Kansainvälisestä yhteistyöstä aiheutuvat vaatimukset ministeriöiden turvallisuustoiminnalle fyysisen turvallisuuden osalta

Kansainvälisen turvallisuusluokitellun tiedon käsittely ja säilyttäminen ministeriöissä

Turvallisuusjohdon koulutusohjelma

Tutkielma

Pekka Järvi

Puolustusministeriö

Helsinki 2017

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Suomi toimii yhteistyössä kaikkien Euroopan turvallisuutta edistävien kumppanien ja organisaatioiden kanssa. Suomi on mukana yhä kansainvälistyvämmässä yhteistoiminnassa eri valtioiden ja erilaisten kansainvälisten organisaatioiden kanssa. Valtiot ja organisaatiot luovuttavat yhteistyöhön liittyen toisilleen jatkuvasti turvallisuusluokiteltua tietoa ja antavat eritasoisia järjestelmiä toiselle käytettäväksi.

Tiedon luovuttajan tulee voida varmistua, että sen luovuttamaa tietoa käsitellään ja säilytetään vaatimustenmukaisella tavalla, jotta yhteistyöhön liittyvä luottamuksellisuus voi toteutua. Nato ja EU ovat määritelleet, miten niiden turvallisuusluokiteltua tietoa pitäisi suojata. Muiden organisaatioiden ja valtioiden tietoa suojataan Suomessa lähtökohtaisesti kuten kansallista turvallisuusluokiteltua tietoa.

Tämän tutkimuksen tavoitteena on löytää edellä mainitut kansainvälisen yhteistyön asettamat keskeisimmät vaatimukset ministeriöille ja muille Suomen viranomaisille kansainvälisen turvallisuusluokitellun tiedon käsittelemiseksi ja säilyttämiseksi. Samalla käsitellään niitä hallinnollisia toimia, jotka tukevat fyysistä turvallisuutta.

Tutkimuksessa tutustuttiin tärkeimpien kansainvälisten yhteistyökumppanien vaatimusdokumentteihin ja kansallisiin vaatimuksiin sekä tehtiin vertailua vaatimusten välillä. Lopuksi tehtiin luettelo asioista, jotka voivat helpottaa turvallisuusalan henkilöstöä fyysisen turvallisuuden suunnittelussa ja toteutuksessa sekä kansainvälisten yhteistyökumppaneiden tarkastuksiin valmistautumisessa.

Avainsanat: Kansainvälinen yhteistyö, kansainvälinen turvallisuusluokiteltu tieto, fyysinen turvallisuus

Abstract

Finland is working in cooperation with all partners and organizations that contribute to Europe's security. Finland is involved in internationally expanding cooperation with various countries and various international organizations. States and organizations exchange continuously classified information and provide varying levels of systems for use in another.

The originator must be able to ensure that its release is handled and stored compliant manner so that confidentiality can be achieved. Nato and the EU have defined how the classified information should be protected. Other organizations and states information is protected in Finland, in principle, as a national classified information.

The aim of this study is to identify the key requirements of the international cooperation to the ministries and other Finnish authorities to handle and store the international classified information. At the same time dealing with those administrative activities that support physical security.

The study explored the major international partner´s requirement documents, national standards and made a comparison between the requirements. Lastly a list of things was made that can make it easier for security staff to plan and implement the physical security, as well as preparing themselves for inspections by international partners.

Keywords: International cooperation, international classified information, physical security

Sisällysluettelo

1 Johdanto

1.1 Tutkimuksen tausta ja lähtökohdat

Suomi toimii yhteistyössä kaikkien Euroopan turvallisuutta edistävien kumppanien ja organisaatioiden kanssa. Edellä mainittuihin kuuluvat etenkin Etyj, pohjoismainen yhteistyö, EU sekä Nato. Suomi, kuten myös Ruotsi, on saavuttanut tasannevaiheen suhteessaan Pohjois-Atlantin liittoon olematta varsinainen jäsen. Tämän sotilaallisen ja diplomaattisen tason lähentymisen kautta Suomella on huomattavan korkea yhteistoimintakyky Naton kanssa. Ratkaisemattomia käytännön tason ongelmia olisi todennäköisesti varsin vähän, jos Suomi päättäisi hakea Naton jäsenyyttä. (Ulkoasiainministeriö, 2016 5-6.)

Suomi on mukana yhä kansainvälistyvämmässä yhteistoiminnassa eri valtioiden ja erilaisten kansainvälisten organisaatioiden kanssa. Valtiot ja organisaatiot luovuttavat yhteistyöhön liittyen toisilleen jatkuvasti turvallisuusluokiteltua tietoa ja antavat eritasoisia järjestelmiä toiselle käytettäväksi.

Suomi on sitoutunut valtiosopimuksissa toteuttamaan tietoturvallisuustoimia sellaisen sopimusosapuolen turvallisuusluokitellun tiedon suojaamiseksi, joka on sopimuksen mukaisesti luovutettu Suomeen. Näiden velvoitteiden yleiseksi toteuttamiseksi on säädetty laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004 muutoksineen). (NSA 2016, 4.) Toisen osapuolen turvallisuusluokiteltu tieto ja järjestelmät tulee kyetä suojaamaan vaatimusten mukaisesti tai yhteistoiminnalta puuttuu toimintamahdollisuudet. Myös Suomen ministeriöiden tulee pystyä vastaamaan näihin vaatimuksiin, mikäli ne aikovat jatkaa hyvin alkanutta yhteistyötä.

Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon visio, Suomi 2025:n mukaan Suomen turvallisuuden ja hyvinvoinnin kannalta tavoiteltavaa on turvallinen ja vakaa kansainvälinen toimintaympäristö, jossa valtioiden, yritysten ja ihmisten toimintaa säätelevät kansainvälinen oikeus ja sille

rakentuvat yhteisesti sovitut säännöt, oikeudet ja velvollisuudet (Valtioneuvoston kanslia 2016, 8).

Tiedon omistajat tarkistavat säännöllisesti asettamiensa vaatimusten toteutumisen yhteistyökumppaneihin kohdistuvilla tarkastuksilla tai auditoinneilla. Tarkastuksissa todennetaan käytännön toimenpitein, miten hyvin vaatimukset on toteutettu. Tarkastuksista laadittuihin raportteihin kirjataan tarkastuskohteessa havaitut puutteet, jotka tulee saattaa kuntoon viivytyksettä. Vaatimuksen laiminlyöminen saattaa aiheuttaa sen, että tietoa ei enää luovuteta ministeriölle ennen kuin vaatimus on toteutettu.

Tässä tutkielmassa selvitetään yhteistyön ja yhteistyöhön luovutetun tiedon sekä tiedon käsittelyyn käytettävien järjestelmien asettamia vaatimuksia ministeriöiden fyysisen turvallisuuden ratkaisuille. Järjestelmien vaatimuksia käsitellään niiden sisältämän tiedon turvallisuusluokan perusteella.

Tutkimuksen tarkoituksena on helpottaa turvallisuusjohdon ja –asiantuntijoiden turvallisuussuunnittelua ja fyysisen turvallisuuden toteuttamista kokoamalla yhteen tärkeimpien toimijoiden vaatimuksia yhdessä kansallisten vaatimusten kanssa. Työ voi helpottaa erityisesti niitä ministeriöitä, jotka ovat vasta aloittamassa kansainvälisen yhteistyön tuottamien asiakirjojen käsittelyä ja säilyttämistä. Tutkimustyö on osa Aalto Pro:n turvallisuusjohdon koulutusohjelmaa.

Tutkija työskentelee itse puolustusministeriön turvallisuuspäällikkönä. Vastuualueenaan tutkijalla on ministeriön sisäisen turvallisuuden johtaminen ja sen eri osa-alueiden yhteensovittaminen ja koordinointi. Kansainvälisen turvallisuusluokitellun tiedon fyysisen turvallisuuden kokonaisuudet kuuluvat yhtenä osana ministeriön sisäiseen turvallisuuteen.

Idea tutkimukselle saatiin valmistauduttaessa EU:n ja Naton tarkastuksiin. Tarkastuksiin valmistauduttaessa verrattiin kansainvälisten vaatimusten toteutumista, mikäli kansalliset vaatimukset toteutettiin. Tärkeimpien lähteiden ja dokumenttien kokoaminen yhteen tutkimukseen katsottiin helpottavan mahdollisesti muiden ministeriöiden vastaaviin tarkastuksiin valmistautumista.

Tutkimuksen työelämän valvojana toimi puolustushallinnon turvallisuusjohtaja Juha Pekkola ja AaltoPro:n asettamana valvojana Vesa Valtonen Turvallisuuskomitean sihteeristöstä.

1.2 Tutkimusongelma

Tutkimus on kartoittava. Tutkimuksessa etsitään vastuksia jäljempänä esitettäviin kysymyksiin. Tutkimus on osittain myös selittävä ja kuvaileva, koska siinä pohditaan erilaisten kansainvälisten määräysten ja vaatimusten suhdetta toisiinsa ja vastaavasti kansallisiin määräyksiin ja vaatimuksiin.

Tutkimuksen tarkoituksena on selvittää:

- Mitkä ovat ne yleisimmät kansainvälisen yhteistyön kumppanit, joiden fyysisen turvallisuuden määräykset ja vaatimukset tulee täyttää, jotta yhteistyön edellytykset täyttyvät? Näiden toimijoiden lisäksi on vielä pienempiä toimijoita, joiden vaatimukset todennäköisesti täyttyvät samalla.
- Mitä nämä eri määräykset ja vaatimukset ovat?
- Miten määräykset ja vaatimukset tulee toteuttaa ja miten ne suhtautuvat kansallisiin määräyksiin ja vaatimuksiin?
- Miten kansainväliset määräykset ja vaatimukset täytetään, kuka voi antaa todistuksen vaatimusten täyttymisestä?

Olettamuksena tutkimukselle on, että toteuttamalla kansalliset fyysisen turvallisuuden vaatimukset, saadaan kansainvälisistä vaatimuksistakin tärkein osa toteutettua.

Tutkimuksessa kootaan samaan dokumenttiin tärkeimpien kansainvälisten yhteistyökumppaneiden vaatimuksia yhdessä kansallisten vaatimusten kanssa. Työn on tarkoitus auttaa fyysisen turvallisuuden suunnittelua ja valmistautumista kansainvälisten yhteistyökumppaneiden tarkastuksiin ja auditointeihin.

Tutkimuksessa käsiteltävistä dokumenteista on poimittu niiden fyysistä turvallisuutta koskevista osista oleellisimmat. Lukijan tulee tutustua itse dokumentteihin, mikäli hän haluaa saada tarkempaa tietoa fyysisen turvallisuuden vaatimuksista.

1.3 Tutkimusmenetelmä

Tutkimuksessa on tarkoitus selvittää, minkälaista kirjallista aineistoa tutkimuksen aiheena olevasta asiasta on olemassa ja samalla kuvailla ja selittää saatuja tuloksia. Tavoitteena on löydetyn tiedon eli erilaisten vaatimusdokumenttien merkityksen ymmärtäminen ja dokumenttien vertailu sekä tärkeimpien vaatimusten kokoaminen yhteen. Tutkimus toteutetaan kirjallisuus- ja asiakirjatutkimuksena, jota täydennetään tarvittavin osin asiantuntijahaastatteluin.

Tiedonkeruumenetelmänä käytetään avoimia, strukturoimattomia haastatteluja täydentämään kirjallisuus- ja asiakirjatutkimuksessa syntyneitä kysymyksiä. Haastattelujen avulla varmistutaan, miten eräät kirjallisuudessa esitetyt asiat on toteutettu Suomessa. Haastateltavat valitaan kansallisen turvallisuusviranomaisen tehtävissä työskentelevien henkilöiden joukosta.

Tutkimustyö on kvalitatiivinen. Lähtökohtana kvalitatiivisessa tutkimuksessa on todellisen elämän kuvaaminen, joka tutkimuksessa on olemassa olevan tiedon kuvaaminen. Tutkimus on luonteeltaan mahdollisimman kokonaisvaltaista tiedonhankintaa, todellisista aineistoista. (Hirsjärvi, Remes & Sajavaara 2009, 161-164.)

Tutkimuksen lähestymistapa on fenomenologinen. Lähestymistavassa pyritään löytämään tutkimuskohteesta sen keskeinen olemus käyttäen hyväksi tutkijan itsensä ja tutkijan omien kokemusten ymmärryksen muodostumista. Tutkimuskohdetta kuvataan ja analysoidaan tutkimusprosessin aikana muodostuneiden kokemusten avulla. (Jyväskylän Yliopisto 2015.)

1.4 Tutkielman rajaus

Kansainvälisen yhteistyön osalta tutkimus on rajattu koskemaan EU:ta ja Natoa. Muista toimijoista on tutkimuksessa vain viitteitä mutta sen laajemmin ei niiden vaatimuksia ole käsitelty.

Kansainvälisen tiedon osalta tutkimus on rajattu koskemaan vain turvallisuusluokitellulle tiedolle asetettuja vaatimuksia tiedon käsittelyn ja säilyttämisen osalta.

Fyysisen turvallisuuden osalta tutkimus on rajattu koskemaan lähinnä toimitilaturvallisuuden keinoja eli tilojen rakenteellisia ja teknisiä vaatimuksia. Hallinnollista keinoista on mukaan otettu keskeisimmät keinot, jotka tukevat toimitilaturvallisuutta.

Fyysisen turvallisuuden vaatimukset on lisäksi rajattu koskemaan vain yhteistyökumppanin Suomelle esittämiä vaatimuksia, ei Suomen yhteistyökumppanille esittämiä.

1.5 Tutkimuksen rakenne

Tutkimus koostuu seitsemästä pääluvusta. Ensimmäinen luku toimii tutkimuksen johdantona, jossa alkuun esitellään tutkimuksen taustaa ja lähtökohtia. Lähtökohtien jälkeen pohditaan tutkimusongelmaa ja –kysymystä. Tutkimusongelman jälkeen esitellään tutkimusmenetelmä ja tutkimukseen tehdyt rajaukset. Lopuksi avataan keskeisimmät tutkimuksessa käytetyt käsitteet niiden käsitteiden osalta, joita ei olla tarkemmin avattu itse tutkimuksessa.

Toisessa luvussa tutkitaan ministeriöiden kansainvälisen yhteistyön fyysiselle turvallisuudelle asettamia vaatimuksia kansainvälisten yhteistyökumppaneiden dokumenttien pohjalta. Alkuun esitellään Suomen Kansallinen turvallisuusviranomainen (NSA). NSA:n esittelyn jälkeen tutkitaan kansainväliseen yhteistyöhön liittyviä tärkeimpiä kansainvälisiä organisaatioita. Lopuksi esitetään ja pohditaan Naton ja EU:n tärkeimmät fyysisen turvallisuuden vaatimuksia kuvaavat dokumentit.

Kolmannessa luvussa tutkitaan ja pohditaan kansallisia vaatimuksia turvallisuusluokitellun tiedon käsittelemiseksi ja säilyttämiseksi. Asiakirjojen kohdalla pohditaan niiden sisältöä fyysisen turvallisuuden kannalta ja sitä, miten asiakirjoja voidaan käyttää hyväksi määriteltäessä kansainvälisen yhteistyön vaatimuksia.

Neljännessä luvussa tutkitaan tärkeimpiä kansallisia asiakirjoja, jotka on annettu kansainvälisien asiakirjojen perusteella. Tarkemmin sanottuna, millaista ohjeistusta Suomi on antanut Naton ja EU:n vaatimusten pohjalta.

Viidennessä luvussa on vertaillaan esitettyjen asiakirjojen pohjalta eräitä tärkeimpiä seikkoja, jotka esiintyvät kaikissa dokumenteissa. Vertailun jälkeen

kootaan karkea luettelo asioista, jotka tulisi ainakin ottaa huomioon suunniteltaessa fyysisen turvallisuuden toimia tai valmistauduttaessa tiedon luovuttajan tarkastukseen.

Kuudennessa luvussa tehdään tärkeimmät johtopäätökset sekä esitetään toimenpiteitä tulevaisuuden kehittämiselle. Seitsemännessä luvussa tehdään yhteenveto.

1.6 Keskeiset käsitteet

Asiakirja

Mikä tahansa tallennettu tieto, sen fyysisestä muodosta tai ominaisuuksista riippumatta (Euroopan komissio 2015).

EU:n turvallisuusluokiteltujen tietojen käsittely

Kaikkia mahdollisia toimia, joita EU:n turvallisuusluokiteltuihin tietoihin voidaan kohdistaa niiden elinkaaren aikana. Tällaisia toimia ovat tietojen tuottaminen, rekisteröinti, muokkaaminen, kuljetus, hävittäminen sekä turvallisuusluokan alentaminen ja poistaminen. (Euroopan komissio 2015.)

Fyysinen turvallisuus

Fyysisen turvallisuuden tarkoituksena on turvata organisaatioiden häiriötön toiminta kaikissa olosuhteissa niiden erityistarpeet ja riskit huomioon ottaen. Kukin organisaatio vastaa itse fyysisestä suojauksestaan. (Valtionvarainministeriö 2009.)

Tähän tietoturvallisuuden osa-alueeseen kuuluvat mm:

- kulunvalvonta
- kameravalvonta
- muu tekninen valvonta ja vartiointi
- palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta.

Euroopan komissiossa turvallisuusluokiteltujen tietojen suojaamiseen tähtäävällä fyysisellä turvallisuudella tarkoitetaan sellaisten fyysisten ja teknisten

suojatoimien toteuttamista, joiden tarkoituksena on estää luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin (Euroopan komissio 2015).

Kansainvälinen turvallisuusluokiteltu tieto

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettu erityissuojattava tietoaineisto, jota Suomen on kansainvälisen sopimuksen tai EU:n turvallisuussääntöjen perusteella suojattava. Kansainvälisiä turvallisuusluokiteltuja tietoaineistoja ovat Suomeen toimitetut asiakirjat, aineistot, materiaalit ja näihin sisältyvät tiedot, joihin luovuttaja on tehnyt turvallisuusluokkamerkinnän kansainvälisen tietoturvallisuusvelvoitteen mukaisesti. (NSA 2016, 5.)

Tunkeutumisaika

Aika, jonka arvioidaan tunkeutujalta kuluvan ensimmäisestä tunkeutumisen ilmaisusta varsinaiselle kohteelle pääsyyn (Vahti 8/2008).

Vasteaika

Aika, joka kuluu hälytyksen lähtemisestä vasteen (vartija, poliisi) hälytyspaikalle saapumiseen (Vahti 8/2008).

2 Kansainvälisen yhteistyön vaatimuksia

2.1 Kansallinen turvallisuusviranomainen (NSA)

Suomella on, monien muiden maiden tapaan, oma Kansallinen turvallisuusviranomainen (NSA, National Security Authority), joka hoitaa ja valvoo Suomen kansainvälisiä tietoturvavelvoitteita sekä edistää Suomen kansain- välistä tietoturvayhteistyötä (Turvallisuuskomitea 2012, 118-119).

Kansallisen turvallisuusviranomaisen tehtävät on organisoitu Suomessa niin, että ulkoasiainministeriö toimii lain kansainvälisistä tietoturvallisuusvelvoitteista 4 pykälän mukaan Suomen kansallisena turvallisuusviranomaisena kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa. Puolustusministeriö, Pääesikunta ja suojelupoliisi toimivat määrättyinä turvallisuusviranomaisina (DSA, Designated Security Authority) ja Viestintävirasto kansallisena tietoliikenneturvallisuusviranomaisena (NCSA, National Communications Security Authority). (588/2004, 4§)

Ulkoasiainministeriöön sijoitettu Kansallinen turvallisuusviranomainen ohjaa ja valvoo, että erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti sekä koko valtionhallinnossa, että niitä käsittelevissä yrityksissä ja laitoksissa. Tämä tapahtuu läheisessä yhteistyössä DSA:iden ja NCSA:n kanssa. NSA:n toimivalta ei kuitenkaan koske kansallista turvallisuusluokiteltua aineistoa. (Turvallisuuskomitea 2012, 118-119.)

2.2 Kansainväliseen yhteistyöhön liittyvät kansainväliset organisaatiot

Tässä tutkimuksessa on keskitytty kansainvälisten organisaatioiden osalta vain Naton ja EU:n vaatimuksiin, vaikka Suomi tekeekin aktiivista yhteistyötä myös muiden toimijoiden kanssa. Suomi tekee aktiivista yhteistyötä esimerkiksi pohjoismaiden kanssa ja toimii vuonna 2017 pohjoismaisen puolustusyhteistyön (Nordefco) puheenjohtajamaana, edistäen Pohjoismaiden yhteistoimintakyvyn tiivistämistä ja alueellista turvallisuutta lujittavia toimia.

Valtioneuvoston ohjesäännön mukaisesti kukin ministeriö käsittelee itse oman toimialansa kansainväliset asiat sekä kansainväliset suhteet yleisesti (Valtioneuvosto 2003, 11§).

Suomi on EU:n jäsenmaa ja sen tulee noudattaa EU:n sääntöjä. Neuvoston turvallisuussäännöt (488/2013) on jäsenvaltioiden kannalta keskeisin EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva säädös. Myös muilla EU:n toimielimillä on omia turvallisuussääntöjä, joissa ne ovat sitoutuneet noudattamaan vastaavia turvallisuusvaatimuksia. (NSA 2016, 7.)

Naton turvallisuusluokiteltua tietoa Suomi suojaa lähtökohtaisesti kansallisen lainsäädäntönsä mukaisesti. Naton vaatimukset Suomi joutuu kuitenkin täyttämään, sillä Suomi toteuttaa laajaa ja kehittyvää kumppanuutta Naton kanssa. Naton vaatimusten täyttäminen on myös edellytys, jotta Suomelle voidaan luovuttaa Naton turvallisuusluokiteltua tietoa. Suomi on osallistunut Naton rauhankumppanuusyhteistyöhön jo vuodesta 1994 alkaen. Euroatlanttisen kumppanuusneuvoston jäsen Suomi on ollut sen perustamisesta 1997 lähtien. Walesin huippukokouksessa 2014 Suomi kutsuttiin edistyneenä kumppanimaana mukaan Naton laajennettujen mahdollisuuksien kumppanuusyhteistyöhön. (NAE 2016.)

Suomen Nato-kumppanuutta ohjaavat hallitusohjelma sekä kansalliset ulko-, turvallisuus- ja puolustuspoliittiset linjaukset. Niiden mukaisesti Suomi tekee pitkäjänteistä ja molempia osapuolia hyödyttävää yhteistyötä Naton kanssa. (NAE 2016.)

Sopimuksia laadittaessa määritellään myös ne vaatimukset, joita tiedon käsittelylle ja säilyttämiselle asetetaan. Säännöt koskevat kaikkia sopimuksen allekirjoittaneita osapuolia.

Suomi on allekirjoittanut useiden valtioiden kanssa valtiosopimuksen, joka sitoo Suomea valtiona. Valtiosopimus tarkoittaa kansainvälistä välipuhetta, joka on tehty kirjallisesti valtioiden välillä ja joka on kansainvälisen oikeuden alainen, katsomatta siihen sisältyykö se yhteen tai useampaan toisiinsa liittyvään asiakirjaan ja riippumatta siitä käytetystä nimityksestä. Valtiosopimukseksi katsotaan myös valtion ja kansainvälisen järjestön ja toimielimen välinen sopimus ja kansainvälisten järjestöjen välinen sopimus sekä eräissä poikkeustapauksissa toisen valtion viranomaisten kanssa tehty sopimus. (Lainkirjoittajan opas.)

2.3 NATO DIRECTIVE on PHYSICAL SECURITY (AC/35-D/2001-REV2)

Pohjois-Atlantin liitto (North Atlantic Treaty Organisation) eli Nato perustettiin vuonna 1949 Washingtonissa. Nato tekee paljon yhteistyötä sotilasliittoon kuulumattomien valtioiden kanssa erilaisten kumppanuusohjelmien kautta. Suomi on osallistunut Naton toimintaan vuodesta 1994 rauhankumppanuuden kautta. (Turvallisuuskomitea 2014, 37.)

Naton turvallisuuskomitean direktiivi AC/35-D/2001 fyysisen turvallisuuden vaatimuksista on Naton jäsenmaita velvoittava ja siinä käsitellään seuraavia asioita:

- turvallisuusvaatimukset
- fyysiset turvatoimet
- vähimmäisvaatimukset Naton luokiteltujen tietojen säilytykselle
- teknisiltä hyökkäyksiltä suojautuminen
- viestintä- ja tietojärjestelmien fyysinen turvallisuus. (AC/35-D/2001, 1.)

Naton turvallisuuspolitiikan vaatimusten mukaisesti kaikki tilat, rakennukset, toimistot, huoneet ja muut alueet, joissa Naton turvallisuusluokiteltua tietoa ja aineistoa käsitellään ja säilytetään, on suojattava asianmukaisin fyysisin turvatoimin. Turvatoimien valintaan vaikuttavat:

- tiedon turvallisuusluokitus
- tiedon määrä ja muoto
- henkilöstön turvallisuusselvitykset ja tarve tiedolle

- paikallinen uhka-arvio
- miten tietoa säilytetään. (AC/35-D/2001, liite1, 1.)

Turvallisuusriskienhallinta korostuu, kun valitaan tehokkaimpia ja samalla kustannustehokkaita menetelmiä uhkien torjuntaan ja kompensoidaan haavoittuvaisuuksia yhdistelemällä erilaisia suojaustoimenpiteitä. Tehokkuus saavutetaan parhaiten määrittelemällä fyysiset turvallisuusvaatimukset osana tilojen suunnittelua. Samalla pienennetään kalliiden korjausten tarvetta. (AC/35-D/2001, liite1, 2.)

Fyysinen turvallisuus perustuu Naton ajatuksen mukaan ”puolustuksen syvyyteen”. Fyysisen turvallisuuden toimien osalta voidaan soveltaa niin sanottuja pääperiaatteita, vaikka toimet ovat pääsääntöisesti paikkasidonnaisia. Ensimmäiseksi pitää tunnistaa kohde, joka vaatii suojausta. Tämän jälkeen muodostetaan erilaisia turvallisuustoimia sisältäviä kerroksia, jotka muodostavat ”puolustuksen syvyyden” ja sisältävät viivyttäviä ratkaisuja. Ulommaisen kerroksen turvallisuustoimien avulla määritellään suojattu alue ja estetään luvaton pääsy alueelle. Seuraavan kerroksen toimenpiteillä havaitaan luvaton tunkeutuminen tai sen yritys ja hälytetään vartijat. Sisimmän kerroksen avulla viivytetään tunkeutujaa, kunnes vartijat ehtivät paikalle. (AC/35-D/2001, liite1, 2.) Pääperiaatteiden avulla tunkeutujan tukeutumisaika saadaan pidemmäksi kuin vartijoiden vasteaika ja tiedon joutuminen luvattomiin käsiin saadaan estettyä.

Yksittäisten turvatoimien tehokkuutta on tärkeää uudelleenarvioida säännöllisesti. Samalla arvioidaan myös koko järjestelmän tehokkuutta.

Nato jakaa alueet turva-alueisiin ja hallinnolliseen alueeseen. Turva-alueita on kaksi: Nato Class I Security Area ja Nato Class II Security Area. Hallinnollisia alueita voidaan perustaa turva-alueiden ympärille tai tiloihin, jotka johtavat turva-alueille.

Direktiivi kuvaa minimivaatimukset Naton turvallisuusluokitellun tiedon säilyttämiselle turvallisuusluokittain. Area I:lle ei Natoon kuulumattomilla ole oikeutta ilman saattajaa. Area II:lle voi Natoon kuulumattomat saada oikeuden liikkua ilman saattajaa. Edellä mainittujen alueiden lisäksi direktiivin käsitteissä on vielä tekninen turva-alue, jonka tarkoituksena on estää teknisesti toteutettu salakuuntelu.

Direktiivin liite 1 kuvaa tarkemmin erilaisia tiedon suojaamiseksi vaadittavia turvatoimia Naton turvallisuusluokittain mutta antaa varsin tiukat vaatimukset Natoon kuulumattomien maiden henkilöstölle Naton turva-alueille pääsemiseksi. Taulukossa 1 on esitetty Natossa ja Suomessa käytettävien turvallisuusluokkien vastaavuudet.

Taulukko 1 Naton ja Suomen turvallisuusluokkien vastaavuudet (NSA 2016, 17).

Naton turvallisuusluokka	Lyhenne	Suomen vastaava turvallisuusluokka (tietoturvallisuusasetus)
COSMIC TOP SECRET	CTS	ERITTÄIN SALAINEN / YTTERST HEMLIG
NATO SECRET	NS	SALAINEN / HEMLIG
NATO CONFIDENTIAL	NC	LUOTTAMUKSELLINEN / KONFIDENTIELL
NATO RESTRICTED	NR	KÄYTTÖRAJOITETTU / BEGRÄNSAD TILLGÅNG

Naton direktiivi määrittelee turvallisuustoimien vaatimukset tarkemmin kuin seuraavassa luvussa esitetty EU:n turvallisuussäännöt.

Turvallisuusluokkaa NATO CONFIDENTIAL ja ylempää voidaan käsitellä ja säilyttää vain turva-alueilla. Hallinnollisella alueella voidaan käsitellä ja säilyttää korkeintaan turvallisuusluokkaa NATO RESTRICTED.

Nato edellyttää erityisiä toimenpiteitä tiedon suojaamiselle alkaen turvallisuusluokasta NATO CONFIDENTIAL.

2.4 EU ja EU:n neuvoston turvallisuussäännöt (2013/488/EU)

Euroopan unionin neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU) eli puhekielessä EU:n neuvoston turvallisuussäännöt, määrittelevät miten EU:n turvallisuusluokiteltua tietoa tulee käsitellä ja säilyttää. Euroopan unionin neuvosto

katsoo, että jäsenvaltioiden olisi kansallisten lakiensa ja asetustensa mukaisesti ja neuvoston toiminnan edellyttämässä määrin noudatettava päätöstä, kun niiden toimivaltaiset viranomaiset, henkilöstö tai hankeosapuolet käsittelevät EU:n turvallisuusluokiteltuja tietoja, jotta kaikki osapuolet voivat olla vakuuttuneita siitä, että EU:n turvallisuusluokiteltujen tietojen suojaamisessa noudatetaan vastaavaa tasoa (2013/488/EU, 1).

Neuvoston turvallisuussäännöt on jäsenvaltioiden kannalta keskeisin EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva säädös (NSA 2016).

Artiklassa 8 määritellään fyysinen turvallisuus fyysisten ja teknisten suojatoimenpiteiden toteuttamiseksi niin, että estetään luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin. Toteuttamistoimet on määriteltävä riskienhallintaprosessin perusteella. (2013/488/EU, artikla 8, kohta 1-2.)

Fyysiset turvatoimet on toteutettava kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa EU:n turvallisuusluokiteltuja tietoja käsitellään tai säilytetään. Alueet, joilla säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL tai sitä korkeamman tason EU:n turvallisuusluokiteltuja tietoja, on määriteltävä turva-alueiksi ja toimivaltaisen viranomaisen on hyväksyttävä ne. (2013/488/EU, artikla 8, kohta 3-4.) Suomessa toimivaltainen viranomainen on Viestintävirasto (Tauriainen 2016). EU edellyttää erityisiä toimenpiteitä tiedon suojaamiselle alkaen turvallisuusluokasta CONFIDENTIEL UE/EU CONFIDENTIAL.

EU:n neuvoston turvasääntöjen liitteessä II käsitellään fyysisen turvallisuuden vaatimuksia tarkemmin. Siinä vahvistetaan EU:n turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen käytettävien tilojen, rakennusten, toimistojen, huoneiden ja muiden alueiden fyysistä suojaamista koskevat vähimmäisvaatimukset (2013/488/EU, liite II, luku I).

Fyysisten turvatoimien tarkoituksena on estää luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin:

- Varmistamalla, että tietoja käsitellään ja säilytetään asianmukaisesti.
- Mahdollistamalla henkilöstön luokitus ja pääsy EU:n turvallisuusluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on, ja tarvittaessa henkilöiden turvallisuusselvitysten perusteella.

- Ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet
- Estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä. (2013/488/EU, liite II, luku I.)

Taulukossa 2 on kuvattu EU:n ja Suomen turvallisuusluokkien vastaavuudet.

Taulukko 2 EU:ssa ja Suomessa käytettävien turvallisuusluokkien vastaavuudet (NSA 2016, 8).

Euroopan unionin turvallisuusluokka	EU-lyhenne	Suomen vastaava turvallisuusluokka (tietoturvallisuusasetus)
TRES SECRET UE / EU TOP SECRET	TS-UE/ EU-TS	ERITTÄIN SALAINEN / YTTERST HEMLIG
SECRET UE / EU SECRET	S-UE/ EU-S	SALAINEN / HEMLIG
CONFIDENTIEL UE / EU CONFIDENTIAL	C-UE/ EU-C	LUOTTAMUKSELLINEN / KONFIDENTIELL
RESTREINT UE / EU RESTRICTED	R-UE/ EU-R	KÄYTTÖRAJOITETTU / BEGRÄNSAD TILLGÅNG

EU:n turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi on perustettava kahdentyyppisiä fyysisesti suojattuja alueita tai vastaavia kansallisia alueita:

- hallinnollisia alueita
- turva-alueita, mukaan lukien teknisesti suojatut turva-alueet.

Hallinnollisella alueella voidaan käsitellä EU-R, EU-C ja EU-S –asiakirjoja, jos pääsy turvallisuusluokiteltuihin tietoihin on estetty sivullisilta. EU-S ja EU-C –asiakirjoja voidaan säilyttää vain turva-alueilla. (2013/488/EU, liite II, luku V.)

Kaikkia turvallisuussäännöissä olevia viittauksia hallinnollisiin alueisiin ja turva-alueisiin, teknisesti suojatut turva-alueet mukaan lukien, on pidettävä viittauksina myös niitä vastaaviin kansallisiin alueisiin. (2013/488/EU, liite

II, luku IV.) Jäljempänä luvussa 3.2 esitellyssä Katakri 2015.ssa on kansallisissa vaatimuksissa suorat viittaukset tähän dokumenttiin.

Hallinnollisten alueiden ja turva-alueiden vaatimukset kuvataan luvussa IV. Luvussa kuvataan liikkumista ja pääsyä alueelle, alueen rajaamista ja alueella tehtäviä tarkastuksia. Luku antaa vaatimuksia mutta ei varsinaisia toteuttamismalleja.

Teknisesti suojatuksi turva-alueeksi luku IV kuvaa turva-alueen, joka on salakuuntelulta suojattu. Tavanomaisten turva-alueiden vaatimusten lisäksi kuvataan lisävaatimuksia, jotka teknisesti suojattujen turva-alueiden tulee täyttää.

Turva-alueita ja teknisesti suojattuja turva-alueita voidaan dokumentin mukaan tilapäisesti perustaa myös hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.

2.5 15386/07 EU risk-management process for physical security

EU:n dokumentti 15386/07 EU risk-management process for physical security on ilmestynyt vuonna 2007 ja se laadittiin alun perin työkaluksi EU:n turvallisuusluokitellun tiedon turvajärjestelyjen täytäntöön panemiseksi. Dokumenttia ei ole uusien turvallisuussääntöjen voimaantulon jälkeen päivitetty. Sitä voi edelleen soveltuvin osin hyödyntää turvallisuustyössä etenkin, jos sitä lukee yhdessä voimassaolevien neuvoston turvasääntöjen kanssa. (Erkkilä 2016.)

Dokumentti on laadittu, jotta kyettäisiin saavuttamaan arvioituihin riskeihin riittävä taso EU:n turvallisuusluokitellun tiedon suojaamiseksi mahdollisimman joustavalla tavalla. Dokumentin avulla pisteytetään erilaiset fyysisen turvallisuuden toimet ja saadun pistemäärän perusteella arvioidaan toimien riittävyys. Apuna työssä käytetään dokumentissa esitettyä laskentataulukkoa, johon saadut arvot sijoitetaan sekä vaatimustaulukkoa, josta pisteet saadaan. Loppusumman tulee olla suurempi kuin taulukon minimivaatimus. Lopullinen arviointi tehdään periaatteella, että ”ketju on vain niin vahva kuin sen heikoin lenkki”. (Council of the European Union 2007, 2.)

Menetelmä on vain suuntaa antava ja määrittelyissä auttava, sillä lopulliset ratkaisut tulee aina valita riskienhallinnan kautta löydettyjen riskien perusteella.

Dokumentti ei varsinaisesti ole riskienhallintaa ja sen ohjeistusta vaan etukäteen asetettujen vaatimusten täyttämiseksi vaadittavia ratkaisuja. Dokumentti ei myöskään auta tunnistamaan uhkia, jotka voivat toteutua tietyssä kohteessa. Dokumentissa on esitetty kolme eri riskitasoa (1-3) mutta niitä ei sen enempää sisällössä määritellä.

Dokumentin esittämät EU:n turvallisuusvyöhykkeet ovat turvallisuussääntöjen myötä vanhentuneet. Dokumentti esittää esimerkiksi turvallisuusvyöhykkeiksi Naton mukaisesti EU Security Class 1 ja 2.

Dokumentti auttaa määrittelemään vaadittavat toimet, antamalla tietylle toiminnalle pisteitä vaatimusten täyttämisen perusteella. Dokumentti ei varsinaisesti auta laskemaan tunkeutumisaikaa, vaikka sen tarkoitus selvästi on esitellä ratkaisuja, joilla tunkeutumisaikaa voidaan pidentää. Dokumentissa sen sijaan kyllä esitetään eri ratkaisuissa käytettävät standardit ja niiden vaatimukset. Dokumentissa esitetyt standardit vastaavat pääsääntöisesti Katakri 2015:n standardeja. Poikkeuksen tekee lukkostandardi.

Dokumentti korostaa, kuten Naton dokumentitkin, ”puolustuksen syvyyttä”. Dokumentti on hyvä apuväline suunniteltaessa kohteiden fyysisen turvallisuuden ratkaisuja. Se antaa perusajatuksen siitä, millaisilla ratkaisuilla tunkeutumisaikaa voidaan pidentää.

3 Kansalliset fyysisen turvallisuuden vaatimukset

3.1 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

Asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) säädetään valtionhallinnon viranomaisen asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista.

Asetuksessa tietoturvallisuudesta valtionhallinnossa säädetään 1 pykälässä valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista ja asiakirjojen luokittelun perusteista sekä luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista (681/2010, 1§).

Asetuksen 3§:n mukaan asiakirjan käsittely sisältää myös asiakirjan säilyttämisen.

Asetuksen 5§:ssä mainitaan tietoturvallisuuden perustason toteuttamiseen liittyen fyysisestä turvallisuudesta:

- Tietojen saanti ja käytettävyys on turvattava erilaisissa tilanteissa ja lisäksi on luotava menettelytavat poikkeuksellisten tilanteiden selvittämiseksi.
- Asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja on varmistettava antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja työtehtäviensä hoitamiseksi. Henkilöstön luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla.
- Asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja.

Tiloja koskevat turvallisuusvaatimukset on määritelty §:ssä 14. Siinä mainitaan asiakirjojen säilyttämiseen ja käsittelyyn käytettävien tilojen turvallisuusvaatimuksiin liittyen, että:

- Tilat, joissa säilytetään tai muutoin käsitellään turvallisuusluokiteltuja asiakirjoja, suojataan asianmukaisesti lukituksella, kulunvalvonnalla ja muilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin asiakirjoihin.
- Henkilöt, joille annetaan pääsy tiloihin, joissa säilytetään tai muutoin käsitellään suojaustasoon I tai II kuuluvia asiakirjoja, ovat tunnistettavissa.
- Suojaustasoon I ja II kuuluvat asiakirjat säilytetään sellaisessa kassakaapissa tai muussa lukittavassa kaapissa, holvissa tai tilassa, joka estää luvattoman pääsyn asiakirjaan sisältyviin tietoihin.
- Henkilöt, joille annetaan pääsy arkistoon taikka tietokonekeskukseen tai muihin tietojärjestelmien ylläpidon tai tietoliikenteen toimivuuden kannalta merkityksellisiin tiloihin, joissa säilytetään tai käsitellään suojaustasoon III kuuluvia asiakirjoja taikka suojaustasoon IV kuuluvia valtakunnalliseen henkilörekisteriin talletettuja asiakirjoja, ovat tunnistettavissa.

Asetus on tullut (22§) voimaan 1.10.2010. 23 pykälä määrittelee siirtymisajaksi toimitilojen osalta viisi vuotta asetuksen voimaantulosta, jos toimitilat ovat olleet käytössä asetuksen voimaantulopäivänä. Siirtymäaika koskee myös toimitiloja, jotka on otettu käyttöön asetuksen voimaantulon jälkeen kahden vuoden sisällä. Näin ollen kaikkien valtion virastojen tulee täyttää määräykset lokakuuhun 2017 mennessä.

Asetuksen vaatimukset asiakirjojen suojaamiseksi eivät ole tarkkoja vaan jäävät hyvin yleiselle tasolle. Asetus ei anna vaatimuksia suojaustason III ja IV asiakirjojen säilyttämiselle. Näitä edellä mainittuja vaatimuksia on otettu tarkemmin huomioon seuraavassa luvussa esitetyssä Katakri 2015:ssa.

3.2 Katakri 2015, tietoturvallisuuden auditointityökalu viranomaisille

3.2.1 Katakri 2015 taustaa

Katakri 2015 on viranomaisen auditointityökalu, jota voidaan käyttää arvioitaessa organisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Siihen on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri 2015 ei työkaluna aseta ehdottomia vaatimuksia mutta siihen on koottu vaatimuksia, jotka perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. (Katakri 2015, 3.)

Katakri 2015:n kehittämistyö ja hallinnointi on annettu ulkoasiainministeriössä sijaitsevan Kansallisen turvallisuusviranomaisen (NSA) ja sen alatyöryhmäksi perustetun ohjausryhmän vastuulle. Katakrin ohjausryhmässä pyritään yhtenäistämään kansallisia vaatimuksia muiden maiden vaatimuksia vastaaviksi (Erkkilä 2016). Ohjausryhmään kuuluu edustajia useista eri ministeriöistä ja niiden hallinnonaloilta, toimivaltaiset viranomaiset sekä edustaja Elinkeinoelämän keskusliitosta (Katakri 2015, 3).

Keskeisin kansalliseen lainsäädäntöön perustuva lähde on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), niin kutsuttu tietoturvallisuusasetus, jota noudatetaan Suomessa niin kansallisen kuin kansainvälisen salassa pidettävän tiedon suojaamisessa. Kansainvälisenä lähteenä Katakri 2015:ssa on käytetty EU:n neuvoston turvallisuussääntöjä (2013/488/EU), jotka sisältävät vähimmäisvaatimukset ja perusperiaatteet EU:n turvallisuusluokitellun tiedon suojaamisessa. (Katakri 2015, 3.)

Katakri 2015 on jaettu kolmeen osa-alueeseen, joista tässä työssä käsitellään lähinnä osa-aluetta F eli fyysistä turvallisuutta. Muut osa-alueet ovat T eli turvallisuusjohtaminen ja I eli tietoturvallisuus. (Katakri 2015, 2.) I-osiota käsitellään siltä osin kuin siinä on mainintoja fyysiseen turvallisuuteen.

3.2.2 Fyysinen turvallisuus

Fyysistä turvallisuutta käsitellään Katakri 2015:ssa viranomaisen salassa pidettävän tiedon suojaamisen näkökulmasta. Ohjeistuksen tarkoituksena on varmistaa, että salassa pidettävät tiedot ovat suojassa paljastumiselta. Fyysisten toimien tarkoituksena on estää tunkeutuminen tiloihin salaa tai väkisin sekä ehkäistä, estää ja havaita luvattomat toimet. Fyysisen turvallisuuden toimien tarkoituksena on lisäksi mahdollistaa henkilöstön luokitus ja pääsy salassa pidettäviin tietoihin sen perusteella, mikä heidän tiedoksisaantitarpeensa on. (Katakri 2015, 16.) Katakri korostaa, että turvatoimien määrittäminen tulee tehdä riskienhallintaprosessin perusteella.

Katakri 2015:ssa tilat ja tila-alueet jaetaan kolmeen alueeseen. Nämä alueet ovat:

- hallinnollinen alue
- turva-alue
- tekninen turva-alue.

Tarve kunkin alueen perustamiseksi riippuu, minkä tasoista tietoa alueella käsitellään tai säilytetään. Katakrin aluejako on vastaavanlainen kuin EU:n neuvoston turvallisuussääntöissä, jotka on esitetty aikaisemmin luvussa 2.4.

Fyysisen turvallisuuden osa-alueeseen on Katakri 2015:ssa koottu vaatimusten lisäksi toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan yleensä saavuttaa hyväksyttävissä oleva minimitaso. Katakri 2015 ei kuvaa kaikkia erillisiä tapauksia vaan lopulliset ratkaisut pitää syntyä suunnittelun ja riskienhallinnan kautta, erilaisia uhkia vastaavaksi. Katakri 2015:sta on luettelo asioista, jotka tulisi vähintään ottaa huomioon turvallisuusratkaisuja suunniteltaessa.

Fyysisen turvallisuuden osalta Katakri 2015:ssa käsitellään seuraavat osa-alueet:

- tiloja ja laitteita koskevat vaatimukset
- luvattoman pääsyn estäminen
- suojaaminen salakatselulta ja salakuuntelulta
- toiminnan jatkuvuuden hallinta.

Fyysisen turvallisuuden osiossa kuvataan fyysisten alueiden osalta vaatimukset varsin tarkkaan. Vaatimusten lisäksi kohdassa F03 kuvataan fyysiseen suojaamiseen hyväksytyille järjestelmille ja laitteille asetetut standardit.

Katakri 2015 on viranomaisen auditointityökalu mutta se antaa fyysisen turvallisuuden osalta hyvät perusteet organisaation turvallisuussuunnittelulle. Työkalu ei yksin anna vastauksia tarkempiin kysymyksiin vaan edellyttää F-osiossa olevan standardiluettelon avaamisen lukijalle tai vastaavan tiedon hankkimisen muualta.

3.2.3 Tekninen tietoturvallisuus

Teknistä tietoturvallisuutta Katakri 2015:ssa käsitellä osa-alueessa I. Osa-alueessa kuvataan vaatimukset, joiden avulla pyritään varmistamaan turvallisuusjärjestelyjen riittävyys viranomaisen salassa pidettävän tiedon sähköisissä käyttöympäristöissä. Osa-alueessa täydennetään lisäksi muiden osa-alueiden kuvauksia paperimuotoisen tiedon suojausvaatimuksista. (Katakri 2015, 29.)

Osa-alue I korostaa osa-alueen F lailla riskienhallinnan ja sen tulosten tulkinnan merkitystä suunnittelussa ja toimenpiteiden toteutuksessa.

Vaatimuksessa I21 käsitellään fyysistä turvallisuutta liittyen salassa pidettävien tietojen käsittelyyn suojattujen alueiden sisällä. Vaatimuksessa esitetään millä alueilla eri tasoisia tietoja voidaan käsitellä ja säilyttää, myös tilapäisesti. Lisäksi se antaa vaatimuksen, että fyysiset turvatoimet toteutetaan kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa tietoja käsitellään ja säilytetään, tietojenkäsittely-ympäristöjen sijoitusalueet mukaan luettuna (Katakri 2015, 61).

Muista vaatimuksista löytyy liittymäpintaa F-osion vaatimuksiin mutta ei niin selkeästi kuin vaatimuksessa I21.

3.3 VAHTI 2/2013

VAHTI 2/2013 eli valtionvarainministeriön toimitilojen tietoturvaohje antaa suuntaviivoja rakentamissuunnittelulle ja ohjeita jo olemassa oleville toimitiloille siitä millaisilla ratkaisuilla turvallisuutta voidaan parantaa. Ohje auttaa ottamaan huomioon lakisääteiset ja kansainvälisten turvallisuussäännöstöjen asettamat vaatimukset toimitilaturvallisuudelle. (VAHTI 2/2013, 5.)

Tietoturvaohjeessa ja sen liitteissä esitetään kaikkien valtionhallinnon toimitilojen fyysisen turvallisuuden yleiset vaatimukset.

VAHTI 2/2013 mukaan lisääntyvä kansainvälinen yhteistyö asettaa vaatimuksen ottaa huomioon kansainvälisten yhteistyökumppaneiden turvallisuusluokitellun tiedon käsittelylle asettamat vaatimukset. Konkreettisemmin vaatimukset näkyvät tiedon käsittely- ja säilytysympäristöille asetetuissa vaatimuksissa. (VAHTI 2/2013, 9.)

Tietoturvaohjeen luvussa 2 kuvataan lait, asetukset ja vaatimusdokumentit, joille tämän ohjeen fyysistä turvallisuutta ohjaava sisältö perustuu ja jotka antavat vaatimuksia fyysisen turvallisuuden toteuttamiselle. Perusteet ovat lähtökohtaisesti jo vanhentuneet mutta niiden uudemmat, päivitetyt versiot ovat helposti löydettävissä internetissä.

Fyysiseen turvallisuuteen liittyvät turvallisuusvyöhykkeet ovat rajattuja alueita, joiden ulkokuoriin ja aukkoihin kohdistuu erityisiä turvallisuusvaatimuksia. Viranomaisilla on käytössä myös tiloja joihin erityisiä turvallisuusvaatimuksia ei kohdistu. Tällaisia tiloja voivat olla esimerkiksi aula- ja yleisöpalvelutilat. (VAHTI 2/2013, 19.)

Turvallisuusvyöhykejako perustuu sekä kansalliseen lainsäädäntöön että kansainvälisten velvoitteiden noudattamiseen. Vyöhykemäärittelyyn vaikuttavat oleellisesti uhka-arviot, riskianalyysit, tiedon suojaustaso, minkä muotoisesta tiedosta on kysymys sekä tarve säilyttää tietoa tilassa. Tietoturvaohjeen mukaiset vyöhykkeet ovat:

- VIHREÄ, jossa käsitellään tai säilytetään muutoin kuin satunnaisesti korkeintaan ST IV –tason tietoa.
- KELTAINEN, jossa käsitellään tai säilytetään muutoin kuin satunnaisesti korkeintaan ST III –tason tietoa.

- SININEN, jossa käsitellään muutoin kuin satunnaisesti korkeintaan ST II –tason tietoa.
- PUNAINEN, jossa käsitellään muutoin kuin satunnaisesti ST I –tason tietoa. (VAHTI 2/2013, 21.)

VAHTI 2/2013 liitteenä 1 on erityinen turvallisuusvaatimustaulukko ja taulukon lopuksi on kuvattu joitain yksittäisiä toteutussuosituksia. Toteutussuositukset ovat suuntaa antavia mutta eivät kovin yksilöllisiä.

Tietoturvaohjeen liitteessä 1 on kuvattu pisteytysmalli, jonka perusteella voidaan laskea, saavuttaako kohde riittävän turvallisuustason, ottaen huomioon toimintaympäristön yleisen riskitason. Pisteytysmalli antaa pisteitä sen perusteella täyttääkö vaatimus turvallisuusvyöhykkeelle tai tasolle esitetyt ehdot.

Turvallisuusvaatimustaulukko ei ota huomioon vasteaikaa, jonka tulisi olla lyhyempi kuin tunkeutumisaika, jolloin tiedon anastaminen voitaisiin estää. Taulukko esittää vaatimuksen vasteajan osalta vain, että mahdollisen vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä. Tunkeutumisaikaa ei taulukon perusteella voi laskea lainkaan.

Vahti 2/2013 on osittain jo vanhentunut. Se on kuitenkin hyvä julkinen lähde ja antaa kattavasti kuvan siitä minkälaisia asioita tulisi ottaa huomioon, kun suunnitellaan tilojen fyysisen turvallisuuden ratkaisuja.

3.4 VAHTI 100

Valtionvarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) toimii julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset. VAHTI –tietoturvaohjeisto on yksi maailman kattavimmista yleisistä ohjeistoista. (valtionvarainministeriö 2016.)

VAHTI-ohjeistus on tätä tutkimusta tehdessä päivityksessä työnimellä VAHTI 100. Ohjeistuksen uudistus tehdään käyttäjälähtöisesti ja koko ohjeistokokonaisuus uudistuu. Aikaisemmin VAHTI –ohjeistus on jaettu kah-

deksaan osioon, uusi ohjeistus jaetaan viiteen osioon. (Janhunen 2016.) Janhusen mukaan vaatimusten, ohjeiden ja tukimateriaalin velvoittavuutta selkeytetään ja VAHTI-vaatimukset uudistetaan. Luvussa 3.2 esitetyssä Katakri 2015:sta saatuja palautteita on hyödynnetty uudessa VAHTI-ohjeistossa.

VAHTI-ohjeita on jatkossa kahta pääluokkaa eli vihreitä, jotka ovat säädösten toimeenpanoon liittyviä ohjeita ja harmaita, jotka ovat yleisohjeita. VAHTI-korteilla tarkoitetaan kokonaisuuksia, jotka muodostuvat:

- säädöksestä ja sitä tulkitsevasta vaatimuksesta
- ohjeesta tarkentavine liitteineen
- tukimateriaalista.

VAHTI 100 luonnoksessa tilaluokkia tai alueita on neljä, joissa tulee huomioida vakiovaatimusten lisäksi vaatimukset ”ei sähköisen” käsittelyn osalta:

- Julkinen alue, jossa voidaan käsitellä korkeintaan ST IV luokan ”ei sähköistä” tietoa.
- Valvottu alue, jossa voidaan käsitellä korkeintaan ST II luokan tietoja, kunhan on varmistuttu, ettei tietoa pääse oikeudettomien käsiin.
- Suojattu alue, jossa on samat vaatimukset kuin valvotulla alueella.
- Teknisesti suojattu alue, jossa on samat vaatimukset kuin valvotulla alueella ja suojatulla alueella. (VAHTI 100.)

VAHTI 100 aineisto on löydettävissä Internetistä vasta beta –versiona, eikä sen lopullisesta käytettävyydestä voida tehdä tarkempia päätelmiä. Myöskään fyysisen turvallisuuden osalta ei beta –versiosta vielä voida saada tarkempaa arviota.

VAHTI 100:ssa fyysisen turvallisuuden vaatimukset tulisi esittää niin, että ne täyttäisivät myös nykyisien kansainvälisten sopimuksien vaatimukset, jolloin fyysisen turvallisuuden keinoin voitaisiin vaikuttaa mahdollisimman moneen vaatimukseen yhtä aikaa.

4 Kansainvälisten sopimusten perusteella annetut kansalliset määräykset ja ohjeet

4.1 Valtioneuvoston asetus 8/2013

Suomen säädöskokoelman n:o 945/2012 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut (945/2012).

Valtioneuvoston asetus 8/2013 on asetus Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen voimaansaattamisesta sekä hallinnollisen järjestelyn ja tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaantulosta.

Hallinnollisen järjestelyn mukaan molempien osapuolten turvallisuusviranomaiset vastaavat asetuksen toimeenpanojärjestelyistä. Suomessa turvallisuusviranomaisena toimii Kansallinen turvallisuusviranomainen (National Security Authority, NSA) (Valtioneuvosto 2013, 2 artikla).

Ennen turvallisuusluokiteltujen tietojen luovuttamista Suomen ja Naton välillä, on vastuullisten turvallisuusviranomaisten todettava hyväksymällään tavalla, että vastaanottaja suojaa saamansa tiedot luovuttajan edellyttämällä tavalla (Valtioneuvosto 2013).

Artiklan viisi mukaan osapuolet soveltavat fyysisen turvallisuuden osalta turvallisuusluokitellun tiedon suojaamiseen ja käyttöön seuraavia määräyksiä:

- Vastaanottava osapuoli antaa kaikelle turvallisuusluokitellulle tiedolle vähintään saman tasoisen fyysisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen.
- Vastaanottava osapuoli noudattaa niitä lisärajoituksia, joita luovuttava osapuoli tai joku muu tämän puolesta voi asettaa turvallisuusluokitellun tiedon käyttämiselle, paljastamiselle, ja luovuttamiselle sekä pääsylle tähän tietoon.
- Vastaanottava osapuoli toteuttaa kaikki tarvittavat toimet suojatakseen turvallisuusluokiteltua tietoa luvattomalta paljastamiselta.

Artiklassa yhdeksän todetaan, että osapuolet antavat toisilleen tiedot turvallisuusluokitellun tiedon suojaamista koskevista turvallisuusvaatimuksistaan, -käytännöistään ja –menettelyistään. Naton osalta vaatimukset on esitetty dokumentissa NATO DIRECTIVE on PHYSICAL SECURITY (AC/35-D/2001-REV2), joka on tarkemmin esitetty luvussa 2.3.

4.2 Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje

Kansallinen turvallisuusviranomainen on laatinut ohjeen kansainvälisen turvallisuusluokitellun tietoaineiston käsittelystä. Ohjeessa on vaatimuksia myös fyysisen turvallisuuden osalta. Ohjetta on viimeksi päivitetty 16.3.2016.

Ohjeen mukaan Suomi on sitoutunut valtiosopimuksissa toteuttamaan tietoturvallisuustoimia sellaisten tietojen suojaamiseksi, jotka on sopimuksen mukaisesti luovutettu Suomeen. Ohje ei korvaa sopimusmääräyksiä tai muita kansainvälisiä tietoturvallisuusvelvoitteita. (NSA 2016, 4.)

Ulkoasiainministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyen kansallisena turvallisuusviranomaisena (National Security Authority, NSA). Kansallisen turvallisuusviranomaisen lisäksi kansainvälisiä tietoturvallisuusvelvoitteita toteuttavina määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA) toimivat puolustusministeriö, Pääesikunta ja suojelupoliisi. Viestintävirasto toimii kansallisena tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta vastaavana viranomaisena (National Communication Security Authority, NCSA). (NSA 2016, 4.)

Turvallisuusluokitellun tiedon suojaamisesta sopiminen Suomen ja vieraan valtion taikka Suomen ja kansainvälisen järjestön välillä edellyttää valtiosopimusta. Sopimusten valmistelusta vastaa NSA. Tietoturvallisuussopimuksissa velvoitetaan sopimuspuolet huolehtimaan, että toisen sopimuspuolen turvallisuusluokiteltua tietoa käsitellään asianmukaisesti. (NSA 2016, 5.) Suomen osalta velvoite löytyy myös laista kansainvälisistä tietoturvavelvoitteista (588/2004).

Turvallisuusluokitellusta EU-tiedosta käytetään kansainvälistä lyhennettä EUCI (European Union Classified Information). EU-tiedolla tarkoitetaan mitä tahansa tietoa tai materiaalia, jolle on määritetty EU:n turvallisuusluokka ja jonka aiheeton paljastuminen voisi aiheuttaa jonkinlaista vahinkoa EU:n tai sen jäsenmaan eduille. (NSA 2016, 8.)

EU:n turvallisuusluokiteltuja tietoja suojataan koko niiden elinkaaren ajan siten, että pystytään estämään ja havaitsemaan niiden vaarantuminen ja katoaminen. Tällaisia turvatoimia liittyy esim. tiedon säilyttämiseen. EU:n turvallisuusluokitelluille tiedoille annetaan suojaa turvallisuusluokituksen mukaisesti siten, että mitä korkeampi turvallisuusluokka on, sitä paremmin tieto tulee suojata. (NSA 2016, 7.)

Käsittelyohjeen mukaan fyysinen turvallisuus on mitoitettava siten, että EU:n turvallisuusluokiteltuun tietoon ei ilman oikeutta päästä käsiksi. Edellä mainittu vaatimus koskee kaikkia tiloja, joissa käsitellään tai säilytetään EU:n turvallisuusluokiteltua tietoa. Toimivaltaisen viranomaisen tulee hyväksyä käytettävät tilat riippuen turvallisuusluokasta. EU:n turvallisuusluokitellun tiedon käsittely on rajauksin mahdollista kolmella eri alueella:

- hallinnolliset alueet
- pääsynvalvonnan piiriin kuuluvat varsinaiset turva-alueet
- teknisin keinoin suojatut turva-alueet, joissa salakuuntelu on estetty. (NSA 2016, 9.)

Käsittelyohjeessa on kuvattu turvallisuusluokittain EU:n yleiset vaatimukset fyysiselle turvallisuudelle ja toimitiloille.

Naton asiakirjoihin sovelletaan salassapitoperiaatetta, mikä tarkoittaa, että Naton asiakirjat ovat lähtökohtaisesti salassa pidettäviä, kun taas Suomen viranomaisten asiakirjoihin sovelletaan julkisuusperiaatetta. Voimassa oleva

Naton turvallisuussäännöstö pohjautuu dokumentaatiokokonaisuuteen, josta käytetään nimitystä Nato Security Policy (NSP). Suomen ja Naton välisessä tietoturvallisuussopimuksessa Suomi on sitoutunut kunnioittamaan Naton turvallisuussäännöstössä esitettyjä vaatimuksia riittävillä kansallisilla toimenpiteillä. (NSA 2016, 16.) Valtioneuvoston asetus Suomen ja Naton välisen tietoturvallisuussopimuksen voimaansaattamisesta ja tietoturvasopimus on esitetty luvussa 4.1. Fyysisen turvallisuuden direktiivi on esitetty luvussa 2.3.

Naton vaatimukset fyysisen turvallisuuden mitoittamiseksi ovat lähtökohtaisesti vastaavat kuin EU:n. Säilytystilan turvallisuustaso tulee hyväksyttää vastuuviranomaisella, mikäli käsiteltävän tiedon turvallisuusluokka on vähintään NATO SECRET. (NSA, 19.) Suomessa vastuuviranomainen on Viestintävirasto (Tauriainen 2016).

Käsittelyohjeessa on kuvattu turvallisuusluokittain Naton yleiset vaatimukset fyysiselle turvallisuudelle ja toimitiloille. Vaatimukset on esitetty tarkemmin kuin EU-tiedon osalta mutta tarkempiin yksityiskohtiin ei käsittelyohjeessa mennä.

Muiden valtioiden ja kansainvälisten järjestöjen tietoaineiston käsittelyvaatimuksista mainitaan lyhyesti, että toisen osapuolen turvallisuusluokitellulle tiedolle annetaan saman tasoinen suoja kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolle. Tätä varten sopimuksissa määritellään turvallisuusluokkien vastaavuudet ja yleiset periaatteet turvallisuusluokitellun tiedon vaihtamisesta.

5 Vaatimusvertailua ja seikkoja, jotka ainakin tulisi ottaa huomioon

Sekä kansainvälisissä että kansallisissa asiakirjoissa on eri tasoiset tilat jaettu alueisiin ja vyöhykkeisiin, jotka tulee hyväksyttää kansallisilla vastuuviranomaisilla. Karkeasti voidaan todeta, että niistä löytyy hallinnollinen alue, jossa voidaan käsitellä ja säilyttää turvallisuusluokiteltuja asiakirjoja ja järjestää tilaisuuksia, jossa käsitellään edellä mainittuja asioita. Niistä löytyy myös turva-alueita tai vastaavia, joilla voidaan käsitellä ja säilyttää turvallisuusluokiteltuja asiakirjoja. Lisäksi on teknisesti suojatut turva-alueet, joissa on otettu huomioon myös toimet sähköisen turvallisuusluokitellun tiedon käsittelemiseksi. Taulukoon 3 on koottu eri dokumenteissa esitetyt turvallisuusvyöhykkeet.

Taulukko 3 Turvallisuusvyöhykkeiden vertailu

EU	Nato	Katakri 2015	Vahti 2/2013	Vahti 100
Hallinnollinen alue	Administrative Zone	Hallinnollinen alue	Vihreä	Julkinen alue
Turva-alue	NATO Class I Security Area NATO Class II Security Area.	Turva-alue	Keltainen Sininen	Valvottu alue Suojattu alue
Teknisesti suojattu turva-alue	Technically Secure Area	Teknisesti suojattu turva-alue	Punainen	Teknisesti suojattu alue

Taulukossa 3 olevia turvallisuusvyöhykkeitä ei voida suoraan verrata toisiinsa niin, että ne vastaisivat sellaisenaan toisiaan. Todelliset vaatimukset tulee aina tarkastaa alkuperäisistä asiakirjoista.

Taulukoon 4 on koottu eri tutkittujen dokumenttien vyöhykevaatimukset eri tason turvallisuusluokitellun tiedon säilyttämiseksi.

Taulukko 4 Turvallisuusluokitellun tiedon säilyttäminen

	EU	Nato	Katakri 2015	Vahti 2/2013	Vahti 100
ST IV/ vast	Hallinnollinen alue lukittu toimis-tokaluste	Administrative Zone lukittu toimis-tokaluste	Hallinnollinen alue	VIHREÄ vyöhyke lukittu kaappi	
ST III/ vast	Turva-alue kansallisesti hyväksytty säi-lytysyksikkö	class I or II se-curity area kansallisesti hyväksytty säi-lytysyksikkö	Turva-alue S2 turva-kaappi	KELTAINEN vyöhyke E II -kassa-kaappi	
ST II/ vast	Turva-alue kansallisesti hyväksytty säi-lytysyksikkö	class I or II se-curity area kansallisesti hyväksytty säi-lytysyksikkö	Turva-alue E II kassa-kaappi	SININEN vyöhyke E II kassa-kaappi	

Säilyttämisen osalta dokumenteissa on lisäksi lisämääreitä tiedon säilyttämiseen liittyen.

Vahti 100 vaatimuksissa ei ollut vielä tämän tutkimuksen aikana vaatimuksia tiedon säilyttämisen osalta, joten niitä ei taulukossa 4 esitetty.

Taulukossa 5 on esitetty vyöhykevaatimukset tiedon käsittelyyn liittyen.

Taulukko 5 Turvallisuusluokitellun tiedon käsittely

	EU	Nato	Katakri 2015	Vahti 2/2013	Vahti 100
ST IV/ vast	Hallinnol-linen alue	Admini-strative Zone	Hallinnol-linen alue	VIHREÄ vyöhyke	Julkinen alue
ST III/ vast	Hallinnol-linen alue	class I or II security area	Hallinnol-linen alue	KELTAI-NEN vyö-hyke	Valvottu alue
ST II/ vast	Hallinnol-linen alue	class I or II security area	Hallinnol-linen alue	SININEN vyöhyke	Valvottu alue

Vahti 2/2013 mukaan vyöhyke, jossa käsitellään, muuten kuin satunnaisesti, suojaustasoon I luokiteltuja tietoja, merkitään PUNAISELLA värillä. Muissa dokumenteissa ei vastaavaa mainintaa löydy.

Tiedon käsittely voidaan sallia vain tietyin ehdoin. Dokumenteissa on kuvattu tarkemmin vaatimuksia, esimerkiksi tiedon sähköisen käsittelyn osalta tai salakatseluun ja –kuunteluun liittyen.

Fyysisen turvallisuuden eri toimien kuten rakenteellisen turvallisuuden, turvallisuusvalvontajärjestelmien ja tilojen sijoittelun tulee antaa ”puolustukseen syvyyttä” hidastamalla tunkeutujan pääsyä kohteelle ja vastaavasti mahdollistamalla hälytyksen saaminen reagoivalle joukolle jo mahdollisimman aikaisessa vaiheessa. Toinen toisiaan tukevien järjestelmien ja rakenteiden avulla voidaan saavuttaa riittävä turvallisuustaso helposti ja näin ollen saavuttaa suuria säästöjä. Korkeamman turvallisuustason tilojen sijoittamisella rakennuksen keskiosiin voidaan myös saada ”puolustukseen syvyyttä”.

Kaikista tutkimuksessa käytetyistä lähteistä löytyy varsin paljon yhteisiä vaatimuksia, jotka tulisi käsitellä ja ottaa huomioon suunniteltaessa fyysisen turvallisuuden keinoja. Yhteisten vaatimuksien lisäksi dokumenteista löytyy lisäksi tarkempia vaatimuksia, joten pelkästään tämän tutkimuksen luettelon pohjalta ei voida olettaa, että kaikki vaatimukset on otettu huomioon. Luettelo on kuitenkin hyvä apu vaatimusten täyttämiseksi.

Fyysisen turvallisuuden ratkaisuja suunniteltaessa tulee ottaa huomioon ainakin seuraavan luettelon mukaisia asioita. Vastaavat asiat tulee selvittää myös

esimerkiksi valmistauduttaessa tiedon luovuttajan suorittamaan tarkastukseen:

1. Minkä turvallisuusluokan tiedosta on kyse ja minkälaisessa muodossa tieto on? Paperisen ja sähköisen tiedon käsittelylle ja säilyttämiselle on yleensä asetettu erilaiset käsittely- ja säilytysvaatimukset.
2. Missä tietoa käsitellään ja missä sitä säilytetään? Erityisesti paperisen tiedon käsittelyvaatimukset ovat huomattavasti helpompi toteuttaa kuin vaatimukset paperisen tiedon säilyttämiselle. Sähköisen tiedon käsittelyvaatimukset taas poikkeavat huomattavasti paperisen tiedon käsittelyvaatimuksista.
3. Vastaavatko tiedon säilytysyksiköt, kuten kaapit, kassakaapit ja holvit vaatimuksia? Kuinka usein tai mistä syystä mahdolliset lukkojen koodit vaihdetaan?
4. Onko alueen, rakennuksen, tilan tai tilaryhmän turvallisuusvyöhykkeet määritelty vastaamaan tiloissa tehtäviä toimia? Onko vyöhykkeet määritelty todellisen tarpeen mukaan toiminnallisiin kokonaisuuksiin? Onko turvallisuusvyöhykkeillä sijaitsevat tilat sijoitettu oikein ottaen huomioon ympäröivät piha-alueet tai naapurihuoneet sekä muut mahdolliset korkeamman riskin aiheuttajat?
5. Onko pääsy turvallisuusvyöhykkeelle rajattu koskemaan vain niitä henkilöitä, joilla on tarvittava käsittelyoikeus tietoon ja joilla on siihen tiedoksisaantitarve?
6. Miten hallinnoidaan kulkuoikeuksia? Kuka myöntää oikeudet? Onko tiedossa kaikki henkilöt, joilla on pääsy tilaan? Milloin tilat siivottaan ja valvotaanko siivouksia? Miten huoltohenkilöstö pääsee kulkemaan tilaan ja onko heillä kulkuun oikeuttavat avaimet tai kulkutunnisteet aina mukanaan?
7. Miten avaintenhallinta on järjestetty? Kenelle on luovutettu avaimia ja ovatko ne kaikki tallessa? Onko mietitty toimenpiteet, jos avain häviää? Viedäänkö kaikkien tilojen avaimia vyöhykkeen tai työpaikan ulkopuolelle? Missä avaimia ja niiden lisätilauksiin tarvittavia dokumentteja säilytetään?
8. Minkälaisilla teknisillä järjestelmillä aluetta, rakennusta, tilaa tai tilaryhmää valvotaan? Täyttävätkö järjestelmiltä vaadittavat standardit?

Millä tavalla järjestelmien tuottamaa tietoa hallinnoidaan? Kenellä on oikeus päästä järjestelmien tuottamaan tietoon käsiksi?

9. Täyttävätkö tilat niille asetetut rakenteelliset vaatimukset, kun otetaan huomioon seinät, lattiat, katot, tilaan johtavat aukot, ikkunat ja ovet? Täyttävätkö ovien lukot vaatimukset?
10. Onko tiloissa, joissa käsitellään paperista tai sähköistä tietoa, salakatselu ja –kuuntelu estetty? Voiko ikkunoista nähdä sisään? Voiko käsiteltävät dokumentit näkyä kamerakuvissa? Onko rakenteiden ja esimerkiksi ilmastointikanavien äänieristys riittävä? Onko otettu huomioon sähkömagneettisen säteilyn (Tempest) vaikutukset?
11. Kuinka pitkä vasteaika on? Lähtökohtana tulee olla, että reagoivan henkilöstön vasteaika tulee olla lyhyempi kuin luvattomaan tunkeutumiseen kuluva aika eli tunkeutumisaika.
12. Miten toimitaan vierailijoiden ja ulkopuolisten palveluntarjoajien suhteen? Saatetaanko vieraat ja ovatko he aina isännän valvonnassa? Ketkä saavat olla vyöhykkeellä ilman isännän valvontaa?
13. Millä kriteereillä omalle tai vieraalle henkilöstölle tehdään tarvittavat taustaselvitykset?
14. Onko oma henkilöstö koulutettu riittävästi toimimaan oikein eri turvallisuusvyöhykkeillä? Onko koulutukset myös dokumentoitu?

Kaikkien edellä mainittujen asioiden tarkoitus on estää oikeudettomien henkilöiden pääsy suojattavaan tietoon. Tekniset ja rakenteelliset ratkaisut tukevat toisiaan oikeassa suhteessa tunnistettuun uhkaan ja säilytettävään tietoon nähden. Ratkaisujen tarkoitus on lisätä tunkeutumisaikaa ja käynnistää vaste mahdollisimman aikaisessa vaiheessa.

6 Johtopäätökset

Tutkimuksen tavoite oli selvittää Suomen tärkeimpien kansainvälisten yhteistyökumppaneiden vaatimuksia turvallisuusluokitellun tiedon käsittelemiseksi ja tiedon säilyttämiseksi. Samalla kartoitettiin vastaavia kansallisia vaatimuksia. Lopuksi vaatimuksia verrattiin toisiinsa. Vertailu tapahtui, työn laajuudesta johtuen, varsin karkealla tasolla. Tavoitteena oli saada aikaan työ, jonka avulla turvallisuusalan henkilöstö voi helpottaa omaa työtään turvallisuusratkaisujen suunnittelussa tai valmistautuessa kansainvälisten yhteistyökumppaneiden auditointeihin tai tarkastuksiin.

Katakri 2015 on Suomessa viranomaisten käyttämä fyysisen turvallisuuden auditointityökalu. Siihen on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri ei itse aseta ehdottomia vaatimuksia vaan siihen kootut vaatimukset perustuvat olemassa olevaan lainsäädäntöön ja Suomea sitovaan kansainvälisiin tietoturvavelvoitteisiin. Katakrin toteuttamisvaihtoehdot eivät ole sitovia mutta niissä kuvataan suosituksia ja parhaita käytäntöjä. Katakri ei yksin riitä täyttämään kaikkia tässä tutkimuksessa esitettyjen dokumenttien vaatimuksia, sillä sen vaatimuksien perusteissa ei ole otettu mukaan esimerkiksi Naton vaatimuksia.

Tässä tutkimuksessa olevat kansalliset ja kansainväliset dokumentit esittävät minimivaatimukset turvallisuusluokitellun tiedon suojaamiseksi. Vaatimukset ovat käytännössä Suomen viranomaisia sitovia. Vaatimusten toteuttamisvaihtoehtojen osalta jää toteuttajalle kuitenkin mahdollisuus valita erilaisia vaihtoehtoja. Vaihtoehtojen suunnittelussa korostuu kohteeseen kohdistuvien uhkien tunnistaminen ja riskienhallinta. Tarkempia ohjeita toteuttamisesta ja eri vaihtoehdoista löytyy kansallisesti Vahti-ohjeista ja kansainvälisesti EU:n ja Naton turvallisuussääntöjä täydentävistä asiakirjoista.

Nato ja EU ovat määritelleet, miten niiden turvallisuusluokiteltua tietoa suojataan. EU:n vaatimuksia Suomi joutuu noudattamaan, koska se on EU:n jäsen. Naton vaatimuksia Suomi joutuu noudattamaan, jotta se voi vastaanottaa Natolta turvallisuusluokiteltua tietoa yhteistyöhön liittyen. Muiden organisaatioiden ja valtioiden tietoa suojataan lähtökohtaisesti kuten kansallista turvallisuusluokiteltua tietoa.

Naton ja EU:n turvallisuusluokitellun tiedon käsittelystä ja säilyttämisestä annetuissa vaatimuksissa on eroavaisuuksia mutta karkeassa mittakaavassa ne noudattavat samaa linjaa. Molempien vaatimuksista käy esille ”puolustuksen syvyys” eli se, että erilaisin toimenpitein pyritään lisäämään tunkeutumisaikaa siten että reagoivan henkilöstön vasteaika kohteelle olisi lyhyempi kuin tunkeutumiseen käytetty tunkeutumisaika.

Tietyn kansainvälisen toimijan vaatimuksia ei lähtökohtaisesti pystytä toteuttamaan pelkästään kansallisia vaatimuksia täyttämällä. Jokaisessa tapauksessa tulee tutustua tarkemmin kyseisen toimijan omiin vaatimuksiin. Usein toimijat ovat antaneet vielä tarkempia vaatimuksia tässä tutkimuksessa käytettyihin ja esitettyihin dokumentteihin. Tarkemmat vaatimukset ovat yleensä itse salassa pidettäviä, eikä niitä siksi avata tässä tutkimuksessa tarkemmin.

Kohteen vartioinnilla ja erityisesti vartijoilla saavutettavalla lyhyellä vasteajalla voidaan korvata rakenteellisia ja teknisiä ratkaisuja, jotka saattaisivat maksaa omistajalle kohtuuttoman paljon tai voisivat olla vaikeita toteuttaa. Vasteaika tulee laskea realistisesti. Vasteajan määrittäminen tulisi tehdä aina pahimman skenaarion mukaisesti, eikä vain laskea sitä lyhimmän käytetyn matkan mukaisesti.

Vasteajan määrittäminen pitää pystyä perustelemaan esimerkiksi kohdetta auditoitaessa. Tarkastuksissa tehdyt ratkaisut ovat usein tarkastavien henkilöiden omia tulkintoja, jotka perustuvat heidän omaan taustaansa.

Fyysisen turvallisuuden suunnittelu on ehdottomasti toteutettava riskienhallinnan kautta. Tietoon, toimintaan ja tiloihin kohdistuvat todennäköiset uhkat on tunnistettava ja niille on määriteltävä riittävät suojautumistoimenpiteet. Riskienhallinnan avulla voidaan lisäksi säästää kustannuksissa, kun toimenpiteet määritellään uhkia vastaaviksi, eikä toimita valmiiden mallien ja taulukoiden varassa. Erityisesti korkeamman turvallisuustason tilat ratkaisuineen maksavat usein enemmän kuin mihin ollaan valmiita panostamaan.

Riskienhallinnan ja fyysisten turvallisuusratkaisujen kohdalla voidaan hyvänä kysymyksenä pitää, että miksi joku haluaisi saada tietyn dokumentin haltuunsa murtautumalla virkamiehen kassakaappiin, jos dokumentin tai sen sisältämän tiedon voi saada huomattavasti helpommin jollain muulla tavalla.

Jokainen ministeriö voi tällä hetkellä itse tehdä aiheesta omat johtopäätöksensä ja ratkaista minkälaiselle tasolle ne haluavat viedä oman fyysisen turvallisuuden tasonsa.

Sähkömagneettisen säteilyn hyväksikäyttöä voidaan pitää sähköisen tiedon kannalta merkittävänä uhkana. Tempest –tiedustelua on vaikea havaita ja tiedusteluun vaadittavat laitteet ovat kohtuullisen yksinkertaisia. Sähkömagneettiselta säteilyltä suojautumisessa on tilojen sijoittelulla suuri merkitys, mikäli ei haluta tai kyetä hankkimaan kalliita rakenteellisia ratkaisuja. Tempest –suojautumiselle eivät tarkastellut dokumentit antaneet juurikaan vastauksia ja aihe on selvästi jatkotutkimuksen aihe.

Toinen jatkotutkimuksen aihe on fyysisen turvallisuuden toteutuminen monitoimitiloissa ja avokonttoreissa. Valtion toimitilastrategian mukaisesti valtioneuvosto ja sen ministeriöt ovat siirtymässä peruskorjatuissa rakennuksissa monitoimitiloihin, joiden suunnittelussa tulee fyysisen turvallisuuden ratkaisut ottaa korostetusti huomioon. On ratkaistava, miten tiedon käsittely toteutetaan vaatimustenmukaisesti tiloissa, joissa liikkuminen on vapaampaa kuin tiloissa, joissa kaikilla on omat toimistot. Hallinnollisen turvallisuuden keinoin voidaan ratkaista kysymyksiä kulkulupiin ja käsittelyoikeuksiin liittyen mutta salakuuntelun- ja katselun estämiseksi vaaditaan myös fyysisen turvallisuuden keinoja.

Suomen kansalliset vaatimukset noudattavat samaa linjaa kuin kansainväliset vaatimukset ja jo pelkästään kansallisten vaatimusten huolellisella täyttämisellä saavutetaan hyvä taso kansainvälisten vaatimusten täyttämisessä.

Kansallinen turvallisuusviranomainen on laatinut kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeen mutta sen jalkauttaminen ministeriöiden toimintaan on kirjavaa. Tehdyt toimenpiteet ja vaatimusten täyttäminen tarkistetaan lähinnä kansainvälisten organisaatioiden tarkastuksiin liittyen. Tarkastuksiin liittyen NSA:n rooli korostuu tilaisuuksien järjestäjänä ja vaatimuksien täyttymisen esitarkastajana.

Valtioneuvoston kanslian tehtävänä on johtaa ja yhteen sovittaa ministeriöiden yhteistä turvallisuutta. Tähän tehtävään liittyen valtioneuvoston kanslia on tarkastamassa ja päivittämässä omaa ohjeistustaan fyysisen turvallisuuden osalta. Kanslian tulisikin laatia riittävä ohjeistus valtioneuvostoon, jonka vaatimukset täyttämällä jokainen ministeriö voisi saavuttaa fyysisen turvallisuuden minimitason. Ohjeistuksen laatimiseksi tulisi perustaa työryhmä, jossa olisi jäseniä eri ministeriöistä ja esimerkiksi Viestintävirastosta ja suojelupoliisista. Kanslian tulisi myös laatia suunnitelma ministeriöiden turvallisuuden minimitason saavuttamisen auditoimiseksi ja saavutetun turvallisuustason säilyttämiseksi.

Ministeriöiden toimintaympäristöt ja niitä uhkaavat asiat vaihtelevat suuresti. Kaikille ministeriöille ei siksi pelkkä minimitason saavuttaminen ole riittävää, jolloin edellä mainitut virastot voisivat laatia oman täydentävän ohjeistuksen itselleen. Ministeriön omat ohjeet tulee kuitenkin hyväksyttää valtioneuvoston kanslialla.

Ministeriöiden tulisi tehdä valtioneuvoston fyysisen turvallisuuden ohjeistuksen jälkeen kartoitus oman turvallisuuden nykytilasta. Kartoituksessa esiin tulevista poikkeamista ohjeistukseen tulisi tehdä poikkeamapäätös, jossa poikkeama todetaan ja samalla suunnitellaan miten ja missä ajassa asia saadaan korjattua. Poikkeamapäätös tulisi tehdä ministeriössä ja hyväksyttää valtioneuvoston kansliassa.

7 Yhteenveto

Kehitystyön aihe syntyi aidosta tarpeesta selvittää, minkälaisia vaatimuksia tärkeimmillä kansainvälisillä yhteistyökumppaneilla on Suomen ministeriöille fyysisen turvallisuuden osalta, jos ministeriöissä käsitellään ja säilytetään yhteistyökumppanin turvallisuusluokiteltuja asiakirjoja.

Tutkimuksessa tutustuttiin aiheesta julkaistuihin tärkeimpiin dokumentteihin ja täydennettiin saatua tietoa haastatteluin. Kaiken hankitun tiedon perusteella vertailtiin eri toimijoiden vaatimuksia ja laadittiin luettelo dokumenttien pääkohdista fyysisen turvallisuuden osalta.

Kehitystyön tekeminen kesti hieman oletettua kauemmin, koska osa tutkimuksessa käytetystä aineistosta ilmestyi vasta joulukuussa 2016. Osa materiaalista oli lisäksi saatavissa vain englannin kielisenä ja siksi materiaalin tutkiminen kesti hieman normaalia kauemmin. Työ tehtiin iltaisin ja viikonloppuisin, joten käytettävä aika jouduttiin rajaamaan varsin tarkasti.

Jo tutkimuksen alkuvaiheessa selvisi, että kattavaa vertailua ei fyysisen turvallisuuden vaatimuksista, tutkimuksen laajuudesta johtuen, pystytä tekemään. Siksi tutkimus päätettiin tehdä malliksi, mihin on kerätty yhteen vaatimuksia tärkeimmistä asiakirjoista. Työ toivottavasti auttaa turvallisuusalan henkilöstöä, ainakin jonkin verran, heidän vaativassa tehtävässään yhteisen turvallisuuden luomisessa.

Nato ja EU ovat määritelleet, miten niiden turvallisuusluokiteltua tietoa suojataan. EU:n vaatimuksia Suomi joutuu noudattamaan, koska se on EU:n jäsen. Naton vaatimuksia Suomi joutuu noudattamaan, jotta se voi vastaanottaa Naton turvallisuusluokiteltua tietoa yhteistyöhön liittyen. Muiden organisaatioiden ja valtioiden tietoa suojataan lähtökohtaisesti kuten kansallista turvallisuusluokiteltua tietoa.

Kansalliset ja kansainvälisten organisaatioiden fyysisen turvallisuuden vaatimukset turvallisuusluokitellun tiedon käsittelemiseksi ovat olemassa mutta tarvitaan yhteinen dokumentti, joka täyttäisi kaikkien tärkeimpien toimijoiden vaatimukset. Tällä hetkelle ministeriöt joutuvat etsimään tietoa monista eri asiakirjoista.

Valtioneuvoston kanslian tulee laatia ohje valtioneuvostolle ministeriöiden fyysisen turvallisuuden minimitason saavuttamiseksi. Ohjeistukseen tulee ottaa kansallisten vaatimusten lisäksi huomioon kansainvälisen turvallisuusluokitellun tietoaineiston fyysisen turvallisuuden vaatimukset. Ohjeistuksen laatiminen tulee tehdä yhteistyössä ministeriöiden kanssa. Fyysisen turvallisuuden suunnittelu ja toimenpiteiden toteuttaminen pitää liittää kiinteästi yhteen riskienhallinnan kanssa

Jatkotutkimusaiheiksi löydettiin kaksi erillistä aihetta. Tilojen suunnitteluun liitettävän Tempest-suojautumisen tutkiminen mahdollistaa paremman suojautumisen sähköinen tiedon käsittelemiseksi. Monitoimitilat ja avokonttorit tarvitsevat lisää ohjeistusta kansainvälisen turvallisuusluokitellun tiedon käsittelyn ja säilyttämisen osalta. Fyysisen turvallisuuden keinot tulee ottaa huomioon jo tiloja suunniteltaessa, jotta voidaan varmistua toiminnan vaatimustenmukaisuuden toteutumisesta.

.

Lähteet

Council of the European Union. 2007. EU risk-management process for physical security.15386/07. Lähde tutkijan hallussa.

Euroopan komissio. 2015. Päätös 2015/444 EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä. Tulostettu 6.11.2016. http://publications.europa.eu/fi/publication-detail/-/publication/41a6eeeb-cc70-11e4-ab4d-01aa75ed71a1/language-fi

Euroopan unioni. 2013. Neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevissa turvallisuussäännöissä. Tulostettu 19.10.2016. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32013D0488&from=FI

Finlex. 2004. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Luettu 13.1.2017. http://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Finlex. 2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Luettu 11.10.2016. http://www.finlex.fi/fi/laki/alkup/2010/20100681

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. Uudistettu painos. Hämeenlinna. Kariston Kirjapaino Oy

Jyväskylän Yliopisto. 2015. Fenomenologinen tutkimus. Tulostettu 5.1.2017. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/fenomenologinen-tutkimus

Lainkirjoittajan opas. Valtiosopimukset Suomen oikeusjärjestyksessä. Luettu 27.1.2017. http://lainkirjoittaja.finlex.fi/8-valtiosopimukset-suomen-oikeusjarjestyksessa/valtiosopimukset-suomen-oikeusjarjestyksessa/

Nato Security Committee. 2008. AC-35-D-2001-REV2 Directive on Pfysical Security. Tulostettu 8.11.2016. http://bip.abw.gov.pl/download/1/1209/AC35D2001REV2.pdf

NSA. 2016. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. Luettu 23.1.2017. http://formin.finland.fi/public/download.aspx?ID=142360&GUID=%7B3601698A-FC0F-485C-84FD-C7CA32513D1E%7D

Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Luettu 12.11.2016. http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Suomen erityisedustusto Natossa (NAE). 2016. Suomen Nato-kumppanuus. Luettu 21.1.2017. http://www.finlandnato.org/Public/default.aspx?contentid=75622

Turvallisuuskomitea. 2012. Turvallinen Suomi –Tietoja Suomen kokonaisturvallisuudesta. Luettu 22.1.2017. http://www.finlandnato.org/public/download.aspx?ID=104374&GUID=%7BF369C2A5-87AB-45BB-89F7-55F04128C9E0%7D

Turvallisuuskomitea. 2014. Turvallinen Suomi –Tietoja Suomen kokonaisturvallisuudesta. Luettu 22.12.2016. http://www.turvallisuuskomitea.fi/index.php/fi/component/k2/45-turvallinen-suomi-tietoja-suomen-kokonaisturvallisuudesta

Ulkoasiainministeriö. 2016. Arvio Suomen mahdollisen Nato-jäsenyyden vaikutuksista. Luettu 5.2.2017. http://www.finlandnato.org/public/download.aspx?ID=157406&GUID=%7B8D6158F6-B7E5-483C-9455-F66D76ACC1FB%7D

Ulkoasiainministeriö. 2016. Kansallinen turvallisuusviranomainen. Tulostettu 21.11.2016. http://formin.finland.fi/Public/default.aspx?nodeid=41940

Valtioneuvosto 2013. Valtioneuvoston asetus 8/2013. Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa

tehdyn tietoturvallisuussopimuksen voimaansaattamisesta. Luettu 28.1.2017. http://www.finlex.fi/fi/sopimukset/sopsteksti/2013/20130008

Valtioneuvosto 2013. Valtioneuvoston ohjesääntö 262/2003. Luettu 21.2.2017. http://www.finlex.fi/fi/laki/ajantasa/2003/20030262

Valtioneuvoston kanslia. 2016. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko. Luettu 21.1.2017. http://valtioneuvosto.fi/documents/10616/1986338/VNKJ072016_fi.pdf/9a3a074a-d97f-43c4-a1d8-e3ddbbd8d1da

Valtionvarainministeriö. 2009. Fyysinen turvallisuus-Vahtiohjeet. Tulostettu 2.1.2017. https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

Valtionvarainministeriö. 2009. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto. Tulostettu 2.1.2017. https://www.vahtiohje.fi/web/guest/maaritelmat-t

Valtionvarainministeriö. 2013. VAHTI 2/2013, toimitilojen tietoturvaohje. Luettu 3.1.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10229

Valtionvarainministeriö. 2016. Tieto- ja kyberturvallisuuden ohjaus. Tulostettu 21.11.2016. http://vm.fi/ohjaus

Valtionvarainministeriö. 2017. VAHTI 100. Beta –versio. Luettu 22.12.2016. https://beta.vahtiohje.fi/etusivu

Seminaariesitelmiä

Erkkilä, J. 2016. Puheenvuoro Puolustusvoimien 10. Yritysturvallisuuspäivä –seminaari.17.11.2016. Helsinki

Janhunen, K. 2016. VAHTI-ohjeet ja KATAKRI2015 –Kohti yhtenäisempää ohjausta. Puolustusvoimien 10. Yritysturvallisuuspäivä –seminaari.17.11.2016. Helsinki

Haastattelut.

Erkkilä, J. 2016. EU risk-management process for physical security. Email johanna.erkkila@formin.fi. 28.11.2016. Tulostettu 12.12.2016.

Tauriainen, A. 2016. NCSA:n päällikön haastattelu 9.11.2016. Helsinki.