Turvallisuusympäristötietoisuus Poliisiammattikorkeakoulussa

Jani Vainio

2020 Laurea

Laurea-ammattikorkeakoulu

Turvallisuusympäristötietoisuus Poliisiammattikorkeakoulussa

Jani Vainio

Turvallisuusjohtaminen YAMK

Opinnäytetyö

Joulukuu, 2020

Laurea-ammattikorkeakoulu Tiivistelmä

Turvallisuusjohtamisen koulutusohjelma

Tradenomi (YAMK)

Jani Vainio

Turvallisuusympäristötietoisuus Poliisiammattikorkeakoulussa

Vuosi 2020 Sivumäärä 89

Turvallisuusympäristön muutos ja sen aiheuttamat vaikutukset Suomen sisäiseen turvallisuuteen edellyttävät poliisilta uudenlaista ajattelua ja turvallisuusympäristötietoisuuden lisäämistä. Turvallisuusympäristössä ilmenevien uhkien havaitseminen, niihin varautuminen ja niiden torjuminen vaatii kokonaisvaltaista turvallisuusajattelua ja sen kehittämistä.

Poliisille kuuluvien tavanomaisten tehtävien lisäksi on huomioitava turvallisuusympäristössä tapahtuvien muutosten aiheuttamat vaikutukset turvallisuuden ylläpitämiseen ja rikollisuuden torjuntaan sekä varauduttava yhteiskunnan toimintakykyä uhkaaviin häiriötilanteisiin. Poliisitoiminnan kannalta turvallisuusympäristön keskeisiä uhkia ovat informaatiovaikuttaminen, kyberuhat ja digitalisaatio, sähkön- ja energiansaannin häiriöt, ääriliikkeet ja terrorismi, järjestäytynyt ja rajat ylittävä rikollisuus sekä hybridivaikuttaminen.

Opinnäytetyö tehtiin Poliisiammattikorkeakoululle ja tutkimuksen tulokset ovat hyödynnettävissä poliisin tutkintokoulutuksissa sekä koulutukseen liittyvän materiaalin tuottamisessa. Opinnäytetyön tavoitteena ja tarkoituksena oli tutkia mitä turvallisuusympäristöllä tarkoitetaan ja mitä vaikutusta sillä on sisäiseen turvallisuuteen, mitä uhkatekijöitä turvallisuusympäristössä ilmenee sekä miten turvallisuusympäristön uhkia vastaan voidaan varautua. Keskeisenä tutkimuskysymyksenä oli selvittää, miten turvallisuusympäristötietoisuus poliisitoiminnassa rakentuu.

Opinnäytetyö toteutettiin laadullisena tutkimuksena, jossa tutkimusmenetelmänä käytettiin dokumenttianalyysia ja varsinaisena analyysimenetelmänä sisällön analyysia. Käytetty tutkimusaineisto perustui valtionhallinnon julkaisemiin strategioihin, selontekoihin, hankeraportteihin, aihealuetta koskevaan kirjallisuuteen sekä muihin työn kannalta tarpeellisiin dokumentteihin ja julkaisuihin.

Tutkimuksessa havaittiin turvallisuusympäristön muutosten vaikuttavan sisäiseen turvallisuuteen monin eri tavoin ja uhkien olevan monimuotoisia ja kompleksisia. Sisäisen turvallisuuden ylläpitäminen vaatii tulevaisuudessa resilienssikykyä ja varautumista yllätyksellisiin ja odottamattomiin uhkiin, mikä asettaa turvallisuusviranomaisille erityisiä suorituskykyvaatimuksia. Turvallisuusympäristön haasteisiin vastaaminen edellyttää tietoisuuden ja osaamisen kasvattamista, kokonaisturvallisuuden kehittämistä sekä kokonaan uudenlaista turvallisuusajattelua.

Tutkimuksen keskeisenä päätelmänä turvallisuusympäristötietoisuuden todettiin rakentuvan kolmesta keskeisestä osiosta, jotka ovat tietämys turvallisuusympäristön vaikutuksesta sisäiseen turvallisuuteen, turvallisuusympäristön erilaisten uhkien tiedostaminen sekä varautumisen merkityksen ymmärtäminen turvallisuusympäristön uhkia vastaan.

Asiasanat: sisäinen turvallisuus, poliisi, turvallisuusympäristö, uhka, varautuminen

Laurea University of Applied Sciences
Degree Program in Security Management
Master´s Thesis

Jani Vainio

Abstract

Security Environmental Awareness at the Police University College of Finland

Year 2020 Pages 89

Changes the security environment and effects the internal security of Finland require a new kind of thinking and increase security environment awareness policing. Detection of threats to the security environment, preparedness and combating against them demands comprehensive thinking security and its development.

In addition to the normal tasks of the police, it is necessary to take into account the effects of changes in the security environment on the maintenance of security and the fight against crime, and to be prepared for disturbances that threaten the functioning of society. Key threats to the security environment for policing include information interference, cyber threats and digitalisation, disruption of electricity and energy, extremism and terrorism, organized and cross-border crime, and hybrid interference.

The thesis was done for the Police University College of Finland and the results of the research can be utilized in police degree programmes and in the production of training-related material. The aim and purpose of the thesis was to research what is meant by the security environment and what effect it has on internal security, what threats occur in the security environment and how to prepare for threats in the security environment. The main research question was to find out how security environment awareness is taken into consideration in policing.

The thesis was carried out as a qualitative research, in which document analysis was used as the research method and content analysis as the analysis. The research material used was strategies, reports, project reports, literature and the other documents and publications necessary for the work.

The research found that changes in the security environment affect internal security in many different ways and that threats are diverse and complex. Maintaining internal security in the future requires resilience and preparedness for surprising and unexpected threats, which imposes specific performance requirements on security authorities. Meeting the challenges of the security environment requires increasing awareness and competence, developing overall security and a completely new kind of security thinking.

The main conclusion of the research that security environment awareness built on three main sections, which are knowledge of the impact of the security environment on internal security, awareness of various security environment threats and understanding importance of preparedness against security environment threats.

Keywords: internal security, police, security environment, threat, preparedness

Sisällys

1 Johdanto

Turvallisuusympäristömme muuttuu jatkuvasti ja siitä aiheutuvat heijasteet vaikuttavat yhteiskunnan turvallisuuteen ja eri toimintoihin. Turvallisuusympäristön ilmiöt, uhkat ja uudenlaiset haasteet vaativat samalla uudenlaista ajattelua ja turvallisuuden ymmärtämistä. Yhteiskunnan turvallisuuden ja siihen vaikuttavien uhkien tiedostaminen on erityisen tärkeää turvallisuudesta vastaaville viranomaisille. Turvallisuusympäristössä vaikuttavien muutosten ja uhkien ymmärtäminen on edellytys ennakoinnille ja varautumiselle sekä päivittäisille toimille yhteiskunnan turvallisuuden ylläpitämiseksi ja näihin uhkiin vastaamiseksi. Sisäisen turvallisuuden ja yhteiskuntarauhan ylläpitäminen kuuluu ensisijaisesti poliisille, mistä johtuen turvallisuusympäristötietoisuuden kehittäminen poliisissa ja poliisikoulutuksessa on ajankohtaista ja jopa välttämätöntä.

Poliisin on tavanomaisen toimintakenttänsä ja siihen kuuluvien tehtävien ohella huomioitava turvallisuusympäristössä tapahtuva muutos ja sen aiheuttamat heijastevaikutukset turvallisuuden ylläpitämiseen ja rikollisuuden torjuntaan. Turvallisuusympäristön nykyiset ilmiöt, haasteet ja erilaiset uhkatekijät ovat laajalaisia-alaisia, moniulotteisempia ja kompleksisia, muuttaen turvallisuusajattelun kokonaisuutta. Informaatiovaikuttaminen, kyberympäristö ja digitalisaatio, järjestäytynyt rikollisuus, terrorismi ja hybridivaikuttaminen jo itsessään yksittäisinä uhkina tai ilmiönä asettavat haasteita yhteiskunnan turvallisuudelle ja kytkeytyessään toisiinsa voivat aiheuttaa monimuotoisia ongelmia sekä mahdollisuuksia häiriötilanteiden syntymiselle.

Tämän opintonäytetyön tarkoituksena ja tavoitteena on kehittää poliisien tietoisuutta vallitsevasta turvallisuusympäristöstä, siinä esiintyvistä uhkista sekä niihin varautumisesta. Opinnäytetyö tehdään Poliisiammattikorkeakoululle ja sen tuloksia voidaan hyödyntää poliisin AMK- ja YAMK-tutkintokoulutuksissa sekä koulutukseen liittyvän materiaalin tuottamisessa. Erityisen tärkeää turvallisuusympäristön ja siinä esiintyvien uhkien laajempi tuntemus on strategisen ja operatiivisen johtamisosaamisen opinnoissa poliisin ylemmässä johtamiskoulutuksessa. Opinnäytetyö rakentuu kolmesta toisiinsa kytkeytyvästä osiosta. Työn alussa tarkastellaan turvallisuusympäristön muutoksen vaikutuksia Suomen sisäiseen turvallisuuteen. Toisessa osassa tutkitaan yhteiskuntaan ja kansalaisten turvallisuuteen kohdistuvia turvallisuusuhkia poliisitoiminnan kannalta ja lopuksi käsitellään yhteiskunnan ennakointia ja uhkiin varautumista.

1.1 Opinnäytetyön tarkoitus ja tavoite

Suorittaessani aiemmin poliisin YAMK-tutkintoa, tein opinnäytetyön aiheesta ”Sisäisen turvallisuusympäristön muutos ja turvallisuustoimintojen kehittäminen”. Opinnäytetyöhön liittyvää tutkimusta tehdessäni huomasin yhteiskunnan turvallisuuden ja sitä ympäröivien uhkien olevan huomattavan laaja kokonaisuus. Globaalissa ja yhä verkottuneemmassa maailmassa monet asiat

ja ilmiöt vaikuttavat jatkuvasti enemmän toisiinsa, eikä turvallisuutta tai sitä vaarantavia uhkia voida useinkaan enää tarkastella kapea-alaisesti tai pelkästään oman organisaation ja toiminnan näkökulmasta. Kyseisten opintojen aikana huomasin, että poliisihallinnossa yhteiskunnallinen turvallisuuskuva voi helposti rajoittua ainoastaan poliisille kuuluvaan yleisen järjestyksen ja turvallisuuden ylläpitämiseen ja rikostorjuntaan. Poliisin päivittäisessä toiminnassa sekä erityisesti johtamistehtävissä yhteiskunnan turvallisuuden kokonaisuutta tulisi kuitenkin pystyä tarkastelemaan tätä laajemmin.

Poliisin peruskoulutus muuttui vuonna 2014 AMK-tasoiseksi ja samalla päällystökoulutus YAMK-tasoiseksi, jolloin pedagogisen kehittämistyön keskeisenä tavoitteena nähtiin tulevan muutoksen systemaattinen ennakointi. Kehittämisajatukseen pohjautuvan toimintamallin mukaisesti Poliisiammattikorkeakoululla tulee systemaattisesti seurata työelämän muutostrendejä, sisäisen turvallisuuden kehittymistä sekä poliisin organisaatioon, työhön ja tehtäviin kohdistuvia muutoksia ja yksittäisen poliisin osaamiseen kohdistuvia odotuksia. (Alkiora 2018. 26-27.) Tällä opinnäytetyöllä osaltaan pyritään vastaamaan tähän tarpeeseen.

Muuttuneen kansainvälisen turvallisuustilanteen vaikutuksesta turvallisuuden osaamisen ja suorituskyvyn uudet vaatimukset perustuvat osin uudenlaisiin tarpeisiin, vaatimusten heijastuessa läpileikkaavasti Euroopan unionin ja sen jäsenmaiden muutosten hallintaan niin poliittisella kuin strategisella ja operatiivisella tasolla. Turvallisuuden muutosten hallinta edellyttää uudenlaista ajattelua ja toimintaa kaikilta turvallisuusyhteisön toimijoilta sekä yksittäisiltä osaajilta omissa tehtävissään. Turvallisuusympäristön muutosten hallintaa tuleekin tukea koulutuksella sekä muulla osaamisen kehittämisellä. (Häikiö & Talvitie & Muttilainen 2018, 57.)

Nykyiset turvallisuushaasteet ovat monimutkaisia, globaaleja sekä alati kehittyviä ja niillä on merkittäviä vaikutuksia lainvalvontatoiminnalle niin Euroopassa kuin sen ulkopuolella, joten ymmärrys turvallisuutta uhkaavista tekijöistä on keskeistä ajateltaessa poliisilta vaadittavaa osaamista näihin haasteisiin vastaamisessa. Turvallisuushaasteita aiheuttavia uhkatekijöitä ovat muun muassa terrorismi, hallitsematon muuttoliike, kyberrikollisuus sekä järjestäytynyt rikollisuus. Nykyisessä tilanteessa koulutuksen ja osaamisen kehittämisen eurooppalaistuminen näyttäytyy haasteena kaikille poliisi- ja turvallisuusalan oppilaitoksille Euroopassa. Osaamisen kehittäminen ja koulutus onkin oleellinen osa rajat ylittävää poliisiyhteistyötä sekä samalla myös tae onnistuneelle yhteistyölle. (Koivuniemi & Kemppainen 2018, 62.)

Opinnäytetyön keskeisenä tarkoituksena on tutkia ja selvittää, mitä turvallisuusympäristöllä tarkoitetaan, miten turvallisuusympäristön muutos vaikuttaa sisäiseen turvallisuuteen, mitä uhkatekijöitä turvallisuusympäristössä ilmenee sekä miten turvallisuusympäristön uhkia vastaan voidaan varautua.

1.2 Aihevalinnan perustelu

Toimintaympäristön ja sen myötä turvallisuusympäristön jatkuva muutos pakottaa Suomen sisäisestä turvallisuudesta vastaavat viranomaiset ja erityisesti poliisin suhtautumaan yhteiskunnan turvallisuuteen uudella tavalla. Nykyisen turvallisuusympäristön ollessa verkostomainen ja kompleksinen, siinä esiintyvät uhkatekijät voivat olla vaikeasti havaittavia, hallittavia ja siten vaikeasti torjuttavia. Uhkien haastavuudesta ja kompleksisuudesta johtuen päivittäistä turvallisuus- ja rikostorjuntatyötä tekevien poliisien on aiempaa paremmin ja kattavammin tiedostettava turvallisuusympäristön uhkatekijät sekä niiden mahdolliset vaikutukset poliisin tavanomaisiin tehtäviin, kuten yleisen järjestyksen ja turvallisuuden valvontaan ja rikostorjuntaan. Tämän lisäksi on hyvä ymmärtää uhkatekijöiden kokonaisvaltaisuus ja läpileikkaavuus sekä mahdolliset heijastevaikutukset yhteiskunnan eri toimintoihin.

Muuttuva turvallisuusympäristömme alleviivaa ennakoinnin ja laadukkaan tietojohtamisen merkitystä, sillä tiedon tehokkaampi hyödyntäminen merkitsee parempaa toimintakykyä, tietoperusteisen toiminnan korostuessa toiminnan kaikilla sektoreilla. Muutos aiheuttaa yhä merkittävämpiä haasteita koko yhteiskunnalle ja poliisitoiminnalle, sillä päivittäisen poliisitoiminnan, rikostorjunnan ja perinteisten uhkakuvien ohella poliisin tulisi kyetä vastaamaan jatkuvasti lisääntyviin uusiin turvallisuushaasteisiin. Onnistunut ennakointi, sekä strategisella että operatiivisella tasolla, parantaa organisaation ja yksilöiden valmiutta vastata kriiseihin sekä vahvistaa tiedonkulkua. Parhaimmillaan se tarkoittaisi ja tuottaisi myös parempaa poikkihallinnollista vuorovaikutusta. Tulevaisuutta paremmin ymmärtämällä ja sitä jäsentämällä, parannetaan tilannetietoisuutta, jolloin myös strateginen viestintä ja kriisiviestintä on tarvittaessa helpompaa. Strategisella ennakoinnilla tuetaan laadukkaampaa ja kustannustehokkaampaa tiedolla johtamista, jonka lisäksi ennakointi luo edellytyksiä tutkimukselle, osoittaen tulevia tietotarpeita. (Laitinen & Jukarainen 2018, 115.)

1.3 Tutkimusmenetelmä ja keskeinen tutkimuskysymys

Opinnäytetyö perustuu kvalitatiiviseen eli laadullisen tutkimukseen. Hirsjärvi, Remes & Sajavaara (2014, 161) pitävät laadullisen tutkimuksen lähtökohtana todellisen elämän kuvaamista, johon sisältyy ajatus siitä, että todellisuus on moninainen ja laadullisessa tutkimuksessa kohdetta pyritäänkin tutkimaan mahdollisimman kokonaisvaltaisesti. Laadullisessa tutkimuksessa on kyse tutkimusprosessista, jonka kohteena on jokin tutkijaa kiinnostava yhteiskunnan ilmiö, mikä voi olla uusi ja selittämätön, ja se halutaan ymmärtää. Laadullisen tutkimuksen tavoitteena on tutkittavan ilmiön kuvaaminen, ymmärtäminen ja tulkinnan antaminen. (Kananen 2017, 35 & 51.)

Laadullisessa tutkimuksessa pyritään ymmärtämään ilmiötä, selittämään ilmiön koostumusta, tekijöitä sekä niiden välisiä suhteita. Laadullisessa kysymyksessä vastataankin kysymykseen

”mistä tässä on kyse?”. (Kananen 2013, 26.) Tämän opinnäytetyön keskeisenä tutkimuskysymyksenä on selvittää, miten turvallisuusympäristötietoisuus poliisitoiminnassa rakentuu.

Eskolan & Suorannan (2001, 62-63) mukaan aineisto on kvalitatiivisessa tutkimuksessa tapauskohtainen, sillä vastauksia tarvitaan vain sen verran, kuin aiheen kannalta on välttämätöntä. Kananen (2017, 131) osaltaan toteaa tietoperustan tarkoittavan samaa kuin teoriaosa tai viitekehys. ”Teoriaosalla kirjoittaja osoittaa aiheeseen liittyvään substanssiin ja menetelmiin perehtymisensä.” Teoriaosa eli viitekehys ymmärretään myös tiedoksi, jota ilmiöstä on olemassa ja opinnäytetyön kirjoittaja nojaa ratkaisunsa tuohon tietoon tai luo uutta tietoa.

Laadullisen tutkimuksen aineistonkeruu voidaan toteuttaa primäärisillä tai sekundäärisillä menetelmillä. Primääriset tarkoittavat havainnointia, haastatteluita ja kyselyitä. Sekundäärisiä menetelmiä ovat erilaiset dokumentit, kuten kirjat, tutkimukset, vuosikertomukset, muistiot, tilastot, videot ja äänitteet sekä kuvat. Kaikkia kirjallisen aineiston muotoja on mahdollista käyttää aineistolähteinä ja kaikkea tutkimuksen kannalta merkityksellistä aineistoa voidaan hyödyntää tutkimusongelman ratkaisussa. (Kananen 2017, 120.)

1.4 Tutkimuksen toteuttaminen

Laadullisessa tutkimuksessa kyse on tutkimusaineiston käsittelystä ja sen analysoinnista. ”Analyysimenetelmillä tutkimusaineistosta puristetaan ratkaisu tutkimusongelmaan tai vastaukset tutkimuskysymyksiin.” Laadullisessa tutkimuksessa tekstejä käsitellään esimerkiksi sisältöanalyysin keinoin, kun vastaavasti kvantitatiivisessa tutkimuksessa tilastotieteellisin menetelmin. (Kananen 2017, 68.)

Tässä laadullisessa tutkimuksessa tutkimusmenetelmänä käytetään dokumenttianalyysia. Ojasalon, Moilasen & Ritalahden (2009, 121) mukaan ”dokumenttianalyysi on menetelmä, jossa päätelmiä pyritään tekemään kirjalliseen muotoon saatetusta erityisesti verbaalisesta, symbolisesta tai kommunikatiivisesta aineistosta. Tarkastelun kohteena olevia dokumentteja voivat olla esimerkiksi tekstiksi muutetut haastattelut, www-sivut, lehtiartikkelit, vuosikertomukset, markkinointimateriaalit, ideointipalaverien muistiot, päiväkirjat, puheet, keskustelut, raportit ja muut kirjalliset materiaalit.” Dokumentteina voidaan käyttää kaikkea tutkittavasta ilmiöstä kirjoitettua, puhuttua tai kuvattua materiaalia, jopa esineistöä, ja tavoitteena on dokumenttien järjestelmällinen arviointi sekä sanallisen ja selkeän kuvauksen luominen tutkittavasta ja kehitettävästä aiheesta. Analyysilla lisätään aineiston informaatioarvoa ja luodaan siihen selkeyttä luotettavien ja selkeiden johtopäätösten tekemiseksi. Dokumenttianalyysin vahvuutena on sen herkkyys asiayhteydelle eli sille, millaisena kehittämisen kohteena oleva ilmiö luonnollisessa ympäristössään näyttäytyy. Dokumenttianalyysia käytetään laajasti esimerkiksi tulevaisuuden tutkimuksessa, jossa tavoitteena on trendien tunnistaminen.

Anttila (2014) mainitsee dokumenttianalyysin tarkoittavan kaiken sellaisen todennettavissa olevan ja sosiaalisia tekijöitä sisältävän tutkimusaineiston analyysia, jota ei saada kokoon suoria ja välittömiä havaintoja tekemällä. Dokumenttien käyttämistä tutkimusaineistona voidaan lisäksi pitää vaihtoehtona sille, että aineistoa kerättäisiin haastattelemalla, kyselomakkeilla tai muulla vastaavalla tavalla ja joskus valmiin aineiston käyttäminen on myös ainoa mahdollisuus jotain tiettyä aihetta koskevan tiedon kokoamiseksi. Valmiit dokumentit ovat erittäin antoisia käytettäväksi silloinkin, kun tutkittava ilmiö on uusi eikä sen keskeisistä kysymyksistä ole vielä paljon tietoa. Dokumenttianalyysin heikkoutena on se, että kaikki aineisto on jo aiemmin ja kenties täysin muuhun tarkoitukseen koottu, jolloin dokumentteja useimmiten käytetäänkin ns. triangulaatiossa, eli useamman lähteen samanaikaisessa ja rinnakkaisessa käytössä. Dokumenttianalyysissa käytettävää dokumenttiaineistoa voivat olla esimerkiksi lait, asetukset, hallinnolliset päätökset, viralliset kirjeet, viranomaisten ohjeet jne. Dokumenttianalyyseissa on mahdollista soveltaa sekä määrällistä analyysia että laadullista analyysia, tavanomaisen sisällönanalyysin soveltuessa monenlaisten teksti- ja kuvadokumenttien käsittelyyn.

Tämän opinnäytetyön tutkimusaineisto perustuu valtiohallinnon julkaisemiin strategioihin, selontekoihin, hankeraportteihin, aihealuetta koskevaan kirjallisuuteen sekä muihin työn kannalta merkityksellisiin dokumentteihin ja julkaisuihin.

Dokumenttianalyysi voidaan toteuttaa kahdella keskeisellä, toisistaan eroavalla analyysitavalla, jotka ovat sisällön analyysi ja sisällön erittely. Sisällön analyysissa pyrkimyksenä on dokumenttien sisällön kuvaaminen sanallisesti, tavoitteena tekstin merkityksien etsiminen ja tunnistaminen. Sisällön erittelyllä puolestaan tarkoitetaan dokumenttien analysointia, jossa tekstin sisältöä kuvataan määrällisesti, erimerkiksi numeroin. Kyseiset tavat eivät ole toisiaan poissulkevia. ”Aineiston käsittely perustuu loogiseen päättelyyn ja tulkintaan, jossa aineisto aluksi hajotetaan osiin, käsitteellistetään ja kootaan uudestaan toisella tavalla loogiseksi kokonaisuudeksi.” (Ojasalo ym. 2009, 122.) Tässä opinnäytetyössä analyysitapana käytetään sisällön analyysia.

Tuomi & Sarajärvi (2002, 110-114) toteavat, että laadullisen aineiston sisällönanalyysi voidaan tehdä joko aineistolähtöisesti, teoriaohjaavasti tai teorialähtöisesti. Varsinaisesta aineiston analyysista puhuttaessa voidaan käyttää ilmauksia aineistolähtöinen eli induktiivinen tai teorialähtöinen eli deduktiivinen. Induktiivisen aineiston analysointi voidaan jakaa karkeasti kolmevaiheiseksi prosessiksi, johon kuuluu 1) aineiston redusointi eli pelkistäminen 2) aineiston klusterointi eli ryhmittely ja 3) abstrahointi eli teoreettisten käsitteiden luominen. Aineiston redusoinnissa analysoitava informaatio eli data kirjoitetaan auki ja pelkistetään siten, että aineistosta karsitaan pois kaikki tutkimuksen kannalta epäolennainen, mikä voi tarkoittaa informaation tiivistämistä tai pilkkomista osiin. Klusteroinnissa aineistosta koodatut alkuperäisilmaukset käydään tarkasti läpi ja etsitään samankaltaisuuksia ja/tai eroavaisuuksia kuvaavia käsitteitä. Klusteroinnin jälkeen seuraava vaihe on abstrahointi, jossa erotellaan tutkimuksen kannalta oleellinen tieto ja valikoidun tiedon perusteella muodostetaan teoreettisia käsitteitä.

Hirsjärvi ym. (2014, 164) muistuttavat, että induktiivisessa eli aineistolähtöisessä analyysissa tutkijan pyrkimyksenä on paljastaa odottamattomia seikkoja, mistä johtuen lähtökohtana ei ole teorian tai hypoteesien testaaminen, vaan aineiston monitahoinen ja yksityiskohtainen tarkastelu. Eskola & Suoranta (2001, 19) puolestaan toteavat aineistolähtöisen analyysin olevan tarpeellista varsinkin silloin, kun tarvitaan perustietoa jonkin tietyn ilmiön olemauksesta.

2 Turvallisuusympäristötietoisuus käsitteenä

”Viime vuosina on kansainvälinen kehitys ollut tulvillaan yllätyksiä. Monet niistä ovat sellaisia, että niiden kaikkia vaikutuksia ei vielä osata arvioida. Moni tuttu ja turvalliseksi koettu tosiasia on vaakalaudalla. Kehitykseen saattaa sisältyä vakaviakin uhkia, joista tunnistamme ehkä vain osan. Turvallisuuden ja uhkakuvien ominaispiirteiksi ovat määrittyneet muutosnopeus, osittainen ennalta-arvaamattomuus ja monimutkaisuus. Tällaisessa uhkien maailmassa elämme myös lähitulevaisuudessa.” (Limnéll & Iloniemi 2018, 7.)

Turvallisuus jo pelkästään terminä on laaja ja moniulotteinen, sisältäen kaksi erilaista lähestymistapaa. Englannin kielessä turvallisuutta kuvataan termeillä ”security” ja ”safety”. Yleisellä tasolla turvallisuudella tarkoitetaan vallitsevaa tilaa, jossa uhkat ja riskit ovat hallittavissa. Samoin sillä voidaan tarkoittaa toimintaa tai eri toimintojen kokonaisuutta, jolla pyritään uhkien ja riskien hallintaan tai ainakin tunteeseen siitä, että ne ovat hallinnassa. Termillä ”security” viitataan niin sanottuun ”kovaan” turvallisuuteen, jolla tarkoitetaan varautumista tarkoituksellista, vahingoittavaa toimintaan vastaan, kuten rikollinen toiminta, väkivalta tai aseellisen voiman käyttö. Kyse voi olla myös suojautumisesta jonkinlaisen hyökkäyksen varalta, tarkoittaen esimerkiksi valtion tai rakennuksen turvallisuutta hyökkääjiä vastaan. Termi ”safety” sen sijaan viittaa ”pehmeään” turvallisuuteen, jolloin turvallisuus ei vaarannu tarkoituksellisen toiminnan seurauksena, vaan vaikkapa tapaturmien, onnettomuuksien tai virheiden vuoksi, kuten työturvallisuus, potilasturvallisuus tai tuotteiden käyttöturvallisuus. Kokonaisturvallisuudesta puhuttaessa käytetään yleisemmin termiä ”security”, kun turvallisuudessa on kyse esimerkiksi yhteiskunnan toimijoiden yhteisestä toiminnasta, jolla pyritään uhkien ja riskien hallitsemiseen, tai tällaisella toiminnalla saavutettuun tilaan. (Kokonaisturvallisuuden sanasto 2017, 16.) Tässä työssä uhkien tarkastelukulma kohdentuu security-tyyppiseen "kovaan" turvallisuuteen.

Leppänen (2006, 52) mainitsee turvallisuus-käsitteen olevan monimerkityksinen, sillä turvallisuutta voidaan käsitellä yksilön kokemana tunteena tai toisaalta menetelmänä tai toimintona, jolla turvallisuuden tunne saadaan aikaan. Turvallisuus voi olla myös ominaisuus ja joillekin ammattiryhmille se on hyvinkin tärkeää. Turvallisuudella voidaan tarkoittaa lähes kaikkea mah-

dollista tai kuitenkaan samalla ei mitään erityistä. Turvallisuuden käsitettä käytetään puhuttaessa valtioiden välisistä suhteista, yritysrakenteiden suojaamisesta, yksilön hyvinvoinnin laadusta tai yleisesti vapauden vertauskuvana.

Turvallisuusympäristöllä ja sen muutoksella tarkoitan tässä työssä Suomen sisäistä ja ulkoista turvallisuutta, niiden keskinäisiä rajapintoja sekä keskinäisriippuvuutta. Yhteiskunnan turvallisuutta koskevissa sisäisen turvallisuuden selonteoissa painotetaan turvallisuusympäristön voimakasta muutosta, jossa sisäinen ja ulkoinen turvallisuus limittyvät vahvasti toisiinsa. Globaali turvallisuuskonteksti on viime vuosina muuttunut ja kansallisten rajojen ulkopuolella olevat tekijät vaikuttavat Suomen sisäiseen turvallisuuteen. Globaalin turvallisuuskontekstin kehityksen merkittävinä muutosajureita ovat toimineet erityisesti Lähi-idän ja Afrikan alueilta lähtöisin oleva väkivaltainen ekstremismi ja terrorismi sekä ääriliikkeiden vahvistuminen, voimakas Eurooppaan suuntautunut muuttoliike sekä muut merkittävät turvallisuusympäristön kehittymiseen vaikuttavat ilmiöt, kuten järjestäytynyt ja rajat ylittävä rikollisuus, hybridi-ilmiöt sekä kyberturvallisuuteen liittyvät haasteet. (Tiimonen & Nikander 2016, 13.)

Tiimonen & Nikander (2016, 13) täsmentävät, että turvallisuusympäristön kokonaiskehitystä leimaa nopeus ja lisääntyvä kompleksisuus, mikä samalla korostaa sisäisen turvallisuuden merkitystä ja monimutkaistaa turvallisuusympäristössä toimimista. Tästä johtuen turvallisuustoimijoille keskeistä on pyrkiä ennakoimaan kehitystä ja analysoida turvallisuusympäristöön liittyviä syy-seuraussuhteiltaan monitahoisia ilmiötä entistä proaktiivisemmin ja kokonaisvaltaisemmin. Turvallisuusympäristön analysoinnissa ja haasteisiin vastaamisessa tulee huomioida, että vastuu sisäisen turvallisuuden tuottamisesta kuuluu viranomaisten ohella monille muillekin yhteiskuntaan turvallisuutta tuottaville tahoille, kuten elinkeinoelämälle, sosiaali- ja terveystoimelle sekä oppilaitoksille. Kansallisten ja kansainvälisten toimijoiden keskinäinen vuoropuhelu sekä yhteistoimintamallien kehittäminen ja yhteensovittaminen onkin välttämätöntä turvallisuusympäristön kehitykseen mukanaan tuomiin haasteisiin vastaamiseksi.

Viimeisimmän Ulko- ja turvallisuuspoliittisen selonteon mukaan Suomen ja Euroopan lähialueiden turvallisuustilanne näyttäytyy epävakaana ja vaikeasti ennakoitavana, jossa suurvaltojen keskinäisen kilpailun voimistuminen ja niiden heikkenevä sitoutuminen sääntöpohjaiseen kansainväliseen järjestelmään ja kansainväliseen oikeuteen kiristävät kansainvälistä tilannetta. Suomen lähialueilla ilmeneviin jännitteisiin vaikuttaa muun muassa asevalvonnan sopimusjärjestelmän heikentyminen, vaikuttamiskeinojen kehittyminen ja monimuotoistuminen sekä kybertoimintaympäristön merkityksen kasvaminen. Suomen turvallisuusympäristön nähdään muuttuneen epävakaampaan suuntaan ja muutoksen arvellaan olevan pitkäkestoinen. (Valtioneuvosto 2020, 18.)

Suomi sijaitsee suurvaltojen näkökulmasta strategisesti merkittävällä alueella, mikä aiheuttaa suoria heijasteita kansainvälisen turvallisuustilanteen muuttuessa. Suomessa turvallisuutta tarkastellaan laajasta näkökulmasta, jossa sotilaallisten uhkien, suurvaltojen välisen kilpailun ja hybridivaikuttamisen lisäksi huomioidaan näköpiirissä olevien globaalien haasteiden, kuten ilmastonmuutoksen, terveysuhkien, ihmisoikeusloukkausten, muuttoliikkeen, talouskriisien, eriarvoisuuden lisääntymisen, terrorismin ja kansainvälisen rikollisuuden vaikutukset turvallisuuteen. Leimallista useille turvallisuuteen vaikuttaville globaaleille ilmiöille on niiden aiempaa tiiviimpi kytkeytyminen toisiinsa. Kiristyneestä kansainvälisestä tilanteesta huolimatta Suomeen ei kohdistu välitöntä sotilaallista uhkaa, joskin sotilaalliseen voimankäyttöön tai sillä uhkaamiseen on kuitenkin varauduttava. Suomen nykyisessä ulko- ja turvallisuuspoliittisessa toimintaympäristössä ja sen kehityspotentiaalin valossa Suomella ei ole mahdollisuutta eikä halua eristäytyä. (Valtioneuvosto 2020, 24-25.)

Yhteiskunnassa turvallisuus aiheuttaa keskustelua siitä, kuka tai mikä pitäisi turvata tai mitä uhkia vastaan suojaudutaan sekä kenen toimesta ja miksi. Turvallisuuden kovassa ytimessä on kyky varmistaa turvallisen olotilan jatkuminen ja arvioitujen uhkien hallinta. Usein turvallisuus mielletäänkin lähinnä toiminnan kautta, sen ollessa konkreettista tekemistä, turvallisuusuhkien torjuntaa sekä yleisen järjestyksen ja turvallisuuden ylläpitämistä. Turvallisuus liittyy läheisesti ihmisen perustarpeisiin ja oikeuksiin tai siitä voidaan keskustella arvona. Turvallisuudessa korostetaan lisäksi eettisiä ja moraalisia arvoja, joita siihen liittyy. On kuitenkin muistettava, että turvallisuus itsessään ei tarkoita mitään, vaan se saa merkityksensä vasta käyttöyhteydessään, mikä koskee myös uhkaa ja uhka-arvioita. Turvallisuudella ei siis tarkoiteta erilaisten riskien ja uhkien poissaoloa, vaan erilaisten uhkatekijöiden tiedostamista sekä riittävää varautumista niihin. (Limnéll & Iloniemi 2018, 15.)

Tämän työn keskeisenä teemana on tietoisuus turvallisuusympäristöstä, joten on oleellista selventää mitä käsitteellä tietoisuus tosiasiassa tarkoitetaan. Haikosen (2017, 202) mukaan tietoisuudella tarkoitetaan laadullista havaitsemista, jossa tietoisuuden sisältö koostuu todellisista ja virtuaalista aistihavainnoista, jotka voidaan ainakin jonkin aikaa muistaa ja raportoida. Tietoisen kokemuksen syntyyn tarvitaan myös huomion kiinnittyminen, sillä mitä emme huomaa, siitä emme voi olla tietoisia.

Hari ym. (2015, 104-110) puolestaan täsmentää tietoisuuden olevan yksi vaikeimmista mieleen liittyvistä käsitteistä ja usein tietoisuuden oletetaankin viittaavan yhteen tiettyyn mielen tilaan, kykyyn tai prosessiin ja toisinaan tietoisuus ajatellaan samaksi asiaksi kuin mieli, joista kuitenkaan kumpikaan ei tee oikeutta tietoisuuden eikä mielen ilmiöille. Tietoisuuden yksi merkitys on tajuisuus, sillä tajuton ihminen ei voi reagoida ulkoisiin ärsykkeisiin eikä kykene kommunikoimaan. Tietoisuuden toinen käsite on tarkkaavaisuus, jolla tarkoitetaan joko ulkoisten ärsykkeiden laukaisemaa "tahatonta" tai yksilön " tahdonalaista huomion suuntaamista johonkin

asiaan tai toimintaan. Tarkkaavaisuus tosin toimii osittain tiedostamattomasti valikoiden tietoiseen jatkokäsittelyyn lähinnä huomiota kaipaavia ympäristön viestejä. Tietoisuuden kolmas käsite on kokemuksellinen tietoisuus, jolla viitataan siihen, miltä aistiminen, kokeminen ja tekeminen tietoisuuden virrassa tuntuu. Kun tajuisuutta määritellään ulkoisten reaktioiden perusteella, vastaavasti kokemuksellinen tietoisuus määritellään sen sisäisen, subjektiivisen, sisällön perusteella. Neljäs tietoisuuden merkitys viittaa tietoiseen ajatteluun, jota voidaan kutsua myös reflektiiviseksi tietoisuudeksi. Kokemuksellisen tietoisuuden sisältöjä voidaan yrittää kuvata kielellisestä, mutta tietoisen ajattelun sisällöt ovat jo kielellisiä. Puhuttaessa tietoisesta toiminnasta, tietoisuutta käytetään toiminnan määreenä, jolloin tietoinen toiminta on tarkoituksellista eli sillä on tietoisesti omaksuttu päämäärä, joka syntyy tuloksena vaihtoehtoisten toimintatapojen välillä käydystä harkinnasta. Yksinkertaistettuna ja arkipuheessa tietoisuudella tarkoitetaan joskus vain tietämistä. Sanoessamme, että "tiedostamme" jonkin asian tai olemme "tietoisia", tarkoitamme yleensä, että tiedämme kyseisen asian ja yritämme ottaa sen huomioon toiminnassamme.

Tietoisuuteen liittyy havainnointia ja kun kyseessä on turvallisuus, tarkoittaa se useimmiten myös ennakointia. Turvallisuusympäristön havainnoinnin ja uhkien arvioinnin ollessa jatkuvaa, kyse on tulevaisuuden ennustamisesta ja ennakoinnista, jolloin on samalla aiheellista kysyä, miten hyvin tulevaisuutta ylipäätään voidaan ennustaa. Tulevaisuuden tutkimuksen ensimmäisen säännön mukaan tulevaisuutta ei voi ennustaa tai on mahdotonta varmuudella sanoa, mitä huomenna tapahtuu. Toinen tulevaisuuden tutkimuksen periaate on, että tulevaisuus ei ole ennalta määritelty, eikä sitä kukaan tai mikään kykene ennakolta määrittelemään. Kolmas ja erityisen tärkeä mielessä pidettävä periaate on, että kun arvioimme tulevaisuutta, tulevaisuuteen voi vaikuttaa teoilla ja valinnoilla. Tulevaisuuden ennustamisen vaikeudesta huolimatta, tärkeintä on kyetä arvioimaan ja pohtimaan erilaisia tulevaisuuden näkökulmia ja todennäköisyyksiä. Turvallisuuden näkökulmasta uhkien pohtiminen ja uhkakuvien luominen todennäköisyyksineen sekä vaikutuksineen onkin eräänlainen välttämättömyys. (Limnéll & Iloniemi 2018, 99-100.)

Toiminta- ja/tai turvallisuusympäristöstä puhuttaessa, samassa yhteydessä saattaa esiintyä termejä, kuten megatrendit, trendit, heikot signaalit tai villit kortit. Toimintaympäristön muutoksia tutkiva sekä tulevaisuuden arviointia ja ennakointityötä tekevä Sitra (2020, 3) toteaa megatrendien tarkoittavan yhteiskunnassa vaikuttavia merkittäviä muutoksia. Megatrendien tarkastelu on oleellinen osa tulevaisuuksien pohdintaa ja sillä käytännössä tarkoitetaan useista ilmiöistä koostuvaa yleistä kehityssuuntaa, laajaa muutoksen kaarta. Megatrendejä tarkastelemalla saadaan hyvä kuva laajoista tulevaisuuden muutoksista, mutta niiden ohella on hyvä tarkastella myös heikkoja signaaleja, tarkempia trendejä sekä jännitteitä erilaisten kehityskulkujen välillä.

Hiltusen (2012, 76) mukaan ”megatrendit ovat laaja-alaisia muutoksia, jotka koostuvat eri trendeistä. Trendit itsessään taas koostuvat erilaisista nousevista asioista, joita voidaan havainnoida heikkojen signaalien avulla. Villit kortit ovat nopeita ja laaja-alaisia muutoksia, kun taas pysyvyydet ovat asioita, jotka eivät hevillä muutu.”

Trendit ovat hyvin laaja-alaisia ja liittyvät kaikkiin elämänalueisiin. Trendien tarkkailussa ja ennakoinnissa käytetään perusluokittelua STEEP, joka jakaa muutokset yhteiskunnallisiin (Social), teknologisiin (Technological), taloudellisiin (Economic), ympäristöön (Enviroment) liittyviin sekä poliittisiin (Political) luokitteluihin, jotka vielä erikseen sisältävät erilaisia alaluokitteluja. (Hiltunen 2012, 96.)

Villi kortti on jokin yllättävä, nopea, laajavaikutteinen ja odottamaton tapahtuma, josta yhtenä esimerkkinä New Yorkissa tapahtunut terrori-isku ja WTC-tornien tuhoutuminen syyskuussa 2001. Villien korttien sijaan tai niiden ohella voidaan joskus puhua myös mustista joutsenista. Tutkijasta riippuen, kyse on erilaisista tulevaisuuden yllätyksistä, strategisista yllätyksistä, äärimmäisistä tapahtumista tai odottamattomista tapahtumista. Käytetyt termit ja edellä mainitut luonnehdinnat ovat joka tapauksessa jollain tavoin synonyymeja toisilleen ja pienistä erovaisuuksista huolimatta ollaan yhtä mieltä siitä, että villeillä korteilla on suuri vaikutus ympäristöön. Kansankielellä villit kortit voidaankin nähdä esimerkiksi katastrofeina. (Hiltunen 2012, 139 & 143.)

3 Sisäinen turvallisuus muuttuvassa turvallisuusympäristössä

Sisäisen turvallisuuden strategiassa (Sisäministeriö 2017, 10) todetaan, ettei sisäisestä turvallisuudesta ole olemassa yhtä selkeää ja vakiintunutta tai yksiselitteistä määritelmää ja perinteisessä tarkastelussa turvallisuus jaetaan usein sisäiseen ja ulkoiseen turvallisuuteen. Ulkoisesta turvallisuudesta huolehtiminen kuuluu puolustusvoimille ja sisäisestä turvallisuudesta vastaa pääasiassa poliisi. Sisäisen turvallisuuden käsite on kuitenkin nykyisin laajempi, kuin pelkästään puolustusvoimien valmius kansallisen koskemattomuuden varmistamiseen tai poliisin ylläpitämä yleinen järjestys ja turvallisuus. Yleisellä järjestyksellä ja turvallisuudella tarkoitetaan tilaa, jossa yleiset paikat ovat turvallisia, yhteiskunnan turvallisuutta uhkaavat teot voidaan estää, yksityisiin henkilöihin ja yhteisöihin kohdistuvat oikeudenloukkaukset ja häiriöt pystytään torjumaan sekä tapahtuneet oikeudenloukkaukset selvitetään (Kokonaisturvallisuuden sanasto 2017, 23).

Viime vuosina Suomessa on laadittu kolme erillistä valtioneuvoston selontekoa: sisäisen turvallisuuden selonteko, ulko- ja turvallisuuspoliittinen selonteko sekä puolustusselonteko. Näiden lisäksi yhteiskunnan laaja varautuminen turvallisuusongelmiin koottiin kokonaisturvallisuuden

ajatuksen mukaisesti yhteiskunnan turvallisuusstrategiaan. Nämä asiakirjat toimivat kansallisena kehyksenä turvallisuuden ohjaukselle ja niiden tarkoituksena on vastata ongelmiin jo ennen kuin niistä tulee riski maan turvallisuudelle. (Häikiö ym. 2018, 57.)

Strategisella tasolla Suomen sisäisen turvallisuuden toteuttaminen rakentuu kolmesta erillisestä ajatusmallista, joita ovat arjen turvallisuus, laaja turvallisuuskäsitys sekä kokonaisturvallisuus. Sisäisen turvallisuuden strategian suuntaviivana ja tiekarttana toimii arjen turvallisuus, millä tarkoitetaan niitä yhteiskunnan ominaisuuksia, joiden johdosta kansalaiset voivat nauttia oikeusjärjestelmän takaamista oikeuksista ja vapauksista ilman rikollisuuden, häiriöiden, onnettomuuksien ja kansallisten tai kansainvälisten ilmiöiden aiheuttamaa pelkoa tai turvattomuutta. Määritelmä pitää sisällään kaksi eri tekijää, selkeät sisäiseen turvallisuuteen vaikuttavat uhkatekijät, kuten rikollisuus, häiriöt, onnettomuudet sekä kansalliset ja kansainväliset ilmiöt. Toisaalta näitä edellä mainittuja voidaan tarkastella sen kannalta, mitkä aiheuttavat tai ainakin voivat aiheuttaa pelkoa tai turvattomuutta. Lähtökohtana on, että lukuisat sisäiset ja ulkoiset muutosvoimat muokkaavat yhteiskuntaa jatkuvasti ja vaikka sisäisen turvallisuuden ydintä onkin yleinen järjestys ja turvallisuus sekä ihmisten oikeus elämään, fyysiseen koskemattomuuteen ja omaisuuden suojaan, turvallisuuden kannalta eri aikoina painotetaan eri asioita. Yhteiskunnassa on lisäksi erilaisia turvallisuusongelmien taustalla olevia juurisyitä, mitkä vaikuttavat turvallisuuden kehitykseen, mutta toisaalta jatkuvasti enenevässä määrin sisäiseen turvallisuuteen vaikuttavat myös Suomen rajojen ulkopuolella syntyvät ilmiöt ja päätökset ja joillakin osa-alueilla turvallisuuskehitys on jopa täysin riippuvainen kansainvälisestä tilanteesta. (Sisäministeriö 2017, 11.)

Arjen turvallisuudessa kyse on siis kokonaisvaltaisesta tavoitteesta kansalaisten hyvinvoinnin ja yhteiskunnan turvallisuuden puolesta. Strategian toimenpideohjelman mukaisesti ja myös käytännössä, se tarkoittaa viranomaisten ja oikeusjärjestelmän toiminnan sekä rikoksia ennalta estävien palveluiden sovittamista yhteen niin, että syrjäytyneiden henkilöiden rikollisuutta voidaan vähentää mahdollisimman tehokkaasti, nuorten syrjäytymiskehitykseen puututaan moniammatillisin keinoin mahdollisimman varhain, toimitaan aktiivisesti ikääntyneiden, lasten ja nuorten turvallisuuden parantamiseksi sekä ehkäistään alueellisen segregaation syntymistä kasvukeskuksissa. Mainituilla toimenpiteillä vastataan tunnistettuihin toimintaympäristössä esiintyviin muutosvoimiin, kuten monimuotoinen polarisaatio, muuttoliikkeiden turvallisuusvaikutukset, arvojen sirpaloituminen sekä ääriliikkeet ja ideologiat. (Sisäministeriö 2017, 12.)

Toimintaympäristön globalisoituessa sekä ulkoisen ja sisäisen turvallisuuden keskinäisriippuvuuden lisääntyessä, käyttöön on vakiintunut termi laaja turvallisuuskäsitys, joka perinteisen sotilaallisen uhkan lisäksi kattaa useita muita ilmiöitä ja haasteita, kuten ilmastonmuutos, energian ja vesivarojen niukkuus, väestönkasvu ja väestöliikkeet, terrorismi, tartuntataudit, järjestäytynyt rikollisuus ja sen erilaiset ilmenemismuodot, kuten huume- ja ihmiskauppa, tietoturvahyökkäykset sekä yhteiskunnan haavoittuvuuden lisääntyminen. Näillä on enenevässä määrin

vaikutusta kansainväliseen yhteistyöhön sekä myös Suomen turvallisuusympäristöön. (Valtioneuvoston kanslia 2012, 12.) Laajan turvallisuuskäsityksen tieteellinen ja toiminnallinen tarkastelu ulottuukin perinteistä ulkoista ja sisäistä turvallisuutta laajemmalle. (Kokonaisturvallisuuden sanasto 2017, 16.)

Sisäisen turvallisuuden kehittämistä ohjaava sisäisen turvallisuuden strategia pohjautuu laajaan turvallisuuskäsitykseen ja siinä kyseisessä kontekstissa laajalla turvallisuuskäsityksellä tarkoitetaan sitä, että vaikka ensisijaisia sisäisen turvallisuuden ylläpitäjiä ovatkin poliisi-, tulli-, pelastus-, rajavartio-, oikeus- ja vankeinhoitoviranomaiset, laajassa turvallisuuskäsityksessä myös sosiaali- ja terveys-, liikenne- ja viestintä-, opetus-, kulttuuri- ja nuoriso- sekä työ- ja ympäristöviranomaisilla on tärkeitä sisäisen turvallisuuden alaan liittyviä tehtäviä. Edellä mainittujen ohella tärkeä osa turvallisuustyötä ovat myös erilaiset järjestöt ja elinkeinoelämä, jotka tuottavat erilaisia tuotteita ja palveluita kansalaisille. Näin ollen yritystoiminnan turvallisuus sellaisenaan on tärkeä osa arjen turvallisuutta. Laajassa turvallisuuskäsityksessä tavoitteena onkin vastata laaja-alaisesti erilaisiin yhteiskuntaan kohdistuviin muutosvoimiin ja turvallisuusuhkiin. (Sisäministeriö 2017, 14.)

Kokonaisturvallisuus puolestaan liittyy yhteiskunnan varautumiseen ja sen kehittämiseen. Kokonaisturvallisuuden ajattelumallia ohjaa Yhteiskunnan turvallisuusstrategia (YTS). Kokonaisturvallisuudella tarkoitetaan tilaa, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuviin uhkiin ja riskeihin on varauduttu. Kokonaisturvallisuuden hallintaan eli yhteiskunnan elintärkeiden toimintojen ylläpitämiseen sisältyy uhkiin varautuminen, häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen. (Kokonaisturvallisuuden sanasto 2017, 16.) ”Suomalaisen yhteiskunnan varautuminen toteutetaan kokonaisturvallisuuden periaatteella, mikä tarkoittaa yhteiskunnan elintärkeiden toimintojen turvaamista viranomaisten, järjestöjen, elinkeinoelämän ja kansalaisten yhteistoimintana" (Turvallisuuskomitea 2018, 9).

Sisäistä turvallisuutta ylläpitämällä ennaltaehkäistään ja torjutaan Suomeen ja sen väestöön kohdistuvia rikoksia, onnettomuuksia ja ympäristövahinkoja tai muita vastaavia häiriöitä ja uhkia sekä hallitaan niiden seurauksia. Poliisin tehtävänä on suojata yhteiskunnan keskeistä infrastruktuuria, ylläpitämällä yleistä järjestystä ja turvallisuutta. Samalla voidaan ennalta estää ja torjua terrorismia, järjestäytynyttä ja muuta vakavaa rikollisuutta sekä vakavia häiriöitä. Toimivalla rikostorjunnalla ja rikosten esitutkinnan avulla ehkäistään rikollisuutta ja ylläpidetään yhteiskuntarauhaa. (Turvallisuuskomitea 2017, 19.)

Limnéllin ja Iloniemen (2018, 208-209) mainitsevat sisäisen turvallisuuden olevan usein hyvin arkista turvallisuuden kokemista ja turvallisuuden tunnetta jokaisena päivinä. On ymmärrettävä, että sisäisen turvallisuuden trendinä on niin uhkien kuin viranomaistyön monimutkaistuminen ja monialaistuminen, mikä käytännössä tarkoittaa ihmisten turvallisuustarpeiden lisääntymistä ja turvallisuusviranomaisilla laajenevaa tehtäväkenttää. Toiminnan edellytyksenä on

viranomaisyhteistyön syventäminen entisestään sekä halukkuus yhteistyöhön, jonka lisäksi kasvavat riskit ja uudet uhkat edellyttävät uudenlaista valmiutta ja varautumista koko yhteiskunnalta. Turvallisuusympäristön arvioinnissa korostuvat yhä vahvemmin kokonaisvaltainen ja poikkihallinnollinen tarkastelutapa sekä niiden edellyttämä yhteiskunnan eri toimijoiden aiempaa vahvempi keskinäinen yhteistyö yhteiskunnan varautumisessa ja häiriötilanteiden hallinnassa. Globaalit turvallisuusuhkat, kuten terrorismi, järjestäytynyt rikollisuus ja kyberrikollisuus osaltaan edellyttävät päästämistä irti siiloutuneesta turvallisuustoiminnasta sekä kykyä ennakkoluulottomaan arvioitiin uhkiin vastaamista, jopa aivan uudenlaisilla turvallisuusrakenteilla. Toinen keskeinen sisäisessä turvallisuudessa kehittävä asia, on parempi ennakointikyky, mikä edellyttää viranomaisilta parempaa ketteryyttä seurata ja sopeutua turvallisuusympäristön nopeaan muutokseen.

Nergin & Himbergin (2018, 12-13) mukaan viimeisimmän sisäisen turvallisuuden strategian valmistelun johtoajatuksena oli, että sisäisen turvallisuuden muutoksiin vaikuttavat eniten usein hitaat ja siksi vaikeasti havaittavat yhteiskunnalliset ja ulkoiset muutostekijät. Laajamittainen, äkillinen yhteiskunnan toiminnan häiriö nähtiin harvinaisena poikkeuksena. Muutoksen hitaus yhdessä riittämättömän ennakoinnin kanssa saattaisi toisaalta johtaa yllättävään tilanteeseen. Strategian pohjana käytettiin laajaan tutkimus- ja selvitysaineistoon perustuvaa analyysia suomalaisen yhteiskunnan muutosvoimista, joita arvioitiin olevan seitsemän: monimuotoinen polarisaatio, arvojen sirpaloituminen, maahanmuuton turvallisuusvaikutukset, ääriliikkeet ja -ideologiat, teknologian kiihtyvä murros, julkisen talouden hidas elpyminen sekä globaali turvallisuusympäristö.

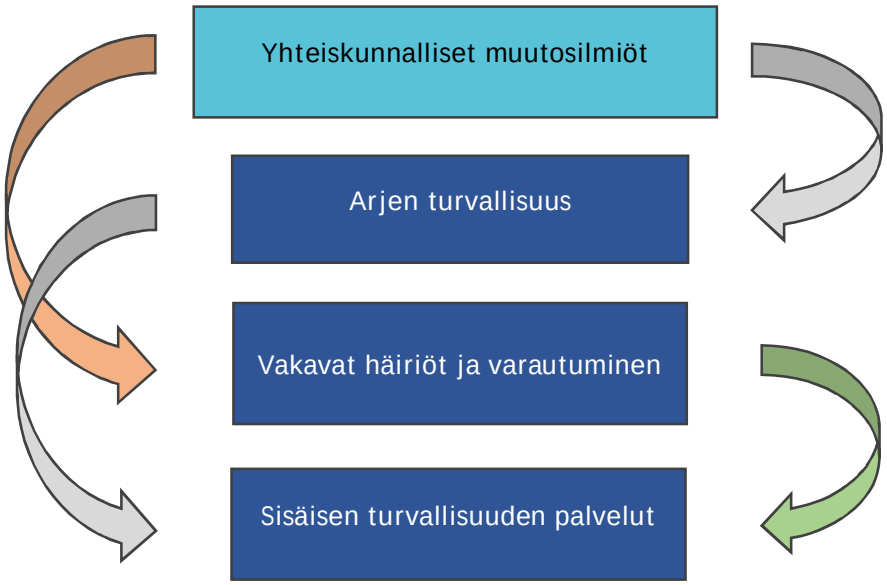
Yhteiskunnan polarisaation reunalla etenevän monimuotoisen syrjäytymisen nähtiin olevan yhteiskukunnan keskeisin turvallisuushaaste ja tutkimusten sekä viranomaiskokemuksen perusteella se onkin usein onnettomuuksien ja väkivallan pääasiallinen taustatekijä. Samalla syrjäytyminen on yksi tärkeimmistä nuoria miehiä ääriliikkeisiin ajavista tekijöistä. Ääriliikkeisiin kytkeytyvä radikalisoitumisen uhka on realisoitunut myös Suomessa ja syrjäytyminen, arvorakenteiden sirpaloituminen, maahanmuutto ja reagointi siihen sekä ääri-ideologiat muodostavat muutostekijöiden rykelmän, jossa yksittäiset ilmiöt kytkeytyvät toisiinsa monin tavoin. Nopea teknologinen muutos on suomalaiselle yhteiskunnalle suuri mahdollisuus, mutta toisaalta se aiheuttaa lukuisia uusia haasteita, joista usein esiin nostettu kyberturvallisuus on vain yksi. Globaali turvallisuuskehitys puolestaan heijastuu myös sisäiseen turvallisuuteen, ja hybridiuhkiin varautuminen antaa aiheen tarkastella ulkoisen ja sisäisen turvallisuuden rajapintaa uudella tavalla. Sisäisen turvallisuuden heikentyminen voi siis aiheutua monien eri sisäisten ja ulkoisten muutostekijöiden ajamana, jossa kuitenkin on huomioitava, että vain osa niistä lankeaa selkeästi turvallisuusviranomaisten toimialalle. (Nerg & Himberg. 2018. 13.)

Vuoden 2019 lopulla käynnistyi uuden Sisäisen turvallisuuden selonteon valmistelu, jossa aiemman selonteon tavoin pyritään huomioimaan turvallisuusympäristön muutostekijät. Selonteko

on kokonaisvaltainen selvitys Suomen sisäisen turvallisuuden tilannekuvasta, uhkista ja tilasta, kansalaisten turvallisuuden tunteesta, sisäisen turvallisuuden viranomaisten suorituskyvystä ja toiminnan tuloksellisuudesta, toimintojen kehittämistarpeista ja haasteista sekä eri tehtävien asianmukaisen hoitamisen edellyttämistä kehittämistoimenpiteistä, kuten myös tehtäväperusteisesti pidemmän tähtäimen taloudellisista ja muista resurssitarpeista. (Sisäministeriö 2020.)

Nykyisessä toiminta- ja turvallisuusympäristössä sisäistä turvallisuutta tehdään ja koetaan yhteiskunnassa laajasti. Turvallisuus ei ole pelkästään turvallisuusviranomaisten vastuulla, joiden perustehtävissä korostuu akuuttien tilanteiden hoitaminen, vaan turvallisuuden perustyön tekemisestä vastaavat eri sektorit, kuten elinkeinoelämä, oppilaitokset, järjestöt, erilaiset yhteisöt sekä ihmiset itse. Poliisi hoitaa yleisen järjestyksen ja turvallisuuden ylläpitämisen, mutta arjen turvallisuuteen vaikuttavat monet laajemmat ilmiöt, kuten kasvava syrjäytyminen. (Sisäministeriö 2020.)

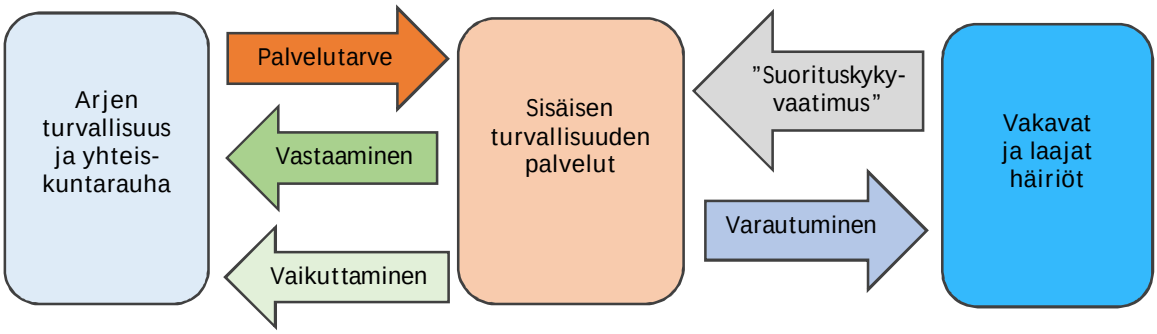
Sisäisen turvallisuuden tulevaisuutta luotaavassa selonteossa sisäistä turvallisuutta tarkastellaan kuviossa 1 esittävän kolmen ulottuvuuden kautta. Ensimmäisenä ulottuvuutena on ajatus siitä, että arjen turvallisuuden ja yhteiskuntarauhan kannalta Suomen tulisi olla maailman turvallisin maa, turvallisempi kuin koskaan. Toinen ulottuvuus koskee yhteiskunnan turvallisuuspalveluiden tuottamista eli sitä arkista resurssia ja toimintakykyä, millä jokapäiväinen turvallisuus tuotetaan. Kolmantena ulottuvuutena on jatkuvasti muuttuvan toimintaympäristön mukanaan tuoma varautuminen vakaviin ja laajoihin häiriöihin, pitäen sisällään niin perinteiset kuin uudetkin uhkakuvat. Koska turvallisuus rakentuu monen eri tahon ja toimijan yhteistyönä, arjen ensimmäisen ulottuvuuden eli arjen turvallisuuden toteutuminen asettaa erityisen palvelutarpeen turvallisuuden eri toimijoille ja niitä tuottaville palveluille, mikä puolestaan vaatii vastaamista ja vaikuttamista asetettuihin tarpeisiin. Turvallisuuden palveluita tuottavien tahojen eli viranomaisten on pystyttävä arjen perustoimintojen ohella vastaamaan tarvittaessa myös mahdollisiin häiriötilanteisiin, jopa laajoihin sellaisiin, mikä puolestaan asettaa erityisiä suorituskykyvaatimuksia. Kolmas ulottuvuus eli mahdolliset vakavat ja laajat häiriöt velvoittavat varautumiseen esimerkiksi kansallisten ja alueellisten riskiarvioiden tuottamien tietojen vaatimalla tavalla. (Sisäministeriö 2020.)



Kuvio 1: sisäisen turvallisuuden rakenne

Sisäisen turvallisuuden taustalla piilevät muutokset syntyvät useimmiten seurauksena laajemmista yhteiskunnassa vaikuttavista muutosvoimista ja ilmiöistä. Muutoksista aiheutuvat seuraukset eivät useinkaan ole selkeästi kielteisiä tai myönteisiä, vaan ne sisältävät molempia. Samalla muutosilmiöllä on mahdollisesti erilaiset vaikutukset arjen turvallisuudelle, turvallisuuden palveluille sekä vakaville häiriöille. Yhteiskunnassa vallitsevia keskeisiä muutosvoimia ovat väestön ikääntyminen, kaupungistuminen, jatkuvasti etenevä teknologinen kehitys, arjen kokemusten eriytyminen ja väestön eriarvoistuminen, ilmastonmuutos, luonnon monimuotoisuus ja luonnonvarat, talouden murros sekä demokratian ja osallistumistapojen muutos. (Sisäministeriö 2020.)

Kaikki mainitut kolme sisäisen turvallisuuden ulottuvuutta vaikuttavat toisiinsa ja ovat riippuvaisia toisistaan siten, että arjen turvallisuus asettaa turvallisuutta tuottaville palveluille palvelutarpeen, joilla vastataan ja vaikutetaan arjen turvallisuuden kehittämiseen ja ylläpitämiseen. Turvallisuutta tuottavien palveluiden on samaan aikaan varauduttava vakaviin ja laajoihin häiriöihin, mikä puolestaan edellyttää turvallisuutta tuottavilta toimijoilta tarpeellista suorituskykyä, jotka mallinnetaan kuviossa 2. (Sisäministeriö 2020.)

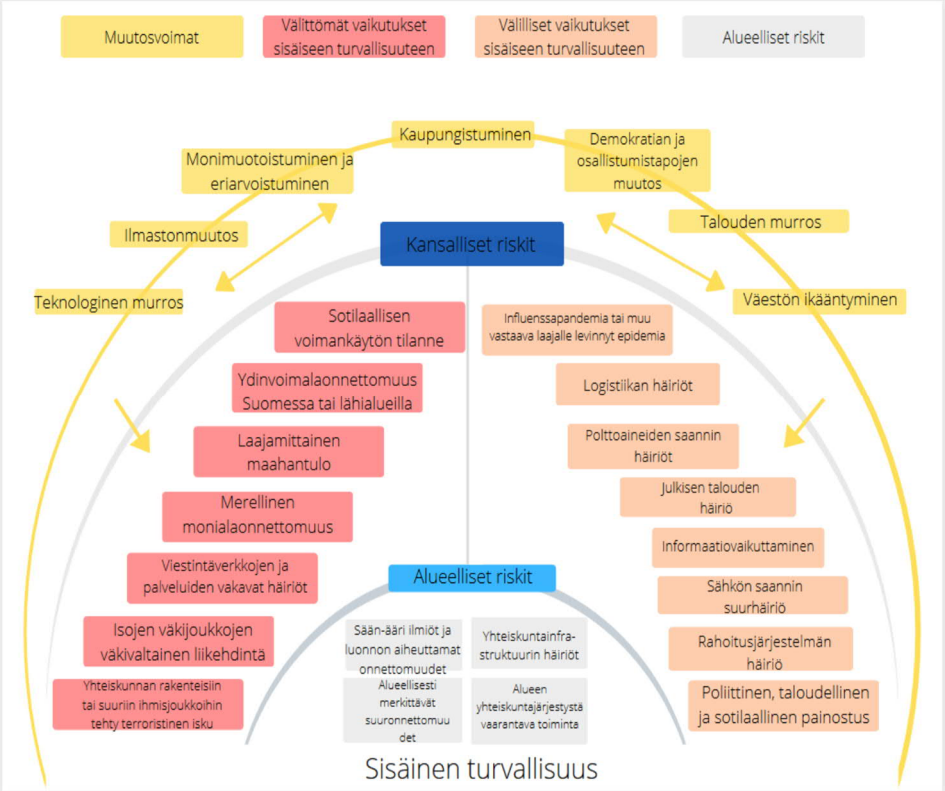


Kuvio 2: sisäisen turvallisuuden tietomalli

Sisäisen turvallisuuden selonteon ajatuksen mukaisesti arjen turvallisuus ja yhteiskuntarauha koostuu neljästä eri elementistä, joita ovat kansalaisten turvallisuuden tunne (pelot, turvallisuuden kokemus), rikollisuus (väkivalta, omaisuusrikollisuus, kyberrikollisuus, huumeet, ihmiskauppa, laiton maahantulo, järjestäytynyt rikollisuus), onnettomuudet ja tapaturmat (tapaturmat, liikenneonnettomuudet, tulipalot) sekä yhteiskuntarauha ja vakaus (luottamus viranomaisiin, yleinen järjestys-ja turvallisuus, väestösuhteet, maahanmuuton hallinta, terrorismi ja ääriliikkeet, tiedustelu, vihamielinen tiedustelu, vihamielinen vaikuttaminen). (Sisäministeriö 2020.)

Sisäisen turvallisuuden palveluiden tuottajia ovat keskeiset sisäisen turvallisuuden viranomaiset, kuten poliisi, SUPO, Rajavartiolaitos, pelastustoimi ja Hätäkeskuslaitos. Muita sisäisen turvallisuuden tehtäviä hoitavia viranomaisia ovat lisäksi maahanmuuttovirasto, siviilikriisinhallinta, Tulli, ensihoito, Rikosseuraamuslaitos sekä syyttäjälaitos ja tuomioistuimet varsinaisen rikosprosessissa. (Sisäministeriö 2020.)

Vakavia ja laajoja häiriöitä koskevan varautumisen pohjana on kansallisessa riskiarviossa tunnistetut uhkamallit, joiden painopiste on kuviossa 3 esitettävissä välittömissä sisäiseen turvallisuuteen vaikuttavissa riskeissä. Riskiarviossa huomioidaan, että kaikki esiintyvät riskit eivät ole ensisijaisesti sisäisen turvallisuuden riskejä, vaikka lähes kaikilla riskeillä siihen jokin vaikutus onkin, esimerkiksi pandemia. (Sisäministeriö 2020.)



Kuvio 3: vakavat ja laajat häiriöt ja niihin varautuminen

Sisäisen turvallisuuden rakenteen ja sen eri elementtien kohdalla on muistettava, että yhteiskunnan turvallisuutta rakennetaan yhdessä, mikä tarkoittaa, ettei turvallisuutta voida tarkastella toimialalähtöisesti vaan se tulee toteuttaa ilmiölähtöisesti. Yhteiskunnan turvallisuuteen vaikuttavien ja sitä kehittävien toimijoiden on kyettävä tunnistamaan oma roolinsa sekä tietonsa ja toimenpiteensä erilaisiin ilmiöihin liittyen. (Sisäministeriö 2020.)

Limnéllin & Iloniemen (2018, 115-116) mukaan elämme maailmassa, jota leimaavat epävakaus (Volatility), epävarmuus (Uncertainty), monimutkaisuus (Complexity) ja monimerkityksellisyys (Ambiquity). Tätä kutsutaan VUCA-ajatusmalliksi, joka turvallisuuden ja yritystoiminnan yhteydessä on noussut esille yhä voimallisemmin. VUCA-kuvauksen voitaisiin ajatella oleva aikamme ”uusi normaali”, sillä yleisesti ottaen maailma on nyt ja tulee tulevaisuudessakin olemaan kaikkia edellä mainittuja. Tulevaisuus näyttäytyy epäselvempänä ja vaikeammin ennakoitavana, jossa muutosnopeus ei tule hidastumaan ja samalla syy-seurausketjut muuttuvat. VUCA-maailman haasteisiin joudutaan tulevaisuuden yhteiskunnissa ja organisaatioissa tarttumaan entistä tietoisemmin ja suunnitelmallisemmin, mikä yksilöiden, organisaatioiden ja valtion näkökulmasta tarkoittaa tehokkaampaa oppimista hyväksyä ja hyödyntää epävarmuutta ja jatkuvia muutoksia. VUCA-mallin omaksuminen onkin ominaispiirre tulevaisuuden uhkakuvien ymmärtämisessä ja niihin varautumisessa. Tulevaisuuteen varautumisen ollessa entistä vaikeampaa, juuri siitä syystä on erityisen järkevää ennakoida eli kartoittaa etukäteen erilaisia mahdollisia

tulevaisuuksia ja tapoja toimia niissä. Samalla se on ehdoton vaatimus vastattaessa tulevaisuuden uhkakuviin.

4 Turvallisuusympäristön uhkatekijät ja haasteet

Opinnäytetyön toisessa kokonaisuudessa tarkastellaan turvallisuusympäristössä ilmeneviä uhkia ja niiden vaikutusta yhteiskunnan turvallisuuteen. Puhuttaessa uhkista, kyse on samalla riskeistä, niiden kartoittamisesta ja analysoinnista. Riskien ja uhkien arvioinnin pohjalta voidaan laatia erillisiä riski- ja uhka-arvioita. Riski on jonkin kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä, jossa riski voidaan laskea ja määritellä tapahtuman todennäköisyyden (t) ja sen mahdollisen vaikutuksen (v) tulona (riski = t * v). Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin. (Kokonaisturvallisuuden sanasto 2017, 40.)

Leppäsen (2006, 30-31) mukaan ”riskillä tarkoitetaan vaaraa, yllättävää tapahtumaa, joka kielteisellä tavalla estää realisoituessaan kokonaan tai väliaikaisesti jonkin tavoitteen toteutumisen. Riski on vahingonvaara tai vahingonuhka; vaaratekijä, joille ihmiset ovat alttiina tietyllä hetkellä.” Riski on jokin ihmisen henkeen, terveyteen tai omaisuuteen kohdistuva epäsuotava tapahtuma, jonka lisäksi riskin häiriöuhka voi kohdistua tuotantovälineisiin, järjestelmiin, yhteiskunnallisiin toimintoihin tai luontoon. Riskit voidaan jakaa 1) onnettomuuden luonteen mukaan (luonnollinen vs. teknologinen tai akuutti vs. krooninen), 2) riskin ilmenemisen mukaan (kausaalisuus - ilman tai veden saastuminen ja siitä aiheutuvat seuraukset) tai 3) seurausten luonteen mukaan (vammat vs. vahingot).

Riskiin sisältyy kolme tekijää, jotka vaikuttavat riskin kokemiseen. Ensimmäinen on mahdollisesti toteutuvaan tapahtumaan liittyvä epävarmuus, tapahtumaan liittyvät odotukset sekä tapahtuman laajuus ja vakavuus. Riskin lähtökohtana on, että tapahtumaan tulee liittyä jonkinlainen epävarmuus. Jos tapahtuman, toimenpiteen tai muun vastaavan seuraus tai tulos on jo ennalta täysin tiedossa, kyseessä ei ole riski. Toinen riskiin sisältyvä tekijä eli odotukset, vaikuttavat siihen, minkälaisena koemme riskin ja sen mahdollisen toteutumisen. Kolmantena seikkana on tapahtuman laajuus ja merkityksellisyys, niin itselle kuin muille, mikä vaikuttaa koetun riskin vakavuuteen. Riskiä arvioitaessa punnitaankin aina olemassa olevia mahdollisuuksia sekä asiaan liittyviä uhkia. Arvioinnissa on mahdollista hyödyntää olemassa olevaa kokemusperäistä tietoa, tapaustutkimuksia ja/tai riskiarvion laskemista. Lisäksi on huomioitava, että riskin todennäköisyyttä voidaan arvioida vain tyypillisten riskien osalta. Mikäli tarkastelun alla on uusi ja tuntematon riski, todennäköisyyden tarkka arviointi voi olla hyvin vaikeaa. (Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 7-8)

Riskille läheinen termi uhka, puolestaan tarkoittaa mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua. Uhkalle läheinen synonyymi on vaara, näiden kahden erotessa toisistaan siinä, että uhka on epävarmempi kehityskulku, kun taas vaara puolestaan käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävä asia. (Kokonaisturvallisuuden sanasto 2017, 40.)

Limnéll & Iloniemi (2018, 14 & 16) toteavat uhkan olevan useimmiten sanana pelottava ja parempihan olisi, jos uhkia ei olisi. Uhkat on kuitenkin ymmärrettävä aina oleviksi, joskus jopa tarpeellisiksi, osaksi kaikkea toimintaa ja elämää. Uhkien arviointi ja riskeihin varautuminen ovat keskeinen osa yhteiskuntien toimintaa ja joskus valtioilla on jopa tarve luoda itselleen uhkakuvia, sillä ne antavat valtiolle itselleen tarkoituksen. Uhka nähdään usein turvallisuuden vastakäsitteenä, sillä toteutuessaan uhka heikentää turvallisuutta. Eron tekeminen uhkan ja riskin välillä saattaa olla usein haastavaa, sillä niiden käsitteet ovat rinnasteisia, vaikkakin esimerkiksi yhteiskunnan turvallisuuspolitiikassa uhkille annetaan suurempi painoarvo. Riskiä käsitteenä voidaankin pitää uhkaa lievempänä ja arkipäiväisempänä, joskin rajat ovat häilyvät.

Uhkaa, sen lähdettä ja merkitystä voidaan arvioida tarkemmin laatimalla erillinen uhka-arvio. Uhka-arvio on tehdyn uhkamallin pohjalta laadittava arvio, jossa konkreettisesti käsitellään uhkan lähdettä, kohdetta, toteutumistapaa, todennäköisyyttä, vaikutuksia tehtävien hoitamiseen sekä vastatoimenpidemahdollisuuksia ja niiden valmisteluun tarvittavaa aikaa. Uhka-arviolla mahdollistetaan sellaisten toimien tarkastelu, joihin organisaation on ryhdyttävä uhkan ehkäisemiseksi tai sen torjumiseksi ja sen vaikutuksista selviämiseksi. Arvion pohjana käytettävä uhkamalli on yleinen kuvaus yhteiskunnan turvallisuusympäristöön sisältyvistä uhkista, mikä laaditaan helpottamaan ja yhdenmukaistamaan suunnittelua ja varautumista. Uhkamalli on uhka-arvion eri osa-alueista koostuva arvio koko yhteiskuntaa koskevista tyypillisistä strategisen tason uhkatilanteista ja tarvittaessa sitä voidaan muuttuvan uhka-arvion perusteella tarkentaa. Yhteiskuntaan kohdistuvia uhkia voivat olla esimerkiksi erilaiset onnettomuudet, kuten suuronnettomuudet ja ympäristövahingot, taloudellinen uhka, kyber- ja tietoturvauhka, vakava rikollisuus, terrorismi, laajamittainen maahantulo, sotilaallinen uhka, säteilyvaara sekä epidemia tai jopa pandemia (Kokonaisturvallisuuden sanasto 2017, 41-42).

Uhka voidaan ymmärtää konkreettisena asiana, jossa kyse on tekijästä tai tekijöiden summasta ja joka arvioidulla todennäköisyydellä luo pelkoa, vaaraa tai riskiä sekä tuottaa epävarmuutta siitä, että toteutuessaan se yleensä tuo mukanaan jotain ikävää. Uhkan keskeisten tekijöiden ollessa konkretisoitumisen todennäköisyys sekä vaikutusten arviointi, yhteiskunnan on järkevää varautua hyvin epätodennäköisiltäkin vaikuttaviin uhkiin, kuten sotilaalliseen uhkaan, koska toteutuessaan se pahimmillaan voisi merkitä kansallisen määräämisoikeuden ja kansakunnan loppua. Samaan aikaan tulisi laajasti varautua todennäköisempiin, kuten kybermaailman uhkiin, vaikka asiaa ei aina välttämättä ymmärretä tärkeäksi tai vaikutukset omalta osalta koetaan hyvin pieniksi. Kolmantena, todennäköisyyden ja vaikutusten ohella, uhkaa tulisi arvioida myös uhkan tuottajan (uhkaajan) motiivin näkökulmasta. Tästä esimerkkinä terroristien motiivi ja

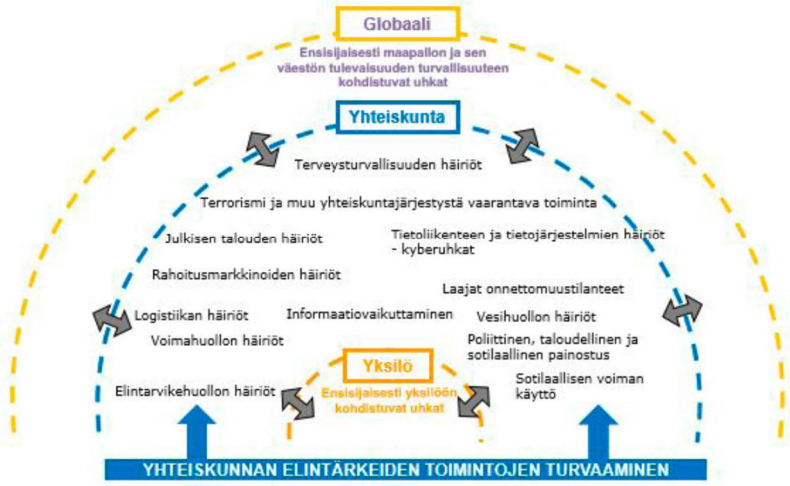
tahto järjettömiltä tuntuviin iskuihin. Toisaalta, aina mitään selkeää tarkoitusta tai motiivia ei ole edes löydettävissä. Tärkeää onkin muistaa, että uhka voi olla tarkoituksellinen, ei-tarkoituksellinen, tahallisesti tehty tai tahattomasti aiheutunut. (Limnéll & Iloniemi 2018, 19-20.)

Suomalaisen yhteiskunnan varautumistyön pohjana käytetään erikseen laadittua kansallista riskiarviota. Kansallisen riskiarvion laatiminen perustuu Euroopan parlamentin ja neuvoston päätökseen unionin pelastuspalvelumekanismiin, jonka ohella tavoitteena on kyetä ennakoimaan Suomeen kohdistuvia äkillisiä vakavia tapahtumia. Tällaisten tapahtumien toteutuessa, saattaisivat ne aiheuttaa merkittäviä ihmisten henkeen tai terveyteen, talouteen ja ympäristöön sekä yhteiskuntaan vaikuttavia vahinkoja. Kansallisen riskiarvion tarkoituksena on arvioida turvallisuusympäristön mahdollisia uhkia ja häiriötilanteita. (Sisäministeriö 2019, 9 & 22.)

Kansallisen riskiarvion laatimisessa hyödynnetään mahdollisimman paljon eri toimijoiden jo tehtyjä riskiarvioita tai muita vastaavia tuotteita ja prosesseja. Riskiarviota koostettaessa eri hallinnonaloilla tehdyistä uhkamalleista ja häiriötilanteista kuvataan niiden taustalla oleva uhka tai uhat, uhkan kohde, toteutumistapa sekä vikojen ja häiriöiden ketjuuntuminen ja kertautuminen. Uhkamallien sekä häiriötilanteiden osalta arvioidaan myös niiden todennäköisyyden muutostrendi, mikä voi johtua esimerkiksi toimintaympäristön yleisimmistä muutoksista tai teknologisesta kehityksestä. Varsinaisessa vaikutusarvioinnissa arvioidaan kunkin uhkamallin ja häiriötilanteen mahdollinen välitön tai välillinen vaikutus yhteiskunnan elintärkeisiin toimintoihin. Riskiarviossa laaditaan lisäksi alueelliset riskiarviot, jotka toteutetaan poikkihallinnollisesti niin, että valmistelussa ja arvioinnissa ovat edustettuina alueen kunnat, viranomaiset, elinkeinoelämä sekä järjestöt. Alueellisissa riskiarvioissa tarkoituksena on tunnistaa, valita ja listata nimenomaan kaikille alueen toimijoille yhteisesti merkittävimmät uhkat tai häiriötilanteet. (Sisäministeriö 2019, 12.)

Toimintaympäristön muutoksilla on monenlaisia vaikutuksia Suomen sisäiseen kehitykseen ja niiden myötä yhteiskunnan turvallisuuteen kohdistuu uusia epävarmuustekijöitä. Yhteiskuntaan kohdistuvat uhkat ovat dynaamisia, rajat ylittäviä ja muuntuvia ja kansallisessa riskiarviossa uhkamallilla tarkoitetaan kuvausta turvallisuusympäristön mahdollisista häiriöistä. Riskejä arvioitaessa häiriötilanteella tarkoitetaan jotain sellaista uhkaa tai tapahtumaa, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. Uhkien tunnistamisen ja niiden vaikuttavuuden arvioinnin ollessa haasteellista, toimintaympäristön muutosten seurannan ja analysoinnin sekä ennakointivalmiuksien ylläpitämisen tuleekin olla kaikkien yhteiskunnan varautumisesta ja häiriötilanteiden hallinnasta vastuussa olevien tahojen jatkuvaa ja aktiivista toimintaa. (Sisäministeriö 2019, 22.)

Riskiarviossa käsiteltyjä mahdollisia häiriötilanteita aiheuttavia uhkia ja uhkamalleja kuviossa 4 kuvattu informaatiovaikuttaminen, poliittinen, taloudellinen ja sotilaallinen painostus, sotilaallisen voiman käyttö, terrorismi ja muu yhteiskuntajärjestystä vaarantava toiminta, julkisen talouden häiriö, rahoitusjärjestelmän häiriö, voimahuollon eli sähkön- ja energiasaannin häiriöt, tietoliikenteen ja -järjestelmien häiriöt eli kyberuhat, logistiikan häiriöt, terveysturvallisuuden häiriöt, vesihuollon häiriöt, elintarvikehuollon häiriöt sekä laajat onnettomuustilanteet. (Sisäministeriö 2019, 22).



Kuvio 4: kansallisen riskiarvion uhkamallit

Kaikki edellä mainitut uhkat ja uhkamallit ovat merkityksellisiä yhteiskunnan kokonaisturvallisuuden kannalta, joista kuitenkin käsittelen tarkemmin vain tiettyjä. Tarkasteluun on valikoitunut sellaiset uhkatekijät, jotka sisäisen turvallisuuden viranomaisten ja erityisesti poliisin näkökulmasta tuottavat yhteiskuntaan turvallisuushaasteita joko pidemmällä aikavälillä tai jotka akuutisti toteutuessaan voisivat aiheuttaa välitöntä uhkaa tai häiriötilanteita viranomaistoiminnalle tai vaaraa kansalaisten turvallisuudelle.

4.1 Informaatiovaikuttaminen yhteiskunnan piilevänä uhkana

Monille edelleen hieman jopa tuntematon ja vaikeasti havaittava, mutta kansallisesti merkittävä ja erityisen tarkasti huomioitava uhkatekijä on informaatiovaikuttaminen. Informaatiovaikuttamisella tarkoitetaan suunnitelmallista toimintaa, jossa tavoitteena on informaatiota muokkaamalla saada aikaan omien tavoitteiden mukaisia muutoksia kohteen informaatio- ja mielipideympäristössä (Kokonaisturvallisuuden sanasto 2017, 45).

Informaatiovaikuttamisen tavoitteena on saavuttaa tilanne, jossa vaikuttamisen kohde saadaan tekemään itselleen haitallisia päätöksiä tai toimimaan omaa etuaan vastaan. Toiminnan erityi-

senä tavoitteena ja tarkoituksena on vedota ihmisten tunteisiin, sillä tunteisiin perustuvat käsitykset syntyvät nopeasti ja sen seurauksena vaikuttamisen kohteet haluavat levittää omaa maailmankuvaansa totuuden jäädessä toissijaiseksi. Laajalle levinneen valheellisen tiedon oikominen voi olla jälkikäteen vaikeaa, eikä sillä voida poistaa jo levinnyttä väärää tietoa sekä siitä aiheutuneita vahinkoja. Informaatiovaikuttamisen muoto voi olla suoraa tai hienovaraista ja sen tyypillisiä keinoja voivat olla puolitotuudet, liioittelu, suoranainen valehtelu, painostaminen, valeuutisten kierrätys sekä verkossa olevat valesivustot. Tarvittaessa todenperäistä tietoa voidaan näiden ohella hyödyntää tarkoitushakuisesti. Informaatiovaikuttamiseen voidaan vastata lisäämällä ihmisten medialukutaitoa ja opastamalla suhtautumaan kriittisesti sosiaalisen median käyttöön, tunnistamalla esimerkiksi siellä olevia valetilejä. (Sisäministeriö 2018, 24-26.)

Ilmiönä informaatiovaikuttaminen ei ole kovinkaan uusi, lähinnä sen käyttötavat ja vaikuttavuus ovat olennaisesti muuttuneet nykyisessä sähköisessä mediaympäristössä. Päämääränä ja tavoitteena yleensä on, käyttämällä eri toimintatapoja useilla eri median alustoilla, vaikuttaminen päätöksentekijöihin ja päätöksentekoprosessiin ja sen avulla saada vaikuttamisen kohde tekemään itselleen haitallisia tai vaikuttajan kannalta myönteisiä päätöksiä. Usein vaikuttaminen tapahtuu myös välillisesti niin sanotun suuren yleisön kautta, mutta se voi kohdistua myös suoraan päätöksentekijöihin tai päätöksentekoprosessiin. Yleistä mielipidettä muokkaamalla saatetaan pyrkiä vaikuttamaan henkisen tilan hallintaan tai avoimessa yhteiskunnassa saattaa joskus riittää pelkästään hajaannuksen aikaan saaminen, mikä puolestaan voi vaikeuttaa viranomaisten ja poliittisen johdon työtä sekä tehdä tilannekuvan muodostamisen ja sen jakamisen vaikeaksi. (Hallintovaliokunta 2017.)

Informaatiovaikuttamista voidaan käyttää sekä hybridi- että kybervaikuttamisen välineenä, eikä merkitystä ole sillä, onko vaikuttaja valtiollinen tai valtiosta riippumaton toimija. Informaatiovaikuttamisessa on tyypillistä, että päätöksentekoa pyritään ohjaamaan muun muassa erilaisen disinformaation avulla tai vaillinaista tietoa jakamalla. Yhtä lailla tiedon jakamatta jättäminen voi olla informaatiovaikuttamista, kuten myös sinänsä oikean tiedon jakaminen vaikkapa mainonnan avulla, jolloin tiedolla pyritään vaikuttamaan kohteen mielikuviin ja tunteisiin. Tämän kaltaisen psykologisen vaikuttamisen korostuminen olemassa olevassa ja tulevaisuuden turvallisuusympäristössä tarkoittaa sitä, että tunteisiin vetoaminen ja siten vaikuttamisen ihmisten käyttäytymiseen saattaa muuttua arkipäiväiseksi. Oman haasteensa tiedon luotettavuuden arviointiin tuo digitalisaation ja tietotekniikan kehittyminen, sillä kehittyvä teknologia tekee toteuttavissa informaatio-operaatioissa informaation väärentämisestä yhä helpompaa. Uskottavuuden heikentämiseksi on mahdollista tuoda julkisuuteen esimerkiksi vääristeltyjä asiakirjatietoja henkilön terveydentilasta, ja jo tällä hetkellä on kehitteillä teknologiaa, jonka avulla videokuvan muokkaaminen reaaliajassa on mahdollista. Kohdennettu informaatiovaikuttaminen ja siihen liittyvät kampanjat eivät välttämättä tulevaisuudessa liity ainoastaan poliittisiin päättäjiin ja yhteiskunnan avainhenkilöihin, vaan myös kansalaisiin, joihin

vaikuttamalla ja heidän kauttaan vaikutetaan samalla yhteiskunnan keskeisiin toimijoihin. Huomionarvoista onkin, että onnistuneessa vaikuttamiseen keskittyvässä informaatio-operaatiossa toiminnan kohteena olevat eivät edes tiedä olevansa kohdehenkilöitä. (Hallintovaliokunta 2017.)

Suomessa luotetaan laajasti viranomaisiin ja viranomaistoimintaan, jota kuitenkin informaatiovaikuttamisella ja väärän tiedon levittämisellä eli disinformaatiolla voitaisiin pyrkiä tietoisesti horjuttamaan. Limnéll ja Iloniemi (2018, 200-201) muistuttavat, että jos suomalaiset menettäisivät luottamuksen viranomaistoimintaan ja oikeusvaltioon, olisivat sen vaikutukset erittäin vakavia Suomen ja suomalaisten turvallisuudelle. Jokin ilkeämielinen taho saattaisi pyrkiä vaikuttamaan tähän sekä konkreettisin toimin että voimakkailla psykologisilla operaatioilla, mikä tarkoittaisi yhteiskunnan vakauden, viranomaistoiminnan puolueettomuuden sekä sisäisen koheesion heikentämistä tarkoituksellisesti ja monin eri keinoin. Luottamuksen heikentäminen tarkoituksellisesti tai jopa ilman ulkopuolista vaikuttamistakin tapahtuva luottamuksen vakava horjuminen, on yksi Suomen vakavampia turvallisuusuhkia.

4.2 Kyber ja digitalisaatio turvallisuusuhkana teknologisessa kehityksessä

Turvallisuuden varmistaminen tietoverkoissa on ollut yksi 2010-luvun keskeisimmistä turvallisuushaasteista, sillä digitalisaation myötä yhä merkittävämpi osa ihmisten elämästä ja siten myös rikollisuudesta sekä kansallista turvallisuutta uhkaavasta toiminnasta kytkeytyy tietoverkkoihin. Sosiaalinen media, pikaviestintävälineet, tiedonhankinta ja tietojen tallennus sekä liikkuminen paikasta toiseen jättävät elektronisia jälkiä, joiden avulla on mahdollista tarkastella henkilön mennyttä ja nykyistä toimintaa sekä yhteyksiä muihin ihmisiin tai saada viitteitä hänen tulevasta toiminnastaan. Samalla kansalliseen turvallisuuteen kohdistuvien uhkien nähdään kytkeytyvän entistä vahvemmin ulkomaille, joten ulkomaita koskevan ja ulkomailta saatavan tiedon merkitystä pidetään entistäkin tärkeämpänä. (Leppänen & Pylväs 2018, 96.)

Ulko- ja turvallisuuspoliittisen selonteon mukaan teknologisessa kehityksessä on meneillään murros, joka koskettaa lähes kaikkia yhteiskunnan osa-alueita. Teknologia tarjoaa uusia välineitä sekä lisää mahdollisuuksia tiedonkulun ja vuorovaikutuksen tehostamiseen. Digitalisaatioon perustuvilla ratkaisuilla voidaan lisätä globaalia turvallisuutta, hyvinvointia ja terveyttä ja esimerkiksi uhkakuvien kartoittamisessa voidaan hyödyntää murrosteknologiaan perustuvia tekoälyjärjestelmiä. Samalla on aiempaa tärkeämpää laaja-alaisesti ymmärtää kehitykseen liittyviä turvallisuusuhkia, väärinkäyttömahdollisuuksia, ihmisoikeuskysymyksiä, taloudellisia mahdollisuuksia sekä keskinäisriippuvuuksia. Teknologisen kehityksen myötä siitä on tullut myös valtioiden välinen kilpailuareena, jossa viestintäverkkojen turvallisuuteen ja yhteiskunnan kriittisen infrastruktuurin haavoittuvuuksiin liittyvät riskit ja uhkat ovat kasvaneet. Yhteiskunnat ja taloudet rakentuvat enenevässä määrin uusien, esineitä ja järjestelmiä, kuten energiaverkkoja ja muuta kriittistä infrastruktuuria yhdistävien viestintäverkkojen varaan, korostaen

tietosuojakysymysten merkitystä. Sähköistyminen ja verkottuminen tehostavat yhteiskuntien toimintaa, mutta samalla verkkojen haavoittuvuudet voivat mahdollistaa vahingollisen toiminnan, jolloin häiriöt tai verkoissa toteutettava vihamielinen toiminta saattaisi vaikuttaa tiedon välittämiseen, tiedon eheyteen, liikenteen toimivuuteen sekä valtioiden toimintakykyyn kriisitilanteessa. Uusien teknologioiden tuomien mahdollisuuksien sekä uhkien arviointi vaatiikin kokonaisturvallisuuden näkökulmasta jatkuvaa ennakointia ja varautumista. (Valtioneuvosto 2020, 15-16)

Kyberuhkalla itsessään tarkoitetaan uhkaa, ”joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kybertoimintaympäristöstä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös sähköisessä viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista”. (Kokonaisturvallisuuden sanasto 2017, 44.)

Käytännön tasolla kyberturvallisuudella ja kyberuhkilla tarkoitetaan erityisesti tietoliikenteen ja erilaisten tietoteknisten järjestelmien häiriöitä. Yhteiskunnan ja elinkeinoelämän palveluiden toimivuuden edellytyksenä on viestintäpalveluiden ja -verkkojen häiriötön toiminta, mikä varsinkin vakavissa häiriötilanteissa ja poikkeusoloissa korostuu, sillä yhteiskunnan johtamisen ja väestön henkisen kriisinkestävyyden kannalta kansalaisten keskinäinen yhteydenpito, hätäpuhelut, viranomaiskanavat sekä joukkoviestintä ovat erittäin tärkeitä. Hätäpuheluiden ohella erittäin oleellista on radiotaajuuksien häiriötön toiminta, pelkästään jo viranomaisten vaaratiedotteiden ja kohdennettujen viranomaistiedotteiden välittämiseksi. Kriittisiä viestintäverkkoja ovat lisäksi koti- ja ulkomaan tietoliikenneyhteydet sekä matkaviestinverkko. (Sisäministeriö 2018, 49.)

Valtakunnallisen toimivuuden ohella, digitaalisten palveluiden toimivuus on vahvasti riippuvainen myös kansainvälisistä yhteyksistä, sillä monien tietoteknisten palveluiden toiminta on ulkomaisten palvelinkeskusten varassa. Käytännössä koko yhteiskunta on siis riippuvainen myös kansainvälisistä tietoliikenneyhteyksistä ja sen infrastruktuurista, mikä korostaa digitaalisten palveluiden ja järjestelmien luotettavuuden, tietoturvallisuuden ja tietosuojan merkitystä yhteiskunnan häiriöttömän toiminnan varmistamisessa. Digitalisaation kehittyessä, samalla myös järjestelmien ja organisaatioiden keskinäisriippuvuudet kasvavat, jolloin pilvipalveluiden ja järjestelmien keskittämisen yleistyessä, yksittäisten järjestelmähäiriöiden kerrannaisvaikutukset voivat olla merkittäviä vikojen ja häiriöiden ketjuuntuessa. Tällä puolestaan voi olla samanaikaisesti vaikutusta useiden eri organisaatioiden palveluiden käytettävyyteen sekä tietojen luottamuksellisuuteen ja/tai eheyteen. Laajamittaisesti ja vahingoittamistarkoituksessa toteutettuna, tällaisella voisi olla ennakoimattomat vaikutukset yhteiskuntaan. (Sisäministeriö 2018, 17-18.)

Viestintäpalvelut ja -verkot ovatkin otollinen kohde erilaisille kyberuhkille, koska niihin kohdistetulla vaikuttamisella tai hyökkäyksellä voitaisiin aiheuttaa laajamittainen ja moniin eri toimintoihin vaikuttava häiriötila. Uhka-arvioiden mukaan viestintäpalveluihin ja -verkkoihin kohdentuvan häiriötilaan syynä voisi käytännössä olla jonkinlainen tietoturvahäiriö tai jokin uudenlainen kyberuhka, tiettyyn käyttäjäjoukkoon tai maantieteelliseen alueeseen vaikuttava viestintäpalvelun toimitushäiriö, sään ääri-ilmiö, viestinnän tahallinen häirintä, kansainvälinen rikollisuus ja/tai terrorismi, suuronnettomuus tai jokin talous- tai työmarkkinahäiriö. Kyseeseen voisi siis tulla myös tietoinen ja tahallinen toiminta, jonka avulla pyritään vaikuttamaan viestintäverkkojen ja -palveluiden toimintaan. Tällaisen toiminnan taustalla voivat olla muun muassa rikolliset, terroristit tai valtiolliset toimijat. (Sisäministeriö 2018, 49.)

Käytännön esimerkkejä yhteiskunnan toimintoihin kohdistetuista kyberoperaatioista ovat suunnitelmallisesti toteutetut ja tarkasti kohdennetut palvelunestohyökkäykset, tietomurrot, kybertoimien avulla muokattu disinformaatio, tietoverkkotiedustelu sekä muunlainen tietoverkkojen häirintä. Terveydenhuoltojärjestelmään, energiantuotantoon tai teollisuuden ohjausjärjestelmiin kohdistettu kyberhyökkäys voisi pahimmillaan aiheuttaa niin materiaalista tuhoa kuin ihmishengen menetyksiä. Pelkästään internetin toimivuuteen vaikuttaisi fi-verkkotunnuksen nimipalveluihin aiheutuva vakava tekninen ongelma, jolloin se pysäyttäisi kaiken internetissä tapahtuvan fi-päätteisen liikenteen. Kyseisen tilanteen voisi synnyttää jokin teknisluontoinen häiriö, kuin yhtä lailla tahallinen vaikuttaminen verkon toimintaan. (Sisäministeriö 2018, 49.)

Erilaisten sähköisten järjestelmien ja palveluiden ollessa hyvinkin keskinäisriippuvaisia toisistaan, vikojen ja häiriöiden ketjuuntumista sekä kertautumista voidaan pitää merkittävänä uhkana. Sähköntuotantoon kohdistuva viestintäverkkojen tai -palveluiden toimivuushäiriö vaikuttaisi laajamittaisesti yhteiskuntaan ja häiriöt jo pelkästään yksittäisissä verkkopalveluissa voivat olla riski palvelujen saatavuudelle, varsinkin jos huomattava joukko muita palveluita on riippuvaisia yhden palvelun toimivuudesta, kuten esimerkiksi tunnistuspalveluista. Keskinäisriippuvuuden merkitystä erilaisten järjestelmien välillä kasvattaa myös esineiden internet ja sen myötä yhä useampien laitteiden kytkeytyminen internetiin. (Sisäministeriö 2018, 50.)

Kybertoimintaympäristössä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan vaikeasti ennakoitavia, vaikka samaan aikaan kybertoimintaympäristö näyttäytyy myös mahdollisuutena ja voimavarana. ”Kyberturvallisuus perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöön sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden häiriötilanteita. Kyberuhkalla voidaan siten tarkoittaa sellaista kybertoimintaympäristöön kohdistuvaa uhkaa, joka toteutuessaan vaarantaa kybertoimintaympäristön oikeanlaisen tai tarkoitetun toiminnan.” (Hallintovaliokunta 2017.)

Kyberuhkien kohdistuessa sähköiseen toimintaympäristöön, kuuluu siihen varsinaisen tiedon ohella useita yhteiskunnan elintärkeitä infrastruktuureita sekä tietoverkoista sovelluksiin ulottuvat infrastruktuuria kontrolloivat ja niitä ohjaavat digitaaliset ohjausjärjestelmät. Kyberuhat voivatkin näyttäytyä siviililuontoisina tai sotilaallisina, toiminnan toteuttajatahosta tai toiminnan tarkoitusperästä riippuen. Siviililuontoiset kyberuhat liittyvät useimmiten terrorismiin, ekstremismiin, vakoilutoimintaan sekä järjestäytyneen rikollisuuteen. Tietojärjestelmiin sekä niitä yhdistäviin tiedonsiirtoverkkoihin liittyvät uhkat voivat olla vakavia, sillä tietojärjestelmät ovat sulautuneet ja verkottuneet globaaleiksi kokonaisuuksiksi, jolloin niiden toiminnalliset häiriöt saattavat ulottua yksittäisiä palveluja laajemmalle ja häiriöiden vaikutuksia voi olla vaikea ennakoida. Useissa Euroopan maissa onkin havaittu toimintaa, jossa ulkopuolinen taho pyrkii tietoteknisesti kartoittamaan kriittistä infrastruktuuria ohjaavien järjestelmien ohjelmistoversioita. Mikäli vihamielinen valtio tai muu toimija saa tietoonsa kohdeympäristön ohjelmistoversiot, toimivien hyökkäysmenetelmien valitseminen onnistuu kriisitilanteessa nopeasti. (Hallintovaliokunta 2017.)

Limnéllin ja Iloniemen (2018, 110) mukaan turvallisuuden erinäisten rajapintojen hämärtyessä myös digitaalisen kyberympäristön ja fyysisen maailman rajat hämärtyvät. Kenties jatkossa kyberturvallisuuden käsitteestä luovutaan ja puhutaan vain turvallisuudesta, jonka erottamaton osa on digitaalinen toimintaympäristö kaikkine uhkine ja mahdollisuuksineen. Tietoliikennekaapeli fyysisesti katkaisemalla voidaan oleellisesti vaikuttaa digitaalisen ympäristön toimintaan, joten turvallisuuden näkökulmasta digitaalista ja fyysistä turvallisuutta on jatkossa yhä vaikeampi ja tarpeettomampi erottaa toisistaan. Näin ollen digitaalinen ja fyysinen turvallisuus todennäköisesti sulautuvatkin lähitulevaisuudessa ”yhdeksi turvallisuudeksi”.

Teknisiin järjestelmiin kohdistuvien kyberuhkien ohella kyberoperaatioihin liittyy myös kybervakoilu. Suomeen kohdistuu jatkuvasti erilaisia kyberoperaatioita, joiden tavoitteena on valtiollinen vakoilu, teknisen ympäristön kartoittaminen tai siihen vaikuttaminen. Kybervakoilua ei kohdisteta ainoastaan julkishallinnon tietoon, vaan kohteena voi olla myös erilaisten yritysten keskeinen tuotekehitystieto sekä yksittäisten henkilöiden luottamuksellinen viestintä. Kybervakoilun avulla hankitaan oikeudettomasti salassa pidettävää tietoa kohdemaan tietojärjestelmistä, tunkeutumalla järjestelmiin teknisesti tai painostamalla jotain omaan vaikutuspiiriin kuuluvaa tahoa, jolla on pääsy kyseisessä valtiossa taltioituun salassa pidettävään tietoon. Huolimatta siitä, että useilla valtioilla on tekniset edellytykset tunkeutua tietojärjestelmiin ohi suojausten, ei se kuitenkaan automaattisesti tarkoita, että noita kykyjä käytettäisiin Suomen kansallista turvallisuutta vastaan. Tehtyjen havaintojen perusteella vakoilua kohdistetaan erityisesti ulko- ja turvallisuuspoliittiseen päätöksentekoon, mutta yhtä lailla tavoitteena näyttää olevan jonkin kehittyvän valtion teknologisen suurvalta-aseman edistäminen ulkomaisten yritysten kustannuksella. (Suojelupoliisi 2019, 2.)

Suojelupoliisi (2019, 2) toteaa Suomen kohdistuvien kyberoperaatioiden jatkuvan myös lähitulevaisuudessa, sillä eri maiden tiedustelupalveluiden kiinnostus Suomen infrastruktuuria kohtaan on kasvanut. Arvioiden mukaan kyberympäristöön kohdistuva kansallisen turvallisuuden uhka on merkittävä, vaikka se ei fyysisenä tuhona ilmenisikään. Kybervakoilulla saadun tiedon avulla on mahdollista vaikuttaa päätöksentekoon, vastoin Suomen omaa intressiä, ja sen kautta kaventaa olennaisesti Suomen toimintavapautta. Suomen keskeisten yritysten tulos perustuu tekniseen kehitystyöhön, jolloin yritysten ja samalla Suomen kilpailukyky rapautuu, mikäli kilpailevat yritykset oman valtiokoneistonsa tuella saavat anastettua suomalaisten yritysten työn tulokset. Yhteiskunnan häiriötön toiminta perustuu tietoon sekä sen oikea-aikaiseen saatavuuteen ja eheyteen, jolloin kriittisen infrastruktuurin päätyminen kybervakoilua tai kybervaikuttamista aktiivisesti harjoittavan valtion hallintaan, aiheuttaa uhkan kansalliselle turvallisuudelle jo ennen kuin vakoilua harjoittava valtio mahdollisesti päättää edes käyttää voimaansa.

Kyberrikollisuudesta itsessään ei olemassa yleisesti käytettyä määritelmää, joten toisinaan käytetään termejä tietoverkoissa tapahtuvat rikokset tai tietoverkkorikokset. Kyberrikosten ytimen muodostavat kuitenkin tietokoneiden ja -verkkojen tiedon eheyteen, luottamuksellisuuteen ja saatavuuteen puuttuvat teot. Europolin Internet Organized Crime Threat Assesment -raportin (IOCTA) mukaan kyberrikollisuus on jatkanut kasvuaan ja kehittymistään ja pienellä määrällä kyberhyökkäyksiä on aiheutettu merkittäviä haittoja. Erityisesti internetiin kytkettyjen laitteiden (IoT) haavoittuvuuksien hyödyntäminen on mahdollistanut merkittävien haittojen tuottamisen yhteiskunnan palveluille. Siinä missä yhteiskunnan palveluiden digitalisointi on tehostanut ja lisännyt palveluiden saatavuutta, on se samalla luonut tietoverkkorikosten tekijöille uusia tapoja haittojen ja vahinkojen aiheuttamiseen. Tietoverkkorikosten kohteet voivat valikoitua satunnaisesti haittaohjelmaa laajalti levittämällä tai ennalta tehdyn tiedustelun tuloksena. Muutamia vuosia sitten rikollisille taloudellisesti tuottoisinta toimintaa oli esimerkiksi pankkihaittaohjelmien levittäminen, mutta nykyisin teknisesti kyvykkäille rikollisille kannattavinta voi olla haittaohjelmien myyminen pimeillä markkinoilla, jolloin niiden varsinaisen hyödyntämisen ja levittämisen hoitaa jokin toinen rikollisorganisaatio tai yksittäinen toimija. (Piiroinen & Ulkuniemi & Toiviainen 2018, 104.)

Teknologian kehittyessä kyberrikollisuuden suuntaviivojen ennustaminen on hankalaa ja lähitulevaisuudessa siihen voi liittyä myös tekoälyn hyödyntäminen rikollisessa tarkoituksessa, minkä avulla voidaan aiheuttaa laajoja vaikutuksia yhteiskunnan elintärkeisiin toimintoihin sekä vaikeuttaa kyberrikosten torjumista. Haasteena voi olla rikosoikeudellisen vastuun määrittäminen itseoppivien järjestelmien suorittamien toimien osalta, koska tuolloin on epäselvää, miltä osin tekoälyn luonut ja sen ohjelmoinut henkilö on vastuussa itseoppivan ohjelmiston toiminnasta, mikäli se toimillaan aiheuttaa rangaistavan teon. (Piiroinen ym. 2018, 104.)

Kyberrikollisuudessa on havaittavissa tiettyjä yleistettävissä olevia piirteitä, kuten se, että usein rikosten takana on useampi henkilö, jotka keskenään toimivat yhteistyösuhteessa ja/tai

ostavat sekä myyvät toisilleen rikollisia palveluja. Henkilöt toimivat usein eri maissa ja rikosta suunnitellessaan ja toteuttaessaan he hyödyntävät erilaisia internetin kaupallisia tai puhtaasti rikollisia palveluita, jotka yhtä lailla sijaitsevat useissa eri maissa. Rikos palveluna eli Crime-as-a-Service (CaaS) näyttäytyy yhtenä merkittävimmistä kyberrikollisuutta lisäävistä tekijöistä, koska se itsessään on tehokas toimintamalli ja sitä on jo kauan käytetty laillisessa liiketoiminnassa alihankinnan nimellä. Tehokkuuden lisäksi se madaltaa nuorten, terroristien sekä perinteisen rikollisten siirtymistä kyberrikollisuuden pariin, sillä omaa osaamista ei tarvita paljoakaan. (Piiroinen ym. 2018, 105.)

Kyberrikollisuudessa tekniikan rooli on merkittävä, rikosten tapahtuessa lähinnä teknisessä ympäristössä ja usein onnistuminen edellyttääkin jonkinlaisten suojausten ohittamista käyttöjärjestelmien ja sovellusten virheitä hyväksikäyttämällä. Tämän ohella ihmisten erehdyttäminen halutun tiedon antamiseen tai tarvittavien toimenpiteiden tekemiseen on edelleen yksi tehokkaimmista hyökkäystavoista. Rikolliset saattavat joskus käyttää myös useampia hyökkäystapoja saavuttaakseen haluamansa ja kaikessa rikollisuudessa tekijän oikean identiteetin peittäminen on sitä suuremmassa roolissa, mitä suunnitelmallisemmin rikos tehdään. Kyberrikokset edellyttävätkin usein suunnitelmallisuutta ja valmisteluja, pitäen sisällään tavan tietoliikenteen alkuperäisen lähteen ja tekijöiden identiteetin peittämiseen. Pimeät verkot, TOR, VPN-palvelut, välityspalvelimet, tiedostojen salaus, virtuaalivaluutat sekä monet muut tekniikat ovat osaavissa käsissä tehokkaita tapoja oikean identiteetin peittämiseen. Viimeisin suurempi muutos kyberrikollisuudessa on ollut rikollisten ja valtiollisten toimijoiden operoiminen samoilla alueilla. (Piiroinen ym. 2018, 105-106.)

Ulko- ja turvallisuuspoliittisen selonteon mukaan ”yhteiskuntien digitalisoituessa on erityisen tärkeää varmistaa kybertoimintaympäristön turvallisuus. Suomen tavoitteena on avoin, vapaa ja turvallinen kybertoimintaympäristö, jossa huomioidaan eettiset näkökohdat sekä tietosuoja- ja sananvapauskysymykset. Digitaalisten palveluiden saavutettavuus, infrastruktuurin käytettävyys sekä tiedon palautettavuus on kyettävä turvaamaan kaikissa olosuhteissa.” Samalla on tiedostettava teknologisesta kehityksestä aiheutuvan syrjäytymisen aiheuttamat turvallisuusriskit sekä huomioitava tulevien viestintäverkkojen turvallisuus- ja häiriönsietokyky, myös poikkeustilanteissa. (Valtioneuvosto 2020, 37-38.)

4.3 Sähkön- ja energiansaannin häiriöt yhteiskunnan kriittisenä uhkana

Voimahuoltoon eli sähkön- ja energiansaantiin kohdistuvia uhkia ja mahdollisia häiriöitä voidaan pitää yhteiskunnan turvallisuuden ja toimivuuden kannalta erittäin merkittävinä, sillä heijastevaikutukset useisiin eri toimintoihin ja kansalaisten arkeen olisivat nopeasti hyvinkin laajat. Globalisoituneessa maailmassa yhteiskunnan vahvasti toisiinsa verkottuneet, monimutkaistuneet ja teknistyneet toiminnot ovat hyvin keskinäisriippuvaisia aiheuttaen haavoittuvuutta ja häiriöalttiutta. Verkottuneessa toimintaympäristössä järjestelmien toimintavarmuus rakentuu

kaikkien toimijoiden ja järjestelmien virheettömän toiminnan varaan. Sähköjärjestelmän ja tietojärjestelmien häiriöttömällä toiminnalla varmistetaan muiden yhteiskunnallisesti tärkeiden toimintojen saatavuus ja järjestelmähäiriön tapahtuessa yhteiskunnan tulisikin pystyä nopeasti vastaamaan vallitsevaan tilanteeseen. (Keränen, Molarius, Heikkilä, Poussa & Partanen 2016, 11.)

Yhteiskunnan eri toimintojen ja erityisesti huoltovarmuuden kannalta erittäin kriittistä on sähkön häiriötön saatavuus, sillä siihen kohdistuva vakava häiriötila aiheuttaisi vaikutuksia kaikkiin yhteiskunnan toimintoihin sekä voisi vaarantaa elintärkeät toiminnot ja väestön hyvinvoinnin. Teollisuudessa ja sen prosesseissa pelkästään lyhyet, jopa alle 10 sekunnin pituiset sähkön saannin häiriöt, voivat aiheuttaa ongelmia osalle teollisuusprosesseista. Häiriötilanteen jatkuessa ja sähkönsaannin samalla heikentyessä, useimmat yhteiskunnan toiminnot häiriintyisivät suuresti tai niiden toiminta pysähtyisi kokonaan, mikä puolestaan horjuttaisi kaikkia yhteiskunnan elintärkeitä toimintoja. (Sisäministeriö 2018, 44-45.)

Yhteiskunta on nykyisin hyvin riippuvainen keskeytymättömästä sähkönsaannista, sillä sähkönsaannin häiriöttömyys on perusedellytys lähes kaikille yhteiskunnan kriittisille toiminnoille, kuten vesi- ja jätehuolto, elintarvikehuolto, pankit ja maksuliikenne, liikenne ja polttoainehuolto, tele- ja tietoliikenne, lämmitys, päiväkodit ja koulut, sairaalat ja terveyskeskukset, maatalous sekä pelastus- ja turvallisuustoimi. Sähkön rooli on vaikeasti korvattavissa, ainakin lyhyellä aikavälillä, jolloin palautuminen laajoista häiriöistä on sekä kallista että hidasta. Teknisten vikojen ohella energian tuotanto- ja siirtojärjestelmien toimivuutta uhkaavat erityisesti sään ääri-ilmiöt ja luonnononnettomuudet, kyberuhat sekä tuonti- ja jakeluyhteyksien katkeaminen erinäisistä syistä johtuen. (Turvallisuuskomitea 2017, 89-90.)

Varautumisen tarpeisiin liittyvän tutkimuksen mukaan normaalioloissa todennäköisimpiä sähkönsaannin ja jakeluverkon häiriötilanteita ovat myrskyistä ja lumikuormista aiheutuvat katkokset, mistä johtuen sähkön jakeluverkkoyhtiöt ovat velvoitettuja varautumaan ja valmistautumaan tämän kaltaisiin tilanteisiin. Epätodennäköisempi, mutta huomattavasti ongelmallisempi on sekä kantaverkkoon että jakeluverkkoon kohdistuva häiriötilanne, jossa häiriön syy on tuntematon. Tällainen häiriötilanne voisi johtua esimerkiksi tunnistamattomasta sähköverkon ja tietoliikenneverkon keskinäisvaikutuksesta tai kantaverkkoa tai jakeluverkkoja ohjaaviin järjestelmiin kohdistuvasta kyberhyökkäyksestä. (Valtioneuvoston kanslia 2016, 19-20.)

Sähkönjakelua, polttoainehuoltoa ja/tai teleoperaattoreiden toimintaa heikentävä ja kenties pidempään kestävä häiriötilanne saattaisi aiheuttaa huomattavia ongelmia esimerkiksi poliisitoiminnalle. Teleoperaattoreiden linkkimastojen varavirtalähteiden kestävyys voi esimerkiksi talven kovissa pakkasissa olla heikko ja toisaalta kesäaikaan pienemmän telemastot eivät pysty varavoiman avulla ylläpitämään tarvittavaa jäähdytystä, jolloin häiriötilanteessa lämpötila voi

nousta korkealle hyvinkin nopeasti ja tällöin masto ajaa varotoimena itsensä alas. Sähkönjakelun häiriötilanteessa myös televiestintä on todennäköisesti normaalia laajempaa, jolloin mobiiliverkko tukkeutuu nopeasti. Viranomaisille sen voisi aiheuttaa suuria ongelmia viranomaisverkon (VIRVE) toimintaan, millä vastaavasti on suoria vaikutuksia esimerkiksi poliisin operatiiviseen toimintakykyyn. (Valtioneuvoston kanslia 2016, 21.)

4.4 Ääriliikkeet ja terrorismi kansalaisten turvallisuusuhkana

Suojelupoliisin julkaiseman Kansallisen turvallisuuden katsauksen (2019, 3) mukaan terrorismin uhka on Suomessa tällä hetkellä kohonnut ja tulee ainakin lyhyellä aikavälillä säilymään kohonneena eli neliportaisen asteikon tasolla kaksi. Keskeinen uhkaan vaikuttava tekijä on Syyrian ja Irakin konfliktialueille lähteneiden vierastaistelijoiden mahdollinen paluu Suomeen. Suojelupoliisin mukaan Suomessa esiintyy merkittävää terrorismin tukitoimintaa, vaikka Suomi ei näyttäydykään ensisijaisena terroristi-iskujen kohdemaana. Suomessa on kuitenkin olemassa ryhmiä ja henkilöitä, joilla on motivaatio ja kyky terrori-iskun toteuttamiseen. Lisäksi on olemassa merkittävimmän uhkan muodostavia yksittäisiä henkilöitä tai pienryhmiä, joiden motivaation lähteenä on radikaali-islamistinen propaganda. Syyrian ja Irakin konfliktialueen muuttuneesta tilanteesta huolimatta on muistettava, että alueella toimiva terroristijärjestö ISIL eli ”Islamilainen valtio” aiheuttaa kannattajineen edelleen maailmanlaajuisen uhkan ja pyrkii kehittämään uusia taktiikoita iskujen toteuttamiseksi. (Suojelupoliisi 2019, 3.)

Suomessa olevien, terrorismintorjuntaan kytkeytyvien kohdehenkilöiden määrä jatkaa kasvuaan ja yhteydet kansainväliseen terrorismiin ovat lisääntyneet. Yhä suurempi osa näistä henkilöistä on osallistunut aseelliseen toimintaan tai vastaanottanut terroristista koulutusta. Kotoperäistä radikalisoitumista sekä Syyrian ja Irakin konfliktialueen heijastevaikutuksia voidaankin pitää keskeisinä vaikuttavina tekijöinä nimenomaan kohdehenkilöiden lukumäärän lisääntymiseen sekä terrorismin uhkan kasvuun. (Suojelupoliisi 2019, 3.)

Terroristisen toiminnan taustasyy on väkivaltainen ekstremismi ja siihen liittyvä radikalisoituminen, joka puolestaan voi johtua useista eri syistä. Ei ole olemassa tietynlaista henkilötyyppiä tai profiilia, jonka avulla voitaisiin helposti tunnistaa sellaiset radikalisoituneet henkilöt, jotka kenties suunnittelevat terroristista rikosta tai laajamittaisen väkivaltaisen teon toteuttamista. (Sisäministeriö 2018, 35.)

”Väkivaltaisella ekstremismillä tarkoitetaan sitä, että väkivaltaa käytetään, sillä uhataan, siihen yllytetään ja kannustetaan tai se oikeutetaan aatemaailmalla perustellen. Väkivaltainen ekstremismi ei ole rikosoikeudellinen käsite. Ekstremistinen väkivalta ei välttämättä ole kumouksellista, ja se kohdistuu usein viholliseksi määriteltyyn ryhmään tai yksilöihin. Se aiheuttaa pelkoa ja turvattomuuden tunnetta paikallisesti, esimerkiksi yksittäisissä kaupunginosissa tai

asuinalueilla ja voi kohdistua myös omaisuuteen. Rikokset, joiden motiivina on viha ja/tai rasismi (viharikos), voivat olla myös ekstremistisiä rikoksia silloin, kun teon motiivina on kokonainen aatemaailma.” (Sisäministeriö 2020, 11.)

Väkivaltaisen ekstremismin tilannekatsauksessa todetaan, että suurin vakavan väkivallan, kuten joukkosurman, uhka liittyy yksittäisiin toimijoihin, joiden motiivi voi liittyä laajasti väkivaltaiseen ekstremismiin. Yksittäiset toimijat kuitenkaan harvoin toimivat yksin, vaan ovat yleensä osa jotain sosiaalista ympäristöä internetissä. Tällä hetkellä, suurimman uhkan arjen turvallisuudelle muodostaa väkivaltainen ulkoparlamentaarinen äärioikeisto, joka ilmenee esimerkiksi spontaanina katuväkivaltana, kohdistuen vihollisiksi koettuihin henkilöihin, jotka voivat valikoitua uhriksi sattumanvaraisesti. Ulkoparlamentaariseen väkivaltaiseen äärivasemmistoon, erityisesti anarkismiin ja antifasismiin liittyvä radikaaliliikehdintä on ollut viime vuosina vähäistä ja sitä ilmenee pääsääntöisesti mielenosoitusten yhteydessä. (Sisäministeriö 2020, 11.)

Terrorismissa kyse on aina väkivaltaisesta ekstremismistä, mutta kaikki väkivaltainen ekstremismi ei kuitenkaan ole terrorismia. Terroristisessa tarkoituksessa tehdyt rikokset määritellään rikoslaissa (RL 34a). Terroristinen väkivalta on kumouksellista ja sen kohteina ovat maat tai kansainväliset järjestöt ja toiminnan tarkoituksena on muun muassa aiheuttaa vakavaa pelkoa väestön keskuudessa. Ekstremistisessä rikoksessa motiivi liittyy tekijän aatemaailmaan. Viharikoksen ja ekstremistisen rikoksen erottaa toisistaan se, että viharikoksen motiivi liittyy uhrin yksittäiseen ominaisuuteen, mutta ekstremistisen rikoksen motiivi liittyy kokonaiseen aatemaailmaan.

Ekstremistiseksi väkivallaksi katsotaankin kaikki sellainen väkivaltarikollisuus, joka liittyy väkivaltaisiin ekstremistisiin ryhmiin ja niiden jäsenten toimintaan. Näkyvien ekstremistisen ryhmien käyttämä väkivalta on välineellistä, riippumatta väkivallan kohteesta tai hetkellisestä motiivista, jolloin yleinen väkivallan uhka lisää ryhmän pelotevaikutusta. Ekstremistisiksi rikoksiksi ei kuitenkaan katsota sellaisia väkivaltarikoksia, joilla on selkeästi jokin muu motiivi, kuten esimerkiksi muuhun rikollisuuteen liittyvä väkivalta, yksityiselämään liittyvä riita tai perhe- ja lähisuhdeväkivalta. (Sisäministeriö, 2020, 15.)

Väkivaltaiseen ekstremismiin liittyvä väkivaltainen radikalisoituminen on ”prosessi, jonka myötä yksilöt päätyvät käyttämään väkivaltaa tai uhkaamaan sillä, kannustamaan siihen tai oikeuttamaan se aatemaailmalla perustellen. Radikalisoitumisprosessin edetessä yksilö alkaa hyväksyä ja ihannoimaan väkivaltaa riippumatta siitä, millaisella aatemaailmalla tai eri aatteista otetuilla vaikutteilla hän väkivaltaa perustelee.” Radikalisoitumisen taustalla olevat syyt liittyvät yleensä yleisiin yhteiskunnallisiin, sosiaalisiin ja yksilötason tekijöihin, jonka lisäksi tekijät voidaan jakaa vetäviin ja työntäviin. Radikalisoitumisessa sosiaalisella verkostolla on merkitystä ja yksilö voikin radikalisoitua osana sosiaalista verkostoa. Tunteilla on radikalisoitumisessa tärkeä merkitys, jonka ohella myös ideologisilla tekijöillä on vaikutusta. Syrjäytyminen

ja ongelmat toimeentulossa voivat edistää väkivaltaista radikalisoitumista, mutta eivät yksin selitä sitä, sillä usein myös erilaiset tilannetekijät vaikuttavat siihen, miksi jotkut yksilöt radikalisoituvat ja toiset eivät. (Sisäministeriö, 2020, 14-15.) Ongelmat nuorten koulutuksessa, työelämässä tai terveydenhuollon palveluissa voivat kasvattaa näköalattomuutta, epätasa-arvon kokemista sekä valtioiden sisäistä epävakautta, luoden kasvualustaa väkivaltaiselle ekstremismille ja terrorismille. (Valtioneuvosto 2020, 23.)

Radikalisoituminen voi tapahtua tai sitä voidaan edistää vankilassa, jossa radikalisoituneet henkilöt pystyvät helposti verkostoitumaan muiden rikollisten ja erityisesti järjestäytyneen rikollisuuden edustajien kanssa. Terrorismiin ja radikalisoitumiseen perehtynyt amerikkalainen professori Muqtedar Khan (2017) mainitsi luennollaan Poliisiammattikorkeakoululla, että erityisesti vankilassa tapahtuvan verkostoitumisen ja kontaktiensa kautta radikalisoituneilla henkilöillä ja/tai ääriryhmien edustajilla on saatavilla tietoa ja osaamista helposti valmistettavista aseista ja räjähteistä, ajoneuvojen anastamisesta, verkossa tehtävistä rikoksista sekä monista muista rikollisen toiminnan osa-alueista. Verkostoitumisen myötä voidaan myös helposti tehdä erilaisia ”alihankintasopimuksia”, jossa kaikki osapuolet hyötyvät haluamallaan tavalla.

Toteutuessaan terroristinen isku voisi kohdistua yhteiskunnan johtamiseen, kriittiseen infrastruktuuriin, julkisiin paikkoihin tai laajoihin ihmisjoukkoihin, jonka seurauksena voitaisiin aiheuttaa joko rajattuja tai välittömästi merkittäviä sekä myös pidempiaikaisia vaikutuksia. Terroristinen isku voisi aiheuttaa pelkoa kansalaisissa, mikä puolestaan saattaisi lisätä suoraan kansalaisiin vaikuttavien erilaisten turvallisuustoimien tarvetta ja näin ollen terroristisen teon vaikutukset saattaisivat olla varsinaista tekoa paljon laajemmat. Käytännön esimerkkinä mainittakoon tietoliikenteen ja sähköverkon solmukohtiin tai joihinkin muihin yhteiskunnan keskeisiin elintärkeisiin toimintoihin kohdistuva terroristinen isku, jolla voitaisiin saada aikaan laajoja ja merkittäviä yhteiskunnan toimintoihin kohdistuvia seurannaisvaikutuksia. (Sisäministeriö 2018, 35-36.)

Viime vuosina maailmalla tehdyissä terrori-iskuissa on niin sanottujen perinteisten pommi-/räjähdeiskujen ohella käytetty erilaisia helposti toteutettavia sekä kustannuksiltaan edullisia menetelmiä, kuten ajoneuvoja ja teräaseita. Tarvittaessa yksinkertaisilla menetelmillä tehtyjä iskuja voidaan toteuttaa melko helposti ja nopeasti, eikä niiden toteuttamisessa vaadita erityistä osaamista tai sen kaltaista pidempää valmistautumista ja suunnittelua kuin räjähde- tai ampuma-aseiskuissa. Tämä ei kuitenkaan tarkoita sitä, että uhka perinteisiin räjähde- tai ampuma-aseiskuihin olisi poistunut ja nykyisin niin sanottuihin perinteisiin iskuihin voidaan liittää myös CBRNE-aineiden käyttöä. Teknologisen kehityksen myötä ei myöskään kannata unohtaa helppokäyttöisten ja edullisten miehittämättömien ilma-alusten eli dronejen käyttöä, joista esimerkkejä on jo olemassa. (Sisäministeriö 2018, 35-36.) CBRNE tai CBRN on lyhenne englannin kielen sanoista chemical (kemiallinen), biological (biologinen), radiological (säteily), nuclear

(ydin-) ja explosive (räjähtävä, räjähde). Lyhennettä käytetään sellaisista ydinuhkista ja uhkista, jotka liittyvät kemiallisiin, biologisiin tai säteileviin aineisiin tai räjähteisiin. (Kokonaisturvallisuuden sanasto 2017, 48.)

Ääriliikkeiden ja terrorismin ohella yhteiskuntajärjestystä ja kansalaisten arkista turvallisuutta saattaa uhata myös suurista kokoontumisista tai mielenosoituksista alkunsa saava isojen joukkojen väkivaltainen liikehdintä, joita viime vuosina on Euroopan suuremmissa kaupungeissa nähty. Toiminta on saattanut kestää jopa päiviä ja usein tällaiseen liikehdintään osallistuu myös sellaisia henkilöitä ja ryhmiä, joiden tavoitteena on muuttaa tilanne väkivaltaiseksi mellakaksi. Suomessa tällainen samaan aikaan useassa paikassa tai eri kaupungeissa tapahtuva laajamittainen väkivaltainen levottomuus saattaisi aiheuttaa tilanteen, jossa poliisin voimavarat tilanteen hallitsemiseen eivät enää riittäisi. Riskiä tällaisten levottomuuksien syntymiseen muodostaa ja sitä kasvattaa yksittäisten kansalaisten arkeen vaikuttavat yhteiskunnalliset epäkohdat sekä eriarvoisuuden kokeminen, syrjäytymisen lisääntyminen, ääriliikkeiden toiminta, yhteiskunnan toimintojen häiriintyminen tai niiden pysähtyminen kokonaan esimerkiksi sähkönsaantiin tai kybertoimintaympäristöön kohdistuvan häiriön vuoksi, sosiaalisen median vaikutus sekä kiristynyt yleismaailmallinen tilanne. (Sisäministeriö 2018, 37.)

Ihmisten tyytymättömyyttä ja jännitteiden purkamista on mahdollista tietoisesti sekä suunnitelmallisesti kiihottaa ja syntyvien levottomuuksien avulla on mahdollista heikentää kansalaisten turvallisuutta ja turvallisuuden tunnetta sekä aiheuttaa taloudellisia vahinkoja. Samalla voidaan vaikuttaa yhteiskunnan toimintoihin, vähentää luottamusta poliittiseen päätöksentekoon sekä viranomaisten toimintaan. Sosiaalisen median avulla tai siellä tapahtuvan informaatiovaikuttamisen keinoin voidaan levittää vihapuhetta ja valeuutisten kautta ruokkia ihmisten tyytymättömyyden tunnetta ja siten madaltaa kynnystä osallistua väkivaltaiseen liikehdintään. (Sisäministeriö 2018, 38.)

4.5 Järjestäytynyt ja rajat ylittävä rikollisuus kasvavana uhkana

Kansallisessa riskiarviossa ei käsitellä järjestäytynyttä ja rajat ylittävää rikollisuutta, joka kenties näyttäytyy ennemminkin suoraan turvallisuusviranomaisten tehtäväkenttään kuuluvana ilmiönä ja uhkatekijänä. Vaikka kyseessä ei olisikaan varsinainen yhteiskuntaan kohdistuva uhkatekijä, asettaa järjestäytynyt ja rajat ylittävä rikollisuus kasvavia haasteita viranomaisille sekä vaikuttaa organisaatioiden, yritysten ja kansalaisten turvallisuuteen monimuotoistuvan ja jatkuvasti toimintatapojaan kehittävän rikollisen toiminnan kautta. Käsiteltävistä uhkatekijöistä järjestäytynyt rikollisuus näyttäytyy kenties konkreettisimpana poliisitoiminnan kannalta, jonka lisäksi sillä on erinäisiä kytköksiä myös muihin käsiteltyihin turvallisuusympäristön uhkiin. Järjestäytyneen rikollisuuden kohdalla on huomioitava, että useimmiten sillä samaan aikaan tarkoitetaan vakavaa rikollisuutta. Järjestäytynyt rikollisuus sellaisenaan ei kuitenkaan

ole oma erillinen rikollisuuden alansa, vaan kyse on tavallisista rikoksista, kuten huumausainerikoksista, talousrikoksista tai henkeen ja terveyteen kohdistuvista rikoksista, joita kuitenkin tehdään erityisen systemaattisesti sekä erityistä ryhmärakennetta hyödyntämällä. (Poliisihallitus 2019, 5.)

Euroopan unionin lainvalvontaviranomaisena toimiva Europol tukee toiminnallaan unionin jäsenvaltioita vakavan kansainvälisen rikollisuuden ja terrorismin torjunnassa sekä tekee yhteistyötä monien EU:n ulkopuolisten kumppanivaltioiden ja kansainvälisten organisaatioiden kanssa. Laajojen rikollisverkostojen ollessa merkittävä uhka EU:n sisäiselle turvallisuudelle sekä ihmisten turvallisuudelle ja toimeentulolle, Europolin tärkeimpiä torjunta-alueita ovat terrorismi, huumekauppa, rahanpesu, eurovääreennökset, ihmissalakuljetus ja ihmiskauppa sekä verkkorikollisuus. Euroopan unionin keskeinen idea on vapaa liikkuvuus, joka parhaiten toteutuu Schengen-alueella, mutta samalla siihen liittyy myös monia riskejä Suomen sisäiselle turvallisuudelle. (Turvallisuuskomitea 2017, 84).

Järjestäytynyt rikollisuus on ilmiönä laaja ja monimuotoinen. Europolin mukaan Euroopassa toimii kaikkiaan noin 5000 järjestäytynyttä rikollisryhmää, joista arvioiden mukaan Suomessa noin 90 ryhmää ja niihin kuuluu kaikkiaan noin 1000 henkilöä. Järjestäytyneen rikollisuuden ryhmärakenteille on ominaista niiden verkostomaisuus sekä tapauskohtainen ja tarpeenmukainen nopea joustavuus. Euroopan alueen helppo ja nopea liikkuvuus sekä tietoverkkojen näkyvä viestintä osaltaan mahdollistaa monia uudenlaisia kehittyviä toimintatapoja ja -rakenteita. Rikoksia voidaan myös toteuttaa eri maissa tehtyinä osatekoina, joissa tekijät eivät välttämättä edes tunne toisiaan. Rikollisuuden eri tasot kytkeytyvät rikoksenteossa toisiinsa periaatteella: organisoijat, rahoittajat, asiantuntijat, järjestyksenpitäjät, ammattitekijät ja taparikolliset. Vaikka yleinen käsitys järjestäytyneestä näyttäytyykin ”liivimiehinä” ja erilaisina jengitunnuksina, käsittää se paljon muutakin, mikä läheskään aina ei näyttäydy erillisinä ulkoisina tunnusmerkkeinä. (Poliisihallitus 2019, 5.)

Europolin Serious and Organised Crime Threat Assesment -raportin (SOCTA) mukaan järjestäytyneen rikollisuuden toimijat omaksuvat ja pystyvät nopeasti integroimaan uudenlaista tekniikkaa ja sen hyödyntämistä mukaan toimintaansa uusia liiketoimintamalleja rakennettaessa. Rikosten tekemisessä hyödynnetään digitaalisen verkon tarjoamia mahdollisuuksia, kuten toiminnan laajentumista verkkokauppaan sekä salattujen viestintäkanavien käyttämistä. Asiakirjapetokset, rahanpesu sekä laittomien tuotteiden ja palveluiden verkkokauppa ovat järjestäytyneen rikollisuuden toiminnan ajureita EU:ssa ja vaikka asiakirjapetoksilla tai rahanpesulla ei olekaan suoraa vaikutusta useimpiin EU:n kansalaisiin, hyödyttää se ennen kaikkea vakavaa ja järjestäytynyttä rikollisuutta. Laittomien tuotteiden ja palveluiden verkkokauppa kasvaa nopeasti ja lähes kaikenlaista laitonta tavaraa ostetaan ja myydään online-alustojen kautta, niiden tarjotessa vastaavanlaisia käyttö- ja ostokokemuksia kuin useimmilla laillisilla online-alustoillakin.

Hyödykkeen ja palvelun tyypistä riippuen, näitä kaupankäynnin alustoja löytyy sekä pintaverkosta että pimeästä verkosta, Darknetistä. Monien ns. tavanomaisten myyntituotteiden ohella kauppatavarana voi olla myös ostajalle hyödyllistä tietoa ja dataa. Laittomien tavaroiden ja palveluiden verkkokaupan odotetaankin häiritsevän vakiintuneita rikollismarkkinoita ja niiden perinteisiä jakelumalleja lähivuosina. Teknologisella kehityksellä kaikkinensa arvellaan olevan perustavanlaatuinen ja kestävä vaikutus rikollisen toiminnan luonteeseen. (Europol 2017, 10.)

Rikollisjärjestöjen ollessa erittäin joustavia ja sopeutumiskykyisiä ja mukauttaessaan toimintansa tai kokonaisen liiketoimintamallinsa ympäristön muutoksiin, monet rikolliset toimet ovat yhä monimutkaisempia ja niiden toteuttaminen vaatii erityisiä taitoja ja asiantuntemusta. Parhaiten menestyvät ne, jotka pystyvät sijoittamaan merkittävät voittonsa lailliseen talouteen sekä omiin rikollisiin yrityksiinsä, varmistaen näin liiketoiminnan jatkuvuuden ja rikollisen toiminnan laajentumisen entisestään. (Europol 2017, 10.)

Järjestäytyneen rikollisuuden rikollisryhmittyvät toimivat usein verkostomaisesti, jossa tilanteen ja tarpeen mukaan voidaan käyttää tarvittavaa erikoisosaamista ja asiantuntemusta. Tämän kaltainen kysyntä antaa mahdollisuuksia eräänlaisille rikollisuuden "yksityisyrittäjille", jotka tarjoavat rikoksia erillisinä ostopalveluita (Crime as a Service - CaaS), harjoittaen omaa rikollista toimintaansa ilman perinteisiä järjestäytyneiden rikollisryhmittymien ylläpitämiä infrastruktuureja. Näiden yksittäisten palveluntarjoajien toiminnan mahdollistaa jo aiemmin mainittu laittomien tavaroiden ja palveluiden verkkokauppa, jossa kyseisiä ostopalveluita on tarjolla esimerkiksi kyberhyökkäysten toteuttamiseksi. (Europol 2017, 13.)

Järjestäytyneeseen rikollisuuteen kytkeytyy erilaisia toimintatapoja sekä toiminnan muotoja, jotka liittyvät keskeisesti varsinaisten rikosten tekemiseen tai joiden avulla voidaan tukea rikollisen toiminnan toteuttamista tai mahdollistaa niiden tekeminen. Rikollisiin toimintamalleihin sisältyy korruptio, vastatoimet viranomaisia kohtaan, talousrikollisuus (rahanpesu), asiakirjaväärennökset, laiton verkkokauppa, teknologian hyödyntäminen sekä väkivalta ja kiristys.

Rikollinen toiminta itsessään on monimuotoista ja Europolin mukaan järjestäytyneen rikollisuuden toiminnan muotoja ovat valuuttaväärennökset, kyberrikollisuus, huumausaineiden tuotanto, salakuljetus ja levittäminen, petokset, laittomat jätekuljetukset, väärennettyjen tuotteiden kauppa, maahanmuuttajien salakuljetus, organisoitu omaisuusrikollisuus, urheiluun kytkeytyvä korruptio, uhanalaisten eläinlajien salakuljetus, laiton ampuma-asekauppa sekä työperäinen ihmissalakuljetus. Europolin näkemys järjestäytyneen rikollisuuden määritelmästä ja rakenteesta on nähtävissä kuviossa 5. (Europol 2017, 13.)

Kuvio 5: Europolin määritelmä järjestäytyneen rikollisuuden rakenteesta

Globaalien uhkien tapaan kansainvälisessä rikollisuudessa tapahtuvat muutokset heijastuvat ja ulottuvat nopeasti myös Suomeen, tuoden samalla mukanaan uusia tekotapoja ja rikosilmiöitä. Kansainvälisyydestä johtuen Suomessa asuvien ulkomaalaistaustaisten rikollisten kontakteja voidaan hyödyntää rikoksenteossa ja yhtä lailla ääriliikkeiden ja terroristisen toimijoiden on halutessaan mahdollista hyödyntää olemassa olevia järjestäytyneen rikollisuuden rakenteita. Järjestäytyneen rikollisuuden kasvaessa ja laajentuessa, puutteellinen tietoisuus järjestäytyneen rikollisuuden toimintatavoista ja vaikutuksista jättää helposti tilaa toimia ja integroitua yhteiskuntaan sekä talouselämään. Järjestäytyneen rikollisuuden toimijat ja toimintatavat tulisikin tunnistaa ja sen myötä ylläpitää ajantasaista tilannekuvaa, niin eri viranomaisten kuin

yksityisen ja kolmannen sektorin toimijoiden kesken. Järjestäytyneen ja vakavan rikollisuuden torjuntaa voidaan toteuttaa tehokkaasti ainoastaan tiiviillä moniviranomaisyhteistyöllä sekä yhdessä yksityisen sektorin kanssa, ennalta estävää toimintaa kehittämällä ja korostamalla. (Poliisihallitus 2019, 5.)

Järjestäytyneen rikollisuuden hakeutuminen elinkeinoelämän ja yritystoiminnan pariin houkuttaa, sillä niiden rakenteita on mahdollista käyttää monenlaisiin rikollisiin tarkoituksiin, jolloin laillisen ja laittoman talouden erottaminen toisistaan vaikeutuu. Laittoman talouden rikollisuus toimiikin kysynnän ja tarjonnan ehdoilla sekä hyödyntää tehokkaasti toimintaympäristössä tarjoutuvia mahdollisuuksia. Samaan aikaan liiketoimintaa tehdään kuitenkin myös laillisen talouden puolella, mikä auttaa rikollista toimintaa sekoittumaan osaksi laillista talousjärjestelmää ja vaihdantaa. Yritystoiminnassa järjestäytynyt rikollisuus hyödyntää laittomia menettelyjä kilpailuasemansa parantamiseksi ja esimerkiksi harmaan talouden yrittäjät menestyvät tarjouskilpailuissa tarjoamalla näennäisesti edullisia urakointeja pitämällä kustannukset alhaisina, jättämällä yhteiskunnalliset velvoitteet hoitamatta sekä hyödyntämällä laittomasti hankittua materiaalia. (Poliisihallitus 2019, 5-6.)

Tullin tekemät havainnot osaltaan vahvistavat vakavan ja ammattimaisen rikollisuuden toimintatapojen monipuolistumista ja näyttäytymistä muun muassa elinkeinoelämän toimijoiden tuottamien palveluiden lisääntyneenä käyttönä rikollisissa tarkoituksissa. Ammattimaisessa rikollisuudessa laillisten tavaravirtojen volyymia pyritään käyttämään laittoman toiminnan peittämiseen sekä saamaan ulkopuoliset laillisten palveluiden tuottajat suorittamaan joitain rikoskokonaisuuden osatekoja heidän puolestaan. Käytännössä tämä voi tarkoittaa logistiikkaan erikoistuneiden yritysten suorittamia kuljetuksia toimeksiannossa ilmoitetuille vastaanottajille, tietämättä tai tuntematta kuitenkaan usein lähetysten todellista sisältöä tai asiakkaan toiminnan luonnetta. Tästä syystä viranomaisten ohella myös yksityisen sektorin toimijoita olisi erityisen tärkeää saada sitoutettua järjestäytyneen rikollisuuden torjuntaan. (Poliisihallitus 2019, 27.)

Järjestäytyneen rikollisuuden roolin vahvistuminen yritystoiminnassa ja varsinkin talousrikollisuudessa mahdollistaa rikollisjärjestöille tehokkaan tavan tukea rikollista toimintaa sekä hankkia haluamaansa vaikutusvaltaa. Liiketoimintaan pyritään mukaan etenkin sellaisilla sektoreilla ja toimialoilla, joilla toimimisesta on hyötyä rikosten tekemisen ja sitä varmistavan kontrollin kannalta. Järjestäytynyttä rikollisuutta esiintyykin erityisesti rakennusalan aliurakoinneissa, jonka lisäksi erityisen kiinnostavia ovat tietyt elinkeinoelämän alat, kuten turvallisuusalan liiketoiminta ja järjestyksenvalvontapalvelut, hotelli- ja ravintola-ala, siivous- ja kuljetusala, ajoneuvokauppa ja kuljetustoiminta sekä tieto- ja logistiikkaturvallisuus. Europolin arvioiden mukaan järjestäytynyt rikollisuus tuleekin tulevaisuudessa suuntautumaan yhä laajemmin palvelutuotannon pariin. (Poliisihallitus 2019, 6 & 21 & 29.)

Tieto- ja viestintäteknologian alueella järjestäytyneen rikollisuuden uhkat kohdistuvat yhteiskunnan kriittisiin järjestelmiin, jonka lisäksi ajankohtainen uhka yritystoiminnassa on erityisesti investointitoimintaan ja maksuliikenteeseen kohdistuvat petokset. Digitalisoituneessa ja verkottuneessa yhteiskunnassa tuleekin kiinnittää aiempaa suurempaa huomiota sekä henkilökohtaiseen että organisaatiokohtaiseen tietoturvallisuuteen, kuten myös yhteiskunnan elintärkeiden toimintojen suojaamiseen verkon kautta tai verkkoa hyödyntämällä tehtyjä hyökkäyksiä vastaan. Yrityksiin ja kansalaisiin kohdistetaan verkon kautta yhä enemmän huolellisesti valmisteltuja suuren vahinkoriskin aiheuttavia rikoksia sekä myös lukuisista pienistä yksittäisistä huijauksista koostuvia, sarjamaisia ja usein kansainvälisesti toteutettuja rikoksia. Suurin osa kontakteista, rikollisessa toiminnassa tarvittaviin ja hyväksikäytön kohteena oleviin ihmisiin luodaan nimenomaan tieto- ja viestintävälineillä. Toimintaympäristön muuttuminen ja tietoverkoissa tapahtuvan toiminnan kasvu edellyttääkin aivan uudenlaista ajattelua ja uusia toimintamalleja sekä viranomaisilta että yksityisiltä toimijoilta. Tietoverkottuneessa ympäristössä viranomaistoiminta ja lainvalvonta perustuu yhä enemmän yhteistyöhön ja tiedon jakamiseen muiden sektorien, etenkin paikallishallinnon sekä yksityisen sektorin kanssa. (Poliisihallitus 2019, 5 & 23-24.)

Järjestäytyneen rikollisuuden ollessa liiketoiminnan tavoin dynaamista ja sopeutuvaa, toimii se yhä useammin löyhinä, vaikeasti hahmotettavina ja joustavina verkostoina. Rikollisuudessa tapahtuu erikoistumista ja rikoksia voidaan toteuttaa keikkatyöläisen tavoin tilauksesta. Etninen monimuotoisuus järjestäytyneessä rikollisuudessa on lisääntynyt, jonka lisäksi perinteisten näkyvien, niin sanottujen tunnuksellisten rikollisjengien ohella rikollisuudessa esiintyy tietoverkkokontakteihin perustuvia, erikoistuneiden tekijöiden muodostamia verkostomaisia rakenteita. Tyypillistä on, että rikollisia hankkeita toteutetaan usein pieninä osatekoina tai erilaisista tekovaiheista koostuvina sarjoina laajoilla alueilla, jolloin toiminnan suunnitelmallinen kokonaisuus jää hankalasti hahmotettavaksi. Ihmisten hyväksikäyttöä harjoittava rikollisuus sekä väkivaltaiset yksittäiset toimijat ja tekijäryhmät pystyvät organisoitumaan ja aktivoitumaan verkkokontaktien avulla yhä tehokkaammin. Tietoverkkojen yhteydenpitomahdollisuuksien sekä helpon liikkuvuuden myötä myös kriisialueilla toimivien terroristien ja ääriliikkeiden aiheuttama väkivallan uhka muodostuu entistä konkreettisemmaksi. Tähän kytkeytyy ääriliikkeiden ja terrorismin yhteydet järjestäytyneeseen rikollisuuteen, sillä molemmat hyödyntävät toiminnassaan samantyyppisiä toimintatapoja ja rikollinen toiminta onkin varteenotettava keino ääriainesten toiminnan rahoittamiseen. (Poliisihallitus 2019, 17-19.)

Terroristit ja ekstremistisiä rikoksia toteuttavat ryhmät ovat kehittyneet merkittävästi viime vuosikymmenen aikana ja EU on ollut toistuvien terrori-iskujen kohteena näinä vuosina. Terrorismin ja järjestäytyneen rikollisuuden yhteydestä kertoo se, että tehtyjen terroristi-iskujen tutkimuksissa on paljastunut joidenkin tekijöiden osallistuneen vakavaan ja järjestäytyneeseen rikollisuuteen sekä erityyppisiin rikoksiin, kuten huumausaineiden salakuljetukseen. Tämän li-

säksi on ilmennyt henkilökohtaisia kontakteja rikollisryhmiin, jotka toimivat laittomien ampuma-aseiden kaupassa sekä tuottavat väärennettyjä asiakirjoja. Tutkimuksissa on myös paljastanut, että olemassa olevia maahanmuuttajien salakuljetusverkostoja on käytetty terroristisen toimijoiden tuomiseksi EU:n alueelle. Rikollisen toiminnan harjoittaminen terroristisen toiminnan tukemiseksi ei sinällään ole ilmiönä uusi ja henkilöt, joilla on mittava rikollinen tausta, pääsy järjestäytyneen rikollisuuden verkostoihin sekä mahdollisuus saatavilla olevien resurssien ja välineiden hyödyntämiseen, ovat merkittävä uhka, kun huomioidaan mahdollisuus nopeaan radikalisoitumiseen sekä halukkuus terrori-iskujen toteuttamiseen jo hyvinkin nopeasti radikalisoitumisen tapahduttua. Vakavan ja järjestäytyneen rikollisuuden sekä terrorismin välisten yhteyksien aiheuttamaa uhkaa voidaan pitää kaksijakoisena. Järjestäytyneen rikollisuuden rakenteita on mahdollista hyödyntää tarvittavien välineiden, kuten ampuma-aseiden tai väärennettyjen asiakirjojen hankkimiseksi ja niiden siirtämiseksi tai iskuissa käytettävä välineistö voidaan tilauksesta toimittaa suoraan terroristiryhmille. Toisaalta, osallistuminen vakavaan ja järjestäytyneeseen rikollisuuteen voi antaa terroristisille toimijoille mahdollisuuden varojen keräämiseen terrorismin rahoittamiseksi. Terroristiset toimijat ovatkin osallisena useilla rikollisuuden alueilla, kuten rahanpesussa, maahanmuuttajien salakuljetuksessa, heroiinin ja ampuma-aseiden kaupassa, järjestäytyneessä omaisuusrikollisuudessa sekä ihmiskaupassa. Nämä henkilöt toimivat kuitenkin tyypillisesti järjestäytyneen rikollisuuden matalalla tasolla, eikä heillä ole merkittäviä rooleja järjestäytyneen rikollisuuden verkostoissa. (Europol 2017, 55.)

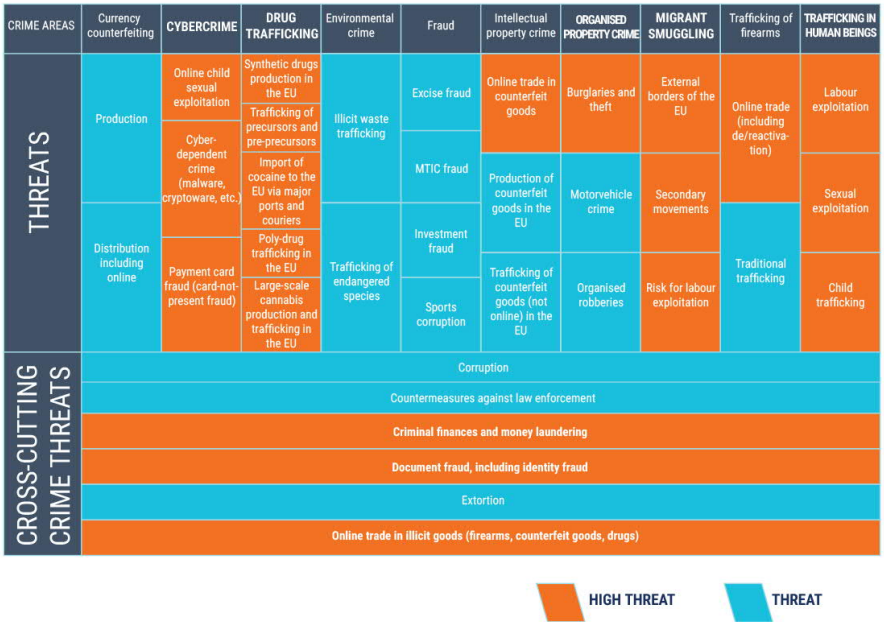
Poliisihallituksen (2019, 20-22) näkemyksen mukaan Schengen-alueen ja vapaan liikkuvuuden laajentuessa, myös Suomesta on tullut olennainen osa EU-maissa vaikuttavaa, rajat ylittävän järjestäytyneen rikollisuuden toimintaympäristöä, mikä tarkoittaa muualla Euroopassa havaittavien rikollisuuden ilmiöiden saapumista Suomeen entistä todennäköisemmin ja nopeammin. Arvioiden mukaan lähitulevaisuuden vakavan ja järjestäytyneen rikollisuuden keskeisimmät uhkatekijät tulevat liittymään rikollisuuden organisoitumiseen, jengiytymiseen sekä siitä koituvaan väkivaltaan, helppoon ja nopeaan rajat ylittävään liikkumiseen sekä tietoverkossa tapahtuvan rikollisen toiminnan maailmanlaajuiseen hyödyntämiseen.

Europolin tekemässä tulevaisuusennusteessa tunnuksellisten rikollismuodostelmien määrän nähdään entisestään kasvavan ja samalla niiden toimintarakenteet uudistuvat. Lisääntyvän jengiytymisen myötä uhkailu, kiristys ja väkivalta tulee yleistymään. Yritystoiminnan rooli rikoksenteossa vahvistuu ja laillisen liiketoiminnan rakenteisiin tulee lähitulevaisuudessa liittymään ennennäkemätön määrä rikollisuutta. Etnisyyden monimuotoistuminen rikollisuudessa ja etenkin väkivaltaan kouliutuneiden sekä konfliktialueilla toimineiden henkilöiden osallistuminen järjestäytyneen rikollisuuden toimintaan, voi johtaa entistä väkivaltaisempien toimintamuotojen voimistumiseen. Monien rikollisryhmien ja -verkostojen toiminta ulottuu useisiin eri maihin, jolloin tämänkaltaiset rikollisverkostot pystyvät helposti laajentumaan muun muassa diasporayhteisöjen jäseniin tukeutuen. Järjestäytyneen rikollisuuden tärkeimpiä ominaisuuksia onkin

sen kyky rajat ylittäviin toimintatapoihin sekä tekojen koostuminen suurestakin määrästä paikallisesti toteutettuja osatekoja tai vaiheita, millä suojataan rikollisorganisaatiota ja sen johtoa paljastumiselta. Tästä syystä, ammattimaisen, järjestäytyneen ja vakavan rikollisuuden torjuntaan liittyvän yhteistyön on oltava tehokasta ja saumatonta kaikilla eri viranomaistoiminnan tasoilla ja sektoreilla sekä yhdessä yksityisen sektorin toimijoiden kanssa. (Poliisihallitus 2019, 22-24.)

Kansainvälisen ja erityisesti vakavan ja järjestäytyneen rikollisuuden eri muotojen tunnistamisen, ehkäisemisen ja torjumisen kannalta oleellista onkin tiedon ja parhaiden käytäntöjen jakaminen sekä osallistuminen rikostorjuntaan kansainvälisesti. Yhtä lailla, kansainvälisen turvallisuustilanteen, epävakauden ja erilaisten konfliktien heijastevaikutuksena aiheutuva kansainvälinen terrorismi edellyttää kansainvälistä yhteistyötä, terrorismin muodostaessa uhan kansalliselle turvallisuudelle. (Valtioneuvosto 2020, 34.)

Europol toteaa vakavan ja järjestäytyneen rikollisuuden olevan keskeinen uhka EU:n turvallisuudelle, johtuen sen kyvykkyydestä sopeutua yhteiskunnan muutoksiin ja teknologisen kehityksen ollessa yksi avaintekijä rikollisen toiminnan kehittymisessä. Kuviossa 6 esitettyjä tulevien vuosien erityisiä sekä ensisijaisia rikollisuuden uhkatekijöitä tulevat olemaan verkkorikollisuus, huumeiden valmistaminen, salakuljetus ja jakelu, maahanmuuttajien salakuljetus, järjestäytynyt omaisuusrikollisuus sekä ihmiskauppa. Näiden lisäksi rikollisen toiminnan läpileikkaavina uhkina nähdään talousrikollisuus ja rahanpesu, asiakirjapetokset sekä laittomien tavaroiden ja palveluiden verkkokauppa. Rikollisuuden ensisijaiset uhkatekijät havainnollistettuna kuviossa 6. (Europol 2017, 56-57.)



Kuvio 6: tulevaisuuden erityiset ja läpileikkaavat rikollisuuden uhkatekijät

4.6 Hybridivaikuttaminen turvallisuusympäristön uhkailmiönä

Hybridivaikuttaminen on vaikeasti hahmotettava ja ennakoitava uhkatekijä, jonka merkitys tämän hetkisessä turvallisuusympäristössä ja kansallisessa riskien arvioinnissa on huomattava. Hybridivaikuttamisella tarkoitetaan turvallisuusympäristöön liittyviä muutosilmiöitä, joissa turvallisuusuhkien ennakkovaroitusaika on lyhentynyt, mikä puolestaan asettaa haasteita päätöksenteolle, viranomaisten toimintavalmiudelle sekä viranomaisyhteistyön sujuvuudelle. (Sisäministeriö 2018, 14 & 16.)

Viimeisimmässä Ulko- ja turvallisuuspoliittisessa selonteossa todetaan, että hybridivaikuttamisen lisääntyessä ja monimuotoistuessa, on siitä samalla tullut aiempaa suurempi turvallisuusuhka. ”Hybridivaikuttamisessa valtiollinen tai muu ulkoinen toimija pyrkii vaikuttamaan samanaikaisesti tai jatkumona, suunnitelmallisesti ja eri keinoja käyttäen kohteen haavoittuvuuksiin omien tavoitteidensa saavuttamiseksi. Keinovalikoima on laaja, ja siihen kuuluu muun muassa poliittisia, diplomaattisia, taloudellisia ja sotilaallisia keinoja sekä informaatio- ja kybervaikuttamista. Vaikuttaminen on vahingollista ja sitä pyritään tekemään niin, että se on kiistettävissä. Valtiotoimijat käyttävät usein hybridivaikuttamisessa kolmansia toimijoita, kuten ekstremistisiä ja järjestäytyneen rikollisuuden ryhmiä. Hybridivaikuttamiseen voidaan käyttää myös muuttoliikettä, pakolaisia tai hybridivaikuttamista toteuttavien maiden kansalaisia muissa maissa. Vaikuttamista voi tapahtua myös epidemioiden ja pandemioiden varjolla.” Vaalivaikuttaminen ja demokraattisten rakenteiden horjuttaminen muodostavat yhä suuremman hybridiuhan, johon teknologinen kehitys ja muuttunut toimintaympäristö, kuten sosiaalisen median erilaiset alustat, tarjoavat uudenlaisia vaikuttamismahdollisuuksia. Tarkoitushakuinen yhteiskunnallisen keskustelun sekä poliittisesti motivoitunut historian uudelleentulkinta näyttäytyvät tyypillisenä toimintana disinformaatio- ja vaikuttamiskampanjoissa, jonka ohella hybridivaikuttamisen kohteeksi valikoituu myös kriittinen infrastruktuuri. (Valtioneuvosto 2020, 14-15.)

Hybridivaikuttamisessa, yksittäisiä tai useampia keinoja käyttämällä on mahdollista aiheuttaa häiriötila tai jopa vakava häiriötila, jolla heikennetään vaikuttamisen kohteena olevan toimintakykyä. Turvallisuuskomitean (2017, 18) mukaan ”hybridivaikuttaminen voi näyttäytyä vain yhden komponentin tai muutaman komponentin yhdistelmän matalamman intensiteetin toimina, joissa hyökkääjän olemassaolo pyritään joko kokonaan salaamaan tai ainakin kiistämään”. Hybridivaikuttamisessa tavanomaisia ja epätavanomaisia keinoja voidaan yhdistellä ja soveltaa joustavasti tilanteen mukaan. Hybriditoiminta näyttäytyy erilaisina vaikuttamisyrityksinä yhteiskunnan poliittiseen, taloudelliseen, sotilaalliseen, informatiiviseen ja infrastruktuurin rakenteisiin. Hybridivaikuttamisen tavoitteena on saada aikaan tehokas vaikutus fyysisessä ympäristössä sekä erityisesti vastustajan mielessä. Vastustajan käyttäytymistä ohjaillaan haluttuun suuntaan ja osin jopa keinoilla, joita tämä ei edes havaitse. Hybridiuhat ovat monimutkaisia ja haastavia asioita käsiteltäväksi, sillä ne haastavat vakiintuneet käytännöt erilaisten tilanteiden hallinnassa. Pelkästään turvallisuusviranomaisten toiminta sellaisenaan ei yksistään

riitä yhteiskunnan puolustamiseen. Hybridivaikuttamisessa hyökkääjä voi iskeä yllättävästi ja samanaikaisesti useita tai jopa kaikkia yhteiskunnan elintärkeitä toimintoja vastaan sekä säädellä kunkin osa-alueen painetta haluamallaan tavalla. (Turvallisuuskomitea 2016, 3.)

Hybridivaikuttamisen keinovalikoima ollessa laaja ja monimuotoinen, joista yksi sen tehokkaimmista työkaluista on kyber ja kyberympäristössä tapahtuva toiminta, mitä helpottaa jatkuvasti voimistuva digitaalinen kehitys. Käytettävyydellään nämä asettavat toiminnan kohteena olevalle merkittäviä haasteita. Teknologia ja digitaalinen kehitys helpottavat elämäämme monin tavoin, mutta asettavat samalla yhä useammat palvelut aiempaa riippuvaisemmiksi viestintäpalveluiden ja -verkkojen sekä radiotaajuuksien ja tietojärjestelmien häiriöttömästä toiminnasta. Kuten jo aiemmin mainittiin, useat yhteiskunnalliset toiminnot ja keskeiset palvelut sekä erilaiset esineet, laitteet ja julkiset liikennemuodot ovat sidoksissa digitaalisiin järjestelmiin sekä internetiin ja niiden toimintaa ohjataan digitaalista tietoa käsittelemällä. Tieto- ja viestintäverkkoihin kohdistuvat häiriöt vaikuttaisivatkin näihin toimintoihin ja niiden ylläpitämiseen hyvinkin keskeisesti. (Sisäministeriö 2018, 17-18.)

Kyberin ja digitalisaation kytkeytyessä pian kaikkeen, muodostuu se hybridivaikuttamisessa enemmänkin toiminnan välineeksi, kuin varsinaiseksi toiminnan päämääräksi. Esineiden internetin (Internet of Things) jatkuvasti kasvaessa, asettaa se uusia haavoittuvuuksia niin yrityksille kuin yksittäisille kansalaisille, jolloin mahdollinen kyberhyökkäys voisi levitä ja eskaloitua huomattavasti laajemmalle, kuin alun perin ajatellaan tai ennakoidaan. Erilaisten pienimuotoisten toimintahäiriöiden ollessa lähes arkipäiväisiä, tarkoituksellinen hybridivaikuttamiseen kytkeytyvä kyberhyökkäys voitaisiin helposti suunnitella ja käynnistää salassa, mikä mahdollistaisi erilaisiin järjestelmiin tunkeutumisen pidemmällä aikavälillä, jolloin varsinainen hyökkäys voitaisiin käynnistää yhdenaikaisesti. Tarvittaessa, kybertoiminnan ja sen vaikutusten ohella, hyökkäykseen on mahdollista liittää myös fyysistä tuhoamista, murtamalla esimerkiksi olemassa olevat varmennukset. (Turvallisuuskomitea 2017, 21.) Tällä viitataan aiemmin mainittuun fyysisen ja digitaalisen ympäristön rajapinnan hämärtymiseen sekä niiden keskinäiseen sulautumiseen.

Hybridivaikuttamisen yhtenä muotona voi olla haitanteko ja vaikuttaminen sen avulla. Koska tulevaisuudessa tämän kaltaista haitantekoa tullaan kohdistamaan enenevissä määrin teknologiaan, kasvattaa se tietoturvan merkitystä entisestään. Yhteiskunnan elintärkeät toiminnot tulevat olemaan yhä riippuvaisempia esineiden internetistä, jossa älykkäät esineet ja laitteet keräävät ja välittävät tietoa sekä kommunikoivat ympäristön kanssa internet-verkon välityksellä. Siinä missä IoT tulee avaamaan yhteiskunnallemme paljon mahdollisuuksia, altistaa se samalla elintärkeitä järjestelmiämme uudenlaisille uhkille. Tiedon suojaamisen merkitys tulee korostumaan entisestään interaktiivisten laitteiden määrän lisääntyessä niin teollisuudessa kuin yksityiskäytössäkin, sillä verkkoon kytkettäviin laitteisiin hakkeroituminen sekä niiden käyttäminen muun toiminnan alustoina tai välityspalveluina on osa arkipäivää jo nyt. (Turvallisuuskomitea 2016, 18)

Hybridivaikuttamisessa, kybertoiminnan ohella, toinen keskeinen työkalu on informaatiovaikuttaminen ja usein näitä kahta jopa pidetäänkin lähes synonyymeina toisilleen. Yhteneväistä molemmille on toiminnan hienovaraisuus ja pitkäkestoisuus, millä saadaan häivytettyä tietoisuus ja ymmärrys vaikuttamisen kohteena olemisesta. Kybertoimintaa käyttämällä on mahdollista avata väyliä informaatiovaikuttamiselle tai jopa informaatiosodankäynnille, toteuttamalla tietomurtoja ja murtautumalla verkkosivustoille sekä estämällä niiden käyttö. Tällaisessa hyökkäyksessä saattaa joissain tilanteissa olla mahdollista hyödyntää myös sisäpiiriläistä, joka tahallisesti toteuttaa hyökkäyksen tietoteknisten muurien sisäpuolelta. (Turvallisuuskomitea 2017, 21-22.)

Hybridivaikuttamisessa varsinaista informaatiovaikuttamista voidaan joskus käyttää hyvinkin avoimesti ja suoraviivaisesti, sitä suuremmin peittelemättä. Tietylle vastaanottajajoukolle suunnattu, kohdistettu ja systemaattisesti toteutettu virheellisen informaation syöttäminen voi olla yksi näkyvimmistä hybridivaikuttamisen keinoista. Tällöin toiminta on osittain jopa erittäin räikeää, niin ettei suoranaista valehtelua edes koiteta vältellä. Sosiaalinen media tarjoaa tällaiselle suoralle vaikuttamiselle erityisen hyvän paikan ja mahdollisuuden yksipuolisen tai vääristellyn tiedon levittämiseen globaalisti. Joissakin valtioissa myös valtamedioiden uutistuotanto voi olla tiukasti kontrolloitua, jolloin nekin saadaan toistamaan haluttua sanomaa. (Turvallisuuskomitea 2016, 4.)

Rinnakkainen muoto hybridivaikuttamiselle on hybridisodankäynti. Hybridivaikuttamisessa ja erityisesti hybridisodankäynnissä toiminnan keskeiseksi kohteeksi valikoituu helposti yhteiskunnan kriittinen infrastruktuuri ja elintärkeät toiminnot, kuten energian saantiin liittyvät toiminnot, joiden toimivuudella on suora vaikutus sekä talouteen että kansalaisiin. Suomen pitkä talvi, pitkät keskitetyt energiasiirtoyhteydet, korkea sähköriippuvuus, kasvava tietoliikenneriippuvuus sekä pitkät logistiset reitit antavat hybriditoiminnassa mahdollisuuden esimerkiksi alueiden eristämiseen tai laajojen kumuloituvien ongelmien aiheuttamiseen. (Turvallisuuskomitea 2017, 20.)

Hybridivaikuttamisen muuttuessa hybridisodankäynniksi, ollaan tilanteessa, jossa perinteisen sodankäynnin kohteet ovat lähinnä sotilaallisia ja välineet sen mukaisia, mutta hybridisodankäynnissä kohteeksi voi valikoitua siviilikohteita kuten sähkönjakelua, vesilaitoksia tai tietoliikenneyhteyksien kaltaisia kriittisen infrastruktuurin rakenteita. Yhdistämällä näitä kohteita samanaikaiseen kyberhyökkäykseen, puolustaja voidaan pakottaa heikommin suojattujen varajärjestelmien käyttöön tai ylittää sellainen rajapinta, jota kyberin avulla ei kenties muutoin kyettäisi toteuttamaan. (Turvallisuuskomitea 2017, 26.)

Tietoverkoissa ja mediassa tapahtuvan kybertoiminnan ja informaatiovaikuttamisen lisäksi, yksi hybridisodankäynnin käytännönläheisempi muoto voisi olla tunnuksettomien erikoisjoukkojen käyttäminen. Toiminnan ollessa kuitenkin melko näkyvää, kynnys tämän kaltaiseen toimintaan

on hyvin korkealla. Toisaalta, mikäli toimintaa halutaan peitellä, tämän kaltaisia ”palveluita” on ostettavissa rikollisilta tai terroristeilta, minkä avulla toiminnan todellinen toteuttaja ja ”tilaaja” saadaan helpommin häivytettyä. (Turvallisuuskomitea 2017, 26).

Hybridisodankäynnissä hyökkäystoiminta voidaan jakaa kolmeen eri vaiheeseen: 1) poliittiseen päätökseen ja tavoitteenasetteluun, 2) puolustajan haavoittuvuuksien ja niihin kytkettävien mahdollisimman hyvin valmisteltujen keinojen valintaan sekä 3) toteuttavien operaatioiden suunnitteluun ja resursointiin läpi hallinnonalojen. Hyvillä ja kattavilla ennalta tehdyillä valmisteluilla saavutetaan tilanne, jossa hyökkääjällä on aina useita merkittäviä etuja puolustautujaan nähden. (Turvallisuuskomitea 2017, 27).

Hybridisodankäynnin hyökkäysvalmistelut aloitetaan tunnistamalla kohteen haavoittuvuudet, mikä saattaa kestää useita vuosia tai jopa vuosikymmeniä. Tätä varten suoritettavia testauksia tai pitempiaikaisen operaation vaiheita voidaan kutsua esimerkiksi informaatio-, talous- tai kybervaikuttamiseksi. Tiedon keräämisessä hyödynnetään tarvittaessa myös mahdollisia vahinkoja ja onnettomuuksia tai jonkun muun tekoja, sillä tärkeintä on tunnistaa tapahtuman vaikutusmekanismi sekä siitä aiheutuva ”tulos” ja sen vaikutus yhteiskuntaan. Tämän pohjalta voidaan valmistella vastaavan tapahtuman tuottaminen tarkoituksellisesti tai mahdollinen seuraavan vastaavan tilanteen hyväksikäyttö. Hybridisodankäynnissä käytettävien aseiden ”valmistaminen” on loppujen lopuksi melko arkinen prosessi ja sopivia keinoja voidaankin tavallaan kerätä varastoon aiheuttamalla niitä joko itse tai käyttämällä muutoin ilmi tulleita puolustajan haavoittuvuuksia hyväksi. Kaivinkoneen katkaistessa esimerkiksi jonkin keskeisen datakaapelin, ilman että koko kaapelia siirretään, kriittinen piste on tämän jälkeen tiedossa. (Turvallisuuskomitea 2017, 28).

Suunnittelu- ja kartoitusvaiheen päätyttyä varsinainen hyökkäys käynnistetään päätöksellä ja tavoitteen asettamisella. Puolustautuja pystytään yllättämään sitä paremmin, mitä keskitetympi vallankäyttö hyökkääjällä on ja mitä paremmin hyökkäys kyetään näin ollen salaamaan. Kuten todettua, hybridivaikuttamisen tasolla salaaminen voi olla mahdollista pidemmänkin aikaa, koska lähes kaikki toimintaan kytkeytyvät komponentit voidaan piilottaa, ostamalla haluttu palvelu esimerkiksi rikollisilta, suuntaamalla huomio toisiin tai yksinkertaisesti kieltämällä asia pitävien todisteiden puuttuessa. Hybridivaikuttamisessa hyökkäys voidaan aina valmistella, harjoitella ja jopa käynnistää salassa, kun taas hybridisodankäyntiä ei sen intensiteetin takia voida salata. Siltikin siinä voidaan hyödyntää toiminnan erilaista kirjoa laajasti, kuten harhauttamista, kiistämistä, intensiteetin vaihtelua tai käyttämällä yllättäviä käänteitä hyväksi. Valittaessa toiminnan kohteita laajemmin, tapahtuu se operaatiosuunnitelmaan sitoutuen aivan kuten missä tahansa muussakin sodankäynnissä. Keinoja yhdistelemällä, hyökkäyksiä eri tavoin aikauttamalla sekä vaikutuksia synkronoimalla, voidaan helposti moninkertaistaa yksittäisten tekojen yhteisvaikutusta. Kohteena voi olla esimerkiksi jokin tietty alue, elinkeinon ala tai jokin yhteiskunnan kriittisen toiminnan osa. (Turvallisuuskomitea 2017, 28-29).

Hybriditoiminnassa tärkeintä on tiedostaa, että hybridivaikuttamisessa ja varsinkaan hybridisodankäynnissä kyseessä ei ole joukko sattumuksia, vaikka ne sellaisilta voivatkin vaikuttaa tai hyökkääjä ne sellaisina pyrkii esittämään. Hybridivaikuttamisen tai -sodankäynnin seurauksena kriisiytyneessä yhteiskunnassa tapahtuu myös helposti erilaista resonointia ja vahinkojakin, jotka hyökkääjä voi halutessaan kytkeä osaksi omaa suunnitelmaansa. (Turvallisuuskomitea 2017, 27).

Limnéll & Iloniemi (2018, 67) toteavat, että nykyisessä turvallisuusympäristössä ja tämän hetken uhka-arvioissa hybridiuhkat näyttäytyvät vahvoina, jossa uhka muodostuu niin sotilaallisten kuin ei-sotilaallisten uhkien yhteisvaikutuksena, ja jossa toiminta tarkoituksellisesti tapahtuu julistettavan sodan kynnyksen alapuolella.

Hybridivaikuttamisen ja hybridisodankäynnin torjunnassa ongelmallista on, että vaikka puolustautujalla olisikin hyvä valmius torjua yksittäisiä komponentteja, nykyisen toimintaympäristön myötä uutta ja haasteellista on niiden yhteisvaikutus. Hybridivaikuttamisen torjuntaan tulisi kyetä riittävän laajalla resurssikirjolla sekä jo ilmentyneitä kuin aivan uusiakin uhkakomponentteja vastaan, mutta ennen kaikkea näiden yllättäviä yhdistelmiä sekä kumuloituvaa yhteisvaikutusta vastaan. Käytännössä tämä tarkoittaa esimerkiksi sitä, että jos osaamme toipua myrskyn aiheuttamista sähkö-, tele- ja liikennekatkoksista, evakuoida kansalaisia tulvan oloissa ja pelastaa ihmisiä suuronnettomuuksissa, harjoittelemme siinä samalla hybridikomponenttien torjuntaa sekä lisäämme kansallista resilienssiä niin valtion, maakuntien ja kuntien kuin kansalaisten ja yritysten tasolla. Sellaisenaan se ei kuitenkaan vielä riitä, sillä arjessa mahdollisia yllättäviä eri komponenteista aiheutuvia yhteisvaikutuksia ei esiinny. (Turvallisuuskomitea 2017, 30.)

Hybridivaikuttamisen ja ennen kaikkea hybridisodankäynnin kohdalla, viranomaistoiminnan yhteistyön niin kenttätasolla kuin erityisesti johtamisessa, tulisi olla tiivistä, harjoiteltua ja usein toteutettua. Oleellista siinä on alueellinen koordinointi, jonka lisäksi tulisi pystyä kehittämään ja rakentamaan pysyviä yhteistoimintarakenteita sekä kykyä näiden ja yhtenäisten johtamisjärjestelmien muodostamiseen nopeassakin tilanteessa. Yhteistyörakenteiden tulisi ulottua aina valtiojohtoon saakka, kytkien mukaan kaikki oleelliset toimijat kokonaisturvallisuuden mallin mukaisesti. Varautumisen ja valmiuden keskeinen osa on johtaminen, sillä yhteiskunnan toimivuus kaikissa tilanteissa edellyttää eri toimijoissa ja eri tasoilla tapahtuvaa johtamista sekä siihen liittyvää yhteistoimintaa. Johtosuhteet, organisaatiot ja vastuunjako tulisikin säilyttää mahdollisimman muuttumattomina kaikissa tilanteissa. Yhteiskunnan johtamiseen ja siihen liittyvien yhteistoiminnan muotojen keskeisimpiä ja todennäköisimpiä uhkia ovat niihin kohdistuva painostus informaatiovaikuttamisen, keskeisten viestimien häiritsemisen sekä valtionhallintoon kohdistuvien kyberhyökkäysten keinoin. Kohteeksi voivat valikoitua jokapäiväiset ja toiminnan kannalta tärkeät johtamisessa käytettävät järjestelmät sekä tärkeän tiedon käsittelyyn liittyvät menettelytavat. (Turvallisuuskomitea 2017, 30-32)

Tästä voidaan päätellä, että huomioiden esimerkiksi viranomaisverkon (VIRVE) sekä muiden käytössä olevien tieto- ja johtamisjärjestelmien merkityksen viranomaisten operatiiviseen toimintaan, sen kaikilla tasoilla, verkon kaatuminen saattaisi merkitä huomattavia ongelmia poliisin operatiiviselle johtamiselle ja organisoinnille ja sen käytännön toteutukselle.

Limnéll & Iloniemi (2018, 108) huomauttavat, että yhteiskunnan tavoin hybridiuhkiin varautuminen koskettaa myös elinkeinoelämää ja yrityksiä. Viranomaisille kuuluneiden tehtävien ulkoistamisen, yhteiskunnan digitalisoitumisen sekä elinkeinoelämän ja viranomaisten välisen verkottumisen lisäksi, yritykset kantavat usein vastuun kriittisen infrastruktuurin toiminnasta niin normaali- kuin poikkeusoloissa. Yritys voi toimia varsinaisen hybridivaikuttamisen kohteena, mutta todennäköisempää on sen käyttämisen reittinä tai välikappaleena lopulliseen strategiseen tavoitteeseen pyrittäessä. Vaikka yritys tunnistaisikin itseensä kohdistuvan vain yhdenlaista vaikuttamista, se ei sulje pois mahdollisuutta, että yritys on osa laajempaa hybridivaikuttamisoperaatiota, jossa eri kohteisiin kohdistetaan eri vaikuttamisen keinoja.

Turvallisuuskomitean (2016, 8) julkaisemassa hybridiuhkia koskevassa katsauksessa todetaan, että varautumisessa ja ennakoinnissa tarvittavaa realistista tilannekuvaa muodostettaessa, yhteiskunnan vallitseva turvallisuusympäristö ja sen uhkat huomioiden, jatkossa on yhä enemmän varauduttava hybridivaikuttamiseen tai hybridisodankäyntiin, kyberuhkiin, strategisen kommunikaation tuomiin haasteisiin, perinteiseen sotilaalliseen uhkaan, taloudellisen keskinäisriippuvuuden tuomaan haavoittuvuuteen sekä ennen kaikkea yllätyksellisyyteen.

Hybriditoiminnan taustalla olevissa operaatioissa saattaa olla jokin strateginen tavoite, mihin voi liittyä niin sotilaallinen kuin yhtä lailla ei-sotilaallinen ulottuvuus. Kyberuhkien keskeisenä haasteena on teknologinen osaaminen sekä virtuaalimaailman luomat uudet ulottuvuudet konfliktitilanteessa. Haasteita strategiseen kommunikaatioon aiheuttavat niin hetkellinen disinformaatio, pitkäaikainen propaganda kuin operatiivinen strateginen harhautus, joiden käyttäminen vaikuttamisen välineenä voi vaihdella tilanteesta riippuen. (Turvallisuuskomitea 2016, 8.)

Suojelupoliisin arvioiden mukaan valtiollisten toimijoiden valmius voimakkaidenkin hybridivaikuttamisen keinojen käyttöön tulee pysymään korkeana ja Suomi säilymään aktiivisen hybridivaikuttamisen kohteena. Valtiollisella tasolla hybridivaikuttaminen ilmenee muun muassa sotilaallisen, poliittisen, taloudellisen sekä informaatio- ja kybersektorin toimintana. Kansainvälisesti hybridivaikuttamiselle on viime vuosina ollut ominaista keinovalikoiman monimuotoistuminen, mikä on näyttäytynyt esimerkiksi vaalihakkeroinnin tai mittavien, tilastollista analyysia hyödyntävien somekampanjoiden muodossa. Vastaavanlaisen toiminnan ja kehityksen odotetaan jatkuvan myös lähitulevaisuudessa ja valtiollisten toimijoiden valmius voimakkaidenkin hybridivaikuttamisen keinojen käyttöön omien tavoitteidensa edistämiseksi tulee säilymään korkeana. (Suojelupoliisi 2019, 3)

Yhteiskunnan turvallisuuteen ja hybriditoimintaan kytkeytyy myös Suomeen kohdistuva tiedustelutoiminta. Aktiivinen, vieraiden valtioiden Suomeen kohdistama tiedustelutoiminta tulee jatkumaan laajamittaisena ja Suomi kiinnostaa erityisesti Venäjän ja Kiinan tiedustelupalveluita. Suomessa on pysyvästi sijoitettuna useita kymmeniä ulkomaisten tiedustelupalveluiden työntekijöitä, jonka lisäksi vuosittain arviolta saman verran ulkovaltojen tiedusteluorganisaatioiden työntekijöitä käy lyhyillä operatiivisilla tehtävillä Suomessa. (Suojelupoliisi 2019, 2.)

Ulkomaisten tiedustelupalveluiden toimintaa Suomessa kuvastaa pitkäkestoisuus ja suunnitelmallisuus ja toiminnan keskeisimpiin päämääriin kuuluu Suomen harjoittaman politiikan eri osa-alueiden ennakoiminen sekä poliittiseen päätöksentekoon vaikuttaminen. Ulkomaisia tiedustelupalveluita kiinnostaa lisäksi suomalainen teknologia ja siihen liittyvä osaaminen. Pidemmän aikavälin kiinnostuksen kohteita ovat ulko- ja turvallisuuspoliittinen keskustelu, EU- ja Nato-suhteet, Suomen energiapolitiikka, arktinen ulottuvuus, Itämeren alueen turvallisuustilanne sekä yhteiskunnallinen talous- ja huoltovarmuustoiminta. Viime aikojen keskeisiä kiinnostuksen kohteita ovat olleet muun muassa Suomen toiminta EU:n puheenjohtajamaana, Suomen asema EU:n pakotepolitiikassa, kansallinen innovaatiotoiminta sekä korkean teknologian tuotteet. Kiinnostusta ilmenee myös Suomen uutta tiedustelulainsäädäntöä sekä kyberturvallisuusrakenteita ja informaatiovaikuttamiselta suojautumista kohtaan. Kiinnostus Suomen kriittistä infrastruktuuria sekä muille strategisille aloille suuntautuvia investointeja kohtaan on yhtä lailla lisääntynyt. Tämän lisäksi tietyt turvallisuus- ja tiedustelupalvelut pyrkivät kontrolloimaan sekä painostamaan Suomessa asuvia tai täällä muutoin oleskelevia nykyisiä tai entisiä kansalaisiaan. Toiminnan kohteeksi voi valikoitua myös Suomessa asuvia toisen maan kansalaisia tai kantaväestöön kuuluvia henkilöitä. (Suojelupoliisi 2019, 2.)

4.7 EU:n turvallisuusstrategia globaalissa turvallisuusympäristössä

Kansallisessa riskiarviossa esitettyjen uhkatekijöiden peilaamiseksi ja osaltaan niiden vahvistamiseksi myös globaalissa kontekstissa. Ulottamatta turvallisuusympäristön tarkastelua sen laajemmin Suomen rajojen ulkopuolelle, EU:n turvallisuusstrategia omalta osaltaan osoittaa turvallisuusympäristön muuttuneen ja siinä ilmenevien uhkien olevan globaaleja ja rajat ylittäviä. Samalla se vahvistaa Suomen kansallisessa riskiarviossa esitettyjä näkemyksiä yhteiskuntaan ja ihmisten turvallisuuteen kohdistuvista uhkista. EU:n laatimalla turvallisuusstrategialla saattaa lisäksi olla välillisiä tai välittömiä vaikutuksia Suomen sisäisen turvallisuuden kehittämiseen ja sitä kautta poliisitoimintaan. Tämän opinnäytetyön tarkoitus ja Poliisiammattikorkeakoulun osaamista ja oppimista kasvattava rooli huomioiden, kansainvälisyysosaaminen näyttäytyy pedagogisessa kehyksessä vahvana, mikä edellyttää turvallisuusympäristön tarkastelua hieman laajemmin.

Uusimmassa EU:n turvallisuusstrategiassa käsitellään globaalissa turvallisuusympäristössä esiintyviä uhkia ja turvallisuutta vaarantavia tekijöitä ja strategian avulla tuetaan EU:n jäsenmaiden

sisäisen turvallisuuden kehittämistä ja uhkien torjuntaa. Tehtyihin uhka-analyyseihin pohjautuvassa turvallisuusstrategiassa kuvataan vallitsevia globaaleja uhkia sekä niiden torjuntaan kohdennettavia toimenpiteitä. Näiden uhkien torjumiseksi ja EU:n yhteisen turvallisuuden kehittämiseksi on määritelty neljä strategista prioriteettia globaaleihin uhkiin ja haasteisiin vastaamiseksi sekä turvallisuutta edistävien toimenpiteiden kohdentamiseksi. Uhkien torjunnan ja turvallisuustoimien prioriteetteja ovat tulevaisuuden kestävä turvallisuusympäristö, kehittyvien uhkien torjunta, eurooppalaisten suojeleminen terrorismilta ja järjestäytyneeltä rikollisuudelta sekä vahva eurooppalainen turvallisuusekosysteemi, jotka kuvataan kuviossa 7. (European Commission 2020, 6.)

Kuvio 7: EU:n turvallisuusstrategia

Tulevaisuuden kestävä turvallisuusympäristö sisältää kolme erillistä alakohtaa: kriittisen infrastruktuurin turvaaminen ja resilienssi, kyberturvallisuus sekä julkisten tilojen turvaaminen. Kriittisen infrastruktuurin turvaamisella ja resilienssillä viitataan keskinäisriippuvuuden lisääntymiseen, jossa yhden sektorin häiriöillä voi olla välitön vaikutus myös muiden sektoreiden toimintaan. Hyökkäys sähköntuotantoon voisi kaataa tietoliikenteen, sairaalat, pankit tai lentokentät, kun taas digitaaliseen infrastruktuuriin kohdistuva hyökkäys voisi johtaa häiriöihin sähkö- tai rahoitusverkoissa. Koska taloutemme ja yhteiskuntamme liikkuu yhä enemmän verkossa, tämän kaltaiset riskit kasvavat jatkossa yhä enemmän. Yhteenliitettävyyden ja keski-

näisriippuvuuden lisääntyessä, kriittisen infrastruktuurin suojaamiseksi tulisi toteuttaa vankkoja suojaus- ja sietokykytoimintoja, niin kyberympäristöt kuin fyysiset ympäristöt huomioiden. Tärkeät palvelut on suojattava riittävän hyvin sekä nykyisiltä että ennakoiduilta uhkilta, mutta samalla niiden on oltava joustavia, mikä järjestelmien osalta tarkoittaa suunnitelmallista varautumista, sietokykyä sekä parempaa toipumista ja sopeutumista haitallisiin tapahtumiin. (European Commission 2020, 6.)

Kyberhyökkäysten määrä kasvaa entisestään, hyökkäysten ollessa kehittyneempiä kuin koskaan. Kyberhyökkäyksiä toteutetaan laajalti useista eri suunnista EU:n sisällä sekä sen ulkopuolella, niiden kohdistuessa mahdollisimman haavoittuville alueille. Hyökkäyksiä toteuttavat valtiot tai valtioiden tukemat toimijat ja hyökkäysten kohteiksi valikoituvat digitaalisen infrastruktuurin avainkohteet, kuten suuret pilvipalveluiden tarjoajat. Yhä vähemmän dataa varastoidaan varsinaisiin datakeskuksiin, sillä tiedon käsittely tapahtuu lähempänä käyttäjää niin sanotulla 'reunalla', joten kyberturvallisuus ei voi enää keskittyä pelkästään keskuspisteiden suojaamiseen. Tiedustelupalvelujen, EU INTCEN sekä muiden turvallisuuteen osallistuvien organisaatioiden välisten uusien sekä tehostettujen yhteistyömuotojen tutkimisen tulisikin olla osa kyberturvallisuuden kehittämistä ja terrorismin, ääriliikkeiden, radikalismin sekä hybridiuhkien torjunnan pyrkimyksiä. (European Commission 2020, 8.)

Viime vuosina tapahtuneet terrori-iskut ovat keskittyneet pitkälti julkisiin paikkoihin, mukaan lukien erilaiset uskonnolliset kohteet ja liikennekeskukset, koska niiden avoimuus ja pääsyn helppous on helposti hyödynnettävissä. Poliittisten tai ideologisesti motivoituneiden ääriliikkeiden aiheuttama terrorismin nousu on tehnyt uhasta entistäkin vakavamman, mikä edellyttää tällaisilta kohteilta vahvempaa fyysistä suojausta sekä riittäviä valvontajärjestelmiä, ihmisten vapauksia kuitenkaan vaarantamatta. Julkisten tilojen suojelemiseksi EU komissio kehottaakin lisäämään julkisen ja yksityisen sektorin yhteistyötä niiden toimintaa rahoittamalla, hyviä kokemuksia ja käytäntöjä vaihtamalla sekä tarkempia ohjeita antamalla ja tietoisuutta lisäämällä. Tämän lisäksi valvontalaitteiden suorituskykyvaatimusten kasvattaminen ja testaaminen sekä taustatarkastusten tehostaminen sisäpiiriuhkien torjumiseksi voisi olla yksi lähestymistapa asiaan. Dronejen markkinat kasvavat edelleen ja vaikka niillä onkin monia käytännöllisiä ja laillisia käyttötarkoituksia, rikolliset ja terroristit voivat kuitenkin halutessaan käyttää niitä väärin, jolloin julkiset paikat ovat erityisen uhattuina. Kohteina voivat olla yksilöt, ihmisten kokoontumiset, kriittinen infrastruktuuri, lainvalvontaviranomaiset, raja-alueet tai julkiset tilat. Tietämys dronejen käytöstä hyökkäystarkoituksessa voi kantautua Eurooppaan joko suoraan konfliktialueilta palaavien ulkomaisten terroristitaistelijoiden mukana tai verkon välityksellä. (European Commission 2020, 9-10.)

Strategian prioriteeteista toinen, kehittyvien uhkien torjunta, pitää sisällään verkkorikollisuuden, viranomaistoiminnan nykyaikaistamisen, laittoman verkkosisällön torjunnan sekä hybri-

diuhkien torjunnan. Teknologia tuo uusia mahdollisuuksia yhteiskunnalle, tarjoten samalla uusia työkaluja oikeuslaitokselle ja lainvalvontaviranomaisille, mutta avaten myös ovia rikollisille. Haittaohjelmat, henkilökohtaisten tai yritystietojen hakkerointi ja varastaminen sekä taloudellisten tai mainehaittojen aiheuttaminen digitaalinen verkko kaatamalla on kasvussa. Torjuntatoimista ensimmäinen on vahva, mutta joustava kyberturvallisuusympäristö. Toisekseen, lainvalvontaviranomaisten tulisi pystyä työskentelemään kattavammin digitaalisen tutkinnan alueella, mikä samalla vaatisi riittävän selkeää ohjeistusta rikosten tutkimiseksi ja syytteeseen asettamiseksi sekä tarpeellisen suojelun tarjoamiseksi uhreille. Verkkorikollisuus on maailmanlaajuinen haaste, jossa tarvitaan tehokasta kansainvälistä yhteistyötä. Verkkorikollisuuden torjuminen tarkoittaa eteenpäin katsomista, sillä kun yhteiskunta hyödyntää uutta teknologista kehitystä talouden ja yhteiskunnan vahvistamiseksi, samaan aikaan rikolliset voivat pyrkiä käyttämään näitä työkaluja negatiivisiin tarkoituksiin. Rikolliset voivat esimerkiksi hyödyntää tekoälyä salasanojen havaitsemiseen ja tunnistamiseen, haittaohjelmien luomisen yksinkertaistamiseen tai kuvien ja äänen tuottamiseen, joita voidaan sen jälkeen käyttää identiteettivarkauksissa tai petosrikoksissa. (European Commission 2020, 10-11.)

Teknologian ja digitalisaation ja samalla verkkorikollisuuden voimistuessa, viranomaistoiminnan nykyaikaistamisella tarkoitetaan lainvalvontaviranomaisten ja oikeusalan ammattilaisten sopeutumista uudenlaiseen tekniikkaan ja sen hyödyntämiseen. Teknologinen kehitys ja siihen liittyvät uhkat edellyttävät uusia työkaluja lainvalvontaviranomaisille, uusien taitojen hankkimista sekä vaihtoehtoisten tutkintatekniikoiden kehittämistä. Lainvalvontaviranomilla tulisi olla tarvittavat valmiudet rikostutkinnassa tarvittavien tietojen tunnistamiseen, suojaamiseen ja lukemiseen sekä näiden tietojen hyödyntämiseen todisteina. Tähän sisältyy myös laittoman verkkosisällön torjuminen. Verkossa ja fyysisessä ympäristössä tapahtuvien tekojen tuominen samalle tasolle tarkoittaa jatkuvia toimia laittoman verkkosisällön torjumiseksi. Yhä useammat kansalaisiin kohdistuvat keskeiset uhkat, kuten terrorismi, ääriliikkeiden toiminta tai lasten seksuaalinen hyväksikäyttö perustuu digitaaliseen ympäristön hyödyntämiseen, mikä edellyttää konkreettisia toimia perusoikeuksien kunnioittamisen varmistamiseksi. Ensimmäinen tärkeä askel on saada voimaan terroristista verkkomateriaalia koskeva lainsäädäntö ja sen toimeenpanon varmistaminen. Avainasemassa on myös lainvalvontaviranomaisten ja yksityisen sektorin vapaaehtoisen yhteistyön lujittaminen taistelussa terrorismia, väkivaltaisia ääriliikkeitä ja rikollista toimintaa vastaan. Europolin internetyksiköllä onkin jatkossakin ratkaiseva rooli terroristiryhmien, verkossa ja sen eri alustoilla tapahtuvan toiminnan seuraamisessa. Vihapuheen leviämistä verkossa tulisi estää, jonka ohella toimenpiteitä tulee kohdentaa lasten seksuaaliseen hyväksikäyttöön liittyvien haasteiden ratkaisemiseen verkkoympäristössä sekä pyrkiä maksimoimaan käytettävissä olevien välineiden hyödyntäminen näiden rikosten torjunnassa. (European Commission 2020, 11-13.)

EU:n turvallisuusstrategian ulkopuolelta mainittakoon, että Poliisiammattikorkeakoulun toimintaympäristö -julkaisussa käsitellään digitaalisen näytön hyödyntämistä rikostutkinnassa. Nykyisin digitaalista rikostutkintaa voidaan suorittaa monin eri tavoin, esimerkiksi palauttamalla hävitettyjä tietoja tai luomalla keinotekoista verkkoliikennettä, jossa hyökkäyksiä voidaan rakentaa uudelleen ja simuloida niitä. Tietoteknisen rikostutkinnan vakiotyökalupakki kattaakin kaikki verkkorikostutkintamenettelyn erilaiset näkökohdat ja välineet, joita poliisi voi käyttää digitaalisen todistusaineiston keräämiseen. Tietoteknisessä rikostutkinnassa tietokoneiden kovalevyjen sisältö pystytään kopioimaan niin, että sieltä voidaan palauttaa kovalevyltä poistettuja tiedostoja sekä tarkastella myös tiedostojen ja ohjelmistojen metadataa. Soveltuvia työkaluja löytyy lisäksi internetistä löytyvien (historia)tietojen kuten chattien, selaushistorian ja verkkosivuilta ladattujen sekä niiltä poistettujen tiedostojen tarkasteluun. Tietynlaisia työkaluja on käytettävissä myös muisti- ja SIM-kortteista sekä mobiili- ja GPS-laitteista saatavan tiedon kopiointiin ja tarkasteluun, joilla tarkastelun lisäksi voidaan muun muassa luokitella lapsipornografista aineistoa sekä suodattaa haettua ja tutkinnalle relevanttia materiaalia. Nopeat muutokset tieto- ja viestintätekniikan alueella aiheuttavat usein haasteita tietotekniselle rikostutkinnalle, mistä johtuen uusia työkalujen kehittäminen on jatkuvaa. Valtaisat tietomäärät, heterogeeniset tieto- ja viestintätekniikat sekä rajattomat kyberinfrastruktuurit luovatkin jatkuvasti uusia haasteita tietoverkkorikollisuutta tutkiville turvallisuusalan asiantuntijoille ja lainvalvontaviranomaisille. (Rajamäki 2018, 108.)

EU:n turvallisuusstrategian mukaan hybridiuhkien laajuus ja monimuotoisuus näyttäytyy tällä hetkellä ennennäkemättömänä. COVID-19-kriisin aikana on saatu lisää todisteita siitä, että useat valtiolliset sekä valtiosta riippumattomat toimijat pyrkivät käyttämään pandemiaa hybridivaikuttamisen ”välineenä”, manipuloimalla erityisesti tietoympäristöä sekä haastamalla ydininfrastruktuureita. Toiminnalla pyritään heikentämään sosiaalista yhteenkuuluvuutta ja luottamusta EU:n toimielimiin sekä jäsenvaltioiden hallituksiin. Vaikka vastuu hybridiuhkien torjunnasta kuuluukin ensisijaisesti jäsenvaltioille, sisäisten yhteyksien takia kansallisen turvallisuuden ja puolustuspolitiikan mahdolliset haavoittuvuudet ovat yhteisiä kaikille jäsenvaltioille ja jotkut näistä uhkista ulottuvat jopa yli rajojen, kuten hybriditoiminnan kohdentaminen rajat ylittäviin verkkoihin tai infrastruktuureihin. Hybridiuhkiin varautumisen tulee kattaa sekä ulkoinen että sisäinen ulottuvuus ja siinä tulee yhdistyä sekä kansalliset että EU:n laajuiset näkökohdat. Varautumisen on katettava kaikki osa-alueet - varhaisesta havaitsemisesta, analysoinnista, tietoisuuden lisäämisestä, sietokyvyn rakentamisesta sekä ennalta estävistä toimista aina kriisiajan toimintaan ja sen seurausten hallintaan. Hybridiuhkien estämisessä ja niiltä suojautumisessa keskeisintä onkin juuri sietokyvyn rakentaminen. (European Commission 2020, 14-15)

Kolmas prioriteetti rakentuu nimensä mukaisesti terrorismiin ja radikalisoitumiseen sekä järjestäytyneeseen rikollisuuteen kohdistuvista toimista. Terrorismin uhka EU:ssa on edelleen kor-

kea ja hyökkäysten määrän vähentymisestä huolimatta, niiden vaikutukset saattavat siitä huolimatta olla tuhoisia. Radikalisoituminen voi polarisoida ja horjuttaa sosiaalista yhteenkuuluvuutta laajemminkin, joten radikalisoitumisen torjunnan tulisi kulkea käsi kädessä sosiaalisen yhteenkuuluvuuden edistämisen kanssa sekä paikallisella että kansallisella kuin myös Euroopan tasolla. Radikalisoitumisen ja terrorismin torjunnan ensisijainen vaihe on perimmäisten syiden poistaminen. Yhteiskunnan polarisaatio, todellinen tai tiedostettu syrjintä sekä muut psykologiset ja sosiologiset tekijät saattavat vahvistaa ihmisten alttiutta radikaaleille keskusteluille. Pehmeän vaikuttamisen keinot, kuten koulutus, kulttuuri, nuoriso ja urheilu voivat edistää radikalisoitumisen ehkäisemistä, tarjoamalla riskiryhmiin kuuluville nuorille mahdollisuuksia ja yhteenkuuluvuutta. Ensisijaisia toimia ovatkin varhaisen havaitsemisen ja riskienhallinnan, sietokyvyn rakentamisen ja toiminnasta irtautumisen sekä kuntouttamisen ja yhteiskuntaan sopeuttamisen edistäminen. (European Commission 2020, 15-16.)

Terrori-iskujen pelkoa ja uhan vaarallisuutta kasvattaa terroristien pyrkimys ”aseistautua” kemiallisilla, biologisilla tai säteily- ja ydinmateriaaleilla (CBRN), jonka lisäksi kiinnostusta ja halukkuutta ilmenee osaamisen ja kyvykkyyden kehittämiseen niiden käytössä. CBRN-hyökkäysten potentiaali tulee näkyvästi esiin terroristisessa propagandassa ja varsinkin kun potentiaaliset vahingot olisivat hyvinkin suuret, asiaan on kiinnitettävä erityistä huomiota. Huolimatta lainsäädännöstä, jolla pääsyä räjähteiden valmistusaineisiin rajoitetaan, on tehty havaintoja epäilyttävistä liiketoimista, joiden tarkoituksena on itsetehtyjen räjähteiden valmistaminen. Kotitekoisten räjähteiden uhka onkin edelleen korkea ja niitä on käytetty useissa hyökkäyksissä kaikkialla EU:ssa. (European Commission 2020, 16.)

Järjestäytynyt rikollisuus aiheuttaa EU:n alueella valtavia taloudellisia ja henkilökohtaisia kustannuksia. Järjestäytyneen rikollisuuden ja korruption aiheuttaman taloudellisen tappion arvellaan olevan noin 218–282 miljardia euroa vuodessa ja yli 5000 järjestäytynyttä rikollisryhmää oli tutkinnan alaisena Euroopassa vuonna 2017, mikä on 50 % enemmän kuin vuonna 2013. Järjestäytyneen rikollisuuden toiminta on yhä enemmän rajat ylittävää, ulottuen myös EU:n välittömiin naapurimaihin, mikä vaatii tehostettua operatiivista yhteistyötä ja tiedonvaihtoa naapurimaiden välillä. Yli kolmannes EU:ssa toimivista järjestäytyneen rikollisuuden ryhmistä osallistuu huumeiden tuotantoon, kauppaan tai jakeluun. Suurin osa huumekaupasta tapahtuu rajojen yli ja niistä saadut voitot ohjataan lailliseen talouteen. Järjestäytyneet rikollisryhmät ja terroristit ovat lisäksi avaintoimijoita laittomien ampuma-aseiden kaupassa ja vuosina 2009-2018 Euroopassa tapahtui 23 joukkoampumista, joissa kuoli yli 340 ihmistä. Ampuma-aseita salakuljetetaan EU:hun usein sen välittömässä läheisyydessä olevien naapurimaiden kautta, mikä viittaa tarpeeseen vahvistaa koordinointia ja yhteistyötä EU:n sisäisesti sekä muiden maiden kanssa. (European Commission 2020, 17-18.)

Rikollisjärjestöt käyttävät maahanmuuttajia ja kansainvälistä suojelua tarvitsevia ihmisiä hyödykkeinä ja 90 % EU:n alueelle tulevista laittomista maahanmuuttajista saapuu rikollisverkoston

avustama. Siirtolaisten salakuljetus on myös usein yhteydessä muihin järjestäytyneen rikollisuuden muotoihin, erityisesti ihmiskauppaan. Ihmiskauppaan liittyvä kaikentyyppisen hyväksikäytön tuottama vuotuinen voitto on maailmanlaajuisesti 29,4 miljardia euroa. Tämä kansainvälinen rikollisuuden muoto vaikuttaa kaikkiin EU:n jäsenvaltioihin ja heikot tulokset näiden rikosten tunnistamisessa, syytteeseenpanossa ja tuomitsemisessa edellyttääkin uudenlaista lähestymistapaa toiminnan tehostamiseksi. Järjestäytyneet rikollisryhmät - samoin kuin terroristit - etsivät jatkuvasti erilaisia toimintamahdollisuuksia kaikilta toimialoilla ja etenkin niiltä, joista on saatavissa suuria voittoja pienellä kiinnijäämisriskillä, josta esimerkkinä ympäristörikollisuus. Luonnonvaraisten eläinten laittomasta metsästyksestä ja kaupasta, laittomasta kaivostoiminnasta, hakkuutöistä sekä laittomasta jätteiden hävittämisestä ja niiden siirtämisestä onkin tullut neljänneksi suurin rikollisuuden toimiala. Yhdeksi kannattavimmista rikollisen toiminnan aloista on muodostunut kulttuuriesineiden laiton kauppa, joka toimii niin terroristien kuin järjestäytyneen rikollisuuden tulonlähteenä ja sen arvioidaan olevan kasvussa. Näiden ohella, muista järjestäytyneen rikollisuuden toimialoista talous- ja finanssirikokset ovat aina erittäin monimutkaisia, mutta ne koskettavat miljoonia kansalaisia ja tuhansia yrityksiä EU:ssa vuosittain. Niihin kytkeytyvien petosrikosten kattava torjunta onkin ratkaisevan tärkeää ja edellyttää kattavia EU:n tason toimia. Järjestäytyneen rikollisuuden ja korruption välillä on vahva yhteys ja karkeasti arvioiden pelkästään korruption arvellaan maksavan EU:n taloudelle 120 miljardia euroa vuodessa. (European Commission 2020, 18-20.)

Laiton jätteiden hävittäminen saattaa äkkiseltään tuntua hieman oudolta rikollisuuden alalta, mutta sen tarkasta sääntelystä huolimatta, tarjoaa se silti monia rikollisen toiminnan mahdollisuuksia. Laittomaan jätekauppaan liittyvien tuottojen arvellaan olevan jopa yhtä merkittäviä kuin esimerkiksi huumausaineiden salakuljetuksesta saatavat tuotot ja kyseisen toiminnan negatiiviset seuraukset ulottuvat ympäristöön liittyvistä riskeistä aina terveydellisiin haittoihin sekä taloudellisiin vaikutuksiin. Jätekuljetuksiin liittyvien rikosten arvallaan olevan yleisiä ja merkittäviä myös tulevaisuudessa ja niissä esiintyy usein myös muuta rikollisuutta, kuten lahjontaa, anastusrikoksia, liikenne- ja työturvallisuusrikoksia, rahanpesua, ihmissalakuljetusta, laitonta jätteiden keräämistä ja hylkäämistä sekä petoksia ja veropetoksia. Jätekuljetuksiin liittyvän rikollisuuden ollessa kansainvälistä, toteutusmuodot liittyvät jätekuljetusten todellisen luonteen peittämiseen sekä toimintatapoihin, joilla päätetään kuljetuksen reitti. Merkittävimpänä rikoksen toteutusmuotona pidetään kuitenkin dokumenttien väärentämistä. Viranomaisten kohdalla keskeisenä ongelmana onkin, ettei tarkastustilanteessa aitoja dokumentteja osata erottaa väärennetyistä. (Kankaanranta & Suvantola 2018, 90 & 92.)

Turvallisuusstrategian neljäs ja viimeinen prioriteetti pitää sisällään yhteistyön ja tiedonvaihdon, vahvat ulkorajat, tutkimuksen ja innovatiivisuuden vahvistamisen sekä taitojen ja tietoisuuden lisäämisen. Toimivan ja tehokkaan turvallisuusunionin on oltava koko yhteisön ja sen kaikkien osien yhteinen pyrkimys. Hallitusten, lainvalvontaviranomaisten, yksityisen sektorin, oppilaitosten sekä kansalaisten itsensä on oltava sitoutuneita sekä oikealla tavalla varautuneita

ja asennoituneita yhteisen valmiuden ja sietokyvyn rakentamiseen. Yhteistyö ja tiedonvaihto ovat tehokkaimmat keinot rikollisuuden ja terrorismin torjuntaan sekä oikeudenmukaisuuden pyrkimyksiin. Jotta toiminta olisi tehokasta, tulee sen olla kohdennettua ja oikea-aikaista ja sitä tulee toteuttaa yhteisesti, yhteisillä vastatoimilla ja kontrollilla. (European Commission 2020, 20-21.)

Tietoisuus turvallisuuskysymyksistä sekä taitojen lisääminen mahdollisten uhkien torjumiseksi yhdessä valtiohallinnon, yritysten ja yksilöiden kanssa ovat välttämättömiä yhteiskunnan resilienssin rakentamiseksi. IT-infrastruktuurin ja e-järjestelmien haasteet ovat osoittaneet tarpeen parantaa ihmisten valmiuksia kyberturvallisuudessa ja uhkiin vastaamisessa. Pandemia osaltaan on korostanut digitalisaation merkitystä kaikilla EU:n talouden ja yhteiskunnan alueilla. Pelkästään jo perustietämyksellä tietoturvauhkista ja niiden torjunnasta voi olla merkittävä vaikutus yhteiskunnan sietokykyyn. Kyberhyökkäysten torjumiseksi, tietoisuuden ja ymmärryksen lisääminen verkkorikollisuuden riskeistä sekä suojautumiseksi niiltä, on toteuttavissa yhdessä palveluntarjoajien suojausten kanssa. (European Commission 2020, 25.)

EU:n uusi turvallisuusstrategia luo perustan turvallisuusekosysteemille, joka kattaa koko eurooppalaisen yhteisön. Se perustuu ymmärrykseen siitä, että turvallisuus tarkoittaa jaettua vastuuta. Turvallisuus on asia, joka vaikuttaa kaikkiin, mistä johtuen kaikkien hallintoelinten, yritysten, yhteiskunnallisten organisaatioiden, instituutioiden ja kansalaisten on täytettävä oma velvollisuutensa yhteisön turvallisuuden parantamiseksi. Turvallisuuskysymyksiä on tarkasteltava paljon laajemmasta näkökulmasta kuin aiemmin ja fyysisen sekä digitaalisen toimintaympäristön väliset rajapinnat on ylitettävä. EU:n turvallisuusstrategiassa kerätään yhteen kaikki keskeiset turvallisuuden haasteet sekä niiden tärkeimmät osa-alueet, jotka tulevat tulevina vuosina olemaan kriittisimmät EU:n turvallisuuden kannalta. Strategia osoittaa, etteivät turvallisuusuhkat kunnioita maantieteellisiä rajoja ja että sisäisen ja ulkoisen turvallisuuden välinen yhteys kasvaa yhä jatkossakin. (European Commission 2020, 26.)

5 Varautuminen turvallisuusympäristön uhkatekijöihin

Opinnäytetyön kolmas kokonaisuus koskee yhteiskunnan varautumista ja ennakointia turvallisuusympäristön uhkia vastaan. Turvallisuusympäristössä ilmenevien uhkien ohella, poliisityön ja kokonaisvaltaisen turvallisuusajattelun kannalta tulee ymmärtää, miten niihin varaudutaan, sillä mahdollisessa häiriötilanteessa varautumis- ja valmiussuunnittelun mukaiset toimet koskettavat poliisiorganisaatiota konkreettisesti. Tilanteessa, jossa uhka pystytään etukäteen tiedostamaan ja siihen konkreettisesti varautumaan, uhkan mahdollisuus toteutumiseen pienenee. Haavoittuvuutemme on vähäisempi, jos tietokoneen tietoturva on ajan tasalla tai puolustusvoimilla on riittävä puolustuskyky ja se kykenee toimimaan ennaltaehkäisevänä pidikkeenä mahdollista sotilaallista uhkaa vastaan. Uhkien jatkuva muuttuminen, nopeastikin, on luonnollista,

jossa uhkien todennäköisyydet kasvavat ja heikkenevät, kuten uhkien vaikutuksetkin. Uhkista osa poistuu ja uusia tulee tilalla, joskin osa niin sanotuista vanhoista uhkista säilyy vuosikymmenistä toiseen. Uhkien arviointi ja uhkiin varautuminen onkin jatkuvaa ja kun uhkat muuttuvat, myös hallintakeinojen tulisi muuttua. Uhkien muutosnopeus ja lisääntynyt haavoittuvuus vaikuttavatkin sietokyvyn eli resilienssin merkityksen korostumiseen. Sietokyvyssä kyse on niin toiminnallisesta kuin henkisestä kyvystä selviytyä erilaisista, niin yllättävistä kuin vähemmän yllättävistä, normaalista poikkeavista tilanteista sekä kyvystä palautua normaalitilaan mahdollisimman nopeasti. (Limnéll & Iloniemi 2018, 20-21.)

Yhteiskunnan turvallisuuteen kohdistuvia uhkia pyritään torjumaan monin eri tavoin. Merkittävimpien uhkien kohdistuessa yhteiskunnan kriittisiin ja elintärkeisiin kohteisiin, varautumis- ja valmiussuunnittelua toteutetaan sen mukaisesti. Yhteiskunnan varautumisessa huomio pyritään keskittämään yhteiskunnan toimivuuden ja sen turvallisuuden kannalta olennaisimpiin kohteisiin, joista tärkeimpinä erilaiset kriittisen infrastruktuurin kohteet. Yhteiskunnan varautumisella ja valmiussuunnittelulla tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen sekä mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet normaaliolojen häiriötilanteissa ja poikkeusoloissa. ”Varautumistoimenpiteitä ovat muun muassa valmiuslakiin, pelastuslakiin sekä muuhun varautumisesta annettuun erityislainsäädäntöön perustuva valmiussuunnittelu, jatkuvuudenhallinta sekä kaikenlainen etukäteisvalmistelu, kuten koulutus ja valmiusharjoitukset. Varautuminen perustuu valmiuslain (1552/2011), pelastuslain (379/2011) ja muun erityislainsäädännön varautumisvelvollisuuteen.” (Turvallisuuskomitea 2017, 9.)

”Kriittisellä infrastruktuurilla tarkoitetaan yhteiskunnan perusrakenteita, palveluita ja niihin liittyviä toimintoja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi” (Kokonaisturvallisuuden sanasto 2017, 32).

Viranomaisten tehtävänä ja velvollisuutena on hoitaa heille määritellyt tehtävät niin normaalioloissa kuin normaaliolojen häiriötilanteissa. Valmiuslain (1552/2011) mukaisesti viranomaisilla on lisäksi velvollisuus varautua myös poikkeusolojen tilanteisiin. Käytännössä tämä tehtävä lankeaa pitkälti kuntien vastuulle, mikä tekee niiden roolista yhteiskunnan varautumisessa ja häiriötilanteiden hallinnassa merkittävän. (Valtioneuvoston kanslia 2016, 17.)

Varautumisen yleinen prosessi pitää sisällään ennakoinnin, joka kattaa niin suunnittelun kuin sen mukaisen toiminnan sekä näistä kerätyn palautteen. Tämän ohella varautumisen yleisiä prosesseja voidaan käsitellä erilaisissa yhteistoimintafoorumeissa, joissa arvioidaan yhteisiä toimintoja koskevia riskejä sekä niiden todennäköisyyksiä ja vaikutuksia. Erityistä huomiota kohdistetaan eri toimijoiden ja sektoreiden rajapinnoissa oleviin riskeihin sekä yhteistoiminta-

mahdollisuuksiin seuraamalla toimintaympäristössä esiintyviä muutostrendejä sekä toteuttamalla harjoituksissa erilaisia skenaarioita, joiden avulla voidaan lisätä valmiuksia toimia erilaisissa odottamattomissa tilanteissa. (Turvallisuuskomitea 2017, 9-10.)

Turvallisuuskomitean mukaan Suomen tämän hetkisessä muuttuneessa ulko- ja turvallisuuspoliittisessa toimintaympäristössä ominaista on muutoksen nopeus ja ennakoimattomuus, mikä samaan aikaan erilaisten epävarmuustekijöiden myötä vaikuttaa Suomen sisäiseen kehitykseen ja turvallisuuteen. Nykyisessä toiminta- ja turvallisuusympäristössä yhteiskuntaan kohdistuu dynaamisia, muuntuvia ja rajat ylittäviä uhkia. (Turvallisuuskomitea 2017, 6.) Varautumisella sekä erilaisilla valmiustoimilla ylläpidetään ja kehitetään yhteiskunnan ja organisaatioiden jatkuvuudenhallintaa ja samalla määritellään merkittävimmät toiminnot ja palvelut, joiden häiriöttömyys tulee turvata (Valtioneuvoston kanslia 2016, 9).

Yhteiskunnan toimivuuden kannalta on määritelty erilaiset elintärkeät eli kriittiset toiminnot, jotka ovat välttämättömiä yhteiskunnan toimivuuden kannalta ja joiden toiminta pyritään turvaamaan kaikissa mahdollisissa tilanteissa (Turvallisuuskomitea 2017, 93). Häiriö- ja kriisitilanteisiin sekä poikkeusoloihin pyritään varautumaan mahdollisimman hyvin ennalta ja tätä tarkoitusta varten on laadittu Yhteiskunnan turvallisuusstrategia YTS. Yhteiskunnan turvallisuusstrategia sisältää kokonaisturvallisuuden yhteistoimintamallin, jonka pohjalta erilaisiin mahdollisiin häiriötilanteisiin varaudutaan ja niissä toimitaan. Yhteiskunnan turvallisuusstrategia on laadittu laaja-alaisessa yhteistyössä eri toimijoiden kanssa ja siihen kuuluvaa kokonaisturvallisuuden ajattelumallia toteutetaan yhdessä niin viranomaisten ja elinkeinoelämän kuin järjestöjen ja kansalaisten kanssa. (Turvallisuuskomitea 2017, 1.)

Yhteiskunnan turvallisuusstrategiassa määriteltyjä elintärkeitä toimintoja ovat johtaminen, kansainvälinen toiminta ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys (resilienssi). Kaikki mainitut toiminnot ovat yhteiskunnan toimivuuden kannalta välttämättömiä, kaikissa tilanteissa ylläpidettäviä toimintokokonaisuuksia, johon sisältyy yhteiskunnan toimijoiden yhteinen riskien ennakointi, varautumisen suunnittelu sekä koulutus ja harjoittelu. Yhteiskunnan eri toimijoita koskevaa yhteistoimintamallia toteutetaan sekä paikallisella että alueellisella kuin myös valtakunnallisella tasolla. (Turvallisuuskomitea 2017, 9.)

Yhteiskunnan elintärkeiden toimintojen jatkuvuus tulee turvata kaikissa mahdollisissa turvallisuustilanteissa, mikä puolestaan pohjautuu pitkäjänteiseen ja riittävien suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöönottoon sekä jo olemassa olevien suorituskykyjen hyödyntämiseen. Mahdollisessa hybridiuhkatilanteessa viranomaiset eivät yksin selviä, vaan koko yhteiskunnan tulee kyetä puolustautumaan, mistä johtuen myös järjestöjen ja elinkeinoelämän rooli kokonaisturvallisuuden tuottajina on oleellinen. Kansalaisten ymmärrys

kokonaisturvallisuudesta ja Suomeen mahdollisesti kohdistuvista uhkista onkin yksi tärkeä elementti kansallisessa kriisinsietokyvyssä. Sellaista tilannetta ei saisi syntyä, jossa esimerkiksi lämpö-, vesi-, tai sähkökatkot johtaisivat yhteiskunnan lamaantumiseen tai kansalaisten henkisen kestävyyden murtumiseen. Tällaisessa tilanteessa vastatoimet luonnollisesti poikkeavat toisistaan, jos myrskyn sijaan sähkökatkon syynä onkin tahallisesti toteutettu kyberhyökkäys. (Turvallisuuskomitea 2016, 4.)

Häiriö- ja kriisitilanteessa tai poikkeusoloissa viimeinen vastuu varautumisesta ja sen johtamisesta on viranomaisilla tai siihen erikseen velvoitetuilla turvallisuustoimijoilla, heille erikseen säädettyjen tehtäviensä ja toimivaltansa mukaisesti. Asetetuista velvoitteista huolimatta varautumisen ja siitä huolehtimisen tulisi olla osa kaikkien merkittävien toimijoiden päivittäistä toimintaa, sillä johtosuhteiden, organisaatioiden ja vastuunjaon tulisi säilyä mahdollisimman muuttumattomana kaikissa tilanteissa. (Turvallisuuskomitea 2017, 11-12.)

Yhteiskunnan turvallisuusstrategiassa määritellään viranomaisten strategiset vastuut, kuten myös niiden välistä yhteistyötä ohjaavat periaatteet. Huolimatta jokaiselle strategiselle tehtävälle määritellystä vastuuviranomaisesta, tehtäviä toteutetaan poikkihallinnollissa yhteistyössä. Viranomaisten ohella yhteiseen varautumisyhteistyöhön osallistuvat myös elinkeinoelämä ja kolmas sektori heille kuuluvan roolinsa mukaisesti ja käytännössä onkin niin, että kriittisiä toimintoja koskevissa varautumistoimissa julkisen sektorin varautumistoimet ovat luonteeltaan lähinnä täydentäviä ja pääasiassa käytännön toimet toteuttaa elinkeinoelämä normaaliolojen rakenteisiin perustuen. Taloudellisten toimintojen jatkuvuus, kriittisen infrastruktuurin toimivuus sekä huoltovarmuuden turvaaminen kaikkinensa on laaja kokonaisuus. Eri toimijoiden välinen yhteistyö korostuu erityisesti kriittisen infrastruktuurin ja palveluiden sekä huoltovarmuuden turvaamisessa, sillä suurin osa näitä toimintoja tuottavista ja ylläpitävistä rakenteista, prosesseista sekä resursseista on yksityisen sektorin hallinnassa. Yhteiskunnan toiminnan kannalta kriittiset yritykset ja palveluntuottajat varmistavatkin toiminnan jatkuvuuden joko lainsäädäntö-, sopimus- tai muulla vahvalla perusteella ja joissakin tapauksissa varautumisvelvoite on jopa sisällytetty substanssilainsäädäntöön. Yksityisen sektorin merkittävästä roolista huolimatta, yhtä lailla myös julkisen talouden toimintaedellytysten turvaamiseen tarvitaan yhteistyötä läpi koko yhteiskunnan. (Turvallisuuskomitea 2017, 94-96).

Varautumisen kannalta yhteiskunnan taloutta, kriittistä infrastruktuuria ja huoltovarmuutta vaarantavia keskeisiä uhkia voisivat olla jo kansallisen riskiarvion yhteydessä osittain esiin tuodut elintarvikehuollon vakavat häiriöt, energian saannin vakavat häiriöt, julkisen talouden rahoituksen saatavuuden häiriintyminen, kuljetuslogistiikan vakavat häiriöt, rahoitus- ja maksujärjestelmän vakavat häiriöt, tietoliikenteen ja tietojärjestelmien vakavat häiriöt sekä kyberuhkat, suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhat sekä myös terrorismi tai muu yhteiskuntajärjestystä vaarantava rikollisuus. (Turvallisuuskomitea 2017, 88).

Yhteiskunnan huoltovarmuudella tarkoitetaan toimintaa, jonka tarkoituksena on turvata väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämätön tuotanto sekä palvelut ja infrastruktuuri vakavien häiriötilanteiden ja poikkeusolojen varalta. Huoltovarmuuden kehittämistä tukee, ohjaa ja koordinoi Huoltovarmuuskeskus. (Kokonaisturvallisuuden sanasto 2017, 31.)

Limnéllin & Iloniemen (2018, 112) mukaan turvallisuusympäristön monimutkaistuminen ja dikotomioiden hämärtyminen korostavat tarvetta varmistaa, että valtionjohdolla ja viranomaisilla on luotettavaa tietoa päätöksenteon tueksi, jolloin tiedon ja analyysiin tulee olla monitasoista: strategista, operatiivista sekä taktisen tason tietoa. Reaaliaikaisen tilannetietoisuuden ohella Suomessa on viime aikoina tuotu vahvasti esiin strategisen ketteryyden periaatetta niin yritysmaailmassa kuin julkisellakin sektorilla. Kyse on kyvystä vastata nykyhetken ja etenkin tulevaisuuden haasteisiin strategisen ketterästi, muuttuvan toimintaympäristön pakottaessa muuttamaan ajattelu- ja toimintatapoja. (Limnéll & Iloniemi 2018, 102.)

Varautumisessa ja siihen liittyvässä suunnittelussa on jatkuvasti huomioitava ennakoinnin ja varautumisen moniulotteisuus ja haasteellisuus. Lindéll & Iloniemi (2018, 22) mainitsevat lisäksi, että tämän päivän verkottuneessa maailmassa ja yhteiskunnissa ainoastaan yhden uhkan poiminen ja siihen varautuminen on hyvin vaikeaa, sillä eri uhkatekijät ovat yhä vahvemmin vuorovaikutuksessa toisiinsa. Uhkat voivat esiintyä toistensa jatkumoina, niillä voi olla yllättäviä seurannaisvaikutuksia muihin uhkiin ja niiden kesto vaihtelee.

5.1 Kokonaisturvallisuuden malli ja kriittinen infrastruktuuri

Yhteiskunnan elintärkeiden eli kriittisten toimintojen turvaamiseksi ja varautumisen mahdollistamiseksi kehitetyssä kokonaisturvallisuuden yhteistoimintamallissa eri toimijat jakavat ja analysoivat turvallisuutta koskevaa tietoa sekä suunnittelevat, harjoittelevat ja toimivat yhdessä. Toimijoiden välinen yhteistyö perustuu lakisääteisiin tehtäviin, yhteistoimintasopimuksiin sekä yhteiskunnan turvallisuusstrategiaan. (Turvallisuuskomitea 2017, 5.)

Kokonaisturvallisuuden mallissa kyse on mahdollisimman kattavasta yhteistyöstä viranomaisten, paikallishallinnon, eri hallinnonalojen ja ministeriöiden sekä elinkeinoelämän välillä. Tarkoituksena on tukea samalla myös muita turvallisuustoimijoita. Yhteistyön tavoitteena on pyrkiä luomaan perusta elintärkeitä toimintoja uhkaavien häiriötilanteiden hallintaan, mikä toteutetaan yhteisellä valmiussuunnittelulla, valtakunnallisella sekä alueellisella ja paikallisella koulutus- ja harjoitustoiminnalla, poikkihallinnollisella yhteistyöllä sekä tilanteisiin oikea-aikaisesti reagoimalla. (Turvallisuuskomitea 2017, 15.)

Kokonaisturvallisuuteen perustuvan varautumisen pohjana on erilaisten riskien havaitseminen ja laaditut riskiarviot. Riskien arvioinnissa huomioidaan kaikki yhteiskuntaan kohdistuvat uhka-

tekijät ja erilaiset uhkamallit, joita tarvittaessa tarkennetaan uhka-arvioissa tapahtuvien muutosten perusteella. Tämä edellyttää riskien jatkuvaa ja säännöllistä arviointia sekä riskiarvion jatkuvaa päivittämistä. Riskiarvioita tehtäessä on huomioitava, että erilaiset uhkat saattavat ilmetä itsenäisinä, samanaikaisina tai toistensa jatkumoina, jolloin muutokset ja uhat voivat olla arvaamattomia, nopeita ja kestoltaan vaihtelevia. Osa uhkista saattaa toteutua jonkin toimijan tarkoituksellisena toimintana, kun taas joihinkin tällaista tarkoituksellista pyrkimystä ei sisälly. Tästä johtuen uhkien syitä, lähteitä, täsmällisiä kohteita, tavoitteita, ilmenemisen laajuutta tai seurannaisvaikutuksia on usein vaikea ennustaa. Varsinkin pidemmällä aikavälillä uhkien toteutumisen todennäköisyyden ennustaminen voi olla hyvinkin haastavaa, eikä kaikkia mahdollisia vaikuttamisen keinoja voida aina edes etukäteen tunnistaa. Näin on esimerkiksi hybridivaikuttamisen kohdalla, jolloin laaja-alainen yhteistyö uhkadynamiikan muutoksien havaitsemisessa, riskianalyysin laadinnassa sekä tilanteenmukaisissa ratkaisuissa korostuu. Uhka-arvioinnin keskiössä tulee olla valmius joustavuuteen yllättävissäkin muutoksissa sekä kyky varautua vastaamaan yhteiskuntaan kohdistuviin uhkiin ja niiden eri muotoihin sekä vahvistaa niissä vaadittavia suorituskykyjä. Nimenomaan tästä johtuen toimintaympäristön muutosten seuranta ja niiden analysointi sekä ennakointivalmiuksien ylläpitäminen tulee olla kaikkien yhteiskunnan varautumisesta ja häiriötilanteiden hallinnasta vastuussa olevien tahojen jatkuvaa ja aktiivista toimintaa. (Turvallisuuskomitea 2017, 25.)

Kokonaisturvallisuuteen pohjautuvalla varautumisella sekä systemaattisella jatkuvuudenhallinnan kehittämisellä vähennetään toimintakatkoista aiheutuvia kustannuksia, luodaan organisaation johdolle sekä vastuuhenkilöille toimintakykyä ja -varmuutta häiriötilanteisiin, tehostetaan häiriötilanteiden toimintaa, nopeutetaan toipumista sekä kasvatetaan vastuuhenkilöiden osaamista toiminnan kehittämisessä. Samalla parannetaan organisaation mainetta luotettavana kumppanina. Jatkuvuudenhallinnan toimintamallissa organisaation tai yrityksen tavoitteena ja tarkoituksena on tunnistaa ja arvioida toimintaansa liittyvät riskit, häiriötilanteet ja riippuvuudet, organisoida ja toteuttaa menettelytavat häiriötilanteiden varalle, varmistaa kriittisten kumppaneidensa toimintakyky häiriötilanteissa sekä suojata toimintansa intressit ja arvontuotantokyky. (Turvallisuuskomitea 2017, 95).

Tahallisesti aiheutetussa häiriötilanteessa tai valtakunnallisessa konfliktissa esimerkiksi hybridivaikuttamista ja varsinkin hybridisodankäyntiä kohdistetaan todennäköisimmin yhteiskunnan kriittisen infrastruktuurin kohteisiin. Kriittisen infrastruktuurin kohteet ovat erittäin haavoittuvaisia, koska niillä tuotetaan yhteiskunnan toiminnalle elintärkeitä palveluita. Kriittisen infrastruktuurin kohteita ovat muun muassa energiantuotanto ja -siirtojärjestelmät, tieto- ja viestintäjärjestelmät sekä logistinen järjestelmä. Muita kriittisiä palveluita ovat esimerkiksi ruoka- ja vesihuolto sekä sosiaali- ja terveyspalvelut. Suomessa kriittinen infrastruktuuri on pääosin yksityisten yritysten omistamaa ja operoimaa, mutta lisääntyvässä määrin omistukseltaan ja toiminnaltaan myös kansainvälistä. (Turvallisuuskomitea 2017, 89).

5.2 Kriittisen infrastruktuurin haavoittuvuus ja viranomaisten toimintakyky

Tässä luvussa esitetyt asiat perustuvat suurelta osin Poliisiammattikorkeakoulun, Tampereen yliopiston (aiemmin Tampereen teknillinen yliopisto TTY) sekä Suomen Pelastusalan Keskusjärjestö SPEKin yhteiseen kriittisen infrastruktuurin haavoittuvuutta ja viranomaisten toimintakykyä arvioivaan KIVI-hankkeeseen, jossa projektin koordinaattorina toimi Poliisihallitus. KIVI-hankkeella tuettiin kriittisen infrastruktuurin palveluntuottajien ja viranomaisten ennakointia ja varautumista ihmisen aikaansaamiin, elintärkeään infrastruktuuriin kohdistuviin vakaviin häiriötilanteisiin. Hankkeessa kehitettiin päivitettäviä apuvälineitä kriittisen infrastruktuurin vakavien häiriötilanteiden toimintaympäristövaikutusten arviointiin ja kehittämistyön ytimessä oli julkisen ja yksityisen sektorin keskinäisriippuvuuksien tunnistaminen monimutkaisessa ja jopa kaoottisessa kaupunkimaisessa toimintaympäristössä. Lisäksi hankkeessa tuotiin korostuneesti esiin ihmisen - joko tahallisesti tai tahattomasti - aiheuttamien häiriötilanteiden erityislaatuisuus luonnononnettomuuksiin verrattuna. (Heino, Jukarainen, Kalalahti, Kekki, Mansikkamäki, Takala & Verho 2019, 2.) Vakavalla häiriötilanteella tarkoitetaan tilannetta, joka on tavanomaista häiriötilannetta vakavampi, mutta kuitenkin lievempi kuin poikkeusolot (Kokonaisturvallisuuden sanasto 2017, 60).

Heinon ym. (2019, 3) mukaan kaupungistumisen ollessa yksi globaaleista megatrendeistä, kaupunkilaisten arjen sujuvuus on yhä riippuvaisempi tiheämmistä ja monimutkaisemmista infrastruktuurin rakenteista sekä niiden mahdollistamista palveluista. Infrastruktuurin toimivuus on jatkuvasti kriittisempi tekijä yhteiskunnan ja sen yksittäisten jäsenten turvallisuuden, hyvinvoinnin ja toiminnan kannalta, jossa haasteena on, ettei kriittisen infrastruktuurin järjestelmiä ole lähtökohtaisesti suunniteltu siten, että niiden olisi mahdollista joutua ihmisen tahallaan aiheuttaman hyökkäyksen kohteeksi. KIVI-hankkeen lähestymiskulma poikkeaa hieman kansallisesta riskiarviosta, sillä olennaista ei ole vakavan häiriötilanteen todennäköisyys, vaan aiheutuvien seurausten haitallisuus, niihin varautuminen ja niiden käsittelykyky. Kansallisesta riskiarviosta poiketen, hankkeen tarkastelukulma on myös rajattu nimenomaan ihmisen - joko tahallaan tai tahattomasti - aiheuttamiin häiriötilanteisiin. Syynä tähän on, että ihmisten aiheuttamat häiriöt etenkin kaupunkiolosuhteissa ovat saaneet osakseen suhteellisen vähän pohdintaa ja huomiota, mikä osittain selittyy sillä, että suomalainen yhteiskunta on ainakin toistaiseksi säästynyt laajoilta ja pitkäaikaisilta häiriöiltä.

9/11 terrori-iskujen tutkintakomission arviointiraportissa esimerkiksi todetaan, että vaikka iskut kertoivat ulkopolitiikan ja operatiivisen johtamisen epäonnistumisesta, syy oli ennen kaikkea mielikuvituksettomuudessa. Puuttui syvällisempi analyysi tilanteesta, jossa lentokonetta voitaisiin käyttää aseena, eikä näin ollen oltu pohdittu myöskään indikaattoreita, jotka auttaisivat tällaisten iskujen ennakoinnissa. Vaikka valmiusharjoituksissa hyödynnettäisiin kuvitteellisia tapahtumaketjuja eli skenaarioita ja simuloitaisiin aiemmin tapahtuneita häiriötilanteita, varautuminen pelkästään tunnettuihin tapahtumiin on vaarallista ja ennakoinnin tuleekin olla

avarakatseisempaa. 9/11-tutkintakomissio suosittikin luomaan skenaarioita myös yllättävistä iskuista sekä tunnistamaan niistä vaarallisimmat ja niiden indikaattorit. KIVI-hankkeessa tarkasteltiinkin erityisesti poliisin, pelastustoimen sekä kriittisen infrastruktuurin palveluntuottajien välisiä keskinäisriippuvuuksia sekä häiriötilanteiden aikana että niiden jälkeen. (Heino ym. 2019, 3.)

KIVI-hankkeen keskeisiä käsitteitä ja kiinnostuksen kohteita ovat kriittisen infrastruktuurin vakava häiriötilanne, johon liittyy ajatus monimutkaisesta ja jopa kaoottisesta tilanteesta ja jossa erilaiset syy-seuraussuhteet ovat epäselviä. Tästä johtuen häiriötilanteen johtaminen edellyttääkin normaalista poikkeavia toimia sekä toisenlaista ajattelutapaa. Vakava häiriötilanne voi olla kriisin luontoinen tai jopa lähellä katastrofia. Sähköhuollon kohdalla puhutaan vastaavasti suurhäiriöstä, jolloin kysymyksessä on pitkäkestoinen ja/tai laaja sähkökatko, ja jossa määritelmän mukaan tulisi olla osallisena pelastuslaitoksen lisäksi myös vähintään yksi yhteiskunnan julkista valtaa käyttävä toimija. Kriisin kehittyminen tapahtuu aina nopeasti ja tuo päättäjille paljon ristiriitaista ja virheellistä tietoa tai se haittaa tiedon saantia. Kriittisen infrastruktuurin kriisit voivat kehittyä hitaasti tai nopeasti ja siinä vaiheessa, kun tapahtuma tunnistetaan kriisiksi, on se pahimmillaan saattanut jo karata kontrollista ja edetä katastrofiksi. Hätätilanteissa on vielä mahdollista soveltaa normaaliolojen käytäntöjä ja toimintamalleja, mutta harjoiteltaessa kriisitilanteisiin varautumista, olennainen vaatimus on tehdä merkittäviä muutoksia toimintamalleihin. Vakava häiriötilanne vaarantaa aina yhteiskunnan elintärkeitä toimintoja ja sen hallinta edellyttääkin viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. Vakavissa häiriötilanteissa ilmenee yleensä useita samanaikaisia ja toisiinsa liittyviä kriisitilanteita, jolloin niiden hallinnassa tarvitaan laajojen kokonaisuuksien ymmärtämistä ja systeemiajattelua. (Heino ym. 2019, 5-6.)

Reaktiivisuuden sijaan painopiste on siirtynyt häiriötilanteiden ennakointiin ja vakavat häiriötilanteiden ollessa lähtökohtaisesti kompleksisia ja kaoottisiakin, tilanteet edellyttävät sekä viranomaisilta että palveluiden tuottajilta kykyä joustavaan improvisointiin sekä luovuuteen tilanteissa, joissa valmiiksi kirjoitetut suunnitelmat ja resurssit osoittautuvat riittämättömiksi. Toisaalta on kyse kyvystä ymmärtää, ettei tilanteen kokonaishallinta ja ongelman määrittelyn ainekset ole minkään yksittäisen tahon hallussa, vaan tilanteen dynamiikka ylittää valmiiksi räätälöidyt organisaatiorajat. Tällaisessa tilanteessa tarvitaan tietoa ja ymmärrystä toisten avaintoimijoiden toiminnasta, tilanteeseen vaikuttavista keskinäisriippuvuuksista sekä niiden heijastevaikutuksista. Koska viranomaisten resurssit käyvät hyvin nopeasti riittämättömiksi, kansalaisten järjestäytyneet ja epäviralliset yhteisöt, eli niin kutsutut 3. ja 4. sektori osoittautuvat välttämättömiksi kumppaneiksi. Normaaliolojen tietojohtoiset ja riskiperusteiset toimintamallit kytkeytyvätkin tässä kohtaa aivan uudenlaisiin spontaaneihin ja luoviin ongelmanratkaisumalleihin. Pitäytyminen normaaliolojen rutiineissa, myös kriisitilanteissa, on jossain määrin ymmärrettävää, mutta vakava häiriötilanne saattaa kuitenkin pakottaa improvisoimaan, jotta vakavimmilta seurauksilta säästyttäisiin. (Heino ym. 2019, 7.)

Hierarkkisiin ja byrokraattisiin hallinta- ja toimintakulttuureihin tukeutuvien ja tiettyihin toimintamalleihin tottuneiden organisaatioiden, kuten poliisin ja pelastusviranomaisen, on muutettava toimintakulttuuriaan osallistuessaan verkostomaisiin varautumisen yhteistoiminnan rakenteisiin. Yhtä lailla, kriittisen infrastruktuurin palveluntuottajien ensisijaisena tehtävänä on taloudellisen lisäarvon tuottaminen asiakkaille ja omistajille, ei niinkään yhteiskunnallisen kokonaisturvallisuuden tuottaminen, jolloin kokonaisturvallisuuden ajattelua vahvistamalla nämä erilaiset toimintakulttuurit voidaan saada lähentymään toisiaan. Byrokraattinen organisaatio ja toimintatapa ovat vaikeuksissa silloin, kun toimintaympäristö muuttuu ja muutoksen ennakointi on vaikeaa. KIVI-hankkeen lähtöajatuksena onkin ollut kriittisen infrastruktuurin vakavan häiriötilanteen aiheuttama muutos totuttuun toimintaympäristöön. Tällaisessa häiriötilanteessa muodostuva toimintaympäristö edellyttää kykyä luoda hetkessä yhteistoiminnallisia verkostoja voimavarojen yhdistelemiseksi. Ennakoinnissa ja varautumissuunnittelussa olennaista onkin sekä yksilöllisten että organisatoristen kyvykkyyksien arviointi, sillä KIVI-hankkeen mukaan niin viranomaisten kuin kriittisen infrastruktuurin palveluntuottajien resilienssin yksi keskeinen rakennusaine on kyky tehdä tarkoituksenmukaista yhteistyötä vakavan häiriötilanteen eri vaiheissa sekä mahdollisissa erityistilanteissa. (Heino ym. 2019, 8-9.)

Ennakointivaiheen osalta tämä tarkoittaa kykyä osallistaa eri toimijoita laajasti valmiussuunnitteluun sekä toimijoiden kesken yhdessä arvioida keskinäisriippuvuuksista aiheutuvia vaikutuksia omalle toimintakyvylle. KIVI-hankkeessa muodostuneen näkemyksen mukaan resilientti organisaatio seuraa toimintaympäristöään ja sopeuttaa toimintaansa muutosten edellyttämällä tavalla, ennakoi ja harjoittelee vakavia häiriötilanteita ja arvioi niiden seurauksia, reagoi tehokkaasti sekä ennakoituihin että ennakoimattomiin häiriötilanteisiin ja oppii saaduista kokemuksista. Ennakointi antaa aikaa varautua erilaisiin tilanteisiin ja sopeutuvuus ja joustavuus tarkoittavat, että varautumissuunnittelun perusteita on arvioitava ajoittain, ettei jäätäisi kiinni rutiineihin ja tottumuksiin. Todellinen tilanne eroaa usein odotetusta tai kuvitellusta, eikä näin ollen kaikkiin mahdollisiin tilanteisiin voida kehittää täydellistä ratkaisua, joten organisaation onkin kyettävä sovittamaan toimenpiteensä niin, että ne vastaavat nykyisiä olosuhteita suhteessa vaatimuksiin ja resursseihin. (Heino ym. 2019, 8-9 & 18-19.)

Ennakoinnissa ja varautumissuunnittelussa keskinäisriippuvuudet ovat erityisen merkityksellisiä, sillä siinä missä kriittiset infrastruktuurit mahdollistavat kaupunkien sujuvan arjen, tekevät ne siitä samalla haavoittuvan. Monissa kaupungeissa infrastruktuuria palvelevien järjestelmien väliset kytkennät ovat lisääntyneet ja tihentyneet, mikä aiheuttaa erilaisia keskinäisriippuvuuksia näiden järjestelmien välille ja niiden rajapinnoille. Keskinäisriippuvuuksista johtuen mahdolliset häiriöt ulottuvat järjestelmästä toiseen ja voivat siten tuottaa uusia häiriöitä. Tämä kasvattaa kokonaiskompleksisuutta sekä värittää koko kriittisen infrastruktuurin riski- ja haavoittuvuusmaisemaa. Vesihuolto esimerkiksi on hyvin riippuvainen sähkönsaannista. Teknisten järjestelmien ja niiden välisten keskinäisriippuvuuksien ohella piileviä haavoittuvuuksia voi

esiintyä myös organisaatioiden välisessä tiedonvaihdossa, yhteisen tilannekuvan muodostamisessa sekä erilaisten toimintakulttuureihin ongelmien identifioinnissa ja yhteisvasteiden luomisessa. Keskinäiskytkentöjen ja haavoittuvuuksien myötä monimutkaisiin verkostomaisiin rakenteisiin muodostuu kriittisiä pisteitä – toimintoja lamauttavia ja häiriöitä kuljettavia kohtia – joita hyväksikäyttämällä on mahdollista saada panostukseen nähden verrattain laajamittaisia seurauksia. Vaatimattomillakin resursseilla toteutettu terroristinen hyökkäys strategisesti ja systeemisesti oikein valittuihin kohteisiin, voi ketjuuntuvien seurannaisvaikutusten kautta aiheuttaa lopulta jopa laajallekin levinneitä häiriöitä. Varautumisessa ja riskienhallinnassa olisikin kiinnitettävä erityistä huomiota nimenomaan keskinäisriippuvuuksiin, jotta jo ennalta kyettäisiin estämään vaikutusten potentiaalinen, usein ennustamattomasti etenevä vahinkokierre. (Heino ym. 2019, 8-9 & 21-22.)

Poliisin kannalta, etenkin kaupunkioloissa tapahtuva vakava häiriötilanne, voisi aiheuttaa monia haasteita ja erinäisiä ponnisteluita poliisille perustehtävän ollessa yleisen järjestyksen ja turvallisuuden ylläpitäminen ja rikosten ennalta estäminen. Kriittiseen infrastruktuuriin kohdistuvan vakavan häiriötilanteen syy voi olla pitkäänkin epäselvä, mutta käytännössä se kuitenkin käynnistää välittömästi viranomaistoiminnan tilanteen normalisoimiseksi tai sen hallintaan saattamiseksi sekä lisävahinkojen syntymisen estämiseksi. Väestö saattaisi lähteä hakeutumaan pois kaupungeista, mikä synnyttäisi liikenneruuhkia ja etenkin isommissa kaupungeissa esimerkiksi sähkökatko sotkisi myös kaupungin sisäistä liikennettä ja aiheuttaisi ruuhkia sekä onnettomuuksia. Häiriötilanteen kohdistuessa vesihuoltoon, voisi se aiheuttaa samankaltaista liikehdintää ja yllätyksellisiä seurauksia. Kansalaisten tiedonhalu saattaisi aiheuttaa ylimääräistä liikehdintää ja mahdolliset vihaisten joukkojen laajat kokoontumiset sekä halu omien etujen turvaamiseen voisi aiheuttaa erilaisia järjestyshäiriöitä. Mikäli taustalla olisi häiriötilanteen tahallinen järjestäminen, mahdollista on, ettei avustus- ja korjaustoimenpiteitä voitaisi suorittaa turvallisesti ilman poliisin läsnäoloa. Pitkittyneessä häiriötilanteessa myös ruoanjakelu saattaisi vaatia yleisen järjestyksen takaamista ja koska laajamittaisessa ja pitkittyneessä sähkökatkossa käteiselle rahalle tulisi tarvetta, rahojen kuljetuksen ja jakelun tulisi tapahtua turvallisesti, jolloin yksityiset turvallisuusyritykset saattaisivat tarvita poliisin resursseja riittävän turvallisuuden takaamiseksi. (Heino ym. 2019, 12.)

KIVI-hankkeen johtopäätöksissä todetaan, että perinteisen riskienhallinnan ohella tarvitaan myös resilienssin rakentamista vakaviin häiriötilanteisiin varautumiseksi. Varautumisessa ja valmiussuunnittelussa tulee aiempaa vahvemmin huomioida ihmisen tahattomasti tai tahallisesti aiheuttamat pitkäkestoiset ja laajat häiriötilanteet. Samoin operatiivisen toiminnan tasolla on syytä varautua myös sellaisiin tilanteisiin, joissa erilaisia ja toisistaan poikkeavia ilmiöitä esiintyy samanaikaisesti (hybridivaikuttaminen). Viranomaisten viestinnästä vastaavia henkilöitä tulee esimerkiksi kouluttaa vastaamaan informaatiovaikuttamiseen. Viranomaisten ja kriittisen infrastruktuurin palveluntuottajien resilienssin keskeinen rakennusaine on kyky tehdä tarkoi-

tuksenmukaista yhteistyötä vakavan häiriötilanteen eri vaiheissa ja erityistilanteissa, mikä tarkoittaa toimijoiden osallistamista laajasti ennakointiin ja toiminnan suunnitteluun sekä keskinäisriippuvuuksien ja toimintakyvyn arviointiin. Kyseessä on tällöin aito kokonaisturvallisuusajattelun sisäistäminen. (Heino ym. 2019, 39.)

Toimintaympäristön kehittymistä tulee seurata ja arvioida erilaisilla ennakointimenetelmillä sekä kerätä tietoa epätavanomaisiltakin foorumeilta. Tämän lisäksi viranomaisten ennakointia palvelisi erikseen kehitettävä toimintamalli myös niin kutsuttujen hiljaisten signaalien (kuten henkilöstön arjen havaintojen) keräämiseen ja käsittelyyn osana toimintaympäristön seurantaa. Tavanomaisen valmiussuunnittelun ohella tulisi panostaa ennalta ehkäisevään turvallisuussuunnitteluun, jossa aikaperspektiivi on pidempi ja pyrkimyksenä on vaikuttaa turvallisuusriskien juurisyihin. Turvallisuussuunnittelu avaa keinon osallistaa elinkeinoelämää sekä kansalaisjärjestöjä ja -verkostoja ja samaan aikaan viranomaisten tulisi yhteensovittaa valmiussuunnittelua keskeisimpien sidosryhmien kanssa nykyistä laajemmin. Tärkeintä onkin ymmärtää, että laaja-alaisen yhteistyön edellytykset on rakennettava jo normaaliolojen aikana. Viranomaisten on tiedostettava kriittisten toimintojen suorittamiseen liittyvät suoritus- ja toimintakyvyt sekä sellaiset kynnysrajat, joissa tarvitaan lisäresursseja oman organisaation ulkopuolelta, kuten myös tilanteet, joissa on mahdollista tukea muita tahoja heidän kriittisissä toiminnoissaan. Viranomaisten, yhteistyöverkostojen ja muiden sidosryhmien tulisi harjoitella sellaisia häiriötilanteita ja niissä tapahtuvaa toimintaa keskenään, joissa häiriön laajuus, kesto, johtovastuu sekä käytettävissä olevat resurssit eivät ole varmuudella tiedossa. Harjoittelussa tulisi, edes pienimuotoisesti, riskiarvion perusteella huomioida epätodennäköistenkin häiriötilanteiden aikaista toimintaa. Viranomaisilla tulisi lisäksi olla ymmärrys siitä, että vakavassa häiriötilanteessa voi paljastua myös ennakoimattomia keskinäisriippuvuuksia (ns. mustia joutsenia). (Heino ym. 2019, 39-40.)

Turvallisuuden ja uhkien arvioinnin mittavin haaste tulevaisuudessa onkin turvallisuusympäristön kompleksisuuden ymmärtäminen ja edes sen osittainen hallinta, sillä Suomea ja suomalaisten paikkaa maailmassa määrittää yhä enemmän globaali keskinäisriippuvuus ja sen jatkuva tiivistyminen. Elämme turvallisuusympäristössä, jossa kaikki todellakin vaikuttaa kaikkeen ja missä uhkat kietoutuvat yhä vahvemmin toisiinsa. Näitä uhkien vuorovaikutussuhteita kuin kokonaisuuttakin, tulee osata tulkita mahdollisimman realistisesti. Helppoa, yhä kompleksisemmaksi käyvän turvallisuusympäristön ymmärtäminen ei ole, mutta ennakoitaessa tulevaisuuden uhkia, on se yhä välttämättömämpää. (Limnéll & Iloniemi 2018, 111.)

Ulko- ja turvallisuuspoliittisen selonteon mukaan, nopeasti muuttuvassa toimintaympäristössä yhteiskunnan kriisinsietokyvyn merkitys korostuu. Keskeistä kriisinsietokyvyn vahvistamisessa on vahvan kansallisen puolustuskyvyn sekä sisäisen turvallisuuden ylläpitäminen. Yhteiskunnassa tulee laaja-alaisesti varautua monitahoisiin yhteiskunnan hyvinvointiin ja turvallisuuteen

vaikuttaviin uhkiin, kuten hybridivaikuttamisen lisääntymiseen ja monimuotoistumiseen, ilmastonmuutoksen vaikutuksiin, ihmisen tai luonnon aiheuttamiin katastrofeihin sekä epidemioiden ja pandemioiden seurauksiin. Yhteinen varautuminen, suunnittelu, harjoittelu ja toimeenpano tulee toteuttaa kokonaisturvallisuuden periaatteen mukaisesti niin, että yhteiskunnan elintärkeistä toiminnoista huolehditaan laajassa yhteistyössä. Tärkeä osa kriisinsietokykyä on huoltovarmuuden turvaaminen kaikissa olosuhteissa ja sen ylläpitämisessä ja kehittämisessä tulisi huomioida tunnistetut kehitystarpeet. Sotilaallisessa huoltovarmuudessa oleellista on tärkeimpien suorituskykyjen operatiivisen toimintakyvyn turvaaminen. Toimintaympäristön muutos korostaa kyberpuolustuksen kehittämisen ohella informaatiopuolustuksen eli väärän tiedon oikaisemisen ja tiedon eheyden varmistamisen laaja-alaista kehittämistä. Hybridivaikuttamisen kytkeytyessä Euroopan huonontuneeseen turvallisuustilanteeseen, on huomioitava, että nopea teknologinen kehitys ja digitalisaatio luovat jatkossakin uusia välineitä myös vahingolliselle toiminnalle. Hybridivaikuttamisen osalta on lisäksi varauduttava myös muuttoliikkeen sekä erilaisten kriisitilanteiden tai historiatulkintojen varjolla tapahtuvaan hybridivaikuttamiseen. Yhteiskuntaan ei saa päästä syntymään sellaisia sisäisiä jakolinjoja, joita ulkoinen toimija voisi toiminnassaan hyödyntää, mikä ei myöskään saa päästä tapahtumaan ulkoisen vaikuttamisen seurauksena. Monialaisiin hybridiuhkiin varautuminen edellyttääkin yhteistä tilannekuvaa ja kokonaisvaltaista ennakointitoiminnan kehittämistä. (Valtioneuvosto 2020, 33.)

6 Johtopäätökset

Opinnäytetyön tavoitteena ja tarkoituksena oli selvittää mistä asioista turvallisuusympäristötietoisuus poliisitoiminnan kannalta koostuu ja mitä se pitää sisällään. Työn tarkoituksena on kehittää ja lisätä turvallisuusympäristötietoisuutta Poliisiammattikorkeakoulussa annettavissa poliisin AMK- ja YAMK-tutkinnoissa sekä poliisihallinnossa yleisesti. Kehittämistyö tukee Poliisiammattikorkeakoulun pedagogisia tavoitteita vastata tulevaisuuden tarpeisiin opetuksen ja osaamisen kehittämisessä toimintaympäristössä tapahtuvien muutosten mukaisesti. Tutkimus toteutettiin kvalitatiivisena eli laadullisena tutkimuksena, jossa tutkimusmenetelmänä käytettiin dokumenttianalyysia. Tutkimuksessa hyödynnettiin valtiohallinnon julkaisemia strategioita, selontekoja, valmisteluasiakirjoja, hankeraportteja ja muita julkaisuja sekä aihealueeseen liittyvää kirjallisuutta. Lähteiden alkuperä huomioiden, niitä voidaan pitää luotettavina.

Työn keskeisenä tarkoituksena oli hankkia tietoa turvallisuusympäristön muutoksesta ja sen vaikutuksesta sisäiseen turvallisuuteen, tarkastella turvallisuusympäristössä vallitsevia uhkia ja niiden merkitystä yhteiskunnan turvallisuudelle ja häiriöttömälle toiminnalle sekä tuoda esiin varautumisen merkitystä turvallisuusympäristön uhkia vastaan. Tutkimuksen tuloksia voidaan hyödyntää Poliisiammattikorkeakoulun opetuksessa sekä aihealuetta koskevan opetusmateriaalin valmistelussa. Keskeisenä tavoitteena on poliisin ammattitaidon ja osaamisen kehittäminen

sekä erityisesti poliisin johtamistehtävissä toimivien henkilöiden turvallisuusajattelun kasvattaminen. Poliisi on sisäisen turvallisuuden ensisijainen toimija ja nykyisessä turvallisuusympäristössä yleisen järjestyksen ja turvallisuuden ylläpitämisen sekä rikostorjunnan ohella on oltava tietoinen yhteiskuntaan kohdistuvista uhkista sekä varautumisen merkityksestä niin yhteiskunnan kuin viranomaisten toimintakyvyn ylläpitämiseksi.

Turvallisuusympäristötietoisuus rakentuu kolmesta tärkeästä kokonaisuudesta ja niiden ymmärtämisestä. Turvallisuusympäristötietoisuuden pohjana on käsitys sisäisen turvallisuuden ja siten myös yhteiskunnan turvallisuuden rakenteesta sekä sen kehittämistä ohjaavista toimista. Sisäisen turvallisuuden kehittämistä ohjataan sisäisen turvallisuuden strategialla, jonka ohella merkityksellisiä ovat ulko- ja turvallisuuspoliittinen selonteko ja puolustusselonteko. Sisäiseen turvallisuuteen liittyy kolme toimintaa ohjaavaa ajattelumallia, joita ovat arjen turvallisuus, laaja turvallisuuskäsitys ja kokonaisturvallisuus. Arjen turvallisuus pitää sisällään sellaisia yhteiskunnan turvallisuuteen sellaisia kohdistettavia toimia, jotta Suomi olisi maailman turvallisin maa ja jossa kansalaiset voisivat nauttia heille kuuluvista oikeuksista ja vapauksista ilman pelkoa ja turvattomuuden tunnetta. Arjen turvallisuuteen liittyy perinteisiä yhteiskunnallisia haasteita, kuten syrjäytyminen ja niin sanottu tavanomainen rikollisuus. Laaja turvallisuuskäsitys on ajattelumalli, mikä turvallisuusympäristön muutoksen myötä on otettu käyttöön kuvaamaan ulkoisen ja sisäisen turvallisuuden keskinäisriippuvuuden lisääntymistä. Turvallisuusympäristön uudet uhkatekijät ovat perinteisestä sotilaallisesta uhkasta poikkeavia, eikä ulkoisen ja sisäisen turvallisuuden välistä rajapintaa voida muutoinkaan enää määritellä niin tarkasti kuin aiemmin. Kokonaisturvallisuuden ajattelumalli liittyy yhteiskunnan kokonaisvaltaiseen varautumiseen mainittuja turvallisuusympäristön uhkia vastaan. Tulevaisuuden poliisitoiminnassa olisi tarkkaan huomioitava, että muutosilmiöt ja turvallisuusympäristön uhkat asettavat uudenlaisia haasteita ja vaatimuksia arjen turvallisuudelle sekä sisäisen turvallisuuden toimijoille vakaviin ja laajoihin häiriötilanteisiin varauduttaessa, kuten kuviossa 1 kuvattiin. Häiriötilanteisiin varautumisen keskeisenä tarkoituksena ja tavoitteena on kriittisen infrastruktuurin ja yhteiskunnan elintärkeiden toimintojen turvaamisen mahdollisessa häiriötilanteissa tai poikkeusoloissa.

Kuviossa 2 esitetyn mukaisesti turvallisuusviranomaiset ovat tavallaan kahden tulen välissä, sillä arjen turvallisuuden ja yhteiskuntarauhan ylläpitäminen asettaa tietyn palvelutarpeen, johon tulee normaalioloissa vastata ja toisaalta samaan aikaan varauduttava vakaviin häiriötilanteisiin, mikä asettaa esimerkiksi poliisille erityisiä suorituskykyvaatimuksia. Kuviossa 3 esitetyt vakavien ja laajojen häiriöiden taustalla vaikuttavat muutosvoimat muodostavat aiempaa suurempia uhkia kriittistä infrastruktuuria kohtaan, mikä tekee varautumisesta aiempaa vaikeampaa, varsinkin kun muistetaan turvallisuusympäristön jatkuva muutos ja uhkien kompleksisuus. Poliisin ja muiden viranomaisten ohella vastuu kokonaisturvallisuuden kehittämisestä ja ylläpitämisestä sekä häiriötilanteiden hoitamisesta myös yksityisen sektorin toimijoille, kuten yrityksille ja yhteisöille. Kokonaisturvallisuuden ajattelumallin toteuttamiseksi tämä tarkoittaa po-

liisille kiinteää sidosryhmäyhteistyötä yksityisen sektorin toimijoiden kanssa. Nämä yhteiskunnan turvallisuutta edistävät ajattelumallit ja niiden periaatteet tulisi poliisien tietää ja sisäistää, jotta tietämys sisäisen turvallisuuden perusrakenteesta olisi riittävällä tasolla. Kokonaisuuden hahmottamisessa sisäisen turvallisuuden kannalta merkitykselliset strategiat ja selonteot luovatkin eräänlaisen pohjan turvallisuusympäristötietoisuudelle ja poliisitoiminnan merkitykselle siinä.

Turvallisuusympäristötietoisuuden toinen ja kenties sen oleellisin kokonaisuus kohdentui turvallisuusympäristössä ilmeneviin uhkiin ja niiden aiheuttamiin haasteisiin. Uhkien tarkastelu perustui kansallisessa riskiarviossa esitettyihin uhkiin ja uhkamalleihin, jotka esitettiin kootusti kuviossa 4. Tämän tutkimuksen kannalta tarkempaan tarkasteluun valikoituivat poliisitoiminnan kannalta oleellisimmat uhkatekijät, joita olivat informaatiovaikuttaminen, kyberuhkat, voimahuollon eli sähkön- ja energiansaannin ongelmat häiriötilanteessa, ääriliikkeet ja terrorismi, hybridivaikuttaminen sekä riskiarvion ulkopuolelta järjestäytynyt ja rajat ylittävä rikollisuus, sen ollessa erityisesti poliisitoiminnan ja rikostorjunnan kannalta konkreettinen, kasvava ja siten merkittävä uhka yhteiskunnan turvallisuudelle. Seuraavassa joitain keskeisiä havaintoja turvallisuusympäristön uhkista.

Informaatiovaikuttaminen näyttäytyy osittain vielä tuntemattomana ja piilevänä uhkana, jonka avulla aktiivisesti ja tietoisesti pyritään vaikuttamaan ihmisten mielipiteisiin ja asenteisiin muokkaamalla niitä haluttuun suuntaan. Joissakin tapauksissa voidaan levittää disinformaatiota eli valheellista tietoa, joka voi olla hyvinkin suoraviivaista ja peittelemätöntä, mikäli sen katsotaan sopivan tilanteeseen tai edistävän omaa tavoitetta piilovaikuttamista paremmin. Ongelmallista informaatiovaikuttamisessa on sen havaitseminen, sillä usein kyseisen toiminnan kohteena olevat eivät välttämättä edes tiedosta olevansa informaatiovaikuttamisen alaisena ja tästä syystä informaatiovaikuttaminen onkin yksi hybridivaikuttamisen keskeinen väline. Informaatiovaikuttamisen torjuminen ja sen aiheuttamaan uhkaan vastaaminen edellyttää parempaa ymmärrystä informaatiovaikuttamisesta sekä sen keinoista ja tavoitteista, mikä puolestaan vaatii medialukutaidon lisäämistä sekä kattavampaa ymmärrystä ja osaamista niin viranomaisilta kuin viestinnän asiantuntijoilta. Informaatiovaikuttamisen seurauksena syntyvä, eritoten tahallisesti aiheutettu yhteiskunnan sisäinen vastakkainasettelu saattaisi johtaa sisäisten rakenteiden heikentymiseen, valtiojohdon tai viranomaistoiminnan kyseenalaistamiseen tai muihin yhteiskuntaa horjuttaviin vaikutuksiin. Informaatiovaikuttaminen ja sen merkitys uhkatekijänä tuleekin huomioida poliisissa tarkkaan. Tietoa lisäämällä ja poliiseja kouluttamalla voidaan kehittää informaatiovaikuttamisen havaitsemista sekä opastaa torjumaan vahingoittamistarkoituksessa kohdennettuja vaikuttamisyrityksiä.

Teknologinen kehitys ja kaiken laaja digitalisoituminen tuo omat kasvavat haasteensa niin yhteiskunnan ja kansalaisten turvallisuudelle kuin poliisin operatiiviselle toimintakyvylle ja kybe-

riin liittyvien uhkien torjumiselle. Kyberympäristöjen ja digitalisaation myötä muodostuu uudenlaisia, moniulotteisia ja pahimmillaan laajalle levittäytyviä uhkia yhteiskunnan tietoverkottuneelle infrastruktuurille sekä kansalaisille kasvavan verkkorikollisuuden muodossa. Tätä, osaltaan negatiivista kehitystä edesauttaa esineiden internet eli IoT, jossa useat tietotekniset laitteet verkostomaisesti kytkeytyvät toisiinsa. Verkottuneiden tietojärjestelmien varaan rakentuva yhteiskunnan kriittinen infrastruktuuri tuottaa kasvavia haavoittuvuuksia ja siitä muodostuvia haasteita kyberuhkien torjumiselle sekä niiden kautta syntyvien häiriötilanteiden torjumiselle. Kyber ja tietoverkot eivät tunne rajoja ja sitä voidaan hyödyntää informaatiovaikuttamisen ohella hybridivaikuttamisessa monin eri tavoin. Oman erityisen haasteen kyberympäristöön tuo sen jakautuminen fyysiseen ympäristöön sekä tietoverkoissa tapahtuvaan liikenteeseen. Vaikuttamalla vahingollisesti toiseen tai jopa molempiin, voidaan helposti aiheuttaa vahinkoa kyberympäristön toimivuudelle. Jatkossa kenties puhutaankin ainoastaan digitaalisesta toimintaympäristöstä, mihin sisältyy sekä fyysinen ympäristö että varsinainen tietoliikenne. Kyberuhkien erilaiset mahdollisuudet ovat lähes rajattomat, ainakin niin kauan, kun ollaan tekemisissä kyberympäristön tai digitalisaation kanssa. Kyberuhkien torjuminen vaatiikin laajaa yhteistä rintamaa ja tietoisuutta kyberiin ja tietoturvallisuuteen liittyvistä uhkista aina yhteiskunnan johdosta, organisaatioiden, yritysten ja viranomaisten kautta yksittäiseen kansalaiseen.

Poliisien käytössä olevan välineistön teknistyessä ja digitalisoituessa teknologisen kehityksen myötä, aiheuttaa se omat haasteensa poliisin tietojärjestelmien toimivuuden sekä operatiivisen toimintakyvyn varmistamiselle. Käyttäjätasolla tulisi ymmärtää ja tiedostaa kyberympäristöön liittyvät riskit, uhkat ja haavoittuvuudet sekä huomioida ne kaikessa omassa toiminnassa, aina kun ollaan tekemissä tietoteknisten päätelaitteiden, tietojärjestelmien tai muutoin kyberympäristöön kytkeytyvien toimintojen kanssa. Poliisityön ja rikostorjunnan näkökulmasta ei pidä myöskään unohtaa kyberympäristössä ilmenee rikollisuutta verkkoympäristöjen moniin erilaisiin rikollisiin tarkoituksiin, jota esimerkiksi järjestäytynyt rikollisuus käyttää häikäilemättömästi hyväkseen.

Sähkön- ja energiansaannin toimintavarmuus on erittäin kriittistä yhteiskunnan häiriöttömän toiminnan turvaamiseksi ja arjen sujuvuuden varmistamiseksi. Toimintavarmuudella on läheinen suhde kyberuhkiin, sillä niiden avulla voidaan helposti iskeä yhteiskunnan voimahuoltoa ylläpitäviin teknisiin ja verkottuneisiin järjestelmiin, jotka lisäksi ovat äärimmäisen keskinäisriippuvaisia, haavoittuvia ja häiriöalttiita. Sähkön- ja energiansaantiin kohdistuvassa häiriötilanteessa sillä olisi hyvinkin nopeat ja laajat vaikutukset lähes kaikkiin yhteiskunnan kriittisiin ja elintärkeisiin toimintoihin ja siten kansalaisten arkeen.

Suomessa erityisiä ongelmia kyseisessä häiriötilanteessa aiheuttaisi pitkät siirtoetäisyydet ja sen kumuloituvat vaikutukset tai sähkösaannin katkeaminen esimerkiksi talviaikaan. Yhtä lailla viestintäverkkojen kaatuminen aiheuttaisi välittömiä ja suoria vaikutuksia sekä kansalaisille

että viranomaisten operatiiviseen toimintakykyyn. Hybridivaikuttamisessa ja erityisesti hybridisodankäynnissä sähkön- ja energiansaantiin kytkeytyvät tekniset järjestelmät lienevätkin toiminnan kärkikohteita. Operatiivisen toimintakyvyn ohella tällaiset häiriötilanteet voisivat tuottaa poliisille suuria haasteita lähinnä seurausten ja niiden hallinnan muodossa, sillä sähköjen katkeaminen pidemmäksi aikaa tai vesihuollon järjestelmien toimimattomuus saattaisi melko nopeastikin aiheuttaa kansalaisissa levottomuutta, mikä puolestaan voisi ilmentyä levottomuuksina tai muuna yleistä järjestystä ja turvallisuutta uhkaavana toimintana.

Informaatiovaikuttamisen, kyberuhkien sekä sähkön- ja energiansaannin häiriöiden liittyessä lähinnä verkkoympäristöön ja teknisiin järjestelmiin, ääriliikkeiden toiminta ja terrorismi sen sijaan näyttäytyy ihmisille kenties hieman konkreettisempana uhkatekijänä. Huolimatta siitä, ettei Suomi näyttäydy terrorismin ensisijaisena kohdemaana, yksi terroristinen isku on jo tapahtunut ja Suojelupoliisi on jo muutaman vuoden ajan pitänyt terroristisen iskun uhkamahdollisuutta kohonneena. Keskeisenä uhkana ovat Lähi-Idän konfliktialueilta palaavat terrorisista koulutusta saaneet ja konflikteihin osallistuneet vierastaistelijat, jonka lisäksi Suomessa havaitaan merkittävää terrorismin tukitoimintaa. Uhka-arvioiden mukaan Suomesta löytyy sekä ryhmiä että henkilöitä, joilla on motivaatio ja kyky terrori-iskun toteuttamiseen. Yhteiskunnan turvallisuuden ja poliisitoiminnan kannalta merkittävimmän uhkan muodostavat kuitenkin yksittäiset henkilöt ja pienryhmät, joiden motivaation lähteenä toimii radikaali-islamistinen propaganda. Kotimaisten ääriliikkeiden osalta Suomessa ilmenee väkivaltaisen äärioikeiston ja väkivaltaisen äärivasemmiston toimintaa, joista tällä hetkellä äärioikeisto sattumanvaraisen katuväkivallan myötä muodostaa suurimman uhkan arjen turvallisuudelle. Äärivasemmiston harjoittama anarkismiin ja antifasismiin liittyvä liikehdintä on sen sijaan vähentynyt ja sitä esiintyy lähinnä mielenosoitusten yhteydessä.

Ääriliikkeiden toiminnan ja terrorismin keskeinen tekijä on radikalisoituminen ja siitä aiheutuva väkivaltainen ekstremismi. Suurin väkivallan uhka liittyykin nimenomaan radikalisoituneisiin yksittäisiin toimijoihin. Radikalisoitumisella nähdään olevan selkeä yhteys syrjäytymiskehitykseen ja ulkopuolisuuden tunteeseen, liittyen siten myös suoraan sisäisen turvallisuuden strategiassa esitettyyn arjen turvallisuuden edistämiseen, jossa yhteiskunnan yhtenä isona ongelma ja turvallisuushaasteena näyttäytyy kasvava syrjäytymiskehitys. Radikalisoitumisen taustasyihin vaikuttamalla sekä näköalattomuutta ja epätasa-arvon kokemuksia vähentämällä voidaan vaikuttaa mahdolliseen radikalisoitumiskehitykseen estävästi. Tietoisuus radikalisoitumisen syistä ja radikalisoitumiskehityksestä sekä ennalta estävän toiminta merkityksestä poliisissa, yhdessä muiden avaintoimijoiden kanssa, on oleellinen tekijä terrorismin ja väkivaltaisen ekstremismin torjunnassa. Radikalisoitumisen estämisessä on huomioitava myös vankilassa tapahtuva radikalisoituminen sekä mahdollinen rekrytointi ääriliikkeisiin. Kenttätasolla toimittaessa poliisien tulisikin pystyä tunnistamaan mahdollisia radikalisoituminen merkkejä ja/tai sen ensiaskeleita.

Operatiivisen poliisitoiminnan kannalta terroristisiten iskujen estäminen vaatii kattavaa ja laaja-alaista yhteistyötä poliisihallinnon sisällä sekä kansainvälisesti, kuin myös siihen liittyvää koulutusta, varautumista ja valmiuden kehittämistä terroristisiin tilanteisiin. Viime vuosina terroristisia iskuja on toteutettu ajoneuvoja ja/tai helposti saatavilla olevia välineitä, kuten teräaseita käyttämällä. Ampuma-aseiden tai räjähteiden käytön mahdollisuutta ei kuitenkaan voida sulkea pois ja teknologisen kehityksen myötä miehittämättömät ja räjähteillä tai jopa CBRN-aineilla lastatut miehittämättömät lennokit luovatkin aivan uudenlaisia uhkakuvia. Poliisitoiminnassa ja terroristisiin tekoihin varautumisessa on huomioitava potentiaaliset terroristisiten iskujen kohteet, joista maailmalla tapahtuneiden iskujen perusteella ensisijaisia ovat julkiset paikat ja laajat ihmisjoukot. Yhtä lailla isku voisi tarkoitushakuisesti kohdistua yhteiskunnan johtoon tai kriittisen infrastruktuurin kohteisiin, josta esimerkkinä tietoliikenteen tai sähköverkon kriittiset pisteet tai yhteiskunnan elintärkeät toiminnot. Potentiaalisten kohteiden tunnistaminen ja uhka-analyysien tekeminen edellyttääkin poliisilta yhteistyötä muiden viranomaisten, kuntien ja kaupunkien sekä kriittisen infrastruktuurin toimijoiden kanssa.

Yleisen järjestyksen ja turvallisuuden näkökulmasta on huomioitava lisäksi kansalaisten arkiseen turvallisuuteen vaikuttavat ja sitä mahdollisesta uhkaavat laajat ihmisjoukkojen kokoontumiset ja mielenosoitukset sekä niistä mahdollisesti eskaloituva väkivaltainen liikehdintä. Poliisitoiminnan kannalta huomionarvoista on tällaisiin tapahtumiin osallistuvat henkilöt tai ryhmät, joiden pääasiallisena tavoitteena voi olla näiden kokoontumisten muuttaminen väkivaltaiseksi liikehdinnäksi tai jopa mellakaksi. Väkivaltaisuuden lietsomisessa ja "negatiivisen ilmapiirin" nostattamisessa voidaan hyödyntää informaatiovaikuttamista tai jopa selkeää disinformaatiota, minkä avulla voidaan vahvistaa vihan ja katkeruuden tunteita yhteiskuntaa, hallintoa ja viranomaisia kohtaan. Vaikuttamisen moottorina voidaan käyttää yhteiskunnallista syrjäytymiskehitystä ja valikoidusti kohdentaen vaikuttaa tiettyihin ihmisryhmiin, jotka kokevat yhteiskunnan toimivan epäoikeudenmukaisesti ja olevan syynä vallitsevaan eriarvoisuuteen. Ihmisjoukkojen kokoamisessa ja halutun informaation jakelussa voidaan helposti hyödyntää sosiaalista mediaa, jonka avulla tavoitetaan suuria ihmismääriä hyvinkin nopeasti. Poliisilta tämän kaltaisten tilanteiden ennakointi edellyttää reaaliaikaista tiedustelutoimintaa sekä sosiaalisen median hyödyntämistä tiedon hankkimisessa. Tällaisissa tilanteissa on huomioitava, että informaatiovaikuttamisen ja levottomuuksien lietsonnan taustalla voi olla jokin yksittäinen toimija, ryhmittymä tai jopa valtiollinen taho. Poliisitoiminnan kannalta erityisiä ongelmia voisi aiheuttaa väkivaltaisen liikehdinnän tai mellakoiden massiivinen laajentuminen, jolloin poliisin operatiivinen toimintakyky ja voimavarat joutuisivat koetuksella tai eivät yksinkertaisesti riittäisi.

Turvallisuusympäristön uhkien tarkastelussa järjestäytynyt ja rajat ylittävä rikollisuus sai eniten huomiota, sillä poliisitoiminnan kannalta se näyttäytyy välittömänä ja konkreettisimpana uhkatekijänä, jolla on laaja-alaisia vaikutuksia sekä yhteiskunnan että ihmisten turvallisuuteen. Vaikka käsitellyistä uhkista kaikki voivat olla rajat ylittäviä ja globaaleja, järjestäytynyt rikollisuus on sitä tosiasiallisesti, mikä vaatii poliisilta jatkuvaa kansainvälistä yhteistyötä muiden

maiden viranomaisten kanssa. EU:n alueella toimii oma erillinen lainvalvontaviranomainen Europol, jonka toimintakenttänä ovat kaikki EU:n jäsenvaltiot. Huomioitavaa on järjestäytyneen rikollisuuden selkeät kytkökset kyberuhkiin ja verkkorikollisuuteen, ääriliikkeisiin ja terrorismiin kuin myös hybridivaikuttamiseen. Järjestäytynyt rikollisuus ulottaa toimintaansa kasvavassa määrin organisaatioihin, yrityksiin ja liike-elämään, toimien tehokkaasti harmaalla alueella, niin laillisen kuin laittoman liiketoiminnan keinoin. Ennalta estävän toiminnan kehittämiseksi ja järjestäytyneen rikollisuuden torjumiseksi, poliisin ja muiden viranomaisten sekä yritysten ja liike-elämän toimijoiden tulisikin tehdä säännöllistä yhteistyötä vakavan ja järjestäytyneen rikollisuuden torjumiseksi, mikä varsinaisen rikostorjunnan ohella vaatii poliisilta ymmärrystä liike-elämän rakenteista ja yritystoiminnan riskienhallinnasta.

Järjestäytyneessä rikollisuudessa kyse on useimmiten vakavasta rikollisuudesta, jota toteutetaan erityisen systemaattisesti ja erityistä ryhmärakennetta hyödyntämällä. Ryhmärakenteet toimivat verkostomaisesti ja ovat tapauskohtaisesti toiminnaltaan hyvin joustavia. Rikollisjärjestöissä toimivat verkostot koostuvat erilaisista toisiinsa kytkeytyvistä tasoista ja toimijoista, kuten toiminnan organisoijat, rahoittajat, asiantuntijat, järjestyksenpitäjät sekä ammattitekijät ja taparikolliset. Järjestäytyneen rikollisuuden yksi tärkeimmistä ominaisuuksista on sen kyky rajat ylittävään toimintaan ja usein rikollisryhmittymien ja -verkostojen toiminta ulottuukin moniin eri maihin. Järjestäytynyt rikollisuus määritellään sen rakenteen ja toiminnan kautta, mitä havainnollistettiin kuviossa 5.

Poliisin ja rikostorjunnan kannalta järjestäytyneestä rikollisuudesta tekee haastavan sen kyky omaksua nopeasti uusia toimintatapoja ja liiketoimintamalleja, jossa se kattavasti hyödyntää ja integroi toimintaansa uudenlaista tekniikkaa rikollisen toiminnan toteuttamiseksi. Järjestäytyneessä rikollisuudessa hyödynnetään tehokkaasti ja kattavasti digitaalisen verkon tarjoamia mahdollisuuksia sekä siellä olevia salattuja viestintäkanavia ja verkkoalustoja, joissa myydään laittomia tuotteita ja palveluita, sisältäen kaikkea mahdollista väärennetyistä asiakirjoista ja huumausaineista aina ostajalle hyödylliseen tietoon ja dataan. Pimeästä verkosta, rikollisuuden yksityisyrittäjiltä, on ostettavissa kohdennettuja palveluita ja erikoisosaamista esimerkiksi kyberhyökkäysten tai tietomurtojen muodossa, josta käytetään termiä Caas (Crime as a Sevice). Järjestäytyneen rikollisuuden monimuotoisuus ja toiminnan laaja-alaisuus asettaakin huomattavia ja jatkuvasti kasvavia haasteita poliisille, mistä johtuen järjestäytyneen rikollisuuden toimijat ja toimintatavat tulisi tunnistamaan aiempaa paremmin. Tulevaisuusennusteissa järjestäytyneen rikollisuuden nähdään entisestään kasvavan ja sen katsotaan olevan keskeinen uhka EU:n turvallisuudelle tulevaisuudessa, varsinkin teknologisen kehityksen tuodessa jatkuvasti uusia rikollisen toiminnan mahdollisuuksia. Jatkossa rikollisuuden ensisijaisia uhkia tulevat olemaan verkkorikollisuus, huumausainerikollisuus, maahanmuuttajien salakuljetus, järjestäytynyt omaisuusrikollisuus sekä ihmiskauppa. Rikolliseen toiminnan läpileikkaavia uhkia ovat talousrikollisuus ja rahanpesu, asiakirjapetokset sekä laittomien tavaroiden ja palveluiden verkkokauppa. Järjestäytyneen rikollisuuden tulevaisuuden uhkat esitettiin kuviossa 6.

Käsiteltyjen uhkien osalta on havaittavissa niistä löytyvän huomattavan monia liityntäpintoja sekä keskinäisiä kytköksiä toisiinsa. Uhkien yksittäisen tarkastelun ja niiden analysoinnin lisäksi, turvallisuusympäristötietoisuuden kannalta on oleellista ymmärtää myös niitä yhdistäviä tekijöitä ja niiden läpileikkaavuutta sekä pohtia muodostuvia uhkaskenaarioita sekä mahdollisia yhteisvaikutuksia. Tämän kaltaisella ajattelulla päästään lähemmäs erilaisten uhkatekijöiden yhteenliittymää eli hybridivaikuttamista.

Sisäistä turvallisuutta ja turvallisuusympäristöä koskevissa dokumenteissa hybridivaikuttaminen nousee kattavasti esiin ja sitä voitaisiinkin kuvata eräänlaisena uhkailmiönä, koska sille ominaiseen tapaa, se on erittäin vaikeasti hahmotettava ja ennakoitava uhkatekijä, jonka merkitystä yhteiskunnan turvallisuuden kannalta on tällä hetkellä huomattava. Hybridivaikuttamisessa keskeistä on suunnitelmallinen ja usein jatkumona tapahtuva vahingollinen vaikuttaminen, jossa erilaisia keinoja monimuotoisesti yhdistelemällä vaikutetaan toiminnan kohteena olevan haavoittuvuuksiin omien tavoitteidensa saavuttamiseksi. Hybridivaikuttaminen halutaan lähtökohtaisesti toteuttaa peitellysti tai ainakin niin, että se on kiistettävissä. Keinovalikoima on laaja, koostuen poliittisesta, diplomaattisesta ja taloudellisesta vaikuttamisesta aina sotilaallisiin keinoihin. Hybridivaikuttamisen keskeisiä työkaluja ovat jo mainitut informaatio- ja kybervaikuttaminen, yhdessä tai erikseen, käyttämällä niitä sujuvasti digitaalista verkkoa ja/tai sosiaalisen median kanavia hyödyntäen. Kuten jo aiemmin asiaa sivuttiin, tarpeen mukaan hybridivaikuttamista voidaan kohdentaa laajamittaisesti sähkön- ja energiansaantiin tai kyberympäristöön ja tietojärjestelmien toimintaan voidaan vaikuttaa fyysisesti rakenteita tuhoamalla, josta esimerkkinä tietoliikennekaapelin katkaiseminen tai vaikkapa viestintäverkkoa ylläpitävän telemaston räjäyttäminen. Hybridivaikuttamisen konkreettisempana muotona voidaan tarvittaessa käyttää ostopalveluna hankittuja kolmansia osapuolia, kuten järjestäytynyttä rikollisuutta tai terroristeja, esimerkiksi edellä mainittujen tuhotöiden tekemiseen. Kyseisten toimijoiden myötävaikutuksella tai avustuksella, on mahdollista käyttää hallitsematonta muuttoliikettä ja pakolaisia vaikuttamisen välineenä tai toiminnassa voidaan hyödyntää kohdemaassa olevia, vaikuttamisen takana olevan maan omia kansalaisia. Hybridivaikuttamista voidaan toteuttaa myös epidemioiden ja pandemioiden varjolla, kuten on havaittu laajasti tapahtuneen COVID-19 kriisin aikana. Tarkoituksena on horjuttaa kohteena olevan valtion vakautta hyödyntämällä jo olemassa olevaa kriisiä. Yhtenä hybridivaikuttamisen keinona voidaan joissakin tilanteissa käyttää tunnuksettomia sotilaita, joskin se tekee toiminnasta melko näkyvää. Todellisen toimijan hämärtämiseksi, kyseinen palvelu on kuitenkin yhtä lailla ostettavissa edellä mainitulta kolmannelta osapuolelta. Tämä osaltaan vahvistaa aiempaa mainintaa uhkien keskinäisestä yhteydestä sekä useiden eri uhkatekijöiden mahdollisesta hyödyntämisestä monimuotoisesti ja samaan aikaan.

Hybridivaikuttamisessa erilaisia uhkatekijöitä yhdistellen ja uhkamalleja toteuttaen saadaan aikaan kohteen toimintakykyä heikentäviä häiriötilanteita tai jopa vakavia häiriötilanteita, ni-

menomaan tekee siitä merkittävän uhkatekijän. Tällä viitataan sisäisen turvallisuuden rakenteessa ja tietomallissa esitettyyn mainintaan vakavista ja laajoista häiriötilanteista sekä viranomaisten suorituskykyvaatimuksesta, jota kuvattiin kuvioissa 1 ja 2. Hybridivaikuttamisessa käytettävä hyökkäys on mahdollista toteuttaa useasta suunnasta ja monin samanaikaisin keinoin, mikä tekee toiminnan kohteesta erityisen haavoittuvan. Hybridivaikuttamisen kohdalla on huomioitava, että häiriötilanteissa tai varsinkaan vakavissa sellaisessa, turvallisuusviranomaisten toimintakyky itsessään ei riitä yhteiskunnan puolustamiseen, minkä takia hybridiuhkiin varautuminen koskettaa viranomaisten ohella myös elinkeinoelämää ja yrityksiä. Hybridivaikuttamisen näkyvämpi ja tehokkaampi muoto on hybridisodankäynti, jossa hyödynnetään hybridivaikuttamisen keinovalikoimaa, kuitenkin usein paljon voimakkaammin ja usein yhdessä perinteisen sotilaallisen toiminnan kanssa.

Poliisitoiminnan sekä muun viranomaistoiminnan kannalta on oleellista tiedostaa, että turvallisuusympäristön uhka-arvioissa erilaiset hybridiuhkat näyttäytyvät vahvoina ja arvioiden mukaan Suomi tulee pysymään aktiivisena hybridivaikuttamisen kohteena myös tulevaisuudessa. Viranomaisille ja erityisesti poliisille se aiheuttaa huomattavia haasteita toiminta- ja suorituskykyvaatimuksien osalta, mikä edellyttää parempaa tietoisuutta hybridivaikuttamisesta ja sen merkityksestä kriittisenä uhkatekijänä yhteiskunnan turvallisuudelle. Hybridiuhkien aiheuttamat haasteet poliisille näyttäytyvät monin eri tavoin ja toteutuessaan niiden vaikutukset voivat ulottua poliisin moniin eri toimintoihin väkivaltaisista levottomuuksista aina kriittisten kohteiden sabotaasiin ja moniulotteisiin kyberhyökkäyksiin. Kun huomioidaan, että hybridivaikuttamisen välineenä voidaan hyödyntää järjestäytynyttä rikollisuutta tai terroristisia toimijoita, tekee se hybridiuhkiin vastaamisesta vielä sitäkin haastavampaa.

Kansalliseen riskiarvioon perustuvan uhkien tarkastelun ohella, otin mukaan myös EU:n turvallisuusstrategian, jossa esiteltiin EU:n turvallisuuden keskeiset strategiset prioriteetit sekä tehtyihin uhka-arvioihin perustuvat uhkatekijät koko EU:ssa. Turvallisuusstrategian sisältö esitettiin kuviossa 7. Mainittuja turvallisuuden kehittämisen prioriteetteja ovat tulevaisuuden kestävä turvallisuusympäristö, kehittyvien uhkien torjunta, eurooppalaisten suojeleminen terrorismilta ja järjestäytyneeltä rikollisuudelta sekä vahva eurooppalainen turvallisuusekosysteemi. Tarkennettuja toimenpiteitä tulisi kohdistaa kriittisen infrastruktuurin turvaamiseen ja resilienssin kasvattamiseen, kyberturvallisuuteen, julkisten tilojen turvaamiseen, verkkorikollisuuden torjuntaan, viranomaistoiminnan nykyaikaistamiseen, laittoman verkkosisällön torjuntaan, hybridiuhkien torjuntaan, terrorismin ja radikalisoitumisen sekä järjestäytyneen rikollisuuden torjuntaan, yhteistyöhön ja tiedonvaihtoon, vahvoihin ulkorajoihin, tutkimuksen ja innovatiivisuuden vahvistamiseen sekä taitojen ja tietoisuuden lisäämiseen.

EU:n turvallisuusstrategia osaltaan alleviivasi tässä työssä esitettyjä asioita turvallisuusympäristön muutoksesta ja siinä ilmenevistä uhkista. Samalla se linjaa turvallisuusuhkien monimuo-

toisuutta ja niiden vaikutusta yhteiskuntaan ja ihmisiin. Kohdennettujen toimenpiteiden merkitystä uhkien torjunnassa korostetaan, mikä tarkoittaa turvallisuustoimintojen kehittämistä kansainvälisesti ja kansallisesti kuin myös laaja-alaisessa yhteistyössä eri sektoreiden kesken. Poliisitoiminnassa tulisi aiempaa tehokkaammin panostaa uusien uhkatekijöiden sekä kasvavan rikollisuuden torjuntaan, mikä vaatii uusia välineitä ja työkaluja järjestäytyneen rikollisuuden ja terrorismin torjuntaan niin fyysisessä kuin digitaalisessa ympäristössä. Turvallisuutta koskevan tietoisuuden kasvattaminen ja esimerkiksi tietoturvallisuuteen liittyvän osaamisen kehittäminen nähdään keskeisenä tekijänä resilienssin rakentamisessa niin yhteiskunnassa kuin yrityksissä ja yksilötasolla. Uuden turvallisuusstrategian avulla halutaan luoda perusta koko EU:n kattavalle turvallisuusekosysteemille, mikä pohjautuu ymmärrykseen yhteisestä vastuun jakamisesta, jossa yhteiskunnan eri toimijoiden ja kansalaisten on täytettävä oma velvollisuutensa turvallisuuden kehittämiseksi. Turvallisuuskysymyksiä on tarkasteltava aiempaa laajemmin ja unohdettava fyysisen ja digitaalisen toimintaympäristön rajapinnat, sillä nykyisessä turvallisuusympäristössä turvallisuutta tulee tarkastella kokonaisuutena.

EU:n turvallisuusstrategiassa esitetyt näkemykset kertovat turvallisuusympäristön ja uhkien globalisoitumisesta sekä turvallisuusajattelun kokonaisvaltaistumisesta. Poliisitoiminnassa kansainvälinen kehitys näyttäytyy yhä vahvempana monin eri tavoin, joten poliisien turvallisuusympäristötietoisuuden kehittämisessä tulee jossain määrin huomioida myös turvallisuusympäristön ja uhkien globaali ulottuvuus.

Opinnäytetyön kolmantena kokonaisuutena tutkin yhteiskunnan varautumista turvallisuusuusympäristön uhkia kohtaan. Osion merkitys tämän työn kokonaisuuden kannalta on oleellinen, sillä mahdollisessa yhteiskuntaan kohdistuvassa häiriötilanteessa poliisin on ensisijaisena toimijana omalta osaltaan välittömästi reagoitava häiriötilanteen aiheuttamiin vaikutuksiin ja huolehdittava turvallisuuden ylläpitämisestä jopa odottamattomissa ja yllätyksellisissä tilanteissa. Tähän liittyy oleellisesti jo aiemmin mainittu turvallisuusviranomaisten velvoite erityisestä suorituskykyvaatimuksesta tulevaisuuden turvallisuusympäristössä. Yhteiskunnan turvallisuusstrategiaan perustuva varautuminen ja kokonaisturvallisuuden ajattelumalli ovat tärkeä osa ennakointia, koskien erityisesti poliisia, sillä jos uhkia pystytään etukäteen kartoittamaan ja tiedostamaan ja niihin konkreettisesti varautumaan, uhkien toteutumisen mahdollisuus pienenee. Uhkien arvioinnin ja niihin varautumisen tulee olla jatkuvaa ja uhkien muuttuessa, myös hallintakeinoja tulee muuttaa. Varautumisessa, ennakoinnissa ja uhkiin vastaamisessa korostuu niiden muutosnopeus ja yhteiskunnan kasvanut haavoittuvuus, mikä korostaa resilienssin eli sietokyvyn merkitystä. Sellaista tilannetta ei saisi syntyä, jossa esimerkiksi lämpö-, vesi-, tai sähkökatkot johtaisivat yhteiskunnan lamaantumiseen tai kansalaisten henkisen kestävyyden murtumiseen.

Koska viranomaisille ja siten myös poliisille valmiuslain velvoittamana kuuluu sille kuuluvien tehtävien hoitaminen myös häiriötilanteissa ja poikkeusoloissa, eikä poliisi todennäköisesti pysty suoriutumaan yksin, varautumisessa ja ennakoinnissa huomiota on kiinnitettävä eri toimijoiden ja sektoreiden rajapinnoissa oleviin riskeihin ja yhteistoimintamahdollisuuksiin. Toimintaympäristön muutostrendien ja turvallisuusympäristön uhkien seuraaminen sekä erilaisten skenaarioiden luominen ja toteuttaminen yhdessä, parantaa yhteistä toimintakykyä erilaisissa odottamattomissa tilanteissa. Valmius ja toimintakyky odottamattomiin ja yllätyksellisiin tilanteisiin rakennetaan normaaliolojen aikana, mikä poliisin kohdalla tarkoittaa varautumisvelvoitteiden huomioimista osana päivittäistä toimintaa. Tätä voidaan kehittää varautumiseen liittyvää tietoisuutta lisäämällä ja turvallisuusajattelua kasvattamalla. Varautuminen sisältää myös ajantasaisen tilannekuvan ylläpitämisen turvallisuusympäristön uhkista, sillä valtionjohdolla ja viranomaisilla on oltava luotettavaa strategista, operatiivista sekä taktisen tason tietoa päätöksenteon tueksi häiriötilanteen eskaloituessa.

Varautumista koskevan koulutuksen lisääminen, kokonaisturvallisuuden merkityksen ymmärtäminen ja sen kytkeminen poliisin päivittäiseen toimintaan mahdollistaa ennakoinnin ja paremman operatiivisen toimintakyvyn erilaisissa ja odottamattomissa häiriötilanteissa. Reaaliaikaisen tilannetietoisuuden ohella, on muutettava myös ajattelu- ja toimintatapoja, mikä poliisihallinnossa tarkoittaa varautumiseen liittyvän ajattelun omaksumista ja sen sisällyttämistä poliisin koulutukseen sekä operatiiviseen toimintaan. Osana yleistä varautumista, kävin läpi viranomaisten toimintakykyyn ja varautumiseen liittyvää KIVI-hanketta, koska sillä nimenomaan poliisitoiminnan kannalta on erityinen merkitys. KIVI-hankkeen tarkoituksena on ollut kriittisen infrastruktuurin palveluntuottajien ja viranomaisten ennakoinnin ja varautumisen tukeminen ihmisen aiheuttamissa elintärkeään infrastruktuuriin kohdistuvissa vakavissa häiriötilanteissa, keskittyen erityisesti julkisen ja yksityisen sektorin keskinäisriippuvuuksien tunnistamiseen monimutkaisessa kaupunkimaisessa toimintaympäristössä.

Turvallisuusympäristötietoisuuden, varautumisen ja poliisitoiminnan kannalta KIVI-hankkeessa on merkityksellistä se, että siinä tutkittiin kaupunkimaisen kriittisen infrastruktuurin haavoittuvuutta, joko tahallisesti tai tahattomasti aiheutetun, ihmisen tekemän hyökkäyksen seurauksena. Lähestymiskulmana oli häiriötilanteesta aiheutuvien seurausten haitallisuus eikä niinkään häiriötilanteen todennäköisyys. Kaupunkien kriittisen infrastruktuurin havaittiin olevan hyvinkin haavoittuvainen, sillä sitä ei ole alun perin suunniteltu kestämään tahallista hyökkäystä. Keskeisenä suosituksena olikin poikkeuksellisten skenaarioiden luominen myös täysin odottamattomia ja ennalta-arvaamattomia iskuja vastaan, jossa mielikuvituksen monipuolinen hyödyntäminen on enemmän kuin suositeltavaa. Vakavissa häiriötilanteissa saattaa ilmetä useita samanaikaisia ja toisiinsa liittyviä kriisitilanteita, jolloin toimijoilta vaaditaan laajojen kokonaisuuksien ymmärtämistä ja systeemiajattelua. Yhtenä tarkastelun kohteena hankkeessa olikin erityisesti poliisin, pelastustoimen sekä kriittisen infrastruktuurin palveluntuottajien väliset keskinäisriippuvuudet niin häiriötilanteiden aikana kuin niiden jälkeenkin.

Skenaarioiden ja ennen kaikkea mielikuvituksellisten skenaarioiden luominen vaatii kattavaa ymmärrystä turvallisuusympäristön uhkista sekä niiden keskinäisistä kytköksistä, johon jo uhkien käsittelyn yhteydessä viittasin. Häiriötilanteen kriittisten toimijoiden keskinäisriippuvuuksien havaitseminen ja arviointi puolestaan tarkoittaa tiiviistä sidosryhmäyhteistyötä ja sen kehittämistä sekä konkreettista yhteisharjoittelua ja erilaisten häiriötilanteiden kattavaa analysointia. Tällöin voidaan puhua aidosta kokonaisturvallisuuden sisäistämisestä. KIVI-hankkeessa esitetyn näkemyksen mukaan toimintakykyinen ja siten resilientti organisaatio seuraa toimintaympäristön tapahtumia ja sopeuttaa toimintaansa muutosten edellyttämällä tavalla. Nykyisessä ja tulevassa turvallisuusympäristössä poliisiorganisaation ja muiden viranomaisten tulisi siis pystyä tähän haasteeseen vastaamaan.

Poliisitoiminnalle kaupunkioloissa toteutuva häiriötilanne toisi omat haasteensa jo pelkästään yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikosten estämiseksi. Huolimatta häiriötilanteen taustasyystä, poliisin on kuitenkin välittömästi käynnistettävä toimintansa tilanteen hallitsemiseksi ja sen normalisoimiseksi. KIVI-hankkeen skenaarioiden mukaan, esimerkiksi laajamittainen sähkökatko voisi sotkea kaupunkien sisäistä liikennettä ja aiheuttaisi kansalaisissa ylimääräistä liikehdintää, mikä taas synnyttäisi ruuhkia ja onnettomuuksia. Häiriötilanteen kohdistuessa vesihuoltoon, tilanne voisi olla lähes samankaltainen. Kansalaisten ärtymys, turhautuminen ja tiedonhalu voisi johtaa vihaisten joukkojen laajoihin kokoontumisiin tai halu omien etujen turvaamiseen saattaisi aiheuttaa erilaisia järjestyshäiriöitä. Tahallisesti järjestetyssä häiriötilanteessa, kuten hybridivaikuttamisessa, on mahdollista, ettei korjaus- ja avustustoimenpiteitä voida suorittaa turvallisesti ilman poliisia. Resilienssin ja toimintakyvyn varmistamiseksi, poliisin operatiivisessa toiminnassa olisikin syytä varautua myös tilanteisiin, joissa samanaikaisesti esiintyy useita erilaisia ja toisistaan poikkeavia häiriöitä tai ilmiöitä.

Tutkimuksen keskeisenä havaintona nousi esiin Uhkakuvat -kirjassa esitetty toteamus siitä, että turvallisuuden ja uhkien arvioinnin suurin haaste tulevaisuudessa on turvallisuusympäristön kompleksisuuden ymmärtäminen ja edes sen osittainen hallinta, varsinkin kun turvallisuutta yhä enemmän määrittää globaali keskinäisriippuvuus ja sen jatkuva tiivistyminen. Siinä missä yhä kompleksisemmaksi käyvän turvallisuusympäristön ymmärtäminen ei ole helppoa, tulevaisuuden uhkia ennakoitaessa se on yhä välttämättömämpää. Suomen sisäiseen turvallisuuden kehittämiseen olennaisesti vaikuttava Ulko- ja turvallisuuspoliittisen selonteko korostaa kriisinsietokyvyn eli resilienssin merkitystä, jossa keskeistä on kansallisen puolustuskyvyn ja sisäisen turvallisuuden ylläpitäminen. Yhteiskunnassa tulisi laajasti varautua erilaisiin yhteiskunnan hyvinvointiin ja turvallisuuteen vaikuttaviin uhkiin, joita tässäkin tutkimuksessa on käsitelty. Kokonaisturvallisuuden periaatteen mukainen yhteinen varautuminen, suunnittelu ja harjoittelu tulisi toteuttaa laajassa yhteistyössä eri toimijoiden kesken. Poliisitoiminnan osalta se tarkoittaa turvallisuusympäristötietoisuuden lisäämistä ja sen rakentumisen kokonaisvaltaista ymmärtämistä.

Poliisin kokonaisvaltaisen turvallisuusajattelun ja tietoisuuden kasvattaminen on tärkeää, jos todellisuudessa halutaan vastata poliisille asetettuihin velvoitteisiin yhteiskunnan turvallisuuden ylläpitämiseksi nykyisessä turvallisuusympäristössä ja sen muutoksessa. Poliisin on tiedostettava turvallisuusympäristön monimuotoisuus ja kompleksisuus sekä jatkuvasti muuttuvat uhkakuvat. Uhkat voivat näyttäytyä monin eri tavoin ja niiden väliset rajapinnat voivat olla häilyviä. Uhkien havaitseminen ja turvallisuusympäristön käytännön haasteisiin vastaaminen lähtee usein kenttätasolta, mikä asettaa poliisityölle uudenlaisia ja jatkuvasti muuttuvia haasteita. Tämän tutkimuksen perusteella on muodostunut käsitys turvallisuusympäristötietoisuuden kriittisimmistä tekijöistä poliisityön ja kokonaisvaltaisen turvallisuusajattelun kannalta.

Poliisissa turvallisuusympäristötietoisuutta voidaan lähestyä kahdesta erilaisesta tarkastelukulmasta. Turvallisuusympäristön uhkia voidaan tarkastella poliisille kuuluvan yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikollisuuden torjumiseksi ja rikosten tutkimiseksi. Toinen tarkastelun kulma on uhkien merkitys ja vaikutus poliisin operatiiviselle toimintakyvylle. Varautumisen osalta turvallisuusympäristöä voidaan tarkastella poliisille kuuluvan häiriötilanteisiin liittyvän toimintavelvoitteen kautta tai oman operatiivisen toimintakyvyn ylläpitämiseksi.

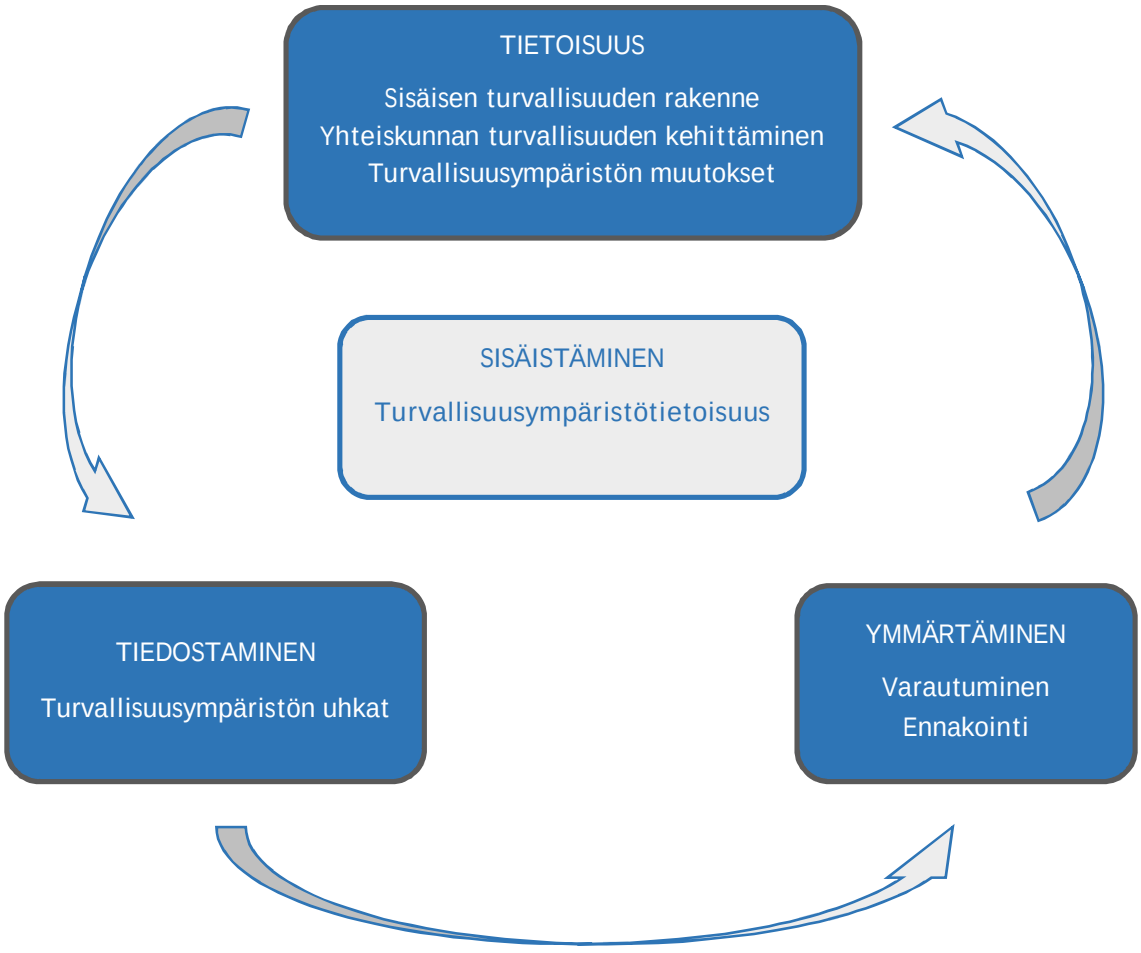
Tutkimuksessa keskeisenä tutkimuskysymyksenä oli selvittää, miten turvallisuusympäristötietoisuus poliisissa rakentuu. Turvallisuusympäristötietoisuuden rakentaminen ja kokonaisvaltaisen turvallisuusajattelun lisääminen tulee aloittaa jo poliisin tutkintokoulutuksessa, mikä mahdollistaa tiedon ja osaamisen hyödyntämisen poliisin eri tehtävissä. Turvallisuusympäristötietoisuuden sisäistäminen vaatii sen kokonaisvaltaista hahmottamista, rakentuen kolmesta merkityksellisestä osiosta.

Ensimmäinen osio koostuu sisäistä turvallisuutta ja yhteiskunnan turvallisuuden kehittämistä koskevan tiedon omaksumisesta. Samalla on huomioitava turvallisuusympäristön muutokset ja niiden vaikutus sisäiseen turvallisuuteen. Tietämys sisäisestä turvallisuudesta ja turvallisuusympäristöstä muodostaa yhteiskuntaa koskevan turvallisuustietoisuuden perustan. Koulutuksen tukena voidaan käyttää sisäistä turvallisuutta ja turvallisuusympäristöä koskevia strategioita, selontekoja tai muita aiheeseen liittyviä dokumentteja.

Toinen turvallisuusympäristötietoisuuden osio koostuu yhteiskunnan turvallisuuteen kohdistuvien uhkien tiedostamisesta sekä niiden syntymekanismin ja rakenteen ymmärtämisestä. Tiedostamalla turvallisuusympäristössä ilmeneviä, poliisitoiminnan kannalta merkityksellisiä uhkia, niihin on mahdollista reagoida tarpeellisten toimenpiteiden kohdistamiseksi ja uhkien torjumiseksi. Koska uhkia voi esiintyä yksittäisinä tai useampien uhkien yhdistelminä, edellyttää se kykyä erilaisten uhkaskenaarioiden luomiseen, mikä on otettava koulutuksessa huomioon. Uhkien tunnistamisen ja niiden tiedostamisen tukena voidaan hyödyntää tehtyjä riskiarvioita ja turvallisuusstrategioita sekä kansallinen että globaali turvallisuusympäristö huomioiden.

Turvallisuusympäristötietoisuuden kolmas osio koostuu varautumisen ja ennakoinnin merkityksestä ymmärtämisestä yhteiskunnan turvallisuuden ja poliisin operatiivisen toimintakyvyn ylläpitämiseksi. Varautumiseen liittyvän koulutuksen yhteydessä on tuotava esiin teknologisen kehityksen ja digitalisoitumisen merkitys yhteiskunnan kriittisen infrastruktuurin haavoittuvuudelle sekä poliisin omalle toimintakyvylle. Varautumisen osalta tulee painottaa sen kokonaisvaltaista merkitystä yhteiskunnan eri toiminnoissa sekä resilienssikyvyn kasvattamiseksi viranomaistoiminnassa.

Turvallisuusympäristötietoisuuden koulutuksellinen rakenne kuvattuna kuviossa 8.



Kuvio 8: turvallisuusympäristötietoisuus Poliisiammattikorkeakoulussa

Lähteet

Painetut

Eskola, J. & Suoranta, J. 2001. Johdatus laadulliseen tutkimukseen. Jyväskylä: Gummerus kirjapaino Oy.

Haikonen, P. 2017. Tietoisuus, tekoäly ja robotit. Tallinna: Printon.

Hari, R. & Järvinen, J. & Lehtonen, J. & Lonka, K. & Peräkylä, A. & Pyysiäinen, I. & Salenius, S. & Sams, M. & Ylikoski, P. 2015. Ihmisen mieli. Tallinna: Printon Trükikoda.

Hiltunen, E. 2012. Matkaopas tulevaisuuteen. Helsinki: Talentum.

Hirsjärvi, S. & Remes, P. & Sajavaara, P. 2014. Tutki ja kirjoita. Porvoo: Bookwell Oy.

Iloniemi J. & Limnéll J. 2018. Uhkakuvat. Jyväskylä: Docendo Oy.

Juvonen, M. & Korhonen, H. & Ojala, V-M. & Salonen, T. & Vuori, H. 2005. Yrityksen riskienhallinta. Suomen vakuutusalan koulutus ja kustannus Oy. Helsinki: Yliopistopaino.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylän ammattikorkeakoulun julkaisuja. Jyväskylä: Juvenes Print.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylän ammattikorkeakoulun julkaisuja. Jyväskylä: Juvenes Print.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Ojasalo, K. & Moilanen T. & Ritalahti J. 2009. Kehittämistyön menetelmät - Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro Oy.

Poliisiammattikorkeakoulu. Alkiora, P. & Himberg, K. & Häikiö, A. & Jukarainen, P. & Kankaanranta, T. & Kemppainen, P. & Koivuniemi, T. & Laitinen, K. & Leppänen, A. & Muttilainen V. & Nerg, P. & Piiroinen, T. & Pylväs, K. & Rajamäki, J. & Suvantola, L. & Talvitie, A. & Toiviainen, T. & Ulkuniemi, K. 2018. Poliisin toimintaympäristö 2018. Poliisiammattikorkeakoulun katsaus 2018. Tampere: Juvenes Print - Suomen Yliopistopaino Oy.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällön analyysi. Jyväskylä: Gummerus kirjapaino Oy.

Sähköiset

Anttila, P. 2014. Metodix. Tutkimisen taito ja tiedon hankinta. Viitattu 6.11.2020. https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Elinkeinoelämän keskusliitto. 2016. Elinkeinoelämän yritysturvallisuusmalli. Viitattu 27.9.2020. https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

European Commission. 2020. EU Security Union Strategy. Viitattu 8.10.2020. https://ec.europa.eu/home-affairs/what-we-do/policies/security-union-strategy_en

Europol. 2017. Serious and organised crime threat assessment - Crime in the age of technology. Viitattu 22.11.2020. https://www.europol.europa.eu/socta-report

Hallintovaliokunta. 2017. Valiokunnan mietintö sisäisen turvallisuuden selonteosta. HaVM 5/2017 vp. 65. Viitattu 17.10.2020. https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/HaVM_5+2017.aspx

Keränen, J. & Molarius, R. & Heikkilä, A-M. & Poussa, L. & Partanen, J. 2016. Varautumisen kehitystarpeet turvallisessa yhteiskunnassa. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 12/2016. Viitattu 24.10.2020. https://tietokayttoon.fi/documents/10616/2009122/12_Varautumisen+kehitystarpeet+turvallisessa+yhteiskunnassa.pdf/bb4b6c20-173a-451e-8cfa-73c657fc2b70?version=1.0

Ossi Heino, O. & Jukarainen, P. & Kalalahti, J. & Kekki, T. & Mansikkamäki, S-T. & Takala, A. & Verho, P. 2019. Kriittisen infrastruktuurin haavoittuvuus ja viranomaisten toimintakyky. Viitattu 22.10.2020. https://www.kivihanke.fi/julkaisut-ja-tuotokset/

Poliisihallitus. 2019. Järjestäytyneen rikollisuuden torjunnan käsikirja. Viitattu 22.8.2020. https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/79346_JR-kasikirja_nettiversio.pdf?242c71e50d1cd888

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisu 22/2017. Viitattu 3.10.2020. https://julkaisut.valtioneuvosto.fi/handle/10024/80013.

Sanastokeskus TSK. 2017. Kokonaisturvallisuuden sanasto. Viitattu 17.10.2020. https://turvallisuuskomitea.fi/materiaalit/kokonaisturvallisuuden-sanasto/

Sisäministeriö. 2017. Hyvä elämä - turvallinen arki. Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta. Viitattu 22.8.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80782/sisaisen-turvallisuuden-strategia-verkko.pdf

Sisäministeriö. 2019. Kansallinen riskiarvio. Viitattu 16.8.2020. https://intermin.fi/julkaisut/julkaisu?pubid=URN:ISBN:978-952-324-245-6

Sisäministeriö. 2020. Väkivaltaisen ekstremismin tilannekatsaus 2020. Arvio väkivaltaisen ekstremismin tilanteesta Suomessa vuonna 2019 ja kehityksen suunta. Sisäministeriön julkaisu 2020:8. Viitattu 18.10.2020. https://julkaisut.valtioneuvosto.fi/handle/10024/162174

Sisäministeriö 2020. Sisäisen turvallisuuden selonteko. Hankkeet ja lainvalmistelu. Viitattu 19.8.2020. https://intermin.fi/hankkeet/hankesivu?tunnus=SM048:00/2019

Sitra. 2019. Megatrendit 2020. Viitattu 6.10.2020. https://www.sitra.fi/julkaisut/megatrendit-2020/

Suojelupoliisi. 2019. Kansallisen turvallisuuden katsaus. Viitattu 16.10.2020. https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/78653_20191205_Supo_kansallinen_turvallisuus_web.pdf?f546eb9c6979d788

Suomen Riskienhallintayhdistys. 2013. PK-RH-riskienhallinta. Viitattu 4.10.2020. https://pk-rh.fi.

Tiimonen, H. & Nikander, M. 2016. Sisäisen ja ulkoisen turvallisuuden keskinäisriippuvuus. Sisäministeriön julkaisu 34/2016. Viitattu 11.10.2020. https://julkaisut.valtioneuvosto.fi/handle/10024/79229

Turvallisuuskomitea. 2016. Katsaus hybridiuhkiin ja niiden vaikutuksiin. Viitattu 23.9.2020. https://turvallisuuskomitea.fi/katsaus-hybridiuhkiin-ja-niiden-vaikutuksiin/

Turvallisuuskomitea. 2017. Turvallinen Suomi 2018. Tietoja Suomen kokonaisturvallisuudesta. Viitattu 26.9.2020. https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/

Turvallisuuskomitea. 2017. Yhteiskunnan turvallisuusstrategia. Viitattu 26.7.2020. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Valtioneuvosto. 2020. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko. Viitattu 5.11.2020. https://julkaisut.valtioneuvosto.fi/handle/10024/162513

Valtioneuvoston kanslia. 2012. Suomen turvallisuus- ja puolustuspolitiikka 2012. Valtioneuvoston kanslian julkaisusarja 5/2012. Viitattu 4.10.2020. https://vnk.fi/documents/10616/622970/J0512_Suomen+turvallisuus-+ja+puolustuspolitiikka+2012.pdf/b534174a-13bc-4684-beb0-a093be30ce2a?version=1.0

Julkaisemattomat

Khan, M. 2017. Poliisiammattikorkeakoulu. Luento ja luentomateriaali 19.10.2017.

Sisäministeriö. 2020. Sisäisen turvallisuuden selonteko. Luonnos 18.6.2020.

Sisäministeriö. 2020. Sisäisen turvallisuuden selonteko. Valmisteluasiakirja.

Kuviot