelyyn, internetin hallintaan kuin kyberpuolustukseenkin. Myös tässä työssä valtioiden yhteistyö ja jatkuva vuoropuhelu yritysmaailman, tutkimusmaailman ja kansalaisjärjestöjen kesken on kestävän politiikan pohja.

Tekoälyn aikakausi voidaan nähdä kybermaailmaa seuraavana vaiheena. Teknisen kyberturvallisuuden varmistaminen tulee yhä olemaan avainasemassa ja kansainvälistä yhteistyötä tällä sektorilla tarvitaan. Taloudellisten ja yhteiskunnallisten ulottuvuuksien ohella tekoälyn vaikutuksia on syytä alkaa pohtia myös ulko-, turvallisuus-, ja puolustuspolitiikan kannalta – aivan kuten on tehty jo kyber-kysymyksissä. Kansainvälinen oikeus, kehityskysymykset, kyberpuolustus ja muut jo edellä kuvatut ulkopolitiikan sektorit tulevat osin uuteen valoon uusien teknologioiden käytön myötä.

EU:n lisäksi kaikki keskeiset kansainväliset järjestöt – niin mm. YK, ETYJ, Nato, OECD, Euroopan Neuvosto - ja myös muut alueelliset järjestöt, tarkastelevat tällä hetkellä kyberkysymyksiä omien mandaattiensa puitteissa. Myös maiden kahdenvälisissä suhteissa teemat nousevat esiin. Jo nyt on nähtävissä, että keinoälyyn liittyvät kysymykset ovat tulossa vahvasti mukaan keskusteluun kaikilla näillä foorumilla.

Kysymyksiä, joita tekoälykeskustelussa nostetaan esiin, on moninaisia, Näitä ovat esimerkiksi: kuinka tekoäly vaikuttaa kansainvälisen oikeuden eri osa-alueisiin; kuinka yksityisyyden suoja, inhimillinen kohtelu, koulutus ja sen laatu, pääsy informaatioon, sananvapaus ja etiikkakysymykset otetaan huomioon ihmisoikeuksissa; millä tavoin kehityskysymyksissä otetaan huomioon globaali vastuu ja millä tavoin lisätään kehitysmaiden mahdollisuuksia käyttää hyväksi tekoälyä ja siihen liittyvien teknologioiden mukanaan tuomia mahdollisuuksia ja estetään digitaalisen kuilun syveneminen; mitä näkökohtia tulee ottaa huomioon autonomisten aseiden käytössä konfliktitilanteessa; miten mahdollinen päätöksenteon delegoiminen tekoäly-pohjaisille ratkaisuille vaikuttaisi esimerkiksi konflikti-/sotatilanteissa; tai minkälaisten moraalikäsitysten ja arvojen pohjalta tekoälyyn pohjautuvaa teknologiaa ja laitteita kehitetään ja miten niitä käytetään jne.

Kaiken kansainvälisen työn taustalla on valtioiden ja muiden keskeisten toimijoiden välisen luottamuksen lisääminen. Siihen tähtää niin perinteinen ulkopolitiikka, siihen tähtää parhaillaan kyberaikakauden politiikka ja siihen pohjaa tekoälyaikakauden yhteistyö. Koska internetin aikakaudella ja kybertoimintaympäristössäkin kansainvälinen yhteisö on herännyt pelisääntöjen luomiseen hyvin myöhään, nyt on mahdollisuus olla ajan tasalla ja tarttua uusiin haasteisiin jo nyt, eli tekoälyn ja siihen liittyvien teknologioiden vasta kehittyessä.

Suomi voi olla pro-aktiivinen tämän agendan edistämisessä. Toimimalla näkyvästi kansainvälisillä foorumeilla Suomen intressejä ja tavoitteita ajaen, voimme olla vaikuttamassa kansainvälisesti sekä kybertoimintaympäristön kuin myös nyt mukaan tulevan tekoäly-aikakauden ulko-, turvallisuus- ja puolustuspoliittisiin linjauksiin.

2.3. Hybridiuhat

- Hybridivaikuttaminen länsimaita kohtaan on lisääntynyt: vaalivaikuttaminen, kyberhyökkäykset, tiedon varastaminen ja informaatiovaikuttaminen
- Länsimaat eivät ole olleet varautuneita hybridiuhkiin

- Varautumisen parantaminen on keskeinen teema kansainvälisessä yhteistyössä
- Hybridivaikuttamisessa yhdistellään tavanomaisia ja epätavanomaisia keinoja, mikä edellyttää koko yhteiskunnan toimijoita kattavaa varautumista ja koordinoitua vastinetta
- Resilienssiin Suomessa vaikuttaa kokonaisturvallisuuden malli ja sitä kautta tuleva viranomaisyhteistyö, myös medialukutaidolla on suuri merkitys
- Meidän on syytä parantaa kykyjämme ymmärtää, havaita, kestää ja torjua meihin kohdistuvaa hybridivaikuttamista - alkaen siis medialukutaidosta, jne.

3. Turvallisuuskriittisen tiedon tunnistaminen

Selontekotyössä on noussut esille tiedon merkitys liiketoiminnalle ja yksilölle. Entä tiedon yhteiskunnallinen merkitys, erityisesti kriittisen tiedon tunnistaminen?

- Kokonaisturvallisuuden kannalta tiedon vaihto on arvo sinänsä – onnistunut, oikea-aikainen tiedon jakaminen edistää turvallisuutta.
- Tiedon merkitys turvallisuusviranomaisille = yhteiskunta toimii, kansalainen hyötyy.
- Tunnistettava yhteiskunnan toiminnan kannalta kriittinen tieto. Kriittinen infrastruktuuri ja henkilöt on jo tunnistettu.
- Kansallisen turvallisuuden kannalta haaste, jos tieto leviää ulkopuolisille.
- Yhteiskunta ei voi taata yksilön turvaa, jos kaikki tieto on avointa tai leviää tahoille, joille se ei kuulu.
- Yhteiskunta ei voi taata yksilön turvaa, jos kriittinen tieto ei ole käytettävissä

	MyData	Avoin data	Kriittinen data/tieto
Käyttö	tiedon omistajan valittavissa	vapaata kaikille	hallittua
Uudelleen käyttö	tiedon omistajan valittavissa	vapaata kaikille	hallittua
Jakaminen	tiedon omistajan valittavissa	vapaata kaikille	hallittua

Kuva 2: MyDatan, avoimen datan ja kriittisen datan/tiedon vertailua

Ydinkysymys on, miten kriittinen tieto tunnistetaan? Kenen tehtävä on tunnistaa kriittinen tieto? Tiedon tuottajan ja omistajan vastuu? Kriittisen tiedon saatavuus ja tähän tietoon pohjautuva toiminnan jatkuvuuden hallinta tulee varmistaa.

Kuva 3. Datan jalostaminen ymmärrykseksi yhdistettynä julkinen-kriittinen –aspektiin.

Julkisuuslain määritelmä salassa pidettävästä tiedosta ei riitä kattamaan digitaalisen toimintaympäristön ominaisuuksia ja mahdollisuuksia datan käsittelylle. Tietopoliittiseen keskusteluun tulee nostaa vahvemmin esille kriittinen data – data, joka ei (vielä) ole salassa pidettävää mutta on kriittistä sellaisenaan tai yhdistettynä muuhun dataan kansallisen turvallisuuden tai kokonaisturvallisuuden kannalta.

Open Knowledge Finland on lanseerannut sloganin: ”Suomi = paras paikka henkilötietoon liittyvien innovaatioiden kehittämiseen”.

Mikä voisi olla turvallisuustoimijoiden slogan? ”Suomi = turvallisin paikka kriittisen tiedon hallintaan” …?

Suomi turvaa tiedot = turvaa tiedosta. Turvallisesti avoin Suomi.

3.1. Näkemyksiä kriittisestä informaatiosta ja sen suojasta

Julkisyhteisön data on periaatteessa julkista ja se laitetaan kaikkien saataville, ellei sen omistaja ole sitä tietosuojalain mukaisesti ei-julkiseksi luokitellut. Samoin voivat yritykset ja yhteisöt julkistaa omistuksessaan olevaa dataa oman harkintansa mukaan. Tämä voi aiheuttaa valtakunnan turvallisuutta uhkaavan tai heikentävän lopputuloksen, vaikka yksittäinen tieto ei välttämättä edes tarvitse sen luonteesta johtuen suojausta. Kokonaisuus voi kuitenkin olla valtion kriittisen infrastruktuurin tai toiminnan turvallisuutta vaarantavaa. Ajatellaan logistiikkajärjestelmää. Julkisen liikenteen reaaliaikainen paikkatieto on laajalti saatavilla niin junaliikenteen kuin bussiliikenteenkin osalta. Sen seuraaminen antaa jokseenkin hyvän tilannekuvan jatkuvasti ihmisten liikkuvuudesta ja keskimääräisistä sijainneista vaikkapa tietyissä kriittisissä kohdissa, mikäli niin halutaan tehdä. Joihinkin palveluihin liittyy myös ajo-olosuhdetietojen välityspalvelu. Monilla kuljetusliikkeillä on toimitusten seuraamissovelluksia. Tiedossani ei ole, onko julkisesti saatavilla geneeristä sovellusta, jolla voi seurata palveluntarjoajan kapasiteetin sijaintia ja suorituskykyä. Joka tapauksessa kriittinen liike on ainakin osittain seurattavissa julkisiin lähteisiin

perustuen. (Tätä voi tutkia laajemminkin.) Rakennuskanta (osin tarkkoine sisäkuvineen) ja muu fyysinen infrastruktuuri on suurelta osin julkisesti saatavilla. Televerkkojen kattavuus ja tukiasemien sijainnit ovat saatavilla. Moni muu kriittiseen infrastruktuuriin liittyvä data on julkisesti saatavilla. Kun näitä kaikkia tietoja yhdistelee ja analysoi, saa varsin mainion kuvan yhteiskunnan erilaisten kriittisten toimintojen toimivuudesta sekä kokonaistoiminnan kannalta keskeisten solmukohtien haavoittuvuudesta. Asiantila on faktisesti tämä eikä ole näköpiirissä, että tiedon julkaiseminen mitenkään vähenisi ajan saatossa. Pikemminkin päinvastoin, sillä se mahdollista erialisten palveluiden ja toiminnallisuuksien helpomman saavutettavuuden ja luo uusia liiketoimintamahdollisuuksia sekä myös aidosti säästää rahaa ja aikaa. Ilmiö kokonaisuudessaan on uusi. Turvallisuuskysymyksen siitä tekee abstraktiotason nousu. Datajyvä itsessään saattaa olla merkityksetön (bussi 86 pysähtyy Herttoniemen pysäkillä kuuden minuutin kuluttua), mutta yhdistettynä kaupungin kokonaislogistiikkajärjestelmän toiminnallisuuteen eri aikoina ja analysoimalla sen toimivuudessa ilmenevät anomaliat, voidaan päätellä jo vallan muuta. Julkisesta datasta nousee kokonaisuuksia analysoimalla esiin toiminnallisia ominaispiirteitä, joiden muutoksista voidaan päätellä kaupungissa mahdollisesti muutoin tapahtuvia asioita. (Lisää tutkittavaa löytyy tästä.) Erittäin herättävä tutkimus on VTT:n ja MPKK:n VNK:lle vuonna 2017 yhdessä tekemä esitys siitä, mitä Hannu-Tapani-myrsky aiheutti Hankoniemellä ja mitkä olivat kriittisen infrastruktuurin toipumisajat. Tulos ei sinänsä ole tässä oleellinen vaan se, että pääosa tiedosta on saatu julkisista ja avoimista lähteistä. (VNK selvitys- ja tutkimustoiminnan julkaisusarja 19/2017 ”Kriittisen infrastruktuurin tilannetietoisuus”.

Digitaalisessa maailmassa sijaitsevan informaation paikkatieto (siis tieto, joka kertoo sijainnin ja informaation ominaisuudet) on varsin usein sijainnin osalta epämääräinen tai tuntematon. Tämä koskee sen käyttöä ja siirtoa. Suurimman osan tiedosta digitaalisella sijainnilla ei ole merkitystä. Kun kyseessä on kokonaisturvallisuuden kannalta merkittävä tieto tai kokonaisturvallisuuteen yhdessä vaikuttavien tietojen yhteisvaikutus (ks. edellinen kohta), tulee digitaalisessa maailmassa olevan informaation paikkatiedosta merkittävää. GDPR normittaa yksilön suojan statuksen EU:n alueella. Hallussani ei ole tietoa siitä, onko näitä asioita perusteellisesti selvitetty nimenomaan kansallisen turvallisuuden näkökulmasta. Erityisen kiinnostava selvitettävä asia on nimenomaan tuo toisen asteen tai yleensä yhdistellyn ei-turvakriittisen tiedon paikkatiedon epämääräisyydestä ja oman kontrollin ulkopuolella olevan informaation paikkatiedon epämääräisyydestä esiin ponnistava turvallisuusuhka yhteiskunnan kriittisille toiminnoille.

Kolmas tässä esiin nostettava ilmiö on erilaisten sähköisten päätelaitteiden ominaisuudet toimia monipuolisina sensoreina. Usein ja lähtökohtaisesti aina, ellei käyttäjällä ole ollut mahdollisuutta sensoritoimintoja poistaa (toisinaan ei edes ole) nuo laitteet välittävät paikkatietoa (siis tietoa sijainnistaan sekä sensorien havaitsemista ominaisuuksista) vähintään palveluntarjoajalle. Aina käyttäjä ei edes tiedä, mitä tietoa välitetään ja minne se palveluntarjoajalta menee edelleen. Ihmiset kuljettavat pääsääntöisesti mukanaan vähintään yhtä sensorijärjestelmää, usein useita. Kotona on lisää kahvinkeittimestä ja leivänpaahtimesta lähtien. Usein näissä ei ole minkäänlaista tietoturvaa. Saatavilla on siten määrätön määrä dataa, josta on mahdollista tehdä kokonaisuutta, sen toiminnallisuuksia ja kriittisiä kohtia koskevaa analyysiä. Tämä kaikki tiedon keruu tapahtuu (jos on tapahtuakseen) periaatteessa ihan lainsäädännön puitteissa. Haastavin kohta on saada oleellinen data yhtä aikaa ja yhteen pisteeseen analysoitavaksi.

En käsitellyt tekoälyä tai tietoturvaa tai kvanttilaskentaa tai mitään muutakaan keskusteluun noussutta asiaa lainkaan. Ne ovat olemassa ja vaikuttavat teknologioina informaation hankintaan, käsittelyyn, siirtoon

ja käyttöön. Jätin myös luottamuksen tai sen puuttumisen pois. Se on aivan oleellinen joko mahdollistajana tai pelin pysäyttäjänä, kun kriittistä informaatiota suojataan.

Joten elämme siis tuollaisessa maailmassa. On vain mutusteltava mitä se tarkoittaa valtioturvallisuuden ja kokonaismaanpuolustuksen kannalta ja mitä se tarkoittaa Puolustusvoimien ja muiden turvallisuusviranomaisten tehtävien toteuttamiselle. Lienee tarkasteltava kriittisesti resurssien priorisointiperiaatteita ja toimivaltuuksien reunaehtoja. Kun verrataan tällaista toimintaympäristöä Lakiin Puolustusvoimista, johtanee se pohdintaan ainakin siitä, miten tuota lakia pitää tulkita uudessa ympäristössä.

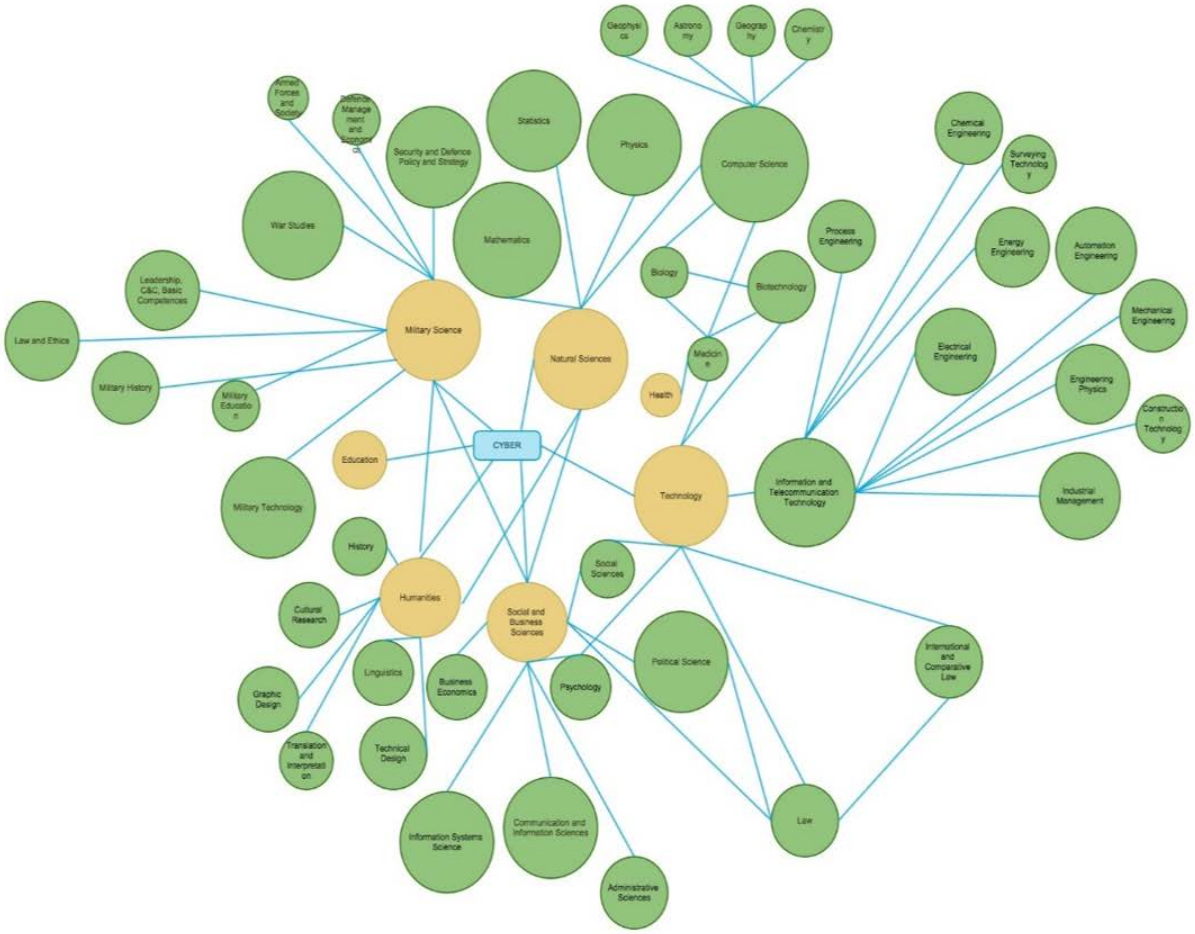
4. Osaaminen – valmiuden ja varautumisen huomioiminen

Selontekotyössä ovat nousseet esille osaamiseen liittyen kilpailukyky, syrjäytyminen ja jatkuva osaamisen kehittäminen. Tärkeitä teemoja kaikki.

Turvallisuustoimijoiden näkökulmasta katsottuna tietoon liittyvä kansallinen osaaminen tulee varmistaa, erityisesti varautumisen ja valmiuden näkökulmat:

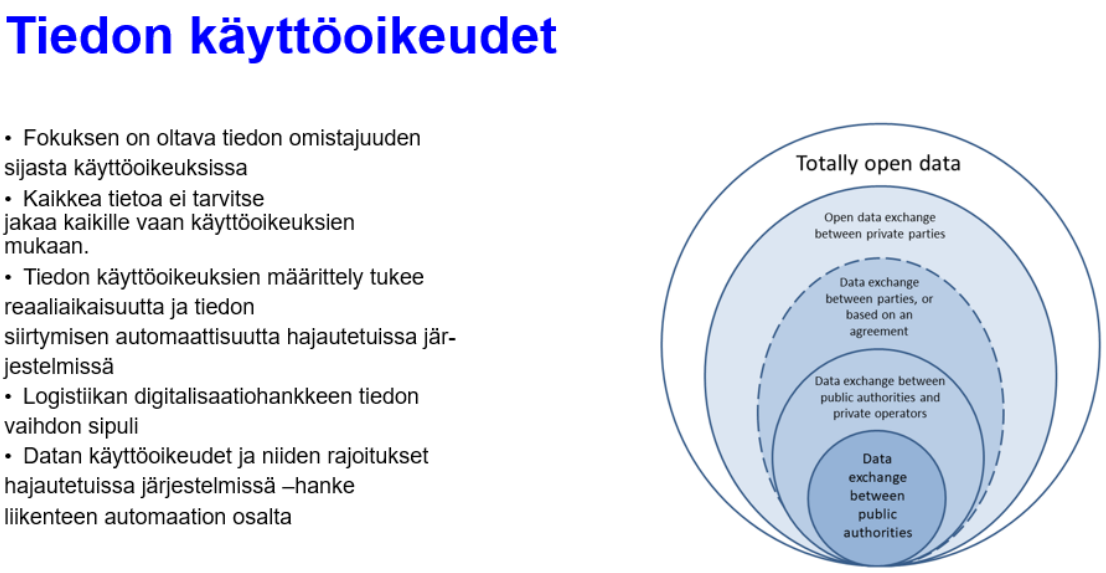
- Mitkä ovat tietoon liittyvät kriittiset suorituskyvyt (tiedonhallinta, käyttäjien tunnistaminen…) ja mistä suorituskyky koostuu, kriittisen infrastruktuurin varautumisen vaatimukset.
- Kansallisen yrityskentän, osaamisen ja tutkimuksen tämän hetkinen tilanne.
- Ketkä ovat keskeisiä toimijoita.
- Kumppanuudet vs. viranomaisten oma toiminta.
- Kansainvälisen yhteistyön arviointi.

Minkälainen kuva muodostuu tietopolitiikasta ja siihen kytkeytyvistä tieteenaloista? Minkälaista osaamista ja toimintamalleja tarvitsemme jatkossa pärjätäksemme valtiona ja yhteiskuntana?



Kuva 4. Puolustusvoimien tutkimuslaitoksen informaatiotekniikkaosaston esitys kyberiin liittyvistä tieteenaloista. Tärkeämpää kuin nähdä jokaisen pallukan teksti, on ymmärtää, kuinka monitieteisestä ja verkottuneesta asiasta on kysymys.

5. Tiedon luovuttamisen hallinta



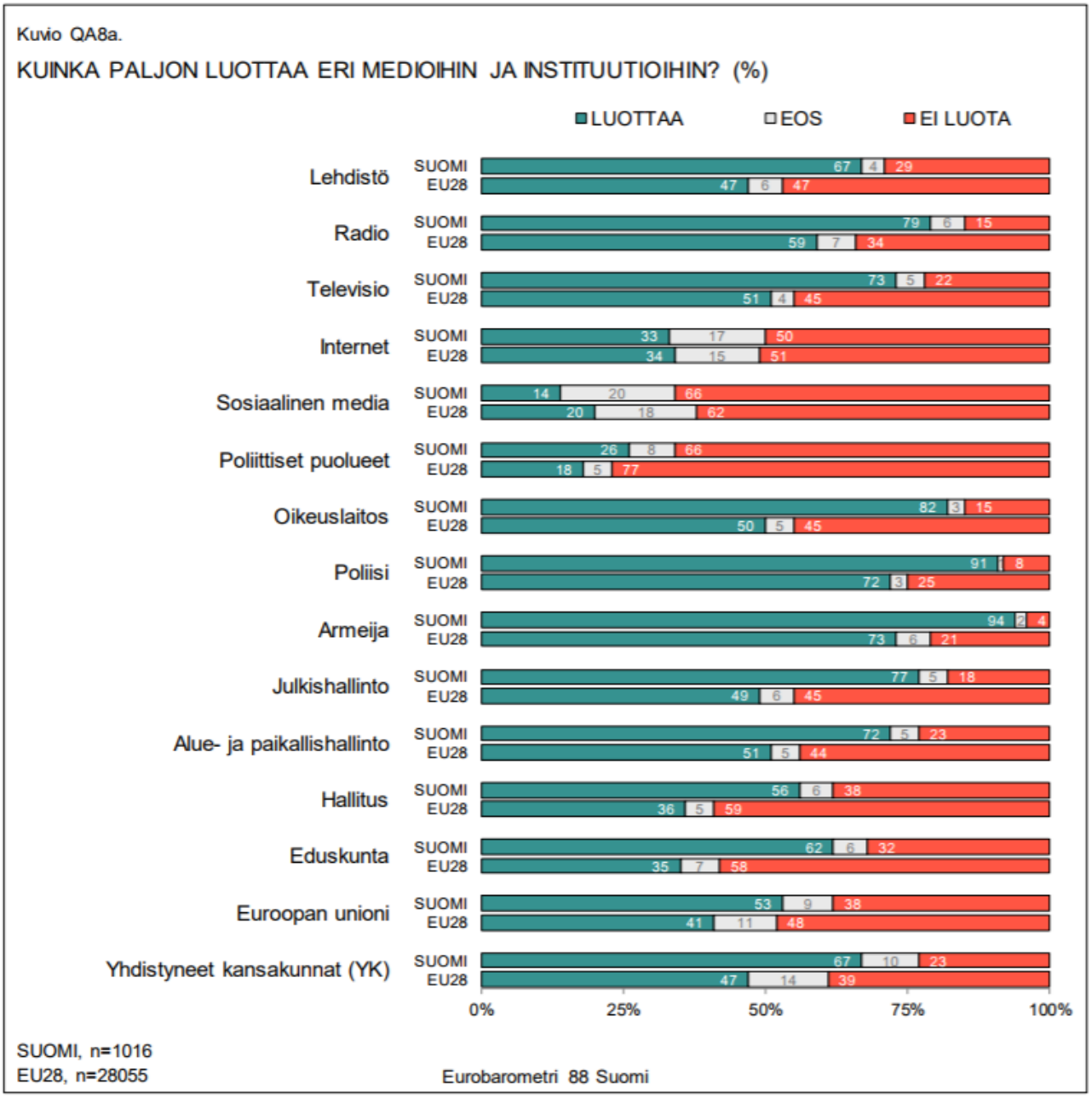
Kuva 5: Tiedon jakamisen sipulimalli (LVM)

Käyttöoikeuksilla tapahtuva tiedon hallintamalli on ideaalinen, mutta siihen liittyy merkittäviä tietosuojaan ja tietoturvaan liittyviä riskejä, joita ei tekniikan avulla voida täysin hallita. Erityissuojattava tieto on edelleen järkevintä erottaa erillisiin ympäristöihin.

Pitäisikö kriittinen tieto käsitteellisesti jakaa kahteen osaan, jossa osa tiedosta voi olla saatavissa internet-yhteyden kautta, mutta edellyttää lupaa ja vahvaa tunnistamista. Toinen osa on se viranomaistieto, joka on korkeammalla suojaustasolla (erityissuojattava). Pitäisikö lisäksi siis olla käytettävissä käsite ”jakelurajoite” vrt. unclassified.

6. Etiikka ja luottamus

Luottamuksella on merkitystä taloudelle. Näkyvin tai suurin ilmentymä epäluottamuksesta lienee Venäjän pyrkimys rakentaa kansallinen riippumaton internet, RuNet (Russian Internet). Venäjän viestintäministeriön mukaan internetin venäläinen osa irrotetaan globaalista verkosta venäläisen ”kriittisen infrastruktuurin suojaamiseksi”. Tämä pyrkimys on hyvin erilainen kuin maailmanlaajuinen tavoite luoda ”avoin ja turvallinen” sekä luottamukseen perustuva internet. Läntisessä ajattelussa keskitytään turvaamaan tiedon ja datan vapaa liikkuvuus, joka perustuu avoimeen globaaliin verkkoon. Tässä kybertilassa perinteinen valtiollinen suvereniteetti on lähes mahdoton ajatus. Avoin internet perustuu laajalla kansainvälisellä yhteistyöllä saavutettavaan avoimeen kybertilaan, jossa toimijoiden turvallisuudesta huolehtii jokainen itse suojaamalla omat järjestelmänsä. Venäjällä asia nähdään lähes päinvastoin. (Lähde: Puolustustutkimuksen vuosikirja 2018)



Kuva 6: Luottamus viranomaisten toimintaan on korkealla, Euroopan Komission tilaama ”Kansalaismielipide Euroopan unionissa, Suomi syksy 2017”

Mikä on tietopolitiikan merkitys luottamukselle? Voidaanko tietopolitiikalla lujittaa/vähentää luottamusta?

Avoimuus pääsääntöisesti lisää luottamusta, mutta hallinnon avoimuus huonosti hoidettuna voi merkitä luottamuksen menettämistä.

Miten käy perinteisten instituutioiden nauttiman luottamuksen silloin kun luotettavuus perustuu yksilöiden antamaan arviointiin verkossa? Esimerkkinä Airbnb. Sen tarjoamien majoituspalveluiden laatu ei perustu viranomaisten laatimaan luokitusjärjestelmään ja tarkastuskäynteihin vaan Airbnb:n asiakkaiden reaaliaikaisiin arviointeihin. Millä keinoin viranomaiset pysyvät luotetuimpien instituutioiden joukossa Suomessa?

Luottamuksen ja turvallisuuden suhde

- Hyvä kontrollijärjestelmä saa aikaan luottamusta
- Turvallisuus astuu esiin silloin kun luottamus loppuu
- Oikein säilytettyyn tietoon luotetaan → lisää turvallisuutta
    - Kohut ja kansalaismielipide salassa pidettävän tiedon paljastumisesta? Esimerkkinä Viestikoelaitokseen liittyvä artikkeli HS:ssa joulukuussa 2017.

Yksilön ja yhteiskunnan tietosuojasta

- Tiedon eheys on merkittävää sekä yksilölle että yhteiskunnalle
- Viranomaisten intressit johtavat myös yksilön intresseihin
- Digitaalisessa maailmassa on samat tavoitteet kuin fyysisessäkin ympäristössä – kansalaisen suojaaminen

7. Tekoäly

Yhteiskunnan elintärkeiden toimintojen, erityisesti kriittisen infrastruktuurin ratkaisujen turvaaminen tekoälyn avulla.

Tekoälyn hyödyntäminen hybridianalyysin apuna.

Tekoäly pitäisi suunnata myönteisiin asioihin ja tavoitteisiin. Samalla on syytä todeta, että tekoäly on asia, joka luultavammin antaa uusia keinoja niille tahoille, ketkä tekevät vihamielistä hybridivaikuttamista.

Erityisenä tutkimuskysymyksenä puolustushallinnossa on koneautonomian soveltamisen vastuukysymykset asejärjestelmäsovelluksissa, kontekstina kansainvälinen humanitäärinen lainsäädäntö (ns. sodan lait).