Irina Lönnqvist

LÄHTEEN JA TIEDON LUOTETTAVUUDEN MATRIISI KYBERTIEDONVAIHTOON

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Lönnqvist, Irina
Lähteen- ja tiedonluotettavuuden mittaristo kybertiedonvaihtoon
Jyväskylä: Jyväskylän yliopisto, 2024, 94 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Lehto, Martti; Eronen, Juhani

Tilannekuvan ja tietojen jakaminen ovat keskiössä nopeasti muuttuvassa kybertoimintaympäristössä. Tätä varten eri kansainväliset toimijat hyödyntävät tiedon ja lähteen luotettavuuden matriiseja tietoa jakaessaan. Matriiseissa on kaksi erillistä kategoriaa, lähde ja tieto, joiden avulla saatua tietoa pyritään luokittelemaan. Suomessa ei tällä hetkellä käytetä viranomaisten väliseen tiedonvaihtoon yhteistä matriisia, jossa lähteen ja tiedon luotettavuus merkittäisiin. Tarve tällaiselle tiedon luokitukselle on kuitenkin tunnistettu. Työn tarkoituksena oli selvittää, minkälainen lähteen ja tiedonluotettavuuden matriisi olisi sopiva kybertiedonvaihtoon. Lisäksi työssä kartoitettiin, miten jo olemassa olevista matriiseista, voisi rakentaa kybertiedonvaihtoon sopivaa matriisia. Tämän lisäksi pyrittiin selvittämään, miten lähteen ja tiedon luotettavuutta kuvaavat matriisit tulisi määritellä, jotta ne palvelisivat parhaalla mahdollisella tavalla eri toimijoita ja olisivat sovellettavissa kybertoimintaympäristössä tapahtuvaan tiedonvaihtoon. Työn fokuksessa olivat suomalaiset kyberturvallisuusviranomaiset, mutta elinkeinoelämän tarve tunnistettiin osana työtä. Työn teoreettinen kehys muodostui tiedon ja informaation luotettavuutta käsittelevistä teorioista sekä erilaisista lähteen ja tiedon luotettavuutta kuvaavista matriiseista. Tutkimuksen aineisto kerättiin hyödyntäen kvalitatiivisia tutkimusmenetelmiä. Aineisto koostuu kahdesta osasta. Työn alussa kutsuttiin Delfoi-asiantuntijapaneeli tekemään määrittelytyötä, jonka lopputuloksena syntyi matriisi, joka olisi sovellettavissa kybertiedonvaihtoon. Tätä aineistoa täydennettiin valtion kyberturvallisuusjohtajan haastattelulla, joka näki paneelin lopputuloksena syntyneen matriisin ja pääsi kommentoimaan sitä ja sen hyödyllisyyttä.

Asiasanat: tilannekuva, tiedon luotettavuus, lähteen luotettavuus, kybertoimintaympäristö

ABSTRACT

Lönnqvist, Irina
Source and information reliability matrix for cyber information exchange
Jyväskylä: University of Jyväskylä, 2024, 94 pp.
Cyber Security, Master's Thesis
Supervisors: Lehto, Martti; Eronen, Juhani

The situational awareness and information sharing in the rapidly changing cyber environment is important. For this purpose, various international actors use the information and source reliability metrics when sharing information. The matrices have two separate categories, source, and information, which are used to classify the information obtained. In Finland, there is currently no common metrics used for the exchange of information between authorities, which would mark the reliability of the source and the information. However, the need for such classification of information has been identified. The purpose of the work was to find out what kind of source and information reliability metrics would be suitable for cyber information exchange. In addition, the work mapped out which of the already existing metrics could be used to build a set of metrics suitable for cyber data exchange. In addition to this, an effort was made to find out how the metrics describing the reliability of the source and information should be defined so that they would serve different authorities in the best possible way and apply to the exchange of information in a cyber environment. The focus of the work was Finnish cyber security authorities, but the need of business life was recognized as part of the work. The theoretical framework of the theses consists of theories conceptualizing the reliability of knowledge and information, as well as various matrices describing the reliability of the source and information. The research material was collected using qualitative research methods. The material consists of two parts. At the beginning of the work, a Delphi panel of experts was invited to do the definition work, the result of which was a matrix that would be applicable to cyber information exchange. This material was supplemented by an interview with the state's cybersecurity director, who saw the matrix created because of the panel and was able to comment on it and its usability.

Keywords: situational awareness, information reliability, source reliability, cyber operational environment

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Eri viranomaiset kuten poliisi, puolustusvoimat ja tiedustelutoimijat hyödyntävät työssään tiedon luotettavuuden mittareita. Näitä mittareita on sekä kansallisella tasolla, mutta myös sellaisia mittareita, joita hyödynnetään yhteisesti eri maissa tai esim. Euroopan unionin tasolla. Näistä esimerkkeinä Naton käyttämä amiraliteettikoodi (engl. Admiralty code) sekä 4x4-matriisi, jota esimerkiksi Europolin käyttää tiedon luotettavuuden matriisina. Näiden mittareiden avulla pyritään arvioimaan lähteen luotettavuutta sekä saadun tiedon luotettavuutta. Mittareissa on kaksi erillistä kategoriaa, sillä esimerkiksi lähde voi olla luotettavaksi todettu, mutta sen jakamaa tietoa ei voida varmistaa ja näin ollen se saa sopivan arvon, joka kuvaa lähdettä ja siltä saatua tietoa. (esim. Hibbs Pherson ja Pherson, 2021.)

Kybertilannekuvan rakentaminen on keskeistä eri viranomaisille, ja ne tarkastelevat kybertoimintaympäristöä kukin omasta lähtökohdastaan. Suomessa kybertilannekuvaa muodostavat erityisesti Kyberturvallisuuskeskus, Poliisi ja erityisesti Keskusrikospoliisin kyberrikostorjunnankeskus, Puolustusvoimat ja Suojelupoliisi. Viranomaiset saavat tietoa eri verkostojensa kautta. Tilannekuvan ja tiedon jakaminen ovat keskiössä, jotta kokonaiskuvaa kybertilannekuvasta voidaan rakentaa.

Viranomaiset tekevät tiivistä yhteistyötä ja tietoja vaihdetaan osana normaaleja prosesseja. Useasti viranomaiset tarkistavat tiedon huolellisesti ennen kuin jakavat sitä eteenpäin. Epävarmaa tai vahvistamatonta tietoa jaetaan harvoin eteenpäin. Kybermaailmassa tilanne elää nopeasti ja tieto saattaa olla jo vanhentunutta tai epärelevanttia, kun se ollaan erilaisten tarkistusprosessien jälkeen valmiita jakamaan.

Toimijoille kertyy paljon erilaista tietoa, joka ei välttämättä ole relevanttia niille itselleen. Ne kuitenkin tunnistavat, että kyseinen tieto voisi olla toiselle viranomaiselle tärkeää tietoa. Jos virnaominen ei voi olla varma jakamastaan tiedosta, saattaa se jättää sen jakamatta. Yhteinen malli tiedon ja lähteen luotettavuuden merkitsemiseksi mahdollistaa esimerkiksi epävarman tai tarkistamattoman tiedon jakamisen edelleen matalammalla kynnyksellä.

Toinen seikka tiedon jakamisessa on useasti se, että tiedon lähdettä ei saa tai sitä ei haluta paljastaa. Joko tiedon jakanut taho on sen kieltänyt tai halutaan suojella lähdettä. Yhteisen matriisin ja siihen liitetyn ohjeen avulla tietoa voitaisiin jakaa lähdettä paljastamatta. Tämä kuitenkin mahdollistaisi sen, että vastaanottavalla taholla olisi mahdollisuus ymmärtää, minkälaisesta lähteestä tieto on peräisin, kun määrittelytyö tehdään yhdessä matriisia käyttävien viranomaisten kesken. Vaikka lähdettä ei tiedetä, mutta voidaan tehdä siitä jonkinlaista arviota, auttaa tämä myös tiedon vastaanottajaa arvioimaan omalta osaltaan tiedon luotettavuutta. Samalla voidaan myös tehdä mahdollista arviota siitä, onko sama tieto saatu omalta lähteeltä ja tehdä mahdollista arviota siitä onko tieto mahdollisesti jopa samasta lähteestä.

Erityisesti kansanvälisessä yhteistyössä viranomaiset voivat saada tiedon omilta vastinpareiltaan, jotka saattavat olla samaa organisaatiota. Esimerkiksi kyberturvallisuuskeskus saattaa eri EU-maissa olla osa maan puolustusvoimia. Näin ollen he antavat tiedon Suomessa erillisenä viranomaisena toimivalle Kyberturvallisuuskeskukselle, mutta sama tieto saatetaan antaa Puolustusvoimille, sillä paikallinen kyberturvallisuuskeskus on osa maan puolustusvoimien organisaatiota. Kun molemmat viranomaiset saavat saman tiedon, mutta eri lähteiden kautta voi syntyä vahvistusharha, että on olemassa kaksi tietoa, jotka tulevat eri lähteistä ja näin ollen tieto validoidaan. Todellisuudessa tieto onkin peräisin samasta lähteestä.

Työn tavoitteena on tuottaa suomalaisten kyberviranomaisten käyttöön lähteen ja tiedon luotettavuuden matriisi, jotta tietoa voitaisiin jakaa nopeammin ja siten, ettei sitä ole aina ehditty itse tarkistamaan. Näin ollen tarkoituksena on selvittää, minkälainen tiedonluotettavuuden matriisi olisi sopiva ja miten lähteen ja tiedon luotettavuutta kuvaavat kategoriat tulisi määritellä, jotta ne palvelisivat parhaalla mahdollisella tavalla eri toimijoita. Matriisi on tarkoitettu vain kybertiedonvaihtoon ja näin ollen ulkopuolelle rajataan muut tiedon keräyksen muodot, kuten esimerkiksi henkilötiedustelu, jossa arvioidaan lähteen luotettavuutta ja sitä, kuinka kauan lähde on tuottanut tiedustelupalvelulle tietoa.

Teoreettinen kehys muodostuu tiedon ja informaation luotettavuutta käsittelevistä teorioista sekä erilaisista lähteen ja tiedon luotettavuutta kuvaavista matriiseista. Viitekehys koostuu esimerkiksi amiraalikoodistosta, jota hyödynnetään erityisesti eri maiden puolustusvoimassa ja NATO-yhteydessä, sekä 4x4-matriisista, jota esimerkiksi Europol hyödyntää yhdessä EU:n jäsenvaltioiden poliisiviranomaisten kanssa käytävässä tiedonvaihdossa. Eri esimerkkimittareiden pohjalta kehitettiin työssä tehty matriisi. Hyödyntämällä olemassa olevia mittareita ja sovittamalla ne kansalliseen viitekehykseen, ei varsinaisesti luotu kokonaan uutta mallia vaan sovitettiin olemassa olevia malleja kansallisesti. Tarkoituksena oli, että työssä tehty matriisi on helposti käännettävissä myös amiraalikoodiston tai 4x4-matriisin luokkiin. Tämä mahdollistaa myös tiedonjaon kansainvälisille verkostoille, jossa eri mittareita hyödynnetään.

2 TUTKIMUSONGELMA JA TUTKIMUKSEN TAVOITTEET

Viranomaisten kybertilannekuva ja sen koostaminen sekä kybertiedon jakaminen viranomaisten välillä on ollut esillä viime vuosina, sillä vastuu jakautuu eri viranomaisten kesken eikä keskity vain yhdelle toimijalle Suomessa. Puolustusministeriön ja Sisäministeriön johtama hanke (2022–2023) ”Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa” pyrki selvittämään nykytilaa ja antamaan tulevaisuuteen kehittämisehdotuksia kansallisen kyberturvallisuuden varmistamisesta, kyberrikollisuuden torjunnasta, kyberpuolustuksesta sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavista tilanteista, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuvan kehittymisen. Selvitystyössä käydään läpi eri viranomaisten roolit, jotka erityisesti kyberturvallisuustyöhön osallistuvat. Keskiössä oli kybertilannekuvan muodostaminen ja toiminta kybertoimintaympäristössä. Samalla selvitystyössä nostettiin esille myös oikeudellisia puutteita, jotka tiedonvaihtoa estävät. (Valtioneuvoston julkaisuja, 2023, 3.)

Työn tarkoituksena on tuottaa lähteen ja tiedonluotettavuuden matriisi kybertiedonvaihtoon. On tärkeää, että matriisia luodessa keskitytään vain kybertiedonvaihtoon, sillä se rajaa matriisin ulkopuolelle muut tiedustelulajit kuten esimerkiksi henkilötiedustelun, jossa lähteen luotettavuutta arvioidaan hyvin eri tavalla. Henkilötiedustelussa tieto tulee perinteisesti ihmiseltä, eikä siinä ole teknisiä elementtejä samalla tavalla kuin kybertiedonvaihdossa, jossa suuri osa vaihdetusta tiedosta on jollain tavalla digitaalisessa muodossa. On mahdollista, että eri viranomaiset hyödyntävät jo nyt erilaista tiedon luokittelua omassa työssään. Työtä varten tehdyssä aineistohaussa ei löytynyt tietoa siitä, että suomalaiset viranomaiset hyödyntäisivät kyberkontekstissa yhteistä lähteen ja tiedon luotettavuuden matriisia.

2.1 Tutkimuskysymys

Tutkimuskysymys ja tarve mittareille nousi käytännön havaintojen ja keskusteluiden kautta, jossa asiantuntijat toivoivat tiedon jakamisen olevan helpompaa. Tähän yksi vastaus oli esimerkiksi se, että tiedon voisi jollakin tavalla luokitella. Kyberympäristössä tilanne elää nopeasti ja tiedon jakaminen niin nopeasti, kuin mahdollista on tärkeässä roolissa, sillä tieto vanhenee myös nopeasti. Tietoa ei aina ehditä tarkastamaan ja erillinen luokittelutieto auttaisi tämän kertomisessa.

Työn tavoitteena on tuottaa suomalaisten kyberviranomaisten käyttöön lähteen ja tiedonluotettavuuden matriisi. Näin ollen tarkoituksena on selvittää:

- Minkälainen lähteen ja tiedonluotettavuuden matriisi olisi sopiva kybertiedonvaihtoon?

Kysymystä tullaan tarkentamaan alakysymyksillä:

- Voitaisiinko jo olemassa olevista matriiseista, kuten amiraalikoodisto ja 4x4-matriisi, rakentaa kybertiedonvaihtoon sopiva mittaristo?
- Miten lähteen ja tiedon luotettavuutta kuvaava matriisi tulisi määritellä, jotta se palvelisi parhaalla mahdollisella tavalla eri toimijoita (suomalaiset kyberturvallisuusviranomaiset).

2.2 Työn rajaukset

Edellä esitetyn lisäksi toinen tunnistettu tarve on tiedon jakaminen viranomaisilta elinkeinoelämälle esimerkiksi huoltovarmuuskriittisille toimijoille sekä muille yhteiskunnan toimivuuden kannalta keskeisille yrityksille. Tiedon jakaminen elinkeinoelämälle rajataan työn ulkopuolelle. Työssä tehtyä matriisia voitaisiin kuitenkin soveltaa tiedonvaihdossa elinkeinoelämän suuntaan. Se voisi nopeuttaa viranomaisen jakamaa tietoa yrityksille, sillä se mahdollistaisi myös epävarman tiedon jakamisen. Luokittelun avulla voitaisiin kertoa, että tietoa ei ole voitu vahvistaa. Kriittinen infrastruktuuri on pääosin yritysten ylläpitämä, jolloin kybertilannetiedon- ja tilannekuvan jakaminen yrityksille on tärkeää, jotta ne voivat suojata kriittistä infrastruktuuria.

Tässä työssä ei ole tarkoitus nostaa juridista puolta esille kybertiedonvaihdossa, sillä se muodostaa oman kokonaisuuden. Tällä hetkellä laki mahdollistaa tietynlaisen kybertiedonvaihdon viranomaisten välillä, mutta kuten Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa (2023) tuodaan esille, halutaan tiedonvaihtoa sujuvoittaa ja helpottaa, jotta nopeasti muuttuvan toimintaympäristön esittämiin haasteisiin voidaan vastata. Tässä työssä on tunnistettu lainsäädännön mahdolliset puutteet, mutta niitä ei erikseen tässä käsitellä vaan keskistytään matriisin rakentamiseen lähteen ja tiedon luotettavuuden

näkökulmasta, sillä matriisin käyttö ei edellytä juridisia toimia, vaan tietoa voidaan vaihtaa voimassa olevan lainsäädännön mukaan.

3 TYÖN TEOREETTINEN VIITEKEHYS JA KESKEISET KÄSITTEET

Tässä osiossa käydään työn kannalta keskeiset käsitteet. Työssä käytetään paljon kyber-alkuisia termejä, joilla on oma merkityksensä. Yksittäisenä sanana kyber ei tarkoita mitään, vaan sitä käytetään määriteosana yhdessä muiden sanojen kanssa. (Moilanen ja Lönnqvist, 2017.) Sanan merkitys liittyy yleensä digitaalisessa muodossa olevan tiedon tai informaation käsittelyyn ja useasti vasta koko yhdyssanalla voidaan ajatella olevan oma merkityksensä (Laari, Flyktman, Härmä, Timonen ja Tuovinen, 2019, 9).

Käsitteiden lisäksi osiossa avataan niiden keskeisten viranomaisten rooleja kyberturvallisuuden toimijoina, joille matriisi ensisijaisesti on suunnattu. Suomessa useampi viranomainen vastaa kybertilannekuvan rakentamisesta. Kokonaiskuvan rakentamiseksi viranomaisten keskinäinen tiedonvaihto on avainroolissa, jotta kokonaistilannekuvaa pystytään rakentamaan, sillä eri toimijoille kertyy paljon erilaista tietoa.

Osion lopussa esitellään jo olemassa olevia lähteen ja tiedon luotettavuuden mittareita. Nämä matriisit ovat sellaisia, joita eri viranomaiset kansainvälisesti jo käyttävät. Mittareita on otettu myös eri puolilla kansallisesti käyttöön, jolloin niitä on saatettu muokata hieman omiin tarpeisiin sopivaksi. Esitellyt matriisit ovat toimineet perustana työssä tehdylle matriisille.

3.1 Kybertoimintaympäristö

Kyberympäristö voidaan jakaa kahteen osa-alueeseen niin fyysisen kuin digitaalisen maailman. Monet arkemme toiminnoista fyysisessä maailmassa ovat nykyisin täysin riippuvaisia digitaalista tietojärjestelmistä, joiden toimivuus vaikuttaa arjen sujuvuuteen. (Moilanen ja Lönnqvist, 2017.) Kybertoimintaympäristö rakentuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä, joka ei ole maantieteellisesti rajattu. Tämän takia kybertoimintaympäristössä etäisyyttä on arvioitava eri tavalla. Esimerkiksi tietty komponentti saattaa sijaita fyysisesti

toisella puolella maailmaa kuin sen käyttäjät. (Laari ym., 2019, 9-10.) Tämän takia kybertoimintaympäristö on tullut entistä vahvemmin osaksi myös ulko- ja turvallisuuspolitiikkaa (Ulkoministeriö, 2010). Kyberympäristö on myös digitalisoituneen yhteiskunnan ja valtion tehokkaan toiminnan edellytyksiä, jossa viestintäverkkojen toimivuus sekä viranomaisten tietovarantojen eheys, luottamuksellisuus ja saatavuus voidaan turvata (Valtioneuvoston julkaisuja, 2023, 11).

Kybertoimintaympäristön ominaisuuksiin kuuluu kehityksen suuri nopeus. Tämän vuoksi hektisyys kuvaa kybertoimintaympäristön tapahtumia hyvin. Eri järjestelmien kompleksisuus ja niiden riippuvuus toisiinsa on välillä vaikeastikin hahmotettavissa. Informaatioteknologian osalta kehityssykli on lyhyt ja sama trendi koskee eri kyberhyökkäysmuotoja ja haittaohjelmia eli kyberuhkia. Kybertoimintaympäristölle on ominaista kiihtyvä muutosnopeus, ilmiöläheisyys, kompleksisuus ja osittainen ennalta-arvaamattomuus. (Lehto, Limnéll, Kokkomäki, Pöyhönen, 2018, 12.)

3.2 Kyberturvallisuus

Kybertoimintaympäristön ohella myös kyberturvallisuuden termiä käytetään useasti eri yhteyksissä, kuten mediassa. Toisinaan sitä käytetään kuin synonyyminä kyberympäristölle, mutta tämän lisäksi sillä on myös toisenlainen merkitys. Kyberturvallisuus on kybertoimintaympäristön turvallisuutta. Se tarkoittaa sitä, että kybermaailmaan kohdistuvat uhat ovat hallinnassa ja kybertoimintaympäristö toimii oikein ja virheettömästi. (Moilanen ja Lönnqvist, 2017.) Tällöin huomioidaan myös kybertoimintaympäristön vaikutukset fyysiseen maailmaan ja kyberturvallisuus rakennetaan yhdessä eri toimijoiden kesken (Laari ym., 2019, 9). Kyberturvallisuus on tavoitetila, jossa kyberympäristöön voidaan luottaa ja jossa sen toiminta turvataan (Turvallisuuskomitea, 2017, 35).

3.3 Kyberuhka ja uhkatieto

Yhteiskuntien digitalisoituminen, nopea teknologinen kehitys ja erilaisten toimijoiden kykyjen kasvu ovat moninaistaneet ja kasvattaneet kyberuhkia yhteiskunnassa. Tämä on näkynyt niin vakavan kyberrikollisuuden kasvuna kuin kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvina uhkina. (Valtioneuvoston julkaisuja, 2023, 11.) Vaikka kybertoimintaympäristö on valtion rajat ylittävää, on sillä vaikutuksia erityisesti kansallisesti ja siellä tapahtuviin poikkeuksiin reagoidaan kansallisesti tai yhdessä yhteistyössä muiden valtioiden kanssa.

Uhkatieto on dataa, jota kerätään, käsitellään ja analysoidaan uhkatoimijan motiivien, kohteiden ja hyökkäyskäyttäytymisen ymmärtämiseksi. Uhkatietojen avulla voidaan tehdä nopeampia, tietoisempia, tietoturvallisia päätöksiä ja muuttaa heidän käyttäytymistään reaktiivisesta ennakoivaksi taistelussa uhkatoimijoita vastaan. (esim. Baker, 2023.)

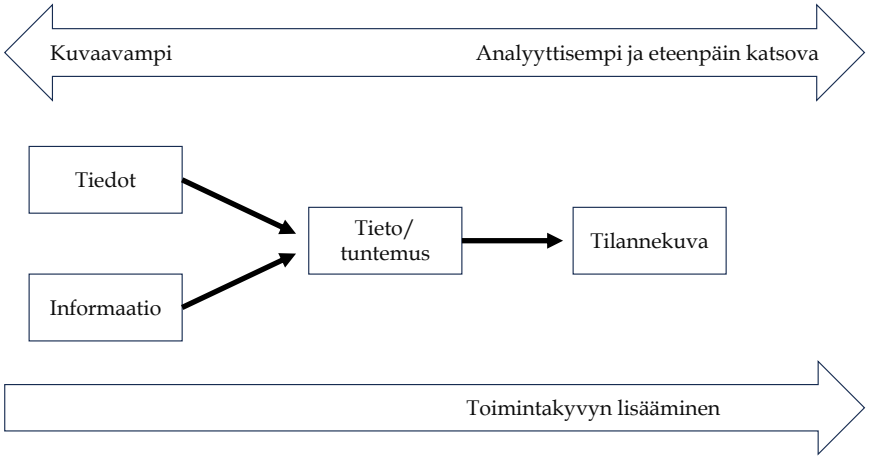
Työssä kyberiin liitetty uhkatieto halutaan ymmärtää laajasti, se voi olla teknistä tietoa, kuten esimerkiksi vaarantumisindikaattori (engl. Indicator of Compromise, IoC). Esimerkiksi havainto kartoitustoiminnasta tai muusta digitaalisesta tai fyysisestä todisteesta, että kyberhyökkääjällä on aikomus hyökätä (engl. Indicator of attac, IoA). Henkilöltä tai verkostolta saatu tieto tai havainto, jossa kerrotaan uhkahavainnosta, mutta sille ei ole antaa tarkempaa teknistä tietoa vaan kyseessä voi olla analyytikon tuottama havainto ja tietojen yhdistäminen, jolla tieto on tuotettu. (esim. Interactive Terminology for Europe, 2017.) Uhkatiedon lisäksi saatu tieto voi olla myös tilannekuvaa tai muuta sellaista tietoa, joka liittyy aiheeseen ja tietoa vaihdetaan kybertoimijoiden kesken.

3.4 Tilannekuva ja tilannekuvan tasot

”Tilannekuvalla tarkoitetaan koottua kuvausta vallitsevista olosuhteista, käsillä olevan tilanteen synnyttäneistä tapahtumista, tilannetta koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista sekä eri toimijoiden toimintavalmiuksista (Turvallisuuskomitea, 2017, 64)”.

Pelkkä yksittäinen tieto tai informaatio ei kuitenkaan vielä tuota tarvittavaa tilannekuvaa vaan tieto tulee tuottaa tiedoksi ja sitä kautta tiedustelutiedoksi, jotta se voidaan liittää paremmin kontekstiin ja tarjota tarvittavaa tilannekuvaa (OSCE Guidebook, 2017, 16-17). ”Tilannekuvan avulla muodostetaan tilannetietoisuutta, jolla tarkoitetaan päättäjien ja heidän avustajiensa päätöksiään varten tarvitsema ymmärrys tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolien tavoitteista ja tapahtumien mahdollisista kehitysvaihtoehdoista (Turvallisuuskomitea, 2017, 64)”.

Kuviossa 1 tiedon jalostumista tilannekuvaksi pyritään kuvaamaan yksinkertaisella tavalla. Alussa on yksittäinen tieto, jota rikastetaan muilla jo olemassa olevilla tiedoilla tai tietoa hankitaan lisää. Tästä kokonaisuudesta lähdetään muodostamaan tilannekuvaa, joka tapauksesta alkaa rakentumaan. Monesti esimerkiksi eri viranomaiset saavat alkuun yksittäisiä tietoja, joita rikastetaan joko hakemalla lisää tietoa tai täydentämällä jo olemassa olevaa tietoa. Tieto tai informaatio voi tulla niin verkon kautta teknisenä havaintona kuin tietona esimerkiksi toiselta viranomaiselta tai kansainvälisen verkoston kautta. Tiedon saamiseen ja sen rikastamisen jälkeen se liitetään osaksi kontekstia, jolloin se muuttuu tilannekuvaksi ja tilannetiedoksi.



KUVIO 1 Yksittäisestä tiedosta tilannekuvaksi (OSCE Guidebook, 2017, 17)

Tilannekuvan muodostaminen edellyttää riittävää kyvykkyyttä havainnoida kyberympäristöä. Tavoitteena on luoda kokonaiskuvaa, joka kertoo mahdollisista uhista ja meneillään olevista tapahtumista. Tähän liittyy niin fyysisen maailman tapahtumat kuin digitaalisen maailman tapahtumat. Vaikka monesti ajatellaan, että kybertapahtumat ovat vain verkossa, niin yhä enemmän myös fyysisen maailman tapahtumat vaikuttavat siihen, mitä verkossa tapahtuu. (Skopik, 2016.)

Tilannekuva voidaan myös jakaa erilaisiin tasoihin, käyttötarkoituksiin ja sisältöihin (esim. (Valtioneuvoston julkaisuja, 2023, 31). Tilannekuvan tasoja voidaan tarkastella neljän eri lähestymistavan kautta:

- Tekninen tilannekuva, jossa käsitellään yksittäistä tietoa. Tämä tieto voi esimerkiksi olla yksittäinen tekninen uhkatieto (IOC). Tekninen tilannekuva on luonteeltaan nopeaa, sillä erilaisia yksittäisiä tietoja tulee paljon ja niitä käsitellään nopeasti. Esimerkiksi tekniset kyberasiantuntijat arvioivat päivittäin useita yksittäisiä uhkatietoja, mutta kaikki näistä havainnoista eivät johda syvempään tutkintaan.
- Taktinen tilannekuva on sellaista, jossa käsitellään tarkemmin yksittäistä tietoa, minkälaisia taktiikoita, tekniikoita ja prosesseja (TTP) hyökkääjä on käyttänyt. Selvitystyö tarvitsee enemmän aikaa, jotta tilannekuvaa voidaan rakentaa.
- Operatiivinen tilannekuva koostaa yhteen teknisen ja taktisen tilannekuvan sekä liittää sen vahvemmin osaksi kontekstia tarkastellen tiettyä tapausta tai tapahtumasarjaa ja sen vaikutuksia. Operatiivinen tilannekuva vaatii enemmän ja syvempiä tietoja tapahtuneesta, jolloin tilannekuvan koostaminen on myös hitaampaa kuin taktisella ja teknisellä tilannekuvatasolla.
- Strateginen tilannekuva on useasti ei-teknisiä elementtejä sisältävää tilannekuvaa, joka on suunnattu johdolle sekä päätöksentekotasolle. Siinä

tavoitteena on kertoa uhasta sekä sen aiheuttamasta riskistä. Strateginen tilannekuva toimii päätöksenteon tukena. Strategista tilannekuvaa rakennetaan pidemmällä aikajänteellä. Silti päätöksentekotason tulee reagoida, jos alemmilta tasoilta tulee tietoa, joka vaatii nopeaa päätöksentekoa.

(esim. Pöyhönen, Rajamäki, Nuojua ja Lehto, 2021, 6-11 ja A Joint Cybersecurity Operations Platform for EU's CSIRT network, 2023.)

3.5 Tiedon vaihto ja tilannekuvan jakaminen sekä sen haasteet

Suomessa kyberturvallisuus jakautuu usealle eri viranomaistoimijalle (kts 3.6), jolloin kokonaistilannekuva voidaan muodostaa vain tietoa jakamalla. Suomi ei ole poikkeuksellinen vaan monessa muussakin valtiossa useat valtion virastot ja toimijat torjuvat kyberuhkia, ja samalla muodostavat niistä syntyvää tilannekuvaa. Tämän takia tilannekuvan jakaminen on tärkeää, jotta voidaan muodostaa valtiotasolla kokonaistilannekuvaa. (Ihsan, 2019, 5.) Suomessa viranomaisilla on pitkät perinteet tilannekuvan jakamisessa toisilleen. Tilannekuvaa jaetaan eri tasoilla. Kyberturvallisuudentilannekuvaa on tuotettu ja jaettu pitkään teknisellä, taktisella ja operatiivisella tasolla. Vuoden 2022 kesästä lähtien myös kyberturvallisuuden strategista tilannekuvaa on jaettu viranomaisten välillä. (Valtioneuvoston julkaisuja, 2023, 31.)

Vaihdettava tieto voi olla yksittäinen tekninen uhkatieto (IOC) tai kyseessä voi olla laajempi kokonaisuus, joka muodostaa jo itsessään tilannekuvaa. Viranomaisten on myös mahdollistaa rikastaa tietoa, jota toinen tuottaa ja näin saadaan luotua kokonaistilannekuvaa esimerkiksi Suomen kybertilannekuvasta. Jakamalla tietoa ja tilannekuvaa organisaatiot kykenevät paremmin tunnistamaan, arvioimaan, seuraamaan, valvomaan ja reagoimaan mahdollisiin uhkiin. Jaettu tieto voi olla myös sellaista, jota organisaatio ei muuten saisi ja tietoa jakamalla se pystyy torjumaan uhkaa. (Rizov, 2018, 44.)

Tiedon jakamisella on useita hyötyjä. Kun tietoa jaetaan, toimijoiden kokonaistilannekuva paranee ja eri toimijat muodostavat tilannekuvaa yhdessä. Tietoa jakamalla kyvykkyydet uhkan ymmärtämiseksi ja tunnistamiseksi paranevat. Tiedon jakaminen myös todennäköisesti parantaa organisaatioiden omaa kypsyystasoa, sillä se voi tunnistaa uhkia paremmin ja tehdä tarvittavia toimenpiteitä omaan toimintaympäristöönsä. Kyberturvallisuus rakennetaan yhdessä ja näin ollen myös uhat torjutaan yhdessä. Jotta eri organisaatiot voivat torjua omalta osaltaan kyberuhkia tarvitaan tietojen jakamista. (Rizov, 2018, 45.)

Tiedon jakamiseen liittyy keskeisesti myös luottamus. Mikäli luottamusta eri organisaatioiden välillä ei ole, ei tietoa jaeta. Mikäli yhteiset prosessit tiedon jakamiselle puuttuvat, voi tämä olla esiteenä tiedon jakamiselle. Haasteina yhteisille prosesseille on aika. Tämä vaatii sitä, että organisaatiot tuntevat pidemmältä ajalta toisensa ja ovat pystyneet rakentamaan yhteiset tavat ja prosessit tiedon jakamiselle. (esim. Ihsan, 2019, 12. ja Rizov, 2018, 47-48.)

Organisaatioille kertyy hyvin erilaista tietoa. Vaikka tieto itsessään ei olisi luokiteltua eli ei julkista, tieto voidaan kokea olevan arkaluontoista, jota ei haluta antaa toisten organisaatioiden tietoon. Erityisesti valtionhallinnon käsittelemä tieto on useasti myös luokiteltua. Tämä tarkoittaa sitä, että tiedon käsittelylle on asetettu tietyt rajoitukset eikä tietoa ole tarkoitettu julkisesti kaikkien saataville. Rajoitukset saattavat toisinaan myös estää tiedon jakamisen sitä tarvitsevalle taholle. (esim. Ihsan, 2019, 12. ja Rizov, 2018, 47-48.)

Vaikka työssä käsitellään keskeisesti viranomaisia ja niiden välistä tiedonvaihtoa, on tärkeä nostaa esille, että yksityinen sektori muodostaa keskeisen osan kybertoimintaympäristöstä ja tästä johtuen myös sieltä muodostuva tilannekuva ja tietojen vaihtaminen ovat keskeisessä roolissa. Kansallinen tilannekuva muodostuu siis usean organisaation tiedoista, jotka tulee koota yhdeksi kokonaisuudeksi. Tämän lisäksi kansallista tilannekuvaa tulee täydentää kansainvälisiltä verkostoilta saatavilla tiedoilla. Tiedonvaihto myös kansainvälisten kumppaneiden kanssa on keskeisessä roolissa kybertilannekuvan muodostamiseksi, sillä kuten jo aikaisemmin todettiin kybertoimintaympäristö ei ole yhteen paikkaan sidottu eikä se tunne valtioiden rajoja.

3.6 Keskeiset viranomaiset kyberturvallisuuteen liittyen

Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä. Turvallisuus on hyvin moninainen ja turvallisuus elää ajan mukana eli muuttuu siinä missä ympäröivä maailma muuttuu. Kyberturvallisuudesta on tullut yksi osa-alue, josta valtiovalta vastaa. (Limnell, Majewski, Salminen, 2014, 27.) Kyberturvallisuuden johtamisen ylimmän tason muodostaa Valtioneuvosto. Valtioneuvoston tehtävänä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen. Eri ministeriöt vastaavat valtioneuvoston ohjeiden mukaisesti oman toimialansa kyberturvallisuudesta ja siihen liittyvien häiriötilanteiden hallinnasta kuitenkin yhteistoiminnassa muiden kanssa. (Valtioneuvoston periaatepäätös, 2013, 4-5.)

Suomen toinen kyberturvallisuusstrategia julkaistiin vuonna 2019. Tässä strategiassa tunnistettiin tarve kansallisen kyberturvallisuuden kokonaistilan parantamiselle. Strategian mukaisesti liikenne- ja viestintäministeriöön perustettiin kyberturvallisuusjohtajan tehtävä koordinoimaan kyberturvallisuuden kansallista kehittämistä. Rooli on ollut ennen kaikkea yhteensovittava ja kyberturvallisuusjohtaja on koonnut eri hallinnonalojen toimijoita yhteen. (Valtioneuvoston periaatepäätös, 2019, 6.) Valtion kyberturvallisuusjohtajan tehtävä on laaja-alainen ja tukee kyberturvallisuuteen liittyvää valtioneuvostotason ennakointia, varautumista ja päätöksentekoa. Valtion kyberturvallisuusjohtaja koordinoi ja sovittaa yhteen kansallista kyberturvallisuuden kehittämistä, suunnittelua ja varautumista, sekä toimii valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa. Rooli on kehittynyt viimeisten vuosien aikana merkittävästi ja

2024 vuoden alusta rooli on muutettu toiminnoksi. (Valtioneuvoston yleisistunto, 30.11.2023.)

Kyberturvallisuuden tilannekuvaa ylläpitävät Suomessa erityisesti eri viranomaiset kuten Kyberturvallisuuskeskus, Poliisi ja Keskusrikospoliisin kyberrikostorjuntakeskus, Suojelupoliisi ja Puolustusvoimat. Kyberturvallisuuden tehtävät on kuvattu osaksi näiden viranomaisten tehtäviä ja tämän lisäksi roolia vahvistetaan lainsäädännön keinoin. Lisäksi ulkoministeriöllä on keskeinen rooli kybertoimijana, sillä kyberuhat ja hyökkäykset eivät valtion rajoja tunne, mutta tekijät niiden takana saattavat olla valtiollisia toimijoita, jolloin saatetaan tarvita kyberdiplomatian keinoja. (esim. Valtioneuvoston julkaisuja, 2023 25.)

”Liikenne- ja viestintäviraston kyberturvallisuuskeskus, jäljempänä Kyberturvallisuuskeskus, tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta.” (Finlex, 2018). Kansallisen tilannekuvan muodostamisessa hyödynnetään koko liikenne- ja viestintäsektorin toimialaa, kansallisia lähteitä, kuten huoltovarmuuskriittisten yritysten verkostoja, muita turvallisuusviranomaisia sekä kansallisia ja kansainvälisiä yhteistyöverkostoja. Tämän lisäksi Kyberturvallisuuskeskus muodostaa tilannekuvaa saamistaan vapaaehtoisista tietoturvapoikkeamailmoituksista, joita yksilöt ja organisaatiot voivat tehdä. (Esim. Valtioneuvoston julkaisuja, 2023, 23 ja Kyberturvallisuuskeskus, 2024.)

Poliisi vastaa yhtenä tehtävänään kyber- ja verkkorikollisuuden torjunnasta. Työtä tehdään niin paikallispoliisissa kuin keskusrikospoliisissa, jonka yhteydessä toimii kyberrikostorjunnan keskus. (Poliisi, 2024.) Poliisi tutkii tietoverkkorikoksia ja pyrkii saamansa tiedon avulla ennalta ehkäisemään mahdollisia tulevia rikoksia. Poliisin tehtävänä on ylläpitää tietoverkkorikosten kansallista tilannekuvaa, jossa kansainvälinen yhteistyö muiden valtioiden poliisiviranomaisten kanssa on arkipäiväinen osa. Poliisi toimii myös esitutkintaviranomaisena rikoksen, sen yrityksen tai valmistelun osalta ja tämä pätee myös rikoksiin kybertoimintaympäristössä. (Valtioneuvoston julkaisuja, 2023, 24.)

Puolustusvoimat vastaavat kyberpuolustuksesta, jolla tarkoitetaan kansallisen kyberturvallisuuden maanpuolustuksellista osa-aluetta. Roolina on Suomen sotilaallinen puolustaminen ja suvereniteetin takaaminen. (Laari ym., 2019, 45-46.) Tämän lisäksi Puolustusvoimien johtamisjärjestelmäkeskus mahdollistaa puolustusvoimien johtamisen. Keskus järjestää puolustusvoimien tietotekniset palvelut ja sen päätehtäviin kuuluu myös kyberpuolustus. Johtamisjärjestelmäkeskuksen kyberosasto suojaa tietoverkkoja ja -palveluita sekä kehittää kyberpuolustusta. Osasto ylläpitää puolustusvoimien kybertilannekuvaa. (Puolustusvoimat, 2024.)

Suomessa on kaksi tiedusteluviranomaista. Siviilitiedustelusta vastaa Suojelupoliisi ja sotilaallisesta tiedustelusta vastaa Puolustusvoimien sotilastiedustelu. Suojelupoliisin tehtävänä on ennaltaehkäistä ja torjua kaikkein vakavimpia kansallisen turvallisuuden uhkia (Suojelupoliisi, 2024). Suojelupoliisin tehtäviin kuuluu myös tiedustelu verkossa tapahtuvien kyberhyökkäysten taustojen ja

motiivien selvittämiseksi sekä kansallisen turvallisuuden suojaamiseksi. Toiminnallaan se tukee valtiojohdon päätöksentekoa sekä jakaa tilannekuvaa ja tietoa muille viranomaisille ja organisaatioille. Puolustusvoimat on toinen tiedusteluviranomainen, ja sen tehtävänä on vastata sotilastiedustelusta. ”Sotilastiedusteluviranomaiset voivat hankkia tietoa sotilaallisesta toiminnasta sekä vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. Sotilastiedustelun kohteena oleva toiminta voi tapahtua myös kybertoimintaympäristössä.” (Valtioneuvoston julkaisuja, 2023, 24.) Sotilastiedustelu ylläpitää oman toimialansa tilannekuvaa.

Kybertilannekuvan koostaminen jakautuu useammalle viranomaiselle, joista jokaisella on oma erityistehtävänsä. Viranomaisten roolista on useasti myös lailla säädetty ja kybertoimintaympäristön seuranta on osa normaaleja toimintoja. Tiedon ja viranomaiselle kertyneen tilannekuvan jakaminen ovat keskiössä, kun tarkastellaan Suomen kybertilannekuvaa kokonaisuutena. Silloin erilaisten tapahtumien ja tietojen yhdistäminen ovat keskiössä ja tarpeellisia, jotta kokonaiskuvaa voidaan rakentaa.

Yllä esitettyjä tehtäviä ja rooleja on kuvattu taulukossa 1. Tässä taulukossa avataan myös tarkemmin ne lain kohdat, joihin viranomaisen toimivaltuudet perustuvat. Viranomaiset saavat ja käsittelevät saatuja tietoja ja havaintoja oman lainsäädäntönsä puitteissa. Esimerkiksi tiedustelulait koskevat vain tiedusteluviranomaisina sotilastiedustelua ja Suojelupoliisia eikä muilla viranomaisilla, jotka kybertoimintaympäristössä toimii, ole samanlaisia oikeuksia tiedon hankintaan ja käsittelyyn. Jokainen toimii oman roolinsa mukaan ja kokonaistilannekuva muodostuu, kun tiedot eri toimijoilta koostetaan yhteen. Vaikka työssä ei ole tarkoitus käsitellä lainsäädäntöä, on sen mainitseminen oleellista sen osalta, että laissa säädetään se, mitä ja miten viranomainen saa tietoa käsitellä ja miten tietoa voidaan edelleen jakaa.

TAULUKKO 1 Keskeisten kyberviranomaisten roolit ja niihin liittyvät toimivaltuudet ja lainsäädäntö

	Traficom, Kyberturvallisuus-keskus	Esitutkinta-viranomaiset	Tiedustelu-viranomaiset	Puolustusvoimat
Tapahtuma	Tietoturvapoikkeama	Rikos, sen yritys ja valmistelu	Kansallisen turvallisuuden tai maanpuolustuksen uhka	Aseellinen uhka tai sitä vastaava ulkoinen uhka
Toimivaltuutus-säännökset	SVPL 172, 244 a, 273 ja 316 §	PKL 10 ja PolL 5-luvut (poliisi ja Supo) SKRTL (PV)	PolL5 a (Supo) SotTiedL (SotTiedVir)	PVL 4 §, SVPL 272 §
Tavoite	Suomeen vaikuttavan teknisen poikkeaman selvittäminen.	Tapahtuman osapuolten ja tosiseikkojen selvittäminen rikosprosessissa	Vahingon selvittäminen ja tiedon tuottaminen muille turvallisuusviranomaisille (supo) tai Puolustusvoimille (SotTiedVir) sekä valtion ylimmälle johdolle (molemmat)	Suomen sotilaallinen puolustaminen ja suvereniteetin turvaaminen
Keskeisiä kysymyksiä	Miten teknisesti esitetään jatkossa? Onko muita kohteita? Miten tunnistetaan jatkossa?	Epäilty rikos, sen teko-olosuhteet, sillä aiheutettu vahinko ja siitä saatu hyöty?	Mikä tekijätaho, miten teknisesti estetään jatkossa, mikä vahinko, mikä interssi, mikä merkitys Suomen interssille? Arvio vihamielisen toiminnan jatkosta.	Mikä intressi? Mitkä vaikutukset? Kuinka torjutaan? Tuleeko vaikuttaa toiminnan keskeyttämiseksi? Onko kyseessä alueellinen hyökkäys vai sitä alempitasoinen vaikuttaminen?
Toimenpide; toimija	Tietoturvatoimenpiteet; Päätöksen sisällöstä riippuen Traficom, LVM tai VN	Rikosprosessi; Poliisi, syyttäjä, tuomioistuin	Torjuntatoimenpiteet tai UTP-prosessi; Päätöksen edellyttämä taho	Vastatoimet. Vaikuttaminen aseellisessa hyökkäyksessä. UTP-päätöksenteko ja päätöksenteko sotilaskäskyasioissa.

Kyberympäristö ei ole erillinen toimintaympäristö, jossa erilaiset poikkeamat tapahtuisivat omassa tyhjiössään vaan yhä enenevissä määrin ne ovat osa isompaa kokonaisuutta ja liittyvät fyysisen maailman tapahtumiin. Näin ollen poikkeamahavaintojen lisäksi tarvitaan tietoa muualla tunnistetuista kyberuhkista, orastavista ilmiöistä niin kybertoimintaympäristössä kuin reaalimaailmassa, järjestelmien toiminnasta sekä niiden keskinäisistä suhteista. Jokaisen viranomaisen näkökulma, näkymä ja analyysi ovat tärkeitä kokonaiskuvanmuodostamisessa. (Lehto ym., 2018, 38.) Kansallisen tilannekuvan rakentamisen lisäksi tarvitaan tietoa keskeisiltä kumppaneilta, kuten EU:n ja NATO:n jäsenmaiden vastaavilta viranomaisilta sekä luottamusverkostoilta. Tämä tiedon ja tilannekuvanvaihto kansainvälisten verkostojen kanssa on osa viranomaisten normaalia toimintaa.

3.7 Tiedon luotettavuus

Tiedon luotettavuutta arvioidaan eri kriteerien pohjalta. Tietoa voidaan arvioida lähteen tai itse tiedon tai informaation perusteella. Tieto voi olla totta tai epätotta. Tiedon lähde voi kertoa oikeaa tai virheellistä tietoa. Tietoa voidaan jakaa sähköisiä apuvälineitä hyödyntäen, jolloin halutaan varmistaa tiedon eheys.

Tieto-oppi on yksi filosofian ydinalueista, joka tutkii tietoa ja uskomusten oikeutusta. Lammenrannan (2014) mukaan tieto-opissa on tapana jakaa tieto kolmeen osa-alueeseen. Nämä ovat:

1) Tuttuustieto eli tieto voi kohdistua johonkin objektiin: ”Tiedän Sauli Niinistön” tai ”Tunnen Jyväskylän kaupungin.
2) Propositionaalinen eli väitelauseilla ilmaistava tieto: ”Tiedän, että maapallo on pyöreä.” Propositionaalinen tieto kohdistuu nimensä mukaisesti propositioon. Propositio on jokin sellainen, joka voidaan uskoa ja väittää ja joka voi olla tosi tai epätosi.
3) Viimeinen tiedon laji ilmaistaan englannin kielessä sanoilla ”know how”, joka voitaisiin vapaasti kääntää kuvaamaan taitoa, kykyä tai osaamista eli tietotaitoa: ”Osaan ajaa polkupyörällä”. Taitoa voidaan kuitenkin pitää yhtenä tiedon lajina, toimintaa koskevana tietona.

Tieto-opissa on keskitytty lähinnä propositionaaliseen tietoon. Propositio on jokin sellainen, joka voidaan uskoa ja väittää ja joka voi olla tosi tai epätosi. Propositionaalinen tieto ilmaistaan tyypillisesti muotoa ”S tietää, että p” olevalla lauseella, jossa S edustaa tiedon subjektia ja p propositiota, johon tieto kohdistuu. (Lammenranta, 2014.)

Tieto-opissa erotellaan myös tieto ja informaatio toisistaan. Niinpä tietoa voi olla vain toimijalla, kun taas mikä tahansa kaikkeuden osa sisältää informaatiota: ihmiset, kirjat, internet jne. Sanastokeskuksen ylläpitämä erikoisalojen sanastojen ja sanakirjojen kokoelma (Sanastokeskus, 2023) määrittelee informaatiota seuraavasti:

> ”Jonkin rakenteen tai koodin kantama semanttinen sisältö. Rakenne, jonka oikeanlainen tulkinta tai käsittely antaa tietoa jostakin asiasta. Mitta informaatiokanavan kyvylle välittää koodattua viestiä. Mitta aineellisen systeemin järjestyneisyyden tai organisoituneisuuden asteelle.”

Termillä "informaatio" on paljon erilaisia käyttöjä niin arkiajattelussa kuin tieteellisissä ja filosofisissa kirjoituksissakin. On varsin tavallista, että käsitettä, johon termillä informaatio viitataan ei spesifioida tai vaikka niin tehtäisiinkin, siihen silti liitetään piirteitä toisista käsityksistä (Sanastokeskus, 2023). Tämän määritelmän kautta tiedon tai informaation luotettavuutta voidaan tarkastella myös informaatioteorian kautta. Se on sovelletun matematiikan haara, joka tutkii informaation mittaamista ja siirtämistä erityisesti eri järjestelmien avustuksella.

Informaatioteorian perusajatuksena on tiedonsiirto, jossa haluttu tieto lähetetään informaation lähteeltä jonkun sähköisen tai digitaalisen kanavan kautta vastaanottajalle. Kanavassa, jonka läpi informaatio kulkee, on useimmiten häiriöitä. Keskeistä on myös se, miten vähentää häiriöiden aiheuttamia virheitä, kun vastaanottaja saa tai purkaa tiedon. Informaatioteoria pyrkii selvittämään mahdollisimman lyhyen koodaustavan lähettää informaatiota luotettavasti kanavan läpi. (Gallager, 1970, 6-7.)

Nykyään moni ohje tiedon luotettavuutta arvioitaessa koskettaa nimenomaan oikean tiedon (informaation) tunnistettavuutta ja mahdollisen disinformaation tunnistamista. Ohjeilla pyritäänkin antamaan keinoja, jolla yksilö voi tunnistaa ja arvioida tiedon luotettavuutta. Nämä ohjeet ovat melko yleismaalisia ja pätevät monenlaiseen tietoon, jota nykyään voimme helposti saada käsiimme erilaisten kanavien kuten sosiaalisen median, verkkolehtien ja ylipäänsä internetin avulla. Ohjeina oikean tiedon tunnistamiselle annetaan mm.

1) On tärkeä tunnistaa lähde, josta tai jolta tieto on peräisin.
2) Tiedon ajantasaisuus eli onko kyseessä vanha tieto tai asia vai onko annettu tieto uutta.
3) Tiedon paikkaansa pitävyys. Onko kyseessä mielipide vai fakta? On tärkeä myös selvittää, voidaanko tieto mahdollista vahvistaa tai tarkistaa toisesta lähteestä. (esim. eNorssi-verkkosivu, 2024.)

Disinformaation lisäksi voidaan tunnistaa myös misinformaatio, joka on myös virheellistä tai väärä tietoa, mutta toisin kuin disinformaatio, misinformaatiolla tarkoitetaan vahingossa levitettyä virheellistä tai harhaanjohtavaa tietoa. Misinformaatiota jaetaan joko tietämättömyyttä tai huolimattomuutta. Nykyisessä informaatiotulvassa myös virheitä sattuu ja virheellistä tietoa jaetaan tahattomasti. (esim. Grym 2020, 17.)

Tiedon luotettavuutta voidaan siis lähestyä monesta eri näkökulmasta, niin lähteen luotettavuudesta kuin siirrettävän tiedon eheydestä ja luotettavuudesta. Kybertoimintaympäristössä tapahtuvaan tiedon luotettavuuteen on molemmat lähestymistavat oleellisia, sillä tietoa vaihdetaan useasti verkon kautta ja tieto saatetaan kerätä verkossa olevista jäljistä, mutta toisaalta tieto voi tulla myös toiselta toimijalta, jossa eri henkilöt ovat tietoa keränneet ja se perustuu myös osin ihmisen omaan tuottamaan tietoon ja tuntemukseen, kuten tieto-opissa.

3.7.1 Kyberympäristön tilannekuva ja tiedon luotettavuus

Hibbs Person ja Person (2021, 136-137) tuovat esille teoksessaan Critical thinking for strategic intelligence kybertoimintaympäristön erityispiirteet ja haasteet. Heidän mukaansa hyökkäyksellisen kyberoperaation toteuttajan tunnistaminen, paikantaminen ja tarvittaessa oikeudelliseen vastuuseen saattaminen sekä tiedon arviointi kyberanalyysiä suoritettaessa voi olla erityisen haastavaa. Ensimmäinen askel, jonka he listaavat tehtävässä keskeiseksi on ymmärtää kybertoimintaympäristön konteksti.

Esimerkiksi Yhdysvaltojen kansallisen tiedustelupalvelun johtaja, joka on osa tiedustelupalvelua (Office of the director of national intelligence, jatkossa ODNI, 2018) on kehittänyt kyberuhkaviitekehyksen, joka auttaa asiantuntijaa ymmärtämään kybertoimintaympäristön kontekstia. Mallin tarkoituksena on lisätä tilannekuvatietoa ja parantaa tiedon jakamista ei toimijoiden välillä.

Viitekehys jakautuu neljään kategoriaan, joista ensimmäinen käsittelee tiedon havaitsemista. Valtiollinen toimija pyrkii useasti rakentamaan jalansijaa uhrin verkkoympäristössä huomaamatta ja se saattaa käyttää tähän aikaa jopa vuosia. Tämän takia valtiollisen toimijan kohdentamaa toimintaa kybertoimintaympäristössä voi olla vaikea havaita. Samaan aikaan kyberrikollisuuden määrä kasvaa ja toimijat saattavat hyödyntää menetelmiä myös ristiin. Teko, joka näyttää valtiollisen toimijan käyttämältä menetelmältä voikin olla rikollisjärjestön käyttämä, joka ei liity valtioon millään tavalla. ODNIn tuottamassa materiaalissa yksi ratkaisu tähän on tietojen jakaminen kansallisesti, sillä tieto siiloutuu ja kokonaiskuvan muodostaminen muuttuu haastavaksi. (ODNI, 2018.)

Seuraavaksi kerätystä raa'asta tiedosta tulisi muodostaa tiedustelutietoa liittämällä tietoa toisiinsa ja yhdistelemällä erilaiset yksittäiset tapahtumat toisiinsa. Tätä prosessia kuvattiin jo aikaisemmin kuviossa 1, jossa yksittäisestä tiedosta muodostetaan tilannekuvaa. Haasteen tässä muodostaa jo yllä esitetty tietojen siiloutuminen. Jos tietoa ei jaeta eri organisaatioiden kesken, tieto siiloutuu eli se jää vain tietylle organisaatioille ja kokonaiskuvan rakentaminen hankaloituu.

Kyberuhkatiedustelun ja raportoinnin lisäksi tietoa tulee voida käyttää ja hyödyntää. Organisaatioiden sisäisistä raporteista ei ole hyötyä, jos tietoa ei oteta päätöksenteon tueksi ja hyödyksi tai jos sitä ei jaeta niille yksityisensektorin organisaatioille, jotka tietoa tarvitsevat. Hyvin usein kriittinen infrastruktuuri on yksityisten yritysten omistamaa ja siksi valtion eri toimijoiden on hyvä tehdä näiden yritysten kanssa yhteistyötä sekä jakaa tietoa. (ODNI, 2018.)

Kun kybertoiminnan konteksti on ymmärretty Hibbs Person ja Person (2021, 136-137) nostavat esille attribuution tekemisen eli " hyökkäyksellisen kyberoperaation toteuttajan tunnistamisen, paikantamisen ja tarvittaessa oikeudelliseen vastuuseen saattamisen" (Turvallisuuskomitea, 2018, 27). Attribuutioarvioinnin tulee osoittaa, oliko tapaus yksittäinen tapahtuma, kuka oli todennäköinen tekijä, mikä oli motiivi ja oliko ulkomainen valtio hyökkäyksen takana (Hibbs Person ja Person, 2021, 136-137).

> ”Suomessa ulko- ja turvallisuuspoliittisessa reagoinnissa on kyse vihamielisestä kybertoiminnasta vastuussa olevan tahon – yleensä valtion – tunnistamisesta sekä toimintaan vastaamisesta tai reagoimisesta erilaisin keinoin. Tätä menettelyä kutsutaan attribuutioksi. Attribuutio on tässä mielessä erotettava oikeudellisen vastuun syyksi lukemisesta. Jos valtion elimiä tai sen puolesta toimivia yksityisiä ryhmiä tai henkilöitä voidaan tunnistaa valtion kansainvälisiä velvoitteita loukkaavan kyberoperaation tekijöiksi, valtiolla on niistä kansainvälinen vastuu. Valtion kansainvälisen vastuun syyksi lukeminen tapahtuu vakiintuneiden oikeudellisten kriteereiden mukaisesti.” (Valtioneuvoston julkaisuja, 2023, 18.)

Suomessa viranomaiset ylläpitävät tilannekuvaa ja voivat tekijän tekniikoita, taktiikoita ja prosesseja arvioimalla selvittää mahdollisen tekijän. Kun attribuutioprosessi käynnistetään, on ulkoministeriöllä keskeinen rooli.

Attribuutio-prosesseja on hyvin erilaisia. Nämä ovat useissa tapauksissa ei julkaista tietoa, miten syyksi lukeminen tehdään. ODNI (14.9.2018) on julkaissut oppaan syyksi lukemiseen kybertoimintaympäristössä tapahtuviin hyökkäyksiin. Sen mukaan kyberhyökkäyksen attribuutioon ei ole olemassa yhtä yksinkertaista teknistä prosessia tai automaatioratkaisua. Selvitystyö vaatii viikkojen ja kuukausien tiedusteluanalyysiä sekä teknistä selvittämistä. Hyökkäyksen attribuoiminen tietylle maalle tai toimijalle edellyttää mahdollisimman paljon datan keräämistä, yhteyksien luomista tapahtumien ja toimijoiden välille. Ensisijaisia indikaattoreita ovat toimijan käyttämät tekniset tunnisteet, hyödynnetty infrastruktuuri, haittaohjelma, jota toimija hyödyntää sekä tarkoitus. Näiden lisäksi tulee hyödyntää ulkoisista lähteistä saatavia indikaattoreita, kuten muiden toimijoiden tuottamat raportit.

3.7.2 Amiraalikoodisto (Admiralty code)

Tiedon ja lähteen luotettavuutta voidaan mitata myös erilaisten matriisien tai mittareiden avulla. Tässä työssä pyritään käyttämään pääasiassa nimitystä matriisi. Yksi mahdollisesti vanhimmista ja tunnetummista matriiseista on Admiralty code eli amiraalikoodisto. Sen historia yltää aina toiseen maailmansotaan, jolloin menetelmä kehitettiin Britannian laivastossa. Sen silloinen johtaja havaitsi, että heillä on paljon tietoa ja erilaisia raportteja, mutta niiden sisältöä ei voinut nopeasti saada katsomalla vaan raportti piti lukea alusta loppuun. Siksi kehitettiin menetelmä, jonka avulla tieto voitiin nopeasti luokitella ja havaita raporttien kansilehdistä. (esim. Irwin ja Mandel, 2020.)

Tätä varten suunniteltiin yksinkertainen matriisi, jossa lähde ja itse tieto arvioitiin erikseen koodaamalla arvio kirjaimilla ja numeroilla "A1" - "D5". Kirjain ilmaisee lähteen luotettavuusasteen ja numero todennäköisyyttä, että tieto on oikeaa tai totta. Syynä lähdearvioinnin erottamiseen itse tiedon arvioinnista oli se, että on mahdollista, että arvokasta tietoa voi tulla huonomaineisesta lähteestä ja päinvastoin disinformaatio voi tulla lähteestä, joka on yleensä luotettava. Tätä tietojen luokitusmenetelmää on sittemmin käytetty eri muunnelmina, ja se tunnetaan nimellä "Admiralty System" tai "Admiralty Code". (esim. Irwin ja Mandel, 2020.)

Amiraalikoodisto koostuu kuudesta kategoriasta niin lähteen kuin tiedon luotettavuuden osalta. Kaksi ensimmäistä kategoriaa kuvaavat luotettavaa tai yleensä luotettavaa lähdettä tai täysin uskottavaa tai todennäköisesti totta olevaa tietoa. Kolmas kategoria kuvaa melko luotettavaa lähdettä tai mahdollisesti totta olevaa tietoa. Kategoriat neljä ja viisi kuvaavat ei luotettavaa lähdettä tai epäilyttävää tietoa. Kuudes kategoria on lähteelle tai tiedolle, jota ei voida tunnistaa tai todistaa. Luokittelu on tehty helpoksi ja nopeaksi eikä kategorioita ole liikaa. Taulukoissa 2. ja 3. kuvataan kategoriat lähteen ja tiedon luotettavuuden osalta sekä avataan kategorioiden tarkenteita, jotka pyrkivät lyhyesti avaamaan kategorian sisältöä.

TAULUKKO 2 Amiraalikoodisto, lähteen luotettavuus

Lähteen luotettavuus		Tarkenne
A	Täysin luotettava	Viittaa kokeiltuun ja luotettavaan lähteeseen, johon voi luottaa
B	Yleensä luotettava	Viittaa lähteeseen, joka on menestynyt aiemmin, mutta jonka osalta tietyssä tapauksessa on edelleen epäilyksiä
C	Melko luotettava	Viittaa lähteeseen, jota on satunnaisesti käytetty aiemmin ja johon voidaan perustaa jonkinasteinen luottamus.
D	Ei yleensä luotettava	Viittaa lähteeseen, jota on käytetty aiemmin, mutta joka on usein osoittautunut epäluotettavaksi.
E	Epäluotettava	Viittaa lähteeseen, jota on käytetty aiemmin ja joka on osoittautunut epäluottamuksen arvoiseksi.
F	Luotettavuutta ei voida todistaa	Viittaa lähteeseen, jota ei ole käytetty aiemmin.

TAULUKKO 3 Amiraalikoodisto, tiedon luotettavuus

Tiedon luotettavuus		Tarkenne
1	Täysin uskottava	Viittaa kokeiltuun ja luotettavaan lähteeseen, johon voi luottaa
2	Todennäköisesti totta	Viittaa lähteeseen, joka on menestynyt aiemmin, mutta jonka osalta tietyssä tapauksessa on edelleen epäilyksiä
3	Mahdollisesti totta	Viittaa lähteeseen, jota on satunnaisesti käytetty aiemmin ja johon voidaan perustaa jonkinasteinen luottamus.
4	Epäilyttävä	Viittaa lähteeseen, jota on käytetty aiemmin, mutta joka on usein osoittautunut epäluotettavaksi.
5	Epätodennäköistä	Viittaa lähteeseen, jota on käytetty aiemmin ja joka on osoittautunut epäluottamuksen arvoiseksi.
6	Totuutta ei voida todentaa	Viittaa lähteeseen, jota ei ole käytetty aiemmin.

Ideaalitilanteessa henkilö, joka vastaanottaa tiedon saisi sen siten, että lähteen tieto olisi raportista piilotettuna. Tällöin tietoa voitaisiin käsitellä objektiivisesti eikä tieto lähteestä vaikuttaisi itsessään tiedon arviointiin. Kun tieto on arvioitu ja sijoitettu sopivaan kategoriaan matriisissa katsottaisiin, kuka tiedon on tuottanut eli saataisiin tieto lähteestä.

Amiraalikoodistoa hyödyntävät monet eri viranomaiset eri puolilla maailmaa, sillä kyseinen matriisi on esimerkiksi osa Naton käyttämiä standardeja. Irwin ja Mandel (2020) tuovat esille, että esimerkiksi amiraalikoodistoa käytetään eri tavoin eri maissa ja siellä tiedusteluviranomaiset saattavat antaa hyvin eri arvoja samanlaisissa tilanteissa, koska ohjeistus on erilainen. Näin ollen jaettaessa tietoa eri maiden viranomaisten välillä, on mahdollista, että annettu arvo lähteen tai tiedon luotettavuudesta vaihtelee, jos luokittelutieto myös jaetaan.

Koska käytännöt eroavat eri maissa eikä ohjeistus ole yhtenäistä, on mahdollista, että päädytään myös niin kutsuttuun vahvistusharhaan. Vahvistusharhalla tarkoitetaan sitä, että tietoa käsitellään jo olemassa olevan tiedon valossa, joka sopii omaan maailmankatsomukseen. Ilmiön toinen puoli on se, että ihminen myös hylkii tietoa, joka sotii tätä maailmankuvaa vastaan. (Interactive Terminology for Europe, 2019.) Esimerkiksi kaksi saman maan viranomaista voivat saada kansainvälisistä lähteistään saman tiedon, jonka ne luokittelevat eri tavalla. Jakaessaan tietoa toisilleen saatetaan päätyä virheellisesti käsitykseen, jossa saatuja tietoja pidetään kahtena eri tietona ja näin ne vahvistavat toisiaan sen sijaan, että tunnistettaisiin kyseessä olevan kahden tiedon sijaan yksi tieto. Mikäli kyseessä olisi merkittävä tieto, joka vaikuttaa maan turvallisuuteen, voisi tästä alkaa laajat toimenpiteet, joiden vaikutukset voidaan arvioida vasta myöhemmin. Näihin toimenpiteisiin on kuitenkin ryhdytty virheellisen tiedon valossa, sillä viranomaisten tuottamaa tietoa ei ole tunnistettu samaksi, vaan niihin on vaikuttanut vahvistusharha ja saatua tietoa on tulkittu toisiaan tukevaksi.

3.7.3 4x4-matriisi

Europolin tiedonhallintamalli kuvaa tiedonkulkua Europolin tasolla. Yhteistyössä jäsenvaltioiden kanssa kehitetty ja Europolin kansallisten yksiköiden päälliköiden hyväksymänä malli määrittelee Europolin ja sen kumppaneiden välisen tiedonkäsittelyn ja -vaihdon käytännön toiminnan. Se varmistaa myös tiukkojen tietoturvamääräysten noudattamisen. Tiedon arviointi perustuu 4x4-matriisiin, jota jäsenvaltioissa käytetään toimitettujen tietojen aitouden ja tarkkuuden määrittämiseksi. Arviointikoodit koostuvat lähteestä ja saadusta tiedosta. 4x4-matriisin käyttö sisältyy analyysimääräyksiin sekä Europolin kolmansien osapuolten kanssa tekemiin operatiivisiin sopimuksiin. (Europol, 2009.)

4x4-matriisia hyödyntävät eri maiden poliisiviranomaiset myös kansallisesti sekä muut virastot ja kansainväliset järjestöt kuten Yhdistyneet kansakunnat. Monet näistä käyttävät tämän matriisin muunnelmia, mutta jokainen on helposti tulkittavissa selittävien taulukoiden avulla, ja tarvittaessa tiedot voidaan muuntaa matriisista toiseen. Yhdistyneiden kansakuntien huumeiden ja rikollisuuden torjunnasta vastaava toimisto (United Nations Office on Drugs and Crime, jatkossa UNODC, 2011, 25-26) on tuottanut rikostiedusteluanalyytikolle

oppaan, jossa yksi lähteen ja tiedon luotettavuuden mittareista on 4x4-matriisi. Oppaassa tuodaan esille, että 4 x 4 matriisi perustuu yksinkertaiseen henkilökohtaiseen tietoon. Näin ollen tiedolla on alhaisempi arvo. Tällä yksinkertaisuudella on arvo sinänsä, koska arvioinnista tulee vähemmän subjektiivinen.

Oppaan mukaan arviointiin sovelletaan kolmea perusperiaatetta: 1. Henkilökohtaiset tunteet eivät saa vaikuttaa arviointiin, vaan sen tulee perustua ammatilliseen harkintaan. 2. Lähteen arviointi tulee tehdä tiedoista erikseen. 3. Arviointi on suoritettava mahdollisimman lähellä lähdettä. (UNODC, 2011, 25.) Toinen kohta on keskeinen, joka nostettiin esille amiraalikoodiston esittelyssä erityisesti tiedon luotettavuuden arvioinnissa. Tiedon luotettavuus voidaan pitää objektiivisempana, kun tietoa lähteestä ei ole nähtävillä.

4x4-matriisi koostuu nimensä mukaisesti neljästä kategoriasta, joilla tiedon ja lähteen luotettavuutta voidaan ilmasta. Taulukossa 4. on avattu 4x4-matriisia tarkemmin. Mikäli lähde on tunnettu tai sen antamista tiedoista ei ole epäilystä ja saadut tiedot ovat oikeellisia, pidetään tietoa luotettavana. Kaikki muu sijoittuu epäluotettavamman tiedon kategoriaan, joka vaatii lisäselvitystä tai tietoa muista lähteistä. Myös 4x4-matriisissa on amiraalikoodistoa vastaava luokka tiedolle ja lähteelle, jonka luotettavuutta ja oikeellisuuta ei voida arvioida.

TAULUKKO 4 4x4-matriisi

	Lähteen luotettavuuden arviointi					
Saadun tiedon / informaation luotettavuuden arviointi			A	B	C	X
		Tarkenne	Jos lähteen aitoudesta, luotettavuudesta ja pätevyydestä ei ole epäilystäkään tai jos tiedot on toimittanut lähde, joka on aiemmin osoittautunut luotettavaksi kaikissa tapauksissa	Lähde, jolta tiedot on saatu, on useimmissa tapauksissa osoittautunut luotettavaksi;	Lähde, jolta tiedot on saatu, on useimmissa tapauksissa osoittautunut epäluotettavaksi;	Lähteen luotettavuutta ei voida arvioida.
	1	Tiedot, joiden oikeellisuudesta ei ole epäilystäkään;				
	2	Lähteen henkilökohtaisesti tiedossa, mutta ei tiedossa henkilökohtaisesti sen välittäjälle;				
	3	Tiedot, jotka eivät ole lähteen henkilökohtaisesti tiedossa, mutta joita muut jo tallennetut tiedot tukevat;				
	4	Tiedot, jotka eivät ole lähteen henkilökohtaisesti tiedossa ja joita ei voida vahvistaa.				

3.7.4 Yhteenveto amiraalikoodista ja 4x4-matriisista

Molemmista matriiseista on saatavilla tietoa hyvin, sillä amiraalikoodisto on pitkään ollut käytössä ja sitä hyödynnetään tänäkin päivänä. Amiraalikoodistoa hyödyntävät erityisesti eri maiden puolustusvoimat. 4x4-matriisi on poliisiviranomaisten käytössä niin kansallisesti kuin kansainvälisessä tiedonvaihdossa. Esiteltyjen matriisien käyttäjät ovat siis todennäköisesti puolustusvoimien tai poliisien edustajia. Suomen kyberturvallisuusviranomaisiin verratessa tästä puuttuu Kyberturvallisuusviranomaiset, kuten CERT-toimijat (computer emergency repsonce teams), joita on esimerkiksi jokaisella EU-maalla. Julkisten lähteiden perusteella CERT-toimijat eivät yhteisesti hyödynnä amiraalikoodistoa tai 4x4-matriisia omassa tiedonvaihdossaan. Eikä niillä ole julkisten lähteiden mukaan käytössä muunlaista vastaavaa matriisia, jota voisi sovittaa lähteen ja tiedon luotettavuuden mittaamiseen. (esim. ENISA, 2016.)

Amiraalikoodisto ja 4x4-matriisi on sovitettavissa melko hyvin yhteen, sillä molemmat matriisit arvioivat tiedon luotettavuutta lähteen ja tiedon perusteella. Amiraalikoodistossa on kuusi kategoriaa lähteen ja tiedon luotettavuudelle, kun taas 4x4-matriisissa on nimensä mukaisesti neljä kategoriaa lähteen ja tiedon arvioimiseksi. Tämän takia matriisien yhteensovittamiseksi on tehtävä hieman tulkintaa, jotta ne voidaan sovittaa yhteen ja löytää vastaavuudet eri luotettavuuskategoriassa.

Taulukossa 5 on yhdistetty amiraalikoodisto ja 4x4-matriisi yhdeksi, jotta niitä voidaan helpommin verrata toisiinsa ja löytää kategoriat, jotka vertautuvat toisiinsa, vaikka niissä on eri määrä lähdettä ja tietoa luokittavia kategorioita. Luotettavan tiedon ja lähteen osalta mallit ovat yhteneväiset ja luotettava tai melko luotettava lähde ja tieto osuvat samantyylisen määritelmän sisälle. Näin ollen luotettava lähde sijoittuu taulukossa 5 arvoille A/A-B/B ja luotettava tieto/informaatio arvoille 1/1-2/2. Myös molemmissa malleissa on selkäesti esitetty epäluotettavan tai vahvistamattoman tiedon käsittely ja luokittelu. Tämä sijoittuu taulukossa lähteen osalta kategoriaan F/X ja tiedon osalta 6/4 kategoriaan. Ei täysin luotettavan tiedon osalta tulkinta oli haastavampaa. Lopputulemana kuitenkin oli sijoittelu siten, että tiedon osalta ei luotettava lähde sijoitettaisiin kategoriaan E/C ja tieto kategoriaan 5/3. Tämä perustui sille, että kyseessä on molempien matriisien viimeinen kategoria epäluotettavalle tiedolle ennen tietoa ja lähdettä, jota ei voida arvioida.

Molemmat mallit hyödyntävät erityisesti henkilötiedusteluun perustuvia mittareita ja tämä näkyy myös niiden tarkenteissa, joita julkisesti on saatavilla. Kybertiedonvaihdon kannalta määritelmissä tulisi huomioida tekninen ympäristö paremmin, sekä kyberkyvykkyydet, jotta näitä voitaisiin paremmin soveltaa kybertoimintaympäristössä tapahtuvaan lähteen ja tiedon luotettavuuden määrittelyyn.

TAULUKKO 5 Amiraalikoodiston ja 4x4-matriisi yhteensovitettuna

	Lähteen luotettavuuden arviointi (Amiraalikoodisto / 4x4)						
Saadun tiedon / informaation luotettavuuden arviointi (Amiraalikoodisto / 4x4)		A/A	B/B	C	D	E/C	F/X
	1 / 1						
	2 / 2						
	3						
	4						
	5/3						
	6						

3.8 Muut matriisit ja työkalut

Amiraalikoodiston ja 4x4-matriisin lisäksi voidaan hyödyntää myös muunlaisia matriiseja. Toisaalta nämä matriisit voidaan nähdä erilaisina tulkintoina jo aikaisemmin esitetyistä matriiseista. Jokainen toimija soveltaa matriisia omaan käyttötarkoitukseensa ja tekee siitä oman näköisensä. On esimerkiksi mahdollista, että pohjalla on amiraalikoodisto ja sitä on täydennetty omalla erillisellä sarakkeella tai osa-alueella, joka huomioi sen toimintakentän, jossa viranomainen työskentelee. (Hibbs Person ja Person, 2021, 127-132.)

Esimerkiksi Iso-Britannian poliisi hyödyntää lähteen ja tiedon luotettavuuden matriisina niin kutsuttua 5x5x5-matriisia, jossa on viisi kategoriaa, joiden välillä lähteen ja tiedon luotettavuutta arvioidaan (College of policing, 2005). Perusidealtaan se noudattelee amiraalikoodiston ja 4x4-matriisin mallia. Erona on kategorioiden määrä, joita nimen mukaisesti on viisi.

Iso-Britannian poliisi on antanut erilliset ohjeet, miten matriisia tulisi käyttää ja millä tavalla tietoon tai raporttiin lisätään erilaiset tunnistetiedot. Lähteen luotettavuudella tarkoitetaan tiedon antanutta henkilöä, organisaatiota tai tekniselle laitteelle annettua arviota. Lähteen luotettavuuden arvioi aluksi tiedon tallentava henkilö, ja se tulee täydentää kaikissa olosuhteissa. Lähteen arviointi ei ole staattinen prosessi, ja sitä tulisi tarkistaa jatkuvasti. Tämä vaikuttaa koko tiedonhallintaprosessiin, erityisesti tiedon jakamiseen ja sen säilyttämisen tarpeeseen. Lähteen arvioinnin tulee mahdollisuuksien mukaan perustua objektiiviseen lähteen tuntemiseen, sillä se vaikuttaa sekä tallennetun tiedon arviointiin että mahdollisiin tietoihin perustuviin toimenpiteisiin. (College of policing, 2005.) Tässäkin viittaus tuntuu olevan vahvasti henkilötiedustelussa, sillä tiedon vastaanottanut taho tuntee lähteen. Mikäli koko organisaatio arvioisi sille keskeisiä lähteitä, ei lähteen arviointi olisi niin vahvasti sidoksissa tiedon vastaanottajaan tai henkilöön, jolle lähde on tuttu, vaan organisaatio tekisi lähteistä säännöllistä listausta ja tarkastelisi niiden luottamushistoriaa.

5x5x5-matriisin käyttö vaikuttaa nopealle ja helpolle tiedon vastaanottajan näkökulmasta. Taulukoissa 6 ja 7 avataan matriisin kategorioita tiedon ja lähteen luotettavuuden osalta. Matriisin eri kategoriat ovat helposti toistensa kanssa vertailtavia ja lähde tai tieto saa pisteitä, joiden perusteella se asetetaan annetulle asteikolle. Tietoa ja lähdettä käsitellään esimerkkiohjeen mukaan yhdessä, jolloin tietoa saatetaan käsitellä puolueellisesti, koska se tulee hyvästä lähteestä. Mikäli tieto käsiteltäisiin ilman tietoa lähteestä, se saatettaisiin tulkita hyvin eri tavalla.

Erona kahteen aikaisempaan matriisiin on pisteytys. 5x5x5-matriisi sisältää viisi kategoriaa, joita arvioidaan viiden kriteerin avulla. Mikäli kaikki nämä kriteerit täyttyvät tulkitaan lähdettä kaikista luotettavimmaksi ja tietoa vahvistetuksi. Kriteereissä on myös painotus. Historiatieto eli se, että lähde on tunnettu ja se on tuottanut aikaisemmin luotettavaa tietoa, saa erillisen painoarvon. Tätä avataan tarkemmin taulukossa 6, jossa lähteen luotettavuusmatriisi on esitelty. Erona edellisiin taulukoihin on myös se, että 5x5x5-matriisissa ei ole kategoriaa,

jossa tietoa tai lähdettä ei kyetä arvioimaan kuten Amiraalikoodistossa sekä 4x4-matriisissa on.

TAULUKKO 6 5x5x5-matriisin lähteen luotettavuus

Lähteen luotettavuus		1. Luotettavuuden historia	2. Lähteen aitous / hyvä tahto	3. Lähteen objektiivisuus	4. Lähteen pääsy tietoihin	5 Lähde ei ole alttiina manipuloinnille	Täyttää kriteerit (1-5)
A	Luotettava	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kaikki 5
B	Useasti luotettava	Kyllä	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Historia + 3
C	Melko luotettava	Kyllä	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Historia + 2
D	Epäluotettava	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	2/5
E	Ei tunnettu	Ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Ei saatavilla

TAULUKKO 7 5x5x5-matriisin tiedon luotettavuus

Tiedon luotettavuus		1. Riippumattomilla todennettavissa olevilla keinoilla	2. Lähdeainekompetenssi	3. Looginen	4. Käytännöllinen ja uskottava	5. Johdonmukaisuus	Täyttää kriteerit (1-5)
1	Tiedot, joiden oikeellisuudesta ei ole epäilystäkään;	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kaikki 5
2	Lähteen henkilökohtaisesti tiedossa, mutta ei tiedossa henkilökohtaisesti sen välittäjälle;	Ei	Kyllä	Kyllä	Kyllä	Kyllä	4
3	Tiedot, jotka eivät ole lähteen henkilökohtaisesti tiedossa, mutta joita muut jo tallennetut tiedot tukevat;	Ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	3
4	Ei voida arvioida	Ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	2
5	Epäilys ei todenmukaisesta tiedosta	Ei	Kyllä tai ei	Kyllä tai ei	Kyllä tai ei	Ei	0-1

Amiraalikoodiston kanssa hyvin samankaltainen matriisi on esimerkiksi Forum of Incident Response and Security Teams (jatkossa First, 2023) suosittelema lähteen ja tiedon luotettavuuden arviointipohja. Kuten amiraalikoodistossa, myös tässä matriisissa on kuusi kategoriaa, joiden kautta tiedon ja lähteen luotettavuutta arvioidaan. Se ei välttämättä ole täysin erillinen amiraalikoodistosta vaan mahdollisesti vain yksi sen tulkinnoista. First viittaa suosittamansa mallin olevan Yhdysvaltojen armeijan käyttämä malli, joka löytyy esimerkiksi henkilötiedustelua, keräystä ja operaatioita käsittelevästä ohjekirjasta. (Department of the Army, 2006.) Tämän mallin mukaan lähteet luokitellaan luotettavuuden alenevassa järjestyksessä "A":sta "E:ksi", jossa "F" on tarkoitettu tapaukseen, jossa lähteen luotettavuutta ei voida määritellä. Tieto puolestaan luokitellaan laskevassa järjestyksessä "1":stä "5:een", jossa "6" on varattu tapaukselle, jossa tiedon luotettavuutta ei pystytä varmistamaan. Lähteen ja tiedon luotettavuuden kategoriat on kuvattu taulukoissa 8 ja 9. verrattaessa taulukoita aikaisemmin esitettyyn

amiraalikoodistoon (taulukot 2 ja 3), voidaan havaita, että kirjain ja numeerinen koodi sekä luotettavuuden selite ovat yhtenäiset. Kategorioiden tarkennuksissa on hieman eroja, mutta perusajatus niissä on samanlainen.

Firstin (2023) sivuilla annetaan lyhyesti myös kaksi esimerkkiä, miten matriisia voitaisiin hyödyntää ja tulkita kybertoimintaympäristössä. Ensimmäisen esimerkin mukaan kyseessä voisi olla kyberuhkatietoa tarjoava palveluntarjoaja, jolla on hyvin luotettavia syötteitä. Kyseinen palveluntarjoaja ottaa käyttöön uutta kokeellista syötettä. Aluksi tämä syöte voidaan luokitella "A3" eli lähde on melko luotettava ja sen jakama tieto mahdollisesti totta Tämä tulkinta tehdään, koska lähde itsessään on tunnettu, mutta datasyöte on uusi eikä se vielä tunnista kaikkia havaintoja toivotulla tavalla.

Toinen esimerkki olisi erilaisilta keskustelualustoilta kerätty tieto. Tällaisella alustalla voisi olla esimerkiksi valkohattuhakkeri eli niin sanottu eettisesti toimiva henkilö, joka on suurimmaksi osaksi antanut hyvää tietoa, mutta tietyissä tapauksissa hänen tietonsa ei sovi yhteen tai on ristiriidassa muun tiedon kanssa, joka voidaan useista lähteistä, voidaan arvioida. Näin ollen tämä lähde ja hänen tietonsa saisivat arvon "B4" eli lähdettä pidetään yleensä luotettavana, mutta jaetun tiedon osalta on epäilyksiä.

TAULUKKO 8 First lähteen luotettavuuden arviointi

Lähteen luotettavuus		Tarkenne
A	Luotettava	Ei epäilystäkään lähteen aitoudesta, luotettavuudesta tai pätevyydestä. Täydellisen luotettavuuden historia.
B	Yleensä luotettava	Pieniä epäilyksiä. Pääosin hyvä luotettavuuden historia.
C	Melko luotettava	Epäilykset. Toimitettu päteviä tietoja aiemmin.
D	Ei yleensä luotettava	Merkittäviä epäilyksiä. Toimitettu päteviä tietoja aiemmin.
E	Epäluotettava	Puuttuu aitous, luotettavuus ja pätevyys. Virheellisten tietojen historia.
F	Luotettavuutta ei voida todistaa	Riittämätön tieto luotettavuuden arvioimiseksi. Voi olla tai ei ole luotettava.

TAULUKKO 9 First tiedon luotettavuuden arviointi

Tiedon luotettavuus		Tarkenne
1	Täysin uskottava	Looginen, yhdenmukainen muiden asiaankuuluvien tietojen kanssa, riippumattomien lähteiden vahvistama.
2	Todennäköisesti totta	Looginen, yhdenmukainen muiden olennaisten tietojen kanssa, ei vahvistettu.
3	Mahdollisesti totta	Kohtuullisen loogista, samaa mieltä joidenkin olennaisten tietojen kanssa, ei vahvistettu.
4	Epäilyttävä	Ei loogista mutta mahdollista, ei muuta tietoa aiheesta, ei vahvistettu.
5	Epätodennäköistä	Ei loogista, mikä on ristiriidassa muun asiaankuuluvan tiedon kanssa.
6	Totuutta ei voida todentaa	Tietojen oikeellisuutta ei voida määrittää.

Vaikka tiedon luotettavuuden mittareita on hyödynnetty tiedustelussa ja eri toimijat hyödyntävät omia mallejaan, ei näitä yleisesti käytetä vastaavalla tavalla kybertoimintaympäristössä tapahtuvassa tiedonvaihdossa. Tällä hetkellä kybertoimintaympäristössä esimerkiksi MISP (Malware Information Sharing Platform) työkalulla, jossa voi jakaa haittaohjelmatietoa, voitaisiin halutessa hyödyntää amiraliteettikoodistoa, jonka avulla tiedon jakava taho voisi merkitä tiedon luotettavuuden, mutta avoimena saatavana olevissa MISPeissä tätä tiedon luotettavuuden matriisia hyödynnetään vähän. (MISP, 2015)

4 DELFOI-METODI APUNA TURVALLISUUSKYSYMYKSEN HAHMOTTAMISEEN

Tutkimuksen menetelmäksi valikoitui kvalitatiivinen eli laadullinen lähestyminen tutkittavaan aiheeseen. Kvalitatiivisessa tutkimuksessa ja tässä työssä on pyrkimyksenä löytää uusia näkökulmia kuin todentaa jo olemassa olevia väittämiä. Kvalitatiiviselle tutkimukselle tyypillisiä piirteitä ovat muun muassa se, että ihmistä suositaan tiedon keruun instrumenttina. Työn aineisto tulee koostumaan haastatteluista ja verkkosovelluksen avulla tehdyistä Delfoi-kyselyistä, joihin asiantuntijat vastaavat. Työn tarkoituksena ei myöskään ole testata valmista teoriaa tai hypoteesia eli työssä käytetään induktiivista analyysiä. Keskiössä tulee olemaan kerätty aineisto ja sen monitahoinen ja yksityiskohtainen tarkastelu. Aineiston avulla tavoitteena on saada asiantuntijoiden ääni kuulumaan, sillä he ovat keskeisessä roolissa lopputuotteen kannalta. Kohdejoukko on valikoitu työtä varten eikä otettu satunnaisotantaa, joka on kvalitatiiviselle tutkimukselle myös tyypillinen piirre. (Hirsjärvi, Remes ja Sajavaara, 1997, 161-164.)

Kvalitatiivisen tutkimuksen lajeja on useita. Haastattelu on yksi käytetyimmistä tiedonhankkimisen menetelmistä. Kysymistä pidetään ensisijaisena ratkaisuna tiedon puutteeseen. Oletus on, että kysyvälle vastataan. (Tiittula ja Ruusuvuori 2005, 9.) Haastattelua voidaan toteuttaa monin eri tavoin. Voidaan hyödyntää asiantuntijahaastattelua, joka on tämän työn keskiössä. Haastattelutapoina ovat sekä verkkosovelluksen kautta toteutettava Delfoi-kysely, että puolistrukturoituhaastattelu, jossa tutkija ja haastateltava ovat samassa tilassa ja kysymyksiin vastataan reaaliajassa. (esim. Alastalo, 2005, 59-60.)

Delfoi on menetelmä, jossa ryhmäkommunikoinnin kautta jokainen ryhmän jäsen yksilönä jäsentää yhteistä monimutkaista ongelmaa (Linstone ja Turoff, 1975, 3). Delfoi-menetelmässä toteutuu kolmen a:n sääntö, joka tarkoittaa, että asiantuntijat argumentoivat anonyymisti. Tunnusomaista Delfoille on juuri anonymiteetti, jolla tavoitellaan sitä, että asiantuntijat esittävät aitoja mielipiteitään ja käsityksiään asiasta, jota tutkitaan. Anonymiteetti takaa sen, että asiantuntijan ei tarvitse pelätä ns. kasvojen menetystä. Haastateltava asiantuntija, voi esimerkiksi olla työnsä puolesta asemassa, jossa hänen omat ajatuksensa ovat

eriäviä yrityksen päälinjan kanssa, eikä hän saa esittää eriäviä mielipiteitä asemansa vuoksi. (Kuusi, 1999.)

Delfoi-menetelmän avulla voidaan selvittää mielipiteitä ja tarkemmin asiantuntijamielipiteitä. Delfoi-menetelmä voi olla samankaltaista kuin yhdessä pohtiminen eli aivoriihityöskentely. Erona tässä on kuitenkin se, että yhteisön paine ei ole niin selkeä, koska jokainen pohtii asiaa omalla tahollaan ja jakaa sen yhteisön kanssa. (Hellsten, 1974, 2-3.) Delfoissa rajoitetaan ilmaisu- ja kuunteluraajoitteita, joita ryhmähaastattelussa voi olla, koska vastaajat ovat samassa tilassa. Delfoissa vahvat keskustelijat eivät nouse esille, ja omilla mielipiteillään vaikuta toisten mielipiteisiin. Survey-metodeista Delfoin erottaa sen palauteosuus, jossa asiantuntijat voivat puntaroida antamiaan vastauksia ja osallistua niistä tehtyihin tulkintoihin. (Linturi, 2007.)

Delfoi-prosessissa saatetaan avoimen asiantuntijatestin ja argumentaation kohteeksi esimerkiksi väitteitä tai näkökulmia. Prosessissa pyritään seulomaan asiantuntijoiden antamat näkemykset jaetuiksi tai erimielisiksi yhteisönäkemyksiksi, joista molemmat lopputulokset ovat arvokkaita. (Linturi, Linturi ja Jauhiainen, 2019.) Tämä tulee olemaan yksi keskeinen osa-alue tässä tutkimuksessa, sillä asiantuntijapaneeli arvioi ja antaa oman näkemyksensä nk. Suomen-mallin kybertiedonvaihdon luotettavuuden määritelmiin niin lähteen kuin tiedon osalta.

Konsensus eli klassinen-Delfoi ja politiikka-Delfoi edustavat kahta pääsuu tausta. Delfoi-menetelmässä Klassinen-Delfoi perustuu siihen, että paneelin keskuudessa saavutetaan yksimielisyys esitettyyn kysymykseen tai kokonaiseen teemaan. Lisäksi voidaan pyrkiä saavuttamaan täsmäennustus tai poikkeavuusperustelu. Poikkeuksena perinteiseen ryhmähaastatteluun tai keskusteluun, jossa yhteinen mielipide pyritään löytämään, on, ettei Delfoissa hyödynnetä yhteiskeskustelua. Yhteinen mielipide pyritään löytämään haastattelukierrosten avulla, ja niistä annetaan palaute, jota panelistit saavat kommentoida. Näin myös vältetään vahvojen persoonien vaikutus tulokseen ja heikommat sekä mahdollisesti ujot panelistit saavat äänensä kuuluviin. (Linturi, 2024.)

Politiikka Delfoi pyrkii tuottamaan erilaisia väitteitä ja argumentteja. Ei riitä, että erilaiset mielipiteet, argumentit ja näkemykset kootaan, vaan niiden tulee myös muodostaa dialogi keskenään. Tässä menetelmässä yhteisöllä on hyvä

oppimismahdollisuus. (Linturi, 2024.) Politiikka Delfoilla pyritään löytämään mahdollisimman monta eri näkökulmaa, jotka ovat perusteltuja. Näin ratkaisuntekeminen aiheesta voi olla esimerkiksi päätöksenteossa helpompaa. PolitiikkaDelfoissa ei ole vain asiantuntijoita vaan asian edustajia ja suosittelijoita. (Linstone&Turoff 1975, 84.)

Argumentoiva Delfoi on yksi politiikka Delfoin alalaji. Osmo Kuusi (1999.) on erotellut tämän omaksi variaatiokseen. Argumentoivalle Delfoille on tyypillistä osallistujien argumentointi keskenään. Tällöin ei etsitä todennäköisyyttä ja toivottavuutta, kuten politiikka Delfoissa. Aiheeseen haetaan eri variaatioita yksimielisyyden sijaan, joka on ollut konsensus Delfoissa tärkeää.

Delfoista voidaan löytää useita eri variaatioita. Eri malleja hyödynnetään tutkimuskohteen mukaan. Tässä työssä on havaittavissa piirteitä klassisesta Delfoista, koska tavoitteena oli löytää yksimielisyys määriteltäessä lähteen ja tiedon

luotettavuuden matriisia ja siihen liittyviä kategorioiden tarkempia kuvauksia. Toisaalta työssä on myös argumentoivan Delfoin piirteitä, koska moni kysymys oli avoin ja niissä haettiin nimenomaan erilaisia näkökulmia, jotta varsinainen matriisi voitiin rakentaa.

Delfoi-prosessin voi jakaa kolmeen osa-alueeseen. Ensimmäinen osa-alue muodostuu haastattelusta, jossa asiantuntijat herätellään vastaamaan kysymyksiin. Ensimmäinen tieto on luonteeltaan eksperttitietoa, jossa tuorein tieto välittyy asiantuntijoiden kautta, koska se ei ole välittynyt vielä kirjojen kansiin. Samalla voidaan vielä tehdä valintoja asiantuntijapanelistien suhteen. (Linturi, 2019.)

Toisessa vaiheessa ensimmäisen kierroksen vastaukset analysoidaan ja tehdään näistä kysymyksiä sekä tarkentavia lisäkysymyksiä tai väittämiä asiantuntijoille. Toisesta kierroksesta voidaan käyttää nimitystä systeemitieto. Systeemisyyskäsite on luotu kuvaamaan ilmiön eri osien välisiä dynaamisia ja monen suuntaisia suhteita. (Linturi ym., 2019.)

Kolmannessa vaiheessa analysointi jatkuu ja annettuja vastauksia voi tarkentaa sekä nostaa esille uusia kysymyksiä. Parhaimmillaan erilaisen tiedon saattaminen yhteen muodostaa näkemystiedon syntymisen. Tätä tietoa kenelläkään ei ollut tutkimuksen alkuvaiheessa, vaan tieto on muodostunut asiantuntijoiden argumenttien ja yhteisen pohdinnan tuloksena. Delfoi-kierroksia voidaan jatkaa niin pitkään kuin katsotaan tutkimuksen osalta olevan tarpeellista. Yleensä kierroksia on kolmesta viiteen. (Linturi ym., 2019.) Kyselykierrokset tulisi viedä mahdollisimman nopeasti läpi, kuitenkin siten, että panelisteilla on aikaa lukea edellisen kierrosten tulokset ja vastata seuraavaan kierroksen kysymyksiin. Kyselyn pitkittyessä tai vastausvälin ollessa liian pitkä vastaajien mielenkiinto saattaa laimentua ja näin vastausten saaminen saattaa jäädä kokonaan saamatta (Hellsten, 1974, 14).

Delfoi-managerin rooli on erityinen, jonka toimenkuva poikkeaa esimerkiksi survey-kyselyllä aineostoa keräävästä tutkijasta. Managerin rooli on tutkijaa aktiivisempi suhteessa sekä tutkimusprosessiin että tietolähteisiin. Managerin rooli on aktiivinen koko delfoi-prosessin ajan ja hänen on tärkeä tietää, mitä tulee tietää ja tehdä. Managerin erityinen taito on saada paneeli soittamaan ja soimaan yhdessä. Työssä tämä näkyy aktiivisena yhteydenpitona panelisteihin sekä jatkuva palautteen analysointi ja synteesi sekä uusien kommenttien kerääminen. (Linturi ym., 2019.)

Yhtä tärkeitä ovat kyselyyn osallistuvat panelistit. Asiantuntijoiden valinta paneeliin on keskeinen ja tärkeä osa Delfoi-tekniikkaa. Tulokset riippuvat paljon siitä, minkälainen paneeli tutkimusta varten kootaan. Paneelin koko vaihtelee tutkimuksen mukaan pienryhmästä tuhansiin vastaajiin. Osmo Kuusi (1999.) on nimennyt viisi seikkaa, jotka tulee huomioida asiantuntijoita valitessa:

1) asiantuntija on oman tiedonalansa kärjessä,
2) asiantuntija on kiinnostunut myös muista tiedonaloista,
3) asiantuntija pystyy näkemään yhteyksiä kansallisen ja kansainvälisen, nykyisen ja tulevan kehityksen välillä,

4) asiantuntija kykenee tarkastelemaan ongelmia myös epätavanomaisesta näkökulmasta ja
5) asiantuntija on kiinnostunut tekemään jotain uutta. Delfoi-raatiin olisi hyvä saada erilaisia asiantuntijoita, jotta tulokset ovat varsin kattavat ja aihetta voidaan tarkastella mahdollisimman monipuolisesti eri tulokulmista.

Delfoi-menetelmä mielletään helposti tulevaisuuden tutkimukseen, jota varten menetelmä on aluksi kehitetty. Myöhemmin on voitu havaita eri tutkimusten kautta, että sillä voidaan tutkia monia sellaisiakin ilmiöitä ja asioita, jotka eivät ole vielä vakiintuneet tai menetelmä voi olla keino jonkun olemassa olevan tilanteen selvittämiseen. Valtonen (2010.) on osoittanut tutkimuksellaan, että Delfoi on erinomainen menetelmä erilaisiin turvallisuustutkimuksiin. Anonymiteetti takaa asiantuntijan mahdollisuuden argumentoida arkaankin aiheeseen, ilman, että oma asema hankaloituu esimerkiksi työyhteisössä. Vaikka työssä käytetään Delfoi-menetelmää, ei sen tavoite ole tulevaisuusorientoitunut vaan jäsentymättömässä asiassa yhteisen konsensuksen löytäminen lähteen ja tiedon luotettavuuden osalta.

5 TUTKIMUKSEN TOTEUTUS JA TULOKSET

Tutkimusta varten kerättiin asiantuntijapaneeli. Kutsu paneeliin osallistumiselle lähetettiin helmikuussa 2024. Paneeliin kutsuttiin 14 osallistujaa. Näistä kutsutuista yhdeksän osallistui paneeliin. Panelistit osallistuivat yksityishenkilönä kyselyyn, mutta heidät valittiin sen perusteella, että he työskentelevät tai ovat työskennelleet kyberteemojen ääressä sekä heillä on työkokemusta sellaisilta hallinnonaloilta, joille matriisin käyttö on ensisijaisesti suunnattu. Näin ollen panelistit valikoituivat puolustushallinnon, sisäisen turvallisuuden, ulkoasianhallinnon sekä liikenne- ja viestintäministeriön hallinnonaloilta.

Kyselyssä oli vain yksi taustakysymys, joka liittyi juuri panelistin taustaan. Tämän kysymyksen avulla pyrittiin hahmottamaan sitä, minkälaista kokemusta vastaajalla on ja miten hänen vastauksensa rakentuu. Taustakysymyksen avulla kävi ilmi, että vastaajat edustivat kaikkia toivottuja hallinnonaloja. Tämän lisäksi esitettiin mahdollisuus valita, mitä eri tilannekuvan tasoja vastaaja edustaa. Saatujen vastausten perusteella suurin joukko vastaajista edusti erityisesti operatiivista tasoa. Strategiselta, taktiselta ja tekniseltä tasoilta löytyi myös taustaosaamista, joten jokainen tilannekuvan taso oli edustettuna. Kysymys oli aseteltu siten, että vastaaja saattoi valita useamman eri hallinnonalan sekä tason, jolla toimii tai on aikaisemmin toiminut, sillä panelisti ja hänen hankkimansa osaaminen ja ymmärrys aiheesta haluttiin nähdä kokonaisuutena.

Panelistit saivat osana kutsuviestiä (liite 1) kuvauksen siitä, mistä työssä oli kyse. Tämän lisäksi mukana oli tietosuojaseloste, joka tutkimusta varten oli tehty (liite 2). Lisäksi ne henkilöt, jotka ilmoittivat osallistuvansa paneeliin, saivat lyhyet kuvaukset Amiraalikoodistosta sekä 4x4-matriisista, jotka toimivat työn pohjalla (liite3). Saatekirjeessä tuotiin esille, että nämä matriisit ovat helpommin käytettävissä esimerkiksi henkilötiedustelussa kuin kybertoimintaympäristössä ja tämän takia ne toimivat tausta-aineistona, mutta työn tarkoitus on tehdä matriisi, joka soveltuu näitä paremmin kybertoimintaympäristöön.

Aineisto kerättiin hyödyntäen eDelphi-nimistä sovellusta, joka on Delfoi-asiantuntijametodin käyttöön suunniteltu avoimen lähdekoodin verkko-ohjelmisto. Tämä mahdollisti sen, että asiantuntijat pystyivät vastaamaan kyselyyn anonyymisti sekä haluamanaan ajankohtana kyselyn ollessa auki. Sovellus

mahdollisti vastausten työstämisen eikä kyselyä tarvinnut heti tehdä valmiiksi, vaan sen saattoi jättää kesken ja palata omiin vastauksiinsa vielä myöhemmin. Myös vastausten muokkaaminen oli mahdollista kyselyn ollessa avoinna.

Kierrokset rakentuivat siten, että ensimmäisellä kierroksella panelistit saivat ensimmäisen luonnoksen (taulukko 10) matriisista kommentoitavakseen. Koska työ toteutettiin Delfoita hyödyntäen, eikä siihen kuulunut esimerkiksi ryhmäkeskustelua tai työpajaa, oli tärkeää, että alussa oli esitetty jo jonkinlainen luonnos matriisista, jotta kysely ja työ saatiin käyntiin. Tavoitteena kuitenkin oli, että ensimmäinen versio ei ohjaisi panelisteja liikaa, jotta he haastaisivat ja kertoisivat näkemyksiään. Tämän takia vastausohjeissa tuotiin useaan kertaan esille, että kyseessä on luonnos, jota pyydetään haastamaan. Lisäksi avoimeen vastausosioon pyydettiin tuomaan esille korjausehdotuksia sekä muutoksia, joita matriisin kyseinen kohta vaatisi toimiakseen.

Jos työ olisi aloitettu kokonaan tyhjästä ja panelistit olisivat joutuneet itse rakentamaan oman matriisin, olisi tämä vaatinut liikaa aikaa. Lisäksi panelistien olisi pitänyt olla syväosaajia ja tuntea esimerkkimatriisit, jotka toimivat työn pohjalla. Tämä ei ollut tarkoituksen mukaista vaan tärkeämpää oli kybertoimintaympäristön sekä viranomaistoiminnan tuntemus. Näiden lisäksi korostuivat tiedonvaihto sekä tilannekuvaymmärrys.

Tutkimuksen aikana kyselykierroksia toteutettiin yhteensä kolme. Kyselykierrosten aikana pyrittiin selvittämään matriisin sopivuutta ja miten sen sanoitukset eri osioissa toimivat. Tämän lisäksi kyselykierroksilla kaksi ja kolme esitettiin avoimia kysymyksiä aiheeseen liittyen. Kysymykset nousivat esille matriisiin annetuista palautteista sekä kierrosten välillä tehtävän synteesin tuotteena.

5.1 Ensimmäinen kierros tiedon ja lähteen luotettavuus kybertoimintaympäristössä

Ensimmäisellä kyselykierroksella vastaajat saivat luonnoksen matriisista, jossa oli esillä sekä lähteen että tiedon luotettavuuden kategoriat. Vastausohjeessa oli nähtävillä yleinen taulukko siitä, mistä kategorioista matriisi muodostuu. Lähteen ja tiedon osalta kummassakin oli kuusi kategoriaa, joissa tietoa ja lähdettä määriteltiin luotettavasta epäluotettavaan. Tämän lisäksi kysymysosiossa oli tarkempi kuvaus siitä, minkälainen määritelmä kyseiseen kategoriaan on liitetty. Tässä panelisteilta kysyttiin, onko kuvaus riittävä. Tähän pystyi vastaamaan monivalintakysymyksenä: kyllä, ei tai en osaa sanoa. Mikäli panelisti kertoi, että määritelmä ei ole riittävä, pyydettiin vastaukselle antamaan täydennys, miten määritelmää tulisi muuttaa tai täydentää, jotta se olisi sopivampi. Työssä käytetyt lainaukset ovat suoria kopioita niistä vastauksista, joita panelistit ovat eDelphi-sovelluksen kautta antaneet.

5.1.1 Lähteen luotettavuus

Lähteen määrittelyssä oli amiraalikoodiston tavoin kuusi kategoriaa, jotka kuvasivat lähdettä alenevassa järjestyksessä luotettavasta epäluotettavaan (A-E). Tämän lisäksi huomioitiin sellainen lähde, jota ei voida määritellä (F). Ensimmäisen kierroksen luonnos matriisista ja lähteen luotettavuuden eri kategorioiden tarkennuksista on esitetty taulukossa 10.

TAULUKKO 10 Lähteen luotettavuus ensimmäinen kierros

Lähteen luotettavuus		
A	Lähde on luotettava	Lähde on tunnettu ja se kuuluu luottamusverkostoon. Lähde on esimerkiksi vastinviranomainen Euroopan Unionissa tai Natossa tai lähde on pienemmän luottamusverkoston jäsen, johon tiedon saanut viranomainen itse kuuluu. Lähde on tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa.
B	Lähde on yleensä luotettava	Lähde on suomalainen tai ulkomainen organisaatio, joka kuuluu luottamusverkostoon, esim. HVK-kriittinen organisaatio tai sellainen maa, joka ei ole Naton tai EU:n jäsen, mutta jonka kanssa tehdään toistuvasti yhteistyötä. Lähde on tunnettu tietoturvatutkija tai yhteisö tai tietoturvatalo, jonka kanssa on tehty yhteistyötä aikaisemmin. Lähde on tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa.
C	Lähde on melko luotettava	Lähde ei kuulu yleisimpiin luottamusverkostoihin, mutta se on tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa. Kyseessä on useasti joku toinen viranomainen, tietoturvatutkija tai tietoturvatalo. Lähde voi olla myös jonkinlainen tietokanta, kuten haittaohjelma-analyysitietokanta (esim. Virustotal tai vastaava palvelu)
D	Lähde ei yleensä ole luotettava	Lähde on toisen maan vastaava viranomainen, joka ei kuulu luottamusverkostoihin tai ei ole aktiivinen ja luotettava toimija niissä eikä sen kanssa tehdä säännöllistä yhteistyötä. Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista. Lähde on organisaatio, jonka oma kyberkyvykkyys on alhaisella tasolla eikä sen toimintaa tunneta tarkemmin.
E	Lähde on epäluotettava	Lähde voi olla toisen maan viranomainen tai suomalainen / ulkomaalainen yritys, tietoturvatutkija tai tietoturvatalo, joka aikaisemman perusteella ei ole tuottanut laadukasta ja luotettavaa tietoa tai kyseessä on uusi toimija, jota ei tunneta eikä taustaa voida arvioida.
F	Lähteen luotettavuutta ei voida todentaa	Lähteen luotettavuutta ei voida arvioida.

Panelistit antoivat ensimmäisellä kierroksella muutosehdotuksia muotoiluihin, jotka huomioitiin seuraavan kierroksen määrittelyissä. Tavoitteena oli, että jos useampi panelisti antoi samasta asiasta palautetta, tämä huomioitiin seuraavalla kierroksella. Toisaalta myös yksittäisten palautteiden arvo oli tärkeää, sillä vastaajajoukko ei ollut suuri ja kaikki eivät nostaneet samoja havaintoja esille.

Tämän takia myös yksittäisiä havaintoja nostettiin osaksi yhteistä keskustelua. Ensimmäisellä kierroksella määritelmissä lähdettiin siitä, että lähde kuvattiin melko tarkasti organisaatio tasolla. Tämä pohjautui siihen, että myös tiedon vastaanottaja voisi helpommin hahmottaa minkälaisesta lähteestä tieto on peräisin, kun tiedon vastaanottanut viranomainen jakaa sen eteenpäin muille. Tämä sai useammalta panelistilta palautetta, ettei tällainen jaottelu olisi toimivaa.

> Yksi panelisteista tiivistää asian hyvin: ”Hankalaa tässä kokonaisuudessa on, että lähde määritellään ennakkoon. Tällöin tehdään ennakko olettamus, ettei A- tason luottamusta voida luoda yllä mainittuihin. Mitä tapahtuu tilanteessa, jossa A: n kaltainen luottamus muodostuu, mutta kyseessä onkin tässä lueteltu toimija. Entä voiko A osiossa luetellut toimijat olla tässä osassa, kun niitä ei nyt luetella tässä. Kokisin, että toimija neutraalit kuvaukset olisivat käytännöllisimmät. En kuitenkaan ole niin syvällisesti perehtynyt kybertiedonvaihdon luonteeseen, että voisin varmasti sanoa, onnistuuko toimijaneutraali kuvaus.”

> Toinen panelisti nostaa esille samaa asiaa hieman eri näkökulmasta osion D palautteessa: ”Tästä puuttuu ei-organisaatio tai yrityskentän toimijat kokonaan? Eivätkö ne voi olla tässä luotettavuustasossa? Kokonaisuudessaan tekisin toimijoista jonkin matriisin, ja katsoisin, että sen matriisin mukaiset "kriteerit" olisi kuvattu joka toimijan osalta jokaisessa kohdassa kulloinkin vaadittavalla tasolla. Näin olleen erityyppisiä toimijoita ilmenee eri luotettavuustasoilla eikä synnyt tämmöisiä katveita kuten tässä.”

Ensimmäisen kierroksen jälkeen oli pohdittava, miten matriisista saisi hyvän viitekehyksen, joka ohjaa tarpeeksi, mutta joka ei rajaisi liikaa. Organisaatiota ei voi kuvata lähteeseen liian tarkasti, sillä jokaisella viranomaisella on omat lähteet ja luottamusverkostot sekä niille omat arvionsa luotettavuuden suhteen. Samalla panelistien keskuudesta nousi esille, että luottamus voidaan menettää vain kerran ja tämä saattaa vaikuttaa lähteen luotettavuuteen ja sitä myötä sen luokitukseen matriisissa. Organisaatioita ei tulisi lukita liikaa osaksi määrittelyjä, jotta niitä voi liikuttaa luotettavuuden kategorioissa vapaammin. Toiselle kierrokselle oli tärkeää tehdä muutoksia juuri organisaatiokuvauksiin ja pohtia näiden sanoittamista toisella tavalla.

Tiedon luotettavuuden määrittely rakentui samalla tavalla kuin lähteen määrittely eli siinä oli kuusi kategoriaa alenevassa järjestyksessä (1-5), jotka pyrkivät kuvaamaan tietoa ja sen luotettavuutta mahdollisimman tarkasti aina luotettavasta epäluotettavaan. Tämän lisäksi oli viimeinen (6) kategoria, jonka avulla kuvattiin tietoa, jota ei pystytään todentamaan. Ensimmäisen kierroksen luonnos matriisista ja tiedon luotettavuuden eri kategorioiden tarkennuksista on esitetty taulukossa 11.

TAULUKKO 11 Tiedon luotettavuus ensimmäinen kierros

Tiedon luotettavuus		
1	Täysin uskottava / vahvistettu muista lähteistä.	Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä voidaan varmuudella todentaa eikä tiedon tarkkuudesta ole epäilystä. Tieto vaikuttaa loogiselta ja se voidaan varmentaa. Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu. Sama tieto ei ole valunut usealle viranomaiselle eri reittejä pitkin ja voidaan poissulkea nk. vahvistusharha.
2	Todennäköisesti totta	Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä voidaan varmuudella todentaa eikä tiedon tarkkuudesta ole epäilystä. Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu. Tieto vaikuttaa loogiselta, mutta sitä ei vielä ole voitu vahvistaa. Sama tieto ei ole valunut usealle viranomaiselle eri reittejä pitkin ja voidaan poissulkea nk. vahvistusharha.
3	Mahdollisesti totta	Jos äskettäin raportoitu tieto ei ole ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa, vaikka vahvistus ei ole riittävää korkeamman todennäköisyyden määrittämiseksi. Kyseessä on uusi tieto, jota ei ole vielä pystytty varmentamaan muista lähteistä, mutta asiantuntija-arvion perusteella tieto vaikuttaa oikealta. Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa vaan saanut tiedon omien verkostojen kautta tai osana laajempaa yhteistyötä. Muu kerätty tieto tukee kyseisen tiedon todenmukaisuutta.
4	Epäilyttävä	Tieto ei vaikuta loogiselta, mutta voi mahdollisesti olla totta. Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa. Tietoa ei vielä ole voitu vahvistaa
5	Epätodennäköinen	Tieto ei ole loogista ja/tai ristiriidat saadun tiedon osalta vaikuttavat, ettei saatu tieto ole uskottavaa. Tietoa ei vielä ole voitu vahvistaa
6	Tiedon oikeellisuutta ei voida todentaa:	Lähde ei tunne tietoa henkilökohtaisesti eikä tiedon oikeellisuutta pystytä varmistamaan muista lähteistä.

Ensimmäisellä kierroksella yksittäiset muotoilut saivat palautetta ja nämä huomioitiin toisen kierroksen muotoiluissa. Palautteissa korostui tekninen toimintaympäristö, sillä tiedon luotettavuuden mittaamisessa oli tärkeää, että tieto oli saatavilla toistettavasti sekä tieto on teknisesti dokumentoitu siten, ettei sitä ole voitu manipuloida. Yksi panelisteista nostaa kategorian kaksi kohdalla vastauksessa useamman panelistin palautteen, joka näkyi laajasti eri kategorioiden palautteissa:

> ”Edelliseenkin kohtaa, mutta myös tähän; pitääko jokaisen virkkeen olla yhtäaikaa "tosi", että tieto päätyy tähän luokkaan, vai tulisiko lisätä ehdollisuutta. Vertailuoperaattoreita käyttöön "joko tai, ja/tai, sekä että, jne

> jne. Nyt esim. jos kaikkien virkkeiden pitää olla samaanaikaan totta, hyvin harva tieto päätyy edes tällä varmuustasolle. Varmuudella, omilla kyvyillä, todentaa? Edelleen tieto tiedon lähteistä, hankintakeinoista ja jakamisesta muille todennäköisesti hyvin hankalaa tai jopa mahdotonta saada, mikä mitigoi kriteeristön tehoa luokittelussa. Viimeistään viimeinen kohta valumisesta muille tappaa koko luokan. Tiedon luotettavuutta pitäisi määrittelemään enemmän sen pohjalta, miten itse kyetään omilla suorituskyvyillä varmistamaan tai miten esim. jonkin elävän elämän tai casejen kautta, jopa tutkimuksen kautta, sitä kyetään todentamaan aidoksi."

Vastauksessa todetaan, että *"viimeistään viimeinen kohta valumisesta muille tappaa koko luokan"*, jolla viitataan kohtaan "sama tieto ei ole valunut usealle viranomaiselle eri reittejä pitkin ja voidaan poissulkea nk. vahvistusharha." Vahvistusharha ja sen huomioiminen tilannekuvan jakamisessa ja kokonaiskuvan muodostamisessa ovat tärkeitä. Palaute on kuitenkin oleellinen, sillä vahvistusharha ei liity itsessään tiedon luotettavuuteen vaan tämä asia tulisi huomioida tietoa jaettaessa eteenpäin ja isompaa kuvaa muodostaessa, jolloin eri lähteistä kerättyä tietoa tulee arvioida omana isona kokonaisuutena.

Vaikka palautteet annettiin aina tiettyyn osioon, oli osa tulkittavissa sellaiseksi, että ne oli tarkoitettu laajemminkin koko matriisiin eikä pelkästään tiettyyn osa-alueeseen. Annettujen palautteiden perusteella asiaa tuli selvittää panelisteilta tarkemmin ja tämän vuoksi alla esitetyn palautteen seurauksena toiselle kierrokselle tehtiin asiaa käsittelevä oma kysymys.

> "Tässä arvioidaan tietoa lähinnä sen lähteiden kautta, mutta miten kriteeristössä arvioidaan omalla tiedonhankinnalla hankitun tiedon luotettavuutta, joka on vastaavasti kyseenalaistettava siinä, missä muualta saatu tieto. Ainakaan kriteeristöä ei saa hyödyntää oman tiedon luokittelussa, jos siihen ei ole kriteereitä. Tämä taas vaikeuttaa kokonaisuudessaan hallussa olevan tiedon käsittelyä, jos omaakin tietoa ei luokitella."

> Palautteissa nousi myös työn lopun kannalta tärkeä seikka esille: "Voisiko olla joku vuokaavio / rastia ruutuun tapa, jolla sitten tiedon (ja lähteenkin) luotettavuudesta saisi tarkan koodin."

Vastaajat eivät nähneet taulukoiden 16 ja 17 kaltaisia kuvauksia vastaustensa aikana ja jo näiden näkeminen olisi saattanut helpottaa hahmottamista, sillä he näkivät ainoastaan kaksi ensimmäistä saraketta vastausohjeen yhteydessä ja kolmas sarake, jossa tarkempi kuvaus oli esitetty, oli vasta kysymyksessä, jossa osiosta pyydettiin palautetta. Palaute oli tärkeä, kun kolmannen ja viimeisen kierroksen jälkeen palautteet käytiin vielä läpi ja matriisin viimeinen versio päivitettiin.

Ensimmäisen kerroksen palautteiden pohjalta tiedon ja lähteen luotettavuuden osalta pystyttiin vahvistamaan molempien osalta viimeinen kategoria eli kohta F ja 6, joissa lähteen ja tiedon luotettavuutta ei pystytä arvioimaan. Näihin osioihin panelistit eivät juurikaan antaneet korjausehdotuksia ja niihin ei enää seuraavilla kierroksilla pyydetty vastauksia. Osioita ei kuitenkaan poistettu

kokonaan vaan ne olivat jokaisella tulevalla kyselykierroksella näkyvissä, mutta niihin ei enää pyydetty kommenttia.

5.2 Toinen kierros tiedon ja lähteen luotettavuus kybertoimintaympäristössä

Toinen Delfoi-kierros rakentui edellisen kierroksen vastausten ja näistä tehdyn synteesin pohjalle. Matriisia päivitettiin saatujen vastausten ja havaintojen perusteella. Matriisin määrittelyn lisäksi toisella kierroksella vastaajille esitettiin seitsemän erillistä kysymystä, joiden avulla heidän näkemyksiään pyrittiin syventämään. Kysymysten avulla pyrittiin lisäksi täydentämään edellisen kierroksen havaintoja, joita palautteiden perusteella oli syntynyt.

> Ensimmäiseksi nostettiin esille kysymys, joka nousi edellisen kierroksen pohjalta organisaatioihin liittyen. Esimerkiksi EU:n ja Naton kautta viranomaisten luottamusverkostoihin kuuluu automaattisesti myös sellaisia valtioita, jotka eivät välttämättä ole niin luotettavia tai niiden tarkoitusperiä voidaan epäillä. Miten matriisissa tulisi huomioida sellaiset valtiot ja/tai organisaatiot, jotka ovat osa jotakin laajempaa verkostoa, mutta joiden tarkoitusperiä tiedon jakamiselle suhtaudutaan epäilevästi tai niiden kanssa yhteistyö ei ole vakiintunutta? Mihin kategoriaan tällaiset valtiot/organisaatiot tulisi laittaa ja minkälaisin perustein?

Tässä kysymyksessä halutiin vielä tarkemmin pureutua edellisen kierroksen palautteiden pohjalta organisaatioihin ja miten organisaatiotietoa voitaisiin matriisissa ottaa huomioon. Panelistien vastausten perusteella luotettavuus voi riippua asiayhteydestä. Lisäksi yksittäiset virkahenkilöt voivat tehdä virheitä ja taas toisaalta yksittäinen virkahenkilö voi tuottaa oikeaa tietoa ja valtion organisaatio voi olla luotettava, vaikka maan johto ajaisi erilaista agendaa tai yksittäinen virkahenkilö tekee virheen. Se olisiko yksi virhe, jo sellainen tekijä, joka laskee lähteen luotettavuutta, oli seikka, jota panelistit pohtivat. Vastausten perusteella asia ei ollut mustavalkoinen vaan virhe ja asiayhteys vaikuttivat kokonaisuuteen. Historiatieto nähtiin tärkeänä, jotta arvioita lähteen luotettavuudesta pystyttiin rakentamaan. Tällä tarkoitettiin sitä, että lähde on tunnettu pidemmän aikaa eikä kyseessä ole uusi toimija. Tämä auttoi muodostamaan kokonaiskuvaa lähteestä ja sen toimittamista tiedoista pidemmällä aikavälillä, jonka perusteella kokonaisarvioita voitiin tehdä.

Yksi panelisti nostaa edellä esitettyjä nostoja omassa vastauksessaan seuraavasti:

> ”Vaikka maan poliittinen tilanne on, mitä on, ja muodostaa potentiaalia siihen, että vastaava toiminta alkaa näkymään myös virasto/virkamiestasolla, niin silti virastoja/virkamiehiä ei voi arvioida täysin epäluotettaviksi. Kuitenkin potentiaali tilanteen muutokseen myös virkakoneiston osalta pitää arvioida lähteen luotettavuuden alkutilassa ennen kuin on muuta kokemuksen tuomaa evidenssiä muuttaa arviota. Näillä toimijoilla

> tieto voi olla luotettavaa, mutta se on yksipuolista, siitä puuttuu faktoja tai painotukset ovat erilaiset kuin muilla mailla tai neutraaleilla toimijoilla. Haaste on, miten näiden toimijoiden, joiden status muuttuu (ylös tai alas) aikaisemmin jakama tieto luokitellaan historiallisesti. Eli miten toimijan luotettavuuden muutos vaikuttaa historialliseen tietoon, ja miten se vaikuttaa esim. omiin analyyseihin ja niiden luottavuuteen."

Edellisellä kierroksella muutamassa vastauksessa nousi esille, kuinka monen kohdan tulisi osiossa täyttyä, jotta tieto tai lähde voidaan sijoittaa tiettyyn kategoriaan. Tämän takia toisella kierroksella asia esitettiin panelisteille kysymyksenä: "Jotta tätä voidaan jollakin tavalla ohjeistaa, kuinka monen tarkennuksen tulisi täyttyä, jotta kyseinen kohta voidaan valita?" Matriisissa ei ole määritelty, kuinka monen kohdan tarkennuksesta tulee täyttyä, jotta lähde tai tieto kuuluisi tiettyyn kategoriaan. Jokainen tilanne ja tapaus vaatii omaa harkintaansa. Suurin osa vastaajista oli sitä mieltä, että kolmen tai useamman kohdan tulisi täyttyä, jotta tieto tai lähde voidaan sijoittaa tiettyyn kategoriaan. Tämäkään ei ollut aivan yksiselitteistä ja tämä nousi esille vastauksissa.

> "Tämä ei ole yksiselitteinen asia. Toisaalta mitä useampi osa-alue viittaa tiettyyn suuntaan, vahvistaa se käsitystä asian tilasta yksittäistä osa-aluetta vahvemmin. Toki osa-alueiden välillä voi olla eroa niiden keskinäisessä merkityksessä ja painoarvossa, joten tältä osin tapauskohtainen harkinta on aina tarpeen. "

Toinen panelisti nosti hyvän kehitysehdotuksen matriisille, joka toisi vastaavan ulottuvuuden matriisiin, joka aikaisemmin esitetyssä 5x5x5-matriisissa on (kts. Luku 3.8).

> "Itse loisin numeraalisen järjestelmän luotettavuuden arviointiin. Taso kohtaiset kuvaukset voivat olla silloin kuten nytkin, mutta samalla kullakin taso osa-alueella on jokin tietty pistemäärä. Osa-alueen pistemäärä on pienempi mitä alemman tason kriteeristöön mennään. Samalla kullekin tasolle pääsemiseen luodaan kynnyspistemäärä, joka eri osakokonaisuuksien yhteenlaskettujen pisteiden tulee täyttää. Tällöin esim., jos toiseksi ylimmän tason kriteereistä täyttyy 3 (esimerkki pistearvo 5), mutta neljäs osa-alue on vaikka alempi (pistearvo alemmalla tasolla esim. 3), toimijan yhteispisteet ovat 18 pistettä. Jos samaan aikaan on määritelty, että toiseksi ylimmälle tasolle pääsemiseen edellytetään 17 pistettä, toimija yltäisi tälle tasolle. Kokonaispistemäärän lisäksi voidaan luoda muita portteja. Esim. jos jonkin osa-alueen osalta toimija on epäluotettava, vaikka kokonaisisteet täyttyisivät, toimija pitää arvioida epäluotettavana. Tai vastaavasti, jos jonkin toimijan jokin osa-alue on yli kaksi pykälää alempi, voisi se laskea kokonaisarviota yhdellä luokalla, vaikka ylemmän tason pisteet täytyy. "

Kolmannen kysymyksen kohdalla pyrittiin selvittämään sitä, millä tavalla myös tiedon vastaanottava organisaatio pystyisi päättelemään tiedon lähdettä, vaikka sitä itsessään ei kerrota vaan ainoastaan tieto. Yleisenä havaintona on ollut se, että tiedon vastaanottava organisaatio haluaisi saada myös tiedon, kuka tiedon

on jakanut. Useastikaan juuri tätä tietoa ei voida jakaa ja matriisin avulla voitaisiin mahdollisesti antaa tästä osviittaa, vaikka itse lähdettä ei paljastetakaan. Kysymyksessä oli mukana esimerkki, jossa kerrotaan, että poliisi jakaa tiedon x Kyberturvallisuuskeskukselle ja Puolustusvoimille, millä tavalla nämä organisaatiot voisivat hahmottaa lähdettä paremmin?

> ”Lähdettä ei voida aina jakaa vaikka tarkemmalle tiedolle olisi perusteltu tarve. Erityisesti kv kumppanilta saadun tiedustelutiedon osalta lähde on käytännössä aina salassa pidettävä tieto, jota ei voida paljastaa vaarantamatta luottamussuhdetta kumppaniin.” Kirjoittaa yksi panelisti.

> ”Lähde voitaisiin luokitella sitä yksilöimättä (yksilö, vapaat lähteet, organisaatio, viranomainen, yms.). Tämä antaisi luotettavuusarvion lisäksi kontekstuaalista tietoa. Esim. luotettava yksittäinen henkilö on vähemmän painava lähde kuin luotettava viranomainen, sillä yksittäisen henkilön luotettavuusluokituksessa on helpompi tapahtua muutoksia ajan kuluessa.”

> ”…on mm. sovittava yhteismenettelystä ml. tiedon luotettavuusarviointiasteikkoa koskien. Lähteen luotettavuutta arvioisi poliisi yhteisesti sovitun arviointikriteeristön pohjalta. Tiedon jakamista säätelevä lainsäädäntö asettaa myös rajoitukset tiedonvaihdolle sen kattavuuden / seikkaperäisyyden suhteen.”

Hieman samaa pohti toinenkin panelisti antaen konkreettisen ehdotuksen siitä, miten tätä voitaisiin tehdä.

> ”Jaetun tiedon taustalähteen ei pitäisi muodostaa minkäänlaista kriteeriä omassa arvioinnissa, koska lähdettä ei systemaattisesti kaikissa tapauksissa tunneta. Korkeintaan lähteen tunnettavuus voisi olla edellä kuvatussa pistelasku/kynnys mallissa kynnys esim. nousulle seuraavalle pykälälle kriteeristössä, jos tiedon "yhteenlaskun" muut kriteerit ylittävät rajaarvon tai jos lähde on epäluotettava, laskea tasoa alaspäin, vaikka pistelaskussa kriteerit jollekin tasolle nousevat. Koska itse ei useinkaan voida arvioida erityisesti, kv-verkostojen viranomaistiedon lähteen luotettavuutta, pitää pystyä huomioimaan sitä, kuinka luotettavaksi tiedon luovuttaja itse tiedon ja sen lähteen luokittelee. Lähteen luotettavuutta voidaan kysyä tiedon luovuttajalta, josta voidaan johtaa arviota itselle. Kriteeristönä voitaisiin käyttää omaa erillistä lähteen luotettavuuskriteeristöä. Näin ollen arviointikehikosta tulee kolmiosainen, jossa yksi osa on tiedon luovuttajan luotettavuus, yksi osan on tiedon lähteen luotettavuus (usein joltakin toiselta saadun tiedon osalta ei pystytä arviomaan itse) ja itse tiedon luotettavuus.”

Neljännessä kysymyksessä nostettiin esille haasteet, joita esimerkiksi amiraalikoodisto on saanut. Kyseistä matriisia sovelletaan eri toimijoiden parissa hyvin eri tavalla. Näin ollen sama tieto saattaa saada toisella viranomaisella aivan eri numeerisen ja kirjain arvon kuin toisella. Panelisteilta pyydettiin näkemystä siitä, miten kybermatriisista saataisiin rakennettua sellainen, että se palvelisi eri viranomaisia tarpeeksi ja että matriisia sovellettaisiin samalla tavalla organisaatosta riippumatta?

Panelistit olivat hyvin yksimielisiä siitä, että määrittelytyötä tulee tehdä kattavammin ja kuvaukset tulee avata erittäin selkeästi sekä avata erot eri luokkien välillä. Määrittelytyötä tulisi tehdä yhdessä niiden viranomaisten kesken, jotka matriisia käyttävät, sillä heillä tulisi olla yhteinen käsitys matriisin käytöstä.

> ”Ongelmana on nähdäkseni se, että lähteen ja tiedon luotettavuuden kuvauksia ei ole avattu riittävästi, jotta eri toimijoiden käsitys esimerkiksi siitä mitä "luotettava" tai "melko luotettava" tarkoittavat. Lähtökohtaisesti käsitys näistä on subjektiivinen ja siten eri henkilöillä erilainen. Matriisin avaaminen lähteen ja tiedon luotettavuuden asteiden tarkempi kuvaus ja etenkin asteiden keskinäisten erojen kuvaaminen yhdenmukaistaisi käytäntöjä ja helpottaisi siten toimijoiden välistä tiedonvaihtoa.”

> ”Kriteeristö pitäisi luoda yhdessä niiden toimijoiden kesken, ketkä sitä kansallisesti yhdessä käyttävät. Se pitää pilotoida, korjata pilotin jälkeen ja sen jälkeen lanseerata käyttöön koulutuksen kera. Kriteeristö pitää tuoda osaksi teknistä toteutusta, esim. MISP injektejä siten, että sen on keskeinen ja pakollinen osa MISPiin syötettävää tietoa tai syntyy osin automaationa esim. joidenkin tagien syöttämisen seurauksena. Esim. SI (Sigint) tagi johtaisi automaationa tiettyyn luotettavuustasoon kuin taas OSINT johonkin muuhun, riippuen muista TAGeista (esim. toimija/lähde). Mitä enemmän tiedon toimijoiden luokittelussa tarvitaan nahkarelettä (ihmistä) sitä korkeammaksi kynnys nousee. Arviointia voidaan ottaa käyttöön ensi vaiheessa analyysien ja raporttien osalta ja myöhemmässä vaiheessa siirtyä kohti yksittäisten tietoalkioiden luokittelua. ”

Ensimmäisen Delfoi-kierroksen aikana nousi esille myös pohdinta siitä, kuinka lähellä tieto tulisi olla tuotettu. Jos lähde jakaa tiedon, jonka se on itse tuottanut tai ollut osana isompaa joukkoa, onko tieto silloin luotettavampaa kuin sellainen tieto, joka ei välttämättä ole lähteen itsensä tuottamaa. Yleisesti kysymys nähtiin haastavana, sillä siihen ei ole yhtä oikeaa ja selkeää vastausta. Itse tuotettu tieto voi olla myös virheellistä ja toisaalta saatu tieto oikeaa tai toisin päin.

> ”Tulosten luotettavuus riippuu enemmän niiden hankintametodista kuin läheisyydestä kohteeseen, myös alkuperäistutkimus voi päätyä väärin johtopäätöksiin, jos metodi on huono. Tähän on vaikea vastata. Nähdäkseni havainnon tulisi olla ensikäden havainto ts. lähteen itse tuottama. MUTTA tässäkin tulee huomioida jollain tapaa myös itse tai lähteen tekemän havainnon luotettavuus. Eli pelkkä oma havainto ei tee tiedosta sen luotettavampaa vaan tällaisenkin tiedon luotettavuutta pitää varmentaa havainnon tekemiseen ja sen tulkintaan liittyvien vääristymien varalta. ”

Kuudes kysymys koski luottamusta. Ensimmäisellä kierroksella nostettiin esille se, että jos lähdeosio matriisista on liian organisaatio keskeinen ei se mahdollista organisaatioiden liikkuvuutta eri kategorioissa. Joku aikaisemmin luotettuna pidetty lähde, voi menettää luottamuksen ja toisaalta sellainen lähde, joka on aluksi tuntemattomampi voi osoittautua yhteistyön tiivistyessä erittäin luotettavaksi lähteeksi. Kuudennessa kysymyksessä panelistien piti pohtia, miten lähdettä,

joka jakaa jatkuvasti virheellistä tietoa tulisi käsitellä? Miten organisaatioiden tulisi voida liikkua eri kategorioissa ja minkälaista dokumentaatiota tästä tulisi olla, jotta viranomainen tunnistaa omat lähteensä sekä niihin liittyvän historiatiedon.

Kuten aikaisemmin jo toimijoiden osalta kysymyksessä yksi, nousi tässäkin kysymyksessä esille se, että toimijat tulee erottaa toisistaan. Yksittäisen ihmisen tekemä virhe, ei tee koko organisaatiosta epäluotettavaa. Dokumentaatio onkin tärkeää, jotta historiatietoa pystytään seuraamaan ja tekemään sisäistä jatkuvaa arviointia siitä, onko lähde edelleen luotettava vai ei ja millä tasolla sen kuuluisi olla. Ero misinformaation ja disinformaation välillä tuli tehdä. Kompleksisessa kybertoimintaympäristössä, jossa tietoa on paljon ja tilanne elää hyvinkin nopeasti, voi vahingossa jakaa virheellistä tietoa. Oleellista on se, miten lähde korjaa jakamaansa virheellistä tietoa.

> ”Luotettavuuden pettämisen syy merkitsee - jos tiedon jakaja on toiminut vilpittömästi, niin luottamusta ei välttämättä menetetä. Mikä tahansa tarkoituksellinen vilppi taas hävittää luottamuksen, vaikka vääristely tiedossa olisi vähäistä. Motiivit ratkaisevat.”

> ”Luotettavuuden portaisiin tulee rakentaa yhteismitallinen kriteeristö joka ottaa huomioon tiedon oikeellisuuden arvioinnin pitkällä aikavälillä. On toki selvää, että runsaasti tietoa tuottavalle lähteeltä tulee virheellisiä tietoja määrällisesti enemmän kuin harvakseltaan tietoa tuottavalta. Luotettavuutta ei voi siten määrittää absoluuttisilla luvuilla vaan se tulee suhteuttaa lähteen tuottaman tiedon määrään. Toisekseen pitää erottaa tahattomasti virheellinen ja tietoisesti annettu väärä tieto toisistaan. Tahaton virheellinen tieto voi johtua yksittäisistä inhimillisistä virheistä tai erehdyksistä lopullisen päämäärän oltua kuitenkin vilpittömästi oikean tiedon tuottamisen. Tahattomasti tuotettu virheellinen tai väärä tieto toistuessaan heikentää luotettavuutta asteittain. Sen sijaan tahallisesti annettu väärä tai harhaanjohtava tieto johtaa lähtökohtaisesti välittömään luottamuksen pysyvään menettämiseen.”

> ” Jos tiedon joltain osin huomataan olevan virheellistä tietoon voisi liittää korjauskertoimen, kun virhe on havaittu. Tarkoittaa että pohjalta lähteneen virheellisen tiedon analyysi on tuottanut uutta tietoa, sen voi vielä korjata korjauskertoimella tai todennäköisyydellä. Organisaation luotettavuus on suoraan verrannollinen niiden saamaan tiedon lähteiden luotettavuuteen, ja niiltä osin, kun ovat itse keränneet tiedon ja tuottaneet sen, luotettavia. Yleinen katselmus tiedon toimijoista saaduista kokemuksista voisi olla paikallaan.”

Viimeinen kysymys käsitteli valkohattuhakkereiden roolia lähteenä. Suomessa valkohattuhakkereiden yhteisö on merkittävä ja he tuottavat tietoa myös viranomaisten tarpeisiin, joiden avulla viranomaiset voivat toteuttaa omaa tietoturvatutkintaa ja selvittää erilaisia tapauksia. Mihin lähdekategoriaan valkohattuhakkerit kuuluvat panelistien mielestä, vaihteli. Kuitenkin se, miten heidän roolinsa tulisi määritellä, oli avoimien vastausten perusteella paljon yhtenäisempi.

Vaikka panelistit sijoittivat valkohattuhakkereita hyvin eri kategorioihin, oli avointen vastausten perusteella selkeää yksimielisyyttä siitä, että valkohattuhakkerit ovat kirjava joukko yksittäisiä lähteitä ja niiden tuottama tieto tulee aina tarkistaa siinä missä jonkun toisen lähteen tuottama tieto.

> ”kategorisointi tässä mielessä on hankalaa ja jopa epärelevantti ja riippuu, kenen käyttöön tuotettu tieto on tarkoitettu. Viranomaisten näkökulmasta se on korkeintaan ilmiannon tason tieto - kuten tavanomaisessa rikostutkinnassa, eli sen paikkansapitävyyttä pitää lähtökohtaisesti todentaa joka tapauksessa riippumatta lähteistä.”

Toisella kierroksella esitetyt kysymykset antoivat lisää syvyyttä panelistien näkemyksiin ja mahdollistivat laaja-alaisemman vastaamisen, kuin pelkkä matriisin kommentointi. Annettuja vastauksia pyrittiin hyödyntämään myös kolmannella kyselykierroksella ja vastauksia pyrittiin sovittamaan osaksi matriisin osa siltä osin, kun se oli mahdollista.

Avointen kysymysten jälkeen jatkettiin itse matriisin työstämistä. Edellisen kierroksen palaute oli huomioitu ja matriisia oli päivitetty tämän pohjalta. Päivitetty matriisi lähteen osalta on esitetty taulukossa 12. Keskeinen muutos oli se, että organisaatioiden määrittelyä loivennettiin ja painotus muuttui enemmän viranomaisen omaan luottamusverkostoon, jonka se itse määrittelee. Organisaatioita oli mainittu ylätasolla esimerkkeinä. Lisäksi luettavuuden kannalta määritelmät myös laitettiin omiksi riveikseen, jotta teksti ei olisi yhtenäistä ja eri kohdat sekoittuisivat helposti toisiinsa.

TAULUKKO 12 Lähteen luotettavuus toinen kierros

Lähteen luotettavuus		
A	Lähde on luotettava	- Lähde on tunnettu ja se kuuluu tiedon vastaanottavan viranomaisen luottamusverkostoon, jonka se on arvottanut itselleen keskeiseksi. - Lähde on esimerkiksi EU tai Nato-organisaatioiden/instituutioiden vastinpari - tai lähde on pienemmän luottamusverkoston jäsen, johon tiedon saanut viranomainen itse kuuluu. - Lähde on organisaatio esim. HVK-kriittinen organisaatio tai tietoturvatalo tai tietoturvatutkija - Lähde on ollut osa luottamusverkostoa pidemmän aikaa ja sen toimintatavat tunnetaan. - Lähde on sellainen, jonka kanssa tehdään toistuvasti yhteistyötä ja se on - tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa.
B	Lähde on yleensä luotettava	- Lähde on organisaatio tai valtio, joka kuuluu tiedon vastaanottaneen viranomaisen luottamusverkostoon, mutta verkosto on esimerkiksi niin suuri, että luottamusta on vaikeampi arvioida tai verkostoa ei ole priorisoitu. - Lähde voi kuulua EU:n tai Natoon. - Lähde on tunnettu tietoturvatutkija tai yhteisö tai tietoturvatalo, jonka kanssa on tehty yhteistyötä aikaisemmin. - Lähde on tunnettu jo jonkin aikaa ja yhteistyö on jo lähes vakiintunutta.

		- Lähde on toimittanut tietoa muutamia kertoja ja sen toimittamat tiedot ovat yleensä olleet oikeita ja oikeanaikaisia.
C	Lähde on melko luotettava	- Lähde ei kuulu tiedon vastaanottaneen viranomaisen yleisimpiin luottamusverkostoihin, mutta se on tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa. - Lähde voi olla valtio, organisaatio tai esimerkiksi tietoturvatutkija. - Lähde tunnetaan, mutta sen kanssa ei ole vakiintunutta yhteistyötä. Se on toimittanut tietoja satunnaisesti. Tiedot ovat olleet useimmiten oikeita ja oikea-aikaisia, mutta välillä virheellisiä ja vanhentuneita. - Lähde voi olla myös jonkinlainen tietokanta, kuten haittaohjelma-analyysitietokanta (esim. Virustotal tai vastaava palvelu)
D	Lähde ei yleensä ole luotettava	- Lähde on esimerkiksi toisen maan vastinviranomainen, kuin tiedon vastaanottanut kotimainen viranomainen, joka ei kuulu kyseisen viranomaisen luottamusverkostoihin tai ei ole aktiivinen ja luotettava toimija näissä verkostoissa eikä sen kanssa tehdä säännöllistä yhteistyötä. - Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista. - Lähteen toimittamat tiedot ovat joskus olleet paikkansapitäviä ja/tai oikea-aikaisia. Suurin osa lähteen toimittamasta tiedosta on kuitenkin ollut virheellistä, paikkaansa pitämätöntä tai vanhentunutta. - Lähde on organisaatio, jonka oma kyberkyvykkyys on alhaisella tasolla tai sen toimintaa ei tunneta tarkemmin.
E	Lähde on epäluotettava	- Lähde voi olla toisen maan viranomainen tai organisaatio, tietoturvatutkija tai tietoturvatalo, joka aikaisemman perusteella ei ole tuottanut laadukasta ja luotettavaa tietoa. - Kyseessä on uusi toimija, jota ei tunneta eikä taustaa voida arvioida tiedonsaantihetkellä. - Lähde ei ole reagoinut tiedon saaneen viranomaisen pyyntöihin esimerkiksi tietopyyntöihin, ilmoituksiin, sivujen alasajoon jne. - Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista. - Lähde tai siihen liitettävä toimija toteuttaa tai on toteuttanut Suomea kohtaan kyberoperaatioita/kyberhyökkäyksiä.
F	Lähteen luotettavuuta ei voida todentaa	- Lähde on entuudestaan täysin tuntematon - Lähde tiedetään, mutta lähde ei ole tuottanut tietoa, jonka luotettavuutta ei olisi voitu arvioida.

Matriisiin tulleet kommentit tukivat jo avoimissa kysymyksissä nousseita vastauksia, ja niissä nousi samoja teemoja uudelleen esille. Panelistit nostivat yksittäisiä tarkennuksia lähteen määrittelyyn edelleen kuten ensimmäisellä kerralla. Mikään yksittäinen teema tai useampi samaa seikkaa nostava kommentti ei toisella kierroksella noussut vahvasti esille lähteen määrittelyä tehtäessä. Kuten jo kysymyksissä, nousi lähteen luotettavuuden osalta se seikka esille, että lähteen luotettavuuteen vaikuttaa myös se, että jos se on tuottanut virheellistä tietoa ja sen havaittuaan korjaa sen, ei se vaikuta luotettavuuteen merkittävästi. Mikäli lähde huomaa virheen, eikä raportoi siitä, tekee se siitä epäluotettavamman.

Tämä kommentti eri tasoisena toistui jokaisessa lähteen arvioinnissa ja alla esimerkki yhdestä määrittelystä:

> ”Lähteen tuottama tieto on virheellistä vain yksittäisissä tapauksissa ja satunnaisesti. Lähde on oma- aloitteisesti korjannut havaitsemansa virheet tai puutteet ja välittänyt korjatun tiedon alkuperäisille vastaanottajille.”

Lähteen luotettavuuden arvioinnin jälkeen jatkettiin tiedon luotettavuuden arvioimista. Matriisissa oli huomioitu ensimmäisen kierroksen palaute ja päivitetty kategorioita sen mukaan. Päivitetty tiedon luotettavuuden matriisi on esitetty taulukossa 13. Tämän lisäksi vastausohjeisiin oli vielä tarkennettu, että tieto halutaan ymmärtää laajasti eli kyse voi olla teknistä tietoa, kuten esimerkiksi vaarantumisindikaattori (engl. Indicator of Compromise, IoC) tai esimerkiksi havainto kartoitustoiminnasta tai muusta digitaalisesta tai fyysisestä todisteesta, että kyberhyökkääjällä on aikomus hyökätä (engl. Indicator of Attack, IoA). Henkilöltä tai verkostolta saatu tieto tai havainto, jossa kerrotaan (uhka)havainnosta tai esimerkiksi tilannekuvasta, mutta sille ei ole antaa tarkempaa teknistä tietoa vaan kyseessä voi olla analyytikon tuottama havainto ja tietojen yhdistäminen, jolla tieto on tuotettu.

TAULUKKO 13 Tiedon luotettavuus toinen kierros

	Tiedon luotettavuus	
1	Täysin uskottava / vahvistettu muista lähteistä.	- Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä voidaan varmuudella todentaa eikä tiedon tarkkuudesta ole epäilystä. - Tieto vaikuttaa loogiselta ja se voidaan varmentaa. - Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu. - Tieto on (tekninen) luotettavasti dokumentoitu tosiseikka, jota ei ole ollut mahdollista manipuloida tai tiedon manipulointi on erittäin epätodennäköistä. - Tieto kyetään omilla kyvyillä varmentamaan ja/tai tieto on saatavilla toistettavasti o Esimerkiksi tekninen uhkatieto olisi toistettavissa omilla menetelmillä.
2	Todennäköisesti totta	- Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä voidaan varmuudella todentaa eikä tiedon tarkkuudesta ole epäilystä. - Tiedon paikkaansa pitävyys/luotettavuus täydennetään muista lähteistä peräisin olevalla tiedolla ja niiden pohjalta tehtävällä kokonaisanalyysillä. - Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu. - Tieto vaikuttaa loogiselta, mutta sitä ei vielä ole voitu vahvistaa.

3	Mahdollisesti totta	- Jos äskettäin raportoitu tieto ei ole ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa, vaikka vahvistus ei ole riittävää korkeamman todennäköisyyden määrittämiseksi. - Kyseessä on uusi tieto, jota ei ole vielä pystytty varmentamaan muista lähteistä, mutta asiantuntija-arvion perusteella tieto vaikuttaa oikealta. - Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa vaan saanut tiedon omien verkostojen kautta tai osana laajempaa yhteistyötä. - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta. - Muu kerätty tieto tukee kyseisen tiedon todenmukaisuutta.
4	Epäilyttävä	- Tieto ei vaikuta loogiselta, mutta voi mahdollisesti olla totta. - Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa. - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta. - Tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan, mutta tästä ei ole suoria indikaattoreita. - Tiedon tuottajalla on ristiriitaisia sidonnaisuuksia. - Tietoa ei vielä ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin.
5	Epätodennäköinen	- Tieto ei ole loogista ja/tai ristiriidat saadun tiedon osalta vaikuttavat, ettei saatu tieto ole uskottavaa. - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta. - Tiedon tuottaneen menetelmät ovat tiedossa, mutta ne ovat todennäköisesti tapaukseen soveltumattomia ja tuottavat virheellistä tietoa. - Tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan ja tämä on voitu selvittää. - Tietoa ei ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin.
6	Tiedon oikeellisuutta ei voida todentaa:	- Tiedon oikeellisuutta ei pystytä varmistamaan muista lähteistä tai omin menetelmin.

Tiedon luotettavuuden osalta nostettiin jälleen yksittäisiä palautteita, joita huomioitiin matriisin päivityksessä. Delfoin yksi tavoite on myös päästä konsensukseen ja toisen kierroksen jälkeen saatettiin jälleen pienin muutoksin vahvistaa tiedon luotettavuuden osalta kategoriat 4. ja 5. Näiden osalta ei enää kolmannella kierroksella pyydettäisi kommentteja.

5.3 Kolmas kierros tiedon ja lähteen luotettavuus kybertoimintaympäristössä

Delfoi-kyselyn alussa panelisteille lähetetyssä saatekirjeessä oli kerrottu, että Delfoi-kierroksia tultaisiin tekemään kaksi tai kolme vastauksista ja kootusta aineisto riippuen. Toisen kierroksen jälkeen tarkennuksille oli vielä tarvetta ja kolmas kyselykierros oli tarpeen toteuttaa. Samalla se oli viimeinen kyselykierros, johon panelisteilta pyydettiin vastauksia. Viimeisellä kierroksella panelistit jatkoivat matriisin määrittelyä. Tämän lisäksi kyselyn lopussa oli vielä lyhyt kysymysosio, jossa oli kaksi matriisia koskevaa kysymystä.

Kolmannella kierroksella matriisia oli jälleen päivitetty saadun palautteen perusteella. Keskeinen muutos ensimmäiseen kierrokseen oli, että matriisia on saatu enemmän yhtenäistettyä niin lähteen kuin tiedon luotettavuuden osalta. Matriisi ei kuitenkaan ollut vielä valmis vaan kolmannen kierroksen palaute oli tärkeää erityisesti myös tästä yhdistämisen näkökulmasta.

Kolmannella kierroksella palautetta ei tullut enää niin paljon, vaan panelistien palaute pureutui enemmän muotoseikkoihin sekä pohdintaan, onko kuvaukset riittävän erilaisia, jotta niiden välillä on helppo tehdä eroa. Matriisin käytettävyys nousi esille palautteissa aikaisempaa enemmän. Hirsjärvi ym. (1997, 182) toteaa, että aineisto on riittävä, kun samat asiat alkavat kertautua haastattelussa. Sisällön osalta voidaan todeta tietynalisen saturaatiopisteen täyttyneen kolmannen kierroksen aikana, sillä uusia havaintoja ei enää tullut, vaan keskityttiin olemassa oleviin tai käytännöllisempiin kysymyksiin, jotka liittyivät matriisin käytettävyyteen. Tämä oli myös merkki siitä, että lisäkierroksia ei olisi ollut mielekästä toteuttaa, sillä uudet kierrokset olisivat vaatineet myös sen, että matriisin olisi voitu tuoda managerin toimesta jotain kokonaan uutta ja testata sen avulla asiantuntijoiden ajatuksia. Samalla lisäkierrokset olisivat vaatineet lisää aikaa, eikä tähän ollut etukäteen varauduttu.

Kolmannella kierroksella panelisteilta pyydettiin aluksi palautettu päivitettyyn matriisiin lähteen luotettavuuden osalta. Päivitetty matriisi on esitetty taulukossa 14. Lähteen luotettavuuden osalta kategorioita saatiin yhtenäistettyä edellisten kierrostenpohjalta ja tämän takia niiden vertailtavuus oli helpompaa.

TAULUKKO 14 Lähteen luotettavuus kolmas kierros

Lähteen luotettavuus		
A	Lähde on luotettava	- Lähde on tunnettu pidemmältä ajalta ja sen toimintatavat tiedetään. - Lähde on sellainen, jonka kanssa tehdään säännöllisesti yhteistyötä ja se on tuottanut aikaisemmin oikeaa ja oikeanaikaista tietoa. - Lähteen toiminnalla on hyvä tarkoitusperä/hyvä tahto. - Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä. - Lähteen tuottama tieto on virheellistä hyvin harvoin/yksittäisissä tapauksissa. - Lähde on korjannut melkein aina oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa. - Lähteen oma kyberkyvykkyys arvioidaan olevan korkealla tasolla. - Lähde voi olla esimerkiksi osa tiedon vastaanottaneen viranomaisen luottamusverkostoa ollen esimerkiksi EU tai Nato-organisaatioiden/instituutioiden vastinpari.
B	Lähde on yleensä luotettava	- Lähde on tunnettu jo jonkin aikaa ja yhteistyö on vakiintunutta tai lähes vakiintunutta. - Lähde on sellainen, jonka kanssa tehdään melko säännöllisesti yhteistyötä ja se on toimittanut muutamia kertoja oikeaa ja oikeanaikaista tietoa. - Lähteen toiminnalla on hyvä tarkoitusperä/hyvä tahto. - Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä. - Lähteen tuottama tieto on harvoin virheellistä. - Lähde on korjannut usein oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa. - Lähteen oma kyberkyvykkyys arvioidaan olevan korkealla tasolla. - Lähde voi olla esimerkiksi osa tiedon vastaanottaneen viranomaisen luottamusverkostoa ollen esimerkiksi EU tai Nato-organisaatioiden/instituutioiden vastinpari.
C	Lähde on melko luotettava	- Lähde tunnetaan, mutta sen kanssa ei vielä ole vakiintunutta yhteistyötä. - Lähde on sellainen, jonka kanssa tehdään silloin tällöin yhteistyötä. - Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä. - Lähde on toimittanut tietoja joskus. Tiedot ovat olleet useimmiten oikeita ja oikea-aikaisia, mutta välillä virheellisiä ja vanhentuneita. - Lähde on korjannut joskus oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa. - Lähteen oma kyberkyvykkyys arvioidaan olevan kohtalainen. - Lähde voi olla esimerkiksi osa tiedon vastaanottaneen viranomaisen luottamusverkostoa ollen esimerkiksi EU tai Nato-organisaatioiden/instituutioiden vastinpari. - Lähde ei kuulu tiedon vastaanottaneen viranomaisen yleisimpiin luottamusverkostoihin.

		- Lähde voi olla valtio, organisaatio tai esimerkiksi tietoturvatutkija. - Lähde voi olla myös jonkinlainen tietokanta, kuten haittaohjelma-analyysitietokanta (esim. Virustotal tai vastaava palvelu).
D	Lähde ei yleensä ole luotettava	- Lähde tiedetään. - Lähde on sellainen, jonka kanssa ei tehdä yhteistyötä säännöllisesti. - Lähteen tuottamaa tietoa voidaan tai ei voida arvioida pidemmältä aikaväliltä (eli luotettavuuden historia). - Lähteen toimittamat tiedot ovat harvoin paikkansapitäviä ja/tai oikea-aikaisia. Usein lähteen toimittama tieto on kuitenkin ollut virheellistä, paikkaansa pitämätöntä tai vanhentunutta. - Lähde on korjannut harvoin oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa. - Lähteen oma kyberkyvykkyys arvioidaan olevan alhaisella tasolla tai sen toimintaa ei tunneta tarkemmin. - Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista. - Lähde voi olla valtio, organisaatio tai esimerkiksi tietoturvatutkija.
E	Lähde on epäluotettava	- Lähde tiedetään tai kyseessä on uusi toimija, jota ei tunneta eikä taustaa voida arvioida tiedonsaantihetkellä. - Lähde ei ole reagoinut tiedon saaneen viranomaisen pyyntöihin esimerkiksi tietopyyntöihin, ilmoituksiin, sivujen alasajoon jne. - Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista. - Lähde tai siihen liitettävä toimija toteuttaa tai on toteuttanut Suomea kohtaan kyberoperaatioita/kyberhyökkäyksiä. - Lähteen tuottamaa tietoa ei voida arvioida pidemmältä aikaväliltä eli luotettavuuden historia on huono. - Lähteen toimittamat tiedot ovat hyvin harvoin paikkansapitäviä ja/tai oikea-aikaisia. Malkein aina lähteen toimittama tieto on ollut virheellistä, paikkaansa pitämätöntä tai vanhentunutta. - Lähde on korjannut hyvin harvoin oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa jättäen virheellisen tiedon voimaan. - Lähteen oma kyberkyvykkyys arvioidaan olevan alhaisella tasolla tai sen toimintaa ei tunneta tarkemmin. - Lähde voi olla valtio, organisaatio tai esimerkiksi tietoturvatutkija.
F	Lähteen luotettavuutta ei voida todentaa	- Lähde on entuudestaan täysin tuntematon - Lähde tiedetään, mutta lähde ei ole tuottanut tietoa, jonka luotettavuutta ei olisi voitu arvioida.

Lähteen määrittelyn osalta päästiin hyvin lähelle konsensusta ja tämä osio matriisista saatiin valmiimmaksi. Lähteen määrittelyssä nousi esille, kuinka monta, yksittäisessä kategoriassa määriteltyä kohtaa tulisi täyttyä, jotta tieto tai lähde vastaa kyseistä kategoriaa. Tämä on noussut useasti esille eri kierrosten aikana ja

tämä kerta ei tehnyt tästä poikkeusta. Pohdinta on oleellista, sillä osioita pitää voida tavalla tai toisella erottamaan toisistaan ja helpottamaan tiedon käsittelijän työtä tiedon tai lähteen luokittelussa. Aikaisemmalla kierroksella annetuissa vastauksissa noin kolmen kohdan täyttyminen oli riittävä, mutta määritelmien tarkentuessa ja laajentuessa ei kolme kohtaa ehkä olekaan enää riittävä panelistien mielestä. Myös eri vaihtoehtojen keskinäisriippuvuus toisiinsa on noussut eri palautteissa esille.

> ”Määritelmä on riittävä, mutta vain 2-3 osumaa ei ole. >50 % pitäisi täyttyä korkeimmalle tasolle. Tämä tietysti tarkoittaa, että kriteerin perusteella arvioinnin taustaoletukset pitäisi olla toisistaan riippumattomia eli kriteerit pitäisivät olla toisistaan riippumattomia. Esim. toinen ja 4 eivät ole toisistaan riippumattomia ja periaatteessa vain yhdellä taustaoletuksella (oikea aikaisempi oikea tieto) pääsee lähteenä jo 2 valintakriteerillä ylimpään luokkaan. Mitä enemmän kriteerien keskinäisriippuvuutta, sitä enemmän pitäisi olla lukumäärällisesti kriteereitä.”

Lähteen luotettavuuden arvioinnin jälkeen panelistit pääsivät antamaan palautetta päivitettyyn matriisiin tiedon luotettavuuden osalta. Päivitetty matriisi on esitetty taulukossa 15. Tiedon luotettavuuden määritelmät olivat toisissa kategorioissa selvästi vielä suppeampia kuin toiset ja tämä nostettiin vastauksissa myös esille. Kategoriassa 2. tiedon ollessa todennäköisesti totta kriteereitä oli vähemmän, kuin esimerkiksi kategorioissa 1. täysin uskottava / vahvistettu muista lähteistä ja 3. mahdollisesti totta, joka varmasti vaikuttaisi myös arviointiin ja käytettävyyteen.

TAULUKKO 15 Tiedon luotettavuus kolmas kierros

Tiedon luotettavuus		
1	Täysin uskottava / vahvistettu muista lähteistä.	- Täysin uskottava / vahvistettu muista lähteistä: - Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden matristo). - Tieto vaikuttaa loogiselta ja se voidaan varmentaa. - Tieto voidaan varmuudella todentaa eikä tiedon tarkkuudesta ole epäilystä. - Tieto kyetään omilla kyvyillä varmentamaan oikeaksi tai vääräksi ja/tai tieto on saatavilla toistettavasti - Esimerkiksi tekninen uhkatieto olisi toistettavissa omilla menetelmillä. - Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu. - Tieto on (tekninen) luotettavasti dokumentoitu tosiseikka, jota ei ole ollut mahdollista manipuloida tai tiedon manipulointi on erittäin epätodennäköistä.
2	Todennäköisesti totta	- Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo).

		- Tiedon paikkaansa pitävyys täydennetään muista lähteistä peräisin olevalla tiedolla ja tämä tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo). - Tieto vaikuttaa loogiselta. - Lähde on tuottanut tai havainnut tiedon itse ja tämä käy ilmi annetusta tiedosta tai ollut osana laajempaa verkostoa, jossa tieto on tuotettu.
3	Mahdollisesti totta	- Jos äskettäin raportoitu tieto ei ole ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa, vaikka vahvistus ei ole riittävää korkeamman todennäköisyyden määrittämiseksi. - Kyseessä on uusi tieto, jota ei ole vielä pystytty varmentamaan muista lähteistä. - Muu kerätty tieto ei ole ristiriidassa tiedon kanssa, mutta ei kuitenkaan riitä varmistamaan, että tieto on todennäköisemmin totta kuin ei totta. - Tieto vaikuttaa loogiselta, mutta sitä ei vielä ole voitu vahvistaa. - Tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo). - Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa vaan saanut tiedon omien verkostojen kautta tai osana laajempaa yhteistyötä. - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta.
4	Epäilyttävä	- Tieto ei vaikuta loogiselta, mutta voi mahdollisesti olla totta. - Lähde ei ole tuottanut tietoa itse tai tehnyt siihen liittyvää tietoturvatutkintaa. - Tieto voi olla peräisin (epä)luotettavasta lähteestä (lähteen luotettavuuden mittaristo). - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta. - Tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan, mutta tästä ei ole suoria indikaattoreita. - Tietoa ei vielä ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin.
5	Epätodennäköinen	- Tieto ei ole loogista ja/tai ristiriidat saadun tiedon osalta vaikuttavat, ettei saatu tieto ole uskottavaa. - Tieto voi olla tai on epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo). - Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta. - Tiedon tuottaneen menetelmät ovat tiedossa, mutta ne ovat todennäköisesti tapaukseen soveltumattomia ja tuottavat virheellistä tietoa. - On olemassa perusteltuja syitä, että tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan, vaikka asiaa ei ole varmuudella voitu todentaa. - Tietoa ei ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin.

6	Tiedon oikeellisuutta ei voida todentaa:	- Tiedon oikeellisuutta ei pystytä varmistamaan muista lähteistä tai omin menetelmin.

Erot eri kategorioiden välillä nousi esille myös panelistien palautteessa.

> ”onko suurin tietomassa tässä vai mahdollisesti pykälää alemmassa? Noudattaako tiedon luotettavuus normaalijakaumaa suhteessa tietomassaan ja jos, niin pitääkö vinoutunutta massaa korjata vastaamaan paremmin. Selkeästi pienempi kriteerien määrä joka tapauksessa vääristää tähän kohtaan tulevan tiedon määrää.”

Kolmannen kierroksen vastausten perusteella matriisista tehtiin vielä lopullinen versio, joka esitellään seuraavassa osiossa.

Kolmannen kierroksen lopussa oli vielä kaksi työn kannalta keskeistä kysymystä. Ensimmäisessä kysymyksessä kartoitettiin matriisin hyödyllisyyttä. Työssä tehty matriisi oli vielä luonnosvaiheessa, mutta kysymyksellä pyrittiin yleisesti selvittämään vastaajien mielipidettä tällaisen tai tämän tyylisen matriisin hyödyllisyydestä. Vastaajat pitivät matriisia hyvänä ideana, mutta määrittelytyötä tarvittaisiin vielä lisää, sekä jo aikaisemmin noussut tarve ohjeistukselle nousi myös tässäkin kohtaa esille.

> ”On ehdottomasti hyödyllinen. Eri viranomaisten käyttämät luokittelut eivät ole olleet yhteismitallisia. On tärkeää, että tiedon luokittelussa käytetään samoja työkaluja viranomaisten kesken. Toisaalta myös käytetyn matriisin soveltaminen on tapahtunut pitkälti subjektiivisista lähtökohdista eli lähteen ja tiedon luotettavuuden arviointi on perustunut arvioijan omiin käsityksiin kunkin portaan sisällöstä. On välttämätöntä, että eri tasojen kriteerit avataan ja käytäntöjä yhdenmukaistetaan.”

Yhtenä työn keskeisenä ajatuksena on ollut se, että yhteinen matriisi voisi mahdollisesti madaltaa kynnystä jakaa tietoa eteenpäin, sillä sen yhteydessä voisi laittaa oman arvion tiedosta ja lähteestä. Kybertoimintaympäristö muuttuu nopeasti ja tiedon jakaminen tässä nopeasti muuttuvassa toimintaympäristössä on tärkeää. Tietoakin tulee voida jakaa nopealla syklillä. Tämä saattaa tarkoittaa esimerkiksi sitä, että tiedon saanut viranomainen ei välttämättä ehdi tehdä itse tarpeellisia tarkistuksia, mutta pitää tiedon jakamista tärkeänä ja haluaa sen edelleen kotimaisille toimijoille. Vaikka jokainen viranomainen tekee omaa arvioitaan tiedon ja lähteen luotettavuudesta omien lähtökohtiensa mukaan, voi yhteinen matriisi antaa jonkinlaisen kuvan tiedosta.

> ”Kyllä. Yhtenäinen arviointikriteeristö edistää tiedon luotettavuuden yhdenmukaista arviointia ja siten parantaa tiedon jakamisen edellytyksiä. Tiedon vastaanottaja pystyy luottamaan tehtyyn arvioon tiedon ja lähteen luotettavuudesta ja tietää millä kriteereillä arvio on tehty. Ei siis tarvitse arvioida tiedon luovuttajan kyvykkyyttä luokitella tiedon ja lähteen luotettavuutta.”

5.4 Matriisin viimeinen versio

Kolmen haastattelukierroksen pohjalta matriisia muokattiin jokaisen haastattelukierroksen välissä ja panelistit saivat antaa palautetta päivitetystä versiosta. Myös viimeisen kierroksen palautteet käytiin läpi ja näiden pohjalta muodostettiin matriisin viimeinen versio työtä varten. Kuten jo aikaisemmin palautteiden pohjalta nousi esille, matriisin varsinainen käyttöönottaminen vaatisi sitä, että ne viranomaiset, jotka matriisia käyttävät osallistuvat matriisin määrittelytyöhön sekä luovat matriisia tukevan ohjeistuksen. Tämä matriisi voisi kuitenkin toimia pohjana ja keskustelun avaajana tässä työssä.

Kummassakin matriisin osissa oli havaittavissa kohtia, jotka tarkoittavat hyvin samaa asiaa tai olivat mahdollisesti ristiriidassa keskenään. Näitä osioita on myös muutettu lopulliseen matriisiin. Lopullisessa matriisissa on pyritty siihen, että kategoriat olisivat helposti keskenään verrattavissa. Tätä vertailtavuustyötä on tehty erityisesti tiedon luotettavuuden kategorioiden osalta, koska se jäi Delfoi-kierroksilla vajaaksi.

Matriisia tulisi mahdollisuuksien mukaan käyttää siten, että saadusta tiedosta poistetaan tai peitetään lähteen tiedot, kun tiedon vastaanottaja analysoi alkuun tiedon luotettavuutta. Tällä pyritään siihen, että arvio olisi mahdollisimman objektiivista ja arvio perustuisi vain tietoon. Kun tieto itsessään on arvioitu, saisi tiedon vastaanottaja tietää lähteen. Käytännön elämässä tämä on melko haastavaa, mutta mahdollisuuksien mukaan siihen olisi hyvä pyrkiä. Kun tiedon saajalla ei ole tietoa lähteestä, on tiedon arvioiminen objektiivisempaa.

Matriisin osalta lähteen luotettavuuden määrittelyssä onnistuttiin paremmin kuin tiedon määrittelyssä, vaikka lähteen määrittelyssä saatiinkin vahvistettua vain yksi kategoria ja tiedon osalta kategorioita saatiin vahvistettua kolme. Lähteen osalta matriisia saatiin rakennettua yhteismitallisemmaksi ja kohdista A-E saatiin rakennettua sellaiset, että lähteen arviointi olisi mahdollista ja matriisin avulla voidaan saada lähde sijoitettua oikeaan osioon. Lähteen määrittelyssä poistettiin kokonaan viittaukset organisaatioon ja tämän tiedon tulisi olla ohjeessa, joka matriisia varten tulisi rakentaa. Ohje kertoisi organisaatio tasolla, minkälaiset organisaatiot kuuluvat lähtökohtaisesti millekin tasolle, mutta samalla niitä arvioidaan yksittäisinä tapauksina ja myös muut seikat vaikuttavat siihen, mihin kategoriaan organisaatio tai verkosto kuuluu.

Lähteen osalta organisaatioiden tulisi määrittää omat listansa, jossa erityisesti tunnetut niin luotettavat kuin epäluotettavatkin lähteet on listattu. Näin lähteen arviointi ei jäisi yksistään tiedon vastaanottajalle vaan lähde arvioitaisiin organisaatiotasolla. Yhteisen ohjeistuksen mukaan lähteet arvioitaisiin säännöllisin väliajoin ja tämä dokumentoitaisiin. Tällä tavoin lähteestä alkaisi kertymään historiatietoa ja sen toimittamasta tiedosta ja tiedon oikeellisuudesta tai virheellisyydestä. Tällöin myös aikaisemmin luotettavan pidetty lähde, joka on toistuvasti toimittanut väärää tai virheellistä tietoa korjaamatta sitä, voitaisiin sijoittaa alempaan luottamuskategoriaan. Samaa ajatusta voisi käyttää myös lähteestä,

joka on aikaisemmin arvioitu epäluotettavaksi, mutta yhteistyön tiivistyessä ja tiedon ollessa oikeellista, se voitaisiin päivittää luotettavampaan kategoriaan.

Matriisin viimeinen versio on esitetty taulukoissa 16 ja 17. Merkittävä muutos aikaisempiin versioihin on otsikoinninmuutos. Matriisiin on lisätty mukaan ensimmäinen sarake, joka kuvaa tarkennusosioiden otsikoita. Lähteen osalta näitä osa-alueita tunnistettiin yhteisesti kuusi. Tämän lisäksi epäluotettavan kategorian alla kaksi tarkennusosiota lisää. Vastaava työ tehtiin myös tiedon luotettavuudelle, jossa tunnistettiin kuusi otsikkoa. Tämän avulla lähteen ja tiedon luotettavuuden kategorioista saatiin tehtyä yhtenäisemmät ja tämän avulla vertailtavuus eri kategorioiden välillä helpottuu.

TAULUKKO 16 Lähteen luotettavuus kybertoimintaympäristössä

Kategoria	A Lähde on luotettava	B Lähde on yleensä luotettava	C Lähde on melko luotettava	D Lähde ei yleensä ole luotettava	E Lähde on epäluotettava	F Lähteen luotettavuutta ei voida todentaa
Tunnettavuus	Lähde on tunnettu pidemmältä ajalta ja sen toimintatavat tiedetään.	Lähde on tunnettu jo jonkin aikaa ja yhteistyö on vakiintunutta tai lähes vakiintunutta.	Lähde tunnetaan, mutta sen kanssa ei vielä ole vakiintunutta yhteistyötä.	Lähde tiedetään, mutta yhteistyö sen kanssa ei ole säännöllistä.	Lähde tiedetään heikosti tai kyseessä on uusi toimija, jota ei tunneta eikä taustaa voida arvioida tiedonsaantihetkellä.	Lähde tiedetään tai on entuudestaan täysin tuntematon
Yhteistyön määrä	Lähde on sellainen, jonka kanssa tehdään säännöllisesti yhteistyötä.	Lähde on sellainen, jonka kanssa tehdään melko säännöllisesti yhteistyötä.	Lähde on sellainen, jonka kanssa tehdään silloin tällöin yhteistyötä.	Lähde on sellainen, jonka kanssa on tehty harvakseltaan yhteistyötä.	Lähde on sellainen, jonka kanssa ei ole tehty säännöllistä yhteistyötä.	Lähde ei ole tuottanut tietoa, jonka luotettavuutta ei olisi voitu arvioida.
Motiivi	Lähteen toiminnalla on hyvä tarkoitusperä/hyvä tahto.	Lähteen toiminnalla on tai ei ole hyvä tarkoitusperä/hyvä tahto.	Lähteen toiminnalla on tai ei ole hyvä tarkoitusperä/hyvä tahto.	Lähteen toiminnalla on tai ei ole hyvä tarkoitusperä/hyvä tahto.	Lähteen toiminnalla on tai ei ole hyvä tarkoitusperä/hyvä tahto.	
Raportointi historia	Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä.	Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä.	Lähteen tuottamaa tietoa voidaan arvioida pidemmältä aikaväliltä eli luotettavuuden historia on hyvä.	Lähteen tuottamaa tietoa voidaan tai ei voida arvioida pidemmältä aikaväliltä (eli luotettavuuden historia).	Lähteen tuottamaa tietoa ei voida arvioida pidemmältä aikaväliltä eli luotettavuuden historia on huono.	
Raportointi-laatu	Lähteen tuottama tieto on virheellistä hyvin harvoin/yksittäisissä tapauksissa.	Lähteen tuottama tieto on harvoin virheellistä.	Lähteen toimittamat tiedot ovat olleet useimmiten oikeita ja oikea-aikaisia, mutta välillä virheellisiä ja vanhentuneita.	Lähteen toimittamat tiedot ovat harvoin paikkansapitäviä ja/tai oikea-aikaisia. Usein lähteen toimittama tieto on kuitenkin ollut virheellistä, paikkaansa pitämätöntä tai vanhentunutta.	Lähteen toimittamat tiedot ovat hyvin harvoin paikkansapitäviä ja/tai oikea-aikaisia. Malkein aina lähteen toimittama tieto on ollut virheellistä, paikkaansa pitämätöntä tai vanhentunutta.	

Laadun-valvonta	Lähde on korjannut melkein aina oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa.	Lähde on korjannut usein oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa.	Lähde on korjannut joskus oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa.	Lähde on korjannut harvoin oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa.	Lähde on korjannut hyvin harvoin oma-aloitteisesti havaitsemansa virheet tai puutteet jakamassaan tiedossa jättäen virheellisen tiedon voimaan.	
Kyber-kyvykkyys	Lähteen oma kyberkyvykkyys arvioidaan olevan korkealla tasolla.	Lähteen oma kyberkyvykkyys arvioidaan olevan korkealla tasolla.	Lähteen oma kyberkyvykkyys arvioidaan olevan kohtalainen.	Lähteen oma kyberkyvykkyys arvioidaan olevan alhaisella tasolla tai sen toimintaa ei tunneta tarkemmin.	Lähteen oma kyberkyvykkyys arvioidaan olevan alhaisella tasolla tai sen toimintaa ei tunneta tarkemmin.	
Luottamus	Voidaan varmuudella sanoa, että poliittinen ohjaus ei tule jostain maan ulkopuolelta ja voi olla puolueellista.	Voidaan varmuudella sanoa, että poliittinen ohjaus ei tule jostain maan ulkopuolelta ja voi olla puolueellista.	Voidaan varmuudella sanoa, että poliittinen ohjaus ei tule jostain maan ulkopuolelta ja voi olla puolueellista.	Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista.	Voidaan myös epäillä, että maan poliittinen ohjaus tulee jostain maan ulkopuolelta ja voi olla puolueellista.	
Luottamus					Lähde ei ole reagoinut tiedon saaneen viranomaisen pyyntöihin esimerkiksi tietopyyntöihin, ilmoituksiin, sivujen alasajoon jne.	
Luottamus					Lähde tai siihen liitettävä toimija toteuttaa tai on toteuttanut Suomea kohtaan kyberoperaatioita/kyberhyökkäyksiä.	

TAULUKKO 17 Tiedon luotettavuus kybertoimintaympäristössä

Kategoria	1 Täysin uskottava / vahvistettu muista lähteistä	2 Todennäköisesti totta	3 Mahdollisesti totta	4 Epätodennäköinen	5 Epäilyttävä	6 Tiedon oikeellisuutta ei voida todentaa
Ristiinvarmistettavuus	Raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto ja tämä tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo).	Tiedon paikkaansa pitävyys täydennetään muista lähteistä peräisin olevalla tiedolla ja tämä tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo).	Jos äskettäin raportoitu tieto ei ole ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa, vaikka vahvistus ei ole riittävää korkeamman todennäköisyyden määrittämiseksi. Tieto ei ole peräisin epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo).	Raportoitu tieto on ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa. Tietoa ei ole aikaisemmin raportoitu ja vertailua ei voida tässä vaiheessa tehdä. Tieto voi olla peräisin (epä)luotettavasta lähteestä (lähteen luotettavuuden mittaristo).	Raportoitu tieto on ristiriidassa jo olemassa olevan tiedon kanssa tai aikaisemmin saadun tiedon kanssa tai tietoa ei ole aikaisemmin raportoitu ja vertailua ei voida tehdä.Tieto voi olla tai on epäluotettavasta lähteestä (lähteen luotettavuuden mittaristo).	Tiedon oikeellisuutta ei pystytä varmistamaan muista lähteistä tai omin menetelmin.
Tiedon loogisuus	Tieto vaikuttaa loogiselta.	Tieto vaikuttaa loogiselta.	Tieto vaikuttaa loogiselta, mutta sitä ei vielä ole voitu vahvistaa.	Tieto ei vaikuta loogiselta, mutta voi mahdollisesti olla totta.	Tieto ei ole loogista ja/tai ristiriidat saadun tiedon osalta vaikuttavat, ettei saatu tieto ole uskottavaa.	
Todennettavuus	Tieto kyetään omilla kyvyillä varmentamaan oikeaksi tai vääräksi ja/tai tieto on saatavilla toistettavasti eikä tiedon tarkkuudesta ole epäilystä.	Tieto kyetään omilla kyvyillä varmentamaan oikeaksi tai vääräksi ja/tai tieto on saatavilla toistettavasti	Tieto kyetään omilla kyvyillä varmentamaan oikeaksi tai vääräksi ja/tai tieto on saatavilla toistettavasti	Tietoa ei vielä ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin. Tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan, mutta tästä ei ole suoria indikaattoreita.	Tietoa ei ole voitu vahvistaa muista lähteistä ja/tai omin menetelmin. On olemassa perusteltuja syitä, että tieto saattaa olla tarkoituksella virheellistä ja pyrkiä johtamaan harhaan, vaikka asiaa ei ole varmuudella voitu todentaa.	

Todennettavuus	o Esimerkiksi tekninen uhkatieto olisi toistettavissa omilla menetelmillä.	o Esimerkiksi tekninen uhkatieto olisi toistettavissa omilla menetelmillä.	o Esimerkiksi tekninen uhkatieto olisi toistettavissa omilla menetelmillä.			
Läpinäkyvyys	Tiedossa on, minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevat menetelmät sopivat kyseisen tapauksen tutkimukseen.	Tiedossa on, minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevat menetelmät sopivat kyseisen tapauksen tutkimukseen.	Tiedossa on, minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta.	Tiedon tuottaneen menetelmät ovat tiedossa, mutta ne ovat todennäköisesti tapaukseen soveltumattomia ja tuottavat virheellistä tietoa.	Tiedossa ei ole minkälaisia tutkintamenetelmiä on käytetty ja/tai tiedossa olevien menetelmien soveltuvuus kyseisessä tapauksessa on kyseenalainen oman arvion pohjalta.	
Eheys	Tieto on (tekninen) luotettavasti dokumentoitu tosiseikka, jota ei ole ollut mahdollista manipuloida tai tiedon manipulointi on erittäin epätodennäköistä.	Tieto on tai ei ole (tekninen) luotettavasti dokumentoitu tosiseikka, jota on tai ei ole ollut mahdollista manipuloida.	Tieto on tai ei ole (tekninen) luotettavasti dokumentoitu tosiseikka, jota on tai ei ole ollut mahdollista manipuloida.	Tieto ei ole (tekninen) luotettavasti dokumentoitu tosiseikka, jota on ollut mahdollista manipuloida.	Tieto ei ole (tekninen) luotettavasti dokumentoitu tosiseikka, jota on ollut mahdollista manipuloida.	

5.5 Kyberturvallisuusjohtajan haastattelu ja matriisin kommentit

Työssä tehty matriisi esiteltiin valtion kyberturvallisuusjohtaja Rauli Paanaselle toukokuussa 2024. Tämän lisäksi hänelle esitettiin muutamia kysymyksiä tilannekuvaan ja tiedonvaihtoon sekä matriisiin liittyen. Haastattelu toteutettiin puolistrukturoituna haastatteluna ja sen aikana tehtiin muistiinpanot käydystä keskustelusta. Osa kysymyksistä oli suunniteltu etukäteen (liite 4) ja osa kysymyksistä syntyi osana keskustelua. Haastattelun tavoitteena oli lisätä näkökulmaa aihekokonaisuuteen, jota jo panelistien kanssa oli Delfoi-kierroksilla käsitelty.

Haastattelun aluksi käytiin taustoittava keskustelu, sillä Paananen ei saanut aineistoa etukäteen. Taustoittavassa keskustelussa käytiin vastaava tausta-aineisto läpi, jonka panelistit saivat itselleen eli amiraalikoodisto sekä 4x4-matriisi, jotka olivat työssä tehdyn matriisin pohjalla. Tämän lisäksi käytiin Firstin suosittelema matriisi läpi sekä työssä asiantuntijapaneelin kanssa tehty matriisi. Taustoituksen jälkeen siirryttiin keskustelemaan teemasta lähteen ja tiedon luotettavuus kybertoimintaympäristössä.

Taustoittavan aineiston käsittelyvaiheessa esille nousi eri viranomaisten rooli ja miten se huomioidaan esimerkiksi lähteen määrittelyssä. Tällä hetkellä matriisi ottaa lähteen osalta kantaa mahdolliseen poliittiseen ohjaukseen tai painostukseen, mutta Paanasen mukaan lähde voi olla myös riippumaton ilman erillistä poliittista ohjausta. Tällä hän tarkoittaa esimerkiksi sitä, että eri maissa kyberturvallisuuskeskukset on sijoitettu eri viranomaisten alle ja Suomen vastaava malli, jossa Kyberturvallisuuskeskus on täysin oma erillinen viranomainen ei ole niin yleinen. Mikäli Kyberturvallisuuskeskus on osana tiedusteluviranomaista, ei keskus pysty itsenäisesti päättämään, mitä tietoa se jakaa, vaan ohjaus tulee omasta organisaatiosta. Tämä vaikuttaa myös toimimiseen esimerkiksi Euroopan yhteisten kyberturvallisuuskeskusten verkostossa, jossa monesti tietoa pystytään jakamaan kansainvälisesti hyvin laajasti ja myös matalalla kynnyksellä. Jos organisaation tiedonjakoa rajoitetaan, niin tällöin se ei toimi yhteisten pelisääntöjen mukaan.

Toinen seikka, joka taustamateriaalin läpikäynnissä nousi esille, oli MISP. eli Malware Information Sharing Platform. Kyseessä on työkalu, jonka avulla voi jakaa haittaohjelmatietoa. Jo aikaisemmin teoriaosuudessa on työssä kerrottu, että amiraalikoodiston käyttö MISPissä on mahdollista, mutta sitä käytetään hyvin vähän tai ei ollenkaan. Saman näkökulman nosti esille myös Paananen, joka korosti, että lähteen ja tiedon luokittelu tällaisissa työkaluissa on tärkeää, jotta suurta tietomassaa pystytään arvioimaan nopeasti ja hyödyntämään sieltä oleellista tietoa. Mikäli MISPistä nostetaan väärää tietoa ja tehdään siitä virheellistä tulkintaa voi tämä Paanasen mukaan johtaa työtä tai tutkintaa väärille urille, jonka seurauksena tehdään turhaa työtä. Väärä tieto saattaa myös vaikuttaa lähteen luotettavuuteen.

Tausta-aineiston läpikäymisen jälkeen siirryttiin varsinaiseen kysymysosioon. Haastattelun aluksi keskusteltiin siitä, hyödyntävätkö suomalaiset

viranomaiset nykyisin yhteistä lähteen ja tiedon luotettavuudenmatriisia vaihtaessaan tietoa kyberkontekstissa. Paanasen vastaus oli lyhyt ja ytimekäs, ”Ei ole”.

Taustalle hän kertoi, että ensimmäisen kyberturvallisuusstrategian julkaisun jälkeen, kun esimerkiksi Kyberturvallisuuskeskusta perustettiin, käytiin keskustelua siitä, että tietoa voitaisiin merkitä yhteisellä tavalla, joka olisi sama kaikilla viranomaisilla. Tällöin haasteena nähtiin se, että yhteistä matriisia on vaikea löytää ja osa viranomaisista hyödyntää jo jotain toista matriisia omassa toiminnassaan. Vaikka tällaiseen tiedon ja lähteen luokitteluun ei päästy, nostaa Paananen TLP-luokittelun eli Traffic Light Protocol -käsittelyluokituksen, jota esimerkiksi Kyberturvallisuuskeskus käyttää. TLP-luokittelussa jaettu tieto luokitellaan viiteen kategoriaan, joka määrittelee sen, miten vastaanottaja tietoa voi käyttää ja jakaa edelleen. (esim. Kyberturvallisuuskeskus, 2023.) TLP-luokittelu on aikoinaan otettu käyttöön yhteisesti ja Paananen pohtii, että miksi tiedon ja lähteen luotettavuudesta kertovaa matriisia ei voitaisi samalla tavalla ottaa käyttöön, kun TPL-luokittelukin on saatu otettua käyttöön. Tämä toki vaatii työtä eikä ole ehkä niin yksinkertaista, mutta ei myöskään mahdotonta.

Paanasen mukaan yhteinen matriisi tiedon ja lähteen luotettavuudesta voisi madaltaa kynnystä tiedon jakamiselle. Keskeistä on, että matriisin käyttö on ohjeistettu yhtenäisesti kaikkien sitä käyttävien organisaatioiden kesken. Ohjeen tulisi olla myös elävä dokumentti, jota päivitetään erilaisten käyttötapauksen syntyessä. Tämä olisi hyödyllistä erityisesti epävarmojen tapausten osalta. Tällaiset esimerkit auttavat yksittäistä asiantuntijaa merkitsemään tietoa oikein ja tulkitsemaan matriisia. Ohjeiden ja niiden tekemisen merkitys korostui myös panelistien vastauksessa aikaisemmin.

Haasteena Paananen näkee matriisin käyttövaikeuden. Mikäli matriisin käyttö on tehty hankalaksi, ei sitä tulla käyttöön ottamaan. Tämän todettuaan hän pohtii, että taustalle voitaisiin luoda pisteytys tai mittari, joka antaa lähteelle ja tiedolle pisteet, jonka jälkeen ne saavat tietyn arvon ja tuottavat koodin esimerkiksi ”A1”. Tämä on hyvin samankaltainen havainto, jonka myös panelistit nostivat omissa vastauksissaan esille. Tähän voitaisiin lähteä soveltamaan 5x5x5-matriisin ajatusta, jolloin tiettyyn kategoriaan pääsee, kun saa tietyn pistemäärän ja tässä voidaan myös tehdä painotuksia kategorioiden eri osa-alueiden välillä. Esimerkiksi 5x5x5-matriisissa luotettavalla lähteellä on hyvä historiatieto aikaisemmin tuotetun tiedon perusteella, joka nostaa sen saamaa pistemäärää ja näin ollen luotettavuutta.

Vaikka työssä tehty matriisi on ajateltu viranomaisten käytettäväksi, Paananen nostaa esille elinkeinoelämän, joka vahvasti vastaa Suomen kyberturvallisuudesta. Tiedon vaihtaminen ja jakaminen yritysten kanssa on tärkeää, jotta kokonaistilannekuvaa voidaan muodostaa. Paananen näkee, että matriisi voisi olla hyödyllinen erityisesti tällaisessa tiedonvaihdossa. Matriisin avulla viranomainen voisi jakaa yritykselle myös epävarmaa tietoa. Nopeasti muuttuvassa kybertoimintaympäristössä nopealle tiedonvaihdolle on tarvetta ja silloin myös epävarmaa tietoa tulisi voida jakaa. Omassa pohdinnassaan Paananen nostaa esille, että matriisi saattaisi olla helpommin otettavissa käyttöön esimerkiksi

Kyberturvallisuuskeskuksen ja elinkeinoelämän tiedonvaihdossa kuin viranomaisten tiedonvaihdossa.

6 TULKINTA JA POHDINTA

Laadullisen tutkimuksen tärkein tavoite on saavuttaa mahdollisimman rikas ja syvällinen käsitys tutkimuskohteena olevasta ilmiöstä (Puusa ja Julkunen, 2010, 195). Tutkimusaineiston keruu Delfoi-menetelmää hyödyntäen osoittautui hyväksi valinnaksi. Työtä olisi voitu tehdä erillisessä työpajassa, mutta asiantuntijoiden saaminen samaan aikaan paikalle yhdeksi kokonaiseksi päiväksi tai useammaksi päiväksi, olisi ollut todennäköisesti erittäin haastavaa. Delfoi-paneeli mahdollisti ajasta ja paikasta riippumattoman osallistumisen työhön. Useampi haastattelukierros mahdollisti sen, että matriisia saatiin käsiteltyä pidempään ja sitä pystyttiin jokaisen kierroksen jälkeen päivittämään ja tuomaan uusia näkökulmia aiheeseen. Myös avoimet kysymykset olivat tärkeitä, sillä niiden avulla panelistien näkemyksiä saatiin syvennettyä. Matriisin kommenteissa havaitut nostot saatettiin muuttaa seuraavalla kierroksella vielä tarkemmaksi kysymykseksi ja saada yhteistä laajempaa näkemystä rakennettua sekä vietyä matriisin määrittelytyötä eteenpäin.

Jokaisessa kategoriassa oli mukana monivalinta, jossa panelisti saattoi valita, että esitetty määritelmä on riittävä, tai sitä tulee täydentää. Oli myös mahdollista valita, ettei osaa sanoa. Erityisesti silloin, jos panelisti vastasi, ettei määritelmä ole riittävä, pyydettiin tätä vastausta täydentämään, jotta seuraavalla kierroksella voitaisiin kehitys- tai korjaustarpeet huomioida. Vaikka jokaiseen kysymykseen muodostui monivalinnan kautta myös numeerista aineistoa, ei tämän käsittely ollut keskeistä työn kannalta. Linturi ym. (2019) nostavat esille, että jakaumadataa olennaisempaa on se kvalitatiivinen asiantuntijatieto, jota tutkimuksessa syntyy. Joissain tilanteissa yli 50 prosenttia vastaajista saattoi olla sitä mieltä, että määritelmä on hyvä, mutta pienempi joukko toi kommenttien valossa hyviä ja tärkeitä havaintoja esille siitä, että kategoriaa on syytä täydentää. Tällainen aineiston tulkintatapa mahdollisti sen, että yksittäisiä argumentteja, kommentteja ja dialogia pystyttiin huomioimaan paremmin.

Matriisin kehittelyvaiheessa vahvistui, ettei aikaisemmat matriisit sopisi kybertoimintaympäristöön sellaisenaan, sillä ne painottuvat vahvasti henkilötiedusteluun erityisesti matriiseihin liitettyjen tarkenteiden osalta. Kybertoimintaympäristössä tietoa koostuu hyvin eri tavalla, jolloin se voi olla henkilön

välityksellä saatavaa tietoa, mutta tätä enemmän kyse on teknisestä tiedosta, jota vastaanotetaan ja käsitellään eri tavalla. Tämän takia myös panelistien asiantuntijuus kybertoimintaympäristöstä oli avainasemassa, sillä nopeasti kategorioihin haluttiin lisätä teknisten tunnisteiden määrittelyjä, jotta ne palvelisivat paremmin kybertoimintaympäristöön suunniteltua matriisia.

Matriisin osalta lähteen määrittelyssä päästiin hyvin pitkälle. Lähteen määrittely eri kategorioissa kehittyi jokaisella kierroksella ja löydettiin yhteismitallisia määritelmiä, jotka saatettiin muuttaa siten, että ne kuvaavat lähteen luotettavuutta luotettavasta epäluotettavaan. Samalla tämä mahdollisti sen, että eri kategorioiden ollessa saman sisältöisiä, olisi niiden käytettävyys selkeämpää ja helpompaa. Tällöin matriisia käyttävä henkilö voisi helpommin löytää sopivan kategorian lähteelle.

Tiedon osalta määrittelytyö oli vaikeampaa ja määrittelytyö jäi osittain kesken. Tätä varten olisi tarvittu lisää kierroksia tai keskustelua siitä, miten sisältöä saadaan päivitettyä paremmin, jotta eri kategoriat eroaisivat tarpeeksi toisistaan. Tämän avulla saatu tieto olisi helppo arvioida matriisin avulla, jotta sen voisi laittaa sopivaan kategoriaan. Tämän takia kolmannen kierroksen jälkeen tiedon luotettavuuden kategorioita päivitettiin huomattavasti enemmän kuin esimerkiksi lähteen. Tiedon luotettavuuden kategorioissa tekninen ulottuvuus korostui erityisesti, sillä tieto, jota kybermaailmassa liikutetaan, on useasti teknistä ja näin ollen tiedon oikeellisuus ja sen tarkistaminen omin keinoin sekä se, ettei tietoa ole muutettu korostuivat eri kategorioiden palautteissa. Tämä pyrittiin huomioimaan matriisin eri kategorioissa.

Kolmannella ja samalla viimeisellä Delfoi-kierroksella kysyttiin työn kannalta oleellinen kysymys, onko tämänlaisesta matriisista hyötyä ja voitaisiinko se ottaa käyttöön. Tällä hetkellä suomalaiset kyberviranomaiset eivät käytä yhteistä tiedon ja lähteen luotettavuuden matriisia ja tämä tarkoittaa myös sitä, että luokittelut eivät ole yhteismitallisia. Vastaajat suhtautuivat matriisiin ja sen tuomiin hyötyihin poistiivisesti. Kommentit matriisin yhteismitallisuuteen ja vertailtavuuteen sekä siihen tehtävään erilliseen ohjeistukseen tulisi kuitenkin huomioida ennen käyttöönottoa.

Delfoi-kyselyssä ei myöskään kysytty hyödyntävätkö panelistit tai ovatko he hyödyntäneet aikaisemmissa työtehtävissään kansainvälisiä mittareita, kuten amiraalikoodistoa tai 4x4-matriisia, joita lähdeaineiston perusteella eri maiden viranomaiset hyödyntävät. Erilaiset kansainväliset matriisit tulisi huomioida, jos suomalaiset viranomaiset ottavat yhteisen oman tiedon ja lähteen luotettavuutta käsittelevän matriisin käyttöön, jotta tiedon jakaminen kansainvälisille verkostoille olisi helppoa ja kategoriat muunnettavissa toiseen matriisin sopivaksi. Tästä tehtiin työn teoriaosiossa esimerkki, kun amiraalikoodisto ja 4x4-matriisi yhdistettiin.

Yhteisen matriisin tavoitteena olisi myös madaltaa tiedon jakamista, sillä matriisin avulla viranomainen voisi viestiä muille viranomaisille, joille tieto jaetaan, että sitä ei ole esimerkiksi voitu vahvistaa, mutta lähdettä pidetään luotettavana. Tällaisessa tilanteessa tieto saataisiin nopeasti jaettua, mutta siihen saataisiin myös niin kutsuttu vastuuvapautuslauseke, jolla tiedon edelleen jakava

viranomainen voisi kertoa, ettei tietoa ole voitu vahvistaa. Tieto nähdään kuitenkin tärkeänä ja se halutaan pian jakoon, eikä odottaa varmistusta.

Vaikka määrittelytyötä ei saatu valmiiksi ja muodostettua yhteistä konsensusta jokaisen kategorian osalta, työssä saavutettiin saturaatiopiste. Kolmannella kierroksella, ei syntynyt enää uusia näkökulmia tai havaintoja. Palautteet käsittelivät erityisesti matriisin käytettävyyttä, joka on erittäin keskeinen palaute muotoiluiden lisäksi.

Panelistit muodostivat kattavan vastausjoukon eri hallinnonalojen edustajista. Vastausten perusteella näkyi myös eri viranomaisten rooli kybertoimintaympäristössä. Eri toimijat tekevät työtä eri toimivaltuuksilla. Tämä näkyi panelistien antamissa vastauksissa erityisesti tiedon luotettavuuden määrittelyissä. Toiset olivat vastausten perusteella varautuneempia ja esimerkiksi menetelmiä, jolla tieto on tuotettu, koettiin olevan vaikea saada, koska toimijat eivät sellaista tietoa jaa. Toiset taas näkivät menetelmien jakamisen mahdollisuutena ja nostivat ne omissa vastauksissaan esille, sillä hallinnonalalla tiedonjaossa totuttu avoimempaan tiedonvaihtoon.

Matriisin jäi kirjaus lähteen hyvästä tahdosta, vaikka siitä ei oltu yksimielisiä. Sanamuotoilu voi olla vaikuttavatekijä tässä, sillä avoimissa vastauksissa nousi esille se, että lähde voi tehdä virheitä, mutta jos voidaan osoittaa, että virhe ei ole tahallinen, ei se vaikuta lähteen luotettavuuteen merkittävästi, kun taas selvästi virheellistä ja väärä tietoa tarkoituksella jakava lähde menettää luottamuksensa. Tässä tehdään eroa juuri mis- ja disinformaation välille. Kybertoimintaympäristö muuttuu nopeasti ja virheellistä tietoa saattaa jakaa vahingossa. Mikäli lähde havaitsee virheen ja korjaan sen, ei tästä tule rangaista ja samalla kannalla olivat panelistit.

Useassa vastauksessa eri kierroksilla ja eri kategorioiden kohdalla nousi esille matriisin käytettävyys ja se, miten lähdettä ja tietoa voitaisiin arvioida ja pisteyttää. Pisteiden perusteella voitaisiin lähde ja tieto sitten sijoittaa tiettyyn kategoriaan, joka vastaa pistemäärää. Panelistit eivät saaneet 5x5x5-matriisia osana ennakkomateriaalia ja tämä olisi varmasti ollut hyödyllistä jakaa se heille osana ennakkomateriaalia, sillä moni haki vastauksissaan vastaava mallia matriisille, joka löytyi jo olemassa olevasta pohjasta. Näin ollen 5x5x5-matriisi olisi ollut hyödyllistä olla ennakkomateriaalissa ja tehtyä matriisia olisi voitu suunnitella heti alusta asti sen mukaan.

Osana 5x5x5-matriisia oli myös historiatieto. Lähteen luotettavuuden osalta tärkeää oli se, että se tunnettiin pitkältä ajalta ja sen tuottamasta tiedosta oli muotoutunut jo jonkinlainen näkemys, jonka perusteella voitiin arvioida, oliko jaettu tieto oikeanlaista ja oikea-aikaista. Tämä pyrittiin huomioimaan matriisin viimeisessä versiossa, jossa lähteen historia vaikutti niin lähteen kuin tiedon luotettavuuteen.

6.1 Tutkimuksen luotettavuuden tarkastelu

Koska matriisin määrittelyn kanssa ei lähdetty nollasta vaan panelistit saivat valmiin luonnoksen, on tämä mahdollisesti ohjannut heidän vastauksiaan ja näin ollen on mahdollista, että joku osa-alue tai havainto on jäänyt kokonaan pois. Panelisteille annettiin etukäteen aineistona tiivistelmät amiraalikoodistosta sekä 4x4-matriisista, joiden perusajatuksen pohjalta matriisia kybertiedonvaihtoon soveltuvaa tiedon ja lähteen luotettavuuden matriisia lähdettiin rakentamaan. Osalle vastaajista esimerkkimatriisit olivat tutumpia kuin toisille. Koska kybertoimintaympäristö poikkeaa esimerkiksi perinteisestä henkilötiedustelusta, ei ollut keskeistä, että panelistit olisivat olleet syväosaajia esimerkkimatriisien käyttäjiä vaan ymmärrys kybertoimintaympäristöstä oli työn kannalta oleellisempaa.

Panelistit osallistuivat kyselyyn yksityishenkilöinä, vaikka he ovat tällä hetkellä tai ovat olleet sellaisilla hallinnonaloilla töissä, joiden käyttöön matriisia on suunniteltu. Tämä valinta tehtiin, jotta aineiston kerääminen olisi verrattain nopeaa. Jos panelistit olisivat edustaneet virallisesti niitä tahoja, joille matriisi on suunniteltu, olisi vastaukset pitänyt todennäköisesti hyväksyttää organisaation prosessin mukaan. Silloin ne olisivat olleet organisaation vastauksia eivätkä yksittäisen henkilön. Tämä toki olisi mahdollistanut sen, että organisaatiot olisivat matriisin tekemisessä mukana. Kääntöpuolena tälle olisi ollut todennäköisesti hitaampi aikataulu.

Puusa ja Juuti (2020, 101) tuovat esille, että laadullinen tutkimus on käsiteherkkää ja jo aineiston keruuvaiheessa tutkija saattaa ohjata omilla sanavalinnoillaan tai käsitteillä huomaamattaan aineistoa tiettyyn suuntaan, jos tähän ei kiinnitä riittävää huomiota. Samalla myös tutkijan oma näkemys saattaa ohjata niitä valintoja, joita hän aineistoista nostaa esille. Laadullinen tutkimus onkin luonteelta vuorovaikutteista eikä puhtaan tiedon esille kaivamista. Tutkimuksen päämäärät vaikuttavat siihen, millaista aineistoa tutkija tutkimukseensa kerää.

Laadullisesta aineistosta on haasteellista tehdä tieteellisesti kestäviä johtopäätöksiä (Puusa 2010, 145). Aineisto, joka työssä on syntynyt, on sisällöltään vivahteikas ja panelistit ovat nostaneet erilaisia näkökulmia esille oman asiantuntijuuden pohjalta. Näitä on pyritty nostamaan työssä esille, kuitenkin siten, että tutkimuskysymys ja sen tavoitteet ovat olleet keskiössä. Mikäli kysely tehtäisiin uudelleen eri vastaajajoukolla, sen toistettavuus olisi haastavaa, sillä jokainen panelisti vastasi henkilökohtaisesti kyselyyn ja oman osaamisensa ja asiantuntijuutensa pohjalta. Näin ollen eri vastaajajoukko saattaisi antaa erilaisia vastauksia, mutta ainoastaan kyselyn toistaminen voisi osittaa kuinka erilaiset vastaukset lopulta saataisiin.

6.2 Havaitut kehitystarpeet ja mahdolliset jatkotutkimusaiheet

Pelkkä matriisi, jota työssä lähdettiin tekemään ei riitä. Matriisi tarvitsee tämän lisäksi erillisen ohjeistuksen, jossa eri kategoriat avataan tarkemmin ja kerrotaan

perusteet, miten tieto tai lähde kuuluu tiettyyn kategoriaan. Ohjeessa voidaan myös avata tarkemmin esimerkiksi sitä, minkä tyylisiä lähteitä kategoriaan voisi kuulua. Alussa matriisi sisälsi organisaatioita, mutta ne poistettiin lopulta viimeisestä versioista kokonaan. Organisaatiotieto olisit sellaista tietoa, joka kuuluu erilliseen ohjeistukseen. Organisaatioita käsittelevä ohjeistus olisi tärkeä tehdä yhteistyössä niiden toimijoiden kanssa, jotka matriisia käyttävät. Tämän lisäksi ohjeeseen voitaisiin laittaa erilaisia tapausesimerkkejä, jotka helpottavat matriisin käyttöä.

Ohjeen tulisi olla myös elävä dokumentti, kuten valtion kyberturvallisuusjohtaja haastattelussaan totesi luvussa 5.5. Ohjetta tulisi päivittää, kun erilaisia käyttötapauksia syntyy. Tämä olisi hyödyllistä erityisesti epävarmojen tapausten osalta. Tällaiset esimerkit auttavat yksittäistä asiantuntijaa merkitsemään tietoa oikein ja tulkitsemaan matriisia. Näiden tapausten läpikäyminen ja niiden vaikutukset matriisiin olisivat myös omia tarkastelevia kokonaisuuksiaan, joita voi tehdä, kun tapauksia kertyy tarpeeksi.

Tiedon luotettavuutta määritellessä myös tekniset työkalut ja tiedon luotettavuuden tunnistaminen on oleellista. Viranomaisten tulee voida käyttää samoja työkaluja tiedon luotettavuutta arvioitaessa. Valtion kyberturvallisuusjohtaja ja eräs panelisti nostivat vastauksissaan esille saman havainnon. Matriisi tulisi ottaa osaksi myös viranomaisen käyttämiä työkaluja, kuten MISPiä, jossa luokittelu voitaisiin tehdä pakolliseksi. Tätä voitaisiin myös osin automatisoida, joka helpottaisi tapausten selvittämistä, tutkimista ja jakamista. Tämä on osaltaan oma ja erillinen määrittelytyö, joka tulisi tehdä. Vaikka MISPissä on tiedon luotettavuudesta kertova ominaisuus, vaatisi sen käyttöönotto ohjeistusta ja esimerkkitapauksia.

Useampi panelisti nosti esille jonkinlaisen pisteytyksen tai tarpeen saada ohjeistusta siitä, kuinka monen kohdan tulisi täyttyä, jotta lähde tai tieto sijoitetaan tiettyyn kategoriaan. Toisella kierroksella asiaa kysyttäessä erillisellä kysymyksellä panelistien arvioin mukaan kaksi tai kolme kohtaa tulisi täyttyä, jotta tieto tai lähde voidaan sijoittaa tiettyyn kategoriaan. Kuten eräs panelisti nosti hyvin omassa vastauksessaan esille korkeimman luokituksen saavan tiedon tai lähteen osalta ei kaksi tai kolme kohtaa riitä, vaan vähintään puolet kategorian vaatimuksista tulisi täyttyä. Mikäli matriiseista saadaan rakennettua sellaiset, että niissä on samantyylinen kohta, joka vahvistuu tai heikkenee sen myötä, onko kyseessä esimerkiksi luotettava tai epäluotettava lähde, olisi pisteytys helpompaa. Tällöin matriisissa voitaisiin helpommin soveltaa 5x5x5-matriisin ajatusta, jossa esimerkiksi lähde saa pisteitä ja pistemäärän ja täytettyjen kohtien mukaan se saisi tietyn kategorian arvon. Yhtenäisempi malli auttaisi myös lähteen tai tiedon käsittelijää laittamaan sen oikeaan kategoriaan helpommin ja nopeammin.

Helppokäyttöisyys on myös tärkeä kehityskohde matriisille. Valtion kyberturvallisuusjohtajan ehdotus automatisoinnista hyödyttäisi varmasti käyttäjiä ja helpottaisi määrittelytyön tekemistä. Tämä toimisi aluksi varmasti perustyökaluilla, kuten Excelillä, mutta pidemmällä aikavälillä taustalle voitaisiin tehdä oma sovellus.

Lainsäädäntö oli rajattu tämän työn ulkopuolelle kuten työn alussa (luku 2.2) todettiin. Aihe kuitenkin nousi panelistien kommenteissa esille. Tiedonvaihtaminen edellyttää ajantasaista lainsäädäntöä ja sitä, että laissa mahdollistetaan viranomaisten välinen tiedonjako ketterästi. Tämä asia nousi esille myös Selvityksessä viranomaisten toimintaedellytyksistä kyberturvallisuudessa (2023), jossa osana tilannekuvaa ja tietojenvaihtoa, on tarkastelu tämän hetken lainsäädäntöä ja sitä, millaisia muutoksia se vaatisi, jotta tiedonvaihto viranomaisten välillä olisi helpompaa.

7 YHTEENVETO

Työn tarkoituksena oli selvittää, minkälainen lähteen ja tiedonluotettavuuden matriisi olisi sopiva kybertiedonvaihtoon. Pääkysymyksen avuksi otettiin kaksi alakysymystä, joiden avulla pääkysymykseen pyrittiin vastaamaan. Työssä selvitettiin aluksi, miten jo olemassa olevista matriiseista, kuten amiraalikoodisto, 4x4- ja 5x5x5-matriisi, voisi rakentaa kybertiedonvaihtoon sopivaa lähteen ja tiedon luotettavuudesta kertovaa matriisia. Tämän lisäksi pyrittiin selvittämään, miten lähteen ja tiedon luotettavuutta kuvaava matriisi tulisi määritellä, jotta se palvelisivat parhaalla mahdollisella tavalla eri toimijoita. Työn fokuksessa olivat suomalaiset kyberturvallisuusviranomaiset ja kybertoimintaympäristö.

Olemassa olevat matriisit, amiraalikoodisto, 4x4- ja 5x5x5-matriisi eivät suoraan ole sovellettavissa lähteen ja tiedon luotettavuuden matriisiksi kyberympäristössä tapahtuvaan tiedonvaihtoon, sillä niiden kuvaukset ja tarkennukset sopivat paremmin henkilötiedusteluun. Amiraalikoodiston kuusi kategoriaa olivat pohjana työssä tehdylle matriisille ja tämän takia sen luokat otsikkotasolla sopivat hyvin pohjaksi, kun määrittelytyötä aloitettiin. Henkilötiedustelun sijaan kategorioiden kuvauksiin haluttiin lisätä elementtejä, jotka toimivat erityisesti tiedon jaossa sähköisessä toimintaympäristössä, jossa tieto liikkuu tietoverkkoja pitkin ja muodostuva aineisto on suullisen tai paperilla saatavan tiedon lisäksi myös teknistä.

Julkisista lähteistä saadun tiedon perusteella, ei suomalaiset viranomaiset käytä tällä hetkellä yhteistä matriisia lähteen ja tiedon luotettavuuden merkitsemiseksi. Tämä tieto vahvistui valtion kyberturvallisuusjohtaja Paanasen haastattelussa, että yhteistä matriisia ei ole. Keskustelua tästä on aikoinaan käyty, mutta lähivuosina sitä ei ole ollut. Firstin tekemän julkaisun perusteella kyberturvallisuusjohtaja Paananen näki, että keskustelu olisi syytä jälleen aloittaa. Hän nosti kuitenkin esille sen, että matriisi voisi olla helpommin otettavissa käyttöön esimerkiksi Kyberturvallisuuskeskuksen ja elinkeinoelämän välillä jaettuun tietoon kuin viranomaisten väliseen tiedonvaihtoon. Tässä työssä elinkeinoelämä oli rajattu ulkopuolelle ja paneeli, jonka kanssa matriisia rakennettiin, muodostui eri hallinnonalan edustajista. Paananen nosti kuitenkin esille, että työssä tehty

matriisi olisi tässäkin hyvä pohja elinkeinoelämän kanssa tehtävään tiedonvaihtoon ja keskustelun avaus.

Niin panelistit kuin valtion kyberturvallisuusjohtaja näkivät matriisin hyödyllisenä ja tarpeellisena työkaluna tiedon vaihtamiselle. Määrittelytyötä matriisin sisällöstä ja sen tarkemmasta ohjeistuksesta tulisi jatkaa niiden toimijoiden kesken, jotka ottavat sen käyttöönsä. Matriisi tulisi rakentaa kategorioiden osalta mahdollisimman yhteismitalliseksi, jotta vertailtavuus niiden välillä olisi helppoa. Tämän lisäksi matriisia käyttävien organisaatioiden tulisi määritellä yhteinen ohje, jota kaikki noudattaa. Amiraalikoodiston osalta on havaittu, että sitä käytetään monenkirjavalla tavalla ja saman valtion sisällä kaksi eri viranomaista saattavat tulkita tietoa ja lähdettä hyvin eri tavalla ja näin ollen ne saavat eri arvot. Yhteisen ohjeistuksen avulla tätä pystyttäisiin välttämään. Tärkeää olisi myös, kuten valtion kyberturvallisuusjohtaja nosti esille, että ohje olisi elävädokumentti. Epäselvissä tapauksissa niistä voitaisiin keskustella ja ne voitaisiin laittaa osaksi ohjetta ja kerrottaisiin, miten tietoa ja lähdettä kyseisessä tapauksessa tulkittiin. Tämä auttaisi myös asiantuntijaa, joka matriisia työssä hyödyntää.

Tiedon luotettavuutta määritellessä myös tekniset työkalut ja tiedon luotettavuuden tunnistaminen ovat oleellista. Viranomaisten tulee voida käyttää samoja työkaluja tiedon luotettavuutta arvioitaessa. Samalla matriisi tulisi huomioida osana näitä työkaluja. Tiedon merkitseminen esimerkiksi MISPissä tulisi olla pakotettuna ja osa prosessia.

Matriisin käyttöä voitaisiin helpottaa myös siten, että siitä rakennettaisiin 5x5x5-matriisin kaltainen, jolloin tiedon ja lähteen luotettavuuden osalta eri kategoriat sisältävät pisteitä. Kun tietty lähde saavuttaa tietyn pistemäärän se saisi oman arvonsa. Vastaavasti tiedon osalta käytäisiin sama läpi ja sille muodostuu oma pisteensä. Näiden pisteiden perusteella muodostuu ne kategoriat, joihin lähde ja tieto kuuluvat ja tälle muodostuu oma koodinsa esimerkiksi ”B3”, jolloin lähdettä pidetään melko luotettavan ja sen tuottama tieto on mahdollisesti totta.

Työssä lähdettiin aluksi selvittämään jo käytössä olevien matriisien soveltuvuutta. Vaikka ne eivät täysin sovellu kybertoimintaympäristöön, on tärkeää, että tehdystä matriisista löytyy vastaavuudet jo olemassa olevien matriisien kanssa ja tieto tai lähde on helposti käännettävissä taulukosta toiseen. Tämä helpottaa organisaation työtä silloin, jos kansainväliset verkostot käyttävät eri matriisia tiedon ja lähteen luotettavuuden ilmaisemiseksi.

Firstin julkaisema (2023) suositus tiedon ja lähteen luotettavuuden merkitsemiseksi vahvistaa sitä, että vastaava matriisi tulisi ottaa käyttöön myös Suomessa. Tämä ei kosketa vain viranomaisia tai vain elinkeinoelämää vaan matriisi helpottaa tiedon ja tilannekuvan vaihtoa erityisesti silloin, kun se on kaikilla toimijoilla sama. Tämä vaatii työtä ja tulee integroida osaksi muuta työtä tiedon ja tilannekuvan vaihtamisessa. Edellisestä keskustelusta on kulunut noin 10 vuotta aikaa ja kybertoimintaympäristö ja sen merkitys ovat kehittyneet tänä aikana merkittävästi. Tämän takia aika voisi olla jälleen kypsä sille, että keskustelua aloitetaan uudelleen lähteen ja tiedon luotettavuuden matriisin käyttöönottamiseksi.

LÄHTEET

A Joint Cybersecurity Operations Platform for EU's CSIRT network (2023). Cyber threat Intelligence – A necessity, not a luxury. Luettu 3.5.2024 https://www.linkedin.com/pulse/cyber-threat-intelligence-necessity-luxury-jcop-eu

Alastalo, Marja (2005). Haastattelu. Tutkimus, tilanteet ja vuorovaikutus. Jyväskylä: Gummerrus Kirjapaino Oy.

Baker, Kurt (2023). What is Threat Intelligence? Luettu 3.5.2024 https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

College of policing (2005). How to Complete a 5x5x5 Form and Relevant Supplements. Luettu 3.5.2025 https://library.college.police.uk/docs/AP-Pref/how-to-complete-5x5x5-form.pdf

Department of the Army (2006). FM 2-22.3 (FM34-52) Human Inttelligence collector operations. Luettu 3.5.2024 https://irp.fas.org/doddir/army/fm2-22-3.pdf

ENISA (2016). A good practice guide of using taxonomies in incident prevention and detection. Luettu 12.5.2024 https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

Enorssi (2024). Tiedon hankkiminen ja sen luotettavuuden arviointi. Luettu 12.5.2024 https://www.retired.jyu.fi/enorssi/opetus/verkko-opetus-1/keittokirja-aloittelevalle-verkko-opettajalle/tiedon-hankkiminen-ja-sen-luotettavuuden-arviointi

Europol (2009). Europol Information Management. Products and services. File no: 2510-271. Luettu 1.12.2023 https://op.europa.eu/en/publication-detail/-/publication/e0120a65-0d70-454c-be47-10a0a584b27e/language-en

Finlex (2018). Laki Liikenne- ja viestintävirastosta. Luettu 20.4.2024 23.11.2018/935. https://finlex.fi/fi/laki/ajantasa/2018/20180935?search%5Btype%5D=pika&search%5Bpika%5D=kyberturvallisuuskeskus

Forum of Incident Response and security Teams (2023). Source Evaluation and Information Reliability. Luettu 14.5.2024 https://www.first.org/global/sigs/cti/curriculum/source-evaluation

Gallager, Robert (1970). Information theory and reliable communication. Wien: Springler-verlag.

Grym, Arna (2020). Feikkiä vai Faktaa. Luotettavan somevaikuttajan käsikirja. Helsinki: Next Print Oy.

Hellsten, Katri (1974). Delfoi-tekniikka ja sen käyttö. Helsingin Yliopisto, Sosiaalipolitiikan Laitos, Tutkimuksia 1974:2.

Hibbs Person, Kathrine & Person, Randolph H. (2021). Critical thinking for strategic intelligence. 3rd edition. United Kingdom: Sage Publications.

Hirsjärvi, Sirkka., Remes, Pirkko. & Sajavaara, Paula. (2010). Tutki ja kirjoita. (15.-16. painos). Helsinki: Tammi.

Ihsan Burak Tolga (2019). Whole-of-Government Cyber Information Sharing. Tallinna: Nato cooperative cyber defence centre of excellence.

Interactive Terminology for Europe (2017). Vaarantumisindikaattori. Luettu 3.5.2024 https://iate.europa.eu/entry/result/3574258/all

Interactive Terminology for Europe (2019). Vahvistusharha. Luettu 3.5.2024 https://iate.europa.eu/entry/result/3621501/all

Irwin & Mandel (2020). Standrads for evaluating source reliability and information credibility in intelligence production. 5/2020. Luettu 12.5.2024 https://cradpdf.drdc-rddc.gc.ca/PDFS/unc351/p812555_A1b.pdf

Kuusi Osmo (1999). Delfoi-metodi. Luettu 12.5.2024 https://metodix.fi/2014/05/19/kuusi-delfoi-metodi/

Kyberturvallisuuskeskus (2024). Tilannekuva ja verkostojohtaminen. Luettu 3.5.2024 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen

Kyberturvallisuuskeskus (2023). Yhteistyöryhmien tiedonvaihtokäytäntöjä. Luettu 9.5.2024 https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

Lammenranta, Markus (2014). Tieto-oppi. Luettu 20.11.2023 https://filosofia.fi/fi/ensyklopedia/tieto-oppi

Lehto, Martti., Limnéll, Jarno., Kokkomäki, Tuomas., Pöyhönen, Jouni. & Salminen, Mirva. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018.

Laari, Tommi., Flyktman, Jouni., Härmä, Katariina., Timonen, Jussi. & Tuovinen, Jussi. (2019). #kyberpuolustus - Kyberkäsikirja Puolustusvoimien henkilöstölle. Maanpuolustuskorkeakoulu, Sotataidon laitos. Julkaisusarja 3: Työpapereita nro 12.

Limnéll Jarno, Majwski Klaus & Salminen Mirva (2014.) Kyberturvallisuus. Jyväskylä: Saarijärven Offset Oy.

Linnstone, Harold A – Murray Turoff (1975). The Delphi Method. Techniques and Applications. Massachusetts: Addison-Wesley Publishing Company Inc.

Linturi, Hannu (2007). Delfoin metamorfoosit. Futura 1/2007.

Lunturi, Hannu, Linturi, Maija, Jauhiainen, Olli-Pekka (2019). Uudistuva Delfoi-menetelmä ja eDelphi 2020. Delfoi-sarja 2/2019. Helsinki: Metodix Oy.

Linturi, Hannu (2024). Delfoin monet tarkoitukset. Luettu 12.5.2024 https://metodix.fi/2020/03/08/delfoin-tarkoitukset/

Lönnqvist Irina & Moilanen Panu (2017). Kyberin taskutieto. Keskeisin kybermaailmasta jokaiselle. Jyväskylä/Rauma: Jyväskylän yliopisto ja Maanpuolustuskoulutusyhdistys.

MISP (2015) Misp-taxonomies/admiralty-scale. 19.11.2015. Luettu 12.5.2024 https://github.com/MISP/misp-taxonomies/blob/main/admiralty-scale/README.md

Office of the director of national intelligence (2018). A guide to cyber attribution. 14.9.2018. Luettu 12.5.2024 https://dl.icdst.org/pdfs/files3/db004a6f55f96c056a23fc4efc6a23ac.pdf

Office of the director of national intelligence (2018). A white paper on the key challenges in cyber threat intelligence: explaining the "see it, sense it, share it, use it" approach to thinking about cyber intelligence. 30.10.2018. Luettu 12.5.2024 https://www.dni.gov/files/NSP/Private_Sector/Feature/1-15-2020-Loretta_Dusek-ODNI_Key_Challenges_in_CTI_White_Paper_Unclass_FINAL-BW2.pdf

Paananen, Rauli (2024). Haastattelu 9.5.2024. Jyväskylän yliopiston Teams-videokeskustelusovellus.

Poliisi (2024). Kyberrikokset. Luettu 3.5.2024 https://poliisi.fi/kyberrikokset

Puolustusvoimat (2024). Puolustusvoimien johtamisjärjestelmäkeskus. Luettu 3.5.2024 https://puolustusvoimat.fi/tietoa-meista/johtamisjarjestelmakeskus

Puusa, Anu & Juuti Pauli (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät. Tallinna: Gaudeamus Oy.

Pöyhönen, Jouni., Rajamäki Jyri., Nuojua Viivi., & Lehto Martti. (2021). Cyber Situational Awareness in Critical Infrastructure Organizations. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies (pp. 161-178). Springer. Studies in Big Data, 84. https://doi.org/10.1007/978-3-030-65722-2_10

Rizov, Vasil (2018). Information Sharing for Cyber Threats. Information & Security: An International Journal, 39(1): 43-50.

Ruusuvuori Johanna & Liisa Tiittula (toim.) (2005). Haastattelu. Tutkimus, tilanteet ja vuorovaikutus. Jyväskylä: Gummerrus Kirjapaino Oy.

Sanastokeskus (2023). Tieto-oppi. Luettu 3.5.2024 https://termipankki.fi/tepa/fi/haku/tieto-oppi

Sanastokeskus (2023). Informaatio. Luettu 3.5.2024 https://termipankki.fi/tepa/fi/haku/informaatio

Skopik, Florian., Setanni, Giuseppe & Fiedler, Roman (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154-176.

Suojelupoliisi (2024). Mitä supo tekee? Luettu 3.5.2024 https://supo.fi/mita-supo-tekee

Turvallisuuskomitea (2017). Kokonaisturvallisuuden sanasto (TSK 50). https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Ulkoministeriö (2010). Kansainvälinen oikeus kyberympäristössä. Suomen kansallisia kantoja. Luettu 12.5.2024 https://um.fi/documents/35732/0/Suomennos+Kansainvälinen+oikeus+kyberympäristössä.pdf/26706a43-4d7e-07da-8c4f-7c53b6ca51ab?t=1602581216672

United Nations Office on Drugs and Crime (2011). Criminal Intelligence Manual for Analysts. Vienna: United nations Luettu 12.5.2024 Office https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

Valtonen Vesa (2010). Turvallisuustoimijoiden yhteistyö – operatiivis-taktisesta näkökulmasta. Helsinki: Edita Prima Oy

Valtioneuvoston julkaisuja 2023:31 (2023). Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa. Helsinki: Valtioneuvosto.

Valtioneuvoston periaatepäätös (2013, 24. tammikuuta). Suomen kyberturvallisuusstrategia. Haettu 3.5.2024 osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

Valtioneuvoston periaatepäätös (2019, 3. lokakuuta). Suomen kyberturvallisuusstrategia 2019. Haettu 3.5.2024 osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Valtioneuvoston yleisistunto (30.11.2023). Valtioneuvoston asetus LVM/2023/6 https://valtioneuvosto.fi/paatokset/paatos?decisionId=100

LIITE 1 SAATEKIRJE

Hyvä vastaanottaja.

Toivon, että voisit antaa aikaasi tutkimukselle ja osallistua asiantuntijapanelistina lähteen ja tiedon luotettavuuden arviointia käsittelevään tutkimukseen kybertiedon kontekstissa. Teen lopputyötä Jyväskylän yliopiston informaatioteknologian tiedekuntaan kyberturvallisuuden maisteriohjelmaan.

Tutkielman tarkoituksena on määritellä kybertiedonvaihtoon mittaristo/matriisi, jossa kuvataan tiedon ja lähteen luotettavuutta. Pohjana hyödynnetään jo olemassa olevia mittareita Amiraalikoodisto (admiralty code) sekä 4x4-matriisi, jota esimerkiksi Europol hyödyntää. Nämä mittaristot ovat laajasti käytössä, mutta eivät ensisijaisesti kybertiedonvaihdossa vaan esimerkiksi henkilötiedustelussa tai järjestäytyneeseen rikollisuuteen liittyvän tiedon vaihdossa viranomaisten välillä. Mittareiden lähtökohta vaikuttaa olevan paljon henkilötiedustelussa ja tämän takia ne ovat työn pohjalla, mutta uutta määritystyötä tarvitaan, jotta matriisit saadaan sopimaan kybertiedonvaihtoon paremmin.

Työn tarkoituksena on tuottaa tiedon ja lähteen luotettavuuden mittari kybertiedonvaihtoon. On tärkeää, että mittaria luodessa keskitytään vain kybertiedonvaihtoon, sillä se rajaa mittariston ulkopuolelle muut tiedustelulajit kuten esimerkiksi henkilötiedustelun, jossa lähteen luotettavuutta arvioidaan hyvin eri tavalla.

Työn tavoitteena on tuottaa suomalaisten kyberviranomaisten käyttöön tiedonluotettavuuden mittaristo. Näin ollen tarkoituksena on selvittää:

- Minkälainen tiedonluotettavuuden mittaristo olisi sopiva kybertiedonvaihtoon?

Kysymystä tullaan tarkentamaan alakysymyksillä:

- Voitaisiinko jo olemassa olevista mittareista, amiraalikoodisto ja 4x4-matriisi, rakentaa kybertiedonvaihtoon sopiva mittaristo?
- Miten lähteen ja tiedon luotettavuutta kuvaavat mittarit tulisi määritellä, jotta se palvelisi parhaalla mahdollisella tavalla eri toimijoita (suomalaiset kyberturvallisuusviranomaiset).

Kybermaailmassa tieto vanhenee nopeasti ja olisi tärkeää, että viranomaiset voisivat jakaa saamaansa tietoa helposti ja nopeasti. Tähän tarvitaan toki tiedonvaihtoa mahdollistavaa lainsäädäntöä, johon tämä työ ei tule keskittymään. Tarkoituksena on, että tietoa voitaisiin jakaa matalammalla kynnyksellä jo nykyisenkin lainsäädännön nojalla matriisin avulla, koska myös vastaanottajat jaksaisivat saman tavan luokitella tietoa ja lähdettä. Matriisin avulla voidaan siis taata myös lähteen anonymiteetti, jota ei useastikaan haluta jakaa muille kuitenkin siten, että tiedon vastaanottaja pystyy tekemään oman arvion saamastaan tiedosta.

Työssä kyberuhkatieto halutaan ymmärtää laajasti, se voi olla teknistä tietoa, kuten esimerkiksi vaarantumisindikaattori (engl. Indicator of Comp-romise, IoC) tai esimerkiksi havainto kartoitustoiminnasta tai muusta digitaalisesta tai fyysisestä todisteesta, että kyberhyökkääjällä on aikomus hyökätä (Indicator of attac, IoA). Henkilöltä tai verkostolta saatu tieto tai havainto, jossa kerrotaan uhkahavainnosta, mutta sille ei ole antaa tarkempaa teknistä tietoa vaan kyseessä voi olla analyytikon tuottama havainto ja tietojen yhdistäminen, jolla tieto on tuotettu. (esim. Sanasto)

Kyselyn käytännön toteutus

Tutkimus toteutetaan delfoi-metodia hyödyntäen. Tämä tarkoittaa sitä, että tutkimuksessa on useampi haastattelukierros. Tutkimus toteutetaan eDelphi-nimisessä sovelluksessa, jonne panelistien tulee kirjautua. eDelphi on Delfoi-asiantuntijametodin käyttöön suunniteltu avoimen lähdekoodin verkko-ohjelmisto.

Tutkimusta ja aineiston keruuta varten on tehty erillinen tietosuojaseloste, joka on tämän viestin liitteenä. Siinä myös kerrotaan, mitä tietoja vastaajasta kerätään tutkijan toimesta sekä mitä tietoja eDelphi-sovellus vastaajasta kerää. Lähtökohtaisesti tietoina kerätään nimi sekä sähköposti. Vastatessasi kyselyyn vastaukset ovat omiasi eivätkä edusta työskentelemäsi organisaation kantoja.

Tulet saamaan linkin ensimmäiseen kyselyyn, jonka yhteydessä sinun tulee luoda tunnukset sovellukseen. Yksi kyselykierros on avoinna viikon ajan, jonka sisällä pyydän sinua vastaamaan kyselyyn. Kyselyssä annetaan aina ehdotus matriisin eri osioiden määrittelystä, mutta tarkoituksena on, että erityisesti alussa ne kumotaan panelistien toimesta ja rakennetaan yhteisten vastausten myötä parempi määrittely ja sellainen, jonka takana mahdollisimman moni panelisti pystyisi olemaan. Ensimmäisellä kierroksella kommentit eivät näy muille, mutta tarkoituksena on, että toisella kierroksella kommentit näkyisivät muille ja myös näitä on mahdollista haastaa ja kommentoida. Sovelluksessa pyydän käyttämään nimimerkkiä, josta sinua ei voida tunnistaa (älä siis käytä esim. somessa käyttämääsi nimimerkkiä). Sovellukseen valittu nimimerkki näkyy vastauksen yhteydessä ja näin ollen sen näkevät kaikki paneeliin osallistuvat, kun kommentit ovat näkyvillä. Paneelin manageri (tutkija) näkee nimimerkin myös silloin, kun kommentit eivät ole avoimia.

Ensimmäisen kierroksen päätyttyä kysely sulkeutuu. Tämän jälkeen käyn annetut vastaukset läpi ja muodostan niiden pohjalta version tiedon ja lähteen luotettavuuden matriisiksi, jota kommentoidaan seuraavalla haastattelukierroksella. Näiden lisäksi saattaa mukana olla tarkentavia kysymyksiä, joihin haetaan teiltä vastauksia. Haastattelukierrosten määrä riippuu siitä, miten tietoa saadaan kerättyä, mutta tämän hetken arvion mukaan kierroksia olisi 2-3. On vaikea sanoa,

kuinka paljon tähän tulee yksittäisellä vastaajalla kulumaan aikaa, sillä jokainen antaa yksilölliset vastaukset. Kokonaisaika tulee olemaan jotain tunteja.

Alustava aikataulu:

- 29.2.-7.3.2024 kysely auki
    - Managerin synteesi kierrosten välissä
- 14.-21.3.2024 kysely auki
    - Managerin synteesi kierrosten välissä
- 28.3-4.4.2024 kysely auki

Yhteystiedot

Työtäni ohjaavat

- Jyväskylän yliopiston professori Martti Lehto sekä
- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen johtava asiantuntija Juhani Eronen.

Pyytäisin sinua vastaamaan mahdollisimman pian, mikäli olet käytettävissä työtä varten. Mikäli osallistut kyselyyn, tulen laittamaan sinulle tausta-aineistona lyhyet kuvaukset amiraalikoodistosta ja 4x4-matriisita sekä niiden määritelmistä. Tämä materiaali tulee löytymään myös eDelphi-ympäristöstä. Mahdolliset lisäkysymykset liittyen tutkimukseen nyt tai paneelin aikana voi esittää minulle.

Terveisin,
Irina Lönnqvist

LIITE 2 TIETOSUOJASELOSTE

Kuvaus henkilötietojen käsittelystä tieteellisessä tutkimuksessa (tietosuojailmoitus EU (679/2016)

1. Tutkimuksessa: ”Kybertiedonvaihto ja luotettavuuden mittaristo” käsiteltävät henkilötiedot

Haastatteluiden avulla kerättyjä tietoja käytetään Irina Lönnqvistin pro gradu-tutkielman ”Kybertiedonvaihdon ja luotettavuuden mittaristo” aineistona. Tutkielman tavoitteena on tuottaa tietoa siitä, minkälainen tiedon ja lähteen luotettavuutta kuvaava mittaristo voitaisiin määritellä suomalaisten viranomaisten väliseen kybertiedonvaihtoon.

Tutkimuksessa Sinusta kerätään seuraavia henkilötietoja: Nimi ja sähköpostiosoite, jotka ovat tutkijan tiedossa. Panelistin käyttämä nimimerkki on paneeliin osallistuvien nähtävillä eDelphi-sovelluksessa sekä työn ohjaajien nähtävillä analyysivaiheessa. Nimimerkki on työn saatteessa pyydetty muotoilemaan siten, ettei siitä voi tunnistaa vastaajaa. Tutkimuksessa hyödynnetään eDelphi- kyselytyökalua, jonne sinun tulee rekisteröityä, jotta voit vastata kyselyyn. Järjestelmä kerää sinusta nimen lisäksi sähköpostitiedot. Ohjelmiston kehityksestä vastaa Metodix Oy ja koodauksesta Metatavu Oy. Metatavu Oy:n tietosuojaselosteen löydät: https://metatavu.fi/tietosuojaseloste/

Tiedote ja tietosuojailmoitus on lähetetty sähköpostin liitetiedostona haastattelupyynnön ja haastattelukutsun mukana.

2. Henkilötietojen käsittelyn oikeudellinen peruste tutkimuksessa/arkistoinnissa

Käsittely on tarpeen tieteellistä tutkimusta varten ja se on oikeasuhtaista, sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen nähden (tietosuojain 4 §:n 3 kohta). Tutkimustulokset ovat julkisesti saatavilla yliopiston julkaisuarkistosta (JYX).

3. Henkilötietojen siirto EU/ETA ulkopuolelle

Tutkimuksessa tietojasi ei siirretä EU/ETA-alueen ulkopuolelle.

4. Henkilötietojen suojaaminen

Henkilötietojen käsittely tässä tutkimuksessa perustuu asianmukaiseen tutkimussuunnitelmaan ja tutkimuksella on vastuuhenkilö. Tutkimuksessa toimitaan niin, etteivät Sinua koskevat tiedot paljastu ulkopuolisille. Tutkimustulosten (Pro Gradu) osalta pyritään siihen, ettei Sinua voida tunnistaa suoraan taikka

välillisesti tutkimustuloksista. Osana Pro Gradua voidaan käyttää suoria lainauksia vastauksistasi sovelluksessa. eDelphi-työkalussa vastataan anonyymisti, joten tutkija tai työn ohjaajat eivät näe, kuka yksittäisen vastauksen on antanut. eDelphi-sovelluksessa on mahdollista käyttää nimimerkkiä, mikäli nimimerkki on esimerkiksi lempinimesi tai sosiaalisessa mediassa hyödyntämä nimi tai haluat laittaa siihen oman nimen, on tämä nimi sellainen, jonka paneeliin osallistuvat näkevät sekä työn ohjaajat.

Nimimerkki tai muu tunnistetieto jää ainoastaan eDelphi-työkaluun eikä itse tutkimuksen tekstissä tule nimimerkit esille vaan panelisteista käytetään kaikista samaa nimitystä, panelisti tai vastaaja. Myös sähköpostiosoitteet hävitetään, kun haastattelu on tehty.

Tutkimuksessa käsiteltävien henkilötietojen suojaaminen
Sähköpostiosoitteet osallistumispyyntöjä ja haastattelukutsuja varten säilytetään tutkijan tietokoneella niin kauan kuin haastattelu on tehty, jonka jälkeen ne poistetaan. Tutkija ei lähetä tutkittaville sähköpostia siten, että muiden tutkimuksiin osallistuvien tiedot näkyisivät vastaanottajakentässä, eikä muutoinkaan toimi niin, että ulkopuolisilla olisi pääsy tutkittavan tietoihin. Tutkija vastaa aineiston hallinnasta sen elinkaaren aikana ja tietojen hävittämisestä tutkimuksen päätyttyä.

eDelphi-sovellukseen luotu kysely ja siihen saadut vastaukset säilytetään korkeintaan viisi vuotta. Tämän lisäksi sovelluksessa on panelistin luoma käyttäjätili, jonka poistamisesta jokainen panelisti vastaa itse.

Tutkimuksesta on tehty erillinen tietosuojan vaikutustenarvio/tietosuojavastaavaa on kuultu vaikutustenarvioinnista

☐ Kyllä ☒ Ei, koska tutkija on tarkastanut, ettei vaikutustenarviointi ole pakollinen.

HENKILÖTIETOJEN KÄSITTELY TUTKIMUKSEN PÄÄTTYMISEN JÄLKEEN

Tutkimusrekisteri hävitetään viimeistään pro gradu -tutkielman valmistuttua (arvio 1.8.2024).

Rekisterinpitäjä(t) ja tutkimuksen tekijät

Rekisterinpitäjä, pro gradu- tutkielman suorittaja ja yhteyshenkilö: Irina Lönnqvist, Maisteriopiskelija, (sähköpostiosoite). Käsiteltäessä tutkittavien henkilötietoja rekisterinpitäjä on taho, joka on vastuussa tutkittavien henkilötietojen asiallisesta ja lainmukaisesta käsittelystä.

Tutkimuksen ohjaajat: Professori Martti Lehto, Jyväskylän yliopiston informaatioteknologian tiedekunta, https://www.jyu.fi/fi/henkilot/martti-lehto

Johtava asiantuntija Juhani Eronen, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus

Rekisteröidyn oikeudet

Oikeus saada pääsy tietoihin (tietosuoja-asetuksen 15 artikla)
Sinulla on oikeus saada tieto siitä, käsitelläänkö henkilötietojasi ja mitä henkilötietojasi käsitellään. Voit myös halutessasi pyytää jäljennöksen käsiteltävistä henkilötiedoista.

Oikeus tietojen oikaisemiseen (tietosuoja-asetuksen 16 artikla)
Jos käsiteltävissä henkilötiedoissasi on epätarkkuuksia tai virheitä, sinulla on oikeus pyytää niiden oikaisua tai täydennystä.

Oikeus tietojen poistamiseen (tietosuoja-asetuksen 17 artikla)
Sinulla on oikeus vaatia henkilötietojesi poistamista tietyissä tapauksissa. Oikeutta tietojen poistamiseen ei kuitenkaan ole, jos tietojen poistaminen estää tai vaikeuttaa suuresti käsittelyn tarkoituksen toteutumista tieteellisessä tutkimuksessa.

Oikeus käsittelyn rajoittamiseen (tietosuoja-asetuksen 18 artikla)
Sinulla on oikeus henkilötietojesi käsittelyn rajoittamiseen tietyissä tilanteissa kuten, jos kiistät henkilötietojesi paikkansapitävyyden.

Vastustamisoikeus (tietosuoja-asetuksen 21 artikla)
Sinulla on oikeus vastustaa henkilötietojesi käsittelyä, jos käsittely perustuu yleiseen etuun tai oikeutettuun etuun. Tällöin yliopisto ei voi käsitellä henkilötietojasi, paitsi jos se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää oikeutesi.

Oikeuksista poikkeaminen
Tässä kuvatuista oikeuksista saatetaan tietyissä yksittäistapauksissa poiketa tietosuoja-asetuksessa ja Suomen tietosuojalaissa säädetyillä perusteilla siltä osin, kuin oikeudet estävät tieteellisen tai historiallisen tutkimustarkoituksen tai tilastollisen tarkoituksen saavuttamisen tai vaikeuttavat sitä suuresti. Tarvetta poiketa oikeuksista arvioidaan aina tapauskohtaisesti.

Profilointi ja automatisoitu päätöksenteko
Tutkimuksessa henkilötietojasi ei käytetä automaattiseen päätöksentekoon. Tutkimuksessa henkilötietojen käsittelyn tarkoituksena ei ole henkilökohtaisten ominaisuuksiesi arviointi, ts. profilointi vaan henkilötietojasi ja ominaisuuksia arvioidaan laajemman tieteellisen tutkimuksen näkökulmasta.

Rekisteröidyn oikeuksien toteuttaminen
Jos sinulla on kysyttävää rekisteröidyn oikeuksista, voit olla yhteydessä tutkimuksen toteuttajaan (sähköpostiosoite)

Sinulla on oikeus tehdä valitus erityisesti vakinaisen asuin- tai työpaikkasi sijainnin mukaiselle valvontaviranomaiselle, mikäli katsot, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja- asetusta (EU) 2016/679. Suomessa valvontaviranomainen on tietosuojavaltuutettu.

Tietosuojavaltuutetun toimiston ajantasaiset yhteystiedot: https://tietosuoja.fi/etusivu

LIITE 3 TAUSTA-AINEISTO

Admiralty code

Amiraalikoodiston historia yltää aina toiseen maailmansotaan, jolloin menetelmä kehitettiin Britannian laivastossa. Sen silloinen johtaja havaitsi, että heillä on paljon tietoa ja erilaisia raportteja, mutta niiden sisältöä ei voinut nopeasti saada katsomalla vaan raportti piti lukea alusta loppuun. Siksi kehitettiin menetelmä, jonka avulla tieto voitiin nopeasti luokitella ja havaita raporttien kansilehdistä. (esim. Irwin ja Mandel 2020.)

Tätä varten suunniteltiin yksinkertainen järjestelmä, jossa lähde ja itse tieto arvioitiin erikseen koodaamalla arvio kirjaimilla ja numeroilla "A1" - "D5". Kirjain ilmaisee lähteen luotettavuusasteen (kuvio 1.) ja numero todennäköisyyttä (kuvio 2.), että tieto on oikea. Syynä lähdearvioinnin erottamiseen itse tiedon arvioinnista oli se, että on mahdollista, että arvokasta tietoa voi tulla huonomaineisesta lähteestä ja päinvastoin disinformaatio voi tulla lähteestä, joka on yleensä luotettava. Tätä tietojen luokitusmenetelmää on sittemmin käytetty eri muunnelmina, ja se tunnetaan nimellä "Admiralty System" tai "Admiralty Code". (esim. Irwin ja Mandel 2020.)

Amiraalikoodisto koostuu kuudesta luokasta niin lähteen kuin tiedon luotettavuuden osalta. Kaksi ensimmäistä luokkaa kuvaavat luotettavaa tai yleensä luotettavaa lähdettä tai täysin uskottavaa tai todennäköisesti totta olevaa tietoa. Kolmas luokka kuvaa melko luotettavaa lähdettä tai mahdollisesti totta olevaa tietoa. Luokat neljä ja viisi kuvaavat ei luotettavaa lähdettä tai epäilyttävää tietoa. Kuudes luokka on lähteelle tai tiedolle, jota ei voida tunnistaa tai todistaa. Luokittelu on tehty helpoksi ja nopeaksi eikä luokkia ole liikaa.

Amiraalikoodistoa hyödyntävät monet eri viranomaiset eri puolilla maailmaa, sillä kyseinen matriisi on osa Naton käyttämiä standardeja. Irwin ja Mandel (2020) tuovat esille, että esimerkiksi amiraliteetti koodistoa käytetään eri tavoin eri maissa ja siellä tiedusteluviranomaiset saattavat antaa hyvin eri arvoja samanlaisissa tilanteissa, koska ohjeistus on erilainen. Näin ollen jaettaessa tietoa eri maiden viranomaisten välillä, on mahdollista, että annettu arvo lähteen tai tiedon luotettavuudesta vaihtelee.

Koska käytännöt eroavat eri maissa eikä ohjeistus ole yhtenäistä, on mahdollista, että päädytään myös niin kutsuttuun vahvistusharhaan. Kaksi saman maan viranomaista voivat saada kansainvälisistä lähteistä tiedon, joka on luokiteltu eri tavalla. Näin ollen tiedon tai lähteen luotettavuus jo vaihtelee. Koska lähteen määrittely on hyvin ylätasolla ei viranomaisilla ole myöskään mahdollisuutta tunnistaa, voiko tieto olla samasta lähteestä ja tieto on tullut vain useampaa eri kanavaa pitkin. Mikäli kyseessä olisi merkittävä tieto, joka vaikuttaa maan

turvallisuuteen, voisivat seuraukset olla huonot, mikäli tiedon lähdettä ja tiedon luotettavuutta ei pystytä tunnista.

Lähde ja tieto on luokiteltu ensin lyhyesti ja tämän lisäksi niitä on vielä avattu erikseen. Työssä on alkuperäiset englanninkieliset tekstit ensin ja sitten vapaat käännökset kustakin suomeksi.

Lähteen luotettavuus	Tarkempi kuvaus
A Completely reliable = täysin luotettava	A Completely reliable: Refers to a tried and trusted source which can be depended upon with confidence. = A Täysin luotettava: Lähdettä on hyödynnetty aikaisemmin ja sen on todettu olevan luotettava. Lähteeseen voidaan luottaa.
B Usually reliable = yleensä luotettava	B Usually reliable: Refers to a source which has been successful in the past but for which there is still some element of doubt in a particular case. = B Yleensä luotettava: Viittaa lähteeseen, joka on ollut luotettava aiemmin, mutta jonka suhteen on tietyissä tapauksissa edelleen epäilyksiä.
C Fairly reliable = melko luotettava	C Fairly reliable: Refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based. = C Melko luotettava: Viittaa lähteeseen, jota on satunnaisesti hyödynnetty aiemmin ja johon voidaan perustaa jonkinlainen luottamus.
D Not usually reliable = ei yleensä luotettava	D Not usually reliable: Refers to a source which has been used in the past but has proved more often than not unreliable. = D Ei yleensä luotettava: Viittaa lähteeseen, jota on käytetty aiemmin, mutta joka on usein osoittautunut epäluotettavaksi.

E Unreliable = epäluotettava	E Unreliable: Refers to a source which has been used in the past and has proved unworthy of any confidence. = E Epäluotettava: Viittaa lähteeseen, jota on käytetty aiemmin ja joka ei ansaitse minkäänlaista luottamusta.
F Reliability cannot be judged = lähteen luotettavuutta ei voida todentaa	F Reliability cannot be judged: Refers to a source which has not been used in the past. = F Lähteen luotettavuutta ei voida todentaa: Viittaa lähteeseen, jota ei ole käytetty aiemmin.

Tiedon luotettavuus	Tarkempi kuvaus
1 Completely credible / confirmed by other sources = täysin uskottava / vahvistettu muista lähteistä	1 Completely credible / Confirmed by other sources: If it can be stated with certainty that the reported information originates from another source than the already existing information on the same subject, it is classified as “confirmed by other sources” and is rated “1”. = 1 Täysin uskottava / vahvistettu muista lähteistä: Jos voidaan varmuudella todeta, että raportoitu tieto on peräisin muusta lähteestä kuin samasta aiheesta jo olemassa oleva tieto, se luokitellaan "muista lähteistä vahvistetuksi" ja sille annetaan arvosana 1.
2 Probably true = todennäköisesti totta	2 Probably true: If the independence of the source of any item or information cannot be guaranteed, but if, from the quantity and quality of previous reports its likelihood is nevertheless regarded as sufficiently established, then the information should be classified as “probably true” and given a rating of “2”.

	2 Todennäköisesti totta: Jos jonkin kohteen tai tiedon lähteen riippumattomuutta ei voida taata, mutta jos sen todennäköisyyttä aikaisempien raporttien määrän ja laadun perusteella kuitenkin pidetään riittävän luotettavana, tieto on luokiteltava "todennäköisesti totta" ja sille on annettava luokitus. "2":sta.
3 Possibly true = mahdollisesti totta	3 Possibly true: If, despite there being insufficient confirmation to establish any higher degree of likelihood, a freshly reported item of information does not conflict with the previously reported behaviour pattern of the target, the item may be classified as “possibly true” and given a rating of “3”. = 3 Mahdollisesti totta: Jos äskettäin raportoitu tieto ei ole ristiriidassa kohteen aiemmin ilmoitetun käyttäytymismallin kanssa, vaikka vahvistus ei ole riittävää korkeamman todennäköisyyden määrittämiseksi, se voidaan luokitella "mahdollisesti tosi" ja sille voidaan antaa arvosana " 3".
4 Doubtful = Epäilyttävä	4 Doubtful: An item of information which tends to conflict with the previously reported or established behaviour pattern of an intelligence target should be classified as “doubtful” and given a rating of “4”. = 4 Epäilyttävä: Tieto, joka on ristiriidassa tiedustelukohteen aiemmin raportoidun tai vakiintuneen käyttäytymismallin kanssa, tulisi luokitella "epäilyttäväksi" ja sille on annettava arvosana "4".
5 Improbable = Epätodennäköinen	5 Improbable: An item of information which positively contradicts previously reported information or conflicts with the established behaviour pattern of an intelligence target in a marked degree should be classified as

	"improbable" and given a rating of "5". = 5 Epätodennäköinen: Aiemmin raportoidut tiedot tai ristiriidat tiedustelukohteen vakiintuneen käyttäytymismallin kanssa tulisi luokitella "epätodennäköiseksi" ja antaa arvosanaksi "5".
6 Truth cannot be judged = tiedon oikeellisuutta ei voida todentaa	6 Truth cannot be judged: Any freshly reported item of information which provides no basis for comparison with any known behaviour pattern of a target must be classified as "truth cannot be judged" and given a rating of "6". Such a rating should be given only when the accurate use of higher rating is impossible. = 6 Tiedon oikeellisuutta ei voida todentaa: Kaikki äskettäin raportoidut tiedot, jotka eivät anna perustaa vertailulle kohteen mihinkään tunnettuun käyttäytymismalliin, on luokiteltava "totuutta ei voida arvioida" ja niille on annettava arvosana "6". Tällainen luokitus tulisi antaa vain silloin, kun korkeamman luokituksen tarkka käyttö on mahdotonta.

4x4-matriisi

Europolin tiedonhallintamalli kuvaa tiedonkulkua Europolin tasolla. Yhteistyössä jäsenvaltioiden kanssa kehitetty ja Europolin kansallisten yksiköiden päälliköiden hyväksymänä malli määrittelee Europolin ja sen kumppaneiden välisen tiedonkäsittelyn ja -vaihdon käytännön toiminnan. Se varmistaa myös tiukkojen tietoturvamääräysten noudattamisen. Tiedon arviointi perustuu 4x4-matriisiin, jota jäsenvaltioissa käytetään toimitettujen tietojen aitouden ja tarkkuuden määrittämiseksi. Arviointikoodit koostuvat lähteestä ja saadusta tiedosta. 4x4-matriisin käyttö sisältyy analyysimääräyksiin sekä Europolin kolmansien osapuolten kanssa tekemiin operatiivisiin sopimuksiin. (Europol.)

4x4-matriisia hyödyntävät poliisiviranomaiset myös paikallisesti ja muut virastot ja kansainväliset järjestöt kuten YK. Monet näistä käyttävät tämän järjestelmän muunnelmia, mutta jokainen on helposti tulkittavissa selittävien taulukoiden avulla, ja tarvittaessa tiedot voidaan muuntaa järjestelmästä toiseen.

Yhdistyneiden kansakuntien huumausaine- ja rikosasioiden toimisto (UNODC) on tuottanut rikostiedustelu analyytikolle oppaan, jossa yksi tiedon luotettavuuden mittareista on 4x4-matriisi. Oppaassa tuodaan esille, että 4x4-matriisi perustuu yksinkertaiseen henkilökohtaiseen tietoon. Näin ollen tiedolla on alhaisempi arvo. Tällä yksinkertaisuudella on arvo sinänsä, koska arvioinnista tulee vähemmän subjektiivinen. (UNODC 2011.)

Oppaan mukaan arviointiin sovelletaan kolmea perusperiaatetta: 1. Henkilökohtaiset tunteet eivät saa vaikuttaa arviointiin, vaan sen tulee perustua ammatilliseen harkintaan. 2. Lähteen arviointi tulee tehdä tiedoista erikseen. 3. Arviointi on suoritettava mahdollisimman lähellä lähdettä. (UNODC 2011.)

4x4-matriisi koostuu nimensä mukaisesti neljästä luokasta, jolla tiedon ja lähteen luotettavuutta voidaan ilmasta. Mikäli lähde on tunnettu tai sen antamista tiedoista ei ole epäilystä ja saadut tiedot ovat oikeellisia, pidetään tietoa luotettavana. Kaikki muu sijoittuu epäluotettavan tiedon kategoriaan, joka vaatii lisäselvitystä tai tietoa muista lähteistä. Myös 4x4-matriisissa on amiraalikoodistoa vastaava luokka tiedolle ja lähteelle, jonka luotettavuutta ja oikeellisuuta ei voida arvioida.

Lähteen luotettavuus
A where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances; = A Lähde on osoittautunut aikaisemmin aina luotettavaksi tai lähteen aitoudesta, eheydestä, luotettavuudesta tai pätevyydestä ei ole epäilystä.
B source from whom information received has in most instances proved to be reliable; = B Lähde, jolta tieto on kerätty, on osoittautunut suurimmassa osassa tapauksista luotettavaksi.
C source from whom information received has in most instances proved to be unreliable; = C Lähde, jolta tieto on kerätty, on osoittautunut suurimmassa osassa tapauksista epäluotettavaksi.
X the reliability of the source cannot be assessed. = X Lähteen luotettavuutta ei voida arvioida.

Tiedon luotettavuus
1 information whose accuracy is not in doubt;

= 1 Tiedon tarkkuudesta ei ole epäilystä.
2 information known personally to the source but not known personally to the official passing it on; = 2 Lähde tuntee tiedon, mutta tiedon välittänyt taho ei. Tieto on loogista ja yhdenmukaista muun aiheeseen liittyvän tiedon kanssa.
3 information not known personally to the source but corroborated by other information already recorded; = 3 Lähde ei tunne tietoa henkilökohtaisesti, mutta muu kerätty tieto tukee kyseisen tiedon todenmukaisuutta.
4 information which is not known personally to the source and cannot be corroborated. = 4 Lähde ei tunne tietoa henkilökohtaisesti eikä tiedon oikeellisuutta pystytä varmistamaan muista lähteistä.

Lähteet

Irwin & Mandel (2020). Standards for evaluating source reliability and information credibility in intelligence production. 5/2020. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc351/p812555_A1b.pdf

Europol. Europol Information Management. Products and services. File no: 2510-271. http://arhiva.mvr.gov.mk/Uploads/Europol%20Products%20and%20Services-Booklet.pdf

United nations office on drugs and crime (2011). Criminal Intelligence

Manual for Analysts. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

LIITE 4 ALUSTAVAT KYSYMYKSEN KYBERTURVALLISUUS-JOHTAJAN HAASTATTELUUN

- Hyödyntävätkö suomalaiset viranomaiset tällä hetkellä vastaavaa matriisia lähteen ja tiedon luotettavuudesta, joka olisi yhteinen kaikilla?
- First on suositellut sen jäseniä käyttämään matriisia, Suomessa KTK on Firstin jäsen, onko tästä keskusteltu Suomessa?
- Voisiko tällaisen matriisin käyttö olla hyödyllistä Suomessa?
- Miten se voitaisiin ottaa käyttöön, millaista keskustelua ja määritystyötä tulisi käydä?
- Voisiko tämä madaltaa tiedon jakamisen kynnystä?
- Minkälaisia haasteita näet matriisin käytössä?