Martti Lehto, Jyväskylän yliopisto
7.10.2024

Eduskunnan puolustusvaliokunta

Asia: VNS 3/2024 vp Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko

1. TEKNOLOGIAN VAIKUTUS KEHITYSKULKUIHIN

Selonteko toteaa alaluvussa 2.4, että murroksellisten teknologioiden ja sovellusten hyödyntämisellä on mahdollista saavuttaa merkittäviä kehitysvaikutuksia eri sektoreilla. Samaa teemaa käsitellään alaluvussa 2.5 sääntöpohjaisuuden näkökulmasta ja alaluvussa 3.1.2 määriteltäessä painopisteitä kehittämistä.

Autonomiset järjestelmät, virtualisaatio, tekoälyn kehitys, nanomateriaalit, bioteknologia ja energiateknologia ovat esimerkkejä teknologioista, joiden merkitystä toimintaympäristölle ei voi ylikorostaa. Selonteon toteamus siitä, että tekoälyn kehitys tekee kyberhyökkäyksistä, informaatiovaikuttamisesta ja disinformaatiosta entistä kohdennetumpaa ja vaikuttavampaa, kuvaa hyvin vallitsevaa tilannetta.

Selonteko näkee teknologisen kehityksen tuovat vihamielisille toimijoille tehokkaita mahdollisuuksia hybridivaikuttamiseen sodan kynnyksen alapuolella. Hybridi-, kyber- ja informaatio-operaatioita toteutetaankin jatkuvasti, siksi tarvitaan rauhan ja sodan ajan käsitteiden uudelleen tarkastelua.

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja korkean käyttövarmuuden omaavista sähköjärjestelmistä, tiedonsiirtoverkostoista ja satelliittijärjestelmistä sekä muista luotettavista ja tietosisällöltään eheistä hallinnon ja kansalaisten palveluista.

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia toteuttaa yhä kehittyneempiä kyberoperaatioita, joilla on sotilaallisia, poliittisia ja taloudellisia tavoitteita. Äärimmillään yhteiskunnan haavoittuvuuksia hyödynnetään kyberoperaatioissa kriittisen infrastruktuurin sabotoimiseen, lamauttamiseen ja tuhoamiseen.

Murrosteknologioiden vaikutus näyttäytyy kaikkialla yhteiskunnan eritoiminnoissa ja digitalisaation edistyessä sen merkitys yhä enemmän vahvistuu.

2. RAUHAN JA SODAN PARADIGMAN MUUTOS

Tarvitaan sodan ja rauhan käsitteiden uudelleen määrittelyä digitalisoituneessa maailmassa.

Perinteinen rauha-sota-asetelma on digitalisaatiokehityksen myötä muuttunut epämääräiseksi, ennustamattomaksi ja epävakaaksi ulko- ja turvallisuuspolitiikan toimintaympäristöksi. Perinteisesti sodankäynnissä valtiolliset toimijat käyttävät fyysistä voimaa toisiaan vastaan jatkaen sillä poliittista toimintaan alistaakseen vastustaja taipumaan tahtoonsa. Traditionaalisen määrittelyn mukaan sotatila ilmentyy sodan osapuolten välillä ja se alkaa joko muodollisella sodanjulistuksella (Ison-Britannian sodan julistus Saksalle syyskuussa 1939) tai aseellisen toiminnan aloittamisella (Venäjän hyökkäys Ukrainaan 24.2.2022). Sotatila päättyy aselepoon ja rauhantekoon.

Rauhan ja sodan väliin on muodostunut osapuolten ulko- ja turvallisuuspolitiikan kriisiytymisvaihe – harmaa vaihe, jossa osapuolet punnitsevat avoimen sodan hyötyjä ja haittoja. Tämän vaiheen erilaiset toiminnat/operaatiot määritellään hybridivaikuttamiseksi.

Venäjä on omassa retoriikassaan todennut olevansa sodassa lännen kanssa. Tämä näkökulma muuttaa edellä kuvattua perinteistä sota-rauha-näkökulmaa. Venäjälle sotatila on keskeinen (normaali) olotila, jonka intensiivisyysasteet vaihtelevat.

Uudessa sodankäynnin paradigmassa valtioiden välille on muodostunut asetelma, jossa sotaa ei julisteta eikä rauhaa solmita. Meillä voi olla epävakaa rauhan tila (ei avointa sotaa). Tämä epävakaus voi kriisiytyä ja johtaa hyvinkin aggressiiviseen hybridivaikuttamiseen eri muodoissaan. Tällainen kriisi voi edelleen eskaloitua avoimeksi sodaksi, jossa käytetään perinteisten kineettisten keinojen (maa, meri, ilma) ohella ei-kineettisiä keinoja (kyberoperaatiot, informaatio-operaatiot, elektronisen sodankäynnin operaatiot ja uutena kognitiivisen vaikuttamisen operaatiot).

Yhteiskunnissa muodostunut digitaalinen kyber- ja informaatioympäristö, jossa voidaan operoida pysyen sodan kynnyksen alapuolella ja toimijoiden attribuution ulottumattomissa, kuten selonteko toteaa. Tämä uusi toimintaympäristö mahdollistaa hyökkääjälle tilan vaikuttaa toisen valtion alueella käyttäen hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi.

3. DIGITAALINEN KYBERTOIMINTAYMPÄRISTÖ

Suomalainen yhteiskuntaa on digitalisoitu voimakkaasti. Tähän ovat vaikuttaneet sekä poliittiset linjaukset että digiteknologian laitteiden ja palveluiden kaupallinen kehitys. Kansalliseen turvallisuuteen ja kansalaisten turvallisuuteen voidaan digitaalisesti vaikuttaa kahta kautta. Digitaalisen maailman toimintaa voidaan häiritä teknisesti, jolloin puhutaan usein kyberoperaatioista kybermaailmassa. Digitaalisen maailman kautta voidaan vaikuttaa myös informaatioon ja sitä kautta eri toimijoiden arvoihin, asenteisiin ja päätöksentekoon. Tällöin puhutaan informaatiovaikuttamisesta

Kansallinen kybertoimintaympäristö koostuu useista eri toimijoista ja toimintokokonaisuuksista. Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on selkeästi määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen. Kybertoimintaympäristössä voidaan nähdä kuusi eri ulottuvuutta, jotka eivät kaikilta osin noudata valtion fyysisiä rajoja.

3.1 Poliittinen ulottuvuus

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu kyberasioiden poliittinen luonne (engl. cyber politics). Kybertoimintaympäristö itsessään ja siihen vaikuttaminen ovat voimakkaassa muutoksen tilassa, ja tätä kehitystä pyritään poliittisin keinoin ohjaamaan. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä kuten EU:ssa, NATO:ssa ja OECD:ssä. Kyberturvallisuudessa etenkin valtioiden välisen luottamuksen lisääminen on keskeinen kysymys. Siihen pyritään tiivistämällä valtioiden välistä keskustelua kybertoimintaympäristöön liittyvistä kysymyksistä niin monenvälisesti, alueellisesti kuin kahdenvälisestikin.

Kybertoimintaympäristö ja kyberturvallisuus on noussut tärkeäksi osaksi Suomen ulko- ja turvallisuuspolitiikkaa. Koska kyberuhat eivät tunne valtioiden rajoja, tarvitaan kyberturvallisuuden vahvistamiseksi ennen kaikkea kansainvälistä yhteistyötä.

3.2 Sotilaallinen ulottuvuus

Kybertoimintaympäristö on yhä merkittävämpi tila, jossa vaikutetaan Suomen kansalliseen turvallisuuteen. 2020-luvun sodankäyntiin kuuluvat kyberoperaatiot elimellisenä osana maa-, meri-, ilma- ja avaruusoperaatioiden rinnalla. Hybridivaikuttamiseen liittyy uusia kyberoperaatioelementtejä, joiden tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpitoa voidaan toteuttaa kyberoperaatioiden avulla rauhan ja sodan aikana. Sodan aikana kyberoperaatioilla pyritään häiritsemään, lamauttamaan ja tuhoamaan vastustajan siviili- ja sotilasinfrastruktuuria sekä tiedustelun, valvonnan ja johtamisen järjestelmät ja asejärjestelmien toiminta.

3.3 Yhteiskuntaulottuvuus

Yhteiskuntaan kohdistuvan kyberuhan kohteista keskeisiä ovat yhteiskunnan elintärkeät toiminnot, joilla turvataan kansalaisten elinmahdollisuudet. 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. Nämä verkostot eivät ole erillisiä entiteettejä vaan muodostava kansallisen kriittisen infrastruktuuriverkoston, jossa on paljon keskinäisriippuvuuksia. Yhden systeemin lamaantuminen tai romahtaminen vaikuttaa verkoston muihin osiin.

3.4 Kansalaisulottuvuus

Teknistaloudellinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Digitalisaatio on synnyttänyt työtä ja kansalaisten elämää helpottavia uusia innovaatioita. Tietoliikenteen, tietojärjestelmien ja viestinnän toimintavarmuus onkin nykyaikaisen yhteiskunnan häiriöttömän toiminnan, turvallisuuden ja kansalaisten toimeentulon välttämätön edellytys. Kyse on kansalaisten luottamuksen ylläpitämisestä yhteiskunnan digitaalisten palveluiden toimintaan.

3.5 Taloudellinen ulottuvuus

Taloudellisen ulottuvuuden keskeisiä elementtejä ovat organisaatioiden kyberturvallisuusinvestoinnit, onnistuneiden kyberhyökkäysten kustannukset organisaatiolle, pitkän aikavälin vaikutukset valtiontaloudelle, ja kyberturvallisuuden parantamisen kustannukset eri tasoilla. Makrotalouden vakauden arvioinnissa on perusteltua ottaa huomioon myös kyberturvallisuuteen liittyvät riskit.

3.6 Teknologinen ulottuvuus

Digitalisaatiosta on tullut yhä tärkeämpi osa yritysten ja ihmisten toimintaa. Digitaalisuus on tänä päivänä myös yhä syvemmällä ihmisten ja yritysten arjessa; digitaaliset palvelut helpottavat yritysten ja ihmisten arkea ja elämää. Digitaalisuuteen pohjautuvia innovaatiomahdollisuuksia syntyy yhä enemmän. Digitaalinen kybermaailma houkuttelee rikollisia, jotka etsivät uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa. Tiedon ja informaation siirtyminen verkkoon on tuonut sinne myös tiedusteluorganisaatiot. Terroristeille kybermaailma on yhteydenpidon, viestinnän ja vaikuttamisen toimintaympäristö, minkä lisäksi se on heille houkutteleva hyökkäyskohde. Asevoimien digitalisaatio on luonut sotilaallisen kybermaailman, jossa vaikuttavat verkottuneiden sotilaiden lisäksi älykkäät ja yhä itsenäisemmät asejärjestelmät.

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. Tähän liittyy selonteossa kuvattujen murrosteknologioiden merkityksen kasvu.

YHDISTELMÄ

Kyberhyökkäykset, haittaohjelmat, palvelunestohyökkäykset ja erilaiset informaatiovaikuttamisen muodot lisääntyvät jatkuvasti. Tämän kehityksen vuoksi on lisättävä edelleen varautumista kyberuhkiin ja -häiriötilanteisiin, jotka vaarantavat yhteiskunnalle välttämättömien tietoteknisten järjestelmien ja rakenteiden toimivuutta

jo normaalioloissa. Suomalaisen yhteiskunnan ja yritysten riippuvuus kybertoimintaympäristöstä kasvaa entisestään tulevina vuosina.

Nykyään taloudellisiin hyötyihin tähtäävien kyberrikollisten ja kehittyneiden valtion sponsoroimien hyökkääjien toiminta ja kyvykkyystaso eivät ole vain hämärtyneet - niitä ei enää ole olemassa. Kyberhyökkäystekniikat ja -työkalut ovat laajasti levinneet eri motivaatioilla toimivien kyberhyökkääjien käyttöön. On tapahtunut konvergenssi, jossa toimijoiden nimeäminen/syyksilukeminen (attribuutio-ongelma) ja heidän motivaationsa paljastaminen on yhä vaikeampaa.

Tulevaisuuden digitaaliset palvelut perustuvat ihmisten, innovatiivisten toimijoiden ja älykkäiden koneiden ekosysteemiin. Kehittyvässä digitaalisessa yhteiskunnassa mahdollisuuksien tila laajenee. Digitaalitalouden kehitystä edistävät kansalaisten identiteetin ja tietokäytäntöjen siirtyminen verkkoon sekä organisaatioiden palvelurakenteiden digitalisaatio yhdistettynä luottamukseen systeemin turvallisuudesta. Näin muodostuu digitaalinen alustatalous, jossa elementteinä ovat teollinen internet, erilaiset sosiaalisen median ja viestinnän alustat sekä hajautetut ja yhteisölliset palvelut. Kansalaisten elämä pyöriikin yhä enemmän ja enemmän interaktiivisten älypuhelinten, -tietokoneiden, -sovellusten, -autojen ja -kotien ympärillä. Samalla se tarkoittaa sitä, että myös rikollisuus ja tiedustelu ovat siirtyneet verkkoon.

Kansallinen kyberturvallisuus on keskeinen osa kokonaisturvallisuutta, johon meidän on kyettävä osallistamaan eri toimijat sekä yhteensovittamaan voimavarat ja toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi. Kyse on koko yhteiskunnan kyberkyvykkyyden kehittämisestä kriittisen infrastruktuurin suojaamiseksi ja kansalaisten elintärkeiden toimintojen turvaamiseksi – resilienssin vahvistamista.

Digitaalinen kyber- ja informaatioavaruus on luonut uuden ja merkityksellisen ulko- ja turvallisuuspolitiikan toimintaympäristön. Tässä ympäristössä on läsnä perinteisiä ulko- ja turvallisuuspolitiikan muotoja mutta myös kokonaan vain sille tyypillisiä elementtejä.

Tutkimusjohtaja, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi