Martti Lehto, Jyväskylän yliopisto
9.2.2021

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko

Asia: VNS 4/2020 vp

1. Turvallisuusympäristön muutos

1.1 Digitalisaatio muuttaa yhteiskuntaa

Yhteiskunnan yksityiset ja julkiset palvelut perustuvat yhä laajemmin ihmisten, erilaisten toimijoiden ja älykkäiden systeemien keskinäisriippuvaan toimintaympäristöön. Digitaalitalouden kehitystä edistävät erilaisten palveluiden ja tietokäytäntöjen digitalisoituminen ja siirtyminen verkkoon. Yhteiskunnan digitalisaatio on vahvistanut kybertoimintaympäristöä, luonut kybertilan, jossa kriittinen infrastruktuuri tuottaa yhteiskunnan elintärkeät palvelut pääosin digitaalisesti. Tämä digitaalinen murros muuttaa tapaa, jolla palveluita ja hyvinvointia tuotetaan eli koko yhteiskunnan toimintalogiikka on muuttunut – kyber on kaikkialla.

Euroopassa turvallisuusuhkaympäristö on muuttunut nopeasti. Euroopan komissio kuvasi tiedonannossaan jo huhtikuussa 2016 yhteistä kehitystä hybridiuhkien torjumiseksi ja EU:ssa tarvittavia toimia. Sen mukaan EU hyötyy paljon siitä, että yhteiskunta on yhdistetty verkkoihin ja digitalisoitu. Hybridiuhkien toteuttajat voivat kuitenkin tehdä kyberhyökkäyksiä, joilla häiritään digitaalipalveluja eri puolilla EU:ta.

Euroopan komissio analysoi pohdinta-asiakirjassaan Euroopan puolustuksen tulevaisuudesta kesällä 2017 tulevaisuuden uhkamaailmaa. Sen mukaan ”massadata, pilviteknologia, miehittämättömät ajoneuvot ja tekoäly mullistavat puolustussektoria. Tämän verrattain helposti saatavilla olevan teknologian käyttö mahdollistaa kuitenkin epätavanomaisten, valtioiden rajat ylittävien ja epäsymmetristen uhkien nopean kasvun. Näitä ovat muun muassa hybridi- ja kyberuhat, terrorismi sekä kemialliset, biologiset ja radiologiset iskut. Internetin käyttäjien määrän nopean kasvun myötä kyberrikollisuudesta ja internetin terrorikäytöstä on tullut 2000-luvulla sodankäynnin uusia muotoja.”

EU:n turvallisuusunionistrategiassa (2020) todetaan, että ”kyberhyökkäyksillä on huomattavia haittavaikutuksia koteihin, pankkeihin, rahoituspalveluihin ja yrityksiin. Fyysisten ja digitaalisten järjestelmien keskinäinen riippuvuus pahentaa mahdollisia vahinkoja entisestään: kaikilla fyysisillä iskuilla on vaikutusta digitaalisiin järjestelmiin, ja tietojärjestelmiin ja digitaalisiin infrastruktuureihin kohdistuvat kyberhyökkäykset voivat lamauttaa keskeisiä palveluita. Siksi kyberturvallisuus on välttämätöntä resilientin, vihreän ja digitaalisen Euroopan rakentamiseksi.”

Kehitys on ollut edellä kuvatun mukaista.

1.2 Puutteellinen kybertilannetietoisuus

EU komissio toteaa uusimmassa kyberturvallisuusstrategiassaan (2020), ettei ”EU:lla ole kollektiivista tietoisuutta kyberuhista. Tämä johtuu siitä, että kansalliset viranomaiset eivät kerää ja jaa järjestelmällisesti tietoja, kuten yksityiseltä sektorilta saatavaa tietoa, mikä voisi auttaa arvioimaan kyberturvallisuuden tilaa EU:ssa. Jäsenvaltiot ilmoittavat vain murto-osasta tapauksista, eikä tietojen jakaminen ole järjestelmällistä eikä kattavaa.” Kyberhyökkäykset ylittävät kansallisvaltioiden rajat, joten laajempi tilannetietoisuus kybertoimintaympäristöstä on aivan välttämätöntä.

1.3 Mikä on kansallinen kybertila/kybertoimintaympäristö

Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen.

Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa. Siten Suomen alueellisen koskemattomuuden valvonta kohdistuu Suomen rajoille. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä alueloukkauksen estämiseksi tai torjumiseksi.

Kansallinen kybertila tulisi määritellä, jotta voitaisiin toteuttaa Suomen kybertilan koskemattomuuden valvonta ja torjunta. Määrittely ei ole yksinkertaista, sillä esimerkiksi käytettäviä digitaalisia palveluita tuotetaan globaalissa tietoverkossa, data liikkuu ja varastoituu globaalisti. Tämä bittien maailma, kun ei tunne valtakunnan rajoja. Kuitenkin tarvitaan selkeä määrittely kansallisesta suvereniteetista kybertilassa. Tässä suhteessa kansallinen kybertila ei ole vain teknologinen toimintaympäristö vaan merkittävällä tavalla turvallisuuspoliittinen toimintaympäristö.

1.3 Raja sodan ja rauhan välillä hämärtyy kybertilassa

Kybermaailman tulo fyysisen maailman rinnalle on aiheuttanut sen, että raja rauhan ja sodan välillä on hämärtynyt. Digitalisaation vahvistuessa ja yhteiskuntien riippuvuuden kasvaessa digitaalisista palveluista, kriittisestä infrastruktuurista kyberhyökkäysten kohteena on muodostunut keskeinen kohde konflikteissa ja sodankäynnissä. Kybertilassa voidaan vaikuttaa etäältä anonymiteetin suojassa ja attribuution tavoittamattomissa.

Mutta kybertilassa sota ja rauha saavat perinteistä poikkeavan merkityksen. Me yleensä ajattelemme, että rauha vallitsee, jos sotaa ei ole. Esimerkiksi venäläisessä narratiivissa he mieltävät olevansa jatkuvassa kamppailussa länttä vastaan. Erityisesti tämä näkyy kyber- ja informaatioympäristössä, jossa he toteuttavat jatkuvasti operaatioita sodan kynnyksen alapuolella. Yksi esimerkki venäläisestä ajattelusta on

tarvittaessa irrottaa Internetin venäläinen segmentti muusta Internetistä. Tämä kyvykkyys on jo testattu.

Venäjälle kyber/informaatiosodan tavoitteena on

- Tappioiden tuottaminen informaatiojärjestelmille, prosesseille ja resursseille, kriittisesti tärkeille ja muille rakenteille
- Poliittisten, taloudellisten ja sosiaalisten järjestelmien lamauttaminen
- Massamainen psykologinen operointi yhteiskunnan ja valtion epätasapainoon saattamiseksi
- Valtion pakottaminen tekemään vastustajalle edullisia päätöksiä.

Ns. Gerasimovin doktriinin mukaan sodankäynnin tavoitteena on vastustajan sotilaallisen ja taloudellisen potentiaalin vähentäminen tuhoamalla vastustajan sotilaallisen ja yhteiskunnan infrastruktuurin kriittiset rakenteet lyhyessä ajassa.

2. Toimijoita ja operaatioita kybertilassa

Selonteko viittaa hybridiuhkien yhteydessä valtiollisiin tai muihin ulkoisiin toimijoihin. Uhkien kannalta tarvitaan analyysi eri toimijoiden motiiveista, jotta turvaamistoimenpiteet voidaan mitoittaa oikein. Vaikuttamista kriittisen infrastruktuuriin ja yhteiskunnan elintärkeisiin toimintoihin tapahtuu eri tavoittein normaaliaikoina. Kybertilassa ilmenee vastaavia uhkailmiöitä kuin fyysisessä maailmassa: anarkiaa, rikollisuutta, vakoilua, terrorismia, sabotaasia ja asevoimien operaatioita.

Kriittinen infrastruktuuri on lisääntyvän toiminnan kohteena. Kybersabotaasissa hyökkääjä operoi tavalla, jolla pysyttäydytään sodan kynnyksen alapuolella. Tavoitteina voivat olla epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäyskykyjen testaaminen, hybridioperaatioiden valmistelu tai sodan valmistelu.

Esimerkiksi Stuxnet-operaatiossa 2009–2010 verkkomato pääsi Iranin ydinpolttoainerikastamoon ja sen sentrifugien taajuushallintajärjestelmään. Hallintajärjestelmän kautta vaikutettiin sentrifugien toimintaan niin, että rikastusprosessi epäonnistui.

Joulukuussa 2015 hakkerit iskivät ukrainalaiseen energiayhtiöön ja onnistuivat katkaisemaan sähkönjakelun. Tämä usealla eri tavalla toteutettu kyberhyökkäys jätti 225 000 ukrainalaista ilman sähköä kuudeksi tunniksi. Samanlainen hyökkäys toteutettiin Kievin alueella joulukuussa 2016.

Kesäkuussa 2017 Petya/NonPetya-haittaohjelma saastutti Ukrainassa M.E.Doc -kirjanpito-ohjelmiston, jonka kautta se levisi nopeasti ukrainalaisiin ja kansainvälisiin toimijoihin, joilla yhteys tuohon ohjelmaan. Ukrainassa mm. pankit, ministeriöt,

sanomalehdet ja sähköyhtiöt joutuivat kohteeksi. Operaatio naamioitiin kiristyshaittaohjelmaksi, mutta hyökkäyksen todellinen tarkoitus oli lamauttaa yhteiskunnan kriittisiä toimintoja ja aikaansaada poliittista epävakautta tai testata hyökkäysoperaation toimivuutta. Tähän saakka hyökkäyksestä aiheutuneet kustannukset ovat olleen noin 10 miljardia dollaria.

Em. esimerkit osoittavat, kuinka kriittistä infrastruktuuria vastaan hyökätään ja aiheutetaan vakavia vaurioita yhteiskunnan elintärkeille toiminnoille ja pahimmassa tapauksessa ihmisten hengelle ja terveydelle jo normaaliaikoina.

Kybertilassa toteutetaan operaatioita päivittäin. Viime vuonna tuotettiin yli 1,2 miljardia haittaohjelmaa. Päivittäin löydetään yli 350 000 uutta haittaohjelmaa ja kun mukaan lasketaan vanhojen haittaohjelmien variantit, niin vastassamme on yli 3 miljoonaa haittaohjelmaa joka päivä.

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia tehdä kehittyneempiä hybridihyökkäyksiä, joissa yhteiskunnan haavoittuvuuksia hyödynnetään erilaisten kyberhyökkäysten, kriittisen infrastruktuurin sabotoinnin ja informaatio-operaatioiden avulla.

3. Kriittisen infrastruktuurin suojaaminen

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 suojaaminen tarkoittaa yksittäisten järjestelmien ja keskinäisriippuvien systeemikokonaisuuksien turvaamista niin, että yhteiskunnan elintärkeät toiminnat voidaan turvata normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa.

Kriittisen infrastruktuurin turvaamisessa on kolme ulottuvuutta:

- Poliittinen
- Taloudellinen
- Tekninen

Poliittinen ulottuvuus kuvaa kansallista intressiä turvata kriittinen infrastruktuuri. Poliittiseen ulottuvuuteen kuuluu kansallinen lainsäädäntö ja kansalliset turvallisuustarpeet sekä kansainvälinen yhteistyö näiden ympärillä. EU on asiakirjoissaan korostanut kaikkien jäsenvaltioiden velvollisuutta edistää kyberturvallisuusvalmiuksia, koska kriittiset infrastruktuurit ja useat digitaaliset palvelut ulottuvat koko EU:n alueelle yli kansallisten rajojen. Näin yhtenäinen lainsäädäntö ja kyberturvallisuuspolitiikka mahdollistavat teknisen yhteistyön tilanteissa, joissa infrastruktuurit ovat usean maan yhteiset.

Taloudellinen ulottuvuus käsittää kaikki yritykset ja taloudelliset toimijat, jotka rakentavat, omistavat ja hallinnoivat infrastruktuurijärjestelmiä ja -laitoksia ja jotka toimivat taloudellisten intressien mukaisesti. Taloudelliseen ulottuvuuteen kuuluu myös turvaamiskustannusten oikeudenmukainen jakaminen eri toimijoiden kesken. Suomessa merkittävin osa kriittisestä infrastruktuurista on yksityisessä ja osin monikansallisessa omistuksessa. Omistajilla on keskeinen vastuu kriittisen infrastruktuurin kyberturvallisuudesta.

Teknologinen 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.

Vahva kansallisen kriittisen infrastruktuurin kyberturvallisuusohjelman avulla varmistettaisiin yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa olosuhteissa. Ohjelmassa tulisi olla poliittinen, taloudellinen ja teknologinen ulottuvuus

4. Informaatiovaikuttamisen torjunnan kehittäminen

Selonteko mainitsee informaatiovaikuttamisen osan globaaleja haasteita ja toteaa lisäksi, että kyberpuolustuksen kehittämisen lisäksi toimintaympäristön muuttuminen korostaa tarvetta informaatiopuolustuksen eli väärän tiedon oikaisemisen ja tiedon eheyden varmistamisen laaja-alaiselle kehittämiselle. Näihin haasteisiin vastataan kokonaisturvallisuuden periaatteen mukaisesti.

Kenen vastuulla on yhteiskuntaan kohdistuvan informaatiovaikuttamisen torjunnan toteuttamisesta? Kuinka hoidetaan normaaliaikoina esiintyvien informaatio-operaatioiden torjunta. Selonteosta saa vaikutelman, että kyber- ja informaatio-operaatiot nähdään kriisinhallinnan näkökulmasta, vaikka informaatiovaikuttamisesta on tullut arjen uusi normaali.

Eri toimijat yhteiskunnassa pyrkivät omilla vastuualueillaan torjumaan disinformaatiota, sekä aggressiivista ja anonyymiä vaikuttamista Internetissä. Tässä riippumaton, itsenäinen media on avainasemassa ja osa yhteiskunnan informaatiopuolustusta.

Em. Euroopan komission tiedonannossa (Yhteinen kehys hybridiuhkien torjumiseksi, 2016) todetaan, että ”On hyvin tärkeää, että hybridiuhkiin kyetään vastaamaan pätevällä strategisen viestinnän strategialla. Yhteiskunnan valmiuksia vastata hybridiuhkiin voidaan parantaa ensisijaisesti antamalla nopeasti asiatietoihin perustuvia vastauksia ja lisäämällä yleistä tietoisuutta.”

Kansallinen informaatiovaikuttamisen torjunnan/informaatiopuolustuksen ohjelman ja toimenpiteiden avulla varmistettaisiin yhteiskunnan toimintakyky sekä normaaliaikoina että poikkeusoloissa. Ohjelman tulisi tuottaa

informaatiovaikuttamisen torjunnan/informaatiopuolustuksen kansallisen strategisen johtamisen rakenteet ja vastuun jakamisen periaatteet.

5. Kyberturvallisuuden strategisen johtamisen haaste

Selonteko käsittelee kyberturvallisuutta globaalien haasteiden ja muutosilmiöiden näkökulmasta sekä kriisinsietokyvyn vahvistamisella. Selonteossa olisi voinut omassa (ala)luvussaan kootusti käsitellä Suomen resilienssin vahvistamista kyber- ja informaatio-operaatioita vastaan. Pelkkä kriisilähtöinen tarkastelu ei ole riittävä, kun kysymys on arjen turvaamisesta.

Keskeisin haaste kansallisen kyberturvallisuuden toteuttamisessa on toiminnan hajautuminen laajalle eri toimijoiden vastuulle. Kokonaisturvallisuus on varautumisen yhteistoimintamallimme, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä.

Kyberturvallisuus on osa yhteiskunnan kokonaisturvallisuutta. Kyberturvallisuusasiat ja informaatiovaikuttaminen näyttäytyvät nykyisin arkisina niin kriittisen infrastruktuurin ja yrityksien kuin kansalaisten piirissä. Kyberturvallisuuden strateginen johtaminen on tätä arjen toimintaa laajempi kokonaisuus käsittäen myös kansallisen turvallisuuden ja suvereniteetin kybertilassa.

Kyberturvallisuuden strategisen johtaminen on valtion kyvykkyyksien ja elintärkeiden toimintojen turvaamista sekä normaaliaikoina että poikkeusoloissa. Normaaliaikana rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliaikojen häiriötilanteiden hallinnassa.

Kyberturvallisuusuhkat näyttäytyvät myös yhä merkittävämpänä osana hybridivaikuttamisessa. Uhkien välisten suhteiden ymmärtäminen edellyttää vahvaa ja keskitettyä havainnointi-tilannekuva-johtamisen kyvykkyyttä. Kyberturvallisuuden strategisessa johtamisessa tarvitaankin tilanneymmärrystä, selkeitä johtamisvastuita ja -rooleja, saumatonta tiedonkulkua ja -vaihtoa sekä lainsäädännön ajanmukaisuutta.

Suomessa on kehitys mennyt merkittävästi eteenpäin vuoden 2013 kyberturvallisuusstrategian julkaisemisen jälkeen. Eri vastuutahot ovat vahvistaneet omaa kyberkyvykkyyttään. Siviili- ja sotilastiedustelulainsäädännön uudistus vuonna 2019 on antanut viranomaisille mahdollisuuksia kybertiedustelun torjuntaan.

Liikenne- ja viestintäministeriön alaisen Kyberturvallisuuskeskuksen tuottamilla tilannekuva-, havainnointi sekä arviointi- ja hyväksyntäpalveluilla on merkittävästi autettu eri toimijoita kyberturvallisuuden toteuttamisessa.

Kuitenkin Suomen suhteellinen asema hyvänä kyberturvallisuusmaana on heikentynyt vuodesta 2012 lähtien. Erilaisilla kansainvälisillä indekseillä mitataan maiden kyberturvallisuuskyvykkyyttä ja näissä arvioinneissa maamme asema suhteessa muihin on alentunut. Euroopassa olemme pudonneet kärki viisikosta kärkikymmenikköön ja globaalissa vertailussa kärkikymmeniköstä kahdenkymmenen joukkoon. Meidän absoluuttinen tuloksemme on parantunut, mutta muut ovat parantaneet suoritustaan vieläkin enemmän. Toisin sanoen toimenpiteemme eivät kaikilta osin ole olleet riittävän vaikuttavia.

Koska kyber on kaikkialla, tarvitaan kansallinen kyberturvallisuuden strateginen johtamismalli, joka tukisi kyberturvallisuuden kokonaisvaltaista varautumista kehittämistä ja laajamittaisten häiriötilanteiden hallintaa.

6. Asejärjestelmien autonomia

Selonteon mukaan ”Täysin autonomisia, kokonaan ihmisen kontrollin ulottumattomissa olevia asejärjestelmiä ei pidä kehittää jatkossakaan.”

Ilmaus on kovin epämääräinen. Tarkoitetaanko, ettei Suomi jatkossakaan näitä asejärjestelmiä kehitä vai maailmalla yleensäkään niitä ei pidä kehittää. Mitä tarkoitetaan ”ihmisen kontrollin ulkopuolella”. Ihmisen osallisuus asejärjestelmässä on jo nykyisellään moniulotteinen ja -muotoinen. Tällä hetkellä on jo käytössä asejärjestelmiä, joiden toiminnan autonomia-aste on hyvin suuri. Erityisesti ohjus- ja rakettitorjunnassa on käytössä täysin autonomisia torjunta-aseita, koska aikaa ihmisen torjuntapäätöksenteolle ei ole.

Esimerkiksi Phalanx-asejärjestelmä on autonominen tutkaohjattu tykki, joka on tarkoitettu torjumaan meri- ja maamaaliohjuksia. Iron Dome on täysin autonominen ohjusten ja rakettien torjuntajärjestelmä. Tutkia vastaan tarkoitettu Harpy on täysin autonominen ase, joka voi tarvittaessa 2,5 tunnin ajan hakea itsenäisesti maalia kohdealueelta.

Kaikki suurvallat rakentavat älykkyyttä pitkän kantaman ohjusjärjestelmiin ja risteilyohjuksiin. Älykkyyden ja autonomisuuden rakentamista asejärjestelmiin ei voi pitää yksiselitteisesti huonona asiana. Tällä kehityksellä voidaan pienentää sivullisille aiheutettuja vahinkoja (ihmiset ja rakenteet) ja omille aiheutettuja tappioita. Nopeissa tilanteissa niin fyysisessä kuin kybertaistelutilassa vaaditaan kykyä nopeaan vasteeseen, jolloin torjuntajärjestelmien itsenäistä ja autonomista toimintakykyä tarvitaan.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi