Valiokunnan lausunto HaVL 7/2018 vp– HE 198/2017 vp

Hallintovaliokunta

Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta

Perustuslakivaliokunnalle

JOHDANTO

Vireilletulo

Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta (HE 198/2017 vp): Asia on saapunut hallintovaliokuntaan lausunnon antamista varten. Lausunto on annettava perustuslakivaliokunnalle.

Asiantuntijat

Valiokunta on kuullut:
- lainsäädäntöjohtaja Tuula Majuri, oikeusministeriö
- erityisasiantuntija Anu Mutanen, oikeusministeriö
- eduskunnan oikeusasiamies Petri Jääskeläinen, Eduskunnan oikeusasiamiehen kanslia
- esittelijäneuvos Mikko Eteläpää, Eduskunnan oikeusasiamiehen kanslia
- vanhempi oikeusasiamiehen sihteeri Minna Ketola, Eduskunnan oikeusasiamiehen kanslia
- johtaja Teija Tiilikainen, Ulkopoliittinen instituutti
- vanhempi tutkija Teemu Tammikko, Ulkopoliittinen instituutti
- kansliapäällikkö Hiski Haukkala, Tasavallan presidentin kanslia
- poliisiosaston lainsäädäntöjohtaja Katriina Laitinen, sisäministeriö
- lainsäädäntöneuvos Marko Meriniemi, sisäministeriö
- neuvotteleva virkamies Heli Heikkola, sisäministeriö
- rajavartioylitarkastaja Reijo Lahtinen, sisäministeriö
- rajaturvallisuusasiantuntija, everstiluutnatti Jussi Sainio, sisäministeriö
- lainsäädäntöjohtaja Hanna Nordström, puolustusministeriö
- hallitussihteeri Kosti Honkanen, puolustusministeriö
- johtava asiantuntija, suurlähettiläs Marja Lehto, ulkoministeriö
- ylitarkastaja Maija Rönkä, liikenne- ja viestintäministeriö
- johtaja Matti Saarelainen, Euroopan hybridiuhkien torjunnan osaamiskeskus
- poliisiylijohtaja Seppo Kolehmainen, Poliisihallitus
- päällikkö, poliisineuvos Robin Lardot, keskusrikospoliisi
- päällikkö, poliisineuvos Antti Pelttari, suojelupoliisi
- poliisipäällikkö, poliisikomentaja Lasse Aapio, Helsingin poliisilaitos
- sotatieteiden tohtori, tutkija Saara Jantunen, Puolustusvoimien tutkimuslaitos
- tiedustelupäällikkö, kenraalimajuri Harri Ohra-aho, Pääesikunta

Valmis
5.0

- vanhempi osastoesiupseeri Juha-Antero Puistola, Turvallisuuskomitea
- apulaisprofessori Katri Pynnöniemi, Aleksanteri-Instituutti, Helsingin yliopisto
- johtaja Jarkko Saarimäki, Viestintävirasto
- Johtaja, suunnittelu- ja analyysiosasto Christian Fjäder, Huoltovarmuuskeskus
- Cyber Security Advisor Erka Koivunen, F-Secure Oy
- professori Mikael Hidén
- professori Jarno Limnéll
- professori Olli Mäenpää

Valiokunta on saanut kirjallisen lausunnon:
- oikeuskanslerinvirasto
- professori Martti Lehto, Jyväskylän yliopisto

HALLITUKSEN ESITYS

Hallituksen esityksessä ehdotetaan muutettavaksi Suomen perustuslain sääntelyä luottamuksellisen viestin salaisuuden suojasta. Esityksessä ehdotetaan perustuslakiin lisättäväksi uusi säännös, johon koottaisiin luottamuksellisen viestin salaisuuden rajoittamista koskeva sääntely. Perustuslaissa ehdotetaan säädettäväksi, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

VALIOKUNNAN PERUSTELUT

Yleistä

Suomessa ei ole tähän mennessä säädetty nimenomaista tiedustelutoimintaa sääntelevää lainsäädäntöä. Esimerkiksi sisäisen turvallisuuden alueella suojelupoliisin toimivaltuudet perustuvat poliisin toimintaa koskeviin yleislakeihin, pääosin poliisilakiin (872/2011), esitutkintalakiin (805/2011) ja pakkokeinolakiin (806/2011). Voimassa olevan lainsäädännön perusteella tiedonhankintavaltuuksien käyttö on sidottu rikoksen ennalta estämiseen, paljastamiseen ja selvittämiseen sekä joissakin tapauksissa vaaran torjumiseen. Edellytyksenä laissa säädettyjen tiedonhankintakeinojen käyttämiseen on, että tiedonhankinta saa kohdistua ainoastaan Suomessa olevan yksittäisen tunnistetun henkilön tietyn todennäköisyyskynnyksen täyttävän yksilöidyn tunnusmerkistön mukaisen rikoksen torjumiseen.

Turvallisuuspoliittisen toimintaympäristön muutoksiin ja uusiin uhkiin vastaamisen on todettu vaativan laajaa keinovalikoimaa ja käytettävissä olevien keinojen kehittämistä. Hallintovaliokunta korostaa sisäisen turvallisuuden selonteon johdosta antamassaan mietinnössä HaVM 5/2017 vp, että on välttämätöntä huolehtia kansallisen sääntelymme ajantasaisuudesta niin, että maamme omilla viranomaisilla on toimivaltuudet ja kyky saada asianmukaista tietoa maamme elintärkeisiin intresseihin kohdistuvista uhkista. Jokaisella valtiolla on velvoite huolehtia omasta ja kan-

salaistensa turvallisuudesta sekä perustaa siihen perustuva päätöksenteko itse hankittuun tietoon. Mainitun mietinnön mukaan onkin välttämätöntä kyetä hankkimaan tiedustelutietoa vakavista maamme kansallista turvallisuutta uhkaavista toiminnoista ja tapahtumista. Muun muassa on kyettävä torjumaan tehokkaasti kansallista turvallisuuttamme vakavasti uhkaavaa tietoverkkoihin tunkeutumista. Emme saa olla kansallista turvallisuuttamme koskevan tiedon hankinnassa liiallisesti riippuvaisia muista valtioista.

Eduskunnan käsittelyssä on tiedustelulainsäädännön kokonaisuus, johon kuuluvat nyt esillä olevan perustuslain 10 §:n muuttamista koskevan hallituksen esityksen lisäksi siviilitiedustelua (HE 202/2017 vp) ja sotilastiedustelua (HE 203/2017 vp) sekä tiedustelutoiminnan valvontaa (HE 199/2017 vp) koskevat hallituksen esitykset. Kokonaisuuteen kuuluu myös puhemiesneuvoston ehdotus eduskunnan työjärjestyksen muuttamisesta (PNE 1/2018 vp), jossa on kysymys tiedustelutoiminnan parlamentaarisesta valvonnasta.

Käsiteltävänä olevassa hallituksen esityksessä HE 198/2017 vp ehdotetaan muutettavaksi Suomen perustuslain sääntelyä luottamuksellisen viestin salaisuuden suojasta. Perustuslain 10 §:ään ehdotetaan lisättäväksi uusi 4 momentti, johon kootaan sääntely luottamuksellisen viestin salaisuuden rajoittamisesta. Perustuslaissa ehdotetaan säädettäväksi, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Siviili- ja sotilastiedustelulainsäädäntöä koskevissa hallituksen esityksissä ehdotetaan uusia toimivaltuuksia sekä siviili- että sotilastiedusteluviranomaisille. Käsiteltävänä olevan lakiehdotuksen keskeisenä tarkoituksena on mahdollistaa tiedusteluviranomaisten toimivallan laajentaminen mainituissa esityksissä ehdotetuilla tavoilla. Luottamuksellisen viestin salaisuuden suojaan puuttuvat toimivaltuudet edellyttävät perustuslain 10 §:n tarkistamista. Ehdotetussa siviilitiedustelua koskevassa lainsäädännössä tällaisia toimivaltuuksia ovat telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta, televalvonta, tekninen kuuntelu, lähetyksen jäljentäminen sekä tietoliikennetiedustelu.

Perustuslain 10 §:n muuttamista koskevan hallituksen esityksen perusteluissa arvioidaan, että jos nyt ehdotettu perustuslain muutos käsitellään normaalissa perustuslainsäätämisjärjestyksessä, voisivat näitä toimivaltuuksia koskevat säännökset tulla voimaan ehkä vasta vuoden 2020 alkupuolella. Käytettäessä kiireellistä perustuslainsäätämisjärjestystä säännökset voisivat tulla voimaan aikaisemmin, mahdollisesti jo vuoden 2018 lopulla esitysten eduskuntakäsittelystä riippuen. Jos esitysten eduskuntakäsittely jatkuu kuluvan vaalikauden lopulle asti, vähentää tämä tarvetta kiireellisen menettelyn käyttöön.

Valiokunta keskittyy tässä lausunnossaan kuvaamaan Suomen turvallisuusympäristöä ja siinä viime aikoina tapahtuneita muutoksia hallintovaliokunnan toimialan kannalta.

Sotilaallinen toiminta

Ehdotetussa sotilastiedustelulainsäädännössä tarkoitettu sotilaallinen toiminta voi olla sekä valtiollista että ei-valtiollista sotilaallisesti järjestäytyneiden joukkojen tai sotilaallisiin voimakeinoihin, kuten aseistukseen ja sotatarvikkeisiin, liittyvää toimintaa. Valtiollinen toiminta palautuu jonkin vieraan valtion asevoimien toimintaan tai siihen rinnastuvaan kansainvälisen, sotilaallisen liittouman tai järjestön toimintaan. Ei-valtiollisella toiminnalla tarkoitetaan puolestaan sellaista sotilaallisesti järjestettyä, aseistettua tai varustettua toimintaa, jolla ei ole edellä tarkoitettua valtiollista alkuperää tai jonka tällaista alkuperää ei voida tunnistaa.

Tiedon hankkiminen sotilaallisesta toiminnasta sisältää Suomeen kohdistuvien sotilaallisten ulkoisten toimenpiteiden kartoittamisen ja seuraamisen. Kyse voi olla esimerkiksi Suomen turvallisuusympäristön kannalta merkityksellisen sotilaallisen toiminnan kehityksen seuraamisesta tilannekuvan muodostamiseksi. Ilmaisu kattaa muun muassa jatkuvan tiedonhankinnan muiden maiden sotilaallisen suorituskyvyn kehittymisestä samoin kuin tiedonhankinnan Suomen maanpuolustukseen kohdistuvasta ulkomaisesta sotilastiedustelusta. Tiedon hankkiminen säännöksessä tarkoitetusta sotilaallisesta toiminnasta ei edellytä, että tällaisesta toiminnasta aiheutuu vakavaa uhkaa kansalliselle turvallisuudelle. Sotilaallista toimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan tarvitsee ehdotuksen mukaan olla välittömästi uhkaavaa seurannan aikana.

Kansallista turvallisuutta vakavasti uhkaava toiminta

Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan ehdotetussa siviilitiedustelulainsäädännössä kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä tai kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Edellytyksenä on, että toiminnalla on jokin kytkentä Suomeen ja että se uhkaa nimenomaan Suomen kansallista turvallisuutta, vaikka toiminta voikin maantieteellisesti tapahtua Suomen rajojen ulkopuolella. Kyse voi olla esimerkiksi Suomen kansallista turvallisuutta vakavasti uhkaavasta terrorismiin liittyvästä toiminnasta, väkivaltaisesta radikalisoitumisesta tai ulkomaisten tiedustelupalvelujen toiminnasta taikka Suomen turvallisuuden kannalta keskeisen valtion levottomuuksista.

Säännöksessä tarkoitettu uhkaava toiminta ei kohdistu ensisijaisesti kehenkään yksilönä, vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön. Kuitenkin myös esimerkiksi yksityishenkilöihin, kuten valtiojohtoon tai yhteiskunnan perustoiminnoista huolehtiviin henkilöihin, kohdistuvat väkivallanteot voivat olla säännöksessä tarkoitettua toimintaa, jos ne ovat kansallisen turvallisuuden kannalta merkittäviä ja voivat siten muodostaa vakavan uhan sille. Säännöksessä ei edellytetä kansallisen turvallisuuden olevan välittömästi vaarantumassa, vaan tiedonhankinta voi koskea myös toimintaa, joka jatkuessaan vaarantaisi kansallista turvallisuutta.

Valiokunta tähdentää, että ehdotetussa säännöksessä edellytetään sen soveltamisalaan kuuluvalta toiminnalta, että siitä aiheutuu vakavaa uhkaa kansalliselle turvallisuudelle. Vakavuusedellytys nostaa säännöksen soveltamiskynnystä, eikä mikä tahansa uhka kansalliselle turvallisuudelle vielä täytä säännöksessä asetettua vaatimusta.

Yhteiskunnan kokonaisturvallisuus

Kolme turvallisuusselontekoa

Eduskunta on käsitellyt kuluvalla vaalikaudella kolme turvallisuuspoliittista selontekoa; ulko- ja turvallisuuspoliittisen selonteon (VNS 6/2016 vp), sisäisen turvallisuuden selonteon (VNS 5/2016 vp) ja puolustusselonteon (VNS 3/2017 vp). Nämä kolme turvallisuusselontekoa ja etenkin niiden pohjalta asianomaisten valiokuntien hyväksymät selontekomietinnöt muodostavat maamme kokonaisturvallisuuden keskeisen viitekehyksen.

Hallintovaliokunta on todennut sisäisen turvallisuuden selonteosta antamassaan mietinnössä (HaVM 5/2017 vp), että eri selontekojen uhkakuvat ovat varsin yhdensuuntaisia. Selontekojen erilaisista toimialakohtaisista lähtökohdista johtuen uhkakuvat eivät kuitenkaan ole täysin yhteneväisiä, vaan ne painottuvat toimialakohtaisesti tavoitteiden ja toimenpiteiden suhteen.

Suomen ulko- ja turvallisuuspolitiikka nojaa perustuslakiin kirjattuihin arvoihin, oikeuksiin ja velvollisuuksiin edistää niitä. UTP-selonteon mukaan Suomen ulko- ja turvallisuuspolitiikan päämäärä on vahvistaa maamme kansainvälistä asemaa, turvata maamme itsenäisyys ja alueellinen koskemattomuus, parantaa suomalaisen yhteiskunnan turvallisuutta ja hyvinvointia sekä ylläpitää yhteiskunnan toimivuutta. Ulko- ja turvallisuuspolitiikan viimesijaisena tavoitteena on välttää Suomen joutuminen sotilaalliseen konfliktiin.

UTP-selonteosta antamassaan lausunnossa hallintovaliokunta toteaa, että ulko- ja turvallisuuspolitiikan keinoin vaikutetaan myös sisäiseen turvallisuuteen. Vastaavasti sisäisen turvallisuuden toimenpiteet tukevat myös ulkoista turvallisuutta. Valiokunta korostaa, että UTP-selontekoon sisältyvästä 15 painopisteestä 14 koskee enemmän tai vähemmän sisäistä turvallisuutta ja sen toimijoita. Tapahtunut painopisteen muutos on olennainen (VNS 6/2016 vp — HaVL 40/2016 vp).

Puolustusselonteko puolestaan sisältää hallituksen puolustuspoliittiset linjaukset Suomen puolustuskyvyn ylläpidolle, kehittämiselle ja käytölle. Puolustusselonteolla ja sen toimeenpanolla on tarkoitus varmistaa, että Suomen puolustuskyky vastaa turvallisuusympäristön vaatimuksiin.

UTP-selonteon ja puolustusselonteon aikajänne ulottuu aina ensi vuosikymmenen puoliväliin saakka. Niissä on tiedostettu myös se seikka, että myös sotilaallisen voiman käyttö ja sillä uhkaaminen ovat palanneet ainakin laajassa turvallisuusympäristömme kokonaisuudessa keinovalikoimaan.

Hallintovaliokunta on antanut maamme historiassa ensimmäisen sisäisen turvallisuuden selonteon johdosta muuttuneesta turvallisuustilanteesta johtuen sekä ottaen huomioon uudet turvallisuusuhkat laajan, kattavan ja perusteellisen sisäisen turvallisuuden mietinnön HaVM 5/2017 vp. Hallintovaliokunta toteaa mietinnössään, että sisäinen ja ulkoinen turvallisuus limittyvät yhä vahvemmin toisiinsa. Uudessa tilanteessa sisäisen turvallisuuden merkitys korostuu. Sisäinen turvallisuus on suomalaisen demokratian ja hyvinvointiyhteiskunnan kivijalka. Lisäksi on syytä muistaa, että perinteisen sisäisen turvallisuuden toimialan tilannekuva on voimakkaasti muuttunut. Sisäisen turvallisuuden tehtäväkenttä ulottuu myös entistä selvemmin perinteisen UTP-toimialan tehtäväalueelle. Hallintovaliokunta on sisäisen turvallisuuden selontekomietinnössään ulottanut

tarkastelun aikajänteen kahta muuta selontekoa vastaavasti ensi vuosikymmenen puoleen väliin saakka.

Sisäisen turvallisuuden selontekomietintö ja toimintaympäristön muutos

Sisäisen turvallisuuden selontekomietinnöstä ilmenee se tosiasia, että Suomen sisäinen turvallisuus on sidoksissa muiden EU:n jäsenvaltioiden ja naapurivaltioiden turvallisuustilanteisiin. Eurooppalainen turvallisuusympäristö on muuttunut nopeasti lähialueiden kriisien, erityisesti Syyrian kriisin, terrorismin, maahanmuuttokriisin ja Ukrainan konfliktin jatkumisen takia.

Muutos näyttää jatkuvan Suomen lähialueilla ja maailmanlaajuisesti. Sisäisen ja ulkoisen turvallisuuden uhkat limittyvät yhä tiiviimmin toisiinsa. Se, mitä Syyriassa tai muualla kriisialueilla tapahtuu, johtaa vaikutuksiin myös Suomen sisäisessä turvallisuudessa. Suurin muutos turvallisuustilanteessa onkin tapahtunut niissä tekijöissä, jotka vaikuttavat Suomen turvallisuuteen ulkoapäin ja hyvin kaukaakin. Tällaisia ovat muun muassa Lähi-idän ja Afrikan väkivaltainen ekstremismi ja terrorismi sekä ISISin väkivaltainen toiminta. Lisäksi esimerkiksi järjestäytynyt rikollisuus, joka toimii laajalti yli rajojen, hyödyntää yhteiskuntien ja ihmisten ongelmia sekä lain ja järjestyksen puutteita. Tämä näkyy muun muassa ihmissalakuljetuksessa.

Venäjän ja lännen suhteiden huononeminen kuuluu keskeisiin uusiin uhkiin turvallisuusympäristössämme. Tässä suhteessa on huomattava esimerkiksi, että laitonta maahantuloa voidaan käyttää myös voimapolitiikan välineenä. Turvallisuustilanteen ennustettavuus on heikentynyt merkittävästi, eikä tilanteessa ole nähtävissä muutosta parempaan. Lisäksi rajapinnat sotilaallisten ja ei-sotilaallisten uhkien välillä ovat ohentuneet. Syntyneessä tilanteessa onkin sisäisen turvallisuuden näkökulmasta otettava huomioon myös suunnitelmallinen ei-sotilaallisen voiman käyttäminen erilaisten yhteiskuntaamme vaikuttavien tavoitteiden aikaan saamiseksi.

Samalla sisäisen ja ulkoisen turvallisuuden keskinäinen suhde on muovautunut uudelleen ja niiden välinen rajapinta on hälventynyt. Selontekomietinnössä tuodaan myös esiin, että turvallisuuskentässä on havaittu suhteellisen uusia epäsymmetrisiä ja koko turvallisuuskenttää läpileikkaavia uhkia, joista voidaan käyttää yläkäsitteenä nimitystä hybridiuhkat. Kysymys ei kuitenkaan ole esimerkiksi hybridi-, kyber- ja informaatiovaikuttamisessa pelkästään uhkista, vaan maassamme parhaillaan tapahtuvasta tai maahamme kohdistuvasta toiminnasta, joka edellyttää viranomaisten toimenpiteitä. Suomen kokonaisturvallisuusympäristössä ja -tilanteessa on tapahtunut voimakas ja nopea muutos.

Hallintovaliokunta viittaa lisäksi laajemminkin sisäisen turvallisuuden selontekomietintöönsä, etenkin suojelupoliisin, terrorismin, kyberuhkien, informaatiovaikuttamisen ja hybridiuhkien kokonaisuuden osalta lausuttuun. Sinänsä jo mainitussa mietinnössä HaVM 5/2017 vp lausuttu puoltaa käsiteltävänä olevan hallituksen esityksen hyväksymistä.

Kansallisen turvallisuuden tilannekuvaa

Yleisiä näkökohtia

Edellä mainittujen selontekojen ja sisäisen turvallisuuden selontekomietinnön osalta on niiden todettava olevan kiinteässä yhteydessä maamme kansalliseen turvallisuuteen. Kansallisen turvallisuuden sisältö määrittyy hallintovaliokunnan toimialalla säädettävänä olevan siviilitiedustelulainsäädännön (HE 202/2017 vp) mukaisesti.

Kansalliseen turvallisuuteen kohdistuvien uhkien torjunnasta vastaa nykyään suoraan sisäministeriön alaisuudessa toimiva suojelupoliisi. Suojelupoliisin tehtävänä on torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi.

Suojelupoliisin tiedonhankinta on hankaloitunut merkittävästi voimakkaan digitalisaatiokehityksen myötä. Tiedonhankinnan kohteena olevien henkilöiden toimintaan liittyvien tietovälineiden sisältämät tietomäärät ovat kasvaneet huomattavasti. Tämä johtuu muun muassa sosiaalisen median nopeasta kehityksestä ja sen kasvavasta käytöstä kommunikaatiossa. Tämä ja järjestelmien kasvava kryptaus on kasvattanut yhä enemmän henkilö- ja tietoteknisten resurssien tarvetta.

Suojelupoliisin toiminnassa korostuu tiedustelullinen toimintatapa (HaVM 5/2017 vp). Tiedustelutieto on tärkeää myös siitä näkökulmasta, että sillä tuetaan osaltaan turvallisuusympäristöä koskevaan valtiollisen päätöksenteon perustumista relevantteihin, ajantasaisiin ja luotettaviin tietoihin.

Yleisen kehityksen seurauksena yksittäisten valtioiden turvallisuuskysymykset ovat kansainvälistyneet. Maamme turvallisuutta uhkaavat ilmiöt ja niiden taustatekijät liittyvät laajalti maamme ulkopuolisiin ja osin vaikeasti hahmotettaviin tapahtumiin ja kehityssuuntiin. Turvallisuuskysymysten rajat ylittävän luonteen vuoksi analysoidun kansainvälisen turvallisuustiedustelutiedon tarve on kasvanut merkittävästi. Tehokas globaaleihin uhkiin liittyvä turvallisuustiedustelu vaatii aiempaa monimuotoisempia keinoja ja lähestymistapoja.

Yleistä turvallisuuteen liittyvän toimintaympäristön muutoksesta

Hallituksen esityksen säätämisjärjestysperusteluissa viitataan siviili- ja sotilastiedustelulainsäädäntöä koskeviin hallituksen esityksiin, joissa on kuvattu seikkaperäisesti Suomen turvallisuustilanteen heikkenemiseen ja monimutkaistumiseen liittyviä näkökohtia. Suomen turvallisuustilanteen muutokseen on vaikuttanut muun ohella sotilaallisen toiminnan ja jännityksen lisääntyminen lähialueillamme. Kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat nykyään hyvin usein alkuperältään tai kytköksiltään kansainvälisiä ja siten vaikeammin hallittavia. Lisäksi viestintäteknologian nopea kehitys on tehostanut ja helpottanut Suomelle uhan muodostavien tahojen välistä yhteydenpitoa ja verkostoitumista sekä vaikeuttanut uhkien taustalla olevien tahojen tunnistamista. Eri toimijat kommunikoivat myös laajalti yli valtionrajojen. Teknologian kehittyminen on myös mahdollistanut kansallista turvallisuutta vaarantavien tekojen valmistelun ja toteuttamisen entistä lyhyemmässä ajassa. Samalla uhat ovat muuttuneet toteutuessaan vaikutuk-

siltaan aiempaa laajemmiksi, moniulotteisemmiksi ja vaarallisemmiksi yksittäisten ihmisten ja koko yhteiskunnan kannalta.

Suomen ulkoinen turvallisuusympäristö on viime vuosina heikentynyt voimakkaasti ja monialaisesti. Maamme lähialueiden turvallisuustilanne on jatkuvasti heikentynyt sitä mukaa kuin kansainvälispoliittiset jännitteet ovat ulottuneet vaikutuksiltaan alueellisesti aiempaa pohjoisemmaksi. Suurvaltojen käyttäytymisessä ja niiden välisissä suhteissa on myös nähtävissä yhä vaikeampaa ennakoitavuutta.

Perinteisen sodankäynnin sijasta asemia pyritään vahvistamaan hybridivaikuttamisen ja erilaisten informaatio-operaatioiden avulla. Tällaisia operaatioita, joiden tavoitteena on aiheuttaa epävarmuutta, eripuraa ja pelkoa kohdemaiden poliittisissa päätöksentekojärjestelmissä ja kansalaisten keskuudessa, on viime vuosina kohdistettu lukuisiin Euroopan maihin. Operaatioihin valmistautumista ja niiden toteuttamista tuetaan kohdemaihin kohdistettavan vakoilun avulla. Suojelupoliisin tietoon tulee saadun selvityksen mukaan jatkuvasti konkreettisia tapauksia, joissa vieraat valtiot pyrkivät hankkimaan haltuunsa Suomen turvallisuuden ja kansantalouden kannalta kriittisen tärkeää tietoa.

Perinteisen vakoilun rinnalle on noussut kybervakoilu, jossa tekijävaltio ilman merkittävää riskiä kiinnijäämisestä pystyy hankkimaan erittäin suuria määriä kohdevaltion turvallisuutta vahingoittavaa tietoa. Yhteiskunnan elintärkeiden toimintojen keskinäisriippuvuudesta ja verkkopohjaisuudesta johtuen kriittinen infrastruktuuri ja huoltovarmuus ovat yhä alttiimpia tietoverkkojen välityksellä toteutettavalle valtiolliselle sabotaasille ja kokonaisvaltaiselle lamauttamiselle.

Samanaikaisesti kun erilaiset valtioperäiset uhkat ovat lisääntyneet, myös Suomen terrorismitilanne on kehittynyt vakavammaksi kuin koskaan aiemmin. Kansainvälisiin terroristijärjestöihin kytköksiä omaavien henkilöiden määrä Suomessa on kasvanut ennen näkemättömän nopeasti, ja esimerkiksi suojelupoliisin kohdehenkilöiden määrä on kaksinkertaistunut muutamassa vuodessa. Suomi on noussut terroristijärjestöjen viholliskuvassa muiden Pohjoismaiden rinnalle. Syyrian ja Irakin konflikteissa taistelleet palaavat jihadistit muodostavat sekä akuutin että pitkäkestoisen uhkan Suomen ja muun Euroopan turvallisuudelle. Terrorismitilannetta monimutkaistavat kansainväliset pakolais- ja maahanmuuttovirrat ja niiden vaikea hallittavuus sekä se, että niitä hyödynnetään valtiollisessa hybridi- ja informaatiovaikuttamisessa epävarmuuden ja yhteiskunnallisten ristiriitojen kylvämiseksi Länsi-Euroopan demokratioihin.

Turvallisuusympäristön nopeat muutokset edellyttävät viranomaisilta aiempaa tehokkaampaa kykyä havaita myös aivan uudentyyppisiä uhkia. Tietoa uusista uhkista tarvitsevat sekä kansallisesta turvallisuudesta vastaavat viranomaiset näiden uhkien ennalta estämiseksi että ylin valtionjohto päätöksentekonsa tueksi. Tiedustelu on usein paras ja joskus myös ainoa keinoa saada ensihavainto ja hankkia tietoa näistä uhkista.

Terrorismi

Suojelupoliisin esittämän arvion mukaan Suomeen kohdistuva terrorismin uhka on neliportaisella tasolla ilmaistuna tällä hetkellä tasolla 2 — kohonnut. Uhka on vakavampi kuin koskaan aiemmin. Valiokunnan saaman selvityksen perusteella suojelupoliisin tietoon on tullut aiempaa vaka-

vampia terrorismiin kytkeytyviä suunnitelmia ja hankkeita. Terrorismin uhka Suomessa on noussut muiden Pohjoismaiden tasolle, eikä terrorismin toimintaympäristössä ole nähtävissä uhkaa laskevia kehityskulkuja. Päinvastoin uhkan kasvu on todennäköistä keskipitkällä aikavälillä. Suomen uhkatilanteen muutoksessa merkittävää on sen nopeus. Muissa Pohjoismaissa vastaava muutos on tapahtunut pidemmällä aikavälillä, jolloin siihen on kyetty varautumaan asteittain.

Suojelupoliisin terrorismin torjunnan kohdehenkilöiden määrä on kasvanut voimakkaasti viime vuosina. Kohdehenkilöiden lukumäärä on tällä hetkellä noin 370. Kohdehenkilöiden sidokset terroristiseen toimintaan ovat yhä suorempia. Vielä nopeasti kasvanutta määrääkin huolestuttavampaa on laadullinen muutos. Suojelupoliisin tietoon on tullut aiempaa vakavampia terrorismiin kytkeytyviä hankkeita sekä suunnitelmia. Useissa tapauksissa nämä hankkeet ja suunnitelmat kytkeytyvät Suomen ulkopuolella vaikuttaviin toimijoihin. Radikalisoitumisen ja uusien verkostojen paljastumisen seurauksena kohdehenkilöiden määrän arvioidaan kasvavan myös lähivuosina. Seurannan kohteena olevien henkilöiden määrästä huomattavan osan muodostavat henkilöt, joilla on selkeä terroristinen vakaumus sekä kyky ja taito tehdä terroristinen teko.

Suomen terrorismitilanne on tiiviisti kytköksissä kansainvälisen terrorismin kehityskulkuihin ja trendeihin. Konfliktialueilla on keskeinen rooli radikaali-islamistisen terrorismin kehityksessä. Viime vuosina erityisesti Syyrian ja Irakin konfliktialue on toiminut terrorismin kasvualustana. Konfliktialue on nyt murroksessa, ja sen seurauksena radikaali-islamistiset verkostot myös Euroopassa arvioivat toimintaansa uudelleen.

Vierastaistelijailmiö vaikuttaa merkittävästi Suomen terrorismin uhkaan. Vaikutus on sekä suoraa että epäsuoraa. Suoran turvallisuusuhan aiheuttavat palaavat tai palaamaan pyrkivät vierastaistelijat tai heidän verkostonsa. Epäsuora uhka nousee propagandan, värväyksen ja vaikuttamisen kautta. Lisäksi vierastaistelijailmiö on aiempaa vahvemmin sitonut myös Suomessa toimivat ja Suomeen kytkeytyvät radikaaliverkostot osaksi kansainvälisiä verkostoja. Tämä nostaa suomalaisten tai Suomeen sidoksissa olevien henkilöiden terrorihankkeisiin kytkeytymisen todennäköisyyttä joko maassamme tai ulkomailla. Valiokunnan käsityksen mukaan Suomessa käytännössä merkittävimmän uhkan muodostavat tämän hetken tietojen perusteella terrorismin yksittäiset toimijat ja pienryhmät. Tässä yhteydessä valiokunta kiinnittää huomiota myös siihen, että värväystoimintaa kohdistuu myös henkilöihin, joilla ei ole radikalisoitumista edistävää taustaa tai yhteyttä radikaaliverkostoihin.

Syyrian ja Irakin konfliktialueella oleskelee tällä hetkellä kymmeniä Suomesta matkustaneita henkilöitä, heidän joukossaan useita lapsia. Syyrian ja Irakin alueella toimivien terroristijärjestöjen aiemmin hallinnoimilla alueilla on kasvanut uusi jihadistisukupolvi, jossa on mukana myös suomalaisia. Tästä johtuen ilmiön arvioidaan vaikuttavan Suomessa vielä pitkään. Suomesta lähteneiden taistelijoiden vuoksi myös ulkomaiset radikaali-islamistit tuntevat Suomen entistä paremmin.

Suomen profiili radikaali-islamistisessa propagandassa on kohonnut. Suomalaisia on esiintynyt esimerkiksi terroristijärjestö "Islamilaisen valtion" (IS/ISIL/ISIS) propagandassa. Propagandaa on julkaistu suomeksi ja iskuihin kehotetaan myös Suomessa. Sekä suomalaisten että Suomesta matkustaneiden tiedetään osallistuneen propagandan tuottamiseen, ja joissain tapauksissa he ovat pyrkineet nimenomaisesti suuntaamaan viestiä Suomeen. Tämä osaltaan kannustaa Suomessa

oleskelevia radikaaleja henkilöitä myös väkivaltaiseen toimintaan. Virtuaaliset verkostot ovat nousseet yhä keskeisempään rooliin. Propagandan levitys on siirtynyt suojattuihin pikaviestisovelluksiin. Viranomaisten vastatoimien ja tiedustelun suhteen tämä on erityisen haasteellista.

Laiton ulkomainen tiedustelu

Laittoman tiedustelutoiminnan torjuminen on muuttunut nopeasti aiempaa monimutkaisemmaksi. Ulkomaisten tiedustelupalveluiden tiedustelutoiminta Suomessa on aktiivista. Ulkomaisten tiedusteluorganisaatioiden Suomen valtion turvallisuusintresseihin kohdistama tiedustelu jatkuu edelleen laajamittaisena, luonteeltaan pitkäkestoisena ja jatkuvana henkilötiedusteluna, mutta samalla vakoilu on siirtynyt merkittävästi myös tietoverkkoihin. Maan väkilukuun suhteutettuna Suomeen pysyvästi sijoitettujen ulkomaalaisten tiedustelu-upseereiden määrä on yksi suurimmista länsimaissa.

Ulkomaisen tiedustelun keskeisimpiin päämääriin kuuluvat Suomen politiikan ennakoiminen ja päätöksiin vaikuttaminen. Säännöllisesti on myös havaittu pyrkimyksiä vaikuttaa yleiseen mielipiteeseen. Tietojen hankintaa ja vaikuttamisyrityksiä kohdistetaan etenkin päätöksiä valmisteleviin ja niitä toteuttaviin tahoihin.

Valtiollinen tiedustelutoiminta on luonteeltaan pitkäjänteistä, ja sen keskeisiä kiinnostuksen kohteita Suomessa ovat muun muassa poliittisen johdon ja väestön suhtautuminen mahdolliseen Nato-jäsenyyteen, Suomen energiapoliittiset päätökset ja energiahuoltovarmuus sekä Suomen kyberturvallisuusrakenteet.

Viranomaisten tiedossa on konkreettisia tapauksia vieraiden valtioiden pyrkimyksistä hankkia Suomesta salaisia tietolähteitä toimittamaan tietoja, jotka eivät ole julkisesti saatavilla. Tiedusteluorganisaatiot pyrkivät hankkimaan avustajikseen lisäksi henkilöitä, joiden avulla on mahdollista vaikuttaa poliittiseen päätöksentekoon ja yleiseen mielipiteeseen. Valtiollisten tahojen suorittama laiton tiedustelu aiheuttaa vahinkoa myös suomalaisille korkeateknologian yrityksille ja tutkimuslaitoksille. Toiminta voi aiheuttaa yritystasolla kriittistä vahinkoa, ja sillä on potentiaalisesti myös kansantaloudellista merkitystä.

Tietoverkkojen välityksellä valtiolliset ja muut hyvin resursoidut toimijat pyrkivät aktiivisesti hankkimaan poliittiseen päätöksentekoon ja merkittäviin tuotekehitysinnovaatioihin liittyvää tietoa. Verkkovakoilulta ja verkkovaikuttamiselta suojautumiseen ja siihen puuttumiseen kansallisen turvallisuuden suojelemiseksi tarvitaan nyt ehdotettua uutta lainsäädäntöä. Vastatiedustelun olennaisena lähtökohtana on löytää tiedustelutoimintaa harjoittavat henkilöt, joiden toiminta aiheuttaa vakavaa uhkaa kansalliselle turvallisuudelle.

Tiedustelun torjunnan näkökulmasta merkityksellinen on myös kysymys kaksoiskansalaisuudesta siltä osin kuin se asettaa Suomen kansalaisuuden omaavan kaksoiskansalaisen asemaan, jossa tämä voi joutua toimimaan Suomen etujen vastaisesti. Esimerkiksi kaikki Venäjän kansalaiset ovat kaksoiskansalaisuudesta riippumatta Venäjän lakien mukaan velvoitettuja auttamaan Venäjän turvallisuusviranomaisia.

Kyberuhkat

Kybertoimintaympäristössä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan vaikeasti ennakoitavia. Kyberturvallisuus perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöön sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden häiriötilanteita.

Kyberuhkalla tarkoitetaan sellaista kybertoimintaympäristöön kohdistuvaa uhkaa, joka toteutuessaan vaarantaa kybertoimintaympäristön oikeanlaisen tai tarkoitetun toiminnan. Uhkaan liittyy usein sähköisen toimintaympäristön turvallisuuteen liittyvää uhkaa, johon kuuluvat itse tiedon lisäksi myös esimerkiksi digitaaliset ohjausjärjestelmät, jotka kontrolloivat ja ohjaavat yhteiskunnan monia elintärkeitä infrastruktuureita sekä koko muuta infrastruktuuria tietoverkoista sovelluksiin.

Kyberuhat voivat olla joko siviililuontoisia tai sotilaallisia riippuen yhtäältä niiden toteuttajatahosta ja toisaalta toiminnan tarkoitusperästä. Tietojärjestelmiin ja niitä yhdistäviin tiedonsiirtoverkkoihin liittyvät uhkat voivat olla vakavia senkin vuoksi, että tietojärjestelmät ovat sulautuneet ja verkottuneet globaaleiksi kokonaisuuksiksi, joiden toiminnan häiriöt saattavat ulottua yksittäisiä palveluja laajemmalle. Tällaisten häiriöiden vaikutuksia voi olla vaikea ennakoida. Pahimmillaan kyberoperaatiolla saatetaan lamauttaa koko yhteiskunta.

Sisäisen turvallisuuden selonteosta antamassaan mietinnössä hallintovaliokunta toteaa saamansa informaation perusteella, että useissa Euroopan maissa on havaittu toimintaa, jossa ulkopuolinen taho on pyrkinyt tietoteknisesti kartoittamaan kriittistä infrastruktuuria ohjaavien järjestelmien ohjelmistoversioita. Jos toinen valtio tai muu toimija tietää kohdeympäristön ohjelmistoversiot, toimivien hyökkäysmenetelmien valitseminen käy saadun selvityksen mukaan kriisitilanteessa nopeasti. Valiokunnalle ilmoitetun perusteella Suomessa havaitaan jatkuvasti myös ulko- ja turvallisuuspoliittiseen päätöksentekoon kohdistuvaa kybervakoilua.

Valiokunnan saaman selvityksen mukaan lisäksi on selviä viitteitä valtiollisilla resursseilla varustettujen toimijoiden pyrkimyksistä vaikuttaa yhteiskunnan kriittisen infrastruktuurin toimintaan. Tunnettuna esimerkkinä laajamittaisesta vaikutusoperaatiosta voidaan mainita Ukrainan kolmen alueellisen sähköyhtiön verkkoinfrastruktuuriin joulukuussa 2015 kohdistunut kyberhyökkäys. Haittaohjelmia apuna käyttäen tuolloin on tuhottu sähköverkko-operaattorien hallintajärjestelmä ja aiheutettu sähkökatko 255 000 kuluttajalle.

Merkittäviä palvelunestohyökkäyksiä on Suomessa kohdistunut viime vuosina mediatoimijoihin, pankkien verkkopalveluihin ja julkishallinnon internetpalveluihin. Viime aikojen kansainvälinen kehitys viittaa merkittävien palvelunestohyökkäysten aikaansaamiseen käytettävissä olevan hyökkäyskapasiteetin kasvaneen merkittävästi. Julkisuudessakin kerrottu hyökkäyskapasiteetti voi olla niin suuri, että se saattaa suomalaisiin internetpalvelujen tarjoajiin kohdistuvana pahimmillaan estää niiden toiminnan. On lisäksi huomattava, että ulkomaiseen toimijaan kohdistunut hyökkäys voi ulottaa kansainvälisissä verkottuneissa järjestelmissä vaikutuksensa myös meille Suomeen.

Eri arvioiden mukaan kyberturvallisuutta eniten muokkaavat voimat ovat yhä laajeneva kyberhyökkäysala, hyökkääjien osaamisen parantuminen, kyberrikollisuuden teollistuminen ja tietovuodot. Kybermaailmassa erityisesti esineiden internet, pilvipalvelut, suuret datamassat ja lisääntyvä mobiilipäätelaitteiden käyttö luovat hyökkääjille uusia hyökkäyskohteita. Pilvipalveluiden lisääntyminen tarkoittaa uusia mahdollisuuksia kyberhyökkääjille. Pilvipalvelut ovat usein kolmansien osapuolien toimittamia, jolloin asiakkaalla ei ole kunnollista näkymää palvelun laatuun tai turvallisuuteen. Älykkäitä Big data -sovelluksia käytetään jo paljon, mutta uhkana on, että suurten datavarastojen lisääntyessä lisääntyvät riskit tahattomille tai tahallisille väärinkäytöksille. Mobiliteetista ja uusista päätelaitteista haetaan tehokkaampia tapoja toimia ja osa ihmisten työstä tehdään mobiilisti. Tämä kehitys on lisännyt merkittävästi haittaohjelmia ja hyökkäyksiä mobiilipäätelaitteisiin.

Valiokunta toteaa, että yhteiskuntamme, sen toiminta, talous ja päätöksenteko on täysin riippuvainen sähköisestä digitaalisesta toimintaympäristöstä. Tämä riippuvuus tulee kasvamaan edelleen voimakkaasti. Valiokunta arvioi, ettei suomalaisessa päätöksenteossa vielä kuitenkaan ymmärretä täysin muutoksen voimakkuutta ja nopeutta, mikä osaltaan saattaa altistaa yhteiskunnan ja siinä toimivat organisaatiot jatkuvasti kasvavalle joukolle kyberuhkia.

Kyberrikollisuuden ja sen torjunnan voidaan sanoa olevan maailmanlaajuisestikin iso haaste. Volyymien kasvaessa rikollisuuden yhteiskunnille aiheuttamat haitat ovat myös jatkuvassa kasvussa. Viranomaisten toimivaltuudet, tiedonvaihtoa koskevat säännökset ja kansainväliset sopimukset eivät tue tällä hetkellä kunnolla kyberrikostorjuntaa. Torjunnassa tarvitaankin säädettävän normiston ohella laajaa kansainvälistä ja kansallista yhteistoimintaa. Vaikeusastetta lisää se seikka, että rikoksentekijät ja uhrit voivat olla useassa eri maassa ja näyttö rikoksiin on hankittava eri puolelta maailmaa sijaitsevilta palvelimilta.

Hallintovaliokunta korostaa, että kyberhyökkäysten torjunta edellyttää maamme toimivaltaisilta viranomaisilta korkeatasoista osaamista ja asianmukaisia toimivaltuuksia. Puutteet mainitussa suhteessa voivat altistaa yhteiskunnan sen toimintoja kattavasti lamaannuttavaan aiempaa suurempaan hyökkäykseen, johon ei osata varautua. Kybermaailman tulevaisuudessa olennaista on myös yhteiskunnan kyky sietää kyberhyökkäysten vaikutuksia. Haastava tilanne koko yhteiskuntamme kannalta syntyy, jos esimerkiksi sähköt katkeavat talvella pitkäaikaisesti tai internetoperaattorit menettävät toimintakykynsä yhtä aikaa muutoin kuin lyhytaikaisesti.

Hallintovaliokunta tähdentää, että kybertoimintaympäristön merkitys kansallisen turvallisuuden ylläpitämisessä kasvaa jatkuvasti. Kyberkeinoja käytetään muun muassa poliittisten päämäärien saavuttamiseksi. Tietoliikenneverkkojen kautta tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion kansalliselle turvallisuudelle ja sen eduille. Tietoverkoissa tapahtuva sabotaasi ja tiedon vääristäminen ovat myös merkittäviä uhkia kansalliselle turvallisuudelle. Kybervakoilulla saatua tietoa voidaan käyttää myös informaatiosodankäynnissä, josta esimerkkinä on esitetty Yhdysvaltojen vaaleihin vaikuttaminen.

Suomen turvallisuusympäristön muutoksen kannalta olennaiset ulkovallat panostavat valiokunnan saaman selvityksen perusteella hyökkäyksellisen kyberkapasiteettinsa rakentamiseen. Tämä vaatii näiltä valtioilta aiempaa enemmän tukea perinteisessä reaalimaailmassa tapahtuvalta tie-

dustelutoiminnalta, kuten tiedonkeräämistä henkilötiedustelun keinoin potentiaalisista kybervakoilun kohteista tai sellaisten henkilöiden löytämistä, jotka vahingossa tai tarkoituksellisesti auttaisivat valtiollisen haittaohjelman viemisessä kohdeorganisaation tietojärjestelmään. Julkisuudessa on uutisoitu kyvystä tunkeutua ja onnistuneesta tunkeutumisesta suuren EU:n jäsenvaltion sisäiseen suljettuun viranomaistietojärjestelmään.

Kybervakoilu tarjoaa valtioille lähes riskittömän tavan hankkia tietoa riippumatta niiden taloudellisesta ja yhteiskunnallisesta kehitystasosta. Kybervakoilu on halpa tiedonhankintamenetelmä suhteessa potentiaalisesti saatavilla olevan tiedon määrään.

Yksityisten yritysten tietopääoman anastamiseen pyrkivistä hyökkäyksistä iso osa jää kokonaan pimentoon, koska yrityksillä tai kolmannella sektorilla ei ole valmiutta tunnistaa valtiollisen toimijan uhkaa. Erityisen kriittisenä uhkana valiokunta näkee kyberoperaatiot, joissa hyökkääjä on hyväksikäyttänyt suoraan organisaation luotettuja palveluketjutoimintoja. Saadun selvityksen perusteella tieto tällaisista hyökkäyksistä tulee suojelupoliisille lähes poikkeuksetta ulkomaisten kumppanien vinkkeinä. Viedyn tietopääoman arvo keskisuuren yrityksen tapauksessa voi nousta kymmeniin miljooniin euroihin vuodessa. Hyökkäystoiminnan nopea havainnointi minimoisi viedyn tiedon määrän ja sen aiheuttamat potentiaaliset menetykset yritykselle.

Tietoverkkoihin kohdistuvat hyökkäykset ovat erittäin vaarallinen uhka ainakin kahdesta syystä: 1) niihin soveltuva teknologia kehittyy jatkuvasti ja 2) niissä on usein valtiotoimijoiden apuna järjestäytyneen rikollisuuden edustajia ja hakkereita. Valtiollinen toiminta, kansalaisyhteiskunta ja rikollisuus sulautuvat toisiinsa, minkä vuoksi valiokunta painottaa, että uhkien torjumiseksi Suomen turvallisuusviranomaisten teknisen suorituskyvyn tulee olla erittäin korkea ja jopa hyökkääjää parempi. Vastaavasti korkean suorituskyvyn käyttämiseen tarvittavien valtuuksien tulee olla sellaiset, että uhkien muodostuminen voidaan havaita jo ennalta estävästi ja joka tapauksessa mahdollisimman aikaisin. Jos viranomaiset kykenevät pelkkään reagoimiseen vahinkojen jo tapahduttua, yhteiskunnan elintärkeät toiminnot ja samalla kansallinen turvallisuus ovat erittäin suuressa vaarassa.

Informaatiovaikuttaminen

Informaatiovaikuttaminen ei ole ilmiönä uusi. Sen käyttötavat ja vaikuttavuus ovat kuitenkin muuttuneet aivan olennaisesti nykyisessä sähköisessä mediaympäristössä. Kansalliseen turvallisuuteen ulottuvassa informaatiovaikuttamisessa tavoitteena on muun muassa vaikuttaa viime kädessä päätöksentekijöihin ja päätöksentekoprosessiin sekä saada sen kohde tekemään itselleen haitallisia tai vaikuttajan kannalta myönteisiä päätöksiä taikka käyttää erilaisia toimintatapoja useilla eri median alustoilla. Vaikuttaminen tapahtuu usein myös välillisesti niin sanotun suuren yleisön kautta, tai se voi kohdistua suoraan päätöksentekijöihin tai päätöksentekoprosessiin. Esimerkiksi vaalitulokseen voidaan pyrkiä ennakolta vaikuttamaan vaikkapa Twitterin avulla kohdistamalla toiselta puolelta maapalloa viestejä äänioikeutetuille siitä, miten ehdokkaat menestyivät vaaliväittelyssä.

Kysymys voi olla esimerkiksi siitä, että yleistä mielipidettä muokkaamalla pyritään kohteen henkisen tilan hallintaan. Avoimessa yhteiskunnassa voi olla riittävää hajaannuksen aikaan saaminen yhteiskuntaan, mikä puolestaan voi vaikeuttaa viranomaisten ja poliittisen johdon työtä sekä

tehdä tilannekuvan muodostamisen ja sen jakamisen vaikeaksi. Kun erilaiset kannatusta saavat mielipiteet ovat riittävän vahvoja, päätöksenteossa valintojen ja yleensäkin ratkaisujen tekeminen vaikeutuu. Päätöksentekijän edellytykset toimia ja tehdä päätöksiä saatetaan myös menettää. Vaikuttamisen asteesta riippuen voidaan puhua jopa informaatiosodasta.

Informaatiovaikuttaminen on sekä hybridi- että kybervaikuttamisen väline, eikä sen määritelmän osalta ole merkitystä, onko vaikuttaja valtiollinen tai valtiosta riippumaton toimija. Informaatiovaikuttamisen osalta on tyypillistä, että päätöksentekoa ohjataan muun muassa erilaisen disinformaation avulla tai jakamalla vaillinaista tietoa. Myös tiedon jakamatta jättäminen voi olla informaatiovaikuttamista, kuten myös sinänsä oikean tiedon jakaminen valikoidusti eri kohderyhmille. Tämä voi tapahtua esimerkiksi mainonnan avulla pyrkimällä vaikuttamaan kohteen mielikuviin ja tunteisiin.

Niin sanotun trollaamisen avulla voidaan myös vaikuttaa eri informaatiotoimijoihin muun muassa kyseenalaistamalla heidän tai median välittämän tiedon oikeellisuus tai jopa hyökätä henkilön persoonaa ja/tai uskottavuutta kohtaan. Toiminnan tarkoitus voi olla moninainen, mutta itse informaatiovaikuttaminen on kohdistettua. Käytännössä on ilmennyt tapauksia, joissa informaatiovaikuttamisesta uutisoineet toimittajat ovat joutuneet systemaattisen, massiivisen ja pitkäkestoisen informaatiohyökkäyksen kohteiksi. Operaatioihin on onnistuttu saamaan mukaan myös kotimaisia trollaajia. Laajan sananvapauden nimissä on harjoitettu muun muassa nettikiusaamista, uhkailua ja vainoamista. Toiminnan tarkoituksena nähdään olevan sen, ettei informaatiovaikuttamisesta tule uutisoida.

Tutkijapiireissä nähdään, että nykytila on vasta alkua voimistuvalle informaatiovaikuttamiselle. Yhtenäiskulttuurin murenemisen ja mediakentän sirpaloitumisen meneillään olevassa murroksessa katsotaan luovan avoimessa yhteiskunnassa uudenlaisen mediamaiseman, jossa valtion rooli keskeisenä auktoriteettina uhkaa marginalisoitua. Informaatiovaikuttamisen tai informaatiosodan ja muun vihamielisen vaikuttamisen näkökulmasta tämä tarkoittaa lukuisia uusia vaikuttamisen mahdollisuuksia. Yhteiskunnan jakolinjat ja polarisoitunut ilmapiiri luovatkin oivallisia manipuloitavia kohdeyleisöjä.

Asiassa on tullut maamme tiedustelukyvyn kannalta merkityksellisesti esiin, että suurvaltatason doktriinissa yhdistyvät pehmeiden (soft power) ja kovien keinojen yhtäaikainen käyttö sekä eräänlaisen "psykologisen etupiirin" luominen lähiympäristöön. Kysymys on psykologisesta vaikuttamisesta, joka perustuu laajaan keinovalikoimaan. Esimerkiksi ulkopoliittisella paineella saatetaan pyrkiä vaikuttamaan kohdevaltioiden sisäpolitiikkaan. Joissakin tapauksissa voidaan hyödyntää myös sisäisen ja ulkoisen turvallisuuden keskinäisriippuvuutta. Psykologisen vaikuttamisen korostuminen tulevaisuuden turvallisuusympäristössä tarkoittaa sitä, että tunteisiin vetoaminen ja siten käyttäytymiseen vaikuttaminen saattavat muuttua arkipäiväisiksi.

Digitalisaatio ja tietotekniikan kehittäminen tuovat uusia haasteita tiedon luotettavuuden arvioinnissa. Kehittyvä teknologia tekee informaation väärentämisestä yhä helpompaa informaatio-operaatioissa. Henkilön uskottavuuden heikentämiseksi on esimerkiksi mahdollista tuoda julkisuuteen vääristeltyjä asiakirjatietoja henkilön terveydentilasta. Jo nyt on kehitteillä teknologiaa, jolla pystytään reaaliajassa muokkaamaan videokuvaa. Kohdistettu informaatiovaikuttaminen ja siihen liittyvät kampanjat eivät tulevaisuudessa liity vain poliittisiin päättäjiin ja yhteiskunnan

avainhenkilöihin, vaan myös kansalaisiin, joihin vaikuttamisen kautta vaikutetaan yhteiskunnan keskeisiin toimijoihin. Onnistuneessa informaatio-operaatiossa kohteena olevat eivät tiedä olevansa kohdehenkilöitä.

Yhtenäiskulttuurin murentuessa kilpailevia tulkintoja, näkökulmia ja puhtaan virheellisiä tai valheellisia tietoja on informaatiossa entistä enemmän, minkä vuoksi virheellisen tiedon korjaaminen on yhä haastavampaa. Lisäksi journalismin periaatteita noudattavan median haasteena on, kuinka turvata nykyoloissa taloutensa ja samalla säilyttää korkeatasoinen tosiasiapohjainen tiedonvälitys. Yhteiskunnassa toimiva ja oikea-aikainen johtaminen perustuu yhteiseen ja muille jaettuun tilannekuvaan. Valiokunnan mielestä oikean tilannekuvan ylläpitäminen edellyttää asiantuntijoiden ja tutkijoiden osaamisen hyödyntämistä. Tiedon väärentämisellä ja tiedon manipuloimisella saatetaan pyrkiä hämärtämään tilannekuvaa. Kansalaisten kannalta heidän yleinen tietopohjansa ja medialukutaitonsa sekä arvomaailmansa joutuvat tällaisessa tilanteessa koetukselle. Pahimmillaan syntyvä tilanne voi uhata demokratiaa ja yhteiskuntarauhaa.

Sisäisen turvallisuuden selontekomietinnössä hallintovaliokunta toteaa, että valiokunnalle esitetyn asiantuntijanäkemyksen mukaan Suomen valtiojohdolla ei ole tähän mennessä ollut käytössään riittävää strategisen viestinnän kulttuuria. Strateginen viestintä on kuitenkin keskeisimpiä johtamisen välineitä informaatiokaudella. Strateginen viestintä parantaisi valtiojohdon ja viranomaisten kykyä toimia epäselvissä tilanteissa ja toimisi työkaluna, jolla vastuulliset toimijat voisivat ylläpitää luottamussuhdetta yhteiskunnassa. Epäluottamusta sen sijaan voi syntyä, jos päättäjät ja viranomaiset eivät kykene jakamaan oikea-aikaista ja paikkansapitävää tilannekuvaa muulle yhteiskunnalle.

Hybridiuhkat

Hybridiuhkien määritelmät vaihtelevat, koska niiden määrittely on haluttu pitää mahdollisimman joustavana uhkien muuttuvan ja moninaisen luonteen vuoksi. Hybridiuhka määritelläänkin yleensä lähinnä kuvaamalla niitä erilaisia keinoja, joita käytetään hybridivaikuttamisessa. Hybridivaikuttamisessa monenlaisia vaikuttamisen keinoja yhdistellään ja sovelletaan joustavasti tilanteen mukaisesti. Yhteinen piirre hybridivaikuttamisen keinoissa on kohteen haavoittuvuuksien hyödyntäminen, erimielisyyksien herättäminen ja päätöksentekoprosessin häirintä. Disinformaatiokampanjat, sosiaalisen median käyttö ja radikalisoitumisen edistäminen ovat sille tyypillisiä toimintatapoja. Hybridiuhkiin, joihin sisältyvät tilannekohtaisesti myös kyberuhat, kuuluu olennaisena osana myös sähköisen toimintaympäristön turvallisuuteen liittyvää uhkaa sekä sähköisten välineiden avulla aiheutettavaa uhkaa. Hybridivaikuttamisella on mahdollisuus luoda uhkien kombinaatioita, joihin ei ole riittävästi varauduttu ja joihin on vaativaa varautua.

Hybridiuhkan käsitteellä tarkoitetaan erilaisia turvallisuutta vaarantavia ja yhteiskuntaa haavoittavia toimia (poliittisia, diplomaattisia, sotilaallisia, taloudellisia, informatiivisia, teknologisia tai infrastuktuuriin vaikuttavia toimenpiteitä). Kysymys on perinteisistä ja uusista menetelmistä, joita valtiolliset tai valtiosta riippumattomat toimijat voivat käyttää koordinoidusti tavoitteidensa saavuttamiseksi. Hybridivaikuttamisessa pyritään usein vaikuttamaan yhteiskunnan lisäksi yksilöön. Yhteiskunnan tukipilarit, kuten hyvinvointiyhteiskunta, yhtenäisyys ja yhteistoiminta voidaan pyrkiä haastamaan. Pidemmälle vietynä saattaa olla kysymys yllättävästä toiminnasta samanaikaisesti yhteiskunnan elintärkeitä toimintoja vastaan sekä eri osa-alueille kohdistettavan

paineen säätelystä halutulla tavalla. Hybridiuhkiin varautumiseen liittyy tärkeänä osana yhteiskunnan ja kansalaisten kriisinsietokyky.

Hybridiuhkassa voi olla kysymys vieraan valtion vihamielisestä vaikuttamisesta toisen valtion päätöksentekijöiden toimintaan laajalla keinovalikoimalla. Vieras valtio pyrkii yleensä toteuttamaan toimenpiteen siten, ettei kohdevaltio voi olla aivan varma, onko kyseessä vieraan valtion ohjaama tietoinen operaatio vai ei. Tavoitteena voi tilanteesta riippuen olla joko peittää valtion vaikuttamispyrkimys, jotta se voidaan kiistää, tai luoda epämääräinen kuva siitä, onko kyseessä valtion tietoinen vaikuttamispyrkimys vai ei. Tällöin hybridiuhka toimii valtion voimapolitiikan yhtenä välineenä.

Hybridiuhka on tullut terminä laajempaan käyttöön Ukrainan kriisin yhteydessä. Itse ilmiö ei kuitenkaan ole uusi. Vaikuttaminen on kuulunut suurvaltojen keinovalikoimaan aina. Tietotekninen kehitys on kuitenkin tuonut vaikuttamiseen aivan uusia ulottuvuuksia ja toimintamalleja. Vihamielisyyden aste on sen sijaan vaihdellut kulloisenkin poliittisen tilanteen mukaan. Vaikuttamisen torjunta on siten myös aiemmin ollut turvallisuus- ja tiedustelupalveluiden keskeinen tehtävä vakoilun torjunnan lisäksi.

Helsinkiin vuonna 2017 perustetun Euroopan hybridiuhkien torjunnan osaamiskeskuksen yhtenä tehtävänä on yhteisen tietoisuuden luominen hybridiuhkista EU:n jäsenvaltioiden kesken. Operatiivisen toiminnan kannalta tärkeä on myös EU IntCeniin perustettu EU:n hybridianalyysikeskus (EU Hybrid Fusion Cell).

Sisäisen turvallisuuden selontekomietinnössä hallintovaliokunta päätyy hybridiuhkiin varautumiseen ja niiden torjuntaan liittyen johtopäätökseen, että hybridi-, kyber- ja informaatio-operaatiot ovat tämän päivän todellisuutta ja että nämä uhkat on kyettävä tunnistamaan nykyistä tehokkaammin. Kysymys ei siten ole vain uhkasta, vaan siitä, että maahamme kohdistuu hybriditoimintaa.

Hybridivaikuttaminen on osa suurvaltojen sekä vahvojen poliittisten tai aseellisten ryhmien toimintaa oman vaikutusvallan lisäämiseksi, vastapuolen toiminnan häiritsemiseksi sekä omien taloudellisten ja poliittisten ja/tai sotilaallisten tavoitteiden saavuttamiseksi. Hybridivaikuttamisen toimijat on tapana jakaa valtiollisiin ja ei-valtiollisiin toimijoihin. Vieraiden valtioiden hybridivaikuttamisen keinot ovat aiempaa monimuotoisemmat (sotilaallinen, poliittinen, taloudellinen, infrastruktuuri, informaatio, kulttuuri, muut keinot). Kansallisen turvallisuuden kannalta tiedusteluviranomaisen kiinnostuksen kohteena hybridiuhista ovat valiokunnan saaman selvityksen perusteella erityisesti vaikuttaminen informaation ja propagandan avulla sekä kybertoiminta. Nykyisillä rikos- ja henkilöperusteisilla toimivaltuuksilla ei ole riittäviä edellytyksiä tunnistaa tai torjua ulkomaisia valtiollisia hybridiuhkia, jotka voivat vakavasti vaarantaa Suomen kansallista turvallisuutta.

Yhteiskunnan toimintaedellytysten lamaantumisen riskitekijöitä

Kansallisen huoltovarmuuden strategisena tavoitteena on turvata kriittisten infrastruktuurien, tuotannon ja palveluiden toimivuus siten, että ne kykenevät täyttämään väestön, talouselämän ja maanpuolustuksen välttämättömimmät perustarpeet kaikissa olosuhteissa.

Tavoitteena on, että myös vakavimmat poikkeusolot voidaan hoitaa kansallisin toimenpitein. Suomen huoltovarmuus on kuitenkin kriittisesti riippuvainen kansainvälisistä yhteyksistä. Esimerkiksi kaksi kolmasosaa energiasta tuodaan Suomen rajojen ulkopuolelta ja tästä kaksi kolmasosaa Venäjältä. Myös esimerkiksi logistiikka- ja finanssisektorit ovat keskeisesti osa maailmanlaajuista verkostoa.

Samaan aikaan, kun huoltovarmuuden riippuvuus kansainvälisistä materiaali-, logistiikka-, informaatio- ja finanssivirroista on lisääntynyt, huoltovarmuuden toimintaympäristö on muuttunut aiempaa ennakoimattomammaksi. Rajat ylittävät uhat, erityisesti kriittistä infrastruktuuria vastaan kohdistetut kyberuhat ja hybridivaikuttaminen voivat häiritä huoltovarmuuden tavoitteiden toteuttamista.

Vuonna 2017 päivitetyn yhteiskunnan turvallisuusstrategian mukaan keskeisiä talouden, kriittisen infrastruktuurin ja huoltovarmuuden uhkia ovat elintarvikehuollon, energiansaannin, kuljetuslogistiikan, rahoitus- ja maksujärjestelmän sekä tietoliikenteen ja tietojärjestelmien vakavat häiriöt, julkisen talouden rahoituksen saatavuuden häiriintyminen, kyberuhat, suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhat. Myös terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus voivat vaarantaa näitä toimintoja.

Suomen energiahuollon toimivuus ja erityisesti sähkön keskeytyksetön saanti on välttämätöntä yhteiskunnan elintärkeiden toimintojen turvaamiseksi. Verkkojen ohjaus- ja valvontajärjestelmät ovat suurelta osin tietoliikenteen varassa. Energian siirto- ja jakeluverkot voivatkin olla mahdollinen kohde terrori-iskulle, järjestäytyneelle rikollisuudelle tai sotilaalliselle vaikuttamiselle.

Globaali kybertoimintaympäristö muodostuu monimutkaisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansalaisten, viranomaisten ja yritysmaailman tietoverkkoja sekä kriittisen infrastruktuurin ohjaus- ja valvontajärjestelmiä. Useimmat yhteiskunnan palvelut ja toiminnot ovat kiinteästi sidoksissa tietoliikenteen kautta sähköisiin palveluihin.

Valtaosa yhteiskunnan kriittisistä palveluista perustuu tiedonsiirtoon ja sähköisten tietovarantojen käyttöön. Palvelut ovat tietoteknisesti ohjattuja tai ne ovat kokonaisuudessaan sähköisiä palveluja. Tietojärjestelmät ja niitä yhdistävät tiedonsiirtoverkot sulautuvat ja verkottuvat laajoiksi, jopa globaaleiksi kokonaisuuksiksi, joiden toiminnan häiriöt saattavat laajeta yksittäisistä palveluista laajasti järjestelmiä ja järjestelmäkokonaisuuksia koskeviksi. Valiokunta toteaa tässä yhteydessä, että uhkiin varautumiseen vaikuttaa keskeisesti käytettävän teknologian erittäin nopea kehittyminen. Sähköinen infrastruktuuri voi muodostaa haavoittuvan ja vaikeasti hallittavan kokonaisuuden. Uhkan merkittävyyttä lisää se, että sähköenergian varassa toimivia tieto- ja viestintäjärjestelmiä käytetään yhteiskunnan johtamiseen sekä väestön varoittamiseen häiriötilanteissa ja poikkeusoloissa. Valiokunta muistuttaa samalla, ettei tule tässä yhteydessä unohtaa myöskään muun muassa huoltovarmuuden turvaamisen edellyttämiä erilaisia fyysisiä huoltovarmuusreittejä.

Sähköisten palveluiden ja viestinnän toimivuutta voivat uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat onnettomuudet sekä järjestelmiin kohdistuvat tahalliset sähköiset ja fyysiset hyökkäykset. Saadun selvityksen mukaan viime vuosina usein käytetty menetelmä on palveluiden häirintä internetin kautta tapahtuvalla palvelunestohyökkäyksellä. Sen

tarkoituksena on ylikuormittaa verkkopalvelimet tai palveluntarjoajan toimintakapasiteetti automaattisesti muodostettavilla viesteillä. Internetpalveluiden häirintään on myös lukuisia muita mahdollisuuksia.

Suomen valtioon tai yhteiskuntaan kohdistuva, valtiollisen toimijan tai esimerkiksi terroristijärjestön tahallisesti aiheuttama kyberhyökkäys voi olla osa laajempaa kriisiä tai konfliktia Euroopassa. Tietoliikenteen ja sähköisten palveluiden yhteiskunnallisen merkityksen vuoksi ne ovat tärkeitä elementtejä myös poliittisissa ja sotilaallisissa kriiseissä. Useimpien valtioiden sotilaalliseen varautumiseen liittyy valmius tietojärjestelmien häirintään, hyväksikäyttöön ja tuhoamiseen. Informaatiosodankäynti on kiinteä osa nykyaikaista sotilaallista varautumista. Järjestelmiin voidaan kohdistaa verkon kautta vaikuttamisen lisäksi perinteisempiä ja vaikutuksiltaan voimakkaampia keinoja, kuten sähkömagneettista pulssia (EMP), mikroaaltoaseita (HPM) tai fyysistä tuhoamista. Valtioiden toteuttamat kyberoperaatiot ovat todennäköisesti vain yksi osa muunlaista painostusta, joten kyberoperaatioiden rinnalla esiintynee myös poliittista, taloudellista ja kenties myös sotilaallista painostusta sekä vaikuttamista sosiaalisessa mediassa ja muissa viestimissä, jolloin voidaan puhua hybridioperaatiosta.

Kriittiseen rahoitusmarkkinainfrastruktuuriin kohdistuvalla kyberhyökkäyksellä voidaan lamauttaa yhteiskunnan toiminnan kannalta välttämätön maksuliikenne ja horjuttaa rahoitusmarkkinoiden vakautta. Kyberhyökkäyksen kohdistaminen sosiaali- ja terveydenhuoltojärjestelmään, energiantuotantoon tai teollisuuden ohjausjärjestelmiin saa pahimmillaan aikaan materiaalista tuhoa ja ihmishengen menetyksiä. Näihin saatetaan yhdistää perinteisiä fyysistä tuhoa aiheuttavia toimia.

Verkon tahattomat tai tahalliset häiriöt voivat kohdistua kaikkiin sellaisiin toimijoihin, jotka käyttävät sähköisiä tietoverkkoja, kuten kaupankäynti, teollisuus, yhteisöt ja julkiset palvelut. Toimiva huoltovarmuus edellyttää aiempaa enemmän turvallisuusympäristön ennakoivaa ja ajanmukaista seurantaa. Turvallisuusympäristön seuranta ei voi rajoittua ainoastaan lähialueille, vaan kykyä havainnoida kauempaa tulevia uhkia tulee kehittää. Saadun selvityksen mukaan kyky ennakoivaan ja ajantasaiseen globaalin toimintaympäristön seurantaan on tällä hetkellä heikko.

Valiokunta painottaa, että lisääntyvä riippuvuus kriittisistä tieto- ja viestintäjärjestelmistä sekä kybertoimintaympäristöstä korostaa kyberturvallisuuden merkitystä yhteiskunnan kriittisten toimintojen turvaamisessa. Eri toimintojen ja järjestelmien keskinäisriippuvuus ja monimutkaistuminen lisäävät häiriöherkkyyttä. Tämän vuoksi on tärkeää parantaa eri toimijoiden mahdollisuuksia torjua kriittistä infrastruktuuria vastaan kohdistuvia kyberhyökkäyksiä.

Yhteenvetoa

Suomen turvallisuuspoliittinen toimintaympäristö on muuttunut monin tavoin. Valiokunta painottaa, että muutos on ollut käynnissä jo pidempään, mutta muutoksen nopeus on viime vuosina kiihtynyt.

Kansallisella kyberkyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen sekä Suomen kilpailukyvyn kannalta. Suomi on yksi maailman digitalisoituneimmista yhteiskunnista.

Nykyisessä turvallisuusympäristössä ovat keskeisesti esillä muutosnopeus, ennalta arvaamaton epävakaus ja kompleksisuus. Lisäksi teknologia ja digitalisaatio ulottuvat lähes kaikille elämänalueille. Yhteiskunta on tämän kehityksen myötä yhä riippuvaisempi ja toisaalta myös haavoittuvaisempi kuin koskaan aikaisemmin. Tällä hetkellä lainsäädäntömme ei ota huomioon kybertoimintaympäristön erityispiirteitä. Lisäksi viimeaikainen huolestuttava kehitys Suomen turvallisuusympäristössä korostaa tarvetta luoda nopealla aikajänteellä säädöstöä ja menetelmiä, joilla parannetaan kyberuhkiin liittyvää torjunta- ja ennakointikykyä.

Kyberuhkat ovat muuttuneet vaikutuksiltaan aiempaa moninaisemmiksi ja haitallisemmiksi niin yksittäisille ihmisille, yrityksille kuin suomalaiselle yhteiskunnalle.

Sen lisäksi, että maahamme kohdistuvan terrorismin uhka on vakavampi kuin koskaan, erityistä huolta on viime aikoina aiheuttanut ääriryhmien ja terroristien kykyjen kehittyminen digitaalisessa toimintaympäristössä. Esimerkiksi ISIS on tehokkaasti hyödyntänyt eri digitaalisia kanavia propagandansa levittämisessä, rekrytoinnissa, rahaliikenteensä hoitamisessa sekä keskinäisessä viestinnässä. Ääriryhmien motiivi luoda pelkoa ja tehdä järjettömiltä tuntuvia iskuja on antanut aiheen pohtia, olisiko ISIS:llä lähivuosina kykyä tehdä digitaalisen maailman kautta iskuja, joilla olisi ihmishenkiä uhkaavia vaikutuksia fyysisessä maailmassa. Erityisesti Yhdysvalloissa ja Isossa-Britanniassa on arvioitu ISIS:n pyrkivän kyberhyökkäyksillä vaikuttamaan kriittisen infrastruktuurin, kuten vesi- ja voimalaitoksien, toimintaan.

Yhteiskuntamme on korostetun riippuvainen luotettavasta tieto- ja viestintäteknologiasta ja automaatiosta. Riippuvuus synnyttää haavoittuvuutta. Tekniseen infrastruktuuriin kohdistetun tahallisen häirinnän keinoin voidaan vaikuttaa laajalti koko yhteiskunnan prosesseihin rahaliikenteestä joukkoliikenteeseen ja tiedonvälityksen kautta energianjakeluun, teolliseen tuotantoon ja jopa vaaleihin. On tärkeää, että valmisteilla olevista hyökkäyksistä saadaan ennakkotietoa tiedustelun keinoin.

Kybermaailmassa muutosajureita on useita, niistä keskeisin on aika. Kyberhyökkäyksen valmistelu on mahdollista toteuttaa salassa ja pitkän ajan kuluessa, mutta itse hyökkäys voidaan toteuttaa erittäin lyhyessä ajassa. Tammikuussa 2003 verkkomato Slammer levisi noin 10 minuutissa hyökkäyksen aloittamisesta arviolta 90 prosenttiin suunnitelluista kohteista (internetiä ohjaavat palvelimet). Slammer aiheutti internetin toiminnan maailmanlaajuisen hidastumisen. Arvioiden mukaan Slammer-verkkomadon kustannukset nousivat 750 miljoonaan euroon.

Tietoverkkoihin ja järjestelmiin kohdistuu yhä enemmän kohdistettuja hyökkäyksiä, tietoturvaloukkauksia sekä haittaohjelmatartuntoja. Vuosien 2012—2017 aikana vuoden aikana havaittujen haittaohjelmien määrä on kasvanut 100 miljoonasta yli 700 miljoonaan (400 000 uutta haittaohjelmaa joka päivä). Hyökkäykset kohdistetaan kansallisiin salassa pidettäviin tietoihin, aineettomiin pääomiin ja henkilötietoihin. Tiedusteluorganisaatiot pyrkivät keräämään heitä kiinnostavaa tietoa poliittisen, taloudellisen tai sotilaallisen edun saavuttamiseksi.

Erityisen haitallisia ovat olleet kohdistetut hyökkäykset (APT), joissa kohde on valittu tarkasti ja kohteesta on myös kerätty tarvittava määrä tietoa hyökkäyksen mahdollistamiseksi. Kohdistetuissa hyökkäyksissä hyökkääjä hyödyntää aktiivisesti löydettyjä kohdeorganisaation palvelujen haavoittuvuuksia ja heikkouksia. Haavoittuvuuksia on ihmisten toiminnassa, organisaatioiden

turvallisuusprosesseissa ja teknologiassa (ohjelmistoissa ja laitteissa). Hyökkäyksiä voidaan muuntaa ja kehittää, jotta voidaan hyödyntää kohdeorganisaation heikkouksia mahdollisimman hyvin. Kohdistetut hyökkäykset toteutetaan usein kampanjoina, jolloin ne koostuvat sarjasta epäonnistuneita ja onnistuneita yrityksiä päästä syvemmälle ja syvemmälle kohdeorganisaation verkkoon.

Johtopäätöksenään hallintovaliokunta katsoo edellä lausutun perusteella, että Suomeen tarvitaan uutta lainsäädäntöä, joka mahdollistaa toimivaltaisille viranomaisille tehokkaan tiedustelutiedon hankinnan:

— maamme turvallisuusympäristön kehityksestä valtiojohdon päätöksentekoa varten
— maamme kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka ei ainakaan vielä ole edennyt rikoksen asteelle
— maamme kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka tapahtuu ulkomailla
— maamme kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, jonka taustahenkilöt eivät ole tiedossa.

Hallituksen esityksen perusteluista ilmenevistä syistä ja saamansa selvityksen perusteella hallintovaliokunta pitää ehdotusta perustuslain 10 §:n muuttamisesta perusteltuna ja puoltaa sen hyväksymistä. Valiokunta pitää myös tähän mennessä saamansa selvityksen perusteella siviilitiedustelulain säätämistä tarpeellisena. Valiokunta tulee ottamaan asiaan tarkemmin kantaa tältä osin erikseen laatiessaan mietintöä hallituksen esityksestä HE 202/2017 vp. Yleisesti voidaan todeta tässä yhteydessä, että siviilitiedustelulain säätäminen tuo suojelupoliisille uusia toimivaltuuksia valtiojohdon tiedonsaannin turvaamiseksi ja kansallista turvallisuuta vakavasti uhkaavan toiminnan torjumiseksi.

Hallintovaliokunta ei ota kantaa perustuslakivaliokunnan toimialaan kuuluvaan kysymykseen kiireellisestä perustuslain säätämisjärjestyksestä. Valiokunta toteaa kuitenkin, että se on sisäisen turvallisuuden selontekomietinnössään HaVM 5/2017 vp pitänyt välttämättömänä, että maamme omilla viranomaisilla on toimivaltuudet ja kyky saada asianmukaista tietoa maamme elintärkeisiin intresseihin kohdistuvista uhkista. Mainitun mietinnön mukaan onkin välttämätöntä kyetä hankkimaan tiedustelutietoa vakavista maamme kansallista turvallisuutta uhkaavista toiminnoista ja tapahtumista. Lisäksi käsiteltävänä olevan hallituksen esityksen valiokuntakäsittelyssä kuullut asiantuntijat ovat laajalti esittäneet kantanaan, että hallituksen esitykseen HE 202/2017 vp sisältyvä siviilitiedustelulainsäädäntö olisi ollut perusteltua saattaa voimaan jo nykyistä aiemmin.

VALIOKUNNAN PÄÄTÖSESITYS

Hallintovaliokunta esittää,

että perustuslakivaliokunta ottaa edellä olevan huomioon.

Helsingissä 11.4.2018

Valiokunnan lausunto HaVL 7/2018 vp

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

varapuheenjohtaja Timo V. Korhonen kesk
jäsen Anders Adlercreutz r
jäsen Antti Kurvinen kesk
jäsen Sirpa Paatero sd
jäsen Olli-Poika Parviainen vihr
jäsen Juha Pylväs kesk
jäsen Veera Ruoho kok
jäsen Joona Räsänen sd
jäsen Vesa-Matti Saarakkala sin
jäsen Matti Semi vas
jäsen Mari-Leena Talvitie kok
jäsen Tapani Tölli kesk
varajäsen Lasse Hautala kesk

Valiokunnan sihteereinä ovat toimineet

valiokuntaneuvos Ossi Lantto
istuntoasiainneuvos Henri Helo