16.2.2018

Marko Meriniemi
lainsäädäntöneuvos

Eduskunnan hallintovaliokunnalle

Hallituksen esitys laiksi Suomen perustuslain 10 §:n muuttamisesta

1 Suomen turvallisuusympäristön muutos

1.1 Muutoksen vaikutuksista

Sisäisen turvallisuuden strategia hyväksyttiin valtioneuvostossa 5.10.2017. Strategia pohjautuu toukokuussa 2016 eduskunnalle annettuun sisäisen turvallisuuden selontekoon. Hallitus vahvisti keväällä 2017 uuden turvallisuuden painopistealueen. Strategian ja selonteon mukaan Suomen turvallisuusympäristö on kiistatta monimutkaistunut. Uudet haasteet ja tehtävät edellyttävät viranomaisilta asianmukaista suorituskykyä.

Suojelupoliisin havainnoissa korostuu omaan toimialaan liittyvä voimakas turvallisuusympäristön muutos, joka kytkeytyy Suomen kokonaisturvallisuuteen laajemmin. Vakavimmat Suomen kansallista turvallisuutta uhkaavat tekijät liittyvät nykyään usein Suomen ulkopuolisiin tapahtumiin. Yleisen globalisoitumiskehityksen seurauksena yksittäisten valtioiden turvallisuuskysymykset ovat kansainvälistyneet. Ulkomaista alkuperää olevan ja siellä syntyvän uhan seuraukset saattavat näkyä Suomessa aiempaa nopeammin. Suomen turvallisuutta merkittävimmällä tavalla uhkaavat ilmiöt ja niiden taustatekijät liittyvät lähes poikkeuksetta maamme ulkopuolisiin ja osin vaikeasti hahmotettaviin tapahtumiin, ilmiöihin ja kehityssuuntiin.

Negatiiviset tapahtumat ja jännitteet kansainvälisessä politiikassa heijastuvat myös Suomen turvallisuus-ympäristöön. Näitä muutoksia ja niiden nopeutta on aiempaa vaikeampi ennakoida ja arvioida. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhkille on yhteistä se, että niiden taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa.

Turvallisuusympäristön muutoksiin on pystyttävä vastaamaan ajanmukaistamalla turvallisuusviranomaisten toimivaltuuksia sekä parantamalla viranomaisten suorituskykyä, jotta Suomen valtion johdolle ja kansallisesta turvallisuudesta vastaaville viranomaiselle pystytään luomaan parempi tilannekuva Suomen turvallisuusympäristöstä ja siihen kohdistuvista vakavista uhkista. Tällä hetkellä suomalaisen yhteiskunnan mahdollisuudet reagoida kansalliseen turvallisuuteen kohdistuviin uhkiin ovat merkittävässä epäsuhdassa uhkien toteutumisesta aiheutuvien vahinkojen kanssa. Vahinkojen mittavuudesta voidaan mainita esimerkiksi Ranskassa tapahtuneet terrori-iskut, jotka Ranskan viranomaisten mukaan aiheuttivat Ranskalle arviolta 750 miljoonan euron menetykset pelkästään turismin vähentymisenä (Reuters in Paris 23.8.2016). Brysselin terroristi-iskujen arvioitiin maksaneen Belgian taloudelle lähes miljardin verran (Politico 26.7.2016).

1.2 Terrorismi

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 mahdollisesti 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.

Syyrian ja Irakin konfliktialueella oleskelee tällä hetkellä kymmeniä Suomesta matkustaneita henkilöitä, heidän joukossaan useita lapsia. Syyrian ja Irakin alueella toimivien terroristijärjestöjen hallinnoimilla alueilla on kasvamassa uusi jihadistisukupolvi, jossa on mukana myös suomalaisia. Tästä johtuen ilmiö tulee vaikuttamaan 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" (ISIL) propagandassa; propagandaa on julkaistu suomeksi ja iskuihin kehotetaan myös Suomessa. Sekä suomalaisten että Suomesta matkustaneiden tiedetään osallistuneen propagandan tuottamiseen, ja joissain tapauksessa 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.

Suojelupoliisin arvion mukaan Suomeen kohdistuva terrorismin uhka on neliportaisella tasolla ilmaistuna tällä hetkellä tasolla 2 - kohonnut. Uhka on vakavampi kuin koskaan aiemmin. Suojelupoliisin tietoon on tullut aiempaa vakavampia terrorismiin kytkeytyviä suunnitelmia ja hankkeita. Terrorismin uhka Suomessa on noussut muiden Pohjoismaiden tasolle, eikä terrorismin toimintaympäristössä ole nähtävissä lainkaan uhkaa laskevia kehityskulkuja. Päinvastoin uhkan kasvu on todennäköistä keskipitkällä aikavälillä. Suomen uhkatilanteen muutoksessa merkittävää on sen nopeus. Muissa Pohjoismaissa vastaava muutos tapahtui pidemmällä aikavälillä, jolloin siihen kyettiin 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. Muutos on ollut siis myös laadullista, ja 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.

Suojelupoliisi kohdistaa jatkuvasti toimenpiteensä ja tiedonhankintansa korkeimman uhan muodostaviin henkilöihin. Kohdehenkilöiden määrän kasvun johdosta kohdentamisessa joudutaan noudattamaan voimakasta priorisointia. Erityisen tärkeää terroristisen uhkien osalta on hankkia tietoa mahdollisimman ennakoivasti, jotta uhkia kyettäisiin torjumaan ennen niiden muodostumista välittömiksi. Suojelupoliisin keskeisenä roolina on tämänkaltaisen tiedustelutiedon hankkiminen.

1.3 Tiedustelu

Laittoman tiedustelutoiminnan torjuminen on muuttunut nopeasti aiempaa monimutkaisemmaksi. Ulkomaisten tiedustelupalveluiden tiedustelutoiminta

Suomessa on aktiivista. 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. Suojelupoliisin tietoon tulee 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.

Vastatiedustelun olennaisena peruslähtökohtana on löytää tiedustelutoimintaa harjoittavat henkilöt, joiden toiminta muodostaa vakavan uhkan kansalliselle turvallisuudelle. Nämä henkilöt eivät kuitenkaan ole aina tiedossa. Siksi tiedustelutoimivaltuudet pitäisi käyttöperusteiden kohdalla irrottaa nykyisten toimivaltuuksien rikos- ja henkilöperusteista.

1.4 Kybertoimintaympäristö

Kybertoimintaympäristön merkitys kasvaa, eikä kyberkeinojen käyttöä poliittisten päämäärien saavuttamiseksi voida sulkea pois. Tietoliikenneverkkojen kautta tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion 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 Yhdysvaltojen vaaleihin vaikuttaminen.

Suomen turvallisuusympäristön muutoksen kannalta olennaiset ulkovallat panostavat mittavasti hyökkäyksellisen kyberkapasiteettinsa rakentamiseen. Tämä vaatii näiltä valtioilta aiempaa enemmän tukea perinteisessä reaalimaailmassa tapahtuvalta tiedustelutoiminnalta, kuten tiedonkeräämistä henkilötiedustelun keinoin potentiaalisista kybervakoilun kohteista tai sellaisen henkilön löytämistä joka vahingossa tai tarkoituksellisesti auttaisi valtiollisen haittaohjelman viemisessä kohdeorganisaation tietojärjestelmään.

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

Kybervakoilun ja -operaatioiden merkitys kasvaa tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Esimerkkeinä valtioihin kohdistuneesta kyberoperaatioista voidaan mainita muun muassa Ukrainan (2014), Georgian (2008) ja Viron (2007) suljettuihin viranomaisverkkoihin kohdistetut verkkohyökkäykset, jotka ovat osoittautuneet hyvin organisoiduiksi ja suunnitelluiksi operaatioiksi, joiden taustalla arvioidaan olevan valtiotoimija tai siihen hyvin läheisesti kytkeytyvät tahot.

Jo nykyisellään uutisoidaan globaalisti hakkeroinneista toisen valtion ohjusjärjestelmiin ja ydinvoimaloihin sekä niin sanottujen kyberpommien kätkemisestä. Myös Suomen kriittisen infrastruktuurin tietojärjestelmiä ja tietoliikenneyhteyksiä sekä avainhenkilöitä tiedustellaan ennakolta, jotta niihin voidaan tarvittaessa vaikuttaa.

Yksityisten yritysten tietopääoman anastamiseen pyrkivistä hyökkäyksistä iso osa jää kokonaan pimentoon, koska yrityksillä tai kolmannella sektorilla ei ole valmiutta tunnistaa valtiollisen toimijan uhkaa. Erityisen kriittisiä uhkia ovat kyberoperaatiot, joissa hyökkääjä on hyväksikäyttänyt suoraan organisaation luotettuja

palveluketjutoimintoja. Tieto hyökkäyksistä tulee suojelupoliisille lähes poikkeuksetta ulkomaisten kumppanien vinkkeinä. Viedyn tietopääoman arvo keskisuuren yrityksen tapauksessa on kymmeniä miljoonia euroja vuodessa. Hyökkäystoiminnan nopea havainnointi minimoisi viedyn tiedon määrän ja sen aiheuttamat potentiaaliset menetykset yritykselle.

Vaikka luotetuilta kumppaneita saadut vinkit auttavat Suomea vastaan kohdistuvien yksittäisten hyökkäysten torjunnassa, tulee huomioida, että ulkomaisten kumppaneiden toiminnan pääprioriteetti on niiden kansallisten toimijoiden suojaaminen. Tiedon välitys Suomen kaltaisille kumppaneille on toissijaista ja aiheuttaa siten välillä merkittävän, kuukausienkin viiveen tiedon saannissa ja edelleen suojautumisessa.

Tietoverkkoihin kohdistuvat hyökkäykset ovat erittäin vaarallinen uhka kahdesta syystä: niihin soveltuva teknologia kehittyy jatkuvasti, ja niissä on usein valtiotoimijoiden apuna järjestäytyneen rikollisuuden edustajia ja hakkereita. Valtiollinen toiminta, kansalaisyhteiskunta ja rikollisuus sulautuvat toisiinsa, joten uhkien torjumiseksi turvallisuusviranomaisten teknisen suorituskyvyn olisi oltava hyökkääjää parempi. Suorituskyvyn käyttämiseen tarvittavien valtuuksien tulisi olla käyttöperusteeltaan olla sellaiset, että uhkien muodostuminen voidaan havaita mahdollisimman aikaisin. Jos viranomaiset kykenevät pelkään reagoimiseen vahinkojen jo tapahduttua, yhteiskunnan elintärkeät toiminnot ovat erittäin suuressa vaarassa.

Tietoliikennetiedustelu mahdollistaa ennakoivan puolustautumisen seuraamalla valtiollisten kybervakoiluoperaatioiden kartoitus- ja hyökkäystoimintaa tietoverkoissa ei vain omaa valtiota kohti, vaan myös muihin maihin kohdistuneena. Toiminnan käynnistämiseksi tarvittava tieto ja osaaminen on jo valtaosin olemassa.

1.5 Hybridivaikuttaminen

Hybridivaikuttaminen on osa suurvaltojen sekä vahvojen poliittisten tai aseellisten ryhmien toimintaa oman vaikutusvallan lisäämiseksi, vastapuolen toiminnan häiritsemiseksi ja omien 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). Suojelupoliisin kiinnostuksen kohteen hybridiuhista ovat erityisesti vaikuttaminen informaation ja propagandan avulla sekä kybertoiminta. Nykyisillä rikos- ja henkilöperusteisilla toimivaltuuksilla ei läheskään kaikissa tapauksissa ole mahdollisuuksia tunnistaa tai torjua ulkomaisia valtiollisia hybridiuhkia, jotka voivat vakavasti vaarantaa Suomen kansallista turvallisuutta.

Informaatiovaikuttamiseen voi liittyä esimerkiksi disinformaation levittämistä, kulttuuriin liittyvän vaikutusvallan kasvattamista, tietojärjestelmäkatkosten aiheuttamista tai hämmennyksen ja epävakauden ruokkimista. Tiedotusvälineet ja sosiaalinen media, mukaan lukien ns. trollien käyttö, on vain pieni osa toiminnasta. Teknisesti vaikuttamiskeinoille kehittyy aivan uusia mahdollisuuksia informaatio- ja kyberteknologian ansiosta. Esimerkiksi Yhdysvaltain presidentinvaaleissa erään globaalin sosiaalisen mediayhtiön tiedotteen mukaan sen palvelimelle laaditut valetilit olivat kahden vuoden aikana julkaisseet noin 80 000 päivitystä, joiden tarkoitus oli ollut vaikuttaa Yhdysvaltain politiikkaan. Presidentinvaalien alla levinneet viestit tavoittivat arviolta jopa 126 miljoonaa amerikkalaista.

Osa informaatio-operaatioista tapahtuu kyberhyökkäysten avulla. Tavoitteena voi olla sellaisten tietojen saaminen, joita voidaan käyttää informaatio-operaatioissa, tai vaikkapa haittaohjelmien asettaminen, jotta saadaan valmius toisen maan tietoliikenneyhteyksien katkaisemiseen tarvittaessa. Uudempi ilmiö on kyberhyökkäysten käyttäminen vaalikampanjoiden aikana ehdokkaiden mustamaalaukseen. Valtiollisten toimijoiden lisäksi huolena on kyberrikollisten kasvava kyky aiheuttaa merkittävää haittaa erilaisille yhteiskunnan kriittisille toiminnoille.

Valtioneuvoston kanslia julkaisi 17.2.2017 riippumattoman tutkimuksen Suomen kyberturvallisuuden tilasta (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017). Tutkimuksen mukaan kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen. Siksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on rajallinen. Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kyberuhkia vastaan ja myös häiriötilanteiden resilienssi (sietokyky) on edelleen osassa suojattavia kohteita heikolla tasolla. Suomen lainsäädäntöä ei ole kyetty ajanmukaistamaan kyberturvallisuuden vaatimuksia vastaaviksi. Tiedustelulainsäädännön uudistaminen arvioidaan välttämättömäksi havainnointikyvyn parantamiseksi.

2 Nykyisten toimivaltuuksien käytön oikeudelliset rajoitteet tiedustelutoiminnassa

Suojelupoliisin nykyisten toimivaltuuksien (salaisten tiedonhankintakeinojen) yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Niitä voidaan kohdistaa vain sellaiseen henkilöön tai käyttää hankittaessa tietoa vain sellaisen henkilön toiminnasta, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn rangaistusuhan ylittävään rikokseen, rikoksen yritykseen tai joissain tapauksissa sellaisen valmisteluun.

Rikostorjuntatoimivaltuuden käyttö tulee lähtökohtaisesti pystyä kohdistamaan aina tiettyyn henkilöön, vaikka henkilön henkilöllisyys ei tarvitse olla viranomaisen tiedossa. Telekuuntelu tai televalvonta voidaan kohdistaa myös tuntemattomaan henkilöön esimerkiksi IP-osoitteen perusteella, vaikka tiedusteluviranomaisella tulee olla tietty varmuus siitä, että kyseinen IP-osoite on tuntemattoman henkilön käyttämä. Jos tällaista tiettyyn henkilöön liittyvää rikostorjunnallista perustetta ei ole olemassa, ei poliisilain mukaisen salaisen tiedonhankintakeinon käyttö ole mahdollista.

Tiedustelutoiminnalle tyypillistä on, ettei tietty henkilö ole aina tiedossa, vaan tiedustelun olennaisena tavoitteena olisi löytää sellaiset henkilöt, joiden toiminta vakavasti uhkaa kansallista turvallisuutta. Siksi tiedustelutoimivaltuuksien käyttöperusteiden kohdalla tulisi irtaantua nykyisten toimivaltuuksien rikos- ja henkilöperustaisuudesta.

Kun nykyisten tiedonhankintatoimivaltuuksien käytön erityiset edellytykset on määritelty rikosten ja niiden vakavuuden perusteella, niin suojelupoliisin käytössä olevat toimivaltuudet eivät mahdollista nykyiselläänkään sille säädetyn tehtävän suorittamista muutoin kuin rikosten torjunnan ja selvittämisen osalta. Mutta sellaisten hankkeiden torjumiseksi, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta, ei salaisia tiedonhankintakeinoja voida käyttää.

Käsiteltävänä olevan lakiehdotuksen sekä edellä kerrotun perusteella tiedustelutoimivaltuuksien erityiset edellytykset määritellään siviilitiedustelulainsäädäntöä koskevassa hallituksen esityksessä (HE 202/2017 vp) uhkalähtöisesti. Salainen tiedonhankinta eli tiedustelumenetelmien käyttäminen ehdotetaan mahdollistettavaksi sellaisen laissa tyhjentävästi säädetyn toiminnan (siviilitiedustelun kohteet) kohdalla, joka vakavasti uhkaa Suomen kansallista turvallisuutta joko suoraan tai välillisesti. Kansallista turvallisuutta vakavasti uhkaava toiminta voi olla sellaista, joka konkretisoituessaan olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä taikka tekijä ei ole tiedossa. Toiseksi kyse voi olla sellaisesta kansallista turvallisuutta uhkaavasta toiminnasta, joka on tiedossa, mutta se tapahtuu toisen valtion alueella eikä siitä ole mahdollista saada tietoa kuin julkisista lähteistä. Kolmanneksi kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostuakaan. Esimerkkeinä voidaan mainita Suomen huoltovarmuuden kannalta merkityksellisten kiinteistöjen siirtyminen ulkomaiseen omistukseen tai toiminta, jolla suomalaiseen ja ulkomaiseen kansalaismielipiteeseen pyritään vaikuttamaan levittämällä järjestelmällisesti väärää tietoa Suomen politiikasta julkisuudessa.

3 Perustuslain 10 §:n muutoksen tarpeellisuudesta

Perustuslain muuttamista koskeva hallituksen esitys HE 198/2017 vp kytkeytyy sisäministeriössä ja puolustusministeriössä valmisteltuihin hallituksen esityksiin, joissa ehdotetaan säädettäväksi siviili- ja sotilastiedustelusta (HE 202/2017 vp ja HE 203/2017 vp).

Sekä tässä muistiossa edellä että siviili- ja sotilastiedustelulainsäädäntöä koskevissa hallituksen esityksissä selvitetään seikkaperäisesti Suomen turvallisuustilanteen heikkenemiseen ja monimutkaistumiseen liittyviä näkökohtia. Suomen turvallisuustilanteen ja -ympäristön muutokseen ovat vaikuttaneet muun ohella sotilaallisen toiminnan ja jännitteen 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. Teknologian kehittyminen on myös mahdollistanut kansallista turvallisuutta vaarantavien tekojen valmistelun ja toteuttamisen entistä lyhyemmässä ajassa. Samalla uhat ovat muuttuneet toteutuessaan vaikutuksiltaan aiempaa laajemmiksi, moniulotteisimmiksi ja vaarallisemmiksi yksittäisten ihmisten ja koko yhteiskunnan kannalta.

Suomen turvallisuustilanteen heikentyminen ja tarve varautua Suomen kansallista turvallisuutta vakavasti uhkaavaan toimintaan muodostavat hallituksen näkemyksen mukaan sellaisen poikkeuksellisen tilanteen, jossa perustuslain kiireelliselle muuttamiselle on osoitettavissa välttämätön tarve.

Siviili- ja sotilastiedustelulainsäädäntöä koskevissa hallituksen esityksissä ehdotetaan tiedusteluviranomaisille uusia toimivaltuuksia. Luottamuksellisen viestin salaisuuden suojaan puuttuvat toimivaltuudet edellyttävät perustuslain 10 §:n 3 momentin tarkistamista. Tällaisia säännösehdotuksia ovat siviilitiedustelua koskevassa esityksessä poliisilain 5 a lukuun esitettävä 6 § (telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta), 7 § (televalvonta), 11 § (tekninen kuuntelu), 31 § (lähetyksen jäljentäminen) ja lakiehdotuksessa tietoliikennetiedustelusta siviilitiedustelussa tarkoitettu tietoliikennetiedustelu. Vastaavia säännösehdotuksia esitetään sotilastiedustelulainsäädäntöä koskevassa hallituksen esityksessä. Jos nyt ehdotettu perustuslain muutos käsitellään normaalissa perustuslainsäätämisjärjestyksessä, voisivat näitä toimivaltuuksia koskevat säännökset sisäministeriön arvion mukaan tulla voimaan aikaisintaan vuoden 2020 alkupuolella, vaikka todennäköisempää on, että ne tulisivat voimaan 2020 loppupuolella.

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.