Kirjallinen lausunto 5.2.2021
Jarno Limnéll
Aalto-yliopisto

Eduskunnan tulevaisuusvaliokunta

VNS 4/2020 vp Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko

Selontekomenettely on vakiintunut Suomessa tavaksi linjata maamme ulko- ja turvallisuuspolitiikkaa kerran hallituskaudessa. Samalla on vakiintunut 1990-luvun puolivälistä alkaen tapa arvioida turvallisuutta ja turvallisuuspolitiikkaa laajan turvallisuuskäsityksen perustalta, mikä on välttämätöntä nykymaailmassa, jossa erilaiset uhkat ja riskit kietoutuvat yhä tiiviimmin toisiinsa. Tuoreinkin selonteko nojaa laajaan turvallisuuskäsitykseen todetessaan, että ”Suomi tarkastelee turvallisuutta laajasta näkökulmasta (s. 24).” Turvallisuuspolitiikan sisältöä ja turvallisuuden käsitettä voi selonteossa katsoa laajennetun entisestään.

Keskinäisriippuvaisuuksien maailmassa turvallisuutta on luonnollisesti tarkasteltava laaja-alaisesti. Samalla kuitenkin on myös arvioitava kriittisesti, että mitkä uhat ja ilmiöt tulisi lukea turvallisuuspolitiikan piiriin ja vastata turvallisuuspolitiikan keinoin. Sama koskee laajemminkin tämän päivän uhkapuhuntaa. Lähes kaikista huolista, murheista ja ongelmista puhutaan tänä päivänä uhkina. Liiallinen uhkapuhunta luo tarpeetonta turvattomuuden tunnetta, ja toisaalta liiallinen uhkiksi kutsuttavien asioiden määrä saattaa viedä huomion sivuun todellisista ja tärkeimmistä uhkaavista tekijöistä. Suuntauksena kuitenkin lähitulevaisuutta arvioitaessa on se, että uhkaksi kutsuttavien asioiden määrä tulee entisestään lisääntymään. Kyky uhkien priorisointiin sekä uhkien toteutumisen vaikutuksien arviointiin korostuu. Sama koskee selonteossa esitettyjen tavoitteiden priorisointia. Esimerkiksi sana ”tärkeä” mainitaan selonteossa 54 kertaa, mikä hankaloittaa oleellisen ymmärtämistä ja priorisointia.

Uhkien määrittelyssä on tarvetta maltillisuudelle, eikä kaikkia nousevia haasteita tulisi välttämättä nähdä turvallisuuspoliittisina uhkina. Etenkään siis uhkia, joihin pitäisi vastata turvallisuuspolitiikan keinoin. On kuitenkin välttämätöntä arvioida erilaisia uhkailmiöitä ja -tekijöitä, sillä se on varautumisen perusta. Jos emme ymmärrä uhkia, emme pysty niihin oikealla tavalla varautumaan. Uhkia ei myöskään saa tarpeettomasti vähätellä. Toteutuessaan uhkan vaikutus on pienempi, kun siihen on oikealla tavalla varauduttu.

Lisääntyneestä laajan turvallisuuden uhkapuheesta huolimatta, voi viime vuosien kehitystä kuvata Euroopassa kovan turvallisuuden comeback:nä. Muiden muassa sodat Ukrainassa ja Lähi-idässä osoittavat, että avointa sotilaallista toimintaa painottava geopolitiikka on voimissaan. Sotilaalliset

uhkakuvat eri muodoissaan koetaan jälleen ajankohtaisiksi ja moni länsimainen valtio ”korjannut” turvallisuusstrategioitaan.

Samalla on tarpeellista huomioida, että turvallisuusympäristö on monimutkainen, jossa eri asiat ja ilmiöt vaikuttavat toisiinsa. Esimerkiksi ilmastonmuutoksen vaikutukset voivat johtaa sotiin tai terroristit käyttävät kybermaailmaa iskujensa tekemiseen. Koronaviruksen aiheuttama kriisi on puolestaan esimerkki siitä, miten globaali, yhteiskunnan ja yksilön turvallisuus kietoutuvat verkottuneessa maailmassa yhteen. Eri tekijöiden ja ilmiöiden vuorovaikutussuhteita on turvallisuusarvioissa kyettävä yhä paremmin tulkitsemaan, mihin kiihtyvällä vauhdilla kehittyvä teknologia tuo vielä merkittävän lisämausteensa. Tämän päivän turvallisuusympäristö rakentuu monimutkaisista ja toisiinsa kytkeytyvistä tekijöistä, mikä puoltaa uhka-arvioissa laajan lähestymistavan tarpeellisuutta.

Merkittävä piirre turvallisuusarvioissa on aiempien dikotomioiden hämärtyminen. Esimerkkinä käy sodan ja rauhan ajan hämärtyminen pitkäaikaiseksi ja tarkoituksellisiksi niin sanotuksi harmaaksi ajaksi tai erilaisiksi harmaan sävyiksi. Tällöin emme ole selkeästi rauhan tilassa, mutta emme sodassakaan. Tämän sodan ja rauhan välissä olevat ”harmaan sävyt” etenkin kyberympäristössä tapahtuvan päivittäisen vihamielisen vaikuttamisen osalta pakottavat pohtimaan nykyistä turvallisuuspolitiikan peruskäsitteistöä. Hybridisodankäynti on puolestaan luonut tilan, joka voi edeltää perinteistä sotaa, ilmetä sodan aktiivisen vaiheen jälkeen tai ilman perinteistä sodankäyntiä. Tällöin esimerkiksi sotaa ei julisteta eikä rauhaa solmita vaan hybridivaikuttamisen kohde joutuu elämään hyvinkin pitkään epävakauden keskellä, jossa yhä enemmän kybertoimintaympäristö on toiminnan kohteena.

Yhä hämärtyvämmiksi käyvät myös monet muut turvallisuuden dikotomiat, kuten yksilön – yhteiskunnan turvallisuus, sotilaalliset – ei-sotilaalliset uhkakuvat, uudet – vanhat uhkakuvat, sisäinen – ulkoinen turvallisuus sekä digitaalinen – fyysinen turvallisuusympäristö. Turvallisuuden dikotomiat hämärtyvät jatkossa yhä enemmän. Käytännön tasolla turvallisuuden rajojen hämärtyminen pakottaa ”eri turvallisuudet” ja turvallisuustoimijat yhä läheisempään niin kansalliseen kuin kansainväliseen yhteistyöhön. Perinteisiä jakolinjoja ylittävän ymmärryksen merkitys korostuu nykyajassa, kuten myös nopean reagoinnin ja valmiuden kyvykkyydet.

Voimistuvat turvallisuustrendit

Tarkasteltaessa tuoretta selontekoa tämän vuosituhannen aiempiin selontekoihin, voi tiettyjen Suomen ja suomalaisten turvallisuuteen vaikuttavien kehityspiirteiden nähdä voimistuvan uuden vuosikymmenen alussa. Hybridivaikuttaminen on uudessa selonteossa ilmaistu aiempaa painokkaammin. ”Hybridivaikuttaminen on lisääntynyt ja monimuotoistunut, minkä takia siitä on tullut aiempaa suurempi turvallisuusuhka (s. 14).” Havainto ja johtopäätös ovat oikeita. Hybridivaikuttamisen korostaminen kuvastaa sitä, miten halutaan painottaa niitä ”kieroja” toimintatapoja ja monimuotoisia turvallisuusuhkia, joita yhteiskuntaamme ja demokratian rakenteisiin tänä päivänä kohdistuu. Esimerkiksi vaalihäirintä ja siihen liittyvä demokraattisten rakenteiden horjuttaminen muodostavat lähivuosina yhä suuremman uhkan yhteiskunnan vakaudelle ja luottamuksen ylläpitämiselle. Vaikka hybridivaikuttaminen osaltaan yhdistyy Euroopan huonontuneeseen turvallisuustilanteeseen sekä teknologian kehitykseen, kuvaa se myös uudella

tavalla pyrkimystä ymmärtää modernin yhteiskuntamme haavoittuvuuksia sekä uudenlaisiin uhkiin varautumista. Hybridivaikuttamisen keihäänkärkinä voi nähdä kyber- ja informaatiovaikuttamisen. Oleellista myös tässä yhteydessä turvallisuuden näkökulmasta on, ettei yhteiskuntaan synny sellaisia sisäisiä jakolinjoja, joita ulkoinen toimija voisi hyödyntää. Vastaavasti on huolehdittava, ettei jakolinjoja synny ulkoisen vaikuttamisen seurauksena.

Myös kyberasiat osana ulko- ja turvallisuuspolitiikkaa saavat aiheellisesti selonteossa aiempaa vahvemman painostuksen. ”Yhteiskuntien digitalisoituessa on erityisen tärkeää varmistaa kybertoimintaympäristön turvallisuus (s. 37).” Valtion täysivaltaisuuden eli suvereniteetin periaate koskee kiistatta myös kyberympäristöä, jonka kehitykselle on ominaista kiihtyvä muutosnopeus, kompleksisuus ja ennalta-arvaamattomuus. Kyberasioiden merkitys turvallisuudelle ja diplomatialle on kasvava, ja sekä ei-valtiollinen että valtiollinen pahantahtoinen toiminta kyberympäristössä on kasvussa.

Selonteossa lisäksi korostetaan tarvetta informaatiopuolustukselle eli väärän tiedon oikaisemisen sekä tiedon eheyden varmistamista, joskin tämä hyvin olennainen asia jää selonteossa varsin vähäiselle huomiolle. Keskeisimmät tämän vuosikymmen ”kybertaistelut” tullaan käymään ihmisten mielistä, ja tähän alati kehittyvä teknologia mahdollistaa uudenlaisia vaikutuskeinoja.

Kyberpuolustuksen käsittely jää selonteossa varsin vähälle huomiolle, vaikka sen merkitys yhteiskuntamme vakauden ja toimivuuden näkökulmasta on keskeinen. Suomen suvereniteettia haastetaan kybertoimintaympäristössä päivittäin. Asiaa tarkennettaneen myöhemmin puolustusselonteossa. Tässä on tarpeellista huomioida, että alueellisen koskemattomuuden turvaaminen kybertoimintaympäristössä edellyttää myös kybervaikuttamisen ja voimankäytön kokonaisvaltaista tarkastelua. Vaikuttamiskyvykkyyden selkeän toimivaltaperusteisuuden lisäksi on ennalta myös valmisteltava poliittista päätöksentekokyvykkyyttä vihamieliseen kybertoimintaan vastaamiseksi sekä kansallisesti että osana Euroopan unionia. On lisäksi tärkeää, että Suomi korostaa myös kybertoimintaympäristössä kansainvälisen oikeuden noudattamista ja vastuullista valtiokäyttäytymistä. Kybertoimintaympäristön merkitys turvallisuus- ja puolustuspolitiikassa kasvaa.

Kaikkia tämän vuosikymmenen kyber- ja informaatiovaikuttamisen uhkamuotoja emme vielä tiedä, sillä teknologian kehitys on tällä hetkellä nopeampaa kuin koskaan aikaisemmin ihmiskunnan historiassa. Teknologian murros koskettaa kaikkia yhteiskunnan ja politiikan alueita – myös turvallisuudessa. Monia rakenteita, kuten 5G, kuitenkin luodaan tällä hetkellä ja emme saa olla liian sinisilmäisiä. Tehtävillä päätöksillä on kauaskantoisia seurauksia.

Teknologiakysymykset näyttäytyvätkin uudella painoarvolla selonteossa. Esimerkiksi globaalista teknologiaherruudesta on tullut keskeinen suurvaltakamppailun kohde erityisesti Kiinan ja Yhdysvaltojen, mutta myös yksittäisten teknologiajättien, välillä. Teknologiapolitiikka on näissä kamppailuissa kauppapolitiikan sijasta ensisijaisesti ulko- ja turvallisuuspolitiikkaa. Näihin kysymyksiin, kuten myös aseteknologian eettisiin kysymyksiin, Suomi joutuu jatkossa yhä vahvemmin ottamaan kantaa.

Selonteossa painottuu nopeasti muuttuvan turvallisuusympäristökuvauksen myötä yhteiskuntamme kriisinsietokyky. Tämä oleellinen huomio selonteossa. Kriisit ja vakavatkin yhteiskunnalliset

turvattomuustilanteet eivät pääty yhteen viruspandemiaan tai yksittäiseen psykoterapiakeskuksen tietomurtoon. Jatkossa turvallisuudessa korostuu yhä enemmän resilienssi eli sietokyky. Se, että osaamme niin yhteiskuntana kuin yksilöinä sekä toimia että osoittaa henkistä sitkeyttä odottamattomissa tilanteissa.

Suomessa on pitkä perinne siitä, kuinka erilaisia uhkia hallitaan viranomaisten yhteistyön ja koko yhteiskunnan sitouttamisen voimin. Tämä suomalainen kokonaisturvallisuuden malli on kansainvälisesti arvostettu ja mallia kannattaa aktiivisesti edelleen kehittää. On toki huomioitava, että viime vuosina turvallisuus ilmiönä on pirstaloitunut ja muuttunut itsestään selvistä, tutuista tai varsin selkeistä kysymyksistä monimutkaisiksi, eri konteksteissa erilaisia sisältöjä saavaksi hybridiksi, jonka omistajuudesta ja hallinnasta on tarpeellista käydä jatkuvaa arviointia. Nykyhetkessä on tarve kyvylle yhdistää erilaisia näkökulmia, käytännön toimia ja myös tieteenaloja, jotta voimme saada syvempää ymmärrystä tämän hetken uhkien luonteesta ja eri toimijoiden keskinäisestä dynamiikasta sekä varautumisen kehittämisestä.

Jarno Limnéll
Kyberturvallisuuden työelämäprofessori, Aalto-yliopisto