INFORMAATIO-VAIKUTTAMISEN TORJUNTA

Esiselvitys

HUOLTOVARMUUSKESKUS

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuuskeskuksen yhteydessä toimii Huoltovarmuusneuvosto sekä pysyvinä yhteistyöeliminä komitean tapaan toimivia sektoreita ja pooleja. Nämä yhdessä muodostavat Huoltovarmuusorganisaation.

Julkaisija: Huoltovarmuuskeskus
Esiselvityksen laatija: Antti Sillanpää
Ohjausryhmä: Sauli Savisalo, Katja Ahola
Kuvat: Shutterstock
Taitto: Up-to-Point Oy
Julkaisuvuosi: 2021
ISBN: 978-952-7470-11-4

HUOLTOVARMUUSKESKUS

Sisältö

1 JOHDANTO

Vihamielinen informaatiovaikuttaminen[1] on noussut merkittäväksi yhteiskuntien välisen ja niiden sisäisen kehityksen uhaksi. Viestintäympäristön tekninen ja rakenteellinen muutos kiihtyvät ja mahdollistavat yhä tehokkaamman ja huomaamattomamman informaatiovaikuttamisen. Pahimmillaan se horjuttaa demokraattisen ja avoimen yhteiskunnan perusteita ja vähintään sen toimivuutta.

Valtioneuvoston päätös huoltovarmuuden tavoitteista esittää, kuinka informaatiovaikuttaminen voi estää huoltovarmuustavoitteiden toteuttamista. Media on informaatiovaikuttamisen kohde, mutta sitä käytetään myös informaatiovaikuttamisen välineenä. Sosiaalinen media on tärkeä osa mediaympäristöä. Myös väärät tiedot leviävät nopeasti sosiaalisen median palveluissa. Niitä voidaan käyttää tahallisen ja vahingollisen informaatiovaikuttamisen välineinä. Parantamalla informaatioympäristön analyysiä ja ymmärtämistä tuetaan ilmaisu- ja lehdistövapautta[2].

Tiedotusvälineiden rooli on merkittävä demokratian peruskivenä. Yhteiskunnan turvallisuutta ja vastuullista sananvapautta tukevan, vapaan ja moniäänisen median toimintaedellytyksien turvaaminen kaikissa olosuhteissa on yhteiskunnan turvaamisen painopisteitä. Joukkoviestinnän ja sen infrastruktuurien turvaaminen sekä toiminnan muu tukeminen on välttämätöntä[3].

Informaatiovaikuttamisen tunnistaminen, uhkan estäminen, kestokyvyn parantaminen ja palautuminen ovat hankalia tavoitteita, eivätkä täydellisesti saavutettavia. Hyviä käytänteitä tarvitsevat niin kansalaiset, elinkeinoelämä kuin viranomaisetkin.

Huoltovarmuuskeskuksen esiselvityksessä on kartoitettu verkostomaisen yhteistyön mahdollisuuksia yhteiskuntaa vahingoittavan informaatiovaikuttamisen tunnistamiseksi ja siltä suojautumiseksi. Työssä on pyritty tunnistamaan menettelyjä ja työkaluja, dataa sekä toimintamalleja informaatiovaikuttamisen tunnistamiseksi ja informaatioympäristön luotettavuuden arvioimiseksi.

Viranomaisilta saatu aineisto koostuu kyselyistä ja työpajoista, jotka on toteutettu usein yhdessä valtioneuvoston viestintäosaston kanssa. Tiedonhankintaa on täydennetty Huoltovarmuusorganisaation Mediapoolissa sekä haastatteluissa. Keskusteluja on käyty lisäksi median, tutkimus- ja yritysmaailman sekä verrokkimaiden viranomaisten kanssa. Nämä tuottivat monia hyödyllisiä ehdotuksia. Osa ehdotuksista sopii paremmin muiden kuin Huoltovarmuuskeskuksen hyödynnettäväksi, mikä on pyritty huomioimaan tekstissä.

Suomalainen ratkaisu perustuu luontevasti laaja-alaiseen yhteistyöhön ja osaamisen kehittämiseen. Yhteistyötä edellytetään niin elinkeinoelämän kuin viranomaisten sisällä kuin välillä. Osaamisen kehittämistä tarvitsee edellisten lisäksi koko väestö.

1) Esiselvityksessä ei oteta kantaa informaatiovaikuttamisen käsitteeseen. Aihepiiristä keskusteltaessa käytetään myös termejä informaatioturvallisuus, -resilienssi, -häirintä ja sen torjunta. Sanastotyö lisäisi termien johdonmukaista käyttöä.
2) Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018.
3) Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018.

Kerätyn aineiston pohjalta esiselvitys on luonut työhypoteesin informaatioturvallisuuden kehittämiseksi. Se perustuu olemassa oleville tai idullaan olevien verkostojen kehittämiselle. Verkostoja tukee ja hyödyntää toiminto, joka on työnimeltään informaatioturvallisuuden osaamiskeskus. Toiminto välittää tietoa ja tuottaa kohderyhmille osin erilaisia palveluja. Tehtävässään se hyödyntää läpinäkyvällä tavalla sovittuja tieto- ja analysointiresursseja.

Verkostomaisuus edellyttää tiedonvaihtoa laajasti alan eri toimijoiden kesken. Viranomaisissa ja mediassa toimii omista lähtökohdistaan toimivia yksiköitä tai henkilöitä, jotka tunnistavat informaatiovaikuttamista tai tekevät töitä uhkan suitsimiseksi. Näitä erilaisia toimijoita kutsutaan tässä esiselvityksessä informaatioanalyysiryhmiksi. Esiselvityksessä käytetystä termistä huolimatta viranomais- tai luottamusverkostojen jäsenet poikkeavat monessa suhteessa merkittävästi toisistaan.

Esiselvityksessä hahmoteltu osaamiskeskustoiminto tukisi itsenäisten toimijoiden ryhmiä muassa datalla, analyyseillä ja menetelmäosaamisen kehittämisellä sekä koulutuksella. Kyberturvallisuuskeskuksen esimerkkiä noudattaen kaikki tuotteet ja palvelut sekä tuotantomenetelmät eivät olisi julkisia. Erilaiset yhteisöt, kuten viranomaiset tai alan toimijoiden luottamusverkostot, voivat edellyttää erilaisia toimintatapoja.

Tässä työssä ei ole esitetty, minne verkostojen keskustoiminto, informaatioturvallisuuden osaamiskeskus tulisi sijoittaa. Verkostomaisen yhteistyön kehittäminen ja elinkeinoelämän osallisuus muistuttavat CERT-fi:n perustamista ja Kyberturvallisuuskeskuksen toimintaa.

Huoltovarmuuskeskuksen rahoitus suuntautuu ainoastaan huoltovarmuuden tukemiseen. Ratkaisussa voitaisiin yhdistää muitakin rahoituslähteitä laaja-alaisen kokonaisuuden saavuttamiseksi. Osaamiskeskuksen ja verkoston tukemisen lisäksi resursseja voidaan suunnata myös alan tutkimukseen, innovaatiotoimintaan ja koulutukseen. Kansainvälisiä esimerkkejä rahoituskohteista ovat muun muassa vaativan faktantarkastuksen tukipalvelut, alan innovaatiot, kurssit ja pelillistäminen. Toteuttajina näissä ovat olleet yliopistot, yritykset ja järjestöt.

Informaatioturvallisuus on keskeinen osa kokonaisturvallisuutta ja yhteiskunnan elintärkeiden toimintojen turvaamista. Olisi luontevaa, että informaatioturvallisuuden kasvava merkitys huomioitaisiin Yhteiskunnan turvallisuusstrategian (YTS) päivityksessä. Yhteiskunnan turvallisuusstrategiasta on johdettu tärkeitä strategisia dokumentteja, jotka liittyvät myös informaatioturvallisuuteen. Informaatio- ja kyberturvallisuus liittyvät yhteen monessa mielessä, ja ne ovat jopa joiltain osiltaan erottamattomia. Esiselvitys ehdottaa tämän vuoksi yhteisen kansallisen informaatiostrategian luomista tiiviissä yhteydessä kyberturvallisuusstrategian kanssa.

2 INFORMAATIOVAIKUTTAMINEN JA SILTÄ SUOJAUTUMINEN

Informaatiovaikuttaminen on toimintaa, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa[4]. Vääristely voi siis tarkoittaa 1) väärän tiedon lisäksi 2) tiedon kanaviin vaikuttamista tai 3) ymmärtämisen harhauttamista. Informaatiovaikuttamiseen kuuluviksi osiksi voidaan ymmärtää laaja kirjo tavoitteita, tavoitteiden ajajia, käytännön toimijoita, toimintatapoja ja -mekanismeja sekä vaikuttamisen kohteita.

Informaatiovaikuttamisen kohteista ensimmäisiä ovat yhteiskuntaa yhdessä pitävät sidokset, päätöksentekijöihin kohdistuvan luottamuksen rapauttaminen sekä yhteiskunnan toimivuus ja sen perusarvot, kuten demokratia, oikeusturva ja ihmisoikeudet. Käytännön keinoja ovat muun muassa päätöksenteon vaikeuttaminen informaatiohälyllä, päättäjien leimaaminen kyvyttömiksi tai yhteiskunnallisten tilanteiden kärjistäminen.[5]

Informaatiovaikuttamisesta Suomeen on vahvoja epäilyksiä ja näyttöjäkin, mutta havainnot ovat sirpaleisia ja kokonaiskuva on puutteellinen. Informaatiotulvassa lähteiden luotettavuus kyseenalaistetaan joskus syyttäkin, koska yhteiset käsitteet puuttuvat. Ongelman epämääräisyys johtaa puutteellisiin toimintamalleihin ja hitaaseen reagointiin.

Yhteiskunnan on tärkeää kyetä parantamaan informaatioympäristön analysointia ja tiedonjakoa, luomaan sietokykyä ja suojautumista informaatiovaikuttamiselle, joka kohdistuu avoimeen demokraattiseen yhteiskuntaan, sen päätöksentekoon ja kansalliseen turvallisuuteen. Suojautuminen voi tarkoittaa hyvin erilaisia toimia, kuten lainsäädännön kehittämistä, kansainvälisen aineiston alkuperän selvittämistä ja luokittelua sekä viestinnällisiä vastatoimia. Tehtävää vaikeuttaa teknologisen kehityksen kiivas tahti, emme esimerkiksi tunne riittävästi ns. deep faken aiheuttamaa uhkaa ja sen muuntumista.

Informaatiovaikuttaminen voi olla osa hybridivaikuttamista. Sanakirjamääritelmässä hybridivaikuttamista on ”poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen”.

”Hybridivaikuttamista tehdään esimerkiksi informaatio-, kyber-, fyysisten ja taloudellisten operaatioiden avulla hyödyntäen avoimen ja keskinäisriippuvaisen yhteiskunnan erilaisia ominaisuuksia. Hybridivaikuttamisen takana voi olla joko valtiollinen tai ei-valtiollinen toimija.”[6] Hybridiuhkissa pahantahtoinen toimija hyödyntää perinteisiä vastuualuerajoja leikkaavia uhkatekijöitä ja eri vaikutusmekanismien yhdistelmiä[7].

4) https://termipankki.fi/tepa/fi/
5) Informaatiovaikuttamiseen vastaaminen. Opas viestijöille, Valtioneuvoston kanslian julkaisuja 2019:11 URN-osoite http://urn.fi/URN:ISBN:978-952-287-708-6
6) https://termipankki.fi/tepa/fi/haku/hybridivaikuttaminen
7) https://puolustusvoimat.fi/documents/1948673/10330463/Puolustustutkimuksen+vuosikirja+2020.pdf/026d187f-21ce-bc50-6591-f3b1f69a7ed0/Puolustustutkimuksen+vuosikirja+2020.pdf?t=1588589919000

Hybridivaikuttaminen pyrkii ainakin alkuvaiheessa piilottamaan toiminnan tavoitteet, alkuperäiset käskijänsä ja tavoitteensa. Vaikka organisoidun toiminnan taustalla olisi valtio, välikädet vaikeuttavat syyksilukemista. Käsitettä hybridivaikutus voidaan käyttää, kun vaikutusmekanismit ja seuraukset ovat samantapaisia mutta takana ei välttämättä ole laajaa, koordinoitua kampanjaa tai toiminnan kohdentuminen on satunnaista. Tapahtumien alkuperä voi olla vaikkapa luonnonmullistus tai epidemia, jonka vaikutukset kumuloituvat laajaksi yhteiskunnalliseksi ongelmaksi. Vihamieliset toimijat pystyvät imitoimaan, hyödyntämään ja vahvistamaan näitä tilanteita.

Euroopan hybridiosaamiskeskuksen verkkosivuilla korostetaan, kuinka hybriditoimijalla on hyvin monipuolisia keinoja. Lisäksi vihamielinen toimija hyödyntää havaitsemisen ja syyksilukemisen kynnysarvoja ja institutionaalisia jakolinjoja sekä kohteen toimintaa sitovia tai velvoittavia lainsäädännöllisiä tekijöitä[8].

Informaatiouhkia torjuu ja kriisinsietokykyä tukee osaltaan kokonaisturvallisuuden toimintamalli. Sen mukaisesti yhteiskunnan kriittistä toimintakykyä ja varautumista rakennetaan viranomaisten, liike-elämän, järjestöjen ja kansalaisten yhteistyössä[9]. Tämä kuvastaa myös yksilön roolia, hän on turvallisuuden kuluttaja mutta myös sen tuottaja.

8) Hybrid threats as a concept – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats, 24.5.2021.
9) Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös / 2.11.2017

Yhteiskunnan turvallisuusstrategiassa henkinen kriisinkestävyys on yksi elintärkeistä toiminnoista. Sillä tarkoitetaan yksilöiden, yhteisöjen ja yhteiskunnan sekä kansakunnan kykyä kestää kriisitilanteiden aiheuttamat henkiset paineet ja selviytyä niiden vaikutuksilta.

Informaatioympäristössä suunnistava tarvitsee tietoa, taitoa sekä työkaluja. Suomessa henkistä kriisinkestävyyttä rakennetaan muun muassa vahvalla demokratialla, avoimuudella, sanan- ja mielipiteenvapaudella, median riippumattomuudella, koko väestön hyvällä koulutuksella ja medialukutaidolla sekä avoimella ja moniäänisellä kansalaiskeskustelulla.[10]

Informaatioturvallisuutta parantavien toimintojen kirjo on laaja, esimerkkeinä ovat toimijoiden keskinäinen koordinaatio, median osaaminen ja taloudelliset mahdollisuudet, yleinen koulutustaso, medialukutaito, tekninen analyysi, sosiaalisen median analyysi, erilaiset työkalut ja niiden hallinta, koulutus, harjoittelu, datan kerääminen ja datan arkistointi. Kokonaisturvallisuuden toimintamallia seuraten informaatioturvallisuudelle on tarvetta luoda yhteistoiminnan laaja-alainen toimintamalli sekä yhteistyön mahdollistavat palvelut.

Toimenpiteiden mosaiikkia voidaan hahmottaa jakamalla suojautuminen neljään luokkaan: 1. estäminen, 2. kestävyyden parantaminen, 3. havainnointi ja arviointi, 4. vaikutusten hoitaminen.

Kustakin näistä löytyy lukuisia esimerkkejä. Ensimmäiseen luokkaan, estämiseen, kuuluu muun muassa sosiaalisen median yritysten toiminnan sääntely, joka tapahtuu pitkälti Euroopan unionin tasolla. Parempi sääntely voi parantaa samalla käyttäjäkokemusta ja hyödyttää myös sosiaalisen median yhtiöitä. Kestävyyden kehittäminen kuuluu toiseen ryhmään. Sitä parannetaan medialukutaidon kehittämisellä sekä kampanjoilla, joilla muistutetaan yleisöä sosiaalisen median ongelmista. Kolmanteen luokkaan kuuluvat muun muassa uhkien kartoitus ja huhujen monitorointi. Viimeinen luokka on vaikutusten vähentämistä. Sitä voidaan toteuttaa esimerkiksi valmiussuunnittelulla ja harhaisiin radikaalitarinoihin vastaamisella.[11] Taulukkoon 1 on vaiheisiin lisätty eri toimenpidekokonaisuuksia ja konkreettisia toimia. Lista ei ole kattava, sillä suojautuminen kehittyy koko ajan jääden silti jälkeen uhan muuntumisen vauhdista.

Tämä esiselvitys keskittyy edellä olevan jaottelun kakkos- ja kolmosvaiheisiin, mutta laajan tiedonkeruun ansiosta tässä esitetään huomioita myös muista kohdista. Esiselvityksessä on keskustelua punaisella kirjoitetuista aiheista.

10) Valtionhallinnon tehostetun viestinnän ohje – Viestintä normaalioloissa ja häiriötilanteissa Valtioneuvoston kanslian julkaisuja 2019:23 URN-osoite http://urn.fi/URN:ISBN:978-952-287-815-1

11) Mukaeltu lähteestä: https://reliefweb.int/sites/reliefweb.int/files/resources/Weaponization_Social_Media_FINAL_Nov2019.pdf 26.5.2021.

Taulukko 1. ***Informaatiovaikuttamiselta suojautuminen ja joitakin kansainvälisiä esimerkkejä konkreettisista toimista***

Suojautumisen vaiheet	Kokonaisuuksia	Joitakin esimerkkejä konkreettisista toimista
1. Estäminen	Pelote	Kansainvälinen yhteistyö, uskottava kyky vastatoimiin
	Lainsäädäntö	Määräykset vihapuheen poistamisesta, algoritmien läpinäkyvyydestä
	Yritysten toiminnan muu sääntely	EU-tason toimet
	Yritysten omat yhteisösäännöt	Valheellisen henkilöllisyyden kielto, mainontasäännöt, eri ryhmien suojaksi asetetut säännöt
	Yritysten toimet	Väärien tilien poistaminen, koulutus, alustojen tekniset muutokset, yhteistyö
	Kansalaisyhteiskunnan aktiivisuus	Aloitteiden tukeminen
	Kyberturvallinen toiminta	Mediayhtiöiden ja kansalaisten tietoturvan parantaminen, viranomaisten tietoturvalliset välineet
2. Kestävyyden parantaminen	Medialukutaidon parantaminen	Opetussuunnitelmat
	Valistuskampanjat ja popularisointi	Kampanjat, digitaaliset tai perinteiset pelit informaatioturvallisuudesta
	Mediayritysten elinkelpoisuus	Tuki alan hankkeisiin, datan tai työkalujen tarjoaminen
	Valmiussuunnittelu ja varautuminen	Informaatioturvallisuusstrategia ja toimeenpano, kokonaisturvallisuuden toimijoiden yhteistyöfoorumit, valmiustoimikunnat, ennakointi, riskienhallinta
	Yhteistyöverkostojen kartoittaminen	Jaettu tieto toimijoista
	Yhteisöjen tukeminen	Osallistaminen, yhteisöjen mukaan ottaminen
	Koulutukset	Kurssit, oppaat ja ohjeet
	Harjoittelu	Kypsyystason arviointi, organisaation omat ja yhteistyöharjoitukset
3. Havainnointi, paljastaminen ja arviointi	Omien haavoittuvuuksien kartoitus	Vihamielisen toimijan mahdollisten kohteiden arviointi
	Informaatioympäristön kartoitus ja tilannekuva	Informaatiotilannekuvan kokoaminen, yhdisteleminen toisiin tilannekuviin ja jakaminen
	Julkisen digitaalisen / sosiaalisen median seuranta	Keruu, kokoaminen, luokittelu, analysointi, raportointi, arkistoiminen
	Riippumaton faktantarkistus	Itsenäisten toimijoiden tukeminen
	Kansainvälinen yhteistyö	Tiedonjako datasta, analyyseistä, toimintatavoista ja muista työkaluista
	Vaikutusten arviointi	Vihamielisten narratiivinen leviämisen mittaus, väestön tai väestöryhmien mitattu asennemuutos tai käyttäytymisen muuttuminen
4. Vaikutusten hoitaminen	Hälytysmekanismi	Ennalta sovitut ja harjoitetut toimintatavat, viestien nopeutetut hyväksymisprosessit
	Väärään informaation vastaaminen	Attribuutio, kansainvälinen yhteistyö, väärän tiedon korjaaminen, disinformaation levittäjän uskottavuuden rapauttaminen, jakeluun vaikuttaminen
	Yhteistyö	Diplomatia

3 VIRANOMAISTEN VARAUTUMINEN JA HAVAITTUJA INFORMAATIOTURVALLISUUDEN KEHITTÄMISKOHTEITA AINEISTON PERUSTEELLA[12]

Seuraavissa kappaleissa perustellaan aineistosta nousseita huomioita. Kansalliset kehittämisideat liittyivät seuraaviin teemoihin: 1. Käsitteet, prosessit ja resurssit, 2. raportointi ja tilannekuva sekä 3. osaaminen. Huoltovarmuuskeskuksen tukitoimet voivat kohdistua vain osaan kehittämisideoista, ja esimerkiksi kokonaisuuden kehittäminen edellyttänee kansallista strategista ohjausta.

Jatkohankkeet ja muut toimet eivät kuitenkaan saa samentaa yksittäisen toimijan omaa roolia. Varautuminen informaatiohäirintää vastaan, kuten kaikki varautuminen, on ensisijaisesti jokaisen organisaation omalla vastuulla.

3.1 Käsitteet, prosessit ja resurssit

Kysely- ja työpajakeskusteluissa vahvistui näkemys, että ongelmien havainnointi on osa perustehtävää ja sen parissa toimivien asiantuntijoiden normaalia toimintaa. Mutta koska ongelmaan on herätty vasta viime vuosina, työnjako ei ole kuitenkaan yhtenäistä.

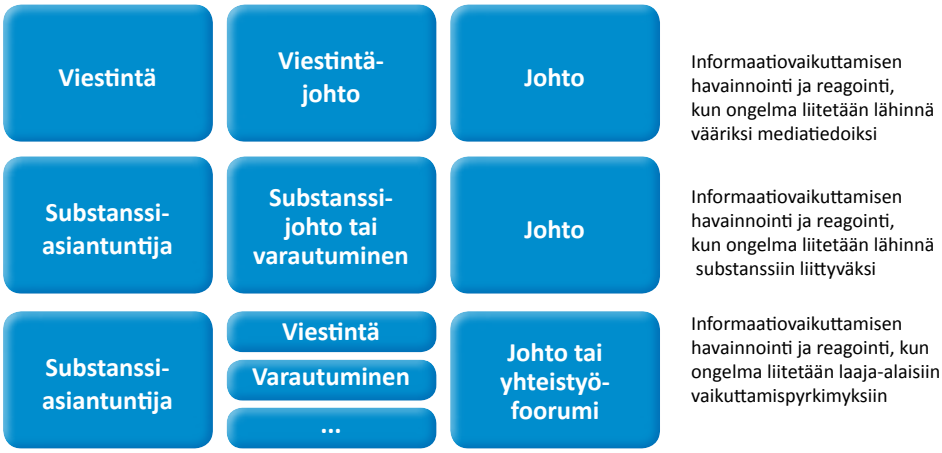
Informaatioturvallisuus, -uhat ja -vaikuttaminen käsitetään eri tavoin. Kyselyvastausten perusteella näyttää siltä, että havaintoja tarkastellaan pitkälti oman yksikön viitekehyksestä. Informaatioturvallisuus on kuitenkin poikkileikkaava aihe. Tulkintojen vaihtelu on osoitus ilmiön monimuotoisuudesta ja kehittymisestä. Epätietoisuus **käsitteistä** jarruttaa myös yhteisten toimintatapojen kehittämistä.

Tämän hetken tilanne viranomaisissa on se, että informaatiovaikuttamisen havainnointi liittyy erityisesti viestijöiden tehtäviin. Tätä puoltaa se, että he seuraavat erilaisia mediakatsauksia ja valmistelevat julkisuuteen suuntautuvia viestejä. Voi olla, että substanssialueista irrallaan olevana yhteisenä toimintona viestinnällä on hyvät mahdollisuudet huomioida organisaation eri osien näkemyksiä. Mutta jos viestintä nähdään pelkkänä työkaluna, uhatkin nähdään helposti pelkkinä maineriskeinä tai väärinymmärryksinä. Jos oma viestintä käsitetään strategisemmin, on helpompaa arvioida paremmin myös vihamielisten toimijoiden viestinnän strategisuutta.

Toisaalta substanssiasiantuntijat voivat havainnoida myös tehtävissään informaatiovaikuttamista. Tässä tapauksessa oman alan osaamisesta voi olla merkittävää hyötyä. Toisaalta haasteena voi olla hahmottaa, kuinka oman informaatiotilan tapahtumat vaikuttavat omaan substanssitehtävään.

12) Luku on kooste seuraavista aineistoista: Huoltovarmuuskeskus lähetti ministeriöille kyselyn niiden sekä niiden alaisen hallinnon tehtävistä ja työnjaosta, johon vastaukset saatiin kesäkuun 2021 aikana. Aiheesta keskusteltiin myös 18.6.2021 HVK:n ja Valtioneuvoston kanslian johtamassa työpajassa. Näiden lisäksi selvitystä varten käytiin keskusteluja Mediapoolin, teknologiayritysten, median, tutkimuksen ja koulutuksen edustajien kanssa. Selvitystyön tässä vaiheessa tiedonhankintaa ei ulotettu laajemmin elinkeinoelämään. Työhön osallistettiin kesän aikana noin sata henkilöä ja 11 kansainvälistä tahoa.

Kaavakuva:



Havainnointia ja asioiden yhdistämistä tekevät myös valmiushenkilöt ja muut riskinhallinnan osaajat. Heidän vahvuutenaan on nostaa havaitut tilanteet monialaiseen keskusteluun. Tiedonvaihtoon sopivat toimijoiden sisäiset valmiustoimikunnat tai laajemmat yhteistyöfoorumit. Osalle ministeriöistä ja alaisesta hallinnosta tämä on arkipäivää. Valtioneuvoston kanslialle, ulkoministeriölle ja perinteisille turvallisuustoimijoille informaatioympäristöstä tuleva ongelma on helpommin sovitettu osaksi aiempaa toimintaa. Näissä paikoissa informaatioturvallisuuteen liittyviä tehtäviä on joidenkin virkamiesten toimenkuvissa. Parempi resursointi ja koetut toimintatavat auttavat ilmiöiden havaitsemista ja niihin reagoimista. Tätä mallia kuvaa kaavakuvan alin rivi. Mallin hyötyihin kuuluu havaintojen nopeampi jakaminen eri osallistujien kanssa.

Työpajassa esitettiin, että pitkäjänteisyyttä ja järjestelmällisyyttä parantaisi, jos ongelmaan varautuminen olisi vähemmän aiheeseen perehtyneeseen henkilöön sitoutunutta. Varautuminen edellyttää parempia prosesseja. Ohjeet, työjärjestykset ja työnkuvat eivät tällä hetkellä riittävän hyvin tunnista informaatioturvallisuuden tehtäväkenttää. Yhteiset käsitteet ja lainsäädännöllinen tarkastelu antavat selkänojaa organisaatioiden toiminnalle.

Kansallisen toimintakyvyn varmistaminen edellyttää ennakointia. Ennakoinnissa on arvioitava, mikä on toiminnan kriisinkestävyys: kuinka hyvin informaatioympäristöämme suojaavat toimintatavat kestävät tilanteen voimakkaan kriisiytymisen, jopa sodan. Informaatioturvallisuus ja -resilienssi sisältävät myös informaatiopuolustuksen. Tässäkin on arvioitava, kuinka pystymme näkemään tilanteen eskaloitumisen tai kuinka siviiliyhteiskunta pystyy tukemaan maanpuolustusta sodan aikana.

3.2 Raportointi ja tilannekuva

Raportoinnissa, tilannekuvassa tai muodostuvassa tilannetietoisuudessa on huomioitava, että yhteiskunta ja toimintaympäristö ovat jatkuvassa muutoksessa. Liian mekanistiset näkemykset uhasta estävät uusien haasteiden havainnoinnin. Esimerkkinä voi toimia informaatiohäirinnän lähtömaa. Jos analyysin aloittaminen edellyttää, että taustalla on ulkomainen valtiollinen taho, niin prosessi

on osin nurinkurinen. Tällaisessa tapauksessa syyksilukeminen tapahtuisi käytännössä ennen oletetun vihamielisen toiminnan analyysiä. Toinen lähtökohta on, että viranomaiset eivät ota alussa asiaan kantaa, vaan arvioivat asiaa ensiksi vaikutusten kautta. Vertailun vuoksi vaalivaikuttamiseen varautumisessa vuonna 2019 todettiin, että uhan lähteen nostaminen tarkastelun keskiöön vaikeuttaa varautumista ja hidastaisi mahdollisia vastatoimia.

3.3 Osaaminen

Ennakointi ja joustavuus edellyttävät laaja-alaista osaamista. Hallinnonaloilla on tehtäviin ja asenoitumiseen liittyviä eroja. Osa eroista on kuitenkin perusteltuja; eri intressiensä mukaisesti hallinnonalat voisivat ottaa kantaakseen erilaisia alueita yhteisestä informaatioympäristön seurannasta.

Osaamisen taso on Suomessa hyvin vaihtelevaa, ja tarpeet ovat erilaisia. Koko väestö tarvitsee parempaa medialukutaitoa ja ymmärrystä informaatiovaikuttamisen mekanismeista. Lisäksi tiettyjen alojen asiantuntijat tarvitsevat hyvin erikoistunutta koulutusta. Informaatioturvallisuuden osaamistarpeet ovat erilaisia myös hallinnon sisällä. Perinteiseen media-analyysiin ja viestintään löytynee osaajia helpommin kuin data-analyysiin ja analyysityökalujen suunnitteluun. Työpajassa pohdittiin, että on helpompi päivittää nykyisten asiantuntijoiden osaamista kuin saada rekrytoitua uusia ammattilaisia.

Koulutus ja oppaat syntyvät pitkälle osallistujien omista intresseistä. Valtioneuvoston kanslia on julkaissut alaan liittyviä ohjeita ja oppaita, osa yhteistyössä Ruotsin Myndigheten för Samhällskyd och Beredskap (MSB):n ja Lundin yliopiston kanssa.

Muun muassa Aalto-yliopisto, Jyväskylän yliopisto ja Maanpuolustuskorkeakoulu antavat aihepiiriin liittyvää koulutusta. Maanpuolustuskoulutusyhdistys tarjoaa myös tehtäväkenttään liittyviä kursseja. Lukuisat yliopistot ja ammattikorkeakoulut kouluttavat niin viestinnän kuin turvallisuuden ammattilaisia. Vahvistuva koulutusyhteistyö muun muassa tukee toimijoita ja kurssien markkinointia.

Informaatioturvallisuuteen liittyvät harjoitukset on koettu onnistuneiksi ja tarpeellisiksi, ja niitä toivotaan lisää. Harjoituksissa pystytään arvioimaan osallistujien tai organisaatioiden kypsyystasoa erityisesti häiriötilanteissa.

3.4 Muita huomioita

Työpajassa keskusteltiin myös median roolista. Vahva, itsenäinen ja moniääninen media on demokratian perusedellytyksiä. On tärkeää, että tiedotusvälineet tekevät omat journalistiset ratkaisunsa. Journalistiset ratkaisut edellyttävät tietoa ja osaamista, esimerkiksi nykyään yhä tärkeämmäksi käyvää data-analyysiä. Oletettavasti osaamisen taso ja pääsy dataan on suomalaisissa tiedostusvälineissä vaihtelevaa.

Tiedotusvälineissä tehdään jatkuvasti faktantarkistusta mutta niistä riippumatonta tarkistuselintä ei ole. Tällä hetkellä ei ole selvää, kuinka sellainen tulisi järjestää vai tulisiko lainkaan. Lisäksi toimittajat ja sosiaalisen median vaikuttajat, niin sanotut influensserit, ovat raportoineet heihin kohdistuneesta maalituksesta. Vaikuttajat eivät myöskään pysty hakemaan tukea työnantajaltaan. Työpajassa pohdittiin median kiinnostusta eräänlaiseen informaatioturvallisuuden vihjetietoon. Median sivuilla oleva ”infovihjenappi” olisi uhrin keino kertoa toimitukselle kokemastaan informaatiohäirinnästä.

Keskusteluissa nousi esille riippumattomuuden merkitys sisältöjen analysoinnissa. Valtiollinen faktantarkastus on konseptina mahdoton. Toisaalta teknisten tai kvantitatiivisten huomioiden julkistaminen sosiaalisessa mediassa julkisesti leviävästä aineistosta olisi ongelmattomampaa. Samantyyppisestä toiminnasta on esimerkkinä Kyberturvallisuuskeskuksen tarjoama informaatio kyberturvallisuutta uhkaavista ilmiöistä.

Tiedotusvälineet voivat hyötyä myös informaatioturvallisuuteen liittyvästä data-aineistosta, työkaluista ja koulutuksesta. Tällainen toiminto edellyttää kuitenkin sopimuksiin ja lainsäädäntöön liittyviä erillistarkasteluja.

Median kyky havaita ympäröivästä maailmasta informaatiovaikuttamista on myös taloudellinen kysymys. Erityisesti alueellisilla medioilla on vain vähän resursseja tehdä data-analyysiä. Tämä on sekä aineistoon että osaamiseen liittyvä ongelma. Myös suuret mediatalot voivat hyötyä uusista data-aineistoista, mutta niillä on paremmat edellytykset kouluttaa omat asiantuntijansa ja luoda menetelmänsä saatavilla olevan aineiston hyödyntämiseen.

4 NÄKEMYKSIÄ VERROKKIMAISTA[13]

Esiselvitystä varten käydyissä ulkomaalaisten viranomaisten haastatteluissa kanssa toistuivat samat laillisuuden ja demokratian vaalimisen periaatteet. Haastattelut osoittivat, että kaikki verrokkimaat ja -organisaatiot ovat huolissaan tilanteesta ja panostavat merkittävästi aiheeseen. Keinovalikoima oli laaja ja painotukset erilaisia. Osa eroista johtui lähestymistavoista, organisatorisista perusratkaisuista ja osa ongelmiin heräämisen ajankohdasta.

Virolainen everstiluutnantti Uku Arold on artikkeleissaan[14] verrannut Suomen, Ruotsin ja Baltian maiden psykologista puolustautumista. Viron kokemusten perusteella hän asettaa suojelun keskipisteeseen perustuslailliset arvot, demokratian suojelun ja kulttuurisen jatkuvuuden. Hänen toinen johtopäätöksensä on, että tehtävä tulisi toteuttaa nykyisen toimijaverkoston valmiuksia kehittämällä ja yhteistyöllä. Tämä tekee järjestelmästä joustavamman sen sijaan, että psykologisen puolustuksen tehtävät keskitettäisiin yhteen laitokseen, oli se sitten opetusministeriö, valtioneuvoston kanslia tai muu. Yhteistyöhön panostaminen hälventää myös pelkoja "propagandaministeriöstä".

Kehitystyö lähtee usein nykyisten kansallisesta yhteistyön vahvistamisesta. Käynnistävänä tekijänä on joko negatiivinen tapahtuma kuten Krimin valtaus tai varautuminen tärkeään tapahtumaan kuten vaaleihin. Prosessin lopputuloksena tai jo alussa päätettynä tavoitteena on erillinen yksikkö. Yleiskuvaksi jäi, että yksikön uskottavuus edellyttää etäisyyttä poliittisiin toimijoihin, riittävää resursointia ja yhteistyömekanismeja. Tehtävän onnistumiseksi mandaatin tulee olla selkeä, ja yksikön on tuotettava selkeitä hyötyjä muillekin viranomaisosapuolille.

Yleisenä suuntauksena näkyy prosessien kehittäminen informaatioturvallisuuden parantamiseksi. Useissa maissa ja Euroopan unionissa päätöksentekijät ovat heränneet informaatiotilaamme kohdistuviin uhkiin. On tärkeää päästä päätöstentekijöiden agendalle, mutta huomiolla on myös haittansa. Disinformaatioon ja vihamielisen vaikuttamiseen vastaamisen varjolla voidaan hyviin hankkeisiin ujuttaa aktiviteetteja, jotka eivät sinne kuulu.

Kansainvälinen yhteistyö on elintärkeää vaikuttamisyritysten rajoittamisessa. Informaatiotilan rajattomuus, yhdysvaltalaiset sosiaalisen median jätit, Euroopan unionin markkinoiden koko, sen kyky reguloida ja sanktioida vihamielisiä toimijoita sekä jälkimmäisten kyky peittää jälkensä perustelevat niin maiden keskinäisiä kuin kansainvälisten organisaatioidenkin järjestelyjä.

13) Lukua varten haastateltiin asiantuntijoita Pohjoismaista, Baltian maista, Alankomaista, Tshekin tasavallasta ja Euroopan unionin ulkosuhdehallinnosta. Esiselvitystä tukivat myös Euroopan hybridiuhkien torjunnan osaamiskeskuksen ja Naton strategisen viestinnän osaamiskeskuksen edustajien kanssa käydyt keskustelut.

14) Põhjala ja Balti riikide psühholoogilise kaitse süsteemide kontseptuaalsed ja praktilised alused, Sisekaitseakadeemia, Sisejulgeoleku instituut, Tallinn 2021, Juurvee, I. & Arold, U. (2021). Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats, Icono 14, 19(1), 70-94. doi: 10.7195/ri14.v19i1.1628

Informaatioympäristön seuranta ei ole uutta. Perinteisen lehdistökatsauksen rinnalle on nousemassa sosiaalisen median seuranta, joka ei ole kuitenkaan ongelmatonta. Lainsäädäntökysymykset liittyvät erityisesti toimijoiden eri mandaatteihin, yksityisyydensuojaan sekä tekijänoikeuksiin. Tällä hetkellä kansalliset lainsäädännöt ja eri maissa olevien virastojen erilaiset toimivaltuudet johtavat hyvinkin erilaisiin käytäntöihin.

Seuraavissa kappaleissa poimintoja Ruotsin, Viron, Liettuan ja Alankomaiden osin erilaisista lähestymistavoista. Muiden haastateltujen maiden kehityslinjat ovat samansuuntaisia tai Suomea vastaavia.

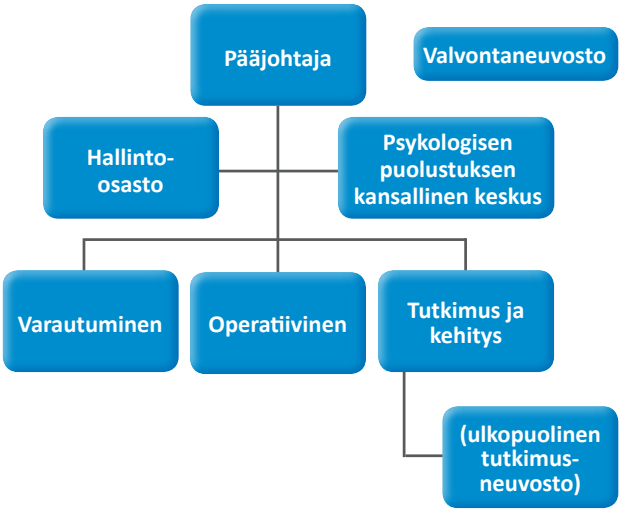
Ruotsalainen lähestymistapa on tiivistetty uudessa Hybrid CoE:n julkaisussa muutamaan kehotukseen:

1. Toteuta kokonaisvaltainen riski- ja haavoittuvuusarviointi
2. Keskity em.arvioinnin perusteella resilienssin vahvistamiseen
3. Arvioi pelotetekijöitä
4. Muodosta kokonaisvaltainen ja tehokas yhteistyö- ja koordinaatiomekanismi
5. Muodosta ja harjoita varoitus- ja havainnointimekanismeja
6. Kouluta ja harjoita keskeisiä toimijoita
7. Toteuta strategista viestintää vihamielisten toimijoiden aikeiden hillitsemiseksi.[15]

Ruotsalaiseen hallintomalliin kuuluvat suhteellisen itsenäiset ja hyvin resursoidut virastot. Niin myös tällä alalla, jossa on käynnissä merkittävä hallinnollinen muutos. Myndigheten för Samhällskyd och Beredskap (MSB):n rooli on ollut keskeisin informaatiovaikuttamisen torjunnassa[16]. Se kuitenkin muuttuu, kun uusi psykologisen puolustuksen virasto, Myndigheten för psykologiskt försvar tulee hoitamaan informaatioympäristön suojelemiseen liittyviä tehtäviä[17].

15) 0210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf
16) 0210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf
17) En ny myndighet för att stärka det psykologiska försvaret, Betänkande av Psykförsvarsutredningen, SOU 2020:29, Stockholm 2020, Kommittédirektiv, Inrättande av Myndigheten för psykologiskt försvar, beslut vid regeringssammanträde 18.3.2021.

Kuva: ***Ehdotus psykologisen puolustuksen viraston organisoinnista***



HENKILÖSTÖ		
Osasto	**Toiminto**	**Henkilötyövuodet**
Johto ja tuki	Pääjohtaja, sihteeri, hallintojohtaja, turvallisuusjohtaja, jurisit, HR, talous, arkisto, vahtimestari, kontrolleri, viranomaisviestintä	12
Operatiivinen	Päällikkö, analyysi, strateginen viestintä, yhteistyö, yhteensovittaminen, tilannekeskus, varautuminen	18
Varautuminen	Päällikkö, analyysi, yhteistyö, yhteensovittaminen, strateginen viestintä	10
Tutkimus ja kehitys	Päällikkö, analyysi, viestintä, tutkimuksen ja ulkopuolisen tutkimus-neuvoston hallinto, koulutus, harjoitukset, sodanajan organisaation kehittäminen	8
Yhteensä		**48**

Vuoden 2022 aloittavassa virastossa tulee suunnitelmien mukaan työskentelemään noin 48 henkilöä[18]. Uudessa virastossa johdetaan psykologisen puolustuksen koordinaatiota, tuetaan kansakuntaa ja hallituksen työtä tällä saralla.

Virossa aihepiiriin liittyvässä toiminnassa näkyvä yhteistyön merkitys sekä varautuminen eritasoisiin riskeihin muistuttavat suomalaista kokonaisturvallisuuden lähestymistapaa. Virolaiset ovat lisäksi muodostaneet yksikön, jolla on selkeä vastuu tästä toiminnasta. Selkeälle roolitukselle on syynsä: ajatushautomo tai yhteistyökokoukset eivät pystyisi tuottamaan riittäviä edellytyksiä strategisen viestinnälle vakavampien kriisien sattuessa.

18) En ny myndighet för att stärka det psykologiska försvaret, Betänkande av Psykförsvarsutredningen, SOU 2020:29, Stockholm 2020, Kommittédirektiv, Inrättande av Myndigheten för psykologiskt försvar, beslut vid regeringssammanträde 18.3.2021

Virossa strategisen viestinnän yksikkö on sijoitettu valtioneuvoston kansliaan. Se on selkeästi erillään hallituksen viestinnästä, ja yksikön mandaatti on kansallisen puolustuksen kehittämissuunnitelmassa vuodelta 2017.

Liettuassa informaatioympäristön systemaattista arviointia on hiottu verrokkimaista pisimpään. Strategisen viestinnän prosesseja säännellään asetuksella, jossa on määritelty alan peruskäsitteet, tiedonkulun menettely, tietotapahtumien riskimittarit ja toimet niiden tapahtuessa.

Alankomaissa sisäministeriön johdolla toteutettavassa toiminnossa on kolme painopistettä.

1. Hybriditoiminnan estäminen, esimerkiksi sosiaalisen median ja EU-sääntelyn avulla
2. Informaatioaseman vahvistaminen
3. Reagointi

Alankomaalainen haastateltu korosti, että informaatioaseman vahvistaminen vaatii toimia useilta tahoilta. Esimerkiksi vaaleissa etsitään koordinoituja epäaitoa käyttäytymistä, kuten botteja ja epäaitoa viestimäärien kasvattamista. Fokus on toimintatavassa, ei sisällössä. Ns. kovan turvallisuuden toimijoiden tehtävät ovat tästä erillään, eikä haastattelussa näistä kerrottu. Informaatioaseman vahvistaminen sisältää myös tukirahoja yliopistoaloitteille, joissa etsitään uhan uusia ilmenemismuotoja. Vaaleja varten rahoitusta annettiin DROG-hankkeelle, jonka sivustolta löytyy muun muassa informaatiovaikuttamiseen liittyvä peli. Nykyaikaisilla toimintatavoilla koulutus tavoittaa uusia kohderyhmiä. Vaalien aikaan projekti tuotti aineistoa myös journalisteille. Lisäksi maassa tuetaan medioiden faktantarkastusta, vaikka valtiolla ei ole mitään suoraa kontaktia tähän toimintaan. Reagointi on useimmissa tapauksessa median ja tutkimuksen tehtävä, mutta vakavissa kriiseissä käytetään esimerkiksi diplomaattisia keinoja ja Euroopan unionia.

Maiden erilaiset oivallukset signaloivat samalla vihamielisille toimijoille, että myös avoimet ja vapaat yhteiskunnat pystyvät puolustamaan informaatioympäristöään.

5 AINEISTOSTA NOUSSEET KEHITTÄMIS-ESITYKSET SUOMEN INFORMAATIO-TURVALLISUUDEN PARANTAMISEKSI

Esiselvityksessä on kartoitettu toimijoiden mahdollisuuksia toimia verkostomaisesti yhteiskuntaa vahingoittamaan pyrkivän informaatiovaikuttamisen tunnistamiseksi ja siltä suojautumiseksi.[19]

Kansainväliset esimerkit osoittavat myös, mitkä voisivat olla kehittämissuuntia. Huoltovarmuuskeskuksella voi olla vain rajattu rooli laajassa tehtäväkentässä.

Informaatioturvallisuuden kehittäminen voidaan nähdä erilaisten päämäärien kautta. Niitä ovat esimerkiksi informaatiovaikuttamisen tunnistamisen ja uhalta suojautumisen kehittäminen ja tiedonjako informaatiouhkista sekä yleisemmin tietoisuuden ja osaamisen lisääminen viranomaisten, median ja kansalaisten joukossa. Huoltovarmuuskeskus voi olla tukemassa näitä päämääriä tukevia aloitteita ja yhteistyötä, mutta sen mandaattiin ei kuulu tähän liittyvä strateginen ohjaus. Esiselvityksessä esitettävä pilotointi tarjoaisi ainutlaatuisia kansallisia syötteitä mahdolliselle strategisemmalle työlle. Esiselvitys ehdottaa informaatio- ja kyberturvallisuusstrategian tiivistä yhteensovittamista. Strategia osoittaa valtion tahtotilan, ruokkii jatkuvaa kehitystä ja yhtenäistää jatkohankkeita. Tässä strategiassa pystyttäisiin myös huomioimaan informaatiopuolustuksen rooli osana informaatioturvallisuutta ja -resilienssiä.

Tässä työssä ehdotetaan suunnittelutyön etenevän pilotoinniksi, jossa kokeiltaisiin uusia yhteistyömuotoja verkostoituneiden toimijoiden kesken. Verkostossa on keskustoiminto (työnimeltään Informaatioturvallisuuden osaamiskeskus) ja itsenäiset mutta verkostoituneet kumppanitoimijat (työnimeltään informaatioanalyysiryhmät). Verkostomaisen toiminnan laajentamiseksi Huoltovarmuuskeskus voisi etsiä rahoituskeinoja, joilla kannustaa media-alan, tutkimuksen ja järjestöjen informaatioturvallisuuden aloitteita. Kansainvälisiä esimerkkejä näistä ovat muun muassa itsenäinen faktantarkastus, alan innovaatiot, koulutusohjelmat ja pelillistäminen.

Alaluvuissa käydään läpi edellä mainittuja ehdotuksia.

5.1 Informaatioturvallisuuden osaamiskeskus -toiminto

Informaatioturvallisuuden osaamiskeskus on toiminto, joka palvelisi kansallisen osaamisen yhteyspaikkana ja verkoston hallinnoijana. Se toimisi yhteyspisteenä eri toimijoille tukien muiden toimijoiden osaamista. Osaamiskeskus ja sen yhteistyöverkostot etsisivät viitteitä informaatiovaikuttamisesta, keinoja sen havainnointiin ja vaikuttamiselta suojautumiseen. Sitä vastoin osaamiskeskukselle ei kuuluisi motiivien arvioiminen, syyksilukeminen tai vastatoimista päättäminen. Tällaisissa tapauksissa vastuu on toimivaltaisella viranomaisella tai poliittisella johdolla.

19) Luku on kooste aiemmissa luvuissa esitetyistä aineistoista. Viranomaisten kantoja on selvitetty kyselyin, työpajoissa ja tapaamisissa. Tiedonhankintaa on täydennetty Mediapoolissa sekä haastatteluissa. Keskusteluja on käyty median, tutkimus- ja yritysmaailman sekä verrokkimaiden viranomaisten kanssa.

Osaamiskeskuksen toimintatavat voidaan jakaa kokonaisuuksiin:

1. Verkostojen hallinta, osaamisen ja tietoisuuden lisääminen
2. Datalähteet, datan jäsentäminen ja tietovarannot
3. Tiedon jalostaminen, tietotuotteet ja -palvelut sekä

5.1.1 Verkostojen hallinta, osaamisen ja tietoisuuden lisääminen

Osaamiskeskus-toiminnon tarkoituksena on tukea elinkeinoelämää, kansalaisia ja viranomaisia tarjoamalla dataa, osaamista ja työkaluja. Osa tuotteista ja palveluista olisi yhteistä ja julkista, osa eriytettyä.

Osaamisverkostossa nykyisiä yhteistyömuotoja lavennettaisiin ja vakiinnutettaisiin sekä kehitettäisiin käsitteistöä. Osaamiskeskukselta tuleva tuki olisi ensisijaisesti tiedon ja osaamisen siirtoa niin toimivaltaisen viranomaisen kuin median ja suuren yleisön hyödynnettäväksi. Viranomaisten välisessä toiminnassa huomioitaisiin myös kriisiajan vaatimukset esimerkiksi turvallisista yhteyksistä. Sisäisten prosessien kehittäminen on kunkin toimijan omalla vastuulla.

Osaamiskeskuksen kiinnostuksen ensisijaisina kohteina olisivat luotettavuuden arvioimiseen, vihamielisen informaatiovaikuttamiseen sekä uhkien muuttumiseen liittyvät aiheet, kuten käsitteet, kvantatiiviset menetelmät, koneoppiminen ja tekoäly. Tutkimusagenda kuitenkin muotoutuu, kun tietoa karttuu.

Yhteistyöverkoston kautta voidaan toimittaa myös toiveita, mitä Suomessa tarvitaan. Mahdollisuuksiensa puitteissa osaamiskeskus tekisi tai teettäisi informaatioturvallisuuteen liittyviä työkaluja. Verkostomaisen toiminnan kehittämiseksi osaamiskeskus kannustaisi taloudellisesti informaatioturvallisuutta tukevia aloitteita. Toteuttajina voisivat olla viranomaiset, media, tutkimusmaailma ja järjestöt. Innovatiiviset, nopeasti toteutettavat työkaluhankkeet, hackathonit ja koulutukset olisivat osaltaan levittämässä informaatioturvallisuuden kulttuuria Suomeen. Tämä voi olla myös keino kielivähemmistöjen tai muiden huonommin tavoitettujen ryhmien huomioimiseksi. Itsenäisen ja erillisen faktantarkastuksen tukeminen voisi olla myös tuen saajana.

Paremman osaamisen ja prosessien kehittämisen ansiosta Suomi olisi varteenotettavampi toimija kansainvälisessä yhteistyössä. Tämä parantaisi otetta kansainvälisiin kumppaneihin ja erityisesti sosiaalisen median alustoihin. Viranomaispuolella yhteistyöjärjestelyt voivat olla jo toimivat, mutta yritysyhteistyö kansainvälisten jättiläisten kanssa edellyttää Suomelta vahvaa asemaa informaatioturvallisuuden toimijana.

Esiselvitys ehdottaa, että osaamiskeskus rakentaisi pysyvät suhteet Ruotsin psykologisen puolustuksen virastoon. Järjestelystä koituu eniten hyötyä lähettävälle ja vastaanottavalle puolelle, jos se toteutetaan työkiertona.

5.1.2 Datalähteet, datan jäsentäminen ja tietovarannot

Osaamiskeskuksen tarkoituksena on kerätä ja analysoida digitaalisessa, erityisesti sosiaalisessa mediassa olevia julkisia ja avoimia aineistoja. Nämä voisivat olla tekstiä, kuvaa tai ääntä. Aineiston

kerääminen ja jäsentäminen olisivat pitkälle automatisoituja. Arkistointi tarjoaa vertailutiedon asiantuntijoiden käyttöön. Normaalin määrittäminen auttaa arvioimaan, milloin yhteiskunta tai yksittäinen toimija kohtaa jotain vakavaa tai kuinka vihamieliset narratiivit kehittyvät. Yksittäisen henkilön aktiviteetteja järjestelmä ei seuraa.

Kansallisen data-altaan perustaminen edellyttää niin lainsäädännöllistä kuin teknistäkin erillistarkastelua, jotta edellä mainittuihin tavoitteisiin voidaan päästä. Tässä vaiheessa epäselvyyttä on seuraavista aihepiireistä: datan saatavuus, hyödynnettävyys ja tietoturvallisuus erilaisissa tilanteissa, data-altaan pääsynhallinta ja käyttäjäryhmien erilaiset oikeudet, sosiaalisen median yritysten käyttäjäehdot, tekijänoikeudet ja yksityisyyden suoja.

5.1.3 Tiedon jalostaminen, tietotuotteet ja -palvelut

Osaamiskeskus jalostaisi itse dataa erilaisiksi tietotuotteiksi ja -palveluiksi. Osaamiskeskus toteuttaisi tässäkin vain niitä tehtäviä, joita toiset eivät tällä hetkellä tee. Tietotuotteiden ja -palveluiden tuottamisessa organisatorinen lokero, niche, löytyisi kyvystä analysoida hallinnonalat poikkileikkaavia, merkittäviä digitaalisia data-aineistoja, usein kvantitatiivisin menetelmin informaatiovaikuttamisen tunnistamiseksi ja siltä suojautumiseksi.

Osaamiskeskuksen oma analyysi ei lähtökohtaisesti puutu tekstin sisältöön ja sen oikeellisuuteen. Selvitettävänä on lähinnä aineistossa olevat, epäaitoa toimintaa kuvaavat piirteet ja mahdolliset viitteet informaatiovaikuttamiseen. Tekninen analyysi datan piirteistä voi osoittaa, että kyseessä on epäaitoa käyttäytymistä, kuten botteja ja väärien tilien avulla kasvatettua huomiota tai viitteitä deep fakesta. Klusteroimalla voidaan selvittää, mihin muihin aineistoihin, lähteisiin tai viittaajiin uusi disinformaatio kytkeytyy. Tällä tavoin voidaan löytää sekä epäaitoa käyttäytymistä että valtiollisten narratiivien kaiuttamista. Trendianalyysit voivat osoittaa tiettyjen ominaisuuksien yleistymistä.

Tällaiset analyysit olisivat lähtökohtaisesti julkisia, kun syyksilukemista ei tehdä. Aineistoa myös peilataan mahdollisesti toisessa viranomaisessa yhteiskunnan haavoittuvuuksiin ja pohditaan toiminnan vaikutusta yhteiskunnalle. Tällöin julkistaminen ei ole aina perusteltua.

Kansainvälisten kontaktiensa ansiosta osaamiskeskus pystyisi välittämään tietoa myös muualta kerätyistä, julkisista havainnoista oman analyysin lisäksi.

Säännöllisiä raportteja voisivat olla epäaidosta toiminnasta kertova raportti ”informaatiosää”, riski-indikaattori ja trendianalyysi niiltä osin kuin nämä eivät kuulu toisen viranomaisen tehtäviin. Mahdollisuuksien mukaan tarjooma on osin itsepalvelua. ”Mistä tämä on kotoisin” kertoisi aineiston alkuperästä tarjoten käyttäjälleen mahdollisuuksia arvioida itse aineiston uskottavuutta. Ideoiden käyttökelpoisuutta voidaan pilotoinnissa arvioida.

Alan kehittyessä voimakkaasti tiedon jalostaminen muuttuu. Kontekstualisointi ja uhka-arviot on tehty perinteisesti ihmisanalyytikoiden toimesta, mutta koneoppiminen ja tekoäly ovat tulossa tähänkin. Luokitteluanalyysin kehittyminen on tästä eräs osoitus. Osaamiskeskus olisi kehittämässä menetelmiä, tuomassa niitä maailmalta ja olisi kannustamassa muita kehitystyöhön projektirahoituksen tai kilpailujen avulla. Mahdollisuuksien mukaan nettisivuille tarjotaan opastus työtavoista tai työkaluista, kuinka eri toimijat voivat itse hyödyntää dataa. Tästä hyötyisivät esimerkiksi tutkivat toimittajat ja muu mediayhteisö.

5.1.4 Osaamiskeskuksen resursointi kansainvälisten esimerkkien valossa

Osaamiskeskusta tarkastellaan tässä työssä funktiona, ei virastona. Osana suunnitteluprosessia on silti arvioitava, mitä resursseja toimenpiteet edellyttäisivät. Arvioinnin pohjana ovat kansainväliset esimerkit.

Ruotsin psykologisen puolustuksen virastossa on henkilötyövuosiksi suunniteltu kokonaisuudessaan 48. Osaamiskeskus vertautuu parhaiten ruotsalaisviraston kahdeksan henkilön tutkimus- ja kehitysyksikköön. Vertailun vuoksi Ranska on käynnistämässä yksikköä, jonka tehtävänä on monitoroida, havaita ja luonnehtia ulkomailta tulevia disinformaatio-operaatioita. Kokoonpano on 65 henkilöä[20].

Aineiston perusteella näyttää siltä, että uuden kyvykkyyden rakentaminen edellyttää erilaisia rooleja. Verkostoyhteistyön kehittäminen, uusimman tutkimustiedon tuominen, kehittäminen ja jakeleminen, data-analyysin rakentaminen ja toteuttaminen, koulutus ja kokonaisuuden johtaminen ovat pohdittuja tehtäviä.

Toiminta voidaan käynnistää vaiheittain. Rekrytointi voisi käynnistyä osaamispohjan laajentamisesta, suunnittelusta ja harjoitustoiminnasta. Hallinnossa ja viestinnässä tukeudutaan mahdollisuuksien mukaan isäntäorganisaatioon.

Budjettivaraus tehdään DT2030-ohjelmassa.

20) Les dessous de «Viginum», la future agence contre les manipulations de l'information – Libération (liberation.fr), selvityksessä 0210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf

5.2 Verkostoituneet informaatioanalyysiryhmät

Huoltovarmuuskeskus haluaa tukea eri toimijoita, kun ne tekevät huoltovarmuuteen liittyviä tehtäviään. Tehtävät ovat kuitenkin hyvin erilaisia elinkeinoelämässä ja viranomaisissa. Toimijat seuraavat mediaa ja muuta informaatioympäristöä omien mandaattiensa ja resurssiensa mukaisesti. Kehitettävän konseptin tulee huomioida osallistujien erilaisuus.

Informaatioanalyysiryhmiksi on tässä kuvattu laajaa kirjoa erilaisia toimijoita, jotka yrittävät ottaa selkoa mahdollisesta informaatiovaikuttamisesta. Esimerkiksi kampanjoiden motivaatioiden arvioiminen ei kuuluisi pohditun informaatioturvallisuuden osaamiskeskuksen rooliin. Viranomaiset tekevät omaa lakisääteistä tehtäväänsä, ja vastaavasti mediayritykset tai järjestöt pohtivat asiaa omista lähtökohdistaan. Toimivaltaisten viranomaisten tehtäviin kuuluu johtopäätösten tekeminen saamastaan aineistosta. Tiedotusvälineet voivat toimia yhteistyössä viranomaisten kanssa tietyin reunaehdoin, joista journalistinen itsenäisyys on ehkä tärkein.

Osaamiskeskus pystyisi tarjoamaan osan verkoston toimijoiden haluamasta digitaalisesta aineistosta, tekemään teknistä analyysiä, rajoitetusti muuta analyysiä, antamaan digitaalisen aineiston menetelmätukea sekä tukea koulutuksessa ja prosessien parantamisessa. Prosessien kehittämisessä tuki voi olla myös yhteisten käsitteiden ja raportoinnin edellyttämien määrittelyjen luomista osaamiskeskuksen kehityshankkeena.

Tiedotusvälineiden kesken on suuria eroja, kuinka ne näkevät tuen tarpeen informaatiovaikuttamisen tunnistamisessa. Työ edellyttää resursseja, joita ei kaikilla ole. Suuret mediatalot voivat hyötyä uusista data-aineistoista, mutta pienemmät toimijat, kuten pienet julkaisut ja yksittäiset toimittajat hyötyisivät myös koulutuksista ja datatyökaluista.

Journalistiset hankkeet hyötyisivät pohditusta heräterahasta innovatiivisille aloitteille. Itsenäisen, vaativan faktantarkastuksen tukeminen voisi olla myös kohteena. Tämä voidaan järjestää myös Mediapoolin kautta. Mahdollisuuksiensa puitteissa osaamiskeskus tekisi tai teettäisi informaatioturvallisuuteen liittyviä työkaluja, jotka voivat liittyä myös journalistien työnkuvaan.

Mediayhtiöiden kanssa on keskusteltava, mitä ne pystyisivät tuomaan verkoston toimintaan. Esimerkiksi kyberturvallisuudessa ja Kyberturvallisuuskeskuksen toiminnassa yritysten panostukset yhteistyöhön ovat merkittäviä ja kaikkia osapuolia hyödyntäviä.

Verkostossa tehtävän tilannekuvatyön kehittämisen tukemiseksi nostettiin esiin keinoja. Verkostomaisessa työskentelyssä viranomaistoimijat ovat toisaalta datan ja analyysin hyödyntäjiä, mutta ne voisivat tuoda jäsennellymmin mukaan omaa osaamistaan ja näkymää informaatiokenttään. Hallinnonalat tekevät tälläkin hetkellä tarpeidensa mukaan omat analyysinsä ja uhka-arvionsa, mutta aihepiiri on osalle vielä vähämerkityksinen. Osaamiskeskus voisi tukea tai muodostaa informaatiouhkien tilannekuvaa niille toimijoille, joiden ei kannata sitä itse rakentaa. Normaali mediaseuranta ei tähän kuuluisi. Työnjako ja tehtävien rajaukset siirtyvät seuraavaan suunnitteluvaiheeseen.

5.3 Muita kehitysehdotuksia

Keskusteluissa nousi esiin useita muita aloitteita. Kansainväliset esimerkit osoittivat, kuinka tärkeää on tietää omat haavoittuvuudet. Hallinnonalat tekevät tätä työtä, ja kansallisessa riskienarvioinnissa käsitykset koostetaan. Jos informaatioturvallisuuteen liittyvät tekijät ovat selkeä kokonaisuus kansallisessa riskienarvioinnissa, se muuttuu helpommin konkreettisiksi varautumistoimiksi.

Esiselvitys ei puutu viranomaisten tai yritysten sisäisiin järjestelyihin informaatiovaikuttamisen havainnoinnissa. Keskusteluissa kävi kuitenkin ilmi, että prosessit kaipaavat kehittämistä. Ohjeet, työjärjestykset ja työnkuvat eivät tällä hetkellä riittävän hyvin tunnista informaatioturvallisuuden tehtäväkenttää. Suunniteltu osaamiskeskus olisi verkoston keskustoimintona luonteva kumppani, jos toimivaltainen viranomainen hankkeeseen ryhtyisi.

Väestö voi itse havaita internetissä epäilyttävää toimintaa. Poliisin sivulla poliisi.fi/nettivinkki on mahdollisuus kertoa tällaisesta sisällöstä tai aineistosta. Poliisi tarkastaa lähetettyjä vihjeitä, jotka eivät ole rikosilmoituksia. Aina kuitenkaan epäily ei viittaa vielä rikokseen. ”Infovihjenappi” olisi keino kertoa koetusta informaatiohäirinnästä, konevoimin vauhditetuista kampanjoista tai muuten koordinoidusta vaikuttamisesta. Tämä voisi olla mediayritysten sivuillaan ja sovelluksissaan tekemä hanke, minkä ansiosta suomalaiset saisivat ripeästi tietoa tämäntyyppisistä tapahtumista.

Koulutus rajautui suurimmaksi osaksi esiselvityksen ulkopuolelle. Suomessa mediakasvatus sisältyy opetussuunnitelmaan. Oppilaitokset ja Maanpuolustuskoulutusyhdistys sekä muut järjestöt kurssittavat aiheesta ja läheisistä aihepiireistä. Aalto-yliopistossa Trollauksen maantiede -kurssi ja käynnistyvä Puolustusvoimien Johtamisjärjestelmäkoulu ovat aihioita, jotka ovat kehittämisen ja kannustamisen arvoisia. Laadun ja jatkuvuuden varmistamiseksi olisi tärkeää, että koulutuksessa siirrytään projektivetoisuudesta pysyvämpiin järjestelyihin.

6 JOHTOPÄÄTÖKSET JA EHDOTUKSET SEURAAVISTA TOIMENPITEISTÄ

Esiselvityksessä on kartoitettu verkostomaisen yhteistyön mahdollisuuksia yhteiskuntaa vahingoittavan informaatiovaikuttamisen tunnistamiseksi ja siltä suojautumiseksi. Haastattelut ovat osoittaneet aihepiirin tärkeyden ja kiireellisen tarpeen toimenpiteille.

Alkuperäinen toimeksianto korosti, että tiedon luotettavuuden arviointiin ja informaatiovaikuttamisen tunnistamiseen tarvitaan työkaluja, dataa ja toimintamalleja. Esiselvityksen aikana ilmeni uusia informaatioturvallisuutta kehittäviä kokonaisuuksia: informaatioympäristön tilannekuva, vastatoimenpiteet, huippuosaamisen tuottaminen ja välittäminen, perustason osaamisen levittäminen alueille ja väestölle sekä kriisinkestävyys. Tavoitteiden moninaisuus, resurssipaineet ja kehityksen kiivaus johtavat siihen, että osa ratkaisuista vanhenee ennen kuin niitä päästään edes toteuttamaan. Merkittävistä kustannuksista huolimatta verrokkimaissa on ryhdytty toimeen ja panostettu asiantilan parantamiseen.

Kansallisena tavoitetilana voidaan nähdä informaatiovaikuttamisen tunnistamisen ja uhalta suojautumisen kehittäminen ja tiedonjako informaatiouhkista sekä yleisemmin tietoisuuden ja osaamisen lisääminen viranomaisten, median ja kansalaisten joukossa. Tästä työstä Huoltovarmuuskeskukselle rajautuu vain osa.

Esiselvitys analysoi nykytilaa ja toimijoiden näkemyksiä sekä luonnosteli mahdollisen jatkotyön lähtökohdat Huoltovarmuuskeskuksen tarkentavaa suunnittelua varten:

1. Laaja-alainen yhteistyö ja verkostomainen toiminta
2. Osaamisen kehittäminen koko verkostossa
3. Toimivaltaisen viranomaisen, elinkeinoelämän ja kansalaisen oman toiminnan tukeminen
4. Oma datan keruu, arkistointi ja analyysi toteutetaan läpinäkyvillä säännöillä. Avoimuus on lähtökohta. Luottamuksen säilyttämiseksi osa työstä voi olla pelkästään viranomaisten tai verkoston omaan käyttöön.
5. Analyysi on lähtökohtaisesti kvantitatiivistä, eikä syyksilukemista tehdä
6. Mahdollinen hanke etenee vaiheittain. Sovituissa päätöksenteko- ja ohjauspisteissä arvioidaan tuloksia ja jatkoa. Hanke päättyisi viimeistään vuoden 2024 lopussa.

Esiselvitys ehdottaa seuraavia elementtejä jatkokehittelyä varten:

1. Informaatioturvallisuuden osaamiskeskus -toiminnon pilotti,
2. verkostoituneet informaatioanalyysiryhmät,
3. heräterahoja aktiviteetteihin, kuten faktantarkastukseen, alan innovaatioihin ja peleihin; ja
4. informaatioturvallisuusstrategia.

Huoltovarmuuskeskuksen rooli tarkentuu keskusteluissa muiden osapuolten kanssa. Tämä koskee erityisesti mahdollisen informaatioturvallisuusstrategian tukemista sekä osaamiskeskuksen sijaintia.

Informaatioturvallisuuden osaamiskeskus olisi kansallinen osaamisen ja tietojen vaihtamisen yhteyspaikka. Verkostojen keskustoimintona se palvelisi yhteyspisteenä eri toimijoille tukien muiden toimijoiden osaamista. Keskus kumppaneineen etsisi viitteitä informaatiovaikuttamisesta, keinoja sen havainnointiin ja vaikuttamiselta suojautumiseen. Pilotointina se tarjoaa syötteitä mahdolliselle strategiatyölle ja mahdollistaa toiminnan uudelleensuuntautumisen, mikäli tulokset eivät ole tyydyttäviä. Pilotoinnin aikana tehdään päätökset jatkosta.

Informaatioturvallisuus on osa digitaalista turvallisuutta, minkä vuoksi Huoltovarmuuskeskuksen DT2030-kokonaisuus on luonteva hallinnollinen järjestely pilotoinnille ja muille tehtäville. Kustannusarviot täsmentyvät jatkosuunnittelussa, mutta ohessa tämän hetkinen näkemys aikataulusta ja kuluista:

- 2021 syksynä HVK:n tahtotilan määrittely ja päätökset, käynnistetään tarvittavat jatkoselvitykset ja työpajatyöskentely, päätökset ohjausryhmästä
- 2022, tehtävinä suunnitelmien tarkennus ja osin käynnistys, jatkopäätökset etappivaiheissa
  - informaatioturvallisuuden osaamiskeskus -toiminnon aloitus
  - verkostoituneet informaatioanalyysiryhmät
  - heräterahoja aktiviteetteihin
- 2023-2024, tehtävinä osaamiskeskuksen ja verkostoyhteistyön täysimittainen pilotointi, heräterahat aktiviteetteihin käynnistetään, päätökset hankkeen jatkosta
- sekä tuen antaminen mahdolliselle informaatioturvallisuusstrategia -hankkeelle

Edellä mainitut jatkoselvitykset ja työpajatyöskentely pureutuisivat seuraaviin aihepiireihin: Tarpeiden täsmentäminen (mm. tehtävän rajaukset, Huoltovarmuuskeskuksen tahtotila)

1. Tuotteet ja hyödyntäminen (mm. kansallisen data-altaan kysymykset)
2. Toimintamalli (mm. toimivaltakysymykset, työn ja tiedonjako viranomaisten kanssa, yhteistyösuhteet median kanssa, informaatioanalyysiryhmien konseptin tarkennus)
3. Resursointi (HVK ja muut rahoituslähteet).
4. Riskit ja mittaaminen

Esiselvitys esittää hankkeelle ohjausryhmää.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY