Suojaamisen näkökulmasta toteutettava tahallisesti aiheutettujen turvallisuutta vaarantavien riskien arviointi

Esko Äärynen

2020 Laurea

Laurea-ammattikorkeakoulu

Suojaamisen näkökulmasta toteutettava tahallisesti aiheutettujen turvallisuutta vaarantavien riskien arviointi

Esko Äärynen
Turvallisuusjohtaminen YAMK
Opinnäytetyö
Huhtikuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtamisen koulutusohjelma
Tradenomi (YAMK)

Esko Äärynen

Suojaamisen näkökulmasta toteutettava tahallisesti aiheutettujen turvallisuutta vaarantavien riskien arviointi

Vuosi 2020 Sivumäärä 70

Tämän opinnäytetyön tavoitteena oli kehittää helppokäyttöinen tahallisesti aiheutettujen turvallisuusriskien arviointityökalu. Opinnäytetyö toteutettiin Puolustusvoimien turvallisuustoimialan tilauksesta ja liitettiin osaksi Puolustusvoimien turvallisuusjohtaminen 1 -kurssin lähiopetusjaksoa, jossa arviointityökalua testattiin ja käytettiin ryhmätöissä opetuksen tukena. Opinnäytetyön tutkimusongelmiksi muodostuivat seuraavat:

- miten tahallisesti aiheutettuja turvallisuusriskejä voidaan arvioida; ja
- millaisella työkalulla arviointi voidaan toteuttaa.

Opinnäytetyö toteutettiin konstruktiivisena kehittämisprojektina, jossa havaittuun kehittämiskohteeseen pyrittiin kehittämään pragmaattisesti ja realistisen evaluaation lähestymistapaa hyödyntäen toimiva ratkaisu. Tutkimuksen aineisto analysoitiin laadullisen sisällönanalyysin menetelmin. Tutkimuksen kannalta merkittävin lähdeaineisto koostui ulkomaisista tutkimusraporteista, tieteellisistä artikkeleista, ammattikirjallisuudesta ja Yhdysvaltojen asevoimien ohjesäännöistä sekä opinnäytetyön tekijän turvallisuusjohtamisen opintokokonaisuuden 1 lähijaksolla teettämästä kyselystä.

Opinnäytetyön viitekehys muotoutui Naton Force Protection -doktriinin mukaisen riskienhallinnan prosessin kriittisyyksien, uhkien ja haavoittuvuuksien arviointivaiheen ympärille. Suojaamisen näkökulmasta tahallisesti aiheutetut turvallisuusriskit muodostuivat suojattavien kohteiden ja tekijöiden kriittisyydestä, haavoittuvuudesta sekä niihin kohdistuvasta vihamielisen toimijan aikeesta ja suorituskyvystä toteuttaa jokin uhkatapahtuma. Kehitetyn arviointityökalun testiversiossa eri osakokonaisuuksien arviointi toteutettiin vastaamalla kysymyksiin kyllä tai ei. Kyllä tai ei -vastausvaihtoehto havaittiin liian jyrkäksi ja mustavalkoiseksi, vaikka arvioinnin lopputulokset vaikuttivatkin oikeasuuntaisilta. Arviointityökalun tekninen ratkaisu toteutettiin Excel -sovelluksella.

Suojaamisen näkökulmasta toteutettavassa tahallisesti aiheutettujen turvallisuusriskien arvioinnissa ei ole vielä vakiintuneita menetelmiä tai termistöä. Turvallisuustoimialalla tulisi kiinnittää jatkossa huomiota juuri tähän. Tämä opinnäytetyö tarjoaa yhden vaihtoehdon tahallisesti aiheutettujen turvallisuusriskien arvioinnin toteuttamiseen.

Asiasanat: turvallisuus, uhka, kriittisyys, haavoittuvuus, riskienarviointityökalu

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Master of Business Administration

Esko Äärynen

Assessing deliberately caused security risks from the force protection perspective

Year 2020 Pages 70

The goal on this master's thesis was to develop an assessment tool for assessing deliberately caused security risks from the force protection perspective. This thesis was done in cooperation with Finnish Defence Forces security sector and the assessment tool was tested and used as part of education at the security management study unit's contact teaching period. The research problems of this study were the following:

- how to assess deliberately caused security risks; and
- what kind of assessing tool would suit for this purpose.

The thesis was implemented as a constructive development project, which aimed at developing a workable solution for the observed development object using a pragmatic and realistic evaluation approach. Documents for this thesis were analyzed by using qualitative content analysis methods. The most important sources for the thesis consisted of foreign research reports, scientific articles, professional literature and US Armed Forces regulations, as well as a questionnaire commissioned by the author of the thesis during the security management program's contact teaching period at the intelligence school.

The framework of the thesis was formed around the NATO force protection doctrine's risk management process's criticality, threat and vulnerability assessment phase. From the force protection perspective the deliberately caused security risks are formed from the asset's criticality, vulnerability and the hostile actor's will and capability to perform specific threats. In the assessment tool developed for this thesis, the assessment was done by answering questions yes or no. As the real world is not black and white the yes and no answers were found to be too strict a way to assess the deliberately caused security risks, although the results seemed to be correct. The assessment tool was built on MS Excel software.

There are no well-established tools or terminology for assessing deliberately caused security risks. The security sector should pay attention to this in the future. This thesis provides one option to implement a deliberately caused security risk assessment from the force protection perspective.

Keywords: security, threat, criticality, vulnerability, risk assessment tool

Sisällys

1 Johdanto

Perinteisesti riskienarviointi liitetään vahinko-, talous-, operatiivisiin ja strategisiin riskeihin. Näistä vahinkoriski mielletään kokonaisuutena, jolla on lähtökohtaisesti vain negatiivisia vaikutuksia. Usein vahinkoriskit aiheuttavat toteutuessaan myös vakavia välillisiä seurauksia. (Riskikompassi 2019) Tästä esimerkkinä Puolustusvoimien ampumaharjoituksissa tapahtuneet kuolemaan tai vakavaan loukkaantumiseen johtaneet onnettomuudet, jotka ovat aiheuttaneet myös suuria taloudellisia seurauksia ja mainehaittaa. Jokaiseen taistelu- ja ampumaharjoitukseen tehdään Puolustusvoimissa riskiarvio ja toteutetaan riskienhallinnan toimenpiteitä. Näin ollen perinteisten vahinkoriskien arviointi ja hallinta on kohtuullisen hyvin hallussa joitain vakavia riskiluonteisesta toiminnasta johtuvia onnettomuuksia lukuun ottamatta.

Viimeisen reilun kymmenen vuoden aikana kansainvälinen suuntaus joukkojen suojaamiseen tähtäävässä riskienhallinnassa on kohdistunut yhä enemmän tahallisesti aiheutettujen turvallisuutta vaarantavien riskien hallintaan. Lisääntyneet sotilaalliset operaatiot yhä kompleksisimmissa ympäristöissä muodostavat uudenlaisia uhkia joukoille ja toiminnan kannalta kriittisille kohteille.

Puolustushallinnon turvallisuusstrategiassa Suomen arvioidaan osallistuvan jatkossa yhä vaativampiin kriisinhallintatehtäviin, joissa paikallisväestö voi olla vihamielinen Suomen joukkoja kohtaan. Tämä lisää myös terrori-iskujen mahdollisuutta kotimaassa asti. Turvallisuusstrategian tavoitetilan mukaan puolustushallinto kykenee hallitsemaan ja vastaamaan olemassa oleviin turvallisuusuhkiin sekä osallistuu kansalliseen ja kansainväliseen yhteistyöhön. Osa kansainvälistä yhteistyötä on myös turvallinen osallistuminen kriisinhallintaoperaatioihin. (Puolustusministeriö 2020)

Puolustusministeriön julkaiseman ilmoituksen Naton kanssa tehdystä isäntämaatukea koskevasta yhteisymmärryspöytäkirjasta mukaan kaikki toimenpiteet tehdään henkilöstön, tilojen, välineiden ja toimintojen suojaamiseksi kaikissa tilanteissa ja mahdollistetaan toiminnan vapaus sekä ylläpidetään joukkojen operatiivinen toimintakyky (Finlex 2014). Tähän liittyen Puolustusvoimat otti vuonna 2017 käyttöön turvallisuustasojärjestelmän, joka pohjautuu Naton suojaamisen doktriiniin (Puolustusvoimat 2017). Tämän doktriinin hyödyntämistä turvallisuusjohtamisen mallina on tutkittu aiemmin, mutta varsinaisia työkaluja ei riskienhallinnan osalta ole kehitetty (Halli 2018).

Lisääntyneiden terrori-iskujen ja yhä kansainvälistyvän järjestyneen rikollisuuden lisääntyminen on nostanut tarvetta tahallisesti aiheutettujen turvallisuusriskien yhä tarkemmalle arvioinnille. Omien joukkojen ja kohteiden suojaamisessa täytyy ottaa yhä vakavammin huomioon se seikka, että jokin vihamielinen taho voi toteuttaa iskun tai hyökkäyksen erilaisia improvisoituja keinoja hyödyntäen aikeenaan vahingoittaa tai tuottaa tappioita kohteelleen.

Tahallisesti aiheutetuille turvallisuusriskeille ei ole tällä hetkellä olemassa yhtä vakiintuneita arviointimenetelmiä kuin esimerkiksi tavanomaisille vahinkoriskeille. Puolustusvoimien turvallisuustoimialan tavoitteena tälle opinnäytetyölle oli kehittää helppokäyttöinen tahallisesti aiheutettujen turvallisuusriskien arviointityökalu. Opinnäytetyön lopputuotteen ei ole valmistuessaan tarkoitus päätyä täysimääräisesti Puolustusvoimissa käyttöön, vaan sen tarkoituksena on tuottaa tietoa, miten tahallisesti aiheutettuja turvallisuusriskejä kannattaa arvioida ja millaisella työkalulla se kannattaa tehdä. Työkalua voidaan hyödyntää eri tasolla toimivien joukkojen komentajien ja heidän esikuntiensa suunnittelutyössä.

1.1 Tavoite ja rajaukset

Opinnäytetyön tavoitteena oli kehittää Naton Force Protection -malliin (esitelty luvussa 2) perustuva helppokäyttöinen ja toimiva arviointityökalu tahallisesti aiheutettujen turvallisuusriskien arvioimiseksi. Opinnäytetyön lopputuotoksena on konkreettinen työkalu, jota on helppo käyttää ja hyödyntää tahallisesti aiheutettujen turvallisuusriskien arviointiin. Työkalu voisi tulla eri tasoilla toimivien komentajien ja näiden esikuntien päätöksenteon tueksi.

Opinnäytetyön tutkimusongelmiksi muodostuivat seuraavat: *miten tahallisesti aiheutettuja turvallisuusriskejä voidaan arvioida* ja *millaisella työkalulla arviointi voidaan toteuttaa*. Ensimmäiseen tutkimusongelmaan vastaamalla saadaan muodostettua käsitys niistä kokonaisuuksista, joita tahallisesti aiheutettu turvallisuusriski pitää sisällään ja miten näitä kokonaisuuksia on mielekästä arvioida. Toinen tutkimusongelma liittyy käytännön tavoitteeseen kehittää työkalu tahallisesti aiheutettujen turvallisuusriskien arviointiin.

Työn tilaajan toiveena oli saada uusia vaihtoehtoja turvallisuusriskien arviointiin. Työkalun kehitystyö rajattiin käsittelemään riskienhallinnan näkökulmasta vain riskien tunnistamista ja arviointia, päähuomion ollessa jälkimmäiseksi mainitussa. Tällöin esimerkiksi riskienhallinnan toimenpiteet riskien pienentämiseksi ja riskien seuranta jäivät työn ulkopuolelle.

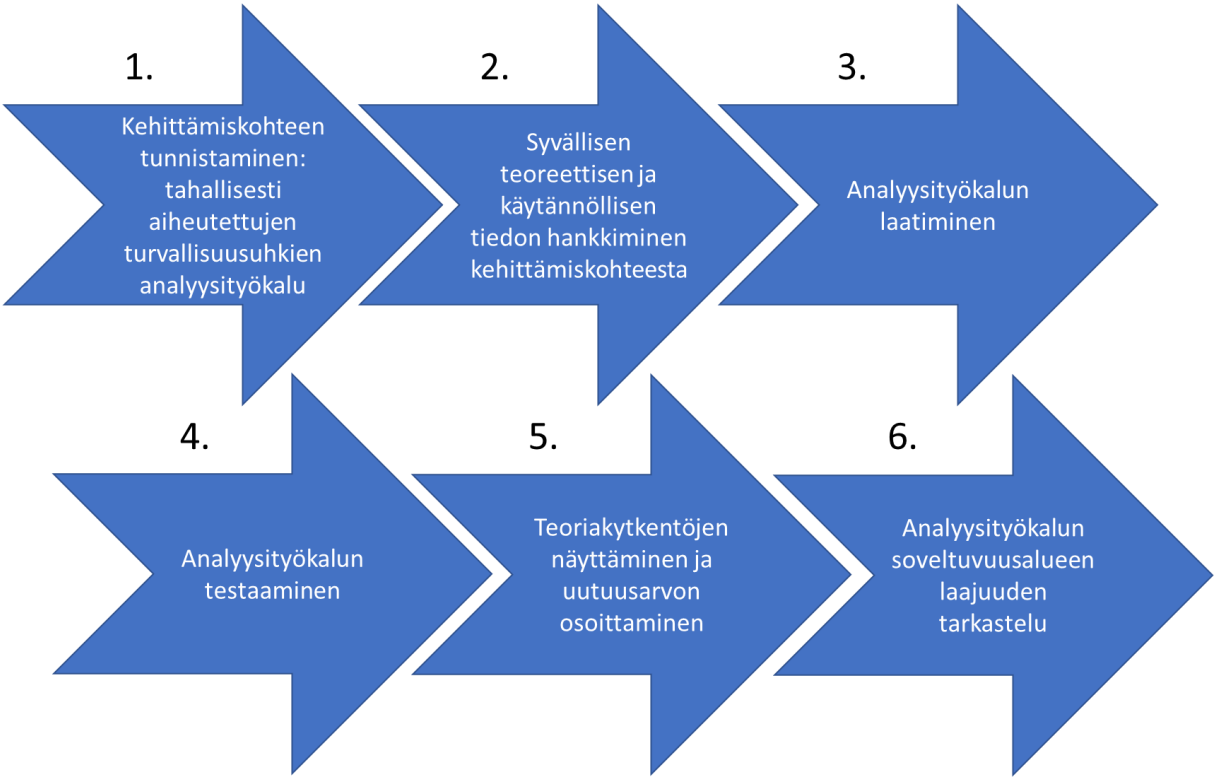
1.2 Toteutus ja analysointimenetelmät

Opinnäytetyö toteutettiin laadullista konstruktiivista lähestymistapaa hyödyntäen. Kehittämistehtävän toteuttaminen konstruktiivisella menetelmällä oli luonnollista, koska opinnäytetyön kehittämisongelmana oli se, että tahallisesti aiheutettujen turvallisuusriskien analysointiin ei ollut yhteistä työkalua. Konstruktiivisessa tutkimuksessa on tavoitteena saada käytännön ongelmaan uusi ja teoreettisesti perusteltu käytännönläheinen ratkaisu. Uuden työkalun ja mallin luominen ei ole innovaation synnyttämistä vaan uudenlaisen rakenteen kehittämistä - tähän prosessiin tarvitaan olemassa olevaa teoreettista sekä uutta empiiristä tietoa. (Ojasalo, Moilanen & Ritalahti 2014, 65)

Konstruktiivisella lähestymistavalla pyritään ratkaisemaan oikea käytännön ongelma ja lopputuotoksena on uusi ja aiempaa parempi ratkaisu ongelmaan. Lähestymistapa mahdollistaa

hyvin pragmaattisen totuuskäsityksen, jossa totuutena pidetään niitä asioita, jotka toimivat käytännössä. Tutkimuksessa kuitenkin tukeudutaan vahvasti aiempaan teoriaan. (Ojasalo ym. 2014, 66)

Opinnäytetyön toteutus tapahtui kehittämisprosessinomaisesti. Toteutukseen sisältyi kuusi vaihetta, joista ensimmäisessä tunnistettiin kehittämiskohde. Toisessa vaiheessa hankittiin syvällinen teoreettinen ja käytännöllinen tieto kehittämiskohteesta. Kolmannessa vaiheessa laadittiin ratkaisu kehittämiskohteelle ja kehitettiin analyysityökalu tahallisesti aiheutettujen turvallisuusriskien analysointiin. Neljännessä vaiheessa analyysityökalua testattiin käytännössä, siitä kerättiin palautetta ja sitä jatkokehitettiin. Viidennessä vaiheessa tarkasteltiin analyysityökalun teoriakytkentöjä ja arvioitiin sen uutuusarvoa. Kuudennessa vaiheessa tarkasteltiin analyysityökalun soveltuvuusalueen laajuutta ja pohdittiin jatkotutkimustarpeita. (Ojasalo ym. 2014, 67 - 68)



Kuva 1. Opinnäytetyön kehittämisprosessi.

Tässä opinnäytetyössä analyysityökalun kehittäminen tapahtui tyypillisestä konstruktiivisesta tutkimuksesta hieman poiketen niin, että opinnäytteen tekijä vastasi työkalun kehittämisestä ja työkalua arvioitiin kolmesti työn tilaajan toimesta, jolloin työkalua myös jatkokehitettiin saadun palautteen perusteella. Työkalua käytettiin osana opetusta ja testattiin käytännössä yhteensä neljän päivän ajan Puolustusvoimien turvallisuusjohtamisen opintotokokonaisuuden 1 lähijaksolla.

Koko opinnäytetyön prosessin ajan pyrittiin pitämään yllä realistisen evaluaation periaatteen mukaista arvioivaa työotetta. Tällöin omaan työhön suhtaudutaan tutkivasti ja muuttuvasti. Keskeistä on prosessien ja työn sisäisen logiikan avaaminen, jotta pystytään tuomaan esiin toimintaan ja sen sisältöön liittyvät piirteet. Huomiota on kiinnitetty siihen, että kehittämisprosessia tarkastellaan sekä vaiheittain että kokonaisuutena ja prosessia taustoitetaan riittävästi. (Anttila 2007, 83 – 86)

Opinnäytetyön aineistoa analysoitiin laadullisen sisällönanalyysin menetelmin. Opinnäytetyötä varten kerätty aineisto on käyty systemaattisesti läpi pyrkien säilyttämään objektiivisuus työn eri vaiheissa. Laadullisella sisällönanalyysillä on tässä opinnäytetyössä pyritty löytämään yhtäläisyyksiä tutkittavasta aineistosta ja saamaan tiivistetty kuvaus tutkittavasta aiheesta ja ilmiöstä. (Tuomi & Sarajärvi 2018, 85 – 90)

1.3 Aineistonhankintamenetelmät

Opinnäytetyön teoriaosuuden aineisto kerättiin tekemällä aineistohakuja kirjastotietokantoihin kuten Laurea Finna, MPKK Finna ja Laurea Libguides. Tämän lisäksi relevanttia tietoa haettiin hauilla hyödyntäen Google scholar -hakupalvelua. Yhdessä ja erikseen sekä eri muodoissa käytettyjä hakusanoja olivat muun muassa *riskienhallinta, turvallisuus, turvallisuusriski, suojaaminen, turvallisuusuhka, uhka-arvio, haavoittuvuus, force protection, riskmanagement, critical asset protection, criticality assessment, threath analysis* ja *vulnerability assessment*. Opinnäytetyön aineisto valikoitui perustuen lähteiden tieteellisyyteen ja relevanttiuteen opinnäytetyön aiheen kannalta.

Opinnäytetyön empiirinen aineisto kerättiin havainnoinnilla ja strukturoidulla kyselyllä. Havainnointi toteutettiin työn tekijän toimesta Puolustusvoimien turvallisuusjohtamisen opintokokonaisuuden 1 lähijaksolla. Havainnointi sisälsi neljän päivän ajan kehitetyn työkalun käytön neuvontaa pulmatilanteissa ja yleistä tarkkailua. Kurssille osallistui kaksikymmentäkaksi oppilasta puolustushallinnosta sekä poliisihallinnosta ja kaikilta kerättiin kyselylomake. Lomake jaettiin kurssilaisille kurssin toisena päivänä ja kerättiin pois kurssin viimeisenä päivänä.

1.4 Aikaisempi tutkimus ja keskeisimmät lähteet

Riskienhallintaa käsittelevää kirjallisuutta ja tutkimuksia on saatavilla runsaasti, mutta aikaisempaa kotimaista tutkimusta tahallisesti aiheutettujen turvallisuusriskien arvioinnista on saatavilla vain vähän. Pääosa opinnäytetyön lähteistä koostuu ulkomaisista tutkimusraporteista, tieteellisistä artikkeleista ja ammattikirjallisuudesta sekä Yhdysvaltojen asevoimien ohjesäännöistä.

Tapio Pihlajamäki (2010) on tehnyt Maanpuolustuskorkeakoulun maanpuolustuksen Professional Development- ohjelmaan lopputyön *Tahallisesti aiheutettujen turvallisuusriskien uhka- ja haavoittuvuusanalyysit*. Työssään Pihlajamäki käsittelee, millaisella mallilla tahallisesti

aiheutettujen turvallisuusuhkien tasoa voitaisiin arvioida ja miten näihin uhkiin liittyviä omia haavoittuvuuksia pystytään mittaamaan. Pihlajamäki toteaa, ettei Suomessa ole tutkittu tarpeeksi uhkan ja haavoittuvuuden käsitteitä ja niiden keskinäisiä suhteita. Raportissaan Pihlajamäki kiistää olemassa olevien riskienanalysointimenetelmien toimivuuden tahallisesti aiheutettujen turvallisuusuhkien analysoinnissa.

Mirkka Kreus (2010) on kirjoittanut väitöskirjaansa pohjautuvan teoksen *Terrorismin torjunta Suomessa*, jossa hän käsittelee tapoja arvioida terroristisessa tarkoituksessa toteutettuja turvallisuusuhkia. Hän käsittelee työssään myös turvallisuuden käsitettä ja uhkaan liittyvää psykologista ulottuvuutta.

Ulkomaisista tutkimuksista mainittakoon William L. McGillin (2008) väitöstutkimus *Critical asset and portfolio risk analysis for homeland security*, jossa hän on kehittänyt kvantitatiivisen todennäköisyyksiin perustuvan riskienanalyysimenetelmän kriittisen infrastruktuurin suojaamiseksi. Menetelmässä huomioidaan vihamielisen toimijan dynaaminen käytös ja taipumus keskittyä houkuttelevimpiin kohteisiin sekä keskittyminen puolustajan heikkouksiin yllätyksen saavuttamiseksi. Menetelmä huomioi haavoittuvuudet perinteiseen tapaan järjestelmien heikkouksina, mutta ottaa huomioon myös vaste- ja palautumiskyvyt. McGill väittää, että hyödyntämällä hänen mallinsa parametreja saadaan tuotettua hyödyllistä tietoa turvallisuusuhkista hyvin vähäisilläkin lähtötiedoilla.

Willis, Morral, Kelly ja Medby (2005) ovat tehneet voittoa tavoittelemattoman RAND -tutkimusorganisaation nimissä tutkimusraportin *Estimating Terrorism Risk*, joka liittyy Yhdysvaltain turvallisuudesta vastaavan viraston ohjelmaan parantaa turvallisuutta ja yleistä valmiutta estää terroriteot, reagoida niihin ja toipua niistä. Raportissa käsitellään muun muassa terrorismiriskiä ja sen osakomponentteja uhka, haavoittuvuus ja seuraukset. Raportissa otetaan huomioon myös terrorismiriskeihin liittyvät epävarmuustekijät. Raportti antaa suosituksia siihen, miten kotimaan turvallisuuden resurssit tulisi jakaa terrorismiriskien hallitsemiseksi.

Joni Halli on tutkinut Laurea ammattikorkeakouluun tekemässään opinnäytetyössä Naton Force Protection -doktriinia turvallisuusjohtamisen mallina. Johtopäätöksissään Halli tuo esiin, että doktriini toimii hallintoyksikön turvallisuusjohtamisen mallina. Jatkotutkimustarpeissa Halli nostaa esiin tarpeen selvittää tarkemmin riskienhallinnan prosessin vaiheet ja kehittää sopivat työkalut, jotka testataan käytännössä. (Halli 2018)

2 Naton Force Protection -doktriini

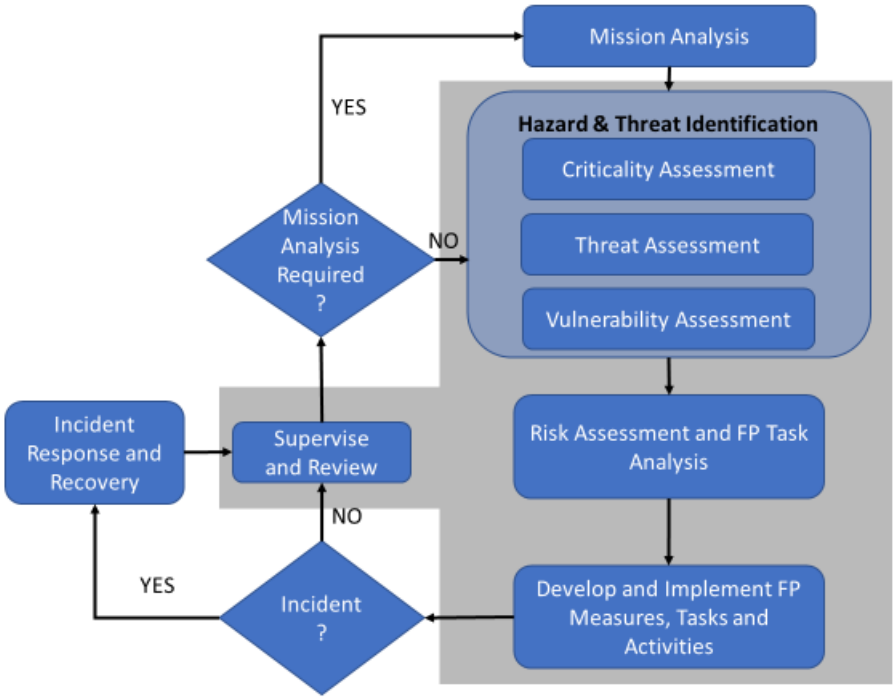
Force protection tarkoittaa joukkojen suojaamista. Tässä opinnäytetyössä käytetään termiä suojaaminen. Naton A*llied Joint Doctrine for Force Protection* (AJP-3.14 2015, 1-1) määrittelee suojaamisen vapaasti suomennettuna seuraavasti: toimenpiteet ja keinot pienentää henkilöstön, tilojen, kaluston, materiaalin, operaation ja aktiviteettien haavoittuvuutta uhkilta ja vahingoilta säilyttäen toiminnan vapauden ja operatiivisen vaikuttavuuden täten myötävaikuttaen tehtävän onnistumiseen.

Suojaamisen koordinointi on keskeistä kaikkien operaatioiden suunnittelu ja toteutusvaiheissa. Suojaamisen koordinointi tulee tapahtua horisontaalisesti ja vertikaalisesti strategisella, operatiivisella ja taktisella tasolla. Vertikaalisuus tarkoittaa sitä, että ylemmän komentajan tahto on muotoiltu selkeästi ja se näkyy alemman tason suunnitelmissa. Horisontaalinen koordinointi taas auttaa integroimaan ja synkronoimaan useat syötteet suunnitelmiin esikunnan eri toimialan edustajilta. Tärkeimpänä päämääränä on, että eri tasojen komentajat osaavat ottaa huomioon riittävät suojaamisen toimenpiteet ja keinot suhteutettuna tehtävään ja uhkaan. (AJP-3.14 2015, 1-2 – 1-3)

Suojaamisen suunnittelua ohjaavat periaatteet ovat uhkien arviointi ja riskienhallinta. Tarkkaan ja reaaliaikaiseen tiedustelutietoon kaikista lähteistä perustuva uhka-arvio antaa perusteita suojaamisen menetelmien ja keinojen suunnitteluun. Se auttaa komentajaa keskittymään tehtävän onnistumisen kannalta kriittisiin tekijöihin. Uhkien jatkuva seuraaminen ja arviointi mahdollistaa suojaustasojen säätämisen tilanteen mukaisesti. Sotilaallinen toiminta on lähtökohtaisesti riskiluonteista toimintaa. Tämän vuoksi suojaaminen perustuu riskienhallintaan eikä riskien poistamiseen. Liiallisella riskien välttämisellä voi olla negatiivinen vaikutus tehtävän onnistumisen kannalta. Uhkista, vahingoista ja haavoittuvuuksista johtuvia riskejä tulisi arvioida jatkuvasti oikean suuruisten suojaamisen toimenpiteiden varmistamiseksi. Tehokas suojaamisen suunnittelu vaatii integroitua vahinkojen ja uhkien tunnistamista, riskianalyysiä ja riskienhallintaa. Koska kaikkea toimintaa ei voida jokaisessa tilanteessa suojata, tulee tehtävän kannalta kriittisten tekijöiden suojaamisesta varmistua. (AJP-3.14 2015, 1-4 – 1-5)

2.1 Riskienhallinta Force Protection -doktriinissa

Force Protection -doktriinin mukainen suojaamisen malli on kuvattu kuvassa 2. Riskienhallinnan osiot on osoitettu tummemmalla taustalla. Tämän opinnäytetyön keskiössä on kuvassa sinisellä korostetut riskienhallinnan osiot uhkien tunnistaminen, kriittisyysanalyysi, uhka-analyysi ja haavoittuvuusanalyysi.



Kuva 2. Force Protection -prosessi. (AJP-3.14 2015, 3-4)

Malli mahdollistaa suojaamisen toteuttamisen siten, että riskienhallinnan avulla joukkoja johtava komentaja voi tehdä informoidun päätöksen, joka sisältää analyysin ja arvioinnin kriittisten tekijöiden, uhkien sekä haavoittuvuuksien osalta. Kriittisistä tekijöistä, uhkista ja haavoittuvuuksista muodostuu riski. Riskin osalta arvioidaan, miten siihen vastataan ja mitä vaikutuksia sillä on tehtävälle. Tämän kaiken toteuttaminen asettaa kuitenkin komentajalle ja tämän esikunnalle monia haasteita lähtien siitä, että riskienhallinnan pitäisi olla J3:n johtamaa syötteiden tullessa J2:lta. Mahdolliset suojaamisen toimenpiteet taas koskettavat kaikkia J1:stä J9:iin. (Alexander 2006, 19 – 20) (J1 – J9 tarkoittavat esikunnan eri toimialoja tai toimistoja. Tässä järjestelmässä J tulee englanninkielisestä sanasta *joint* eli yhteinen. Numerot 1 – 9 tarkoittavat järjestyksessä seuraavaa: 1=henkilöstö, 2=tiedustelu, 3=operaatiot, 4=logistiikka, 5=suunnittelu, 6=kommunikaatio, 7=koulutus, 8=talous ja 9=siviili-sotilasyhteistyö.)

Systemaattisella kriittisyysarviolla komentaja voi paremmin ymmärtää ja tunnistaa tehtävälleen tärkeitä kriittisiä tekijöitä. Systemaattisesti tehty arvio tunnistaa avaintekijät ja infrastruktuurin ja arvioi tekijän vaikutuksen joukon kykyyn jatkaa tehtävää, jos kriittinen tekijä menetetään. Arvioinnissa tulee ottaa huomioon arvioitavien tekijöiden rahallinen arvo, korvattavuus, vaikutus toimintaan ja vaadittava aika tekijän uudelleen rakentamiseen tai korvaamiseen. Tekijöitä voivat olla kaikki asiat, joilla on arvoa: ihmiset, infrastruktuuri, välineet, informaatio, tilat sekä abstraktimmat asiat kuten maine, moraali ja strateginen etu. Kriittisten kohteiden tunnistaminen vaatii analyysiä ja harkintakykyä. Kaikki tekijät eivät ole tehtävän täyttymisen kannalta kriittisiä eikä kaikkia tekijöitä, joilla on jotain arvoa, voida suojata.

Kriittisyysarvion päätarkoituksena on tuottaa tietoa kriittisistä tekijöistä ja määrittää, voidaanko kriittisten tekijöiden toiminnot toteuttaa myös jollain toisella keinolla. (Annex 3-10 – Force Protection 2019, 28 – 29)

Jotta joukkojen komentaja ei toimi sokkona, tulee hänen tietää, millaisia uhkia on odotettavissa. Uhka-arvion tulee perustua monipuolisista lähteistä kerättyyn tiedustelutietoon. Monipuolisilla tietolähteillä pyritään välttämään tietoaukkoja sekä voittamaan vastustajan harhauttamispyrkimykset. Tiedustelutiedon pitäisi vastata uhkiin, jotka koskettavat tehtävän toteuttamista tai henkilöstöä. Tiedustelun pitäisi antaa tietoja muun muassa terrorismista, rikollisista yhteisöistä, ulkomaisista tiedusteluyhteisöistä ja mahdollisen vastustajan sotilaallisista voimista tarpeellisin osin. Tekemällä synteesiä erilaisista lähteistä voidaan analysoida ja tunnistaa indikaattoreita tulevista uhkista. Tyypilliset tietolähteet on avattu seuraavassa kuvassa. (Annex 3-10 – Force Protection 2019, 29 – 30) Riskitason arvioinnin jälkeen arvioidaan riskienhallinnan keinot, jotka otetaan käyttöön. (AJP-3.14 2015, 3-4)

TYYPILLISET TIETOLÄHTEET UHKA-ARVIOON
AVOIMIEN LÄHTEIDEN TIEDOT: - uutiset, media, julkaisut, julkiset kuulemiset, avoimet internet -lähteet, sosiaalinen media
LAINVALVONNAN TIEDOT: - lainvalvontakanavien sääntelemä tiedon keräys, säilyttäminen ja levitys
VALTIOLLINEN TIEDUSTELU- JA VASTATIEDUSTELUTIEDOT: - tiedusteluyhteisön tuotteet ja raportit
PAIKALLINEN ja ALUEELLINEN VIRANOMAISTIETO: - sotilaat ja poliisit, siviilit, yksilöt, joilla on paikallistuntemusta

Taulukko 1. Tyypilliset tietolähteet. (Annex 3-10 – Force Protection 2019, 30)

Haavoittuvuusarvion tulee kattaa ainakin seuraavat alueet: henkilöstö, välineet, tilat, infrastruktuuri ja operaatioalue. Haavoittuvuusarvioinnissa otetaan huomioon tunnistetut ja ennustetut uhkat henkilöstölle, tiloille tai muulle omaisuudelle niiden alueiden tunnistamiseksi, joilla resurssit ovat alttiita tehtävän toteuttamiseen heikentävästi tai estävästi vaikuttaville toimille. Haavoittuvuuksien tunnistamista ja arviointia ei pidä toteuttaa vain uhka-arvion pohjalta. Esimerkiksi terroristit ovat onnistuneet iskemään sotilaskohteisiin, joissa suojaamisen toimenpiteet on toteutettu vastaamaan kohonneeseen terrorismin uhkaan. Myös sellaisiin siviilikohteisiin, joiden uhkatasoa hyökkäyksille on pidetty matalana, on isketty. Historia näyttää siis, että arvoitu uhka ei välttämättä ole tarkka kuvaus todellisesta uhkasta. Tämän takia on merkittävää arvioida ja tunnistaa myös haavoittuvuuksia. (Annex 3-10 – Force Protection 2019, 31)

Riskienarvioinnissa verrataan henkilöstön, omaisuuden tai jonkin tekijän menetyksen tai vahingon suhteellista vaikutusta suhteessa epätoivotun tapahtuman suhteelliseen todennäköisyyteen. Kun kriittisyys-, uhka- ja haavoittuvuusarvioinnit on suoritettu, komentajalla tulisi olla tarvittavat tiedot päätöksenteon tueksi siitä, millainen riskitaso ollaan valmiita hyväksymään. (Annex 3-10 – Force Protection 2019, 31)

3 Tahallisesti aiheutettujen turvallisuusriskien arviointi

3.1 Riskienhallinnan periaatteet

Vaatimukset riskienhallintaan ovat usein sisäisiä tai ulkoisia. Sisäisiä vaatimuksia ovat esimerkiksi organisaation riskienhallintapolitiikka ja sisäiset ohjeet, kuten toimintaohjeet ja jatkuvuudenhallinnan ohjeistukset. Sisäiset vaatimukset ovat usein joko organisaation johdon asettamia tai niistä on sovittu organisaation strategiaa muodostettaessa. Ulkoisia vaatimuksia riskienhallinnalle tulee yleisistä laeista ja säädöksistä, toimialan ja riskienhallinnan standardeista sekä asiakas- tai sidosryhmävaatimuksista. Ulkoiset vaatimukset voivat olla tulla viranomaisten vaatimuksista esimerkiksi tiettyjen standardien seuraamiseksi tai ne voivat olla asiakkaiden ja yhteistyökumppanien kanssa sopimuksiin kirjattuja seikkoja. (Ilmonen, Kallio, Koskinen & Rajamäki 2013, 17-18)

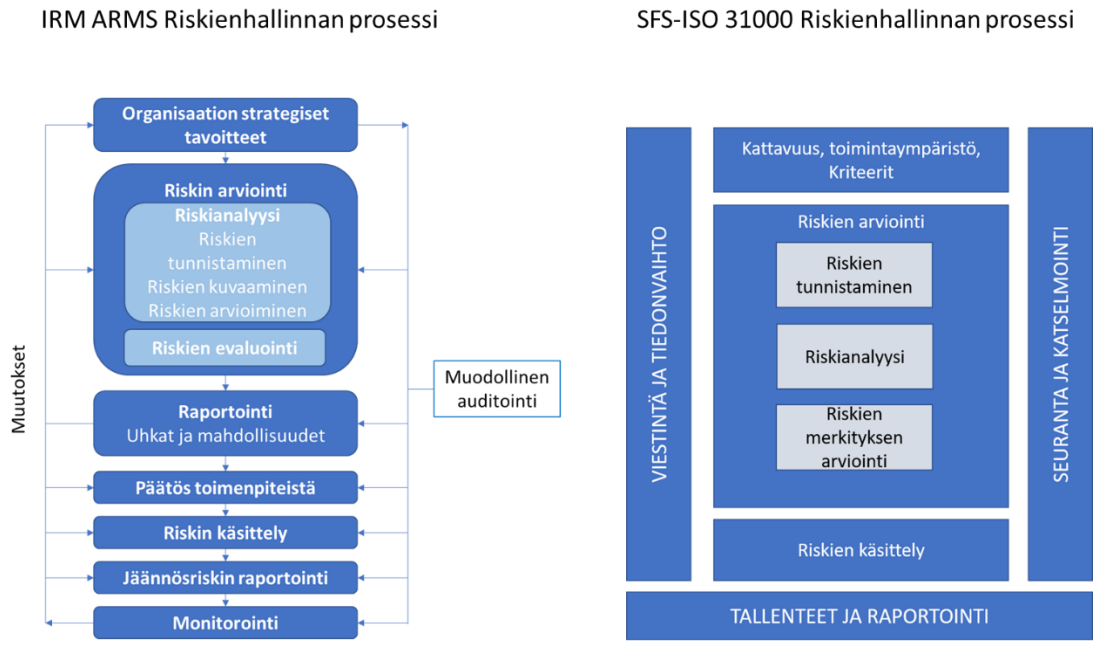
Riskienhallinnan kentän laajuutta kuvaa se, että riskienhallinnan osa-alueiksi on tunnistettu muun muassa henkilöturvallisuus, yritysturvallisuus, ympäristö, tuoteturvallisuus, toimintavarmuus, muutostenjohtaminen, tapahtumatutkinta, kriisienhallinta, yhteistyökumppanit, yhteiskuntavastuu sekä laite- ja tuotantosuunnittelu. (Ilmonen ym. 2013, 17) Riskienhallinnan osa-alueita on monia muitakin ja ne voivat vaihdella organisaation luonteen mukaan. Riskienarviointityötä helpottamaan riskit voidaan jakaa myös riskilajeihin.

Riskien jaotteluja erilaisiin riskilajeihin on olemassa useita. Yksi eniten käytetyistä jaotteluista jakaa riskit vahinkoriskeihin, operatiivisiin riskeihin, taloudellisiin riskeihin ja strategisiin riskeihin. Tässä jaottelussa riskit jaetaan riskin lähteiden ja riskityypin mukaan. Vahinkoriskit ovat esimerkiksi sellaisia riskejä, joilla ei pääsääntöisesti ole kuin negatiivisia vaikutuksia. Tyypillisiä vahinkoriskejä ovat esimerkiksi työtapaturmat tai ympäristöriskit, kuten luonnonilmiöiden aiheuttamat vahingot tiloille tai materiaalille. Operatiivisia riskejä ovat esimerkiksi tapahtumat, jotka ovat seurausta henkilöstön toiminnasta, järjestelmistä tai toimimattomista organisaation sisäisistä prosesseista. Operatiiviset riskit voivat liittyä joko suoraan tai välillisesti organisaation toimintaan ja niillä voi olla haitallisia vaikutuksia maineeseen. Taloudelliset riskit liittyvät organisaation taloudenhallinnan prosessien toimivuuteen ja varojen riittävyyteen. Taloudelliset riskit voivat aiheutua esimerkiksi verokohtelusta, investointien tuottamattomuudesta tai kirjanpidollisista virheistä. Strategiset riskit ovat luonteeltaan pitkäaikaisia ja liittyvät organisaation pitkäaikaisiin tavoitteisiin. Strategisiin riskeihin liittyy epävarmuustekijöitä, jotka vaikuttavat organisaation tavoitteen saavuttamiseen. Operatiivisten, taloudellisten ja strategisten riskien vaikutukset voivat olla luonteeltaan positiivisia tai negatiivisia. Riskien luokittelu auttaa tunnistamaan, arviomaan ja yhteismitallistamaan riskejä monipuolisemmin sekä lisäämään ymmärrystä riskien välisistä suhteista. (Ilmonen ym. 2013, 55-59; Riskikompassi)

Vahinkoriskit	Operatiiviset riskit	Taloudelliset riskit	Strategiset riskit
- terveys ja työturvallisuusriskit - henkilöstöriskit - ympäristöriskit - omaisuuden vahingoittumisriskit - luonnonkatastrofeihin liittyvät riskit - toimitilaturvallisuuden riskit - koneiden, laitteiden ja kulkuneuvojen toimintahäiriöihin tai hajoamisiin liittyvät riskit	- organisaatioon ja johtamiseen liittyvät riskit - teknologiaan liittyvät riskit - tietoturvallisuusriskit - tuotannolliset, toimintaprosesseihin ja tehokkuuteen liittyvät riskit - liiketoiminnan keskeytymisriskit - tuottavuusriskit - projektitoimintaan liittyvät riskit - henkilöstön osaamiseen liittyvät riskit - sopimus- ja vastuuriskit - kriisitilanteisiin liittyvät riskit - rikokset	- maksuvalmiusriskit - korkotuotto- ja menoriskit - valuuttariskit - luotonhallintariskit - maariskit - sopimusriskit - veroriskit - kirjanpidon ja talousraportoinnin riskit - pääomarakenteen riskit	- liiketoiminnan kehitykseen liittyvät riskit - liiketoimintaympäristöön liittyvät riskit - markkinariskit - teknologiariskit - poliittisen, taloudellisen ja kulttuurisen kehityksen riskit - regulaatioriskit - globaaleista ilmiöistä johtuvat riskit - viestintäriskit - M&A-riskit

Taulukko 2. Riskilajit riskilähteiden ja riskityypin mukaan (Ilmonen ym. 2013, 55; Riskikompassi). Taulukkoa on muokattu opinnäytetyön tekijän toimesta.

Jokaisella organisaatiolla tulisi olla käytössään riskienhallintaprosessi. Riskienhallintaprosessin tarkoituksena on luoda puitteet riskien tunnistamiselle, arvioinnille, käsittelylle, raportoinnille ja seuraamiselle. Riskienhallinnanprosessikuvauksia on olemassa kolmen kohdan prosesseista todella laajoihin prosesseihin. Liian yksinkertaisessa riskienhallinnan prosessissa on vaarana, ettei se huomioi kaikkia riskienhallinnan osa-alueita ja eri tekijöitä riittävästi. (Ilmonen ym. 2013, 72-74)



Kuva 3. Riskienhallinnan prosesseja (IRM 2002, 4; SFS-ISO 31000 2018, 14).

Kuvassa 3 on kahden eri standardin mukaiset riskienhallinnan prosessit. Prosessit ovat luonteeltaan hyvin samantyyppisiä, mutta sisältävät joitain toisistaan poikkeavia asioita. Esimerkiksi viestintä ja tiedonvaihto on huomioitu *International Organization for Standardization (ISO) 31000* (2018, 14) riskienhallinnan standardissa, mutta ei *The Institute of Risk Management (IRM) A Risk Management Standard (ARMS)* -standardissa (2002, 4). IRM ARMS taas huomioi esimerkiksi jäännösriskin, jota ISO 31000:ssa ei ole mainittu. Standardien noudattaminen ei ole pakollista tai itsetarkoitus, mutta moni viranomainen voi vaatia tiettyjen standardien noudattamista. Organisaation kannalta on oleellista osata muodostaa riskienhallintaprosessista sellainen, että se istuu hyvin organisaation muuhun toimintaan ja tulee osaksi sitä.

Riskienhallinta on luonteeltaan tukeva prosessi. Onkin tärkeää, että se on osa organisaation pääprosesseja. On hyvin merkittävää, että riskienhallinta tehdään oikeaan aikaan ja se saadaan kytkettyä osaksi organisaation pää- ja muita prosesseja. Oikea-aikaisella riskienhallinnalla säästetään aikaa ja resursseja sekä vältytään vahingoilta ja saadaan tehostettua organisaation toimintaa. Riskien tunnistaminen kannattaa tehdä esimerkiksi organisaation strategian ja tavoitteiden asettamisen jälkeen, jotta niistä saadaan riittävä tausta ja fokus riskienhallinnalle. (Ilmonen ym. 2013, 62)

Naton suojaamisen mallin mukaisen riskienhallinnan prosessin (kuva 2) vaiheet vastaavat osin yleisimpien standardien prosesseja. Yksi merkittävä prosessissa kuvattu ero verrattuna yleisimpiin standardeihin on tehtäväanalyysi. Riskienhallinnan prosessiin on kuvattu myös muutokset tehtävään, jos riskiympäristössä tapahtuu muutoksia tai riskinarvioinnin niin edellyttäessä. Riskiarvioinnin perusteella tehty päätös toiminnan muutoksista tai keskeyttämisestä perustuu aina arvioon jäännösriskistä siten, että riskin käsittely on huomioitu. (AJP-3.14 2015, 3-4 & B-1 – B-5)

3.2 Turvallisuus- ja riskikäsitteistä

Sanastokeskuksen ja Turvallisuuskomitean tuottamassa *Kokonaisturvallisuuden sanastossa* (2017, 16) turvallisuus määritellään ”tilaksi, jossa uhkat ja riskit ovat hallittavissa”. Sanastossa tarkennetaan vielä, että turvallisuudella voidaan tarkoittaa toimintoja, joilla pyritään pitämään uhkat ja riskit hallinnassa tai sillä voidaan tarkoittaa myös tunnetta siitä, että uhkat ja riskit ovat hallinnassa. Englannin kielelle käännettynä turvallisuudelle on kaksi vastinparia: *security* ja *safety*. Näillä termeillä on hieman eri merkitykset, mikä on johtanut siihen, että suomeksi puhutaan kovasta turvallisuudesta ja pehmeästä turvallisuudesta. *Security* viittaa kovaan turvallisuuteen, millä tarkoitetaan tarkoitukselliselta vahingoittavalta toiminnalta suojassa olemista, kuten rakennuksen turvallisuutta aseellista voimankäyttöä, väkivaltaa tai rikollista toimintaa käyttävää hyökkääjää vastaan. *Safety* viittaa pehmeään turvallisuuteen, joka ei kovan turvallisuuden tavoin vaarannu tahallisista toimista. Pehmeä turvallisuus vaarantuu esimerkiksi onnettomuuksien tai tapaturmien takia.

Mirkka Kreus (2010, 32 - 35) on kirjoittanut, että turvallisuus on itsessään hyvin hankala määritellä, koska se on luonteeltaan hyvin suhteellinen ja subjektiivinen käsite. Hän argumentoi myös, että turvallisuus pitää sisällään valtiolliset, sosiaaliset, hyvinvointivaltiolliset, kulttuuriset, ekologiset, yhteisölliset ja terveydelliset lähtökohdat eli lähes kaikki inhimillisen elämän sektorit. Yksi tapa hahmottaa turvallisuutta on jaotella se turvattomuuteen, turvallisuuteen ja ei-turvallisuuteen. Turvallisuus on tilanne, jossa on olemassa uhka ja keino sen torjumiseksi. Turvattomuuden tilanteessa keinoa uhkan torjumiseksi ei ole. Ei-turvallisuus on tilanne, jossa ei ole uhkia ja siten ei tarvetta turvallisuudellekaan. Yhtä kaikki subjektiivisuuslauseen mukaan turvattomuus, turvallisuus ja ei-turvallisuus ilmentyvät kaikki jokaiselle hieman eri tavalla, koska toiselle turvaton voi olla jollekin toiselle aivan turvallista.

Turvallisuutta voidaan kuvata menetelmänä ja tunnetilana, jolla saadaan muutettua riskien aiheuttamaa negatiivista tunnetilaa positiivisemmaksi. Kreusin mukaan olisikin mielekkäämpää keskustella riskeistä kuitenkaan hylkäämättä turvallisuus -käsitettä, koska se kuvaa hyvin sitä tunnetilaa, johon tulisi pyrkiä. Riskiajattelu kuitenkin auttaa keskittämään ajattelua siihen, mikä uhkaa ja mikä on uhattuna sekä kuinka vakava ja todennäköinen uhka on. (Kreus 2010, 35 – 36)

Riski määritellään usein joksikin kielteiseksi asiaksi tai tapahtumaksi riskin todennäköisyyden ja vaikutuksen yhteistekijänä. Riski = todennäköisyys ja vaikutus. (Hopkin 2010, 17-18) Perinteisessä riskiarvioinnissa riskejä on arvioitu niiden todennäköisyyden ja vakavuuden suhteen. Todennäköisyys kuvastaa tapahtumiin liittyvää epävarmuutta ja vakavuus tapahtumien merkittävyyttä. Todennäköisyyttä voi olla mahdollista arvioida realistisesti vain, jos meillä on riittävä määrä historiadataa, josta voidaan tilastollisesti määrittää jonkin tapahtuman todennäköisyys. Tyypillisesti vakavuutta painotetaan riskiarvioissa, koska todennäköisyyden ja vakavuuden ollessa samanarvoisia arvioidaan todennäköisyydeltään erittäin todennäköinen ja ei-vakava riski samanarvoiseksi erittäin vakavan ja epätodennäköisen riskin kanssa. (Mäkinen 2007, 104 - 108) Edellä kuvatun niin sanotun teknisen riskianalyysin lähtökohtana on, että riskit voidaan tunnistaa tieteellisin menetelmin ja niitä voidaan hallita. Taloudellisista lähtökohdista tehtävässä analyysissä vaikutukset tai epätoivottavat seuraukset kuvataankin hyötyinä. Riskien esittäminen hyötynäkökulmien kannalta auttaa liittämään ne paremmin päätöksentekoprosessiin. (Kreus 2010, 42 – 43)

Riski voidaan nähdä varsinkin yritysmaailmassa myös positiivisena asiana, joka voi johtaa esimerkiksi suurempiin voittoihin tai liiketoiminnan kasvuun. ISO 31000 -riskienhallinnan standardissa riski on määritelty epävarmuuden vaikutuksiksi tavoitteisiin. Tällöin vaikutus on poikkeama odotetusta, joka voi olla positiivinen, negatiivinen tai molempia. (SFS-ISO 31000 2018, 6)

Tahallisesti aiheutettujen turvallisuusriskien arviointi poikkeaa hieman perinteisemmästä riskienarvioinnista. Tahallisuutta arvioitaessa on otettava huomioon myös psykologinen ja sosiokulttuurillinen lähestymistapa. Psykologinen lähestyminen laajentaa riskin käsittämään subjektiivisia käsityksiä mahdollisuuksista, ennakkoluuloista ja kontekstisidonnaisista tekijöistä. Käsitykset riskistä voivat vaihdella kulttuurillisten ja sosiologisten ryhmien välillä suurestikin. Sosiokulttuurillisessa näkökulmassa riskit yhdistetään arvoihin sekä yksilön ja yhteisön intresseihin. (Kreus 2010, 43 – 45)

Turvallisuusriskejä voidaan arvioida monesta eri lähtökohdasta. Arviointia voidaan toteuttaa esimerkiksi omaisuuslähtöisesti (*asset-driven*), uhkalähtöisesti (*threat-driven*) tai tapauslähtöisesti (*event-driven*). Omaisuuslähtöinen arviointi ottaa huomioon omat kriittiset tekijät ja niiden haavoittuvuudet. Tässä lähestymistavassa pyritään löytämään omia heikkoja kohtia, joita vastustaja voisi hyödyntää, ottamatta huomioon onko kyseisestä tapahtumasta minkäänlaista tiedustelu- tai historiatietoa saatavilla. Uhkalähtöinen lähestymistapa taas perustuu tiedustelu- ja historiatietoihin ja voi usein sisältää ennalta määritettyjen uhkaskenaarioiden kautta tapahtuvaa arviointia. Tapauslähtöisessä arvioinnissa keskitytään käytännössä vain historiadataa erilaisten riskien alullepanevien tapahtumien tunnistamiseksi. Tapauslähtöinen lähestymistapa sopii riskien alullepanevien tapahtumien tunnistamiseen, mutta on rajoittunut vain ihmisten keräämän historiadatan varaan. Kriittisyyslähtöinen lähestymistapa nostaa esiin kaikki mahdolliset uhkaskenaariot vähentäen ontologista epävarmuutta ja yllätyksen mahdollisuutta, koska se ei rajoitu vain siihen mitä tiedämme mahdollisista vastustajistamme. (McGill 2008, 15 -16)

Tahallisesti aiheutetut turvallisuusriskit käsitetään tässä opinnäytetyössä negatiivisina ja turvallisuutta alentavina kokonaisuuksina. Tämän luvun tarkoituksena on esittää teoriaan pohjautuen, mitä tahallisesti aiheutettujen turvallisuusriskien arviointi tarkoittaa ja miten se voitaisiin tehdä. Tämän opinnäytetyön kontekstissa turvallisuusriski muodostuu luvussa 2 esitellyn suojaamisen mallin mukaisesti kriittisyydestä, uhkasta ja haavoittuvuudesta. Turvallisuusriski = uhka x (kriittisyys + haavoittuvuus).

3.3 Kriittisyys

Minkä vuoksi kriittisyyttä pitäisi arvioida? Force Protection -doktriinissa on lyhyt maininta kriittisyyden arvioimisesta. Sen mukaan kriittisyys on jotain, jolla on arvoa ja jota halutaan suojata. Kaikkea ei voida aina kaikissa tilanteissa suojata, koska usein suojaamiseen käytettävät resurssit ovat rajalliset. Kriittisyysarviolla pyritään tunnistamaan omalle toiminnalle kaikkein merkittävimmät kohteet ja laittamaan ne tärkeysjärjestykseen. (Annex 3-10 – Force Protection 2019, 28 – 29)

Perinteisemmässä riskien analysointiprosessissa kriittisyysanalyysi mielletään tehtäväksi riski- tai vika-analyysin jälkeen. Tällöin kriittissyysanalyysissä määritellään vikamuotojen tai riskien

merkitys laadullisesti, puolilaadullisesti tai määrällisesti. Kriittisyysanalyysi voi perustua siihen todennäköisyyteen, jolla jokin vika tai riski johtaa epätoivottuun tapahtumaan. Kriittisyys voi perustua myös riskilukuun eli prioriteettiin. (SFS-EN 31010 2013, 44)

Sotilaallisessa toiminnassa ja suojaamisen kontekstissa tehty kriittisyysarvio liittyy usein itselle tärkeisiin toimintoihin, arvoihin ja kohteisiin. Kriittisyyttä määritellään enemmän sen kautta, millainen vaikutus jonkin tekijän menettämisellä on omaan toimintaan. Tämä arvio tehdään usein ensimmäisenä, jolloin koko muun prosessin fokus keskittyy itselle tärkeisiin tekijöihin. Liiketoiminta-analyysi (BIA eli Bisness Imbact Analysis) toimii saman tapaisesti kuin sotilaallisessa mielessä tehtävä kriittisyysanalyysi tai -arvio. Liiketoiminta-analyysissä pyritään keskeisten liiketoiminnan toimintojen, prosessien ja niihin liittyvien resurssien sekä keskeisten riippuvuussuhteiden tunnistamiseen ja näiden kriittisyyden arviointiin. Liiketoiminta-analyysin avulla määritetään prosessien ja resurssien (tekniikka, ihmiset, materiaalit) kriittisyys omien tavoitteiden saavuttamisessa. Samalla tunnistetaan myös sisäisiä ja ulkoisia riippuvuussuhteita. Liiketoiminta-analyysissä tehty kriittisyysarvio perustuu riskiin ja haavoittuvuuteen, joiden avulla vahvistetaan organisaation keskeiset prosessit ja niiden kriittisyys. Lopputuotoksena tulisi olla prioriteettiluettelo organisaation kriittisistä prosesseista sekä tieto niiden keskeytymisestä aiheutuvista taloudellisista ja toiminnallisista vaikutuksista. Lisäksi pitäisi olla tunnistettuna kaikki tukiresurssit, joita kriittiset prosessit tarvitsevat toimiakseen. Keskeistä koko prosessissa on tuottaa ymmärrystä kriittisistä prosesseista, jotka tuottavat organisaatiolle kyvyn sille asetettujen tavoitteiden saavuttamiseksi. (SFS-EN 31010 2013, 76 - 80)

Kriittisyyttä tarkastellaan usein yhdessä vaikutuksen kanssa. Mitä suurempi vaikutus kriittisen tekijän menettämisellä on, sitä suurempi on myös kriittisyystaso. McGill, Ayyub ja Kaminskiy (2007, 1267 – 1269) ovat kirjoittaneet artikkelin *Risk Analysis for Critical Asset Protection*, joka käsittää kriittisten kohteiden suojaamisesta tehtävää riskiarviota. Heidän esittämässään mallissa seuraamus- ja kriittisyysarvio tehdään uhkaskenaarioiden tunnistamisen jälkeen. Keskeisiä tietoja, jotka vaikuttavat kohteen kriittisyyteen ovat suurin mahdollinen menetyksen määrä, fyysinen haavoittuvuus ja vastatoimien tehokkuus. Keskeistä on arvioida jokaisen uhkaskenaarion seuraukset ja menetykset olettaen, että vastustaja onnistuisi toteuttamaan uhkaskenaarion täysimääräisesti. Huomio analyysissä on kohteen omistajan näkökulmassa ja siinä, miten kohteen menettäminen vaikuttaa toiminnan jatkumiseen tai henkilöstön suojaamiseen.

Yacov Haimes (2011, 1176 - 1177) on kirjoittanut kriittisyydestä terrorismin näkökulmasta. Hän määrittelee kriittisyysvaikutusjärjestelmän (*criticality-imbact system*) olevan osoitus kansallisesti vaalitusta tai arvostetusta rakenteesta tai muistomerkistä, jonka konkreettisesta uhkasta aiheutuvien aineellisten ja aineettomien seurausten katsotaan olevan merkittäviä sekä kansalaisille että terroristiverkostoille. Hyökkäys kriittisyysvaikutusjärjestelmää vastaan aiheuttaisi laajoja tunteellisia vaikutuksia ja kiinnittäisi yleisön ja median huomion uutisin,

kommentein ja visuaalisin kuvin. Esimerkkejä kriittisyyteen vaikuttavista järjestelmistä ovat suuret kansalliset monumentit, historialliset tai uskonnolliset kohteet ja muut järjestelmät, joilla on kansallinen tai kansainvälinen symbolinen merkitys.

Brashear Jerry ja Jones William (2010, 6) ovat kirjoittaneet riskien analysoimisesta ja hallinnasta kriittisen kohteen tai omaisuuden suojaamisessa. Heidän esittämän mallin mukaan ensimmäinen vaihe prosessissa on omaisuuden luokittelu. Kriittinen omaisuus tai kohde tunnistetaan ja arvioidaan mahdollisten sellaisten seurausten suuruus, joita erilaiset uhkat tai vaarat voivat aiheuttaa. Arvioitavat kohteet pitävät sisällään ne tekijät, jotka ovat suoraan tekemisissä tärkeiden toimintojen tai tavoitteiden saavuttamisen kanssa sekä ne kohteet, jotka tukevat näitä ja infrastruktuuri, josta ne ovat riippuvaisia. Arvioitavat kohteet voivat siis olla fyysisiä rakennuksia, tietoteknisiä järjestelmiä, informaatiota, henkilöstöön liittyviä tai kriittisiä ulkopuolisia toimijoita. Sellaiset kohteet tai omaisuus, jotka ovat suoraan kytköksissä tehtävän täyttämiseen, ovat usein kohtuullisen helppoja tunnistaa. Sen sijaan tukevat kohteet, joista nämä ensisijaiset kriittiset kohteet ovat riippuvaisia, voivat olla hankalampia tunnistaa. Esimerkiksi puhtaan veden saamiseksi vedenpuhdistamossa on järjestelmiä, jotka vaativat sähköä toimiakseen ja ilman puhdasta vettä ei organisaatio voi täyttää tavoitteitaan. Silloin sähkölinjat voivat olla yksi tukeva arvioitava kriittinen kohde. Jos taas on olemassa esimerkiksi varamenetelmä sähkön tuotannolle, kuten generaattorit riittävällä polttoaineen määrällä, voidaan sähkölinjoja pitää vähemmän kriittisenä kohteena, jolloin sitä ei tarvitse myöhemmin arvioida.

Yhteenvetona arvioitava kriittisyys on siis suhteessa turvallisuusriskien vaikutuksiin. Kriittisyyttä on arvioitava kohteen tärkeyden, korvattavuuden ja arvon (rahallinen, maineellinen ja toiminnallinen) mukaan. Jokaisen organisaation on määritettävä itse oman toimintansa kannalta kriittiset tekijät. Eri tekijöiden kriittisyys voi vaihdella toimintaympäristön luonteen ja oman toiminnan mukaan.

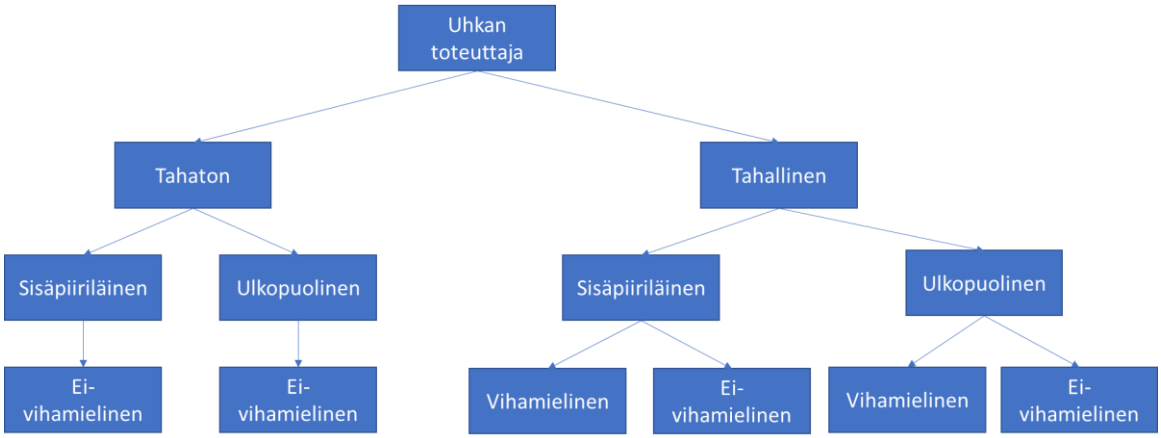
3.4 Uhka

Uhka on käsitteellisesti määritelty monella eri tavalla. Kirjallisuudesta sanaa uhka käytetään myös monessa eri merkityksessä. Suomen kotimaisten kielten keskuksen kielitoimiston sanakirjan (2019) määritelmän mukaan uhka on ”mahdollisesti toteutuva epämieluisa, pelottava tai vahingollinen seikka; vaara, paha, joka uhkaa tai jonka voi kuvitella uhkaavan jotakuta tai jotakin.” Turvallisuuskomitean ja Sanastokeskus TSK ovat koonneet kokonaisturvallisuuden sanastoa ja määrittäneet uhkan mahdollisesti toteutuvaksi haitalliseksi tapahtumaksi tai kehityskuluksi. Uhka kuitenkin eroaa esimerkiksi vaarasta siten, että sillä on epävarmempi kehityskulku ja vaara taas on käytännöllisempi ja riskienhallinnallisin toimenpitein käsiteltävä asia. Ero uhkan ja vaaran merkityksissä on käytännössä siinä, että vaaran on määritetty olevan ”todennäköisesti toteutuva tai jo toteutunut, parhaillaan vaikuttava haitallinen tapahtuma tai kehityskulku.” (Kokonaisturvallisuuden sanasto 2017, 40 – 41). Uhkan tulkintaa

monimutkaistaa toki hieman myös se, kuten kielitoimiston sanakirjassakin määritellään, että uhka on jotain, minkä voidaan kuvitella aiheuttavan jotakin vaaraa jollekin. Ihmisten tulkinnat siitä mikä tosiallisesti voisi uhata jotakin vaihtelevat tulkitsijan mukaan, jos yhteistä määritelmää uhkasta ei ole.

John Moteff (2005, 6- 7) on määritellyt uhkaa siten, että se on mikä tahansa indikaattori, tilanne tai tapahtuma, jolla on potentiaalia aiheuttaa vahinkoa omaisuudelle. Uhka voi olla myös vihamielisen toimijan aikomus ja kyky ryhtyä toimiin, jotka voisivat olla haitallisia puolustavan tahon intresseille.

Uhka voidaan jaotella niiden toteuttajan motivaation mukaan. Kaikki uhkat voivat olla tahattomia tai tahallisia. Esimerkiksi sähkökatko voi olla tahaton luonnon sääilmiöiden seurauksena, mutta se voidaan yhtä hyvin aiheuttaa tahallisesti. Uhkan toteuttaja voi olla sisäpiiriläinen tai ulkopuolinen taho. Uhkan tarkoitus voi myös olla vihamielinen tai vihamielinen. Seuraava kuva havainnollistaa uhkan toteuttajan motivaatiota suhteessa uhkaan. (Vidalis 2003, 14) Kuvassa ei Vidalis ei kuitenkaan huomioi tahattomasti syntyviä uhkia, jotka eivät ole henkilön toteuttamia, kuten luonnononnettomuudet.



Kuva 4. Uhkien jaottelu uhkan toteuttajan motivaation perusteella. (Vidalis 2003, 14)

3.4.1 Uhkien tunnistaminen

Uhkien tunnistamiseen pätee monilta osin samat lainalaisuudet kuin riskien tunnistamiseen. Riskien arviointimenetelmien standardin (SFS-EN 31010 2013, 22) mukaan riskien tunnistaminen on niiden löytämisen, tuntemisen ja tallentamisen prosessi. Riskien tunnistamisen tarkoituksena on löytää niitä tilanteita, jotka vaikuttavat organisaation tavoitteiden saavuttamiseen. Standardi ohjeistaa kolmenkymmenyhden riskienarviointimenetelmän käytön, joista kaksikymmentäkuusi on soveltuvia tai erittäin soveltuvia myös riskien tunnistamiseen. Näistä mainittakoon esimerkkinä aivoriihi, tarkastusluettelot, vaara-analyysit, ohjatut tai osittain ohjatut haastattelut, Delfoi -menetelmä ja syy-vaikutusanalyysi. Nämä menetelmät voivat

olla näyttöön perustuvia ja historiatietoja tarvitsevia menetelmiä. Riskejä voidaan tunnistaa myös järjestelmällisesti asiantuntijaryhmän toimesta kysymysluetteloiden avulla. Riskien tunnistamisen tarkkuuden ja kattavuuden varmistamiseksi standardissa suositellaan käytettävän aivoriihi- ja Delfoi -menetelmiä niin sanottuina tukimenetelminä jonkin muun riskintunnistamismenetelmän rinnalla. Riskien tunnistamisprosessissa tulisi yksilöidä riskien syyt ja lähteet, tapahtumat ja tilanteet tai olosuhteet, joilla voi olla vaikutusta organisaation tavoitteisiin. (SFS-EN 31010 2013, 22 - 40)

Uhkien tunnistamisessa tulee hyödyntää samankaltaisia menetelmiä kuin riskien tunnistamissa on totuttu käyttämään. Uhkien tunnistusvaiheessa tulisi uhkat kategorisoida niiden tyypin (esimerkiksi sisäpiiriläinen, terrorismi, sotilaallinen tai ympäristö), aikeen tai motivaation, triggereiden (tapahtumat, jotka voivat panna alulle hyökkäyksen), suorituskykyjen (taidot, erityistieto ja pääsy materiaaliin tai välineisiin), metodien (yksittäiset itsemurhapommittajat, autopommit, suora hyökkäys, kyberhyökkäys) ja trendien (millaisia tekniikoita on käytetty aiemmin) mukaan. Hyödyllisiä tietoja uhkien tunnistamiseksi voidaan saada tiedusteluyhteisöltä, lainvalvonnasta vastaavilta viranomaisilta, asiantuntijoilta, uutisista, analyyseistä ja tutkimalla menneitä tapahtumia. Uhkien tunnistamisessa voidaan hyödyntää myös ”red team” -ajattelua, missä pyritään ajattelemaan kuten vihamielinen taho suunnitellessaan iskua. (Moteff 2005, 7).

Vaikka uhkien tunnistamisessa keskitytään siihen, millaisia uhkia jokin toimija kykenisi toteuttamaan, tulee tässäkin vaiheessa hyödyntää aivoriihtä ja vastaavia menetelmiä sellaisten uusien ja potentiaalisten uhkien tunnistamiseksi, joista ei ole olemassa historiadataa tai esimerkiksi tiedustelulta saatuja viitteitä. Uhkien tunnistamisessa on pyrittävä löytämään myös yllättäviä toimintavaihtoehtoja ja pyrittävä vähentämään niin kutsuttujen mustien joutsenien mahdollisuutta. Nassim Nicholas Taleb (2008) käyttää kirjassaan *The black swan: The impact of the highly improbable* vertauskuvaa, jossa yleisen käsityksen mukaan kaikki maailman joutsenet ovat valkoisia, kunnes eurooppalaisen ihmisen rantautuessa Australiaan kohdattiin ensimmäinen musta joutsen. Tämä vertauskuva kuvastaa hyvin ihmisen oppimisen ja ajattelun rajoituksia ja sitä miten yksi uusi havainto voi romuttaa koko aiemman käsityksemme jostakin asiasta.

3.4.2 Uhkien analysointi

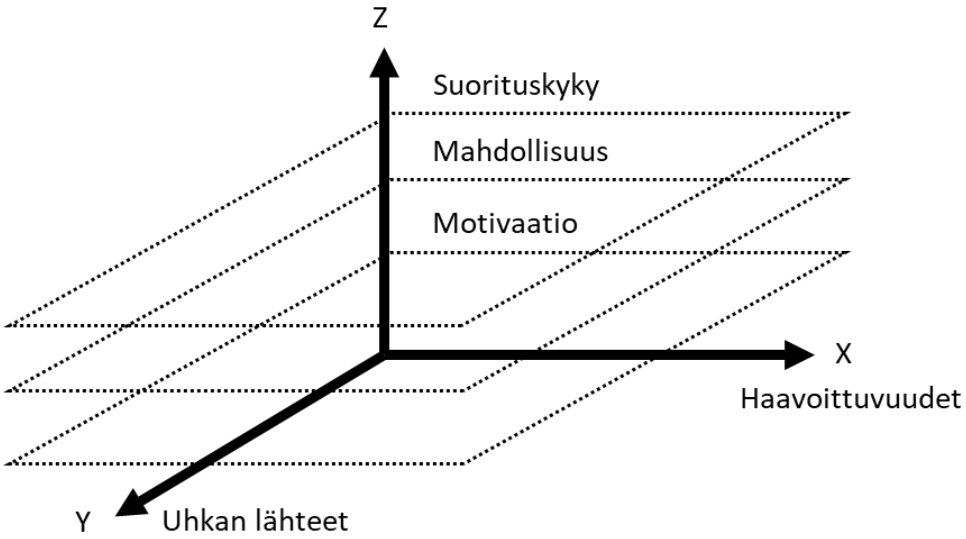
Turvallisuutta heikentävät tahallisesti aiheutetut uhkat ovat niin kutsutusti epäsymmetrisiä uhkia eikä niitä pystytä analysoimaan kovin tarkasti todennäköisyyteen ja vaikutukseen perustuvalla arviointimenetelmällä (Mäkinen 2007, 105). Epäsymmetrisyys pitää sisällään myös Kreusin (2010, 43) mainitseman psykologisen faktorin. Epäsymmetrisiä uhkia muodostava esimerkiksi terrorismi, informaatiosodankäynti ja rajat ylittävä ammattirikollisuus (Mäkinen 2007, 105).

Toisin kuin luonnollisesti esiintyviä, onnettomuuksia tai teknisiä uhkia, ei tahallisesti aiheutettuja uhkia ole mielekästä arvioida niiden tilastollisen todennäköisyyden mukaan (Pihlajamäki 2010, 41). Tahallisesti aihetuttuja uhkia pitäisi tarkastella myös niiden toteuttajien kautta, koska nämä uhkat voivat olla kekseliäitä, ennalta-arvaamattomia ja innovatiivisia keinoja tuottaa vahinkoa perustuen hyökkääjän käsitykseen riskistä, palkkiosta ja mahdollisuudesta. (McGill 2008, 35)

Tapio Pihlajamäki (2010, 43 - 46) on esitellyt Maanpuolustuskorkeakoulun turvallisuusalan laajan ammatillisesti pätevöittävän koulutusohjelman lopputyössään ensimmäisten joukossa Suomessa mallin, jossa tahallisesti aiheutettuja turvallisuusuhkia arvioidaan vihamielisen toimijan kautta tämän aikeen ja suorituskyvyn kautta. Pihlajamäki (2010, 70) toteaa, että tahallisesti aiheutettujen turvallisuusriskien analysoinnissa uhkia analysoitaessa aie ja kyky kuvaavat paremmin toteutuvan uhkan mahdollisuutta, mutta kokonaisriskienhallinnassa ei pidä unohtaa teknistä näkökulmaa.

Yhdysvaltojen National Intelligence Universityn apulaisprofessori Kevin P. Riechle (2013) on esitellyt uhkien analysointiin mallin, jossa uhka on aikeen, suorituskyvyn ja mahdollisuuden tulo. Aie kuvaa tekijän halua toteuttaa uhka. Suorituskyky kuvaa tekijän fyysisiä keinoja toteuttaa uhka. Mahdollisuus kuvaa ajallista ja tilallista suhdetta, mikä tekijällä on kohteeseen, johon tämä aikoo toimia. Jos joku näistä uhkan osatekijöistä puuttuu, pienenee uhka.

Tekijän motivaatiosta, suorituskyvystä ja mahdollisuudesta kirjoittavat myös yhteisessä konferenssijulkaisussaan tohtorit Stilianos Vidalis ja Andrew Jones (2005, 10 – 14). He argumentoivat, että uhka-arvion tarkoitus on olla joko ennaltaehkäisevä tai korjaava ja uhka-arvio voidaan tehdä joko ennen kuin jokin järjestelmä on otettu käyttöön tai järjestelmän tai käyttöönoton jälkeen. Vidalis ja Jones esittävät, että uhkan lähdettä pitäisi tarkastella kolmessa ulottuudessa. X-akselilla ovat omat kriittisen tekijän haavoittuvuudet, jotka on tunnistettu erikseen. Y-akselilla ovat uhkan lähteet, jotka on jo myös tunnistettu aiemmin. Z-akselilla ovat suorituskyky, motivaatio ja mahdollisuus. Nämä tekijät muodostavat omat tasonsa Z-akselilla. Seuraavassa kuvassa on graafinen esitys tästä kolmen ulottuvuuden matriisimallista. Tarkempaan uhka-arviontiin pitäisi valikoitua vain ne uhkat, jotka sijaitsevat kaikilla tasoilla ja kaikissa ulottuvuuksissa.



Kuva 5. Kolmiulotteinen uhkan ja haavoittuvuuden tarkastelu. (Vidalis ja Jones 2005, 10)

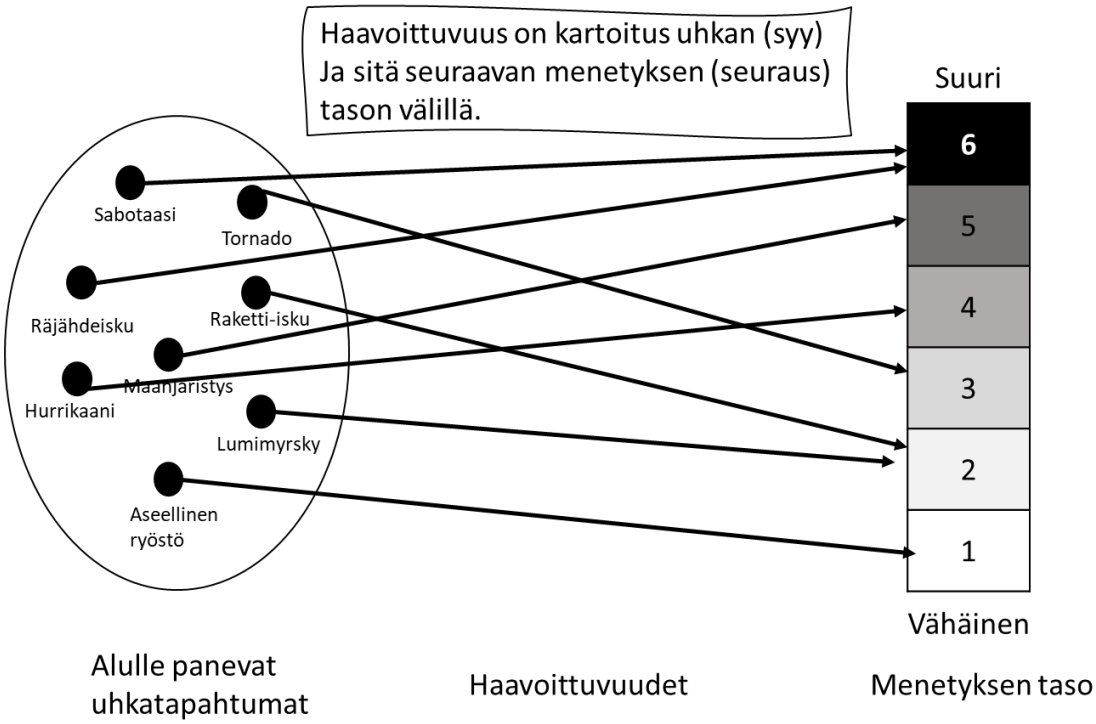
Yhdysvaltain hallinnon Department of Defence (DoD) riskienhallinnan kurssimateriaalissa esitetään malli, jossa uhkaa analysoidaan aikeen, suorituskyvyn ja historian suhteen. Tässä mallissa päätös uhkatasosta tehdään vastaamalla kyllä tai ei -kysymyksiin uhkan toteuttajan aikeesta, suorituskyvystä ja historiasta toteuttaa analysoitava uhka. Kolme kyllä -vastausta muodostaa kriittisen uhkan ja kolme ei -vastausta muodostaa matalan uhkan. Uhkalle arvioidaan myös asteikolla 0.00 – 1 numeraalinen arvio, joka auttaa tekemään eroja uhkien välille ja muodostamaan täten prioriteettijärjestystä. (Risk Management for DoD Security Programs 2019, 6 -12)

Uhkaa tarkastellaan monissa eri lähteissä hieman erilaisin näkökulmin. Yhteistä edellä käsitellyissä lähteissä on käytännössä se, että uhkan todennäköisyyteen tai mahdollisuuteen on sisällytetty vihamielisen toimijan aie sekä kyky toteuttaa uhka. Tämä kuvastaa keskittymisen kohdentumista aina johonkin tiettyyn vihamieliseen tahoon, joka voi olla yksilö tai organisaatio. Tämän kaltaisella analyysillä voidaan tuottaa tarkempaa tietoa tietyssä toimintaympäristössä potentiaalisista turvallisuusuhkista.

3.5 Haavoittuvuus

Sanastokeskus TSK:n termipankki määrittelee haavoittuvuuden alttiudeksi tietoturvaan kohdistuville uhkille. ”Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.” (TEPA-termipankki 2019) Haavoittuvuudesta on löydettävissä monenlaisia määritelmiä, mutta yksi yleisesti tunnettu ja hyväksytty määritelmä on, että haavoittuvuus on mikä tahansa järjestelmän tai toiminnon osa, joka heikentää sen kykyä selviytyä häiritsevässä tai vihamielisessä ympäristössä. Haavoittuvuus

voidaan nähdä myös yhdenlaisena kartoituksena syystä seuraukseen eli uhkasta mahdollisiin vaikutuksiin. (McGill & Ayyub 2007, 25- 28)



Kuva 6. Haavoittuvuuden suhde uhkaan ja vaikutuksiin. (McGill & Ayyub 2007, 28)

Voittoa tavoittelemattoman RAND -tutkimusorganisaation tutkijat Willis, Morral, Kelly ja Medby (2005, 7) ovat määritelleet haavoittuvuutta seuraavalla tavalla: haavoittuvuus on järjestelmän luontaisten tilojen (esimerkiksi fyysisen, teknisen, organisatorisen, kulttuurisen) ilmentyminen, josta voi aiheutua vahinkoa, jos vastustaja hyökkää siihen. Toisaalta voidaan ajatella, että jos uhkaa pidetään voimina, jotka toimivat jotain systeemiä vastaan, voidaan haavoittuvuus nähdä näiden systeemien kykynä tai pikemminkin kyvyttömyytenä vastata tähän uhkaan. Tämä lähestymistapa edellyttää, että haavoittuvuutta tarkastellaan liittyen johonkin tiettyyn uhkaan. (Willis ym. 2005, 7) Tyypillisesti riskienhallinnan kokonaisuudessa haavoittuvuuteen voidaan eniten itse vaikuttaa. (Schnaubelt, Larson & Boyer 2014, 27)

3.5.1 Haavoittuvuuksien tunnistaminen

Usein toteutunut uhka tai haitallinen tapahtuma ei ole ollut yksi riskienhallintaprosessissa tunnistetuista uhkista, vaan se on toteutunut jonkin asteisena yllätyksenä (Annex 3-10 – Force Protection 2019, 31). Yllätyksen pääasiallinen lähde on epäsopiva tai epätehokas epävarmuuden luokittelu. Kun tilanne tai esiin noussut ongelma on uusi tai ainutlaatuinen, haasteeksi muodostuu käytettävissä olevan tiedon hyödyntäminen siten, että saadaan rajattua kaikki kuviteltavissa olevat lopputulemat järkevään muotoon. Mitä enemmän tiedämme vastustajasta, sitä varmempia olemme omista suojaamisen keinoistamme, kun taas vähäisempi tieto

vastustajasta auttaa meitä keksimään laajemman valikoiman mahdollisuuksia. Tunnistamalla omia haavoittuvuuksia pystytään mahdollisesti tunnistamaan uusia uhkia. Voimme myös tunnistaa haavoittuvuuksia, jotka eivät ole näkyviä potentiaaliselle pahantekijälle (McGill 2008, 26 ja 36).

Turvallisuusjärjestelmät perustuvat yleensä heikoin lenkki -periaatteelle, jolloin epäonnistuminen mahdollisen vihamielisin toimijan havaitsemisessa, pysäyttämisessä tai estämisessä antaa tälle paremman mahdollisuuden onnistua hyökkäyksessään ja muodostaa turvallisuusjärjestelmien osalta haavoittuvuuden. (McGill 2008, 55).

3.5.2 Haavoittuvuuksien analysointi

Haavoittuvuuksien analysointi voi olla tehokkaampaa ja johtaa pienempiin epävarmuustekijöihin kuin pelkkä perinteinen uhka-arvio, koska uhka-arviot voivat usein yli- tai aliarvioida uhkia. Tämän takia uhka-arvioihin tulisikin suhtauta pienellä varauksella. (Willis ym. 2005, 14)

Haavoittuvuuksien analysoinnissa tutkitaan myös sitä mahdollisuutta, joka tietyllä vihamielisellä toimijalla on ohittaa vastatoimet ja toteuttaa isku kohdetta vastaan. Turvallisuusuhkissa todennäköisyys riippuu osaltaan puolustajan kyvystä suojata omat kriittiset tekijänsä epäämällä pääsy sensitiivisille alueille, havaita tunkeutujat, kohdata tunkeutujat ja neutralisoida tunkeutujat. (McGill ym. 2007, 1269)

William L. McGill ja Bilal M. Ayyub (2007, 43) esittävät artikkelissaan *The Meaning of Vulnerability in the Context of Critical Infrastructure Protection*, että kokonaishaavoittuvuus on jonkin systeemin herkkyys tietyn tasoisille menetyksille ja tappioille, jotka johtuvat jostain tietystä uhkatapahtumasta. Haavoittuvuuden ollessa uhkatapahtuman syyn ja tästä johtuvien seurausten eli tappioiden välinen kartoitus, voidaan haavoittuvuutta mitata uhkien ja tappioiden yhteisenä todennäköisyytenä. Tämä kokonaishaavoittuvuus voidaan jakaa kahteen kategoriaan: suojaushaavoittuvuudet ja vastehaavoittuvuudet. Suojaushaavoittuvuudet vaikuttavat vaurioiden syntymisen todennäköisyyteen suhteutettuna tiettyihin uhkatapahtumiin. Ne ovat suojaustoimenpiteitä, joilla pyritään minimoimaan vaurioiden todennäköisyyttä, ja joilla vähennetään kohteen saavutettavuutta ja parannetaan kohteen kovuutta. Vastehaavoittuvuudet vaikuttavat vaurioista johtuvien menetysten tasoon ja todennäköisyyteen, jotka ovat riippumattomia vaurion synnyttämän uhkatapahtuman luonteesta. Vastehaavoittuvuudet sisältävät toimenpiteitä, joilla pyritään minimoimaan menetyksen todennäköisyys. Toimenpiteillä pyritään myös parantamaan systeemien tappioidensietokykyä sekä vaste- ja palautumiskykyä.

Haavoittuvuuksia analysoitaessa on muistettava, että näkyvissä olevat kohteet ja haavoittuvuudet ovat todennäköisempiä kohteita hyökkäyksille kuin sellaiset kohteet, joita ei pystytä ulkopuolelta tunnistamaan. (McGill 2008, 36)

Yksi haavoittuvuuksien analysointiin luotu malli on CARVER -malli. CARVER tulee englannin kielen sanoista *critivality* (kriittisyys), *accessibility* (saavutettavuus), *recuperability* (toipumiskyky), *vulnerability* (haavoittuvuus), *effect* (vaikutus) ja *recognizability* (tunnistettavuus). CARVER -malli on kehitetty Yhdysvaltojen erikoisjoukkojen tarpeisiin vihollisen infrastruktuurin maalittamiseksi. CARVER -malli keskittyy vastustajan näkökulmaan ja mahdollista analyytikon tai arviointiryhmän määrittämisen kohteen kovuuden tai pehmeyden rikollisissa tai terroriteoissa. Mallissa kohteet arvioidaan ja pisteytetään kriteeriluettelon perusteella. Kriteerejä on mahdollista muuttaa tehtävän tai operaation tarpeiden mukaisesti. CARCER -malli sopii myös omien haavoittuvuuksien analysoimiseksi vastustajan näkökulmasta katsottuna. (Schnaubelt, Larson & Boyer 2014, 29 - 30)

Esimerkki CARVER -kriteereistä

Kriteeri	Suhteellinen arvoluokitus
Kriittisyys (C)	
Välitön tuotanto pysähtyy tai 100 prosenttia supistuu. Kohde ei voi toimia ilman omaisuutta.	10
Alle yhden päivän pysähdys tai 75 prosentin supistuminen tuloksessa, tuotannossa tai palvelussa.	8
Alle viikon pysähdys tai 50 prosentin supistuminen tuloksessa, tuotannossa tai palvelussa.	6
yli viikon pysähdys tai 25 prosentin supistuminen tuloksessa, tuotannossa tai palvelussa.	4
Ei merkittävää vaikutusta.	1
Saavutettavuus (A)	
"Stand off" -aseita voidaan käyttää.	10
Aidan sisäpuolella, mutta ulkotiloissa.	8
Rakennuksen sisällä, mutta maan tasalla.	6
Rakennuksen sisällä, mutta toisessa tai kellarikerroksessa. Vaatii laskeutumista tai kiipeämistä.	4
Ei saavutettavissa tai ainoastaan erittäin hankalasti saavutettavissa.	1
Toipumiskyky (R)	
Huoltaminen tai korvaaminen uudella vaatii kuukauden tai enemmän.	10
Huoltaminen tai korvaaminen uudella vaatii viikon - kuukauden.	8
Huoltaminen tai korvaaminen uudella vaatii 72h - 1 viikon.	6
Huoltaminen tai korvaaminen uudella vaatii 24h - 72h.	4

Huoltaminen tai korvaaminen uudella onnistuu samana päivänä.	1
Haavoittuvuus (V)	
Haavoittuvainen pitkän kantaman maalinosoituksille, käsiaseille tai pienille räjähteille (painoltaan alle 2kg).	10
Haavoittuvainen kevyille panssarintorjunta-aseille tai räjähteille (painoltaan 2,5-5kg).	8
Haavoittuvainen keskiraskaille panssarintorjunta-aseille, räjähteille (painoltaan 5-15kg) tai tarkasti sijoitetuille pienille räjähteille.	6
Haavoittuvainen raskaalle panssarintorjunta-aseistukselle, suurille räjähdemäärille (painoltaan 15-25kg) tai erikoisaseistukselle.	4
Haavoittuvainen vain kaikkein suorituskykyisimmälle aseistukselle.	1
Vaikutus (väestöön) (E)	
Ylivoimaiset positiiviset vaikutukset, mutta ei merkittäviä negatiivisia vaikutuksia.	10
Kohtalaisen positiiviset vaikutukset ja muutama merkittävä kielteinen vaikutus.	8
Ei merkittäviä vaikutuksia.	6
Kohtalaiset kielteiset vaikutukset ja muutama merkittävä positiivinen vaikutus.	4
Ylivoimaiset negatiiviset vaikutukset, eikä merkittäviä positiivisia vaikutuksia.	1
Tunnistettavuus (R)	
Selkeästi tunnistettavissa kaikissa olosuhteissa ja kaukaa ja tunnustamiseen tarvitaan vähän tai ei ollenkaan henkilöstön koulutusta.	10
Helposti tunnistettavissa käsiaseiden käyttöetäisyydeltä ja vaatii vähän henkilöstön koulutusta tunnistamiseksi.	8
Vaikea tunnistaa yöllä huonon sään aikana tai voidaan sekoittaa muihin kohteisiin tai niiden komponentteihin. Tunnustamiseen vaaditaan jonkin verran henkilöstökoulutusta.	6
Vaikea tunnistaa yöllä tai huonoilla sääolosuhteilla (jopa käsiaseiden käyttöetäisyydeltä). Kohde voidaan helposti sekoittaa muihin kohteisiin tai komponentteihin ja vaatii tunnustamista varten laajaa henkilöstökoulutusta.	4
Kohteita ei voida tunnistaa missään olosuhteissa muuten kuin asiantuntijoiden toimesta.	1

Taulukko 3. Esimerkki CARVER -mallin kriteereistä. (Schnaubelt ym. 2014, 31 - 32)

Edellä olevassa CARVER -mallin kriteeristössä on viisi kuvausta jokaista osa-aluetta kohti. Jokaisesta osa-alueesta valitaan arvioinnin kohteen kannalta sopivin kuvaus ja siihen liittyvä numeraalinen suhteellinen arvoluokitus. Tämän jälkeen arvot lasketaan yhteen ja saadaan kohteen haavoittuvuutta kuvaava lukuarvo.

Esimerkki CARVER -matriisista

Potentiaaliset maalit	C	A	R	V	E	R	YHT.
Kohde A	1	4	10	8	6	6	35
Kohde B	10	10	6	8	3	4	41
Kohde C	5	7	10	8	8	1	48

Taulukko 4. CARVER -matriisi. (Schnaubelt ym. 2014, 32)

Haavoittuvuuksia voidaan arvioida monella eri tavalla. Yksi usein helpoimmalta tuntuva tapa on kutsua asiantuntijoita koolle ja keskustella haavoittuvuuksien mahdollisuuksista. Kuitenkin jokaisesta kriittisestä tekijästä ja uhkasta muodostuvasta parista keskusteluun käytettävä aika voi venyä pitkäksi. Silloin voi olla haastavaa ylläpitää looginen ja johdonmukainen arviointiote lukuisien arvioitavien kohteiden osalta. (Brashear & Jones 2010, 9)

3.6 Yhteenveto

Tahallisesti aiheutettujen turvallisuusriskien arvioinnissa on huomioitava monia tekijöitä. Kriittisyysarviota tehdessä on erityisen tärkeää määrittää itselle tärkeät suojattavat kohteet, arvot, toiminnot, henkilöstö, tieto ja ne asiat, joilla on jotain arvoa omalle organisaatiolle. Kriittinen tekijä on sellainen asia, mikä on merkittävä organisaation tavoitteiden saavuttamiseksi. Kriittisyysarvion tuloksiin perustuvan uhka-arvion tekeminen auttaa säästämään ajallisia ja henkisiä resursseja, kun vain sellaisia uhkia tunnistetaan ja arvioidaan, jotka liittyvät kriittisiksi tunnistettuihin tekijöihin. Tässä on riskinä, että jotain merkittäviäkin uhkia jää tunnistamatta ja arvioimatta, jos niitä ei osata liittää johonkin kriittiseen tekijään. Toisaalta kriittisyysarviossa pitäisi olla tunnistettu ja arvioitu omien tavoitteiden tai tehtävän kannalta merkittävät tekijät, jolloin ei pitäisi olla sellaista vaaraa, että jokin uhka estäisi tavoitteiden saavuttamisen tai tehtävän onnistumisen. Kuitenkin esimerkiksi maine on usein sellainen tekijä, joka sotilaallisessa toiminnassa ei vaikuta alemman tason tehtävän toteuttamisen onnistumiseen, mutta sillä voi olla ylemmän tason tavoitteiden kannalta äärimmäisen suuri merkitys. Tässä tilanteessa olisi kokonaisuuden kannalta hyvin vahingollista sivuuttaa mainetta käsittävät uhkat.

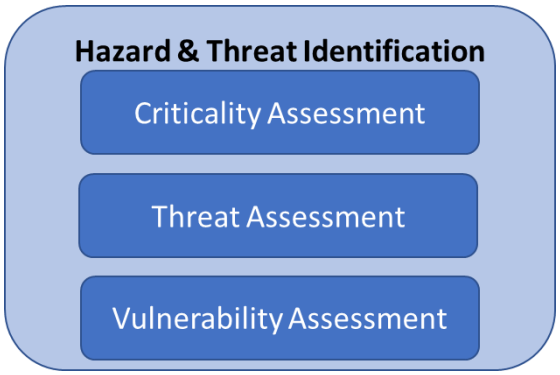
Uhka-arviota ei tulisi pitää absoluuttisena totuutena, koska se sisältää osia, joista osasta voi paikoin olla vaikeaa saada luotettavaa tietoa, kuten vihamielisen toimijan aikeesta toteuttaa jokin uhka. Tahallisesti aiheutettujen turvallisuusriskien arvioinnin kokonaisuudessa onkin tärkeä osa omien haavoittuvuuksien tunnistaminen ja arviointi. Kuten uhka-arvioon, myös haavoittuvuusarvioon on monia olemassa olevia malleja. Keskeisintä on toteuttaa

turvallisuusriskien arviointi sellaisia malleja hyödyntäen, jotka vastaavat oman organisaation toimintaan ja käsiteltävään riskityyppiin parhaiten. Ei voida olettaa, että talousriskeihin suunnatulla mallilla saadaan tahallisesti aiheutetuista turvallisuusriskeistä luotettavia tuloksia tai tuloksia ollenkaan.

4 Arviointityökalu

Opinnäytetyön tilaajan toiveena oli saada helppokäyttöinen työkalu tahallisesti aiheutettujen turvallisuusriskien arviointiin. Alusta asti oli selvää, että analyysityökalu pitäisi kehittää alustalle, joka toimisi kaikissa Puolustusvoimien järjestelmissä. Tämän vuoksi työkalua lähdettiin kehittämään Excel -ohjelmiston pohjalle. Tahallisesti aiheutettujen turvallisuusriskien arviointiin kehitettävän työkalun lähtökohtana oli, että se ei toimi pelkkänä tiedon dokumentointialustana, vaan siinä on kysymyksiä, joihin vastaamalla työkalu muodostaa riskiluvun ja esittää arvioinnin tulokset visuaalisesti selkeällä ja havainnollistavalla tavalla. Tässä luvussa esitellään Puolustusvoimien turvallisuusjohtaminen 1 -kurssin lähiopetusjaksolla testattua arviointityökalun versiota ja sen käyttöperiaatteita.

Alkusi työkalun kehittämisessä oli kaksi eri suuntausta. Ajatuksena oli, että työkaluja voisi kehittää kaksi erilaista, joista parempaa lähdettäisiin jatkokehittämään. Molemmat työkalut sisältäisivät Force Protection -riskienhallinnan prosessissa kuvatut kriittisyys-, uhka- ja haavoittuvuusarvioinnit. Ajankäytöllisistä syistä ja työn laajuuden takia työn tilaajan kanssa sovittiin, että työkalussa keskityttäisiin vain edellä mainittuihin kokonaisuuksiin ja esimerkiksi turvallisuusriskien pienentäminen ja hallintakeinot jätetään tällä erää työkalun ulkopuolelle.



Kuva 7. Arviointityökalun fokus. (AJP-3.14, 3-4)

Toinen kehitettävistä työkaluista perustui opiskelijan omaan näkemykseen ja toinen työkalu malliin, jossa on määritetty valmiit kriteerit kriittisyydelle, uhkalle ja haavoittuvuudelle. Jälkimmäiselle mallille oli jo olemassa taulukoita, joihin täytetään kriteerien mukaiset lukuarvot, joiden summana tai tulona taulukosta riippuen muodostuu riskiluku. Ajankäytöllisistä syistä ei lopulta ollut mahdollista kehittää kahta erilaista työkalua, jotka olisivat molemmat kurssin alkaessa riittävän valmiita testattavaksi. Tämä takia päädyttiin jatkokehittämään opiskelijan näkemyksen mukaista työkalua, koska sillä oli enemmän uutuusarvoa ja sitä kokeilemalla voitaisiin myös kehittää jotain uutta.

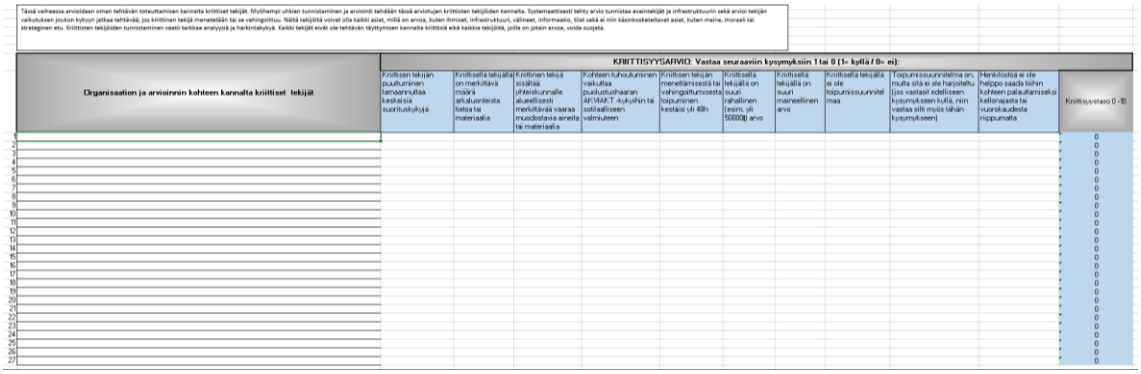
Kehitettäväksi valittu työkalu pitää sisällään kriittisyysarvion, uhka-arvion ja haavoittuvuusarvion. Työkalu jakaantui useampaan vaiheeseen ja jokaiselle vaiheelle on oma välilehtensä.

Suojaamisen mallin mukaisesti työkalua kehitettiin siten, että ensimmäisessä vaiheessa tunnistetaan ja arvioidaan oman toiminnan tai tehtävän täyttämisen kannalta kriittiset tekijät. Toisessa vaiheessa tunnistetaan uhkatapahtumia. Kolmannessa vaiheessa valitaan arviotavat uhkatapahtumat, tunnistetaan uhkan lähteet eli vihamieliset toimijat, tunnistetaan kriittinen tekijä, johon uhka liittyy ja tarkempi kohde, johon uhka kohdistuu. Kolmannen vaiheen tarkoituksena on muodostaa kokonaisuus, josta saadaan myöhempien arvioiden jälkeen muodostettua riskiluku. Tämä tarkoittaa sitä, että turvallisuusriski muodostuu työkalussa uhkatapahtumasta, uhkan lähteestä eli mahdollisesta toteuttajasta, kriittisestä tekijästä ja tarkemmasta uhkatapahtuman kohteesta. Neljännessä vaiheessa työkalussa arvioidaan uhkaa sen toteuttajan kautta. Uhka-arviossa otetaan huomioon uhkan toteuttajan aie ja suorituskyky toteuttaa tietty uhkatapahtuma. Viidennessä vaiheessa tunnistetaan uhkatapahtuman kohteesta haavoittuvuuksia ja kuudennessa vaiheessa arvioidaan näitä haavoittuvuuksia.

Arviointityökalussa osa-alueet on jaettu hieman pienempiin osiin ja näitä osia arvioidaan erivaiheissa vastaamalla kyllä tai ei -tyyppisesti. Käytännön toteutus Excel -sovelluksessa toteutettiin siten, että vastataan numeraalisesti yksi (1) tai nolla (0). Vastaamalla yksi kokonaisriski suurenee ja vastaamalla nolla kokonaisriski ei suurene. Haasteena tämän tyyppisten kysymysten muodostamisessa oli se, että osa kysymyksistä piti muotoilla positiivisiksi ja osa taas negatiivisiksi. Esimerkiksi ei voitu kysyä ”onko kohteella toipumissuunnitelmaa?” koska vastattaessa tähän kysymykseen kyllä eli yksi, riskiluku kasvaisi, vaikka todellisuudessa toipumissuunnitelma pienentäisi riskilukua. Tämän sijaan väittämä piti muotoilla seuraavaksi: ”kohteella ei ole toipumissuunnitelmaa”. Seuraavassa käsitellään tarkemmin, miten eri osa-alueilla tahallisesti aiheutettua turvallisuusriskiä työkalulla arvioidaan.

4.1 Kriittisyysarvio

Työkalun ensimmäinen vaihe on kriittisten tekijöiden tunnistaminen ja niiden arvioiminen. Työkalussa kuvattiin lyhyesti, millaisia asioita kriittiset tekijät voivat olla ja ohjeistettiin kirjaamaan tekijät taulukon vasemmassa reunassa olevaan sarakkeeseen. Kriittisiä tekijöitä arvioitiin tämän jälkeen kymmenellä arviointikysymyksellä ja määritelmällä. Taulukon oikeaan laitaan muodostuu kysymysten vastausten perusteella kriittisyystaso, joka on näiden kymmenen arviointikohdan summa.



Taulukko 5. Kriittisyysarvio.

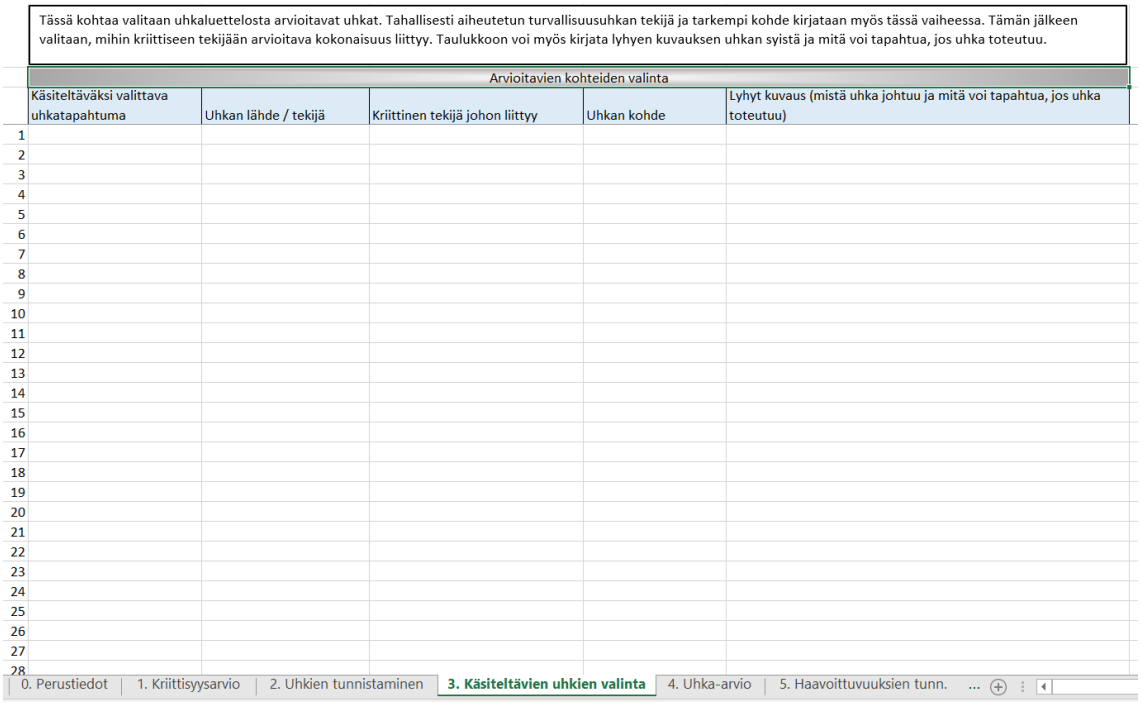
Kriittisen tekijän merkittävyyttä mittaavilla kymmenellä kysymyksellä mitataan tekijän merkittävyyttä organisaatiolle. Kysymykset mittaavat tekijän osuutta keskeisien suorituskykyjen osalta: sisältääkö kriittinen tekijä arkaluonteista tietoa tai materiaalia, sisältääkö tekijä vaarallisia aineita tai materiaaleja, tekijän vaikutusta sotilaalliseen valmiuteen, kriittisen tekijän rahallista ja maineellista arvoa sekä kriittisen tekijän korvattavuutta ja toipumiskykyä sisältäen toipumissuunnitelmat ja henkilöstön.

Kriittisyystaso muodostuu lukuarvojen nolla ja kymmenen välille. Lukemat 0-2 tarkoittavat vähäistä, 3-4 melko vähäistä, 5-6 haitallista, 7-8 merkittävää ja 9-10 erittäin merkittävää kriittisyystasoa.

4.2 Uhkien tunnistaminen ja käsiteltävien uhkien valinta

Uhkien tunnistaminen tehdään työkalussa omalla välilehdellään, jotta fokus pysyisi vain erilaisten uhkien tunnistamisessa ja niiden kirjaamisessa ylös. Uhkien tunnistamiseen ei työkalussa ollut mitään kysymyspatteria tai vastaavaa, vaan lyhyt ohjeistus siitä, että uhkien tunnistaminen tulisi toteuttaa mieluiten esimerkiksi aivoriihen avulla. Työkaluun ei kehitetty uhkien tunnistamista helpottavia kysymyksiä, koska sen ajateltiin ohjaavan liikaa ajatusta siten, että jotain merkittäviäkin uhkia voisi jäädä tunnistamatta.

Käsiteltävien uhkien valita pitää sisällään sellaisten tunnistettujen uhkatapahtumien valinnan, jotka liittyvät aikaisemmassa vaiheessa tunnistettuihin ja arvioituihin kriittisiin tekijöihin. Tämä rajaus tehtiin sen takia, ettei työkalussa arvioitavien uhkien määrä ja samalla arviointiin käytettävä aika nousisi liian suureksi. Tämä vaihe on työkalun toimivuuden kannalta tärkeä, koska siinä niin sanotusti naitetaan yhteen tiedot käsiteltävästä uhkatapahtumasta, vihamielisestä toimijasta eli uhkan toteuttajasta, kriittisestä tekijästä ja uhkan kohteesta. Yhtä riviä arvioidaan työkalussa kokonaisuutena ja riskiluku muodostuu myöhemmässä vaiheessa tästä kokonaisuudesta.



Tässä kohtaa valitaan uhkaluettelosta arvioitavat uhkat. Tahallisesti aiheutetun turvallisuusuhkan tekijä ja tarkempi kohde kirjataan myös tässä vaiheessa. Tämän jälkeen valitaan, mihin kriittiseen tekijään arvioitava kokonaisuus liittyy. Taulukkoon voi myös kirjata lyhyen kuvauksen uhkan syistä ja mitä voi tapahtua, jos uhka toteutuu.

Arvioitavien kohteiden valinta				
Käsiteltäväksi valittava uhkatapahtuma	Uhkan lähde / tekijä	Kriittinen tekijä johon liittyy	Uhkan kohde	Lyhyt kuvaus (mistä uhka johtuu ja mitä voi tapahtua, jos uhka toteutuu)

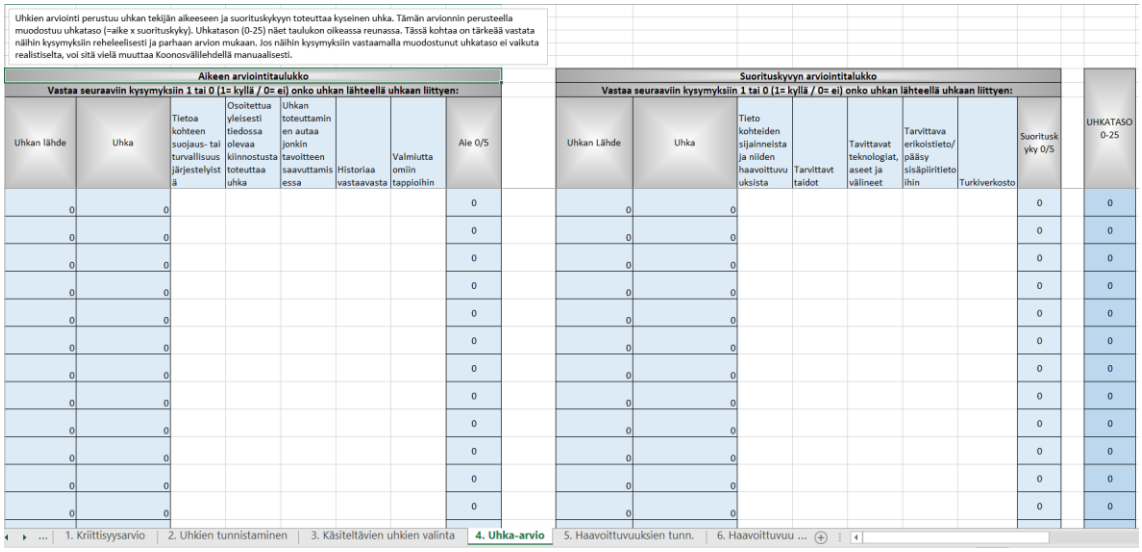
0. Perustiedot | 1. Kriittisyysarvio | 2. Uhkien tunnistaminen | 3. Käsiteltävien uhkien valinta | 4. Uhka-arvio | 5. Haavoittuvuuksien tunn. ...

Taulukko 6. käsiteltävien uhkien valinta.

Arvioitavaksi valitulle uhkatapahtumalle tunnistetaan samalla mahdollinen vihamielinen toteuttaja eli uhkan lähde tai tekijä. Jollakin uhkatapahtumalla voi olla useampi mahdollinen toteuttaja, jolloin sama uhka tapahtuma tulee lisätä taulukkoon yhtä monta kertaa kuin kuinka monta toteuttajaa sille löytyy. Samoin sama vihamielinen toimija voidaan kirjata taulukkoon niin monta kertaa kuin kyseisen toimijan toteuttamia uhkia on tunnistettu. Taulukossa valitaan pudotusvalikosta kriittinen tekijä, johon uhkatapahtuma liittyy. Kriittisessä tekijässä voi olla useampia kohteita, joihin iskeä ja siksi kirjataan vielä tarkempi uhkan kohde kriittiselle tekijälle. Tästä uhkan kohteesta tunnistetaan ja arvioidaan haavoittuvuuksia myöhemmässä vaiheessa.

4.3 Uhka-arvio

Uhka-arvio perustuu tässä arviointityökalussa raportissa aiemmin mainittuihin vihamielisen toimijan eli uhkatapahtuman mahdollisen toteuttajan aikeeseen ja suorituskykyyn toteuttaa kyseinen uhkatapahtuma. Aietta ja suorituskykyä arvioidaan molempia viidellä kysymyksellä tai väittämällä. Taulukon vasemmassa reunassa ennen kysymyksiä näkyy tunnistettu uhkatapahtuma, ja uhkan lähde eli mahdollinen toteuttaja. Molempien kysymyssarjojen oikealle puolelle muodostuu lukuarvo nollan ja viiden väliltä aikeesta tai suorituskyvystä. Uhka taso on aikeen ja suorituskyvyn summa, jolloin taulukon oikeassa reunassa oleva lukuarvo on nollan ja kahdenkymmenenviiden välillä.



Uhkien arviointi perustuu uhkan tekijän aikeeseen ja suorituskykyyn toteuttaa kyseinen uhka. Tämän arvionnin perusteella muodostuu uhkataso (=aike x suorituskyky). Uhkatason (0-25) näet taulukon oikeassa reunassa. Tässä kohtaa on tärkeää vastata näihin kysymyksiin reheleelisesti ja parhaan arvion mukaan. Jos näihin kysymyksiin vastaamalla muodostunut uhkataso ei vaikuta realistiselta, voi sitä vielä muuttaa Koonosvälilehdellä manuaalisesti.

Aikeen arviointitaulukko

Vastaa seuraaviin kysymyksiin 1 tai 0 (1= kyllä / 0= ei) onko uhkan lähteellä uhkaan liittyen:

Uhkan lähde	Uhka	Tietoa kohteen suojaus- tai turvallisuus järjestelyistä	Osoitettua yleisesti tiedossa olevaa kiinnostusta toteuttaa uhka	Uhkan toteuttaminen autaa jonkin tavoitteen saavuttamisessa	Historiaa vastaavasta	Valmiutta omiin tappioihin	Aie 0/5
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0
0	0						0

Suorituskyvyn arviointitalukko

Vastaa seuraaviin kysymyksiin 1 tai 0 (1= kyllä / 0= ei) onko uhkan lähteellä uhkaan liittyen:

Uhkan Lähde	Uhka	Tieto kohteiden sijainneista ja niiden haavoittuvuuksista	Tarvittavt taidot	Tavittavat teknologiat, aseet ja välineet	Tarvittava erikoistieto/ pääsy sisäpiiritietoihin	Turkiverkosto	Suorituskyky 0/5	UHKATASO 0-25
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0
0	0						0	0

Taulukko 7. Uhka-arvio.

Aietta arvioivilla kysymyksillä halutaan selvittää sitä, mikä käsitys arvion tekijöillä on vihamielisen toimijan halusta toteuttaa jokin uhkatapahtuma. Aietta arvioitaessa on nojauduttava kaikkeen saatavilla olevaan taustatietoon. Aikeen arviointi muodostuu seuraavista tekijöistä: vihamielisen toimijan aikaisempi historia vastaavien uhkatapahtumien toteuttamisessa, vihamielisen toimijan tarve toteuttaa uhkatapahtuma osana omien tavoitteiden saavuttamista, tietoa uhkatapahtuman kohteen sijainnista ja turvallisuusjärjestelyistä, yleisesti osoitettua tai tiedossa olevaa kiinnostusta toteuttaa uhkatapahtuma sekä valmiutta toteuttaa uhkatapahtuma mahdollisista omista tappioista huolimatta. Näillä viidellä kohdalla muodostetaan kattava käsitys vihamielisen toimijan aikeesta ja halusta toteuttaa jokin uhkatapahtuma.

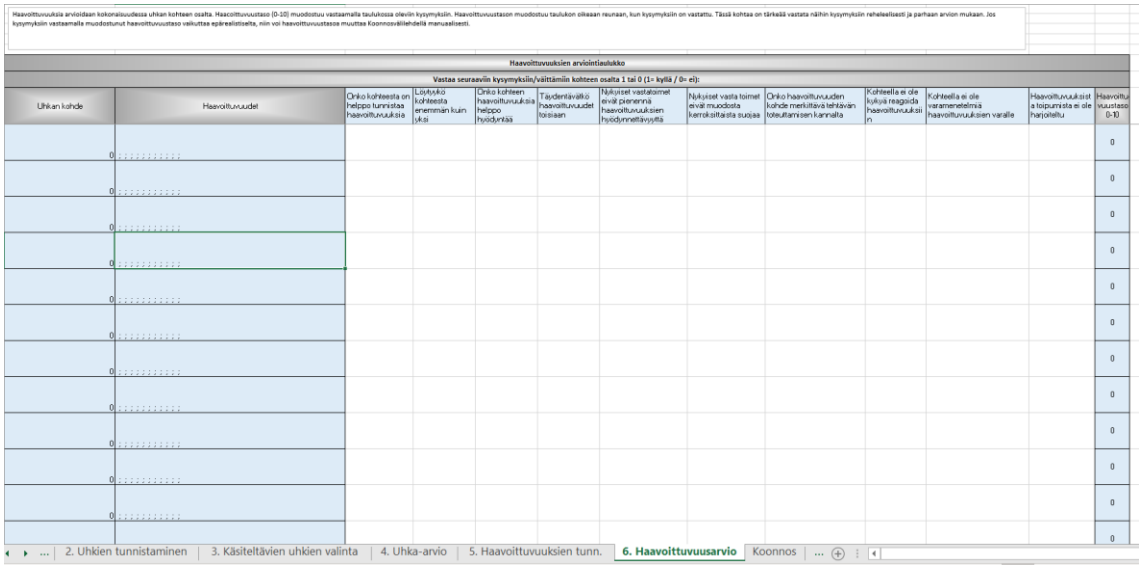
Suorituskykyä arvioivilla kysymyksillä halutaan selvittää, millainen on vihamielisen toimijan kyky toteuttaa kyseinen uhkatapahtuma. Arviointikysymykset on suunniteltu mittaamaan, onko vihamielisellä toimijalla tarvittavat tiedot kohteesta, tarvittavat taidot, hallussaan tarvittava teknologia ja välineet, tarvittava erikoistieto tai pääsy sisäpiiritietoihin sekä tarvittava tukiverkosto uhkatapahtuman toteuttamiseksi.

Huomioitavaa on, että riippuen arvioitavasta uhkatapahtumasta voi saman vihamielisen toimijan aie- ja suorituskykyarviot vaihdella suurestikin. Esimerkiksi tienvarsipommin toteuttamiseen vaaditaan täysin erilaisia suorituskykyjä kuin kyberhyökkäykseen. Tämän takia tässä vaiheessa vihamielistä toimijaa arvioidaankin aina suhteessa tiettyyn uhkatapahtumaan.

4.4 Haavoittuvuusarvio

Ennen haavoittuvuusarviota tunnistetaan kaikki mahdolliset haavoittuvuudet, jotka uhkatapahtuman kohteesta kyetään tunnistamaan. Haavoittuvuuksien tunnistaminen kohteesta voi auttaa tunnistamaan myös uusia uhkia.

Haavoittuvuuksien arviointi toteutetaan työkalussa siten, että kaikkia haavoittuvuuksia per uhkatapahtuman kohde arvioidaan samalla kertaa. Tämä toteutettiin työkalussa näin, ettei arvio lähtisi leviämään ja laajenemaan liikaa, vaan se saataisiin suoritettua kohtuullisessa ajassa.



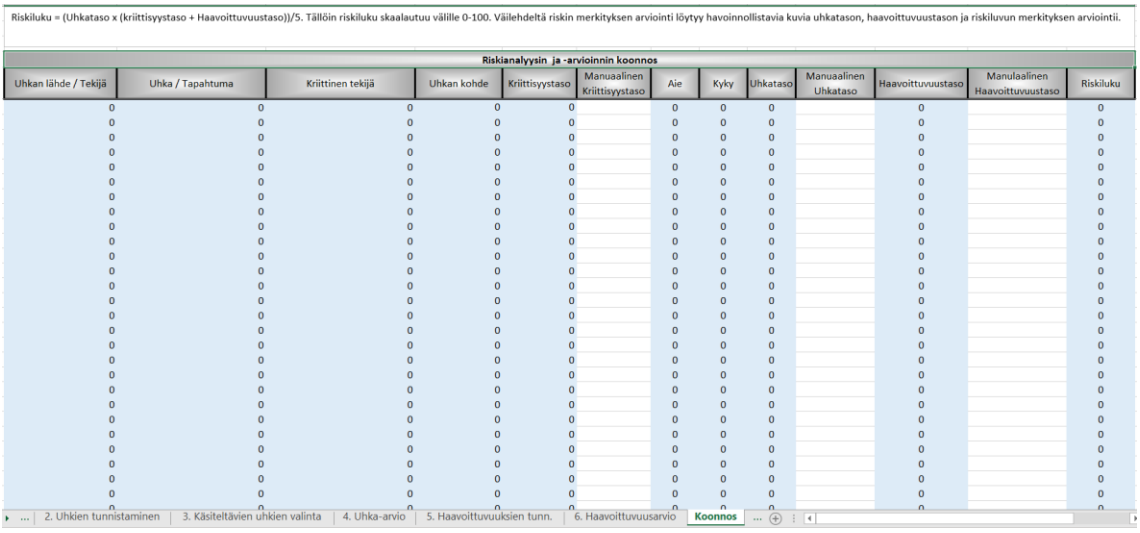
Taulukko 8. Haavoittuvuusarvio.

Haavoittuvuusarviossa pyritään arviomaan kohteen tunnistettavuutta, saavutettavuutta, turvallisuusjärjestelmien tasoa, vastatoimia, tärkeyttä sekä omaa kykyä reagoida haavoittuvuuksiin. Haavoittuvuustasoa nostaa, jos jokin haavoittuvuus tai haavoittuvuudet ovat helposti tunnistettavissa. Tämä lisää selkeästi myös mahdollisuutta, että sellaista haavoittuvuutta hyödynnettäisiin. Lisäksi haavoittuvuustasoa nostaa, jos kohteesta tunnistetaan useampi haavoittuvuus. Vielä vakavampaa on, jos haavoittuvuuden täydentävät toisiaan eli ne ovat yhteydessä toisiinsa ja samalla keinolla voidaan vaikuttaa useampaan haavoittuvuuteen. Haavoittuvuuksien helppo hyödynnettävyys on omiaan lisäämään haavoittuvuustasoa. Hyödynnettävyyttä tulisi ajatella haavoittuvuuden luontaisena ominaisuutena, koska vastatoimia arvioidaan omassa kysymyksessä. Vastatoimet laskevat haavoittuvuustasoa ja jos kohteen vastatoimet eivät ole yksittäisiä vaan koostuvat kerroksittaisista vastatoimista ja suojauksista, laskee se haavoittuvuustasoa yhtä lailla. Omia haavoittuvuustasoon vaikuttavia toimia ovat myös reagointikyky ja varamenetelmät haavoittuvuuden aiheuttamien tappioiden varalle. Reagointikyky tarkoittaa sitä, että kohteella on tarvittaessa irrottaa resursseja haavoittuvuuden kautta muodostuneen uhkan ja sen realisoitumisen paikkaamiseksi. Myös toipumisen harjoittelu laskee haavoittuvuustasoa, koska se vähentää omien toimintojen palauttamiseen tarvittavaa aikaa.

4.5 Riskiarvioinnin koonnos ja raportointi

Riskiarvioinnin koonnokseen kopioituu kaikki oleelliset tiedot nähtäville yhteen taulukkoon. Kuvassa x näkyvän koonnostaulukon oikeaan reunaan muodostuva riskiluku skaalautuu asteikolle nollasta sataan. Riskiluku muodostetaan kaavalla **riskiluku = (uhkataso x (kriittisyystaso + haavoittuvuustaso))/5**. Riskiluvun skaalautumiselle nollan ja sadan välille ei ole muuta perustetta kuin se, että riskin vakavuuden taso olisi helpommin miellettävissä kuin esimerkiksi nollan ja viidensadan välille skaalautuvan riskin vakavuuden taso. Nollan ja sadan välille osuvan riskin taso tarkoittaa tässä työkalussa seuraavia: riskiluku nollan ja kolmen välillä on merkityksetön riski, neljän ja kymmenen välillä on vähäinen riski, yhdentoista ja kahdenkymmenenviiden välillä on kohtalainen riski, kahdenkymmenenkuuden ja viidenkymmenen välillä on merkittävä riski ja viidenkymmenenyhden ja sadan välillä on sietämätön riski.

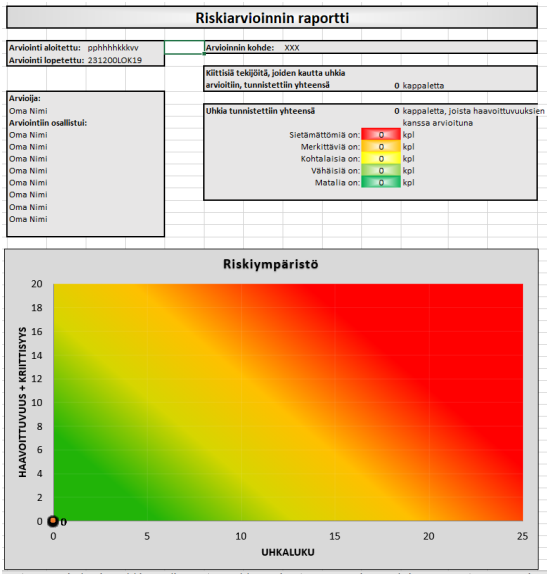
Taulukossa on vielä mahdollisuus manuaalisesti muuttaa arvioinnin tuloksia, jos jostain syystä on herännyt tunne siitä, että arviointikysymyksiin vastaamalla muodostunut kriittisyys-, uhka- tai haavoittuvuustaso on liian suuri tai pieni. Esimerkiksi kriittisyysarvion manuaalinen arvioinnin muutos toteutetaan syöttämällä haluttu lukuarvo sarakkeeseen manuaalinen kriittisyystaso. Tällöin manuaalisesti syötetty luku huomioidaan arvioinnissa koonnostaulukossa automaattisesti näkyvän kriittisyystason sijaan. Taulukko kuitenkin säilyttää näkyvillä myös arviointikysymyksillä muodostetun kriittisyystason. Tämä ominaisuus rakennettiin taulukkoon sen vuoksi, että työkalua käytettäessä arviointikysymyksiin vastattaisiin mahdollisimman rehellisesti ja kaikkiin arvioitaviin kohtiin samalla tavalla. Kuitenkin samalla huomioitiin se, että arviointikysymykset eivät ainakaan työkalun kehitys- ja kokeiluvaiheessa välttämättä vastaa kaikkiin tilanteisiin ja tapahtumiin parhaalla mahdollisella tavalla, jolloin mahdollisuus muuttaa arvioitua kriittisyys-, uhka- ja haavoittuvuustasoa vähentäisi kiusausta vastata kysymyksiin esimerkiksi siten, että saadaan jokin haluttu uhkataso.



Riskiluku = (Uhkataso x (kriittisyystaso + Haavoittuvuustaso))/5. Tällöin riskiluku skaalautuu välille 0-100. Väilehdeltä riskin merkityksen arviointi löytyy havoinnollistavia kuvia uhkatason, haavoittuvuustason ja riskiluvun merkityksen arviointii.

Riskianalyysin ja -arvioinnin koonnos												
Uhkan lähde / Tekijä	Uhka / Tapahtuma	Kriittinen tekijä	Uhkan kohde	Kriittisyystaso	Manuaalinen Kriittisyystaso	Aie	Kyky	Uhkataso	Manuaalinen Uhkataso	Haavoittuvuustaso	Manulaalinen Haavoittuvuustaso	Riskiluku
0	0	0	0	0		0	0	0		0		0

Työkalu muodostaa valmiin arvioinnin perusteella automaattisesti riskiarvioinnin raportin. Raportista ilmenee riskiarvioinnin tekemisen ajankohta ja riskiarvioinnin kohde. Raportti näyttää myös riskiarvion tekemiseen osallistuneet. Näiden perustietojen lisäksi raportista ilmenee, kuinka monta kriittistä tekijää on tunnistettu ja arvioitu sekä kuinka monta tunnistettua uhkatapahtumaa on arvioitu yhdessä kriittisten tekijöiden ja haavoittuvuuksien kanssa. Raportti näyttää myös lukumäärällisesti, kuinka monta arvioiduista tahallisesti aiheutetuista turvallisuusriskeistä on sietämättömiä, merkittäviä, kohtalaisia, vähäisiä tai merkityksettömiä. Tämän lisäksi raporttiin muodostuu riskikartta, jolla pyritään visuaalisesti kuvaamaan arvioitua riskiympäristöä paremmin. Riskikarttaan tulostuu uhkatapahtuman otsikko uhkatason ja haavoittuvuus- ja kriittisyystason perusteella.



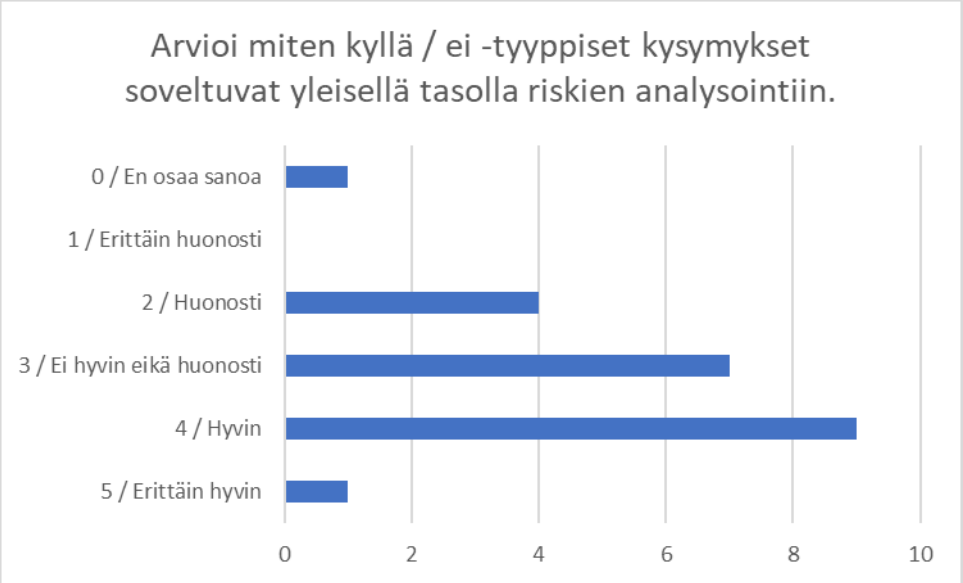
Kuva 8. Riskiarvioinnin raportti.

5 Tulokset

Luvussa neljä esiteltyä versiota tahallisesti aiheutettujen turvallisuusriskien arviointityökalusta testattiin Puolustusvoimien turvallisuusjohtaminen 1 -kurssin lähiopetusjaksolla kurssilaisten toimesta. Kurssi järjestettiin Tuusulassa 17.-20.12.2019. Kurssilla oli 22 osallistujaa. Kurssilaiset tulivat puolustushallinnosta ja poliisista erilaisista ja eritasoisista tehtävistä. Kurssilaisien turvallisuustoimialan työkokemus vaihteli yhdestä vuodesta yli kahteenkymmeneen vuoteen.

Tässä luvussa käsitellään arviointityökalun testaamisessa syntyneitä tuloksia. Luvussa ei esitellä, mitä kriittisiä tekijöitä, uhkia ja haavoittuvuuksia arvioitiin. Huomio keskittyy arviointityökalun käytettävyyteen, arviointikohtien soveltuvuuteen yleisesti sekä siihen, miten työkalua voisi jatkokehittää. Arviointityökalun toimivuutta mittaavaan kyselyyn vastasivat kaikki kurssin 22 osallistujaa. Käytetty kyselylomake on esitettyliitteessä 2. Tämän lisäksi opinnäytetyön tekijä havainnoi työkalun käyttöä koko kurssin ajan muistiinpanoja tehden ja oli tarvittaessa tukemassa ongelmatilanteissa tai epäselvissä kohdissa. Tämä luku perustuu kyselylomakkeen vastauksiin ja tutkijan omaan havainnointiin sekä pohdintaan.

5.1 Kyllä – ei -tyyppisten kysymysten käyttö



Kuva 9. Arvioi miten kyllä / ei -tyyppiset kysymykset soveltuvat yleisellä tasolla riskien analysointiin.

Kyselylomakkeen ensimmäinen kysymys kohdentui kyllä tai ei -tyyppisten kysymysten käyttöön arviointityökalussa. Kyllä tai ei -kysymykset vaikuttivat yksinkertaisilta ja helppokäyttöisiltä arviointityökalussa, jolla on tarkoitus saada helposti tuloksia arvioinnin kohteesta. Kuitenkin tämäntyyppinen kysymyksenasettelu vaatii todella paljon kysymysten muodostajalta, jotta kysymyksistä saadaan riittävän yksiselitteisiä.

”Vain kaksi ääripäätä on liian rajoittava. Usein on mahdotonta tehdä valintaa näiden kahden välillä.” (V15)

”Jos kysymykset ovat sopivia arviointi on helppo toteuttaa. Ongelma on, jos kysymysten vastaus on siinä rajalla. Laajempi asteikko esim. 1-5 toisi tarkkuutta ja mahdollisesti eroja uhkiin.” (V19)

”Kyllä/ei -vaihtoehto on yksinkertainen, mutta se ei kuvaa yksittäisen riskin todennäköisyyttä verrattuna asteikkoon 1-5.” (V4)

”Monessa tapauksessa jaottelu on turhan karkea. 0-3 antaisi paremman hajonnan.” (V20)

Kyllä tai ei -tyyppinen kysymyksenasettelu nähtiin hieman mustavalkoisena ja rajoittavana asetelmana. Tilanteessa, jossa on vain kaksi ääripäätä, ei saada välttämättä luotua riittävää hajontaa arvioitavien riskien välille. Esimerkiksi joissain tilanteissa uhka A ja uhka B voivat saada samaan kysymykseen vastauksen kyllä, joka kasvattaa riskilukua molemmissa yhtä paljon, vaikka uhka B tiedetään olevan merkittävästi uhka A:ta vaarallisempi.

Yksi haaste oli saada kysymyksistä riittävän yleispäteviä kaikkia tilanteita silmällä pitäen. Tämä ei ollut onnistunut täydellisesti arviointityökalun testikäytössä olleessa versiossa. Kyllä tai ei -tyyppiset kysymykset aiheuttivat myös sen, että osa arviointikysymyksistä esitettiin negatiivisessa muodossa ja osa taas positiivisessa muodossa. Tämä johtui siitä, että vastaamalla kyllä riski lisääntyi ja vastaamalla ei riski ei lisääntynyt. Jos arvioitavana asiana oli esimerkiksi se, onko arvioinnin kohteena olevalla kriittisellä tekijällä olemassa olevaa varautumissuunnitelmaa, niin vastaamalla kyllä tässä työkalussa riski lisääntyy. Tästä johtuen kysymys piti muotoilla väittämäksi ja negatiiviseen muotoon: arvioinnin kohteella ei ole varautumissuunnitelmaa. Tähän piti taas vastata kyllä (ei ole), jos halutaan riskin lisääntyvän ja ei (kyllä on), jos ei haluta riskin lisääntyvän. Tällainen kysymysten muotoilu on omiaan sekoittamaan vastaajia ja vie aikaa, jos ei ole täysin selvää mitä kysymyksellä haetaan.

”Kysymysten asettelu tulee olla selkeä positiivinen kysymys, jotta vastaus tulee oikein. Tulee olla kysymys eikä väittämä.” (V5)

”Kysymysten asettelua tarkasteltava. Kysymys tulisi esittää positiivisessa muodossa.” (V6)

Osa kurssilaisista koki selkeästi poissulkevan ja rajaavan kysymyksenasettelun myös positiivisena asiana. Jos kysymyksiä on riittävä määrä, saadaan eri riskit järjestettyä helposti ja esitettyä numeraalisessa muodossa. Hyvin muotoillut kysymykset voivat toimia poissulkevina tekijöinä, jolloin arviointia on yksinkertaisempaa tehdä ilman suurempaa tuntemusta erilaisista analyysi menetelmistä.

”Sinällään ok, mutta vain kaksi vaihtoehtoa tekee asiat aika mustavalkoisiksi. Jos vain kyllä/ei, niin kysymyksiä pitäisi olla enemmän.” (V3)

”Selkeät linjaukset on helpompi järjestää analysointia varten ja saada muutettua numeraaliseen muotoon.” (V14)

”Selkeä esitysmuoto ja pohjautuu samalla poissulkevaan ajatteluun rajaten selvästi eri vaihtoehtoja.” (V10)

Yhteenvetona kyllä tai ei -tyyppisten kysymysten käytöstä on todettavissa, että sellaisenaan ne eivät tuota riittävää hajontaa riskien välille, yksinkertaistavat ja tekevät asioista mustavalkoisia. Kuitenkin riittävällä määrällä hyvin muotoiltuja kysymyksiä saadaan sopivasti eroja aikaiseksi ja sen perusteella osataan kohdistaa resursseja sekä riskienhallinnan toimenpiteitä oikeisiin paikkoihin.

5.2 Kriittisyyden arviointi

Kuva 10. Miten kriittisyyttä arvioivat kysymykset vastasivat mielestäsi arvioitavaan kokonaisuuteen kriittisestä tekijästä?

Puolet kyselyyn vastanneista arvioi kriittisyyttä arvioivien kysymysten vastaavan hyvin arvioitavaan kokonaisuuteen. Kahdeksan vastaajaa eivät kokeneet, että kysymykset olisi sopineet hyvin tai huonosti. Kolme vastasi arvioitikysymysten sopivan huonosti tai erittäin huonosti. Kokonaisuudessaan arviointikysymykset antoivat hyvän kuvan arvioitavan kriittisen kohteen kriittisyystasosta. Arviointikysymysten sopivuuteen vaikutti paljon myös arvioitavan kohteen luonne.

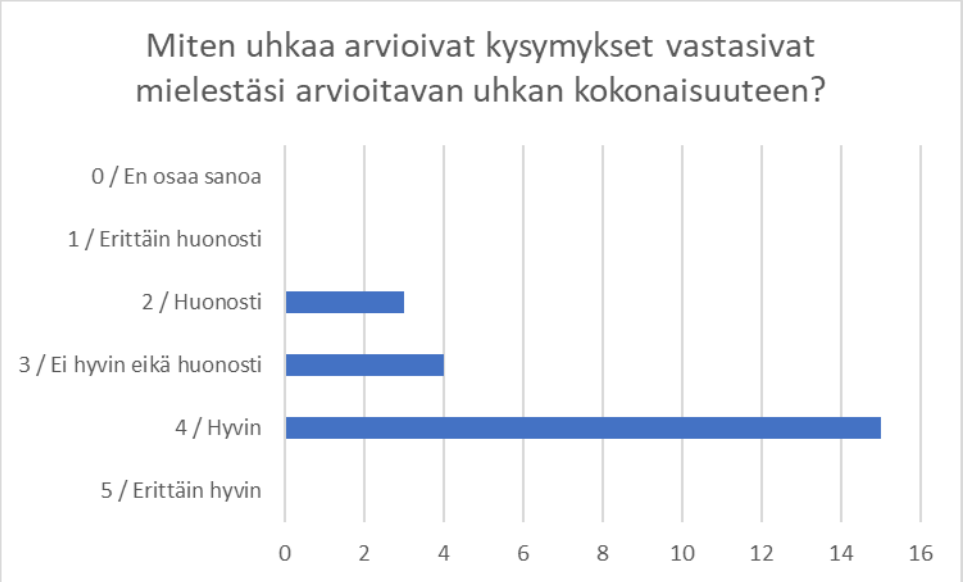
”Soveltui hyvin esimerkkitapaukseen. Ei merkittäviä haasteita pois lukien kielteinen kysymyksenasettelu.” (V1)

”Ryhmämme valitsemiin kriittisiin tekijöihin kysymykset vastasivat huonosti ja jouduimme käyttämään aikaa vastauksen muodostamiseen. Myös tässä olisi helpottanut laajempi asteikko esim. 1-5Monessa tapauksessa jaottelu on turhan karkea. 0-3 antaisi paremman hajonnan.” (V19)

Vaikka testikäytössä olleen tahallisesti aiheutettujen turvallisuusriskien arviointityökalun luonne oli esitelty kurssilaisille, kritisoi osa sitä, ettei työkalun arviointikysymykset vastanneet muihin kuin tahallisesti aiheutettuihin turvallisuusriskeihin. Työkalu kehitettiin tarkasti rajattuun tarkoitukseen ja siksi siinä ei huomioitu tahattomasti aiheutuvia turvallisuutta vaarantavia riskejä. *”Työkalun kysymyksen asettelu sopii ainoastaan tunnetun aktiivisen ihmisperäisen toiminnan arviontiin. Harjoitustehtävään liittyen osa tekijöistä jäi pois arviosta työkalun ominaisuuksien takia.”* (V8) Kriittisen tekijän olemus ja luonne ymmärrettiin eri ryhmissä eri tavoin. Selkeää linjausta siitä, mikä on kriittinen tekijä, ei ole olemassa Työkalussa oli ohjeistettu, millaisia asioita kriittiset tekijät voisivat olla, mutta suoraa vastausta ei asiaan ole, koska jokaisen on itse arviointia tehdessään osattava tunnistaa oman toimintansa kannalta kriittiset tekijät. Tämä johti siihen, että kokemus työkalun toimivuudesta ei ollut sujuva ja osa ryhmistä käytti paljon aikaa omien kriittisten tekijöiden sovittamiseksi työkalulla analysoitavaksi.

Työkaluun toivottiin lisää mukautuvuutta kriittisyyttä arvioivien kysymysten osalta. Kurssilaisten esittämiä vaihtoehtoja olivat esimerkiksi omien kysymysten tekeminen kategorioittain kriittisen tekijän luonteen perusteella. *”Näiden sijaan kategoriakohtaiset määritelmät.”* (V2) Kategoriat voisivat olla esimerkiksi myös Puolustusvoimien riskienhallinnan ohjeistuksessa olevat riskikohteiden alueet: henkilöstö, omaisuus, tieto, toiminta, ympäristö ja maine. (PVOHJEK RISKIENHALLINTA PUOLUSTUSVOIMISSA 2014) Tässä mallissa kehitettäisiin jokaiselle riskikohteen alueelle omat arviointikysymykset ja vastaaminen tapahtuisi vain sellaisiin kysymyksiin, jonka alueeseen kyseinen arvioitava kohde kuuluu. Toinen kurssilaisilta noussut ajatus oli, että kriittisyyttä arvioivia kysymyksiä voisi olla eri toiminnan tasoille räätälöitynä. *”Kysymyksiä ja lomaketta on oltava useamman tasoisia, jotta käytettävyys olisi hyvä.”* (V5) Tällä tarkoitetaan sitä, että yksittäisen joukko-osaston kannalta kriittinen tekijä ei välttämättä ole Puolustusvoimien kannalta kriittinen tekijä. Samoin voi olla, että rahallisesti koko Puolustusvoimien tasolla tietyn suuruinen menetys ei olisi vielä toimintaa lamaannuttava, mutta yksittäisessä joukko-osastossataloudelliset seuraukset olisivat ainakin hetkellisesti merkittävät.

5.3 Uhka-arvio



Kuva 11. Miten uhkaa arvioivat kysymykset vastasivat arvioitavan uhkan kokonaisuuteen?

Uhkaa arvioivia kohtia työkalussa oli yhteensä kymmenen. Vastaajista suurin osa, viisitoista kahdestakymmenestäkahdesta vastasi uhkia arvioivien kysymysten vastaavaan hyvin arvioitavaan kokonaisuuteen. Neljän vastaajan mielestä ne eivät vastanneet hyvin eikä huonosti ja kolmen vastaajan mielestä ne vastasivat huonosti arvioitavaan uhkan kokonaisuuteen. Uhka-arvion osuutta pidettiin arviointityökalun yhtenä parhaiten onnistuneena kokonaisuutena.

Työkalun uhkaa arvioivia kysymyksiä pidettiin pääsääntöisesti riittävinä ja oikeita asioita mittaavina. *”Monipuoliset hyvin kohdistetut kysymykset.”* (V6) *”Riittävästi kysymyksiä. 0/1 skaala turhan jyrkkä.”* (V20) Tässäkin osiossa toivottiin laajempaa arviointivaihtoehtoa kuin kyllä ja ei. *”Osaan kysymyksistä vaikea vastata kyllä/ei -tasolla. Laajempi skaala olisi hyvä. Usein näistä ei tarkempaa tietoa, joten vastaukset osin arpapeliä.”* (V15) Varsinkin uhkatapahtuman toteuttajan aietta toteuttaa kyseinen uhka voi olla hankala arvioida kyllä ja ei -tyyppisillä kysymyksillä. On mahdollista, että joku toinen vihamielinen taho voisi olla halukkaampi toteuttamaan jonkin uhkatapahtuman kuin jokin toinen taho, mutta viidellä joko tai -tyyppisellä kysymyksellä ei saada riittäviä eroja aikaiseksi näiden kahden tahon välille.

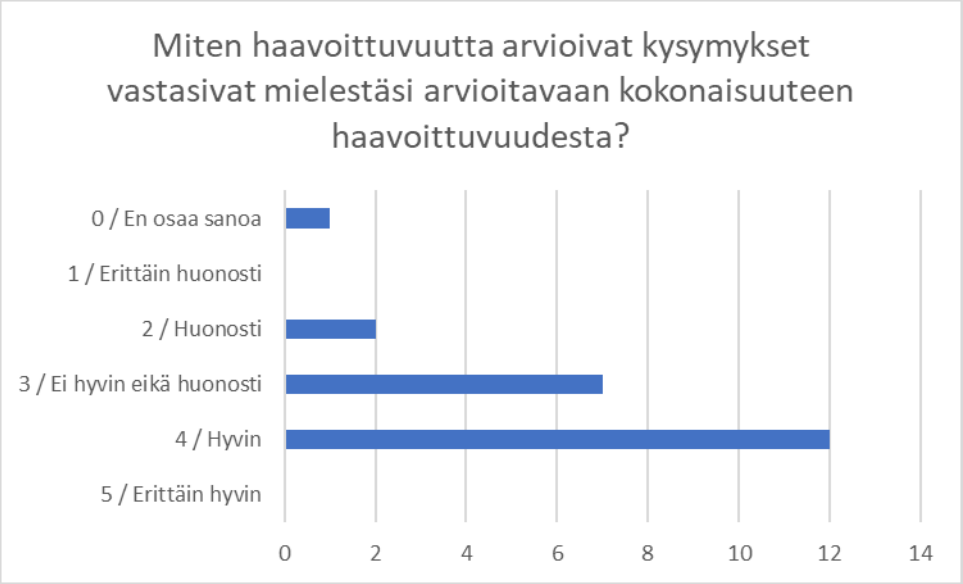
Osa vastaajista jatkoi sen kritisoimista, että työkalussa ei huomioitu kuin tahallisesti aiheutettuja turvallisuusuhkia, joiden uhkatapahtumilla on tunnistettavissa myös uhkan toteuttaja. *”Työkalu ei sovellu ollenkaan ihmisen toiminnasta riippumattomien uhkien arviointiin.”* (V8)

Uhkatapahtumien vaikutuksien arviointia ei oltu sisällytetty työkalun uhka-arvion osuuteen. *”Uhan potentiaalisia vaikutuksia / liitännäisvaikutuksia ei huomioitu.”* (V2) Ajatus siitä, että

vaikutuksia oli arvioitu jo kriittisen tekijän osalta, ei ollut tässä kohtaa siirtynyt. Toki kriittisen tekijän kohdalla ei arvioitu vaikutuksia yksittäisen uhkatapahtuman toteutumisen osalta vaan arvio tehtiin itselle tärkeän kriittisen tekijän kautta.

Uhka-arvio perustui vihamielisen toimijan aikeeseen ja suorituskykyyn toteuttaa jokin uhka, kuten luvussa kolme on esitelty. ”*Perusteet olivat selkeät. Oikeastaan ainoa mikä pitäisi lisätä on todennäköisyys.*” (V3) Työkalun perusteella ei syntynyt riittävää käsitystä siitä, että todennäköisyyttä ei tarvitsisi arvioida erikseen. Työkaluun omaksutussa mallissa todennäköisyys syntyy vihamielisen tekijän aikeesta ja suorituskyvystä toteuttaa jokin uhkatapahtuma.

5.4 Haavoittuvuuksien arviointi



Kuva 12. Miten haavoittuvuutta arvioivat kysymykset vastasivat arvioitavaa kokonaisuuteen haavoittuvuudesta?

Haavoittuvuutta arvioivien kysymysten todettiin vastaajien toimesta vastaavan arvioitavaan kokonaisuuteen kohtalaisen hyvin. ”*Ei ilmaantunut esimerkkitehtävässä mitään miksi ei olisi vastannut.*” (V11) Hieman yli puolet vastaajista arvioi arviointikysymysten vastaavan hyvin arvioitavaan kokonaisuuteen haavoittuvuudesta. Seitsemän kahdestakymmenestäkahdesta vastasi, että kysymykset eivät vastanneet hyvin eikä huonosti, kahden mielestä ne vastasivat huonosti ja yksi vastaaja ei osannut sanoa.

Tässä työkalussa ei yksittäisiä haavoittuvuuksia päästy arvioimaan, vaan haavoittuvuuksia arvioitiin kokonaisuutena uhkatapahtuman kohteen osalta. ”*Jos haavoittuvuudet kohtaan kasaantuu useita asioita, kaikista väittämistä tulee 1.*” (V7) Jos siis kohteesta oli tunnistettavissa useita haavoittuvuuksia, kovin herkästi kaikkiin arvioitaviin kohtiin tuli vastaukseksi kyllä tai 1, mikä tarkoitti haavoittuvuustason nousua ja kokonaisriskiluvun kasvamista. Tämä oli

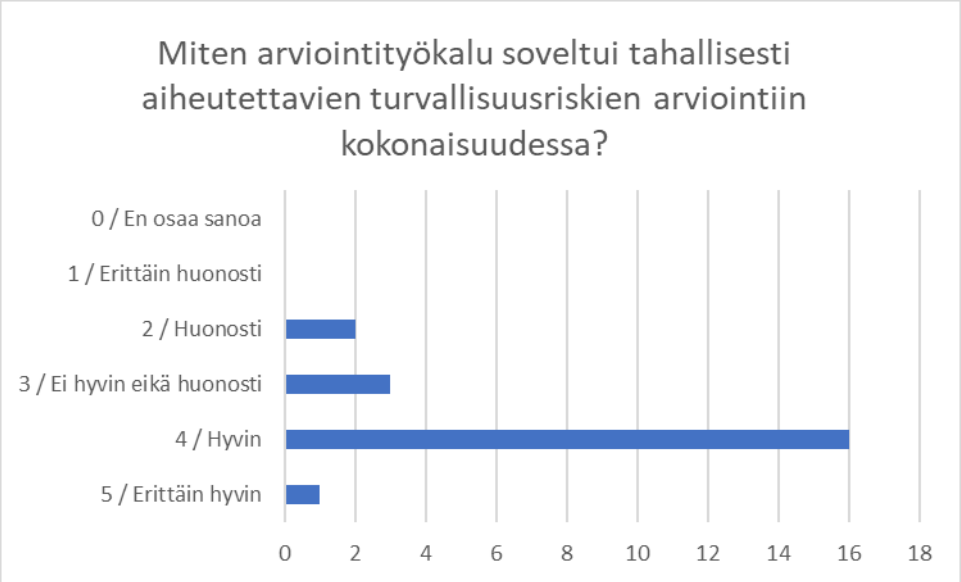
toki yksi työkalun suunnittelun lähtökohdista. On selvää, että jos kohteesta löytyy useita helposti tunnistettavia ja hyödynnettäviä haavoittuvuuksia, näiden yhteisvaikutus kohteen osalta on merkittävä.

Haavoittuvuuksien mahdollistamia vaikutuksia uhkatapahtuman kohteeseen ei työkalussa arvioitu erikseen. ”*Toipuminen on aika iso käsite --> vastaaminen edellyttäisi käsitteen avaamista. Selkeää vaikuttavuuden arviointikohtaa ei ollut --> esitän lisättäväksi.*” (V3) Työkalua kehitettäessä oli ajatuksena, että kriittisyysarviossa olevat arviointikysymykset kuten rahallinen, maineellinen ja toiminnallinen vaikutus, olisivat riittävät kokonaisuudet vaikutusten arvioinnissa. Toki uhkatapahtuman kohteen haavoittuvuuksien toteutumisen vaikutukset voivat hyvin olla sellaisia, ettei kriittisyysarvion sisältämä vaikutusten arviointi kata niitä. Tällöin haavoittuvuuksien vaikutusten arvioinnin lisääminen voisi olla perusteltua.

Haavoittuvuuksia on helpompi tunnistaa ja konkreettisesti osoittaa esimerkiksi fyysisistä kohteista kuten rakennuksista tai erilaisista tiloista ja järjestelmistä. Haavoittuvuutta arvioivat kysymyksetkin sopivat paremmin tällaisten kohteiden arviointiin. ”*Haavoittuvuuteen liittyvät kysymykset sopivat tilaan tai muuhun vastaavaan kohteeseen tapahtuvaan arviointiin.*” (V19) Haavoittuvuutta arvioiviin kysymyksiin voisikin lisätä sellaisia kokonaisuuksia, jotka arvioivat paremmin esimerkiksi ihmisiä ja sisäpiiriuhkan mahdollistavia haavoittuvuuksia.

Myös haavoittuvuusosiossa kritisoitiin yhä, että työkalu oli suunniteltu vain tahallisesti aiheutettujen turvallisuusriskien analysointiin. ”*Osa asioista, joiden vaikutusta tulisi arvioida ja joihin tulisi varautua, jäi pois, koska ne eivät olleet tahallisesti aiheutettuja. Itse tehtävän suorittamiseen niitä ei kuitenkaan tulisi jättää huomioimatta.*” (V8) On totta, että jotkin järjestelmät, tilat, rakennukset ja henkilöstö voivat pitää sisällään haavoittuvuuksia, jotka toteutuessaan ovat vaikutuksiltaan merkittäviä eivätkä vaadi vihamielistä tahallista toimintaa toteutuakseen. Esimerkiksi riippuvuus sähkönjakelusta voi olla haavoittuvuus, jos sähkökatko lamaannuttaa toiminnan. Sähkönjakelussa tapahtuvat katkokset voivat johtua esimerkiksi sääilmiöistä eivätkä siten ole tahallista vihamielistä toimintaa, mutta vaikuttavat haavoittuvuuteen merkittävällä tavalla.

5.5 Kokonaisarvio työkalun toimivuudesta



Kuva 13. Työkalun soveltuvuus tahallisesti aiheutettujen turvallisuusriskien arviointiin.

Suurin osa vastaajista arvioi, että työkalu soveltui hyvin siihen, mihin se oli kehitetty. Yksi arvioi soveltuvuutta erittäin hyväksi, kaksi huonoksi ja kolme arvioi, ettei työkalu sovellu hyvin eikä huonosti tahallisten turvallisuusriskien arviointiin.

Kokonaisuudessaan arviointityökalu soveltui varsin hyvin siihen tarpeeseen, mihin opinnäytetyön tilaaja oli työtä pyytänyt. Työkalussa parhaiten onnistui uhkaa arvioiva osuus. ”*Pureutuu tahallisuuden kokonaisuuteen paremmin kuin tahattomaan tapahtumaan. Aie + suorituskyky osio on hyvä! Ei ilmaantunut esimerkkitehtävässä mitään, miksi ei olisi vastannut.*” (V10) Moni muukin kyselyn vastaajista mainitsi, että työkalu toimi tarkoitukseensa hyvin, mutta ei huomioinut tahattomasti aiheutuvia riskejä. Jatkossa tulisi pohtia olisiko mahdollista yhdistää tahattomien ja tahallisesti aiheutettujen riskien arviointia samaan työkaluun. Excel -sovelluksessa toteutettuna voisi käytettävyys kärsiä entisestään, jos samaan taulukkoon yritettäisiin yhdistää toisistaan hyvin poikkeavia arviointikysymyksiä.

”*Jos on aikaa työkalua voi käyttää. Työkalua tulee käyttää useampi kerta ennen kuin terminologia ja kunkin arviointikohdan merkitys aukeaa.*” (V4) Työkalun toimintalogiikka ei auennut parhaalla mahdollisella tavalla nopeasti sanallisesti selitettynä kurssilaisille. Toisaalta ei ollut myöskään tarkoituksenmukaista kertoa liian tarkasti, mitä mihinkin kohtaan tulisi kirjoittaa, jotta työkalun käytöstä saataisiin monipuolisempia käyttökokemuksia. Tämän lisäksi tärkeähavainto oli se, kuinka työkalun käyttö onnistui intuitiivisesti eli oliko työkalun toimintalogiikka riittävän selkeä. Vasta työkalun kokeilun ja käytön jälkeen monelle työryhmälle aukesi se, minkä tasoisia asioita kannattaisi syöttää kuvan 6 arvioitavien kohteiden valintavälilehden eri sarakkeisiin. Osaltaan työkalun käyttöä varmaankin hankaloitti se, että työkalussa edettiin

vaihe vaiheelta eivätkä kurssilaiset esimerkiksi kiinnittäneet huomiota seuraavilla välilehdillä oleviin arviointikysymyksiin. Tämä johti siihen, että osa työryhmistä joutui palaamaan askeleen taaksepäin ja muuttamaan arvioitavien kohteiden kuvauksia.

”Riittävä määrä verrattavia asioita.” (V14) *”Hyvä perusta, mutta mistä koostuu todennäköisyys.”* (V3) Kokonaisuutena voidaan arvioida, että työkalussa oli riittävä määrä erilaisia tekijöitä, vaikka osa kurssilaisista kokikin, että riskien vaikutuksia tai uhkan todennäköisyyttä ei huomioitu tarpeeksi. *”Kokonaisuutena hyvä. Yksityiskohtia pitää hioa. "pikamenetelmällä" varsin vastaava tulos.”* (V20) Työryhmät tekivät vielä kurssin viimeisenä päivänä nopean analyysin hieman erilaisella menetelmällä ja kaikki pääsivät samansuuntaiseen lopputulokseen tahallisesti aiheutettujen turvallisuusriskien suuruuksista. Analyysin tekeminen onnistui toisella menetelmällä nopeasti, koska kurssilaiset olivat jo pohtineet arvioitavia riskejä testikäytössä olevan työkalun avulla sekä omaksuneet skenaarion ja tilanteen, missä asioita käsiteltiin. On myös mahdollista, että tämän arviointityökalun käyttö ennen toisen menetelmän käyttöä ehti vaikuttaa siihen, miten ja millaisina arvioitavat kokonaisuudet nähtiin.

Työkalun tekniseen toteutukseen jäi vielä kehitettävää. Työkalussa oli joitain kaavoihin liittyviä toimintahäiriöitä ja eri välilehdille ei periytynyt riittävää määrää tietoja, mikä hankaloitti työkalun käyttöä, kun välilehtien välillä piti käydä tarkastamassa eri tietoja. *”Bugeja vielä oli. Monessa kohtaa toivoisia tietueiden periytyvän, ettei tarvitse hyppiä eri välilehtien välillä.”* (V14) Yksi Excel -sovelluksen kaavoihin liittyvä ongelma oli, että työkalu kehitettiin uusimalla sovellusversiolla. Kurssilla oli käytössä erilliskoneet, joihin oli asennettu vanhempi sovellusversio ja vanhemmassa sovellusversiossa ei ollut samoja ominaisuuksia kuin uusimmassa versiossa. Tämä ei estänyt arviointityökalun käyttöä, mutta hankaloitti sitä hieman. *”Pääosin hyvin toteutettu. Version välisisä ongelmia. Raportti ei toiminut käyttäjän toimista johtuen.”* (V19) Raporttivälilehden riskikarttaan periytyvät tiedot puuroutuivat, jos samansuuruisia riskejä oli useampia. Tämän lisäksi murhetta aiheutti se, että soluja ei ollut lukittu ja osa ryhmistä poisti ja lisäili rivejä esimerkiksi arvioitavien riskien valintavälilehdellä. Jotta työkalu olisi toiminut oikein, olisi lopuillekin välilehdille pitänyt lisätä uusi rivi ja kopioida kaava siihen, jotta oikeat tiedot olisivat periytyneet oikeille paikoilleen. Lopullisessa versiossa työkalusta pitäisi siis kaikki kaavoja tai muita tärkeitä toiminnallisuuksia sisältävät solut lukita siten, että tietoja voi poistaa tai syöttää vain niihin soluihin, joihin on tarkoitus.

Kurssilaisia pyydettiin arvioimaan myös sitä, miten työkalu soveltui Force Protection doktriinin riskienhallinnan mallin mukaiseen analyysiprosessiin. Tähän kyselylomakkeen kohtaan jätti moni vastaamatta. Ne ketkä vastasivat, olivat kuitenkin sitä mieltä, että arviointityökalu oli mallin mukainen ja vastasi sitä, mitä mallissa riskienhallinnan osalta haetaan. *”Noudatteli suunnitteluprosessin tiettyjä osia sopivalla tavalla.”* (V1) *”Mallin vaiheet olivat hyvin mukana.”* (V15)

Kyselylomakkeessa kysyttiin myös sitä, mitä kurssilaiset haluaisivat poistaa työkalusta tai lisätä työkaluun. Vastauksista ilmeni, että sen käyttökokemuksen perusteella, jonka vastaajat saivat kurssin aikana, heistä kukaan ei lähtisi poistamaan muuta kuin työkaluun jääneitä kirjoitusvirheitä tai yhtä pientä toiminnallisuutta, joka oli käytännössä hyödytön. ”*Oikeinkirjoitusvirheet :)*” (V1) ”*Uhkien tunnistamisen X sarakkeen*” (V22) Vaikka työkalussa ei olisi suuremminpoistettavia ominaisuuksia, niin moni asia vaatisi silti kehittämistä. ”*Ei välttämättä poistaa, mutta kenties tulisi hioa tiettyjen osien kohdalla, miten hyvin ne soveltuvat arviointiin.*” (V10)

Arviointityökaluun lisättäviä asioita nousi esiin useita, ja niistä monet parantaisivat työkalun käytettävyyttä. Edellä on jo nostettu esiin se, että vaiheesta seuraavaan edetessä arviointityökalun välilehdiltä ei periytynyt tarpeeksi tietoja. ”*viimeistelyä, että ei tarvitsisi siirtyä (palata) edellisiin välilehtiin. Hyvä olisi, jos lopullinen versio olisi mahdollisimman yksinkertainen käyttää.*” (V11) Tämän lisäksi moni vastaaja mainitsi malliesimerkin lisäämisen ensimmäiselle riville, josta selviäisi nopeasti arviointityökalun käyttölogiikka ja se, millaisia asioita eri kenttiin tulisi syöttää. ”*Helppokäyttöisyyttä. Täyttöohjeet, minkä tyypistä asiaa mihinkin tulee täyttää.*” (V7) Tämän lisäksi toivottiin mahdollisuutta muokata kysymyksiä omaa toimintaa paremmin vastaaviksi ja enemmän vaihtoehtoja kuin kyllä ja ei. ”*Kysymysten muokkaus / poistaminen -vaihtoehto mukaan työkaluun. Skaalautuvuus numeroarvojen lisäys.* (V16) Kysymysten muokkaamisen mahdollistaminen olisi helppo toteuttaa, mutta silloin täytyisi muistaa jatkossa käyttää samoja kysymyksiä tahallisesti aiheutettujen turvallisuusriskien arvioinnissa. Jos arviota tekee samaan kohteeseen eri kysymyksillä, eivät eri kysymyksillä tehdyt arviot ole keskenään vertailukelpoisia.

Ajatus kyllä tai ei -tyyppisiin vastauksiin perustuvasta arviointityökalusta houkutti helppokäyttöisyydellään ja yksinkertaisuudellaan. ”*Kyllä ei -vaihtoehtojen tilalle 0,1,2 vaihtoehdot*.” (V22) Kuitenkin näin jyrkkä ja poissulkeva tapa arvioida aiheutti paljon päänvaivaa ja ylimääräistä pohdintaa, jos jokin asia halutaan huomioida, mutta ei yhtä vahvasti kuin jokin toinen asia. Tällöin laajempi arviointiasteikko voisi auttaa asiassa.

Työkalun kehittämisvaiheessa tehtiin rajauksia, jotka mahdollistivat aikataulussa pysymisen sekä sen, että työ ei kasva liian suureksi. Esimerkiksi riskienhallinnan toimenpiteet ja keinot riskin pienentämiseksi päätettiin rajata työn ulkopuolelle. ”*Välilehdet riskien pienentämiselle ts. toimenpiteille. Täyttöesimerkit*.” (V3) Riskien pienentämiselle oli kuitenkin selkeä tarve työkalussa ja tekemällä uuden arvion samalla työkalulla riskienhallinnan toimenpiteiden toteuttamisen jälkeen kuvastaisi hyvin sitä muutosta, joka eri tekijöihin vaikuttamalla voidaan saada aikaiseksi.

5.6 Yhteenveto

Yleisesti ottaen opinnäytetyön aiheena ollut tahallisesti aiheutettujen turvallisuusriskien arviointityökalun tarve oli ilmeinen. Työkalua tarvitaan siihen, että riskienarviointi tehdään aina samalla tavalla ja myös siihen, että tiedot ja arviointiperusteet dokumentoidaan ja niihin on mahdollista palata myöhemmin. Kurssilaiset olivat kaikki lähes yhtä mieltä arviointityökalun tarpeellisuudesta. ”*Työkalu yhtenäistäisi käytäntöjä ja käytettävää terminologiaa valtakunnallisesti. Ehdottomasti kannatettava asia*.” (V20)

Opinnäytetyön arviointityökalun koetiin olevan hyvä avaus ja alusta jatkokehitykselle. ”*Kyllä. Kritiikistä huolimatta periaatteeltaan toimiva strukturoitu, toistettavissa oleva ja visualisoinnin alkeellisesti mahdollistava työkalu. Erittäin tarpeellinen. Lisätestauksella ja kehityksellä tästä voi tulla käyttökelpoinen*.” (V2) Työkalun täydelliseen toimivuuteen pyrkiessä tulisi harkita sovelluksen kehittämistä, jotta olisi mahdollista koodata juuri sellaisia ominaisuuksia kuin on tarpeen. ”*Työkalu on tarpeen. Tämä on hyvä kokeilu, muttei vielä valmis. Tietokantapohja voisi antaa mahdollisuudet tietojen käsittelyyn*.” (V9)

Tässä arviointityökalussa perusajatus ja arvioitavat kokonaisuudet olivat kohdallaan. Kriittisyysanalyysissä tulisi kehittää arviointikysymysten yleistettävyyttä tai luoda eri kategorioille omat arviointikysymyksensä. Uhka- ja haavoittuvuusarvio-osuudet olivat kohtuullisen hyvin toimivia. Kuitenkin koko työkalussa olisi kiinnitettävä huomiota siihen, että kaikilla arviointivälilehdillä olisi riittävästi informaatiota näkyvillä arvioitavan kokonaisuuden käsittämiseksi. Jatkossa tulisi arvioida Excel -sovelluksen käytettävyyttä asiassa. Excel -sovellus mahdollistaa kuitenkin monipuolisen käytön eri ympäristöissä eikä sen käyttöön tarvita esimerkiksi käyttöoikeuksien ylläpitojärjestelmiä toisin kuin monen erillissovelluksen kanssa.

6 Johtopäätökset

Tämän opinnäytetyön tarkoituksena oli kehittää tahallisesti aiheutettujen turvallisuusriskien arviointiin helppokäyttöinen arviointityökalu. Opinnäytetyön tutkimusongelmina olivat: *miten tahallisesti aiheutettuja turvallisuusriskejä voidaan arvioida* ja *millaisella työkalulla arviointi voidaan toteuttaa*.

Tahallisesti aiheutettu turvallisuusriski muodostuu suojattavan tekijän kriittisyydestä, vihamielisen toimijan aikeesta ja suorituskyvystä toteuttaa uhkatapahtuma ja omista haavoittuvuuksista. Yhdistämällä nämä kolme tekijää saadaan toteutettua riittävän kattava arvio organisaatioon, sen toimintaan, tiloihin tai henkilöstöön kohdistuvista turvallisuusriskeistä.

Oman toiminnan kannalta kriittisten tekijöiden tunnistaminen on oleellinen osa jatkuvuudenhallintaa ja auttaa suuntaamaan uhka-arviota oman toiminnan kannalta olennaisimpiin asioihin. Vaarana voi kuitenkin olla, että keskityttäessä vain kriittisiin tekijöihin voi jotain merkittäviäkin uhkia jäädä tunnistamatta ja arvioimatta. Arviointityökalun testaamisen havaintojen perusteella sotilaallisessa organisaatiossa voi olla hankaluuksia mieltää kriittisien tekijöiden kriteerejä, jos niitä ei ole yksityiskohtaisesti käsketty ylemmältä taholta. Asiaan saattoi vaikuttaa se, että arviointityökalun testaamisessa tilanne ja organisaatio olivat kuvitteellisia, jolloin tuntemus arvioitavan kohteen toiminnasta ja organisaatiosta sekä niiden kriittisistä tekijöistä saattoi olla kurssilaisten osalta vajavainen. Kriittisten tekijöiden tunnistamisessa on kuitenkin oleellista, että tuntee oman organisaationsa, sen toiminnan ja toimintaympäristön.

Tahallisesti aiheutettujen turvallisuusriskien arvioinnissa on tarkoituksenmukaista keskittyä uhkatapahtumien aiheuttajaan eli uhkan lähteenä toimivaan vihamieliseen tahoon tai organisaatioon. Vihamielisen tahon aie ja suorituskyky toteuttaa jokin tietyn tyyppinen uhkatapahtuma antavat suuntaa uhkatapahtuman todennäköisyydestä. Syvyyttä riskiarvioon tuo omien haavoittuvuuksien tunnistaminen ja arviointi. Haavoittuvuuksien tunnistamisella ja arvioinnilla voidaan luoda edellytykset haavoittuvuuksien poistamiseksi tai vähentämiseksi ja samalla voidaan poistaa vihamieliseltä toimijalta väylä toteuttaa jokin uhkatapahtuma. Omien haavoittuvuuksien kautta voidaan tunnistaa myös mahdollisia uusia uhkatapahtumia, jotka eivät nousseet esiin uhkien tunnistamisvaiheessa.

Tahallisesti aiheutettujen turvallisuusriskien arvioinnissa huomiota voisi kiinnittää jatkossa kriittisten tekijöiden ja haavoittuvuuksien suhteeseen sekä siihen, millaiset vaikutukset uhkatapahtumilla on. Havaintojen perusteella osa kurssilaisista koki, että turvallisuusriskien vaikutuksia ei arvioitu riittävällä tasolla, vaikka kriittisyysarvion kysymykset perustuivatkin käytännössä siihen, millainen rahallinen, toiminnallinen tai maineellinen vaikutus kriittisen tekijän menettämisellä on. Työkalussa käytetyssä mallissa ei suoraan huomioitu sitä millainen vaikutus tietyllä uhkatapahtumalla voisi olla. Onkin pohdittava, tulisiko kriittisyysarviota tehdä tässä työssä esitetyssä muodossa ollenkaan vai lisätä sen sisältämät osiot uhka- ja

haavoittuvuusarvioon. Kriittisyysarviota kuitenkin puoltaa Naton suojaamisen doktriinin maininta siitä, että on tunnistettava kriittiset tekijät ja suojattava ne tekijät, joilla on eniten arvoa oman toiminnan kannalta. Kaikkea, jolla on jotain arvoa ei voida resurssien puitteissa suojata. Joukon komentajan vastuulle jää rajan vetäminen siihen, mitkä kohteet suojataan. Esikunnan tehtävä on tehdä perusteellinen tahallisesti aiheutettujen turvallisuusriskien arvio, joka antaa joukon komentajalle tarvittavaa tietoa ja perusteet päätöksenteon tueksi.

Riskienhallintaprosessi on luonteeltaan iteroiva, ja niin riskienarviointiprosessinkin tulisi olla. Tällöin arviointityökalussa tulisi olla mahdollisuus palata aikaisempiin vaiheisiin ja lisätä tai muuttaa syötettyjä tietoja. Työkalun kysymysten tulisi olla riittävän yleisiä, jotta eritasoisia asioita voisi arvioida samoilla kysymyksillä. Toinen vaihtoehto olisi tehdä eri tasoille suunnatut kysymyssarjat. Kysymyksiin vastaaminen olisi järkevää toteuttaa muulla tavalla kuin kyllä tai ei -tyyppisesti. Vastausvaihtoehtoja kannattaisi olla enemmän kuin kaksi, jolloin saataisiin paremmin eroja eri turvallisuusriskien välille eikä asioita tarvitsisi yksinkertaistaa tai tulkita mustavalkoisesti.

Analyysityökalun kehitystä jatkettiin siten, että kysymyksiin vastataan numeroilla 0, 1, 2 ja 3. Kysymykset myös muokattiin siten, että ne eivät erilaisen asteikon käytön luontevasti. Lopullinen arviointityökalun kehitysversio on liitteessä 3.

Opinnäytetyön arviointityökalu onnistui tavoitteessaan kohtuullisesti ja sillä tehdyt arviot olivat arvioiden mukaan oikeasuuntaisia. Uhka-arvion ja haavoittuvuusarvion osuudet olivat hyvin onnistuneita. Työkalun jatkokehittämisessä pitäisi kiinnittää huomiota siihen, että toteutuvan uhkatapahtuman vaikutukset tulisivat paremmin esille. Kuvitteellisesta tilanteesta tehtyjen arvioiden perusteella ei voi vetää suoria johtopäätöksiä siihen, miten työkalu toimii todellisessa tilanteessa. Arviointityökalun käyttö koettiin hieman työlääksi. Tämä saattoi osin johtua siitä, että kurssilaiset opettelivat samalla uudenlaisen arviointimenetelmän käyttöä ja tutustuivat kurssilla käytettävään kuvitteelliseen tilanteeseen. Arvioiden mukaan toinen arviointikierros samalla arviointityökalulla olisi helpottanut ja nopeuttanut arvion tekemistä huomattavasti. Arviointityökalun ohjeen tekeminen vaihe vaiheelta auttaisi arviointityökalun logiikan ymmärtämisessä ja helpottaisi arviointityökalun käyttöä.

Arviointityökalun toteuttaminen Excel-sovelluksessa on helppo ratkaisu siinä mielessä, että arviointityökalun jakaminen ja käyttö eri tietosuojaluokan järjestelmissä onnistuu kohtuullisen helposti. Hyödynnettäessä Excel-sovellusta on oltava tarkka siinä, mihin soluihin jättää käyttäjille muokkausoikeudet. Ihminen on luonteeltaan utelias ja arviointityökalun käyttäjä tulee kuitenkin kokeilemaan erilaisten muutosten tekoa työkalun ominaisuuksiin. Riskinä on myös, että tärkeitä kaavoja sisältäviä soluja muokataan vahingossa, minkä jälkeen arviointityökalu ei toimi oikein.

6.1 Analyysityökalun hyödynnettävyys

Tahallisesti aiheutettujen turvallisuusriskien arviointityökalua voidaan hyödyntää sotilaallisessa toiminnassa kaikilla tasoilla, joissa halutaan toteuttaa perusteellinen ja strukturoitu tahallisesti aiheutettujen turvallisuusriskien arviointi omien joukkojen ja kohteiden suojaamiseksi. Arviointityökalu toimii päätöksenteon tukena ja antaa hyvän kuvan kohteen riskiympäristöstä tahallisesti aiheutettavien turvallisuusuhkien ja haavoittuvuuksien suhteen.

Työkalua voidaan hyödyntää myös muussa viranomais- ja siviilitoiminnassa, kun omien kohteiden, henkilöstön ja toimintojen suojaamisen perusteet halutaan arvioida. Ei ole mitään rajoituksia, miksei työkalua tai sen periaatteita voisi hyödyntää muuallakin kuin vain sotilaallisessa kontekstissa päätöksenteon tukena.

6.2 Kriittinen tarkastelu

Turvallisuustoimialalla riskien arvioinnissa ei ole vielä laajaa vakiintunutta sanastoa ja termejä, jotka olisivat yhteisesti käytettävissä. Ulkomaisissa kirjoituksissa törmää usein termeihin, joille ei ole suoraa suomenkielistä vastinetta. Tämä voi aiheuttaa sekaannusta ja varsinaisen asian väärinymmärtämistä. Tässä opinnäytetyössä termien käännöksissä on pyritty siihen, että ne kuvaisivat mahdollisimman paljon alkuperästä tarkoitustaan siinä kontekstissa, missä niitä on käsitelty.

Opinnäytetyöksi kehitetyn arviointityökalun käyttävyyden parantaminen on keskeinen osa työkalun toimivuuden ja käyttäjäkokemusten kannalta. Arviointityökalun kysymysten muotoilussa tulisi kiinnittää huomiota yksiselitteisyyteen ja siihen, että kysymyksillä saadaan arvioitua kaikenlaisia tahallisesti aiheutettuja turvallisuusriskejä. Työkalu soveltuu sellaisenaan kaikkein parhaiten tiloihin ja rajattuihin alueisiin kohdistuvien tahallisten turvallisuusriskien arviointiin.

6.3 Jatkotutkimustarpeet

Yksi arviointityökalun testausvaiheessa esiin noussut jatkotutkimustarve on mahdollisuus arvioida tahallisia ja tahattomia riskejä samalla työkalulla. Monessa tilanteessa myös tahattomasti aiheutuneet turvallisuuden vaarantavat riskit voivat olla organisaation toiminnan kannalta erittäin merkittäviä. Perinteisemmän riskienhallinnan menetelmiä ja työkaluja on olemassa useita. Tässä kohtaa tarkemmin pitäisikin tutkia olemassa olevien menetelmien yhdistämistä tahallisesti aiheutettujen turvallisuusriskien arviointiin.

Opinnäytetyönä kehitetty arviointityökalu rajattiin käsittämään vain kriittisten tekijöiden, uhkatapahtumien ja haavoittuvuuksien arviointiin. Jatkokehittämistarpeena onkin tutkia, miten kehitettyä työkalua voisi hyödyntää riskien seurantaan ja riskejä pienentävien toimenpiteiden vaikutusten arviointiin.

Samalla arviointityökalulla on hankala arvioida jonkin tekijä kriittisyyttä ja merkitystä esimerkiksi rahallisessa, maineellisessa tai sotilaallisessa suorituskyvyssä, jos toinen toimija toimii esimerkiksi joukko-osaton tasolla ja toinen puolustushaaran tasolla. Arviointikriteerejä ja kysymyksiä tulisi pyrkiä jatkokehittämään siten, että ne sopisivat paremmin eritasoisen toiminnan tarpeisiin.

Lähteet

Painetut

Alexander, J. 2006. Force Protection Risk Management. Journal edition 4. Kalkar Germany: The Journal of the JAPCC, 19 – 21.

Anttila, P. 2007. Realistinen evaluaatio ja tuloksellinen kehittämistyö. Hamina: Akatiimi.

Hopkin, P. 2010. Fundamentals of risk management: understanding, evaluating, and implementing effective risk managemen. Lontoo: Kogan Page Limited.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2013. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Helsinki: Finanssi ja vakuutuskustannus.

Juvonen, M., Koskensyrjä, M. Kuhanen, L., Olaja, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Helsinki: Finanssi ja vakuutuskustannus.

Kreus, M. 2010. Terrorismin torjunta Suomessa. Tampere: Poliisiammattikorkeakoulu.

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3. uudistettu painos. Helsinki: Sanoma Pro.

Riehle, K. 2013. Assessing Foreing Intelligence Threats. American Intelligence Journal. Vol. 31, No 1. (US) National Military Intelligence Association, 96 – 101.

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 31010. 2013. Riskien hallinta. Riskien arviointimenetelmät. Helsinki: Suomen Standardisoimisliitto.

Taleb, N. N. 2008. The black swan: The impact of the highly improbable. London: Penguin Books.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Willis, H., Morral, A., Kelly, T. & Medby, J. 2005. Estimating Terrorism Risk. Santa Monica: Rand.

Sähköiset

Annex 3-10 – Force Protection. (2019). Joint Security Operations in Theater. Joint Publication 3-10. Maxwell: U.S. Air Force Doctrine.

Brashear, J. & Jones W. 2010. Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus). Tulostettu 3.1.2020. https://www.researchgate.net/publication/230090388_Risk_Analysis_and_Management_for_Critical_Asset_Protection_RAMCAP_Plus

Eskola, S. 2008. Turvallisuus käsitteenä. Maanpuolustuskorkeakoulu. Strategian laitos Julkaisusarja 3, Strategian asiatietoa, No 10. Tulostettu 23.2.2020. https://www.doria.fi/bitstream/handle/10024/74107/StratL3_10.pdf?sequence=1

Finlex. 2014. Puolustusministeriön ilmoitus Naton kanssa tehdystä isäntämaatukea koskevasta yhteisymmärryspöytäkirjasta. Noudettu 21.4.2020. https://www.finlex.fi/fi/sopimukset/sopsteksti/2014/20140082/20140082_1

Haimes, Y. 2011. On the Complex Quantification of Risk: Systems-Based Perspective on Terrorism. Risk Analysis: An International Journal, 31(8), 1175–1186. Tulostettu 3.1.2020. http://search.ebscohost.com.nelli.laurea.fi/login.aspx?direct=true&db=s3h&AN=65062507&site=ehost-live

Haimes, Y. (toim.). 2015. Risk modeling, assessment, and management. Tulostettu 22.2.2020. https://ebookcentral.proquest.com

Halli, J. 2018. Naton Force Protection -doktriini turvallisuusjohtamisen mallina. Laurea ammattikorkeakoulu.

IRM. 2002. A Risk Management Standard. Tulostettu 1.3.2020. https://www.theirm.org/media/4709/arms_2002_irm.pdf

Kielitoimiston sanakirja. 2019. Suomen kotimaisten kielten keskus. Viitattu 2.12.2019. https://www.kielitoimistonsanakirja.fi/netmot.exe?motportal=80

Kokonaisturvallisuuden Sanasto. 2017. Helsinki: Sanastokeskus TSK. Tulostettu 2.12.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

McGill, W. & Ayyub, B. 2007. The Meaning of Vulnerability in the Context of Critical Infrastructure Protection. Critical Infrastructure Protection: Elements of Risk. Virginia: George Mason University. 25 – 48. Tulostettu 11.12.2019. https://cip.gmu.edu/wp-content/uploads/2016/06/ElementsofRiskMonograph.pdf

McGill, W., Ayyub, B. & Kaminskiy, M. 2007. Risk Analysis for Critical Asset Protection. An International Journal, 27(5). 1265 – 1281. Tulostettu 3.1.2020. http://search.ebscohost.com.nelli.laurea.fi/login.aspx?direct=true&db=s3h&AN=27712431&site=ehost-live

McGill, W. 2008. Critical asset and portfolio risk analysis for homeland security. Tulostettu 9.12.2019. https://drum.lib.umd.edu/bitstream/handle/1903/8351/umi-umd-5614.pdf;jsessionid=6EC45F8CA6D3F21BFA4FFA7D686CC979?sequence=1

Moteff, J. 2005. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Tulostettu 9.12.2019. https://fas.org/sgp/crs/homesec/RL32561.pdf

NATO. What is NATO?. Tulostettu 23.2.2020. https://www.nato.int/nato-welcome/index.html.

Puolustusministeriö. Puolustushallinnon turvallisuus. Tulostettu 29.2.2020. https://www.defmin.fi/julkaisut_ja_asiakirjat/strategia-asiakirjat/puolustusministerion_strateginen_suunnitelma_2030/puolustushallinnon_turvallisuus

Puolustusvoimat. Turvallisuustasojärjestelmä käyttöön Puolustusvoimissa. 14.6.2017. Noudettu 21.4.2020. https://puolustusvoimat.fi/artikkeli/-/asset_publisher/turvallisuustasojarjestelma-kayttoon-puolustusvoimissa

Risk Management for DoD Security Programs. Student guide. Tulostettu 28.11.2019. https://www.cdse.edu/documents/student-guides/risk-management.pdf

Riskikompassi. www.riskikompassi.fi. Noudettu 25.9.2019.

Schnaubelt, C., Larson, E. & Boyer, M. 2014. Vulnerability Assessment Method Pocket Guide – A Tool fot Center of Gravity Analysis. Santa Monica: Rand. Tulostettu 16.12.2019. https://www.rand.org/pubs/tools/TL129.html

Seppälä, P. 2011. Uhka käsitteenä. Maanpuolustuskorkeakoulu. Strategian laitos Julkaisusarja 3, Strategian asiatietoa, No 16. Tulostettu 23.2.2020. https://www.doria.fi/bitstream/handle/10024/74127/StratL3_16w.pdf;jsessionid=2B57201AE48C1FC054E7F05436BB0076?sequence=1

Suomen Standardisoimisliitto. Standardit. Tulostettu 23.2.2020. https://www.sfs.fi/julkaisut_ja_palvelut/usein_kysyttya

TEPA-termipankki. 2019. Sanastokeskus TSK. Viitattu 2.12.2019. http://www.tsk.fi/tepa/fi/haku/haavoittuvuus

Vidalis, S. 2003. A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. Research Gate. Tulostettu 2.12.2019.

https://www.researchgate.net/publication/238659768_A_Critical_Discussion_of_Risk_and_Threat_Analysis_Methods_and_Methodologies

Wolke, T. (2017). Risk management. Tulostettu 22.2.2020. https://ebookcentral.proquest.com

Julkaisemattomat

Pihlajamäki, T. 2010. Tahallisesti aiheutettujen turvallisuusriskien uhka- ja haavoittuvuusanalyysit. Helsinki: Maanpuolustuskorkeakoulu Johtamistaidon laitos.

Vastaajat 1-22. Kyselylomake. Joulukuu 2019. Materiaali opinnäytetyön tekijän hallussa.

Kuviot

Taulukot

Liitteet

Liite 1: Keskeisimmät käsitteet

Allied Joint Publication (AJP)-3.14, Allied Joint Doctrine for Force Protection on Naton julkaisu, jonka tarkoituksena on toimia kehyksenä kokonaisvaltaiselle henkilöstön, infrastruktuurin ja suorituskykyjen suojaamiselle. Se on tarkoitettu operatiivisen tason komentajien käyttöön yhteisoperaatioiden aikana, mutta toimii referenssinä kaikilla tasoilla ja rauhan aikana kansallisella tasolla sekä ohjeena isäntämaille. (AJP -3.14 2015, VII)

Haavoittuvuus on järjestelmän luontaisten tilojen (esim. Fyysisen, teknisen, organisatorisen, kulttuurisen) ilmentyminen, mitä voidaan käyttää hyväksi aiheuttamaan haittaa sille tai vahingoittamaan sitä. (Haimes 2015, 56)

Kriittisyys on jotain, millä on arvoa ja mikä halutaan suojata. Kriittisyyttä on arvioitava kohteen tärkeyden, korvattavuuden ja arvon (sis. rahallinen, maineellinen ja toiminnallinen) mukaan. Jokaisen organisaation on määritettävä itse oman toiminnan kannalta kriittiset tekijät. Eri tekijöiden kriittisyys voi vaihdella toimintaympäristön luonteen ja oman toiminnan mukaan. (Annex 3-10 – Force Protection 2019, 28 – 29; McGill, Ayyub & Kaminskiy 2007, 1267 – 1269; Haimes 2011, 1176 – 1177; Brashear & William 2010, 6)

North Atlantic Treaty Organization (NATO) on vuonna 1949 perustettu poliittinen ja sotilaallinen liittouma. Naton tarkoitus on taata jäsenmaidensa turvallisuus poliittisin ja sotilaallisin keinoin. Natossa on nykyisin 29 jäsenmaata. Naton yhteinen puolustus perustuu artikla viiteen, jonka mukaan aseellinen hyökkäys yhtä jäsen valtiota vastaan on hyökkäys kaikkia jäsenvaltioita vastaa. Artikla viiteen on vedottu vain kerran ja silloin se tapahtui Yhdysvaltojen toimesta syyskyyn 2001 terrori-iskujen jälkeen. (NATO 2020)

Riski on ISO 31000 (2018, 6) standardin mukaan epävarmuuden vaikutus tavoitteisiin. Usein riski mielletään vaaraksi tai vaaran mahdollisuudeksi. Riskikäsitykseen liittyy usein kolme tekijää, jotka ovat tapahtumaan liittyvät odotukset, epävarmuus sekä tapahtuman laajuus ja vakavuus. (Hopkin 2010, 11; Juvonen, Koskensyrjä, Kuhanen, Olaja, Pentti, Porvari, & Talala 2014, 8) Kokonaisturvallisuuden sanastossa (2017, 41) *riski* on määritelty ”*jonkin kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmäksi*”. Riski on käsitteenä laaja ja se voidaan mieltää monenlaisena. Tässä opinnäytetyössä riskillä tarkoitetaan ei toivottuja ja kielteisiä tapahtumia.

Riskienhallinta on ”*koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta*” (SFS-ISO 31000, 6). Kokonaisturvallisuuden sanastossa (2017, 49) riskienhallinta on määritelty hieman laajemmin olemaan ”*järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat*

toimenpiteet”. Riskienhallinnassa huomioidaan yksittäiset riskit ja riskien kombinaatiot sekä riskienhallinnan toimenpiteiden synergia muun toiminnan kanssa (Wolke 2017, 1-3).

Standardit ovat toistuvaan toimintaan kehitettyjä menettelytapoja. Standardit ovat kirjallisia julkaisuja ja luonteeltaan suosituksia, joita viranomaiset voivat kuitenkin vaatia käytettävän. Standardit ovat viranomaisten, järjestöjen tai muiden tunnettujen elinten hyväksymiä. (Suomen Standardisoimisliitto 2020)

Turvallisuus on Kokonaisturvallisuuden sanaston (2017, 16) mukaan ”*tila, jossa uhkat ja riskit ovat hallittavissa*”. Turvallisuus pitää sisällään kaikki inhimillisen elämän osa-alueet ja on myös hyvin subjektiivinen käsite, sillä jollekin toiselle turvallinen asia voi jollekin toiselle ilmentyä turvattomana. Laajemmassa käsityksessä turvallisuus rakentuu sosiaalisten rakenteiden varaan ja saa merkityksensä vasta yhteisymmärryksen ja yhteisten merkityssisältöjen kautta. (Kreus 2010, 32 – 35; Eskola 2008, 1-2)

Uhka on ”*mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku*” (Kokonaisturvallisuuden sanasto 2017, 40). Uhka nähdään perinteisessä sotilaallisessa kontekstissa jonkin toimijan tahtona ja kykynä ”*Uhka = Tahto x Kyky*”. Yksilöä ja esimerkiksi valtioita voivat uhata hyvin erilaiset asiat. Yksilön uhkia voi olla esimerkiksi liikenneonnettomuudet, kun taas valtiota voi uhata sotilaalliset hyökkäykset tai kriittisen infrastruktuurin toimintahäiriöt. Länsimaissa uhka käsite on laajentunut ja sillä on monta eri kategoriaa aina taloudellisista uhkista terrorismiin. (Seppälä 2011, 1-2)

Liite 2: Kyselylomake

LAUREA Yhdessä enemmän

Kyselylomake

Esko Äärynen

Joulukuu 2019

Tämä kyselylomake liittyy Esko Äärysen Laurea ammattikorkeakouluun tehtävään opinnäytetyöhön. Puolustusvoimien tutkimuslupa tälle opinnäytetyölle löytyy päätöksestä AP18236/28.10.2019.

Tämän kyselyn vastaukset tullaan taltioimaan opinnäytetyötä varten nimettöminä eikä henkilötietoja käytetä opinnäytetyössä mitenkään. Kysely sisältää laadullisia ja määrällisiä kysymyksiä. Vastaa monivalintakysymyksiin merkitsemällä **X** valitsemaasi vaihtoehtoon ja muista perustella vastauksesi alle. Tarvittaessa jatka kääntöpuolelle.

1) Arvioi miten kyllä / ei -tyyppiset kysymykset soveltuvat yleisellä tasolla riskien analysointiin?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

2) Miten kriittisyyttä arvioivat kysymykset vastasivat mielestäsi arvioitavaan kokonaisuuteen kriittisestä tekijästä?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

3) Miten uhkaa arvioivat kysymykset vastasivat mielestäsi arvioitavan uhkan kokonaisuuteen?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

4) Miten haavoittuvuutta arvioivat kysymykset vastasivat mielestäsi arvioitavaan kokonaisuuteen haavoittuvuudesta?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

5) Miten arviointityökalu soveltui tahallisesti aiheutettavien turvallisuusriskien arviointiin kokonaisuudessa?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

6) Miten arvioit työkalun teknistä toteutusta. Toimiko työkalu:

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

Perustele vastauksesi:

7) Miten työkalu soveltui Force Protection -mallin mukaiseen analyysiprosessiin?

5/ Erittäin hyvin	4/ Hyvin	3/ Ei hyvin eikä huonosti	2/ Huonosti	1/ Erittäin huonosti	0/ En osaa sanoa

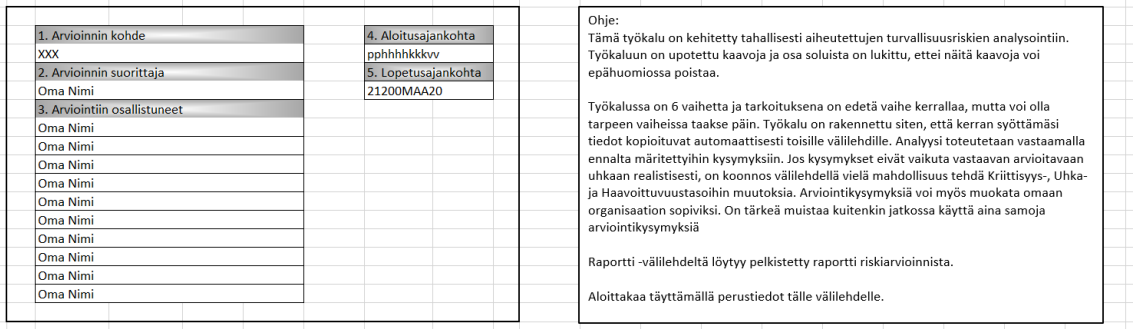
Perustele vastauksesi:

8) Mitä haluaisit poistaa työkalusta?

9) Mitä haluaisit lisätä työkaluun?

10) Onko työkalun (yleisellä tasolla, ei kosketa kurssilla käytettyä työkalua) käyttäminen ylipäätään tarpeellista uhkien tai riskien analysointiin?

Liite 3: Viimeinen kehitysversio tahallisesti aiheutettujen turvallisuusriskien arviointityökalusta



1. Arvioinnin kohde	4. Aloitusajankohta
XXX	pphhhhkkkvv
2. Arvioinnin suorittaja	5. Lopetusajankohta
Oma Nimi	21200MAA20
3. Arviointiin osallistuneet	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	
Oma Nimi	

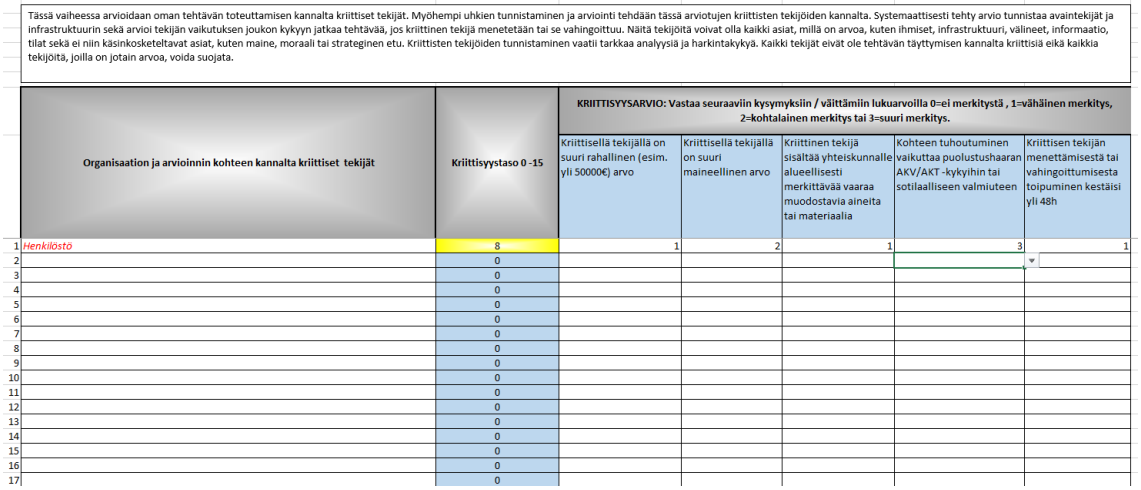
Ohje:
Tämä työkalu on kehitetty tahallisesti aiheutettujen turvallisuusriskien analysointiin. Työkaluun on upotettu kaavoja ja osa soluista on lukittu, ettei näitä kaavoja voi epähuomiossa poistaa.

Työkalussa on 6 vaihetta ja tarkoituksena on edetä vaihe kerrallaa, mutta voi olla tarpeen vaiheissa taakse päin. Työkalu on rakennettu siten, että kerran syöttämäsi tiedot kopioituvat automaattisesti toisille välilehdille. Analyysi toteutetaan vastaamalla ennalta määritettyihin kysymyksiin. Jos kysymykset eivät vaikuta vastaavan arvioitavaan uhkaan realistisesti, on koonnos välilehdellä vielä mahdollisuus tehdä Kriittisyys-, Uhka- ja Haavoittuvuustasoihin muutoksia. Arviointikysymyksiä voi myös muokata omaan organisaation sopiviksi. On tärkeä muistaa kuitenkin jatkossa käyttä aina samoja arviointikysymyksiä

Raportti -välilehdeltä löytyy pelkistetty raportti riskiarvioinnista.

Aloittakaa täyttämällä perustiedot tälle välilehdelle.

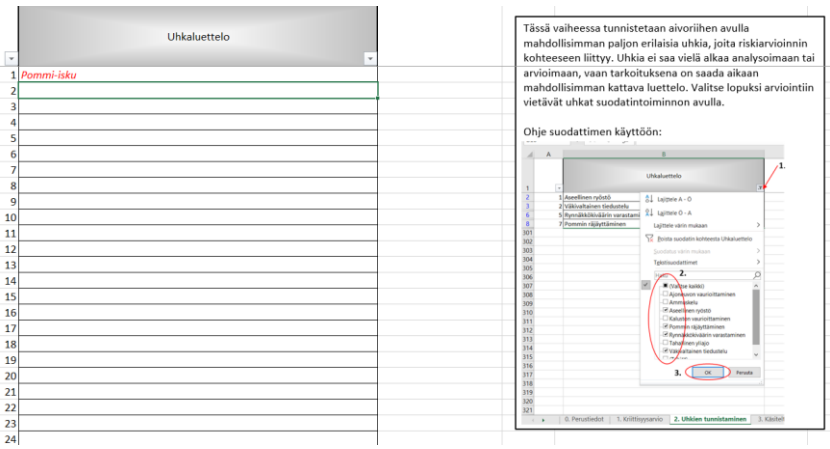
Perustietojen syöttö ja ohjeteksti.



Tässä vaiheessa arvioidaan oman tehtävän toteuttamisen kannalta kriittiset tekijät. Myöhempi uhkien tunnistaminen ja arviointi tehdään tässä arviotujen kriittisten tekijöiden kannalta. Systemaattisesti tehty arvio tunnistaa avaintekijät ja infrastruktuurin sekä arvioi tekijän vaikutuksen joukon kykyyn jatkaa tehtävää, jos kriittinen tekijä menetetään tai se vahingoittuu. Näitä tekijöitä voivat olla kaikki asiat, millä on arvoa, kuten ihmiset, infrastruktuuri, välineet, informaatio, tilat sekä ei niin käsinkosketeltavat asiat, kuten maine, moraali tai strateginen etu. Kriittisten tekijöiden tunnistaminen vaatii tarkkaa analyysiä ja harkintakykyä. Kaikki tekijät eivät ole tehtävän täyttymisen kannalta kriittisiä eikä kaikkia tekijöitä, joilla on jotain arvoa, voida suojata.

	Organisaation ja arvioinnin kohteen kannalta kriittiset tekijät	Kriittisyystaso 0 -15	KRIITTISYYSARVIO: Vastaa seuraaviin kysymyksiin / väittämiin lukuarvoilla 0=ei merkitystä , 1=vähäinen merkitys, 2=kohtalainen merkitys tai 3=suuri merkitys.				
			Kriittisellä tekijällä on suuri rahallinen (esim. yli 50000€) arvo	Kriittisellä tekijällä on suuri maineellinen arvo	Kriittinen tekijä sisältää yhteiskunnalle alueellisesti merkittävää vaaraa muodostavia aineita tai materiaalia	Kohteen tuhoutuminen vaikuttaa puolustushaaran AKV/AKT -kykyihin tai sotilaalliseen valmiuteen	Kriittisen tekijän menettämisestä tai vahingoittumisesta toipuminen kestäisi yli 48h
1	Henkilöstö	8	1	2	1	3	1
2		0					
3		0					
4		0					
5		0					
6		0					
7		0					
8		0					
9		0					
10		0					
11		0					
12		0					
13		0					
14		0					
15		0					
16		0					
17		0					

Kriittisten tekijöiden tunnistaminen ja arviointi.



	Uhkaluettelo
1	Pommi-isku
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	

Tässä vaiheessa tunnistetaan aivoriihen avulla mahdollisimman paljon erilaisia uhkia, joita riskiarvioinnin kohteeseen liittyy. Uhkia ei saa vielä alkaa analysoimaan tai arvioimaan, vaan tarkoituksena on saada aikaan mahdollisimman kattava luettelo. Valitse lopuksi arviointiin vietävät uhkat suodatintoiminnon avulla.

Ohje suodattimen käyttöön:

Uhkien tunnistaminen esimerkiksi aivoriihi -menetelmällä.

Tässä kohtaa valitaan uhkaluettelosta arvioitavat uhkat. Tahallisesti aiheutetun turvallisuusuhkan tekijä ja tarkempi kohde kirjataan myös tässä vaiheessa. Tämän jälkeen valitaan, mihin kriittiseen tekijään arvioitava kokonaisuus liittyy. Taulukkoon voi myös kirjata lyhyen kuvauksen uhkan syistä ja mitä voi tapahtua, jos uhka toteutuu.

	Arvioitavien kohteiden valinta				
Juokseva numerointi	Käsiteltäväksi valittava uhkatapahtuma	Uhkan lähde / tekijä	Kriittinen tekijä johon liittyy (valitaan pudotusvalikosta)	Uhkan kohde	Lyhyt kuvaus (mistä uhka johtuu ja mitä voi tapahtua, jos uhka toteutuu)
1	*Pommi-isku*	*Terroristijärjestö X*	*Henkilöstö*	*Yleisö*	
2					
3					
4					
5					
6					
7					
8					

Arvioitavien kohteiden valinta.

Uhkien arviointi perustuu uhkan tekijän aikeeseen ja suorituskykyyn toteuttaa kyseinen uhka. Tämän arvionnin perusteella muodostuu uhkataso (=aike x suorituskyky). Uhkatason (0-30) näet taulukon oikeassa reunassa. Tässä kohtaa on tärkeää vastata näihin kysymyksiin reheleellisesti ja parhaan arvion mukaan. Jos näihin kysymyksiin vastaamalla muodostunut uhkataso ei vaikuta realistiselta, voi sitä vielä muuttaa Koonosvälilehdellä manuaalisesti.

	Aikeen arviointitaulukko										Suorituskyvyn arviointitalukko						
	Vastaa seuraaviin kysymyksiin/väittämiin lukuarvoilla 0=ei merkitystä , 1=vähäinen merkitys, 2=kohtalainen merkitys tai 3=suuri merkitys.										Vastaa seuraaviin kysymyksiin/väittämiin lukuarvoilla 0=ei merkitystä , 1=vähäinen merkitys, 2=kohtalainen merkitys tai 3=suuri merkitys.						
Juokseva numerointi	Uhkan kohde	Kiittinen tekijä	Uhkan lähde	Uhka	Tieto kohteen suojaus- tai turvallisuus järjestelyistä	Osoitettua yleisesti tiedossa olevaa kiinnostusta toteuttaa uhka	Uhkan toteuttamien autaa jonkin tavoitteen saavuttamis essa	Historiaa vastaavasta	Valmiutta omiin tapioihin	Aie 0-15	Tieto kohteiden sijainneista ja niiden haavoittuvuuksista	Tarvittavt taidot	Tavittavat teknologiat, aseet ja välineet	Tarvittava erikoistieto/ pääsy sisäpiirtieto ihin	Turkiverkosto	Suorituskyky 0-15	UHKATASO 0-30
1	Yleisö	Henkilöstö	Terroristijärjestö X	Pommi-isku	3	1	2	3	1	10	2	3	1	2	3	11	21
2	0	0	0	0						0						0	0
3	0	0	0	0						0						0	0
4	0	0	0	0						0						0	0
5	0	0	0	0						0						0	0
6	0	0	0	0						0						0	0
7	0	0	0	0						0						0	0
8	0	0	0	0						0						0	0

Uhka-arvio.

Tässä vaiheessa tunnistetaan uhkan kohteesta haavoittuvuuksia. Haavoittuvuudet voivat liittyä ihmisiin, toimintaan, informaatioon, tiloihin ja välineisiin sekä harjoitteluun, tilannetietoisuuteen, turvallisuusjärjestelmiin, fyysiseen turvallisuuteen ja varajärjestelmien puuttumiseen. Ihmisen voivat esimerkiksi olla suulaita tai asettaa jonkin asian uhkanalaiseksi oman egonsa takia. Huonosti suunniteltu toiminta tai väärinlaiset käytänteet voivat asettaa uhkan kohteen uhan alle. Informaation osalta huonot järjestelmät tai epäonnistuminen tiedon tarveperusteisessa jakamisessa voivat muodostaa haavoittuvuuksia. Tässä vaiheessa on tärkeä keskittyä sellaisiin haavoittuvuuksiin, jotka voivat vaikuttaa tehtävän toteuttamiseen. Jos listassa on sama uhkan kohde useaan kertaan, voi haavoittuvuudet kopioda riviltä toiselle.
Haavoittuvuudet arvioidaan seuraavalla välilehdellä.

	Haavoittuvuuksien tunnistaminen				
Juokseva numerointi	Uhkan lähde	Uhka tapahtuma	Kriittinen tekijä	Uhkan kohde	Tunnistetut haavoittuvuudet
1	Terroristijärjestö	Pommi-isku	Henkilöstö	Yleisö	*Avoin pääsy* *monta kulkureittiä*
2	0	0	0	0	
3	0	0	0	0	
4	0	0	0	0	
5	0	0	0	0	
6	0	0	0	0	
7	0	0	0	0	
8	0	0	0	0	
9	0	0	0	0	
10	0	0	0	0	
11	0	0	0	0	
12	0	0	0	0	
13	0	0	0	0	
14	0	0	0	0	
15	0	0	0	0	
16	0	0	0	0	
17	0	0	0	0	
18	0	0	0	0	

Haavoittuvuuksien tunnistaminen esimerkiksi aivoriihi -menetelmällä.

Haavoittuvuuksia arvioidaan kokonaisuudessa uhkan kohteen osalta. Haavoittuvuustaso (0-30) muodostuu vastaamalla taulukossa olevile kysymyksiin. Haavoittuvuustason muodostuu taulukon oikeaan reunaan, kun kysymyksiin on vastattu. Tässä kohtaa on tärkeää vastata näihin kysymyksiin reheleellisesti ja parhaan arvion mukaan. Jos kysymyksiin vastaamalla muodostunut haavoittuvuustaso vaikuttaa epämielitelrta, niin voi haavoittuvuustasoa muuttaa Koonnosvälilehdellä manuaalisesti.

	Haavoittuvuuksien arviointitaulukko																
	Vastaa seuraaviin kysymyksiin/väittämiin lukuarvoilla 0=ei merkitystä , 1=vähäinen merkitys, 2=kohtalainen merkitys tai 3=suuri merkitys.																
Juokseva numerointi	Uhkan lähde / tekijä	Uhkatapahtuma	Uhkan kohde	Haavoittuvuudet	Kohteesta on helppo tunnistaa haavoittuvuuksia	Löytyykö kohteesta useita haavoittuvuuksia	Onko kohteen haavoittuvuuksia helppo hyödyntää	Täydentävätkö haavoittuvuudet toisiaan	Pienentävätkö nykyiset vastatoimet haavoittuvuuksia	Muodostavatko nykyiset vastatoimet kerroksittaisen puolan?	Onko haavoittuvuuden kohde merkittävä tehtävän toteuttamisen kannalta	Kohteella ei ole kykyä reagoida haavoittuvuuksiin	Kohteella ei ole varamenetelmiä haavoittuvuuksien varalle	Haavoittuvuuksien toteutumisen harjoitellun taso	Haavoittuvuus 0-30
1	Terroristijärjestö X	Pommi-isku	Yleisö	Avoin pääsy; monta kulkureittiä	3	2	1	0	3	2	1	0	3	2	17
2	0	0	0												0
3	0	0	0												0
4	0	0	0												0
5	0	0	0												0
6	0	0	0												0
7	0	0	0												0

Haavoittuvuusarvio.

Riskiluku = (Uhkataso x (kriittisyystaso + Haavoittuvuustaso))/1,35. Tällöin riskiluku skaalautuu välille 0-1000. Välehdeltä riskin merkityksen arviointi löytyy havoinnollistavia kuvia uhkatason, haavoittuvuustason ja riskiluvun merkityksen arviointii.

Riskianalyysin ja -arvioinnin koonnos

	Uhkan lähde / Tekijä	Uhka / Tapahtuma	Kriittinen tekijä	Uhkan kohde	Kriittisyystaso	Manuaalinen Kriittisyystaso	Aie	Man. Aie	Kyky	Man. Kyky	Uhkataso	Manuaalinen Uhkataso	Haavoittuvuustaso	Manulaalinen Haavoittuvuustaso	Riskiluku	Lisätietoja/kommer
1	Terroristijärjestö X	Pommi-isku	Henkilöstö	Yleisö	8	15	10		11		21		17		498	
2	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
3	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
4	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
5	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
6	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
7	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
8	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
9	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
10	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
11	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
12	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
13	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
14	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
15	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
16	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	
17	0	0	0	0	#PUUTTUU!		0		0		0		0		#PUUTTUU!	

Koonnos.

Riskiarvioinnin raportti

Arviointi aloitettu: pphhhhkkkvv
Arviointi lopetettu: 21200MAA20

Arvioinnin kohde: XXX

Kiittisiä tekijöitä, joiden kautta uhkia arvioitiin, tunnistettiin yhteensä 1 kappaletta

Arvioija:
Oma Nimi
Arviointiin osallistui:
Oma Nimi
Oma Nimi
Oma Nimi
Oma Nimi
Oma Nimi
Oma Nimi
Oma Nimi
Oma Nimi

Uhkia arvioitiin yhteensä 1 kappaletta, joista haavoittuvuuksien kanssa arvioituna

Sietämättömiä on:	0 kpl
Merkittäviä on:	1 kpl
Kohtalaisia on:	0 kpl
Vähäisiä on:	0 kpl
Merkityksettömiä on:	0 kpl

Raportti.

RISKILUKU

Haavoittuvuustaso + kriittisyys

Uhkataso	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
1	1	1	2	3	4	4	5	6	7	7	8	9	10	10	11	12	13	13	14	15	16	16	17	18	19	19	20	21	21	22	23	24	24	25	26	27	27	28	29	30	30	31	32	33	33
2	1	3	4	6	7	9	10	12	13	15	16	18	19	21	22	24	25	27	28	30	31	33	34	36	37	39	40	41	43	44	46	47	49	50	52	53	55	56	58	59	61	62	64	65	67
3	2	4	7	9	11	13	16	18	20	22	24	27	29	31	33	36	38	40	42	44	47	49	51	53	56	58	60	62	64	67	69	71	73	76	78	80	82	84	87	89	91	93	96	98	100
4	3	6	9	12	15	18	21	24	27	30	33	36	39	41	44	47	50	53	56	59	62	65	68	71	74	77	80	83	86	89	92	95	98	101	104	107	110	113	116	119	121	124	127	130	133
5	4	7	11	15	19	22	26	30	33	37	41	44	48	52	56	59	63	67	70	74	78	81	85	89	93	96	100	104	107	111	115	119	122	126	130	133	137	141	144	148	152	156	159	163	167
6	4	9	13	18	22	27	31	36	40	44	49	53	58	62	67	71	76	80	84	89	93	98	102	107	111	116	120	124	129	133	138	142	147	151	156	160	164	169	173	178	182	187	191	196	200
7	5	10	16	21	26	31	36	41	47	52	57	62	67	73	78	83	88	93	99	104	109	114	119	124	130	135	140	145	150	156	161	166	171	176	181	187	192	197	202	207	213	218	223	228	233
8	6	12	18	24	30	36	41	47	53	59	65	71	77	83	89	95	101	107	113	119	124	130	136	142	148	154	160	166	172	178	184	190	196	201	207	213	219	225	231	237	243	249	255	261	267
9	7	13	20	27	33	40	47	53	60	67	73	80	87	93	100	107	113	120	127	133	140	147	153	160	167	173	180	187	193	200	207	213	220	227	233	240	247	253	260	267	273	280	287	293	300
10	7	15	22	30	37	44	52	59	67	74	81	89	96	104	111	119	126	133	141	148	156	163	170	178	185	193	200	207	215	222	230	237	244	252	259	267	274	281	289	296	304	311	319	326	333
11	8	16	24	33	41	49	57	65	73	81	90	98	106	114	122	130	139	147	155	163	171	179	187	196	204	212	220	228	236	244	253	261	269	277	285	293	301	310	318	326	334	342	350	359	367
12	9	18	27	36	44	53	62	71	80	89	98	107	116	124	133	142	151	160	169	178	187	196	204	213	222	231	240	249	258	267	276	284	293	302	311	320	329	338	347	356	364	373	382	391	400
13	10	19	29	39	48	58	67	77	87	96	106	116	125	135	144	154	164	173	183	193	202	212	221	231	241	250	260	270	279	289	299	308	318	327	337	347	356	366	376	385	395	404	414	424	433
14	10	21	31	41	52	62	73	83	93	104	114	124	135	145	156	166	176	187	197	207	218	228	239	249	259	270	280	290	301	311	321	332	342	353	363	373	384	394	404	415	425	436	446	456	467
15	11	22	33	44	56	67	78	89	100	111	122	133	144	156	167	178	189	200	211	222	233	244	256	267	278	289	300	311	322	333	344	356	367	378	389	400	411	422	433	444	456	467	478	489	500
16	12	24	36	47	59	71	83	95	107	119	130	142	154	166	178	190	201	213	225	237	249	261	273	284	296	308	320	332	344	356	367	379	391	403	415	427	439	450	462	474	486	498	510	521	533
17	13	25	38	50	63	76	88	101	113	126	139	151	164	176	189	201	214	227	239	252	264	277	290	302	315	327	340	353	365	378	390	403	416	428	441	453	466	479	491	504	516	529	541	554	567
18	13	27	40	53	67	80	93	107	120	133	147	160	173	187	200	213	227	240	253	267	280	293	307	320	333	347	360	373	387	400	413	427	440	453	467	480	493	507	520	533	547	560	573	587	600
19	14	28	42	56	70	84	99	113	127	141	155	169	183	197	211	225	239	253	267	281	296	310	324	338	352	366	380	394	408	422	436	450	464	479	493	507	521	535	549	563	577	591	605	619	633
20	15	30	44	59	74	89	104	119	133	148	163	178	193	207	222	237	252	267	281	296	311	326	341	356	370	385	400	415	430	444	459	474	489	504	519	533	548	563	578	593	607	622	637	652	667
21	16	31	47	62	78	93	109	124	140	156	171	187	202	218	233	249	264	280	296	311	327	342	358	373	389	404	420	436	451	467	482	498	513	529	544	560	576	591	607	622	638	653	669	684	700
22	16	33	49	65	81	98	114	130	147	163	179	196	212	228	244	261	277	293	310	326	342	359	375	391	407	424	440	456	473	489	505	521	538	554	570	587	603	619	636	652	668	684	701	717	733
23	17	34	51	68	85	102	119	136	153	170	187	204	221	239	256	273	290	307	324	341	358	375	392	409	426	443	460	477	494	511	528	545	562	579	596	613	630	647	664	681	699	716	733	750	767
24	18	36	53	71	89	107	124	142	160	178	196	213	231	249	267	284	302	320	338	356	373	391	409	427	444	462	480	498	516	533	551	569	587	604	622	640	658	676	693	711	729	747	764	782	800
25	19	37	56	74	93	111	130	148	167	185	204	222	241	259	278	296	315	333	352	370	389	407	426	444	463	481	500	519	537	556	574	593	611	630	648	667	685	704	722	741	759	778	796	815	833
26	19	39	58	77	96	116	135	154	173	193	212	231	250	270	289	308	327	347	366	385	404	424	443	462	481	501	520	539	559	578	597	616	636	655	674	693	713	732	751	770	790	809	828	847	867
27	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300	320	340	360	380	400	420	440	460	480	500	520	540	560	580	600	620	640	660	680	700	720	740	760	780	800	820	840	860	880	900
28	19	39	58	77	96	116	135	154	173	193	212	231	250	270	289	308	327	347	366	385	404	424	443	462	481	501	520	539	559	578	597	616	636	655	674	693	713	732	751	770	790	809	828	847	867
29	21	43	64	86	107	129	150	172	193	215	236	258	279	301	322	344	365	387	408	430	451	473	494	516	537	559	580	601	623	644	666	687	709	730	752	773	795	816	838	859	881	902	924	945	967
30	22	44	67	89	111	133	156	178	200	222	244	267	289	311	333	356	378	400	422	444	467	489	511	533	556	578	600	622	644	667	689	711	733	756	778	800	822	844	867	889	911	933	956	978	1000

Riskiluvun muodostuminen.

Liite 4: Tutkimuslupa

Pääesikunta
Suunnitteluosasto
HELSINKI

Päätös

1 (2)

AP18236

28.10.2019

Jääkäriprikaati
Esikunta
Esko Äärynen

MP21190 TUTKIMUSLUPA-ANOMUS (ÄÄRYNEN) 1.10.2019

TUTKIMUSLUPA (ÄÄRYNEN)

1 Tutkimuslupahakemus

Jääkäriprikaatissa työskentelevä kapt Esko Äärynen hakee 1.10.2019 päivätyllä viiteasiakirjalla (MP21190) tutkimuslupaa ylempään ammattikorkeakoulututkintoon kuuluvaan opinnäytetutkimukseen.

Opinnäytetyön tavoitteena on kehittää helppokäyttöinen riskianalyysityökalu, joka olisi yhteisesti käytettävissä Puolustusvoimien turvallisuusalan henkilöstöllä.

Opinnäytetyön tiedot kerätään julkisesta lähdekirjallisuudesta sekä turvallisuuden johtamisen opintojakson opiskelijoilta ja opettajilta kerätyistä tiedonkeruulomakkeista/haastatteluista.

Tutkimus toteutetaan julkisena.

Työn ohjaajana toimii alustavasti komentajakapteeni Richard Wunsch (p. 0299 520 502, Richard.Wunsch@mil.fi).

2 Päätös lupaehtoineen

Pääesikunnan suunnitteluosasto **myöntää** Esko Ääryselle luvan tietojen keräämiseen turvallisuuden johtamisen opintojakson opiskelijoilta ja opettajilta seuraavin ehdoin:

- Lupa on henkilökohtainen ja määräaikainen päättyen 30.6.2020.
- Tutkimuksesta ei saa syntyä kustannuksia Puolustusvoimille.
- Tutkimusaineiston keräämisessä, käsittelyssä, säilyttämisessä ja tuhoamisessa tulee noudattaa henkilötietolakia kokonaisuudessaan sekä hyvää tutkimusetiikkaa.
- Tutkimus on toteutettava kaikilta osin julkisena
- Ennen opinnäytetyön palauttamista oppilaitokseen Puolustusvoimissa toimiva työnohjaaja tarkistaa, ettei opinnäytetyö sisällä suo-

Pääesikunta
Suunnitteluosasto
PL 919
00131 HELSINKI

Puh. 0299 800
Faksi (09) 181 22813

Y-tunnus 0952029-9
www.puolustusvoimat.fi

jattavia tietoja

- Pääesikunnan suunnitteluosastolle toimitetaan opinnäytetyön loppuraportti
- Puolustusvoimilla on oikeus julkaista tutkimusraportti Puolustusvoimien tutkimusrekisterissä.

3 Valitusosoite

Tähän päätökseen tyytymätön voi hakea siihen muutosta valittamalla Helsingin hallinto-oikeuteen tämän asiakirjan liitteenä olevan valitusosoituksen mukaisesti.

4 Yhteyshenkilö

Pääesikunnan suunnitteluosaston yhteyshenkilö tutkimuslupaan liittyen on KTM Katri Järvinen (katri.jarvinen@mil.fi, p. 0299 510 564).

Apulaisosastopäällikkö
Eversti Manu Tuominen

Sektorijohtaja
Everstiluutnantti Petteri Korvala

LIITTEET Valitusosoite

JAKELU

TIEDOKSI Richard Wunsch, Puolustusvoimien tiedustelulaitos Esikunta