EDUSKUNNAN HALLINTOVALIOKUNNALLE

VALTIONEUVOSTON PAIKKATIETOPOLIITTINEN SELONTEKO: PAIKKATIETO JA AVOIN DATA; TURVALLISUUSRISKIT

ASIANTUNTIJALAUSUNTO

PROF MARTTI LEHTO

3.10.2018

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

Asia: VNS 2/2018 vp Valtioneuvoston paikkatietopoliittinen selonteko

1. Johdanto

Tämä lausunto käsittelee Valtioneuvoston paikkatietopoliittista selontekoa erityisesti paikkatiedon ja avoimen data turvallisuusriskien näkökulmasta.

Tulevaisuuden palvelut perustuvat ihmisten, tiedollisten toimijoiden ja älykkäiden koneiden ekosysteemin. Kehittyvässä digitaalisessa yhteiskunnassa mahdollisuuksien tila laajenee. Tilaa laajentavat kyberfyysiset toisiinsa kytkeytyneet järjestelmät, vuorovaikutteisuus, itse tuottaminen ja jakaminen, sekä koneiden älykkyyden ja kyvykkyyden kasvu. Digitaalitalouden kehitystä edistävät kansalaisten identiteetin ja tietokäytäntöjen siirtyminen verkkoon sekä organisaatioiden palvelurakenteiden digitalisaatio. Näin muodostuu digitaalinen alustatalous, jossa elementteinä ovat teollinen internet (Internet of Things, IoT), erilaiset sosiaalisen median ja viestinnän alustat sekä hajautettu ja kollaboratiivinen peer-to-peer -palvelu. Digiyhteiskunta on muuttumassa hybridiyhteiskunnaksi, jossa ihmiset, koneet ja palvelut muodostavat yhteen sulautuneen kyberfyysisen maailman. Digiyhteiskunnassa kaikki alustat ja palvelut perustuvat tai käyttävät hyväkseen paikkatietoa. Digitalisaatiossa onkin kyse yhteiskunnallisesta prosessista, jossa hyödynnetään teknologisen kehityksen uusia mahdollisuuksia.

Digitalisaation on aiheuttanut suuria muutoksia lähes kaikilla liiketoimialoilla. Digitalisaatio on muuttanut perustavalla tavalla useiden yritysten toimintamallit logistiikka- ja arvoketjujen hallinnasta markkinointiin. Digitaalinen murros perustuu ihmisten muuttuneisiin odotuksiin, yhteiskunnan palvelurakenteiden ja -tuotannon kasvaneisiin tehokkuusvaatimuksiin ja teknologioiden tarjoamiin mahdollisuuksiin. Uudet teknologiat, työkalut ja toimintatavat muuttavat ihmisten tapaa toimia arjessa ja työssä, organisaatioiden tapaa toteuttaa tehtäviään ja julkishallinnon tapaa tuottaa palveluita.

Digitaalitalouden kehitystä edistävät kansalaisten identiteetin ja tietokäytäntöjen siirtyminen verkkoon sekä organisaatioiden palvelurakenteiden digitalisaatio yhdistettynä luottamukseen systeemin turvallisuudesta. Globaalissa kehityksessä korostuu suurien palvelutarjoajien kasvu ja markkinoiden hallinta.

Globaali kilpailu pakottaa yritykset tehostamaan toimintaansa ja organisoimaan liiketoimintamallinsa kokonaan uudelleen. Parhaimmillaan digitalisaatio uudistaa kokonaisia toimialoja muuttaen radikaalisti liiketoiminnan arvoketjuja ja ekosysteemeitä. Digitaalisista palvelualustoista tulee globaaleja, kuten olemme nähneet liikenteessä (Uber), hotellialalla (Airbnb), viihdeteollisuudessa (Netflix, Spotify) ja e-kirjaliiketoiminnassa (Amazon).

2. Digitaalisen paikkatiedon tuottamiseen, jakeluun, käyttöön ja hallintaan liittyvät kyberturvallisuusriskit

Digitaaliseen paikkatietoon liittyy keskeisinä riskeinä ohjelmisto- ja alustariskit, laitetason riskit ja yksityisyyteen liittyvät riskit.

Ohjelmistotason riskit

Ohjelmistokehityksessä lopputulos ei aina ole vailla haavoittuvuuksia. Ohjelmistot ovat aina ihmisten tekemiä, mikä merkitsee, että niissä voi olla virheitä, jolloin niiden haavoittuvuudet mahdollistavat hyökkääjän koodin suorittamisen kohdejärjestelmässä. Ohjelmistovirheet ovat mykistäneet teleoperaattoreiden verkkoja, jättäneet lentokoneita kentille, lamauttaneet junaliikennettä ja antaneet kyberrikollisille valtavat ansaintamahdollisuudet.

Järjestelmien manipulointi on mahdollista, jos hyökkääjä pääsee käsiksi ohjelmakoodiin. Lisäksi lähdekoodin omistajalla täydellinen näkyvyys applikaatioon, ohjelmaan ja palveluun. Paikkatietoperustaiset applikaatiot, sovellut ja palvelut ovat alttiita kyberhyökkäyksille, jotka hyödyntävät ohjelmistotason haavoittuvuuksia

Laitetason riskit
Kyberturvallisuusongelmia esiintyy myös laite- ja komponenttitasolla. Paikkatietoa tuottavat ja käsittelevät laitteet voivat olla hyökkäyksen kohteina. Hyökkääjällä voi olla mahdollisuus päästä lataamaan haittaohjelma verkon yli laitteeseen tai kyky manipuloida laitetta komponenttitasolla. Hyökkääjällä voi olla pääsy mikropiirien tuotantoprosessiin ja kyky asentaa haittaohjelmia tai fyysisesti käsitellä niitä tai hänellä on pääsy mikropiirien suunnittelu- ja kehitysprosesseihin, jolloin voidaan takaisinmallinnuksen avulla luoda tehokkaita hyökkäysvektoreita. Tämä tarkoittaa sitä, että laitteet, joissa paikkatietoa käsitellään voivat olla kyberhyökkääjän saastuttamia tai ne voivat joutua hyökkääjän hallintaan.

Yksityisyyden riskit
Yksityisyyteen kohdistuvat riskit koskettavat koko digitaalista yhteiskuntaa. Digitaalinen maailma on luonut ihmiselle erilaisia digitaalisia ja virtuaalisia identiteettejä. Virtuaalisen identiteettimme avulla voimme muodostaa erilaisia verkostoja, joissa toimimme kuhunkin verkostoon valitsemallamme identiteetillä. Yksityisyys tarkoittaa fyysistä ja psyykkistä koskemattomuutta, ja itseään koskevan tiedon kontrollointia. Kysymys on mahdollisuudesta torjua sivullisten tunkeutuminen omaan elämään ja oikeudesta olla yksin. Ihmisten paikkatiedot voidaan tulkita myös henkilötiedoiksi ja siten paikkatietoaineisto voi muodostaa henkilörekisterin.

3. Kyberhyökkäykset

Kyberuhat voivat kohdistua suoraan tai välillisesti kansallisia järjestelmiä ja/tai kansalaisia vastaan maan rajojen sisältä tai ulkoa. Kyberuhat voidaan jakaa viisitasoiseen malliin, jossa luokittelu perustuu toimijoiden motiiveihin. Näillä kaikilla tasoilla paikkatieto voi olla hyökkäyksen suorana tai epäsuorana kohteena. Lisäksi paikkatieto on hyökkääjälle välttämätön elementti hyökkäysvektoria suunniteltaessa ja hyökkäystä toteuttaessa.

Tason 1 muodostaa kybervandalismi, johon kuuluvat mm. hakkerointi, haktivismi ja kyberparveilu. Yksittäisen yrityksen tai yksilön tasolla toiminta saattaa aiheuttaa merkittäviäkin taloudellisia vahinkoja.
Tason 2 muodostaa kyberrikollisuus. Euroopan Yhteisöjen komissio määrittelee kyberrikollisuuden rikoksiksi, "jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin". Paikkatietoa voidaan käyttää apuna hyökkäyksen toteuttamisessa tai sen anastaminen voi olla itse kohde.
Tason 3 muodostaa kybervakoilu. Kybervakoilu voidaan määritellä toimiksi, joilla hankitaan salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa tai tietokoneissa.
Tason 4 muodostaa kyberterrorismi, jossa tietoverkkoja käytetään hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan ja niiden kontrollointiin. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen sekä painostaa poliittista johtoa taipumaan terroristien vaatimuksiin. Paikkatiedon avulla hyökkääjä voi tarkasti maalittaa kohteen.
Tason 5 kybersodankäynti sisältää joukon erilaisia ei-kineettisiä operaatioita sodan voittamiseksi. Paikkatieto on keskeinen resurssi modernissa sodankäynnissä. Sen avulla toteutetaan

operaatioita ja maalitetaan kohteita. Paikkatieto on siis välttämätön kaikissa sotilasoperaatioissa ja se on myös kohde lamautettaessa vastustajan yhteiskunnan elintärkeitä kohteita.

4. Paikkatieto ja kriittinen infrastruktuuri

Kybermaailmassa uhan tärkeimpänä kohteena on kriittinen infrastruktuuri (Critical Infrastructure, CI). Kriittinen infrastruktuuri 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, koko ajan silmällä pitäen infrastruktuurikokonaisuuden toimintaa.
Kriittisen infrastruktuurin turvaamisessa on kolme ulottuvuutta: poliittinen, taloudellinen ja tekninen.

Poliittinen ulottuvuus on syntynyt kansallisesta intressistä turvata infrastruktuurijärjestelmänsä osana yhteiskunnan elintärkeiden toimintojen turvaamista. Poliittiseen ulottuvuuteen kuuluu kansallinen lainsäädäntö ja kansalliset turvallisuustarpeet sekä kansainvälinen yhteistyö näiden ympärillä. Taloudellinen ulottuvuus käsittää kaikki ne yritykset ja muut taloudelliset toimijat, jotka rakentavat, omistavat ja hallinnoivat infrastruktuurijärjestelmiä ja -laitoksia ja jotka toimivat taloudellisten intressien mukaisesti. Tekninen ulottuvuus käsittää tekniikan kehittymisen ja sen hyödyntämisen sekä kaikki ne käytännön ratkaisut ja toimenpiteet, joita valtiot ja yritykset tekevät turvatakseen kriittisen infrastruktuurinsa toimivuutta mahdollisten häiriöiden varalta.

Huoltovarmuuskeskuksen käyttämän määritelmän mukaan ”kriittinen infrastruktuuri muodostuu niistä 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.”

Kriittisen infrastruktuurin eri verkostot eivät ole erillisiä entiteettejä vaan muodostava kansallisen kriittisen infrastruktuurikokonaisuuden, jossa on paljon keskinäisriippuvuuksia. Yhden systeemin lamaantuminen tai romahtaminen vaikuttaa verkoston muihin osiin. Tämän vuoksi kriittisen infrastruktuurin analyysi edellyttää mallintamista, jotta verkoston eri osien keskinäisriippuvuudet voidaan saada esille.

Kriittisen infrastruktuurin sisälle on muodostunut kyberturvallisuuden kannalta merkittävä kokonaisuus, joka on kriittinen informaatioinfrastruktuuri (Critical Information Infrastructure, CII), joka käsittää erilaiset ICT-verkostot ja -palvelualustat. ICT on läsnä niin julkisen sektorin toiminnassa, yritysten liiketoiminnassa kuin kansalaisten arjessa. Tässä verkostokokonaisuudessa paikkatieto on läsnä kaikkialla, siksi se on keskeinen osa kansallista tietopääomaa, joka tulee olla turvallisesti käytettävissä normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa.

5. Kybermaailman luonne

EU:n digitalisaatio käsittelevissä raporteissa on lisääntyvässä määrin oltu huolissaan digitalisaation heikosta kehityksestä Euroopassa. Nykyisten arvioiden mukaan noin 95 % ohjelmistoista tuodaan Euroopan ulkopuolelta; EU:sta onkin tullut suurin ohjelmistotuoja. Sama pätee Suomeen. Euroopan digitaaliset alustat tehdään pääosin USA:ssa ja Kiinassa, ja me olemme keskittyneet tiedon luontiin noilla alustoilla, emme niiden rakenteiden tuottamiseen. Kiina on hyvä esimerkki suunnitelmallisesta kehittämisessä - 15 vuodessa siitä on tullut tasavertainen Yhdys-

valtain kanssa. Saman aikaan Eurooppa on jäänyt jälkeen näistä maista. Myös Venäjä on rakentanut ja rakentamassa on digitaalista palvelualustaansa.

Suomessa käytämme muiden tuottajien alustoja ja palveluita:

- Ohjelmistotuottajat: Microsoft, Apple, IBM, Oracle, SAP, Baidu…
- Alustatuottajat: Google, Amazon, Facebook, Alibaba, Uber, Airbnb, eBay, Twitter…
- Laitevalmistajat: Apple, Dell, Fujitsu, HP, Huawei, Lenovo, Microsoft, Mitsubishi, Samsung…
- Verkkopalvelutuottajat: Nokia, Ericsson, Huawei, ZTE, Samsung, Cisco, NEC, Fujitsu, Casa…
- Paikannuspalvelutuottajat: Galileo, GPS, BeiBou, IRNSS, QZSS…

Digitalisaatiokehitys on johtanut varsin keskittyneeseen alusta- ja palvelurakenteeseen, jossa yhä harvempi joukko toimijoita hallitsee koko markkinaa. Kuten edellä on kuvattu ohjelmistojen, palveluiden ja alustojen omistajat hallitsevat koko systeemiä, eikä käyttäjällä (organisaatio, yritys, kansalainen) ole juurikaan näkyvyyttä tai hallittavuutta systeemien sisälle.

Globaalia digitalisaatiokehitystä leimaa epäluottamuksen kasvu edellä kuvatussa palveluympäristössä. Alla muutama esimerkki:

Euroopan parlamentti äänesti (13.6.2018) Kasperskyn olevan "ei-toivottu/haitallinen" ja kieltää Kasperskyn tietoturvaohjelmistojen jäsenvaltioiden viranomaisten laitteistoissa kansallisen turvallisuuden nimissä. Kaspersky vastasi tähän lopettavansa kaiken yhteistyön kyberrikollisuuden torjunnassa Euroopan kanssa.

Presidentti Donald Trump allekirjoitti lain (13.8.2018), jonka seurauksena Yhdysvaltain valtionhallinto, urakoitsijat ja virastot joutuvat luopumaan suurelta osin Huawein ja ZTE:n valmistamasta teknologiasta.

Elokuussa 2018 Australian hallitus päätti estää kiinalaisyhtiöitä osallistumasta maan 5G-verkkojen rakentamiseen. Päätös kohdistuu juuri Huawei-ZTE -kaksikkoon. Jo aikaisemmin Huawei oli suljettu ulos Australian valokuituverkon rakentamisesta ja Tyyneen mereen lasketтavan datakaapelin toteuttamisesta.

Kiinan internet-sääntelyviranomainen reagoi tähän Australian päätökseen syyskuun alussa sensuroimalla Australian Broadcasting Corporationin sovelluksia ja verkkosivustoja Kiinassa. Sensuroinnin syyksi Kiinan viranomaiset ilmoittivat lakien ja määräysten rikkomisen ABC:n toiminnassa.

6. Paikkatietoalusta

Selonteossa esitetään perustettavaksi turvallisuusviranomaisille yhteinen paikkatietoalusta, mitä lähtökohtaisesti voidaan pitää perusteltuna ajatuksena. Samalla selonteon visio tavoittelee Suomesta maailman innovatiivisinta ja turvallisinta paikkatiedon ekosysteemiä. Kuinka ratkaistaan dilemma laaja-alaisen ja kaiken kattavan paikkatietoekosysteemin tiedon tuottamisen ja jakamisen tarpeen sekä turvallisuustoimijoiden paikkatietotarpeiden välillä? Miten voidaan erotella mikä paikkatiedoista on turvaluokiteltavaa ja mikä ei. Mikä voidaan jakaa kaikkien käyttöön ja mikä on salassa pidettävää.

Kansallisen paikkatiedon hallitsemiseksi voitaisiin rakentaa yksi kansallinen paikkatietoallas (tai erillisten altaiden kokonaisuus) (Data Lake) SOTE-tietoaltaan tapaan. Tietoallas on tiedonhallin-

taan tarkoitettu ratkaisu, joka mahdollistaa erityyppisten tietojen keruun ja tallentamisen edelleen jalostettavaksi. Paikkatietoallas antaisi käyttäjille hallitun rajapinnan kautta pääsyn kaikkeen dataan. Tietoallas antaa analyytikoille kehittäjille mahdollisuuden huomattavalle innovoinnille ja ennakoinnille. Tietoallas voidaan rakentaa pienemmistä keskenään yhteensopivista altaista, jolloin sen infrastruktuuri olisi selkeä ja käyttäjän olisi helppo navigoida läpi tietoaltaan. Keskeistä on luoda kyberturvallinen integraatio eri lähdejärjestelmien kanssa ja turvallinen pääsynhallinta (palveluoperaattori). Paikkatietoaltaassa voidaan tarpeen mukaan toteuttaa tiedon anonymisointia ja pseudonymisointia yksilöiden yksityisyyden ja tietosuojan näkökulmasta sekä luokitella kokonaisturvallisuuden kannalta merkittävää tietoa.

7. Kyberturvallisuus paikkatietopoliittisessa selonteossa

Tässä selonteossa tietoturvallisuus, tietosuoja, kokonaisturvallisuus ja maininta kyberkeinoista on mainittu hajallaan selonteon eri kohdissa. Kuten edellä on kuvattu, turvallisuus on keskeinen osa paikkatietojärjestelmää. Siksi selonteossa turvallisuusnäkökulma tulisikin koota yhteen omaan kokonaisuuteensa.

Siinä tulisi käsitellä paikkatiedon uhka- ja riskiympäristöä ja keskeisiä tavoitteita kyberturvallisuudelle. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturva kohdistuu tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen, mitkä tekijät paikkatiedon osalta ovat aivan keskeisiä. Kyberturvallisuus kohdistuu digitaaliseen ja verkottuneeseen toimintaympäristöön, jossa tarkoituksena on turvata kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Tietosuojan avulla toteutetaan järjestelyt, joilla pyritään varmistamaan paikkatietopohjaisten henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

Näille perusperiaatteille selontekoon tulisi luoda oma paikkatiedon kyberturvallisuutta käsittelevä kokonaisuus kokonaisturvallisuuden mallin pohjalta. Tämä keskitetty kyberturvallisuusosio ohjaisi nykyistä tehokkaammin selonteon toimeenpanoa. Kokonaisturvallisuusajattelun avulla luodaan yhteiskuntaan toimintatapamalli laaja-alaiseen varautumiseen, elintärkeiden toimintojen turvaamiseen sekä erilaisiin häiriötilanteisiin ja poikkeusoloihin yhdessä viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten kesken myös paikkatietoekosysteemissä.

8. Turvallisuuden rakentaminen

Yhteiskunta on yhä riippuvaisempi ohjelmistosta, sähköisistä palveluista, tietokonelaitteistosta ja verkottuneesta toiminnasta ja siksi ICT-järjestelmät ja informaatioperustaiset järjestelmät sekä toiminnat paikkatietoineen ovat kyberhyökkäysten kohteita. ICT-järjestelmien kompleksisuus tekee mahdottomaksi kokonaan eliminoida järjestelmien haavoittuvuudet sekä havaita ja jäljittää tunkeutumiset systeemin sisälle. Verkottuminen lisää tehokkuutta ja suorituskykyä mutta samalla se lisää kyberturvallisuutta vaarantavia haavoittuvuuksia.

Uhat kyber-fyysisessä toimintaympäristössä tulee nähdä osana kyber- ja hybridivaikuttamista. Tämä edellyttää valtioilta vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä. Paikkatieto ja sitä hyödyntävät laitteet, palvelut ja alustat tulee suojata **security by design** -periaatteella.

Paikkatietojen laatuun tulee kiinnittää erityistä huomiota, ei vain osoitetietojen osalta, vaan kaiken digitaalisen tiedon osalta. Erityisen ongelmallinen olisi tilanne, jossa paikkatietodata olisi korruptoitunut, emmekä voisi luottaa sen oikeellisuuteen. Tekoälyn ja autonomisten jär-

jestelmien lisääntyminen edellyttää korruptoimatonta ja puhdasta dataa. Muutoin älykkäiden laitteiden päätöksenteko ja toiminta perustuvat väärille oletusarvoille.

Keskeinen haaste on sovittaa yhteen paikkatiedon monipuolinen ja laaja-alainen käyttö kansallisessa ja kansainvälisessä toimintaympäristössä turvallisuusviranomaisten tarpeeseen kriittisen paikkatiedon ja sen käytön turvaamiseen. Paikkatietojärjestelmien turvallisuus ja turvallinen käyttö perustuvat tietoon ja ymmärrykseen kybermaailman olemuksesta ja lainalaisuuksista. Meidän tulee ymmärtää, että:

- Satelliittijärjestelmät eivät meidän valvonnassa
- Palvelualustat eivät meidän valvonnassa
- Keskeiset ohjelmistot eivät meidän valvonnassa
- Päätelaitteet eivät meidän valvonnassa
- Verkkolaitteet eivät meidän valvonnassa

Turvallisuusratkaisun tulisi tunnistaa paikkatietojärjestelmän osat, joihin meillä on edes jonkinlainen näkyvyys ja osat, joihin meillä ei ole näkyvyyttä lainkaan. Tältä osin pääsemme tekemään riskianalyysiä kunkin paikkatietopalvelun osalta. Riskinhallintakeinoin voimme vähentää ja osin ennaltaehkäistä riskien realisoitumista ja vähentää kyberhyökkäysten vaikuttavuutta maamme kriittisessä infrastruktuurissa.

Kansallisella tasolla meiltä löytyy osaamista ja kyvykkyyttä hallinta kyberuhkia paikkatietojärjestelmää vastaan mm. seuraavin tavoin:

- Palveluoperaattori huolehtimaan altaan käytöstä ja turvallisuudesta
- Robustisten laitteiden käyttö erityisen kriittisissä kohteissa
    - laitteen infrastruktuuri omassa kontrollissa
- Todellinen päästä-päähän tietoliikennesalaus
    - käyttäjä vastaa salauselementtien luomisesta ja käsittelystä ilman kolmatta osapuolta
    - kyky koota ja konfiguroida salausohjelmisto omaan käyttöön
- Avoin lähdekoodi (Linux)
    - täydellinen läpinäkyvyys lähdekoodiin (näkymättömien binaarikoodien välttäminen)

Paikkatiedon turvallisuus tulee nähdä systeemisenä kokonaisuutena, jossa turvallisuus hallitaan tiedon luonnista tallennukseen, käyttöön, jakamiseen ja tiedosta luopumiseen. Tämä vaatimus ei kohdistu vain paikkatietoon, vaan koko kansalliseen digitaaliseen tietovarantoon kokonaisuutena.

Selonteko esittää kehitettäväksi yhteistä paikkatiedon ekosysteemiä, joka tarkoittaa laaja-alaisena yhteistyönä kehitettävää ja ylläpidettävää paikkatietoihin liittyvää tieto- ja palvelukokonaisuutta, jonka ylläpitovastuut ja taloudelliset vastuut on määritelty. Vastuiden määrittelyn lisäksi tulee määritellä johtajuus ekosysteemissä. Ilman selkeää johtajuutta kyberturvallisuus ekosysteemissä ei kehity vastaamaan kybertoimintaympäristön nopeaan muutokseen.

Professori, ST Martti Lehto
Informaatioteknologian tiedekunta
Jyväskylän yliopisto
martti.lehto@jyu.fi