Martti Lehto, Jyväskylän yliopisto
25.2.2021

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.”

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.”

Kybermaailman kehitys ei ole ollut irrallinen ilmiö vaan se yhdistyy vahvasti yhteiskuntarakenteisiin ja eri turvallisuustoimijoiden tarpeisiin ja odotuksiin. Kehitykselle on ominaista nopeus sekä tietynlainen arvaamattomuus tulevaisuudesta.

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.”

SUOSITUS: *Kyberhyökkäykset ylittävät kansallisvaltioiden rajat, joten tarvitaan laajempi ja kattavampi tilannetietoisuus kybertoimintaympäristöstä ml. tiedonvaihtomekanismit.*

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.

SUOSITUS: *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

Digitaalisen maailman 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. Digitaalisessa maailmassa voidaan vaikuttaa etäältä anonymiteetin suojassa ja attribuution tavoittamattomissa.

Digitaalisessa toimintaympäristössä 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.

2. Kyberoperaatioista

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.

2.1 Määrittelyä

Kybersodankäynnissä käytetään perinteisen kineettisen vaikuttamisen rinnalla kyberoperaatioita digitaalisen toimintaympäristön kohteissa = kriittinen infrastruktuuri.

Rauhan aikaisessa kybervaikuttamisessa toteutetaan tiedustelu-, häirintä, lamautus- ja tuhoamisoperaatioita sodan kynnyksen alapuolella tavoitteena epävakauden lisääminen, suorituskyvyn testaus, sodankäynnin valmistelu. Tässä kybersabotaasissa tavoitteina voivat olla epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäyskykyjen testaaminen, hybridioperaatioiden valmistelu tai sodan valmistelu.

Uhkien kannalta tarvitaan analyysi eri toimijoiden motiiveista, jotta turvaamistoimenpiteet voidaan mitoittaa oikein. Vaikuttamista kriittisen infrastruktuuriin ja yhteiskunnan elintärkeisiin toimintoihin tapahtuu eri tavoittein normaaliaikoina: anarkiaa, rikollisuutta, vakoilua, terrorismia, sabotaasia ja asevoimien operaatioita.

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 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. 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.

2.2 Kyberturvallisuuden strateginen johtaminen

Keskeisin haaste kansallisen kyberturvallisuuden toteuttamisessa on toiminnan hajautuminen laajalle eri toimijoiden vastuulle. Kokonaisturvallisuus on varautumisen yhteistoimintamallimme. Kyberturvallisuus on osa yhteiskunnan kokonaisturvallisuutta. Kyberturvallisuus 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.

Uusien 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. 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.

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

SUOSITUS: *Tarvitaan kansallisen kriittisen infrastruktuurin kyberturvallisuusohjelma, jolla varmistettaisiin yhteiskunnan elintärkeiden toimintojen turvaaminen kaikissa olosuhteissa. Ohjelmassa tulee olla poliittinen, taloudellinen ja teknologinen ulottuvuus.*

3. Hybridioperaatioista

Selonteon mukaan ”Hybridivaikuttaminen on lisääntynyt ja monimuotoistunut, minkä takia siitä on tullut aiempaa suurempi turvallisuusuhka.” Linjaus ilmentää hyvin vallitsevaa tilannetta.

Hybridioperaatioita toteuttavat sekä valtiolliset toimijat että muutkin toimijat. Vastustajille on äärimmäisen houkuttelevaa kokeilla hybridioperaatioiden eri menetelmiä, koska niissä on suhteellisen pieni kiinnijäämisriski verrattuna perinteisiin sotilaallisiin operaatioihin tai muihin vaikuttamismenetelmiin.

Digitaalinen toimintaympäristö ja miehittämättömyys ovat alentaneet sodankäynnin kynnystä samalla muuttaen perinteistä sota-rauha-asetelmaa. Kylmän sodan aikana luotiin käsite harmaasta vaiheesta, jolla ymmärrettiin aikaa ennen varsinaista sotaa. Hybridisodankäynti on tuonut tilan, joka voi edeltää perinteistä sotaa, ilmetä sodan aktiivisen vaiheen jälkeen tai ilman perinteistä sodankäyntiä. Uusi sodankäynnin paradigma on syrjäyttämässä perinteisen mallin sodan julistamisesta rauhan sopimukseen luomalla tilan, jossa sotaa ei julista eikä rauhaa solmita, vaan hybridisodankäynnin kohde joutuu elämään hyvinkin pitkään konfliktin ja epävakauden keskellä, jossa yhä enenevässä määrin digitaalinen toimintaympäristö on toiminnan kohteena.

Hybridioperaatioiden havaitseminen ja estäminen olisi tehtävä varhaisessa vaiheessa, ennen kuin hyökkääjä ottaa käyttöönsä koko hybridimenetelmien arsenaalin. Hybridioperaatioiden havaitsemiskykyä (varhaisvaroitus) on parannettava, jotta vastustajan toiminta ja vaikuttamisyritykset voidaan lopettaa ennen kuin ne ovat kunnolla alkaneetkaan.

SUOSITUS: *Lisätään tilannetietoisuutta hybridiuhkista ja tehostetaan alan tutkimusta ja tiedonvaihtoa.*

4. Informaatio-operaatioista

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.

Informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista –> informaatioylivoiman hankkiminen.

Jo rauhan aikana informaatiovaikuttamisella pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn eri kampanjoiden avulla –> informaatiotilan hallinta.

Esimerkiksi Venäjälle kyber/informaatiosodankäynnin 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.

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.”

SUOSITUS: *Tarvitaan kansallinen informaatiovaikuttamisen torjunnan/informaatiopuolustuksen ohjelma, jonka avulla varmistettaisiin*

yhteiskunnan toimintakyky sekä normaaliaikoina että poikkeusoloissa. Ohjelman tulisi tuottaa informaatiovaikuttamisen torjunnan/informaatiopuolustuksen kansallisen strategisen johtamisen rakenteet ja vastuun jakamisen periaatteet.

5. 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. Nykyisin on 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 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.

6. Lopuksi

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia tehdä kehittyneempiä hybridioperaatioita, joissa yhteiskunnan haavoittuvuuksia hyödynnetään erilaisiin kyberoperaatioihin, kriittisen infrastruktuurin sabotointiin ja informaatiovaikuttamiseen sotilaallisten ja poliittisten tavoitteiden saavuttamiseksi. Siksi tarvitaan kansallinen ohjelmakokonaisuus (hybridi-kyber-informaatio) turvaamaan yhteiskunnan elintärkeitä toimintoja normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi