Martti Lehto, Jyväskylän yliopisto
2.5.2022

Eduskunnan hallintovaliokunta

Asia: Ajankohtaisselonteko turvallisuusympäristön muutoksesta, VNS 1/2022 vp

29.4.2022 annetun lausunnon ja suullisen esityksen täydennys

1. INFORMAATIOVAIKUTTAMISESTA

Keskustelussa tuli esille koronarokotuskriittisen viestinnän ja NATO:oon liittymisen vastustamisen mahdollinen yhteys.

On ilmeistä, että poliittiseen järjestelmään ja yhteiskunnallisiin instituutioihin kriittisesti/kielteisesti suhtautuvat hakevat kritiikilleen ajankohtaisen aiheen. Salaliittoteorioihin uskovat näkevät kaikessa yhteiskunnallisessa toiminnassa kielteisiä piirteitä ja pyrkimystä alistaa kansalaiset. Näiden uskomusten takana nähdään olevan pitkän ajan tapahtumasarjan ja/tai kehityskulun, jonka takana on enemmän tai vähemmän taustalla toimiva ryhmä (eliitti), jolla tavoitteena on täydellinen poliittinen valta (uusi maailmanjärjestys).

Venäjän informaatioturvallisuuden doktriinissa on kaksi ulottuvuutta: psykologinen ja tekninen. Psykologisessa ulottuvuudessa pyritään vaikuttamaan ihmismieleen ja teknologisessa ulottuvuudessa kohteena ovat tietoverkot ja kriittinen infrastruktuuri sekä sähkömagneettinen spektri.

Yksi elementti venäläisessä informaatiovaikuttamisessa on saada kohde käyttäytymään näennäisen itsenäisesti ja itsetuhoisesti. Ts. pienillä, pitkän ajan keinoilla luodaan kohdehenkilössä tai kohderyhmässä lisääntyvää epävarmuutta, pelkoa, epäluottamusta valtiovaltaan ja näin saadaan henkilö tai ryhmä näennäisen sisäsyntyisesti tuottamaan disinformaatiota.

Rokotus- ja NATO-vastainen vaikuttaminen on todennäköisesti sekä sisäsyntyistä että ulkoa ohjattua.

1. Salaliittoteoriapohjalta ajattelevat ottavat kohteeksi ajankohtaisen teeman eli siirtyneet koronarokotuksista NATO:n vastustamiseen.

2. Em. ryhmää voidaan tukea ulkoa tuottamalla sille disinformaatiota jaettavaksi ja tukemalla näiden ryhmien ajatuksia (”bensaa liekkeihin”).

3. Tästä ryhmästä voidaan värvätä aktiivisiksi toimijoiksi tukemaan Venäjän informaatio-operaatioita. Nämä voivat saada koulutusta ja materiaaliapua. Tähän

ryhmään kuuluvat ns. ”hyödylliset idiootit” ja tietoisesti nykyistä yhteiskuntajärjestystä vastustavat.

Esimerkit sähköpostien mukana tulleista linkeistä hyvin tehdyille nettisivuille tai videoihin osoittaa taustalla olevan ammattimaista toimintaa. Hyvin tehdyt infosivustot ja videot pyrkivät tehokkaaseen viestintään ja luomaan vaikutelmaa luotettavasta informaatiosta. Jaettavaa väärää informaatiota vaarallisempaa on noille sivustoille meno.

Missään tapauksessa tuntemattomasta lähteestä tulevien (yksityishenkilöt tai organisaatiot) sähköpostien **liitetiedostoja tai nettilinkkejä ei saa avata**. Mikäli valtiollinen toimija tai sellaisen tukema ryhmä on viestin takana, on liitetiedostoon tai nettilinkkiin hyvin todennäköisesti liitetty tiedustelua toteuttava haittaohjelma. Näille toimijoille kansanedustajan sähköpostiliikenne on erinomainen tiedustelukohde.

2. KYBERVOIMAN KÄYTTÖ

Kybervoima/valta kuvaa valtion kybersuorituskykyä vallankäytön välineinä. Tämä mahdollistaa myös vallan väärinkäytön. Autoritäärisissä diktatuureissa kaikki voimankäytön välineet ovat tarvittaessa käytettävissä kansalaisten hallitsemiseen. Esimerkit monista maista osoittavat, että asevoimia ja sisäisen turvallisuuden joukkoja käytetään kansalaisia vastaan. Usein myös koko informaatioympäristö on otettu valtion hallintaan ja johtoon.

Harvardin Kennedy Schoolin Belfer Centerin määrittämän kybervoiman seitsemän indikaattoria eivät lähtökohtaisesti tarkoita hyvää tai pahaa. Kysymys on kybervoimankäytön laillisuudesta (laillisuusvalvonta), parlamentaarisesta valvonnasta ja kansalaisten luottamuksesta.

Meillä tästä on hyvänä esimerkkinä tiedustelulainsäädäntö. Tiedustelutoiminnan laillisuusvalvonnasta huolehtii itsenäinen ja riippumaton tiedusteluvaltuutettu. Tiedustelutoiminnan parlamentaarista valvontaa toteuttaa eduskunnan tiedusteluvalvontavaliokunta. Tällä mallilla rakennetaan kansalaisten luottamusta tiedustelutoiminnan oikeudenmukaisuuteen ja siihen, että sitä toteutetaan vain ja ainoastaan lain sallimissa ja tarkoittamisissa tapauksissa, vaikka itse toiminta tuloksineen on luottamuksellista.

Suomessa tulisi kehittää eri toimijoiden kybersuorituskykyjä laaja-alaisesti, jotta kykenisimme valvomaan kyberalueemme loukkaamattomuutta ja tarvittaessa torjumaan kyberalueellemme kohdistuvat vihamieliset hyökkäykset. Haasteena kybertoimintaympäristössä on se, että vastustaja toteuttaa kyberoperaatioita alle sodan kynnyksen jo rauhan ajan olosuhteissa.

3. DIGITALISAATIO JA KYBERTURVALLISUUS

Suomalainen yhteiskunta digitalisoituu vauhdilla. Tavoitteena on tehdä palveluista toimivampia ja joustavampia sekä kustannustehokkaita. Digitalisaatiossa tulisi aikaan saada entistä paremmat ja luotettavammat palveluketjut ja järjestelmät kansalaisten, julkisen sektorin ja yritysten tarpeisiin.

Suomi on yksi maailman kärkimaista julkisissa sähköisissä palveluissa. Meillä suomalaisilla on myös tutkitusti EU-maiden paras digiosaaminen. Kyberturvallisuutta kuvaavissa arvioinneissa olemme menettäneet asemiamme suhteessa muihin maihin 2010-luvulta lähtien. Aikaisemmin olimme Euroopassa 5:n kärjessä ja maailmassa 10-kärjessä, nyt olemme Euroopassa 10-joukossa ja maailmalla 20-listalla. Mittausten mukaan tekemisemme on parantunut, mutta monet muut ovat parantaneet kyberturvallisuuttaan vieläkin enemmän. Yksi tekijä näyttäisi olevan meillä kyberturvallisuuden toteuttamisen hajanaisuus.

Nykyisen hallitusohjelman yhtenä tavoitteena on edistää ihmisten mahdollisuutta sähköiseen tunnistautumiseen, edistää toimivien tunnistusratkaisujen kehittymistä ja mahdollistaa henkilön mahdollisuuksia hallita omia julkisissa palveluissa olevia tietojaan. Tätä tukee Euroopan komission kesällä 2021 julkaisema lainsäädäntöehdotus eurooppalaisesta identiteettilompakosta.

Lähtökohtaisesti digitalisaation avulla voidaan tuottaa kansalaisten tarvitsemia palveluita aikaisempaa joustavammin ja tehokkaammin. Kovin usein digipalveluiden kehittämisen keskiössä on asiakaslähtöisyys ts. tehdään joustavia ja helppokäyttöisiä ratkaisuja. Digitalisaation vahvistuessa ja laajentuessa keskiöön tulisi nostaa turvallisuus (informaatio- ja kyberturvallisuus). Tällä hetkellä tie-, raide-, vesi- ja lentoliikenteessä kehittämisen keskiössä on turvallisuus. Esimerkiksi kansainvälisen ilmakuljetusliiton (IATA) mukaan ilmailussa turvallisuus on numero 1 (Flying safety). Tämä tulisi olla myös digitalisaatiossa.

Digitalisaatiossa kyberturvallisuuden kohteena ovat ihmisten toiminta (digiturvalliset taidot), palveluntuottajien kyberturvallisuusprosessit (viranomaisten mahdollisuus regulaation avulla määritellä turvallisuustasot) ja kyberturvallisuusteknologia (ratkaisut laiteturvallisuuden, tietoliikenteen ja datan osalta).

Tietovarantoihin kohdistuvat riski datamanipulaatiosta on noussut yhä voimakkaammin esille. Kansalaiset ja viranomaiset luottavat esim. terveystietojen oikeellisuuteen KANTA-järjestelmässä tai kaikki luotamme bitteinä olevaan rahaan pankeissa. Datamanipulaation avulla voidaan horjuttaa uskoa näiden järjestelmien toimintaan. Jo vuonna 2015 Yhdysvaltain johtavat viranomaiset eri turvallisuusyksiköistä näkivät juuri datamanipulaation kaikkein vaarallisimpana kyberhyökkäyksen muotona.

Siksi moneen kertaa toistettu vaade kyberturvallisuuden huomioon ottamisesta järjestelmäsuunnittelun alusta alkaen (Cyber-security by Desing) on aivan välttämätöntä.

4. SOSIAALINEN MEDIA JA KYBERTURVALLISUUS

Hyvä lähtökohta sosiaaliseen mediaan ja Internetin palveluihin on 0-luottamus (Zero Trust). Kun käytämme ilmaisia sovelluksia ja applikaatiota tulisi jokaisen kysyä itseltään: MIKSI PALVELU ON ILMAINEN? Internetissä ja mobiiliverkossa kun ei ole ilmaisia palveluita. Kaikilla on jokin ansaintalogiikka. Palvelut kertovat jollain tavoin tästä käyttöehdoissaan.

Google on kertonut tästä varsin selkeästi: ”Yleisesti ottaen annamme sinulle luvan käyttää palveluitamme, jos suostut noudattamaan näitä ehtoja, jotka ovat sidoksissa Googlen liiketoimintoihin ja tapoihin ansaita tuloja.” ”Tämän käyttöoikeuden nojalla Google saa:

- ylläpitää, jäljentää, jaella, välittää ja käyttää sisältöäsi,
- julkaista sisältöäsi tai esittää tai näyttää sitä julkisesti,
- muokata sisältöäsi esimerkiksi muotoilemalla sitä uudelleen tai kääntämällä sitä,
- alilisensoida nämä oikeudet muille käyttäjille, sopimuskumppaneille.”

Jokainen Googlen ja se eri palveluita käyttävä on sitoutunut näihin ehtoihin. Muilla toimijoilla (Facebook, Instagram, WhatsApp jne.) on vastaavat ehdot. Olemme siis vapaaehtoisesti antaneet paljon tietoa itsestämme ja tekemisestämme some-palveluntarjoajille.

Toiminnan keskiössä on henkilön profilointi ja mikrokohdentaminen. Nettitoiminnastamme meistä muodostuu profiili siitä, mistä pidämme, mitä harrastamme, mitä arvostamme jne. Profilointiin erikoistuneet yritykset kokoavat ihmisistä erilaisia profilointitietoja. Näiden avulla meille voidaan kohdentaa juuri meille tarkoitettua mainontaa. Tässä ympäristössä on oletettavaa, että internet-profiilimme avulla myös meidän verkostomme voidaan identifioida.

Riski muodostuu siitä, mikäli palveluntarjoaja toimii vastoin ilmoittamiaan käyttöehtoja. Säännöllisesti tulee esille myös epäilyjä palveluntarjoajien kyvystä huolehtia henkilöiden tietosuojasta. Myös esille on tullut niiden tietoisia väärinkäytöksiä (esim. Facebook ja Cambridge Analytics case, 2016).

5 KYBERTURVALLISUUDEN KANSALLINEN JOHTAMINEN

Kansallinen kyberturvallisuuden strategisen tason johtaminen muodostuu seuraavista kolmesta osakokonaisuuksista:

1. normaaliaikojen kyberturvallisuuden toteuttaminen (kybersuojaus),
2. laajamittaisten häiriötilanteiden hallinnan johtaminen normaali- ja poikkeusoloissa
3. kybervarautumisen ja -huoltovarmuuden johtaminen

Kohdan 1 toimenpiteistä huolehtii kukin hallinnonalan ja organisaatio osana jokapäiväistä toimintaansa. Arjessa yksilöt ja organisaatiot kohtaavat säännöllisesti kyberhyökkäyksiä, joilta suojaudumme oikean toimintatavan ja teknologian (kuten virustorjunta ja palomuuri) avulla.

Vakavia häiriötilanteita voi esiintyä sekä normaaliaikana että poikkeusoloissa. Normaaliajan häiriötilanteet hallitaan viranomaisten tavanomaisin toimivaltuuksin ja organisaatioiden voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliolojen häiriötilanteiden hallinnassa.

Kohdan 3 mukaiseen varautumiseen yhdistyy huoltovarmuus ja kyberomavaraisuudesta huolehtiminen. Tämä tarkoittaa väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen ja niihin liittyvien teknisten järjestelmien turvaamista poikkeusolojen ja niihin verrattavissa olevien vakavien kyberhäiriöiden varalta. Varautumista ohjaa eri elintärkeille toiminnoille asetetut velvoitteet ja organisaatioiden omat tavoitteet erityisesti toiminnan jatkuvuuden hallinnan kannalta.

Yhteiskunnan digitalisaatio lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien laaja-alaisten kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti.

Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta.

Nykymallin mukaisesti laaja-alaisessa kyberhäiriötilanteessa toimivaltainen viranomainen johtaa operatiivista toimintaa ja poikkihallinnolliset yhteistyöelimet tukevat vastuuviranomaista. Muut viranomaiset, yritykset ja järjestöt osallistuvat toimintaan tilanteen hallinnan edellyttämässä laajuudessa.

Mallin heikkoutena on epävarma kyky reagoida riittävän nopeasti laajamittaiseen kyberhyökkäykseen tai häiriötilanteeseen sekä tuottaa alati muuttuviin kyberuhkiin varautumisen kannalta välttämätöntä ennakoivaa strategista analyysitietoa. Laajamittaisessa kyberhyökkäystilanteessa vastatoimenpiteet tulee aloittaa välittömästi, aikaa ei ole määritellä vastuutahoja tai -toimijoita. Tehokas kyberhäiriötilanteiden torjunta edellyttää hyvää ja kattavaa kybertilannekuvaa.

Nykyistä johtamisrakennetta ei voi pitää varautumisen yhteensovittamisen, strategisten tavoitteiden tunnistamisen tai kansallisen kyberturvallisuusidentiteetin vahvistamisen kannalta optimaalisena. Nykymalli ei ohjaa riittävästi hallinnonalojen, elinkeinoelämän ja kolmannen sektorin kyberturvallisuusvarautumista eikä muodosta riittävän keskitettyä strategista analysointikykyä tilannetietoisuuden tuottamisen tueksi. Kyberturvallisuuden kansallisen omavaraisuuden tunnistaminen ja kehittäminen jäävät nykymallissa puutteelliseksi. Kansainvälisissä vertailuissa korostunut kyberturvallisuuden strategisen johtamisen läheisen yhteyden tarpeellisuus poliittiseen päätöksentekoon ei näyttäydy selkeänä.

Erittäin karkea vertailu Suomen ja Yhdysvaltain kyberturvallisuusrakenteiden välillä on esitetty oheisessa taulukossa:

Kybertoiminta-alue	**Yhdysvallat**	**Suomi**
Kansallisen kyberturvallisuuden johtaminen	Kansallinen kyberjohtajan toimisto (The Office of the National Cyber Director, ONCD) sijoitettuna presidentin kansliaan (White House)	Valtion kyberturvallisuusjohtaja sijoitettuna LVM:ään.
Sotilaallinen kyberpuolustus	Puolustusministeriö (DoD) Cyber Command National Security Agency (NSA)	Puolustusministeriö Puolustusvoimat
Kybertiedustelu ja sen torjunta	Keskustiedustelupalvelu (CIA)	Turvallisuus- ja tiedustelupalvelu (SUPO)
Kyberrikollisuuden torjunta	Yhdysvaltain liittovaltion poliisi (FBI)	Keskusrikospoliisi (KRP)
Kriittisen infrastruktuurin suojaaminen	Kotimaan turvallisuusministeriö (Department of Homeland Security, DHS) Kyber- ja infrastruktuurivirasto (Cybersecurity and Infrastructure Security Agency, CISA)	Tehtäviä monen ministeriön vastuulla. LVM: Kyberturvallisuuskeskus TEM: Huoltovarmuuskeskus

Tämän hyvin karkean esityksen perusteella voidaan todeta, että Yhdysvalloissa (kuten monessa muussa maassa) kyberturvallisuusjohtajalla on toimisto ja se on sijoitettu ylimmän poliittisen johdon yhteyteen (meillä se olisi valtioneuvoston kanslia).

Yhdysvaltain kyberjohtajan toimisto on sijoitettu Valkoiseen taloon tehtävänä ylimmällä poliittisella tasolla:

- varmistaa liittovaltiotason kyberturvallisuusstrategian ja toimintaohjeiden toimeenpano
- parantaa julkista ja yksityistä yhteistyötä (PPP)
- resurssien allokointi liittovaltion tavoitteiden mukaisesti
- olemassa olevan ja tulevaisuudessa tarvittavan kyberresilienssin lisääminen

Ts. ONCD:n tehtävä on varmistaa, että kansallinen kyberturvallisuus rakentuu laaditun kyberturvallisuusagendan tavoitteiden mukaisesti vastaamaan nykyisiin ja tuleviin uhkiin.

Kriittisen infrastruktuurin suojaamiseksi kyberhyökkäyksiltä Yhdysvalloissa nähtiin välttämättömäksi perustaa vuonna 2018 DHS:n yhdeksi operatiiviseksi virastoksi CISA. Se johtaa kansallisella tasolla liittovaltion kyberturvallisuustoimia ja toimii kriittisten infrastruktuurien turvallisuuden ja resilienssin kansallisena koordinaattorina. Sillä on vahva rooli kyberturvallisuuden PPP-toiminnassa.

Lisäksi Yhdysvaltain hallinnolla on kullekin DHS:n määrittämälle kriittisen infrastruktuurin alueelle muodostettu koordinaationeuvosto (Government Coordinating Council, GCC). Kyberturvallisuuden alueella GCC:n tehtävä ja tarkoitus on tarjota tehokas virastojen ja hallinnon alojen välinen toimien, strategioiden ja politiikan koordinaatio aloilla, joita ovat tietotekniikka, kyberturvallisuus sekä infrastruktuurin turvallisuus ja resilienssi.

Meillä voitaisiin kansallista kyberturvallisuutta kehittää käyttäen hyväksi soveltuvin osin perusteita ja kokemuksia CISA:sta, ONCD:stä ja GCC:stä.

Kyberturvallisuuden strategista johtamista on käsitelty raportissa:
”Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.”

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi