2.2.2026

Lausunto Valtioneuvoston selontekoon sisäisestä turvallisuudesta

Kiitän mahdollisuudesta lausua tästä Valtioneuvoston selonteosta sisäisestä turvallisuudesta.

Selonteko on kokonaisuutena hyvä ja tiivis katsaus Suomen sisäiseen turvallisuuteen ja sen uhkaympäristöön. Heti alussa todetaan, että ”*Suomen sisäisen turvallisuuden politiikan tärkeimpänä päämääränä on varmistaa, että Suomi on luottamuksen yhteiskunta, jossa toteutuvat turvallisuus ja oikeudenmukaisuus kaikissa oloissa.”* Tämä on ehdottoman kannatettava päämäärä.

Selonteossa otetaan myös kiitettävästi kantaa erilaisiin kyberturvallisuuteen ja digitaaliseen toimintaympäristöön liittyviin turvallisuusnäkökohtiin. Selonteon toteamus *”Jatkuva teknologinen murros ja muut yhteiskunnalliset muutosvoimat tuottavat viranomaisille uusia tehtäviä ja kompleksisessa maailmassa ongelmat ovat monimutkaisia.”* kuvaa hyvin digitaalisen toimintaympäristön haasteita.

Selonteossa on erittäin hyvä ja kattava osio informaatiovaikuttamisesta, joka on varmasti yksi niistä ilmiöistä, jotka saavat paljon uusia mahdollisuuksia digitaalisessa maailmassa. Selonteossa on tunnistettu useita tärkeitä näkökohtia tähän liittyen. Yhtenä lisäyksenä voisi huomioida, että useat suosituimmat tiedonvälityskanavat ovat erilaisia sosiaalisen median alustoja, joiden omistajien, hallinnoijien ja tärkeimpien sisällöntuottajien toiminta ja tavoitteet voivat hyvinkin olla meidän näkökulmastamme informaatiovaikuttamista.

Pidänkin hieman erikoisena, että useat suomalaiset ja eurooppalaiset poliitikot ja muut vaikuttajat toimivat näillä alustoilla, vaikka samalla julistavat pyrkimystä saavuttaa parempi eurooppalainen digitaalinen suvereniteetti.

Selonteosta puuttuu huomio siitä, että Suomen ja Euroopan (EUn) riippuvuus digitaalisen infrastruktuurin suhteen on myös sisäiseen turvallisuuteen merkittävästi vaikuttava seikka. Selonteossa korostetaan yhteiskunnan resilienssiä ja kriisivalmiutta, mutta ei tuoda esille sitä näkökohtaa, että suuri osa yhteiskuntamme digitaalisesta infrastruktuurista on ulkopuolisten palveluntarjoajien tuottamaa ja tietyssä mielessä näiden ”armoilla”. Näkisin erinomaisena, mikäli selonteossa kyettäisiin ottamaan kantaa myös tähän ilmiöön ja tekemään joitakin johtopäätöksiä siihen liittyen.

Oulun yliopisto

PL 8000
90014 Oulun yliopisto

oulun.yliopisto @ oulu.fi
Puh 0294 480 000
Fax 08 344 064

www.oulu.fi

Kriittinen infrastruktuuri on nostettu hyvin esille selonteossa. Myös tähän liittyvät kyberturvallisuuden näkökohdat on huomioitu melko hyvin. Kuitenkin jo aiemmin mainitut riippuvuudet ulkopuolisista toimijoista vaikuttavat myös tähän eikä niitä ole selonteossa huomioitu. Erityisesti kyberturvallisuuden suhteen olisi hyvä huomioida myös epäsuhta mahdollisesti valtiollisten toimijoiden vaikuttamiskyvykkyyksien ja usein hyvinkin pienten kunnallisten ja/tai kaupallisten toimijoiden kyberturvallisuusresurssien välillä. Osa kriittisen infrastruktuurin toimijoista on melko pieniä ja kuitenkin vastapuolella saattavat olla nämä suuret toimijat. Sisäisen turvallisuuden kannalta olisi hyvä tunnistaa tilanne ja pohtia, miten tähän vastataan koko Suomen näkökulmasta riittävillä turvallisuustoimilla.

Hieman yksityiskohtaisempana huomiona todettakoon, että selonteon sivulla 6 esitetään, että *”Kiristyshaittaohjelmat, lasten seksuaalinen hyväksikäyttö ja tietoverkkoavusteiset petokset ovat kyberrikollisuuden suurimmat ilmentymät.*” Muuten erittäin hyvin viitteistetyssä selonteossa tähän väitteeseen ei ole annettu mitään lähdettä, mikä hieman vähentää väitteen painoarvoa. Koska osa selonteossa esitetyistä johtopäätöksistä sekä toimenpiteistä liittyvät myös kyberrikollisuuden torjunnan mahdollisuuksiin ja viranomaisten toimivaltuuksien lisäämiseen, olisi hyvä tuoda näin merkittävien lähtökohtien taustatiedot ja lähteet myös esille.

Selonteon johtopäätöksissä todetaan lopuksi, että ”*Erityisesti tulee seurata teknologista kehitystä ja ymmärtää kehitykseen liittyviä turvallisuusuhkia sekä toisaalta murroksellisten teknologioiden tuomia mahdollisuuksia turvallisuuden parantamiseen. Sisäisen turvallisuuden toimijoiden kykyä ja kapasiteettia teknologian seurantaan ja hallintaan tulee vahvistaa. Lisäksi Suomen tulee aiempaa systemaattisemmin hyödyntää kansallista ja kansainvälistä tutkimus-, kehittämis- ja innovaatiorahoitusta sekä -yhteistyötä sisäisen turvallisuuden vahvistamiseksi.”* Tämä on erittäin hyvä linjaus ja kannatettava toimintalinja. Kuitenkaan itse toimenpidesuositukset eivät pidä sisällään toimenpiteitä tämän aihepiirin tutkimus-, kehittämis- ja innovaatiotoiminnan suhteen. Voisi kuitenkin olla tarpeen asettaa myös jonkinlainen toimenpidesuositus sen suhteen, miten ja minkälaisilla tavoilla viranomaiset ja tutkimus- ja innovaatiotoimijat voisivat yhdessä toteuttaa erilaisia tutkimuksia, joissa tuota selonteossa mainittua rahoitusta hyödynnettäisiin.

Johtopäätöksissä ja toimenpidesuosituksissa tuodaan hyvin esille tarve panostaa kyberturvallisuuteen ja lisätä tiedonvaihtoa. Selonteossa esitetään myös, että mahdollistetaan viranomaisille oikeus puuttua Suomen ulkopuolella olevien laitteiden ja ohjelmistojen toimintaan, mikäli näitä käytetään vakoiluun tai vaikuttamiseen. Digitaalisessa toimintaympäristössä monilla toteutuksen yksityiskohdilla voi olla suuria vaikutuksia. Onkin mielenkiintoista nähdä, mitkä ovat ne konkreettiset keinot, joilla tuota oikeutta puuttua tällaisiin laitteisiin ja ohjelmistoihin voidaan toteuttaa Suomen ulkopuolella.

Kokonaisuutena selonteossa kyberturvallisuus on huomioitu melko hyvin, mutta siihen liittyvät toimenpiteet ovat hyvin yleisellä tasolla. Erityisesti kyberturvallisuudessa myös teknisillä yksityiskohdilla ja toteutusmenetelmillä on paljon merkitystä. Pelkkien yleisluontoisten johtopäätösten ja toimenpidesuositusten perusteella on vaikea arvioida, mikä olisi paras tapa

toteuttaa haluttu johtopäätös ja minkälaisia vaikutuksia tällä olisi teknologiaan ja/tai sääntelyyn laajemminkin.

Merkittävänä voidaan vielä pitää sitä, että selonteossa todetaan lopuksi, että ”*Tavoitteita toteutetaan olemassa olevien määrärahojen puitteissa”*. On kuitenkin mahdollista, että jotkut ehdotetuista toimista vaativat lisäresursseja, jotta niiden vaikutus olisi täysimääräinen. Riittävä resursointi on erittäin tärkeää, jotta voidaan saavuttaa haluttu turvallisuuden taso.

Oulussa 2.2.2026

Kimmo Halunen

Digitally signed by Kimmo Halunen
DN: cn=Kimmo Halunen, c=FI, o=ITEE, ou=BISG, email=kimmo.halunen@oulu.fi
Reason: I am the author of this document
Date: 2026.02.02 13:37:59 +02'00'

Kimmo Halunen

Kyberturvallisuuden professori

Oulun yliopisto ja Maanpuolustuskorkeakoulu