VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu

Muistio

25.4.2022

Sisällys

1 Johdanto 3
1.1 Tausta 3
1.2 Työn toteutus ja rajaukset 3
2 Kansainvälinen digiaalisen turvallisuuden yhteistoiminnan vertailu 5
2.1 EU:n digitaalisesta turvallisuudesta ja kyberturvallisuudesta 5
2.2 Keskitetyistä tieto- ja kyberturvallisuustehtävistä 6
2.3 Kriittisen infrastruktuurin suojaamisesta 9
2.4 Keskitetyistä tietosuojatehtävistä 10
2.5 Kansallisen turvallisuuden liittymisestä digitaaliseen turvallisuuteen 10
3 Digitaalisen turvallisuuden kansainvälisen yhteistoiminnan foorumeja 12
Liite 1 Yhteiskunnan digitalisoitumisesta ja siihen liittyvistä keskitetyistä tehtävistä 16
Liite 2 Selvityksen maakohtainen aineisto 20
Alankomaat 24
Australia 28
Iso-Britannia 33
Israel 36
Ruotsi 38
Saksa 42
Venäjä 45
Viro 48
Suomi 51

1 JOHDANTO

1.1 Tausta

Valtioneuvosto teki 8.4.2020 periaatepäätöksen Julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:33). Sen mukaan digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet, sekä keskeisiä hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut.

Valtioneuvoston periaatepäätöksen 8.4.2020 linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) (VM 2020:33), johon sisältyy tehtäviä kuhunkin digitaalisen turvallisuuden alueeseen kuuluvista palvelukokonaisuuksista. Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu on osa Haukka-työsuunnitelman tehtävää ”Julkisen hallinnon digitaalisen turvallisuuden kansallinen ja kansainvälinen yhteistoimintamalli”.

1.2 Työn toteutus ja rajaukset

Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälisen vertailun tarkoituksena on selvittää, mitä julkisen hallinnon digitaalisen turvallisuuden toiminnallisen tason keskitettyjä tehtäviä verrokkivaltioissa on tunnistettavissa ja miten ne on organisoitu. Valtioneuvoston periaatepäätöksen 8.4.2020 julkisen hallinnon digitaalisesta turvallisuudesta taustatyönä valmistui helmikuussa 2020 selvitys[1], jossa vertailtiin kahdeksan verrokkivaltion ja Suomen digitaalisen turvallisuuden rakenteita ja toteutuksia. Verrokkivaltiot olivat Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Tämän selvitysraportit tiedot on ajantasaistettu ja tarkennettu ottaen erityisesti huomioon kussakin verrokkivaltiossa keskitetysti toiminnallisella tasolla, lähinnä virastoissa, toteutettuja tieto- ja kyberturvallisuustehtäviä.

Selvityksessä on keskitytty yhteisiin, poikkihallinnollisiin toiminnallisen tason tehtäviin. Ministeriöiden vastuulla olevat tyypilliset tehtävät kuten säädösvalmistelu sekä kansallinen strateginen suunnittelu on rajattu selvityksen ulkopuolelle. Myöskään sektorikohtaisia keskitettyjä tehtäviä ei ole huomioitu. Selvityksestä on pääosin myös rajattu ulkopuolelle verrokkivaltioiden puolustusvoimien tehtävät. Puolustusvoimille tyypillisesti annetuttuja tehtäviä: kyberpuolustus- ja hyökkäyskyky on huomioitu vain siltä osin kuin muut toimijat niitä tukevat.

Julkisen hallinnon digitaalisen turvallisuuden tehtävät sisältyvät usein julkisen hallinnon digitalisaation edistämisen tehtäviin. Tämän johdosta selvityksen liitteessä 1 on luotu katsaus myös verrokkivaltioiden julkisen hallinnon digitalisaatioon – sähköisten palvelujen tarjoamisen kansalaisille, yhteisöille ja hallinnolle – ja digitalisaation edistämisen tehtäviin.

[1] https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf?t=1583343825000

Selvitys perustuu pääosin julkisesti saatavilla oleviin kirjallisiin lähteisiin, kuten esimerkiksi organisaatioiden verkkosivustot ja verrokkivaltioiden julkaisemat kyberturvallisuus- ja digitalisaatiostrategiat. Verrokkivaltioiden toimintaa ja järjestelyjä ei ole tarkasteltu lainsäädännön näkökulmasta, vaan kirjallisten lähteiden perusteella on muodostettu kuva verrokkivaltioiden digitaalisen turvallisuuden käytännön toteutuksista. Eri toimijoiden digitaalisen turvallisuuden tehtävien ja vastuunjaon yksityiskohtaiset kuvaukset eivät tyypillisesti ole julkisesti saatavilla. Selvitysraportin tietojen varmistamiseksi se on käynyt kommentoitavana Suomen suurlähetystöissä verrokkivaltioissa. Tehtyihin havaintoihin ja johtopäätöksiin sisältyy kuitenkin edelleen epävarmuuksia digitaalisen turvallisuuden hallinnon ja käytänteiden luottamuksellisuuden johdosta.

Selvitys on toteutettu julkisen hallinnon digitaalisen turvallisuuden Haukka-ohjelmassa. Selvitysryhmässä on toiminut tietohallintoneuvos Tuija Kuusisto, ja erityisasiantuntija Niko Mäkilä valtiovarainministeriöstä, sekä Haukka-ohjelmaan kilpailutetut konsultit. Selvitystä on tukenut Haukka-ohjelmaan asetettu digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin koordinaatioryhmä.

2 KANSAINVÄLINEN DIGIAALISEN TURVALLISUUDEN YHTEISTOIMINNAN VERTAILU

2.1 EU:n digitaalisesta turvallisuudesta ja kyberturvallisuudesta

Digitaalisen turvallisuuden varmistamiseksi EU-valtioissa on yhteisiä käytäntöjä, kuten yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR[2]), verkko- ja tietoturvadirektiivi (Directive on Security of Network and Information Systems, NIS (EU) 2016/1148[3], sekä sen uudistettu ehdotus (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin (EU) 2016/1148 kumoamisesta, eli niin sanottu NIS 2[4], sekä akkreditointi- ja markkina-valvonta-asetus (New Legislative Framework, NLF) [5], sekä kyberturvallisuusasetus[6], ja Euroopan kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskeva asetus (Regulation of European Cybersecurity Competence Centre and the Network of National Coordination Centres)[7], sekä EU:n radiolaitedirektiivin delegoidut asetukset (Delegated Act supplementing the Radio Equipment Directive). Yleisessä tietosuoja-asetuksessa asetetaan organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. NIS-direktiivissä asetetaan yleisiä tietoturvavaatimuksia erikseen määritellyille kriittisille toimialoille sekä velvoite ilmoittaa merkittävistä tietoturvaloukkauksista. NIS2-direktiiviehdiotus on parhaillaan trilogineuvotteluissa. NIS 2 -direktiiviehdotuksella säädettäisiin tiukempia tietoturvavaatimuksia, laajennettaisiin lainsäädännön soveltamisalaa uusille toimialoille ja toimintoihin, mukaan lukien julkinen sektori ja annettaisiin uusia valvontamenetelmiä kansallisten valvontaviranomaisten käyttöön. NLF-asetuksella on säädetty akkreditointitoiminnasta ja markkinavalvonnan vaatimuksista Euroopan unionin tasolla, mukaan lukien kansallisten akkreditointielimien velvollisuudet tehtävissään. Lisäksi digitaaliseen turvallisuuteen suoraan vaikuttavia säädöshankkeita ovat mm. EU:n kyberresilienssiasetus (Cyber Recilience Act), sekä kriittisiä toimijoita koskeva direktiivi (Directive of the Resilience of Critical Entities).

Vuonna 2019 annettuun asetukseen Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuusertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (kyberturvallisuusasetus), (jatkossa kyberturvallisuusasetus) liittyen valmistellaan asiakohtaisia sertifiointimalleja ja -skeemoja, kuten esimerkiksi eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille. Määritellyn kehyksen ansiosta tieto- ja viestintätekniikan tuotteita ja palveluja koskevat sertifikaatit voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. Uuteen kehykseen sisältyy kattava joukko sääntöjä, teknisiä vaatimuksia, standardeja ja menettelyjä, joiden avulla pyritään raken-

[2] (EU) 2016/679 GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[3] (EU) 2016/1148 NIS https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[4] COM(2020) 823 final NIS2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823
[5] (EC) No 765/2008 NLF https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765
[6] (EU) 2019/881 https://eur-lex.europa.eu/eli/reg/2019/881/oj
[7] (EU) 2021/887 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0887

tamaan luottamusta, lisäämään kyberturvallisuusmarkkinoiden kasvua sekä helpottamaan EU:n laajuista kauppaa. Parhaillaan ollaan esimerkiksi valmistelemassa EU:n yhteistä mallia (skeema) pilviteknologioiden turvallisuuden sertifioimiseksi (European Cybersecurity Certification Scheme for Cloud Services). EU:n vuonna 2004 perustetun kyberturvallisuusviraston (The European Union Agency for Cybersecurity, ENISA) tehtävänä on valmistella malliluonnos komission ja jäsenmaiden käsiteltäväksi. Asetuksella annettiin lisäksi ENISAlle entistä vahvemman mandaatin tukea jäsenmaita, EU:n toimielimiä ja muita sidosryhmiä kyberhyökkäysten torjumisessa ja sen määräaikainen rooli muutettiin pysyväksi samalla, kun sen tehtäväkenttää laajennettiin EU:n verkko- ja tietoturvavirastosta (European Network and Information Security Agency) EU:n kyberturvallisuusvirastoksi.[8,9]

Euroopan Kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskeva asetus (EU 2021/887) tuli voimaan 28.6.2021. Asetuksen tavoitteena on syventää julkisen sektorin, yksityisen sektorin ja tutkimusmaailman välistä yhteistyötä kyberturvallisuustutkimuksen, -tuotekehityksen ja -innovoinnin alueilla. Kyberturvallisuuskeskus on nimitetty Suomen kansalliseksi kyberturvallisuuden koordinointikeskukseksi ja se hoitaa Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen 6. artiklassa tarkoitetun kansallisen koordinointikeskuksen tehtäviä.[10]

Digitaalista turvallisuutta koskevan yhteisen lainsäädännön lisäksi EU:ssa on valmisteltu kyberturvallisuusstrategia. EU:n uuden kyberturvallisuusstrategian tarkoituksena on vahvistaa Euroopan sietokykyä kyberuhkia vastaan ja varmistaa, että kaikki kansalaiset ja yritykset voivat hyötyä täysimääräisesti luotettavista palveluista ja digitaalisista välineistä. Strategia kuvaa kolme instrumenttia (sääntely, investoinnit ja politiikat), joiden avulla ohjataan EU:n toimenpiteitä kolmella alueella:[11]

- resilienssi sekä teknologinen riippumattomuus ja johtajuus,
- operatiivinen kyky häiriöiden havainnointiin ja hallintaan (prevent, deter, respond) ja
- avoimen globaalin kybertoimintaympäristön edistäminen yhteistyön avulla.

2.2 Keskitetyistä tieto- ja kyberturvallisuustehtävistä

Valtioneuvoston periaatepäätöksen 8.4.2020 julkisen hallinnon digitaalisesta turvallisuudesta taustaselvityksenä valmistuneessa kansainvälisessä vertailuselvityksessä[12] yhtenä johtopäätöksenä todettiin, että verrokkivaltioiden julkisen hallinnon digitaalisen turvallisuuden organisoinnissa suunta on

[8] https://www.consilium.europa.eu/fi/policies/cybersecurity/
[9] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[10] Laki sähköisen viestinnän palveluista (2014/917) §304
[11] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[12] https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf?t=1583343825000

kohti keskitetympää mallia. Suomen tulisikin siten ”*arvioida kriittisesti digiturvallisuuden nykyisiä johtamisrakenteita, vastuita ja rooleja sekä uudistaa niitä kansainvälisen kehityksen mukaisesti*”.

Tietoturvayhtiö Check Point Software Technologies Ltd. julkaisi vuoden 2021 puolivälissä raportin, jonka mukaan vuoden ensimmäisen puoliskon aikana kyberhyökkäysten määrä kasvoi 29 % globaalisti ja 36 % Euroopan ja Lähi-Idän (EMEA) alueella. Kiristyshaittaohjelmia käyttävien hyökkäysten määrä kasvoi samaan aikaan yli 90 %[13]. ENISAn lokakuussa 2021 julkaiseman raportin (ENISA Threat landscape 2021) mukaan julkinen hallinto on tunnistettujen tapausten lukumäärällä mitattuna merkittävin hyökkäyskohde[14]. ENISAn mukaan väärän ja virheellisen tiedon levittäminen (misinformation / disinformation) on keskeinen kyberhyökkäysten elementti, kyberhyökkäyksissä käytetään hyvin kehittyneitä menetelmiä ja kiristyshaittaohjelmien käyttö on lisääntynyt selvästi. Eniten käytettyjä haittaohjelmien levittämisvälineitä ovat sähköposti ja etäkäyttöohjelmistot.

Vuoden 2020 kansainvälisen vertailuselvityksen julkaisun jälkeen useimmat verrokkivaltiot ovat päivittäneet digitalisaatio- ja kyberturvallisuusstrategioitaan. Venäjällä, Virossa ja Ruotsissa on edelleen voimassa aiemmin julkaistut strategiat. Strategioissa korostetaan mm. kriittisen infrastruktuurin suojaamista, hallinnon toimintakyvyn ja tietojen turvaamista, uhka-arvioiden nopeaa päivittämistä ja jakamista sekä kaikkien toimijoiden: julkinen sektori, yksityissektori, kansalaiset vastuuta digitaalisen toimintaympäristön turvallisuudesta. Lisäksi painotetaan digitaalisen toimintaympäristön roolia osana kaikkia yhteiskunnan toimintoja niin siviiliyhteiskunnassa kuin sotilaallisessa maanpuolustuksessa.

Vuoden 2020 kansainvälisessä selvityksessä todettiin, että verrokkivaltioiden kansallisen kyberturvallisuuden aktiivisiksi toimijoiksi on tunnistettu julkisen hallinnon lisäksi elinkeinoelämä, tutkimusyhteisöt sekä yksityishenkilöt. Tämän takia koko yhteiskunnan digitaalisen turvallisuuden varmistaminen edellyttää, että kaikki osapuolet huolehtivat osaltaan digitaalisen toimintaympäristön turvallisuudesta mahdollisimman yhtenäisesti. Koska digitaalinen turvallisuus on kaikkiin toimintoihin ja yhteiskunnan tasoihin kiinteästi kuuluva osa, on verrokkivaltioissa tunnistettu tarve vastata erilaisiin digitaalisen turvallisuuden häiriöihin yhtenäisellä ja koordinoidulla tavalla. Tällaisten yhdenmukaisten menettelyjen ja toimintatapojen saavuttamisen on katsottu edellyttävän keskitettyä koordinointia, minkä johdosta yhteiskunnan digitaalisen turvallisuuden ja kyberturvallisuuden operatiivisia vastuita on verrokkivaltioissa koottu yhteen paikkaan.

Digitaalisen ja kyberturvallisuuden päämääriä kuvataan kansallisissa kyberturvallisuusstrategioissa, joiden keskeisiä tavoitteita ovat mm. tietoverkkojen toiminnan turvaaminen, havainto- ja reagointikyvyn kehittäminen, digitaalisen turvallisuuden osaamisen lisääminen kaikilla yhteiskunnan tasoilla sekä kansainvälinen yhteistyö. Strategisen tason kyberturvallisuudesta vastaa valtion ylin johto, ja tehtävän koordinointi on annettu jonkin ministeriön hoidettavaksi. Esimerkiksi Saksassa ja Australiassa päävastuu kyberturvallisuuden strategisesta tasosta on sisäministeriöllä, Venäjällä turvallisuusneuvostolla, Ruotsissa oikeusministeriöllä. Isossa-Britanniassa ja Israelissa päävastuussa on Suomen

[13] https://securitydelta.nl/media/com_hsd/report/443/document/cyber-attack-trends-report-mid-year-2021.pdf
[14] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

valtioneuvoston kansliaa vastaava organisaatio. Kyberturvallisuusstrategian laatii valtion johto erilaisten neuvoa antavien elimien tukemana ja strategian julkaisee joko vastuuministeriö tai jokin sen alainen virasto.

Suomen tavoin jokaisessa verrokkivaltiossa on muodostettu keskitetty kyberturvallisuustoimija, johon on koottu koko yhteiskuntaa palvelevia digitaalisen turvallisuuden ja kyberturvallisuuden tehtäviä. Kyberturvallisuustoimijalle keskitetyt tehtävät palvelevat tyypillisesti yhteiskunnan teknisiä tieto- ja kyberturvallisuuden operatiivisia tarpeita. Kyberturvallisuustoimijalle annetut tehtävät ja se, miten paljon ja mitä tehtäviä on keskitetty yhdelle toimijalle, vaihtelevat maittain. Osassa vertailun maista julkisen hallinnon digitaalisen turvallisuuteen liittyviä tehtäviä ja ohjausta ei ole erotettu muista kyberturvallisuuteen liittyvistä tehtävistä ja ohjauksesta samalla tavoin kuin Suomessa. Toisaalta Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus vastaa monista sellaisista kyberturvallisuuden tehtävistä, jotka eivät kuulu esimerkiksi Ruotsin tai Iso-Britannian Kyberturvallisuuskeskuksen tehtäviin.

Kyberturvallisuudesta vastaavan toimijan organisointi noudattaa verrokkivaltioissa yleensä kahta eri tapaa. Alankomaissa, Australiassa ja Isossa-Britanniassa kyberturvallisuustoimija kuuluu osaksi keskitettyä turvallisuusvirastoa, jonka tehtäviin voi kuulua esimerkiksi sisäinen turvallisuus tai terrorismin torjunta. Israelin, Saksan ja Viron keskitetty toimija on puolestaan suoraan jonkin ministeriön alaisuudessa: Israelissa pääministerin, Saksassa sisäministeriön ja Virossa talous- ja viestintäministeriön.

Keskitetyn toimijan tehtäviin kuuluvat mm. kyberturvallisuushäiriöiden hallinta (CERT- ja CIRT-toiminta), tietoverkkojen valvonta, ympärivuorokautisen tilannekeskuksen operointi sekä kyberturvallisuuden uhka-arvion muodostaminen ja sen jakaminen. Kyberturvallisuuskeskukset antavat myös neuvontaa ja tuottavat digitaalisen toimintaympäristön turvallisuutta koskevia ohjeita hallinnolle, yrityksille ja yksityishenkilöille. Lisäksi kansalliset kyberturvallisuuskeskukset tukevat muita viranomaisia kyberhäiriötilanteiden selvittämisessä ja tutkinnassa.

EU-valtioiden kyberturvallisuuskeskukset ovat NIS-direktiivissä määriteltyjä yhteyspisteitä. Verrokkivaltioiden erityispiirteiden takia kyberturvallisuuskeskuksille on näiden lisäksi annettu tehtäväksi digitaalisen turvallisuuden tuotteiden turvallisuuden arviointi (Iso-Britannia, Saksa ja Suomi), digitaalisen turvallisuuden tutkimuksen koordinointi (Alankomaat[15]) ja digitaalisen turvallisuuden henkilösertifiointi (Australia, Iso-Britannia, Israel ja Saksa). Kyberturvallisuuskeskukset toimivat kiinteässä yhteistyössä muiden turvallisuudesta vastaavien viranomaisten kanssa. Ne toimivat tarvittaessa hallitustensa asiantuntijoina toimialueensa asioissa ja osallistuvat kyberturvallisuusstrategioiden laatimiseen.

Australiassa keskitetyn toimijan (ACSC) alaisuudessa toimii lisäksi yhteisö kyberturvallisuuskeskuksia (Joint Cyber Security Centres, JCSC). Ne tukevat ACSC-kumppanuusohjelmaa, jonka tarkoituksena on tuoda yhteen yrityksiä ja tutkimus-yhteisöä sekä osavaltioiden, alueiden ja Australian hallituksen virastoja avoimessa ja yhteistyöhön perustuvassa ympäristössä.

[15] https://english.ncsc.nl/research

Ruotsissa hallitus on asettanut kansallisen varautumisviranomaisen (MSB), puolustusvoimien, signaalitiedustelun (FRA) ja turvallisuuspoliisin (Säpo) tehtäväksi perustaa Ruotsin kyberturvallisuuskeskus[16]. Keskuksen on tarkoitus käynnistyä vaiheittain 2021-2023 välisenä aikana. Uuden, keskitetyn kyberturvallisuuskeskuksen tavoitteena on koota yhteen ja vahvistaa Ruotsiin kohdistuvien kyberturvallisuusuhkien ennaltaehkäisy-, havainnointi- ja hallintakykyä.[17] Keskuksen toimintaan osallistuvien viranomaisten tehtäviä ei kuitenkaan siirretä perustettavalle Ruotsin kyberturvallisuuskeskukselle, vaan viranomaiset vastaavat edelleen niille lainsäädännössä asetetuista tehtävistä keskuksen toimintaan liittyvien tehtävien rinnalla. Ruotsin kyberturvallisuuskeskuksen ympärille rakennettava kyberturvallisuuden yhteistoimintamalli vastaa osittain Suomen olemassa olevaa yhteistoimintamallia. Ruotsin kyberturvallisuuskeskuksen käynnistymisen jälkeen jokaisessa verrokkivaltiossa on keskitetty, yhden tahon ohjauksessa oleva kyberturvallisuuskeskus.

Venäjällä varsinaista kyberturvallisuusvirastoa ei ole tunnistettu, mutta digitaalisesta kehityksestä, viestinnästä ja joukkoviestimistä vastaavan ministeriön (Минцифры России, ”Mintsifry Rossii”) alle on sijoitettu mm. tietoliikenteen turvaamiseen, teknologioiden seurantaan ja edistämiseen sekä tietosuojaan liittyviä tehtäviä. Lisäksi Venäjän turvallisuuspalvelu (FSB) vastaa turvallisuudesta laajasti.

2.3 Kriittisen infrastruktuurin suojaamisesta

Kriittinen infrastruktuuri (CI) kattaa Kokonaisturvallisuuden sanaston (TSK 50, 2017) mukaan ”perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi”[18]. Kriittisen infrastruktuurin käsite vaihtelee jonkin verran valtioittain, mutta tyypillisesti siihen voidaan sisällyttää ainakin energiantuotanto, vesihuolto, elintarvikehuolto, terveydenhuolto, finanssisektori, logistiikka ja viestintä. Kriittisen infrastruktuurin ja kriittisen digitaalisen infrastruktuurin (CII) käsitteiden välinen ero on epäselvä jatkuvasti digitalisoituvassa toimintaympäristössä, jossa fyysisen infrastruktuurin kohteisiin liittyy usein tietoa tuottavia ja käsitteleviä valvontajärjestelmiä, antureita ja ohjelmistoja.[19] Myöskään digitaaliselle infrastruktuurille ei ole selkeää ja yhtenäistä määritelmää, mutta yleisesti siihen voidaan katsoa kuuluvan mm. tietoverkot, tietojärjestelmät (laitteet ja ohjelmistot) sekä erilaiset laitetilat ja datakeskukset.

Kriittisen infrastruktuurin suojaaminen ja kriiseihin varautuminen on useimmissa verrokkivaltioissa erityisen toimijan tehtävä, mutta näiden tehtäväkentät poikkeavat toisistaan jonkin verran. Ison-Britannian, Saksan ja Venäjän viranomaiset keskittyvät erityisesti fyysisen infrastruktuurin turvaamiseen, Australian CISC:n tehtäväkenttä kattaa myös digitaalisen infrastruktuurin turvaamista ja Alankomaiden NCTV:llä ja Ruotsin MSB:llä on kriittisen infrastruktuurin turvaamisen lisäksi myös muita tehtäviä (NCTV:llä esimerkiksi terrorismin torjunta ja MSB:llä kokonaispuolustukseen osallistuminen ja onnettomuuksien ehkäisy). Missään verrokkivaltiossa ei kriittisen fyysisen infrastruktuurin ja

[16] https://www.regeringen.se/4af5d9/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter.pdf
[17] https://www.cfcs.se/om-centret/
[18] https://termipankki.fi/tepa/en/search/kriittinen%20infrastruktuuri
[19] https://www.huoltovarmuuskeskus.fi/files/019d67575f48fdb84212fd8bd9164b8ac8829ccd/cip-raportti_final.pdf

digitaalisen infrastruktuurin eroa erityisesti korosteta ja kaikissa tapauksissa kriittisen infrastruktuurin turvaamisen viranomaiset ovat tiiviissä yhteistyössä kyberturvallisuustoimijoiden kanssa.

Verrokkivaltioiden kriittisen infrastruktuurin suojaamisesta vastaavan toimijan tavoitteena on varmistaa, että yhteiskunta on toimintakykyinen kaikissa olosuhteissa – myös laajavaikutteisten häiriöiden aikana. Toimijoiden tehtävänä on mm. suojattavien kriittisten kohteiden (esimerkiksi laitokset, toiminnot, järjestelmät) tunnistaminen, kriittiseen infrastruktuuriin liittyvien riskien arviointi ja uhkaarvion muodostaminen sekä varautumiseen liittyvä ohjeistus. Viranomaisilla ei tyypillisesti ole operatiivisia vastuita, vaan varsinaisten suojaustoimien toteuttaminen on kriittisen infrastruktuurin haltijan tai omistajan vastuulla viranomaisen ohjeistuksen avulla.

Kriittisen infrastruktuurin toimijoiden tärkeimpiä yhteistyötahoja ovat kyberturvallisuuskeskusten lisäksi kansallisen turvallisuuden toimijat, yksityissektorin toimijat, lainvalvontaviranomaiset sekä tutkimuslaitokset. OECD:n tekemän selvityksen mukaan verrokkivaltioissa (pl. Venäjä) on määritelty, mitä kriittiseen infrastruktuuriin kuuluu ja että sen suojaamiseksi on olemassa strategiset linjaukset ja vastuuorganisaatiot. Suomessa ja Ruotsissa kriittisen infrastruktuurin kohteita, järjestelmiä, toimintoja ei kuitenkaan ole dokumentoitu toisin kuin muissa verrokkivaltioissa.[20]

2.4 Keskitetyistä tietosuojatehtävistä

Kaikissa verrokkivaltioissa, myös Suomessa, on viranomainen, jonka vastuulla on tieto- ja yksityisyyden suoja. Tietosuojan viranomaistoiminta on EU-valtioissa organisoitu EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisesti, mutta muissakin verrokkivaltioissa (Australia, Israel, Iso-Britannia ja Venäjä) on vastaava viranomainen. Tietosuojan lisäksi voi viranomaisen vastuisiin voi kuulua esimerkiksi tietojen saatavuuden varmistaminen (”freedom of information”).

Tietosuojaviranomainen on useimmiten sijoitettu oikeusministeriön (tai vastaavan) alaisuuteen. Saksan Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BDfI) on täysin riippumaton virasto. Isossa-Britanniassa ja Venäjällä tietosuojaviranomainen on sijoitettu digitalisaatiosta vastaavaan ministeriöön (Department for Digital, Culture Media and Sport, Ministry of Digital Development, Communications and Mass Media vastaavasti).

2.5 Kansallisen turvallisuuden liittymisestä digitaaliseen turvallisuuteen

Kansallisen tuvallisuuden keskitetyllä viranomaisella (Alankomaiden NCTV, Ison-Britannian GCHQ, Australian ASD ja Venäjän FSB) on kyberturvallisuuden lisäksi vastuullaan mm. tiedustelutoiminta, terrorismin ja ääriliikkeiden torjunta, vakavan ja järjestäytyneen rikollisuuden torjunta sekä kyberpuolustuksen tukeminen. Esimerkiksi ASD on ainoa Australian puolustussektorin haara, joka on saanut 2022 julkaistussa liittovaltion budjetissa huomattavaa lisärahoitusta. Useamman vuoden

[20] https://www.oecd-ilibrary.org/sites/ee7bc35f-en/index.html?itemId=/content/component/ee7bc35f-en

aikana lähes 10 miljardin AUD rahoituksella on tarkoitus lisätä henkilöstön määrää merkittävästi ja siten varmistaa Australian kyberturvallisuuden puolustuksellisen ja offensiivisen kyvyn kehittyminen.

Ruotsin MSB ei ole varsinainen kansallisen turvallisuuden keskusviranomainen, mutta sen tehtäväkenttä on laaja ja kattaa kyberturvallisuuden lisäksi mm. pelastuspalvelun koordinointia, onnettomuuksien ehkäisyä, kriisivarautumista, kokonaispuolustukseen osallistumista (totalförsvar) sekä kansainvälisen yhteistyön koordinointia. MSB:n lähin suomalainen vastine on Huoltovarmuuskeskus, joskin MSB on henkilöstömäärältään selvästi suurempi ja sen tehtäväkenttä on laajempi.

3 DIGITAALISEN TURVALLISUUDEN KANSAINVÄLISEN YHTEISTOIMINNAN FOORUMEJA

Digitaalisen turvallisuuden kansainvälisiä yhteistyöryhmiä on useita ja niiden toiminnan painopiste vaihtelee. Suomelle kyberturvallisuuskysymyksissä erityisesti EU on keskeinen toimija ja sitä koskevissa kyberkysymyksissä valtioneuvoston kanslia toimii valtionhallinnon koordinoijana. EU:n ohella kybertoimintaympäristöä koskevaa keskustelua käydään muun muassa YK:ssa, OECD:ssä, NATO:ssa, ETYJ:ssä, Euroopan neuvostossa, ja Pohjoismaiden neuvostossa. Myös useat alueelliset järjestöt käsittelevät kyberturvallisuuskysymyksiä.

Suomessa ulkoministeriö, liikenne- ja viestintäministeriö, sisäministeriö ja puolustusministeriö osallistuvat aktiivisesti kybertoimintaympäristöä koskevaan globaaliin, alueelliseen ja kahdenväliseen keskusteluun ja vaikuttavat kansainvälisellä kyberagendalla olevien kysymysten edistämiseen Suomen etujen mukaisesti.

Alla olevaan taulukkoon on koottu esimerkkejä keskeisistä, kansainvälisistä digitaalisen turvallisuuden aiheiden yhteistyöryhmistä. Näiden lisäksi Suomesta osallistutaan useisiin muihin, lähinnä sektorikohtaisiin yhteistyöryhmiin, joita tässä ei ole käsitelty.

Ryhmä	Kuvaus
The OECD Global Forum on Digital Security for Prosperity	OECD:n Global Forum on Digital Security for Prosperity on kansainvälinen ja monitieteinen ympäristö kaikille sidosryhmille digitaalisen turvallisuuden alalla. Foorumi kokoaa yhteen asiantuntijoita ja päättäjiä edistääkseen säännöllistä kokemusten ja hyvien käytäntöjen jakamista digitaalisen turvallisuuden riskeistä ja niiden hallinnasta. Foorumissa käydään jatkuvasti keskusteluja esimerkiksi kyberturvallisuushäiriöihin reagoimisesta, siilojen hajottamisesta ja kansainvälisen yhteistyön lisäämisestä valtiohallintojen ja muiden sidosryhmien välillä. OECD käyttää termiä digitaalinen turvallisuus, joka viittaa kyberturvallisuuden taloudellisiin ja sosiaalisiin näkökulmiin. [21]
OECD Working Party on Security on the Digital Economy	OECD:n Working Party on Security on the Digital Economy (SDE) toteuttaa OECD:n työtä digitaalisen turvallisuuden alueella. SDE kehittää ja edistää digitalouden turvallisuutta vahvistavia ohjausasiakirjoja ja linjauksia. Se raportoi OECD Committee on Digital Economy Policy (CDEP):lle. Suomesta valtiovarainministeriön sekä liikenne- ja viestintäministeriön edustajat ovat osallistuneet SDE:n työhön. Liikenne- ja viestintäministeriön sekä työ- ja elinkeinoministeriön edustajat ovat osallistuneet CDEP:in työhön.

[21] https://www.oecd.org/sti/ieconomy/digital-security/

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskusverkosto	Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksesta ja kansallisten koordinaatiokeskusten verkoston perustamisesta annetun asetuksen (EU 2021/887) mukaisesti kansainvälisen koordinaation ja yhteistyön kehittämiseksi perustetaan kansallisten koordinaatiokeskusten verkosto. Sen muodostavat jäsenvaltioiden nimeämät kansalliset koordinaatiokeskukset, Suomessa Liikenne- ja viestintävirasto. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus sijaitsee Bukarestissa, Romaniassa.
Forum of Incident Response and Security Teams (FIRST)	FIRST on suurin tietoturvaloukkauksia käsittelevien toimijoiden globaali yhteenliittymä. FIRST ylläpitää CERT- ja muun tietoturvayhteisön kontaktilistaa (valtiohallinnot, kaupalliset tahot sekä oppilaitokset), joka on kaikkien jäsenten käytettävissä.[22] Foorumin tavoitteena on edistää yhteistyötä tietoturvapoikkeamien ehkäisemisessä, poikkeamiin reagoimisessa ja tietojen jakamisessa jäsenten ja koko yhteisön välillä[23]. Tällä hetkellä Suomessa on mukana kolme ryhmää yhteistoiminnassa: Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, Ericssonin Product Security Incident Response Team (PSIRT) ja Tieteen tietotekniikan keskuksen (CSC) Funet CERT (Finnish University and Research Network, Computer Emergency Response Team). Foorumi myös tarjoaa erilaisia koulutuksia sekä järjestä teknisiä keskusteluja turvallisuusasiantuntijoille ja vuotuista konferenssia poikkeamahallinnasta.
CSIRT/CERT-verkostojen yhteistoiminnat	CSIRT-verkosto on perustettu edistämään luottamuksen vahvistumista jäsenvaltioiden välillä sekä nopeaa ja tehokasta operatiivista yhteistyötä NIS 2.0 direktiiviehdotuksen mukaisesti. Verkosto koostuu jäsenvaltioiden, komission ja ENISA:n edustajista. Direktiiviehdotuksella perustetaan myös Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) tukemaan laajamittaisten kyberturvapoikkeamien ja -kriisien koordinoitua hallintaa ja varmistamaan säännöllistä tietojenvaihtoa jäsenvaltioiden ja EU:n toimielinten välillä[24]. CSIRT-ryhmien yhteistoiminnat näkyvät myös tutkimus- ja koulutusverkoston ympäristössä. Esimerkiksi Géant on eurooppalaisten tutki-

[22] https://docplayer.fi/4358759-Kyberturvallisuuskeskuksen-toimintasuunnitelman-liitteet.html
[23] https://www.first.org/about/
[24] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:52020PC0823

	mus- ja opetusverkkojen yhteistyöorganisaatio, ja sen CSIRT-työryhmään (TF-CSIRT, Task Force - Computer Security Incident Response Teams) kuuluvat useimmat eurooppalaiset CSIRT-ryhmät. TF-CSIRT ylläpitää suljettua sähköpostilistaa tiedonvaihtoa varten, järjestää konferensseja ja kursseja sekä muodostaa työryhmiä selvitys- ja kehitysprojekteja varten[25]. Tällä hetkellä Géantin toiminnassa ja sen työryhmässä on mukana Suomesta tieteen tietotekniikan keskuksen (CSC) Funet CERT.
HIMSS-yhteistoiminnat	HIMSS (Healthcare Information and Management Systems Society) toimii kansainvälisenä terveysteknologiayhteisönä ja tarjoaa asiantuntemusta terveysalan innovaatioista, julkisesta politiikasta, työvoiman kehittämisestä, tutkimuksesta ja analytiikasta sidosryhmille ja vaikuttajille eri puolilta ekosysteemiä. Yhteisökeskeisellä lähestymistavalla HIMSS tarjoaa oivalluksia, koulutusta ja tapahtumia terveydenhuollon tarjoajille, startup-yrityksille ja terveydenhuoltojärjestöille[26]. Suomi on aktiivisesti osallistunut HIMSS:n toimintaan eri konferenssien muodossa. Esimerkiksi HIMMSS:n yhteistyössä Suomen sosiaali- ja terveysministeriön kanssa luoma Digital Health Advisory Group for Europe (DHAGE) on Euroopan johtavien päättäjien johtamisalusta digitaalisen terveyspolitiikan alalla[27]. Ryhmän vuonna 2020 järjestämässä HIMSS & Health 2.0 -konferenssissa sosiaali- ja terveysministeriö, Terveyden ja hyvinvoinnin laitos ja Teknologian tutkimuskeskus VTT kokosivat virtuaalitapahtumaan laajan kokonaisuuden suomalaista sosiaali- ja terveydenhuollon huippuosaamista[28]. Myös muiden ministeriöiden ja virastojen (esim. sosiaali- ja terveysministeriö ja Business Finland) sekä yksittäisten kuntien ja tutkimusjärjestöjen osallistuminen (esim. Helsingin kaupunki, Oulu Health, Helsingin yliopisto) näkyy vahvasti yhteistoiminnassa. Lisäksi HIMSS Nordic Community tarjoaa pohjoismaisia terveydenhuoltoresursseja, jotka on erityisesti räätälöity digitaalisen terveydenhuollon alan ammattilaisille sekä julkiselta että yksityiseltä sektorilta Suomessa, Tanskassa, Islannissa, Norjassa ja Ruotsissa[29].
The NATO Cooperative Cyber Defence	CCDCOE sijaitsee Virossa ja on avoin kaikille Naton jäsenvaltioille. Keskuksen ensisijaiset tavoitteet ovat tarjota tietoa, aiheosaamista ja

[25] https://wiki.eduuni.fi/display/funetcert/Yhteistoiminta
[26] https://www.himss.org/who-we-are
[27] https://www.himss.org/membership/get-involved/committees/digital-health-advisory-board-europe
[28] https://valtioneuvosto.fi/-/1271139/suomalainen-terveys-ja-hyvinvointiosaaminen-esilla-himss-health-2.0-suurtapahtumassa-7.-11.9.
[29] https://www.himss.org/membership-participation/himss-nordic-community-nordic-healthcare-professionals

Centre of Excellence (CCDCOE)	apua Natolle kyberpuolustuksen eri näkökohdissa. Esimerkiksi foorumi panostaa konseptin kehittämiseen, koulutukseen ja harjoituksiin, saatujen kokemusten julkaiseminen ja kyberpuolustuksen oikeudellisen kehyksen kehittämiseen. Suomi on mukana foorumin toiminnassa[30].

Suomen kansainvälistä asemaa digitaalisen turvallisuuden alueella seurataan useiden kansainvälisten indeksien perusteella. Niitä ovat International Telecommunication Unionin (ITU) Global Cybersecurity Index (GCI) ja Viron e-Governance Academyn National Cyber Security Index (NCSI). Vuonna 2020 Suomi sijoittui GCI-vertailussa sijalle 22, ja 10.3.2022 Suomi oli sijalla 10 NCSI-vertailussa[31].

GCI:n tuloksia on julkaistu vuosittain alkaen vuodesta 2014. Indeksi kuvaa valtioiden sitoutumista kyberturvallisuuteen ja sen kehittämiseen. Indeksi on kooste useista indikaattoreista (composite index), joihin kerätään tiedot kyberturvallisuuden kehittymisestä viidestä näkökulmasta: lainsäädäntö, tekniset toimenpiteet, organisointi, valmiudet ja yhteistoiminta. ITU:n jäsenvaltiot nimeävät kukin yhteyshenkilön, joka tehtävänä on koordinoida jäsenvaltion tietojen toimittamista. Tiedot indeksiin kerätään GCI:n kehitystiimin lähettämän kyselyn avulla tai GCI:n kehitystiimi kokoaa tiedot erikseen, jos jäsenvaltio ei vastaa lähetettyyn kyselyyn.[32]

NCSI mittaa maiden valmiutta hallita ja torjua kyberuhkia ja -häiriöitä. NCSI sisältää järjestetyn luettelon lisäksi työkaluja vertailujen tekemiseen ja trendien seuraamiseen sekä erilaisia asiakirjamalleja kansallisen kyberturvallisuusvalmiuksien kehittämisen tueksi. Indeksiin koottavat tiedot on jaettu kolmeen luokkaan: lainsäädäntö, organisointi ja yhteistoiminta, ja luokat on jaettu kykyjä kuvaaviin indikaattoreihin. Indikaattoreita ovat esimerkiksi kyberturvallisuuden politiikkojen ja strategioiden taso, kyberturvallisuuden koulutusjärjestelmät, digitaalisten palvelujen turvaaminen, häiriönhallinta, kyberrikollisuuden torjunta ja sotilaallinen kybertoiminta. Valtiot toimittavat indeksiin tiedot koordinoidusti ja indeksin ylläpidosta vastaava NCSI Data Manager myöntää käyttövaltuudet tietojen syöttämiseksi indeksiin. Hyväksyttäviä tietolähteitä ovat lainsäädäntö, viralliset asiakirjat sekä viralliset verkkosivustot. [33] Tarkempaa tietoa siitä, miten Viron e-Governance Academy käsittelee ja arvioi sille toimitettuja tietoja sekä antaa pisteitä eri maille, ei ole julkaistu.

[30] https://ccdcoe.org/
[31] NCSI Finland https://ncsi.ega.ee/country/fi/
[32] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member%20States.pdf
[33] https://ncsi.ega.ee/methodology/

LIITE 1 YHTEISKUNNAN DIGITALISOITUMISESTA JA SIIHEN LIITTYVISTÄ KESKITETYISTÄ TEHTÄVISTÄ

Yhteiskunnan digitalisoituminen näkyy jatkuvasti lisääntyvinä digitaalisina toimintoina ja palveluina. Verkkokauppa jatkaa edelleen kasvuaan ja meneillään oleva pandemia on kiihdyttänyt verkko-ostosten määrää.[34] Digitaalisen toimintaympäristön terveyspalvelut ovat laajentuneet sähköisen ajanvarauksen lisäksi mm. erilaisiin neuvontapalveluihin ja etävastaanottoihin.[35,36] Finanssisektorilla käteisen rahan käyttö on vähentymässä[37] ja digitaalinen rahoitusjärjestelmä (”digital finance”) luo uusia ilmiöitä kuten esimerkiksi lohkoketjuihin perustuvat kryptovaluutat.[38] Kun palvelujen määrä digitaalisessa toimintaympäristössä kasvaa, lisääntyvät myös erilaiset haavoittuvuudet ja niiden myötä uhkat yksilöiden, organisaatioiden ja valtioiden tiedoille ja toiminnalle. Useiden valtioiden digitalisaatio- ja kyberturvallisuusstrategioissa muutokset on tunnistettu ja todettu, että digitaalisen toimintaympäristön turvaaminen edellyttää laajaa yhteistyötä. Saksan digitalisaatiostrategia toteaa, että yhteiskunnan digitaalisen toimintaympäristön kehittämisen osaaminen on hajautunut eri sektoreille eikä yhteistä koordinaatiota ole riittävästi, vaan se tulisi koota yhteen.[39] Alankomaiden digitalisointi- ja kyberturvallisuusstrategioissa todetaan, etteivät valtion rajat rajoita tiedon liikkumista digitaalisessa toimintaympäristössä, minkä johdosta tarvitaan myös kansainvälistä digitaalisen turvallisuuden yhteistyötä niin EU:ssa kuin laajemminkin.

Globaalin digitalisaatiokehityksen aiheuttamat muutokset vaikuttavat myös julkisen hallinnon tarjoamiin rakenteisiin, toimintoihin ja palveluihin. Valtiot digitalisoivat palvelujaan yhä enemmän ja digitalisoinnin toteutuksissa pyritään hyödyntämään teknologioita innovatiivisesti niin, että julkisen hallinnon palvelut ovat helposti ja turvallisesti niitä tarvitsevien saatavilla. Toimintojen digitalisoinnin ja uudelleen organisoinnin avulla voidaan hallinnon asiakkaiden palveluja parantaa ja samalla alentaa kustannuksia.[40] Valtionhallinnon digitalisoinnin tavoitteita kuvataan kansainvälisissä lähteissä käsitteillä ”government as a platform” (GaaP) tai ”whole-of-government”, joilla tarkoitetaan mm. parempia palveluja ja tehokkaampaa toimintaa siiloutuneita toimintoja avaamalla, hallinnon yhteisiä IT-ratkaisuja, digitaalista infrastruktuuria sekä yhteisiä rajapintoja ja avoimempaa tiedon jakamista.[41, 42]

Kaikissa verrokkivaltioissa on päädytty ratkaisuun, jossa julkisen hallinnon digitalisoinnin koordinointia ja ohjausta on keskitetty yhdelle toimijalle. Monissa verrokkivaltioissa myös toteutusvastuu on samalla organisaatiolla. Alankomaiden kokonaiskoordinoinnista vastaa poikkihallinnollinen, konsultoiva toimielin (Digital Government Policy Consultation, OBDO). Sen tukena ovat operatiivinen,

[34] https://www.weforum.org/agenda/2021/07/global-consumer-behaviour-trends-online-shopping/
[35] https://www.oecd.org/health/digital-health.htm
[36] https://stm.fi/-/suomessa-on-kaytossa-useita-sahkoisia-sosiaali-ja-terveyspalveluja-kansalaisille-ammattilaisten-kaytossa-olevien-tietojarjestelmien-kaytettavyytta-ja-
[37] https://www.finanssiala.fi/uutiset/mustread-kateinen-tekee-hidasta-kuolemaa-ja-korona-nopeutti-saattohoitoa/
[38] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en
[39] Digital Strategy 2025, Germany
[40] https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/transforming%20government%20through%20digitization/transforming-government-through-digitization.pdf
[41] https://medium.com/digitalhks/a-working-definition-of-government-as-a-platform-1fa6ff2f8e8d
[42] https://gds.blog.gov.uk/2015/03/29/government-as-a-platform-the-next-phase-of-digital-transformation/

voittoa tavoittelematon organisaatio (Government ICT Unit, ICTU), joka kehittää koko hallinnon laajuisia ratkaisuja sekä Government Shared Services for ICT (Logius), joka ylläpitää yhteisiä ICT-ratkaisuja ja yhteisesti käytettäviä, velvoittavia standardeja. Saksan IT-Planungsrat on poikkihallinnollinen komitea, jossa ovat mukana kaikki hallinnonalat ja osavaltioiden edustus. Komitea määrittää liittovaltiolle ja osavaltioille velvoittavat digitalisaatiohankkeita koskevat säännöt. Komitean tueksi on vuoden 2020 perustettu kansallinen yhteistoimintaorganisaatio (FITKO), jonka tehtävänä on keskitetysti koordinoida komitean digitalisaatiohankkeita ja hallita niihin osoitettua budjettia.

Suomessa yhteiskunnan ja julkisen hallinnon digitalisaation vastuita on useammalla toimijalla. Valtioneuvosto asetti 2.9.2021 uuden ministeriryhmän ohjaamaan digitalisaation, datatalouden ja julkisen hallinnon kehittämistä sekä koordinoimaan näihin liittyviä toimenpiteitä ja tilannekuvaa.[43] Ryhmä jatkaa julkisen hallinnon uudistamisen poliittiselle johtoryhmälle asetettujen tehtävien edistämistä. Ryhmä sovittaa yhteen kehittämishankkeita ja tekee tarvittavia poliittisia linjauksia keskeisistä toimialansa kehittämiseen liittyvistä toimista. Ministeriryhmän vastuulle annettiin 10.3.2022 myös kyberturvallisuuden ja julkisen hallinnon varautumisen ohjaaminen.[44] Ryhmä tekee tarvittavat poliittiset linjaukset toimista, joilla taataan yhteiskunnan toimintakyky ja digitaalinen toimintaympäristö kyberhäiriöissä ja kybervaikuttamisessa.

Digitoimisto on pysyvä yhteistyöryhmä, jonka tehtävänä on vahvistaa ministeriöiden välistä yhteistyötä, koordinaatiota ja tiedonkulkua digitalisaatiossa ja datataloudessa. Julkisen hallinnon digitaalisen turvallisuuden hallinnon kehittäminen liittyy osaltaan myös digitoimiston tehtäviin. Digitoimisto tukee työllään digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministeriryhmän toimintaa. Digitoimisto ylläpitää digi-, data- ja tietopolitiikan tilannekuvaa eli digisalkkua. Tavoitteena on, että liikenne- ja viestintäministeriön, valtiovarainministeriön ja työ- ja elinkeinoministeriön digitalisaation ja datatalouden kehittämisen toimet muodostavat yhtenäisen kokonaisuuden ja jaetun tilannekuvan.

Valtiovarainministeriön tehtävänä on julkisen hallinnon tiedonhallinnan, tietopolitiikan ja sähköisen asioinnin edistäminen. Digi- ja väestötietovirasto ylläpitää yleistä tilannekuvaa julkisen hallinnon tietohallinnosta, tiedonhallinnasta, tietoturvallisuudesta ja digitaalisista palveluista, sekä tuottaa ja kehittää näitä sekä sähköistä asiointia koskevia menetelmiä ja välineitä sekä asiantuntijapalveluita.

Julkisen hallinnon digitaalisten palvelujen ja ratkaisujen perustana on yhteinen ICT-arkkitehtuuri sekä tietoihin ja niiden käsittelyyn liittyvät yhteiset periaatteet kuten tiedon avoimuus, uudelleenkäytettävyys ja eettiset periaatteet. Arkkitehtuuri määrittelee, miten julkisissa digipalveluissa sovelletaan yleisesti hyväksyttyjä, pääasiassa kansainvälisiä standardeja, yhtenäisiä teknologiaratkaisuja ja rajapintoja, joilla varmistetaan, että palvelujen toteutukset ovat kestäviä, turvallisia ja luotettavia. Julkisen hallinnon suurin digipalvelujen käyttäjäryhmä ovat kansalaiset, mutta myös viranomaiset ja muut organisaatiot tarvitsevat yhteisiä ratkaisuja hallinnon toiminnan tehostamisen tueksi.

[43] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80751b54
[44] https://www.lvm.fi/-/ministerityoryhma-vastaamaan-kyberturvallisuudesta-ja-julkisen-hallinnon-varautumisesta-1684814

Verrokkivaltioiden digitalisaatioviranomaiset ja muut digitalisaatiota koordinoivat toimijat määrittävät ja ylläpitävät julkisen hallinnon ICT-arkkitehtuuria ja niiden tehtäviin kuuluvat yleensä myös sähköiset identiteettiratkaisut ja tunnistautuminen julkisen hallinnon palvelujen käyttämiseksi. Viranomaiset määrittävät myös standardit, joita julkisen hallinnon digitalisoinnissa tulee noudattaa. Ruotsin DIGG on linjannut, että ensisijaisesti on käytettävä kansainvälisesti hyväksyttyjä standardeja kuten esimerkiksi ISO-standardit. Alankomaissa Logius ylläpitää luetteloa velvoittavista standardeista[45], joihin kuuluvat esimerkiksi ISO27001 ja ISO27002 sekä ETSIn digitaalista allekirjoitusta koskevat standardit.

Tieto, sen arvo ja merkitys organisaatioiden toiminnalle ja niiden johtamiselle on yleisesti tunnistettu julkisessa hallinnossa. Verrokkivaltioiden digitalisaatiota koordinoivat toimijat pyrkivät edistämään tiedon avoimuutta ja julkisen hallinnon keräämien tietojen (esimerkiksi julkiset hankinnat, ajoneuvotiedot, kiinteistötiedot, karttatiedot, jne.) laajaa käytettävyyttä ja parantamaan tiedon laatua keräämällä tiedon keskitetysti. Alankomaissa kymmenen keskeistä rekisteriä on koottu OBDOn hallintaan ja Virossa RIA (RIHA) ylläpitää yllä luetteloa hallinnon tietojärjestelmistä ja niiden sisältämistä tiedoista sekä tarjoaa välineitä tietojen käyttöä varten.

Isossa-Britanniassa, Israelissa ja Virossa valtio tuottaa omia pilvipalvelualustoja hallinnon käyttöön. Muissa verrokkivaltioissa digitalisaatiosta vastaava toimija ohjeistaa pilvipalvelujen käyttöä julkisessa hallinnossa, mutta ei tarjoa itse varsinaisia pilvipalveluja.

OECD julkaisee hallinnon digitalisaatiota kuvaavaa indeksiä (Digital Government Index, DGI[46]), joka perustuu kuuteen osa-alueeseen: digitaaliseksi suunniteltu (”digital by design”), tiedolla johdettu hallinto (”data-driven public sector”), valtionhallinto alustana (”government as a platform”), avoimuus (”open by default”), käyttäjäkeskeisyys (”user-driven”) ja ennakointi (”proactiveness”). Indeksi kuvaa koko digitalisaation toteutumista ja digitalisaatiokäytäntöjen kypsyyttä koko valtionhallinnon laajuisesti. Verrokkivaltioista Iso-Britannia ja Israel ovat tuoreimman (2019) indeksin perusteella selvästi OECD:n keskiarvoa korkeammalla.

Julkisen hallinnon tiedon avoimuutta kuvaava OECD:n OURdata-indeksi (Open-Useful-Reusable) [47] vuodelta 2019 osoittaa, että verrokkivaltioista Australia ja Alankomaat sijoittuvat OECD:n keskiarvoa paremmin, sijoille 6 ja 13. YK:n E-Government Development Index (EGDI) [48] vertailussa vuodelta 2020 usea verrokkivaltio sijoittui keskiarvion yläpuolelle. Parhaimpina Viro oli sijalla kolmantena, Suomi neljäntenä, Australia viidentenä, ja Ruotsi sijalla kuusi.

DESI seuraa Euroopan yleistä digitaalista suorituskykyä ja EU-valtioiden edistymistä useasta eri näkökulmasta, joita ovat esimerkiksi digitaalinen kilpailukyky, digitaalisten yhteyksien käyttö, digitaalisten taitojen ja digitaalisten julkisten palvelujen kehittyminen sekä tutkimus- ja kehitystoiminta. DESI arvioi kunkin jäsenvaltion digitalisaation tilaa ja tunnistaa ensisijaisia investointeja edellyttävät

[45] https://forumstandaardisatie.nl/open-standaarden/verplicht
[46] https://www.oecd-ilibrary.org/sites/2bed4623-en/index.html?itemId=/content/component/2bed4623-en
[47] https://www.oecd.org/gov/digital-government/open-government-data.htm
[48] https://publicadministration.un.org/egovkb/en-us/Data/Compare-Countries

alat ja toiminnat. Vuonna 2021 Suomi sijoittui DESI-vertailussa toiseksi, ja sen jälkeen verrokkivaltioista Ruotsi kolmanneksi, Alankomaat neljänneksi ja Viro sijalle setsemän.[49]

[49] https://digital-agenda-data.eu/charts/desi-composite#chart={%22indicator%22:%22desi_sliders%22,%22breakdown%22:{%22desi_hc%22:5,%22desi_conn%22:5,%22desi_idt%22:5,%22desi_dps%22:5},%22unit-measure%22:%22pc_desi_sliders%22,%22time-period%22:%222021%22}

LIITE 2 SELVITYKSEN MAAKOHTAINEN AINEISTO

Taulukko 1: Yhteenveto keskitetyistä toimijoista

	Alanko-maat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
julkisen hallinnon digitalisoituminen	OBDO, ICTU, Logius	DTA	GDS	Government ICT Authority	DIGG	IT-Planungs-rat, FITKO	useat minis-teriöt	RIA	DVV
keskitetty digi- ja tietoturvallisuuden hallinta	NCTV/NCSC	ASD/ACSC, CISC	GCHQ/NCSC, CPNI	INCD, ISA	MSB, FRA, Säpo, FM → CFCS	BSI, BMI, BBK	FSB, EMERCOM, Mintsifry Ros-sii	MKM, RIA, CIIP	Turvallisuuskomi-tea, DVV, Tra-ficom, HVK
yleinen tietosuoja	AP	OIAC	ICO	PPA	IMY	BfDI	Roskomnadzor	AKI	tietosuojavaltuute-tun toimisto
kansallinen turval-lisuus	NCTV	ASD	GCHQ	ISA	FRA, Säpo, FM	BfV	FSB	Välisluuramet, RIA	NSA, Supo, PV, Traficom

Taulukko 2: Yhteiskunnan digitalisoitumisen edistäminen

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
valtionhallinnon digitalisointi ja digitaalinen transformaatio	OBDO	DTA	GDS	Government ICT Authority	DIGG	IT-Planungsrat, FITKO, BMI	Mintsifry Rossii ja muut ministeriöt	RIA	DVV
sähköinen tunnistamisen ja identiteetin tarjoaminen	OBDO	DTA	GDS	Government ICT Authority	DIGG	BSI	Mintsifry Rossii	RIA	DVV
julkisen hallinnon ICT-arkkitehtuuri ja standardien käyttö	ICTU, Logius	DTA	GDS	Government ICT Authority	DIGG	BSI, KoSIT	Mintsifry Rossii	RIA	DVV, Traficom
hallinnon yhteiset tietojärjestelmät ja -alustat	ICTU, Logius	valtiovarainministeriö	GDS	Government ICT Authority		BSI	Mintsifry Rossii	RIA, RIKS	Valtori, Suomen Erillisverkot
hallinnon tietoverkot ja tietoliikenteen turvaaminen	Logius	ASD/ACSC	GCHQ/NCSC	Government ICT Authority	MSB	BSI	Mintsifry Rossii	RIA	Valtori, Suomen Erillisverkot
avoin ja jaettu data, perusrekisterit	OBDO	DTA	GDS	Government ICT Authority	DIGG	BMI	Mintsifry Rossii		VM, DVV
julkisen hallinnon digipalvelujen ohjeistus		DTA	GDS	Government ICT Authority	DIGG	BSI		RIA	tiedonhallintalautakunta, DVV
digi- ja ICT-hankintojen ja investointien ohjaus		DTA			DIGG	BMWi		valtiovarainministeriö	VM
keskitetyt digi- ja ICT-hankinnat	PIANOo		Crown Commercial Service (CCS)		Upphandlingsmyndigheten			RIK	Hansel
älykkäät ja oppivat järjestelmät (AI)	Ministerie van Economische Zaken en Klimaat	teollisuusministeriö	Office for Artificial Intelligence						VM/AuroraAI

Taulukko 3: Keskitetty digi- ja tietoturvallisuuden hallinta

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
kansalliset strategiset riskit, uhka-arviointi (erityisesti kyber- ja digiuhkat)	NCTV	CISC	GCHQ/NCSC	INCD	MSB	BSI		sisäministeriö	turvallisuuskomitea, DVV, Traficom, HVK,
kansallisten kyberhäiriöiden hallinta	NCTV/NCSC	ASD/ASCS	GCHQ/NCSC	INCD	MSB	BSI	EMERCOM	RIA	Traficom
kyberresilienssi, kybervarautuminen ja jatkuvuudenhallinta	NCTV/NCSC	ASD/ ACSC	GCHQ/NCSC	INCD	MSB	BSI		RIA	Traficom, HVK
kriittinen infrastruktuuri ja varautuminen (fyysinen)	NCTV	CISC	CPNI	ISA, INCD	MSB	BBK, BMI	EMERCOM	MKM, RIA	HVK
kriittinen digi-infrastruktuuri	NCTV	ASD/ACSC, CISC	GCHQ/NCSC	ISA, INCD	MSB	BSI	Mintsifry Rossii	RIA	HVK, Traficom, Valtori
kansallinen kyberharjoitustoiminta	NCTV/NCSC	ASD/ ACSC (koordinointi)	GCHQ/NCSC (ohjeistus)		MSB (koordinointi)	BSI	EMERCOM	RIA	Traficom, DVV, HVK
kansalliset digiturvavaatimukset, -suositukset ja –ohjeet	NCTV/NCSC	ASD/ ACSC	GCHQ/NCSC	INCD	MSB	BSI	Mintsifry Rossii	RIA	Traficom, tiedonhallintalautakunta, DVV
kansalaisten ja organisaatioiden digiturvakoulutus ja -neuvonta	NCTV/NCSC	ASD/ ACSC	GCHQ/NCSC	INCD	MSB	BSI	Mintsifry Rossii	RIA	DVV, Traficom
kansallinen IT-tuotesertifiointi		ASD	GCHQ/NCSC			BSI, kaupalliset toimijat			
kansallinen kyberturvan henkilösertifiointi			GCHQ/NCSC	INCD		BSI			ei ole

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
digi- ja kyberturvallisuuden tilannekuva	NCTV/NCSC	ASD/ ACSC	GCHQ/NCSC	INCD	MSB	BSI		RIA	VNK, Traficom, ict-palveluntuottajat
CERT-toiminta	NCTV/NCSC	ASD/ ACSC	GCHQ/NCSC	INCD	MSB	BSI	CERT.GOV.RU RU-CERT	RIA	Traficom
NIS-yhteyspiste	NCTV/NCSC	n/a	GCHQ/NCSC	n/a	MSB	BSI	n/a	RIA	Traficom

Taulukko 4: Tietosuoja

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
yleinen tietosuoja ja yksityisyyden suoja	AP	OIAC	ICO	PPA	IMY	BfDI	Roskomnadzor	AKI	tietosuojavaltuutetun toimisto

Taulukko 5: Kansallinen ja sisäinen turvallisuus

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
terrorismin torjunta, järjestäytyneen rikollisuuden torjunta	NCTV	AFP	GCHQ, National Counter Terrorism Security Office (NaCTSO)	ISA	Säpo	BfV, BKA	FSB		Supo, KRP
tiedustelu, signaalitiedustelu		ASD	GCHQ		Säpo?, FRA	BND	FSB	Välisluuramet	Supo, PV
kyberpuolustus ja sotilaallinen kyberulottuvuus		ASD	GCHQ	INCD	FRA, FM	Militärischer Abschirmdienst (MAD)	FSB	RIA, CCDCOE	PLM, PV

ALANKOMAAT

Taulukko 6: Alankomaat – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
The National Coordinator for Counterterrorism and Security (NCTV)	oikeusministeriö	• making the Netherlands cyber secure • preventing attacks and combating terrorism and extremism • making the Netherlands resilient to threats from state actors
The Dutch Data Protection Authority (AP)	oikeusministeriö	• supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data (GDPR)
Digital Government Policy Consultation (OBDO)	intergovernmental consultative body	• coordination of base registries at all subnational levels (regional, local, municipal) • advises the State secretary about the common Digital Government Policy • coordination of digital government infrastructure

Toimija	Ohjaus	Keskeiset tehtävät
National Cyber Security Centre (NCSC)	NCTV	• identify and clarify risks and trends • connect parties, knowledge and information • prevent social damage and mitigate threats • on standby 24/7 in case of a crisis • monitors all (potentially) suspect sources on the internet • advises organisations on how to protect themselves from online threats • monitors developments in digital technology and updates security systems • supporting vital providers and government bodies in implementing measures to ensure the continuity of their services • providing information and advice about threats and incidents relating to the network and information systems of vital providers and the national government • performing analyses and conducting technical investigation in response to threats and incidents
Government ICT Unit (ICTU)	independent consultancy, non-profit organization	• support the government with the development, introduction and implementation of innovative ICT applications (mainly government wide solutions) • executes programmes under commission mostly commissioned by the central government • conducts the day-to-day management of Netherlands Government Reference Architecture (NORA)
Government Shared Services for ICT (Logius)	sisäministeriö	• digital government service of the Netherlands Ministry of the Interior and Kingdom Relations • maintains government-wide ICT-solutions and common standards • supplies products relating to access, data exchange, standardization, and information security
National Crisis Centre (NCC)	NCTV	• Coordinating the response of the different Ministers and public authorities when a crisis affects several departments or regions • Improving preparedness through risk assessments, elaboration of national crisis plans, the organisation of exercises and continuously improving risk- and crisis communication. (lähde)

Taulukko 7: Alankomaat – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
The Dutch Security Cluster (Security Delta)	tutkimus ja kehitys	• enhance knowledge of Dutch organisations about 'security in a digitising world’

Foorumi	Teema	Keskeiset tavoitteet
		• build powerful collaborations leading to valorisation and sustainable security innovations • help organisations make new connections and enter the (inter)national market to scale up innovations • help organisations arrange funding for security solutions and capital for growth • contribute to solving the mismatch between supply and demand of security talent
De Cybersecurity Alliantie (CS Alliantie)	PPP-yhteistoiminta	• platform of the public-private partnership for a digitally resilient Netherlands • parties that are actively involved in the CS Alliance carry out concrete, short-term projects that contribute to the pursuit of a digitally resilient Netherlands • supporting large and small organizations in finding concrete solutions for complex cyber issues
Cyber Security Council (CSR)	PPP-yhteistoiminta	• provide solicited and unsolicited strategic advice on cybersecurity to the Dutch government and the business community • monitor trends and new technological developments and translating these into potential measures to reduce the cybersecurity risks and to increase the economic opportunities • initiate and/or accelerate relevant initiatives in the Netherlands and in the European Union that demonstrably contribute to raising the level of cybersecurity in the Netherlands

AUSTRALIA

Taulukko 8: Australia – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Australian Signals Directorate (ASD)	Department of Defence	• an independent statutory agency • covert acquisition of foreign information not publicly available (signals intelligence) • comprehensively understanding the cyber threat, providing proactive advice and assistance to improve the management of cyber risk by government, business and the community • applying our offensive cyber capabilities offshore, to support military operations, counter-terrorism, counter cyber espionage and serious cyber-enabled crime • deliver offensive cyber operations to support a range of Australian Government priorities
Office of the Australia Information Commissioner (OAIC)	Attorney-General's Department (independent agency)	• privacy and freedom of information • conduct investigations • handle complaints • review decisions made under the Freedom of Information (FOI) Act • monitor agency administration • advise the public, organisations, and agencies
Digital Transformation Agency (DTA)	Australian Government	• government's Chief Digital Advisor • provides strategic leadership on whole-of-government and shared ICT and digital services, including sourcing and capability development • delivers policies, standards and platforms for whole-of-government and shared ICT and digital service delivery • provides advice to agencies and the Government on ICT and digital investment proposals • oversee significant ICT and digital investments, assurance policy and framework, and the whole-of-government digital portfolio
Department of Home Affairs	Australian Government	• lead the development of cyber security policy for the Australian Government, including the implementation of the Government's Cyber Security Strategy and Action Plan

Taulukko 9: Australia – digitaalisen turvallisuuden muita toimijoita

Toimija	Ohjaus	Keskeiset tehtävät
Australian Cyber Security Center (ACSC)	ASD (1.7.2018 →)	• responds to cyber security threats and incidents as Australia's computer emergency response team (Aus-CERT) • collaborates with the private and public sector to share information on threats and increase resilience • works with governments, industry and the community to increase awareness of cyber security • provides cyber security information, advice and assistance to all Australians
Cyber and Infrastructure Security Centre (CISC)	Department of Home Affairs (1.9.2021 →)	• industry partnerships, collaboration, engagement and best practice advice • identification and mitigation of all hazard risks • critical infrastructure modelling • standards, accreditation and regulatory reform policy • support for industry and government capabilities • compliance and regulatory functions that prioritise education and partnerships ahead of enforcement and compliance outcomes • a background checking service including implementing reforms to use criminal intelligence to treat trusted-insider risks in the aviation and maritime sectors, as well as issuing body reforms
The independent Inspector-General of Intelligence and Security (IGIS)	independent statutory office	• ensure that the intelligence agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights
Australian Security Intelligence Organisation (ASIO)	Minister for Home Affairs	• Australian intelligence agency and the nation's security service • protects Australians from religiously motivated and ideologically motivated violent extremism • counters espionage and foreign interference • supports whole-of-government efforts to protect Australia's border integrity
Australian Secret Intelligence Service (ASIS)	Minister for Foreign Affairs	• Australia's foreign intelligence collection agency • collect and distribute secret foreign intelligence, information which would be otherwise unavailable to Australia, in order to protect Australia and further Australian interests • statutory agency that provides foreign intelligence for those departments that formulate policy

Taulukko 10: Australia – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
Joint Cyber Security Centres (JCSC)	kyberturvallisuus	• quickly sharing sensitive information, including actionable cyber threat intelligence between and among partners • develop solutions to cyber security risks and issues through collaboration and without commercial bias • common understanding of the cyber security environment and optimal mitigation options is achieved through sharing and analysis of incidents, threats and risks • organizations at all levels have access to practical tools and resources to improve their cyber security • consistent education and awareness messages are promoted with and among partners
Defence Science and Technology Group (DSTG)	maanpuolustusteknologiat	• Australian government's lead agency responsible for applying science and technology to safeguard Australia and its national interests • work with industry, universities and the scientific community to enhance the combined ability to support Australia’s defence and national security capabilities and to contribute to national wealth

Foorumi	Teema	Keskeiset tavoitteet
Information Warfare Division (IWD)	informaatiosodankäynti	• part of Australian Defence Forces; warfare capability • C4 and cattle management capability • capability support directorate • Joint Cyber Unit
The Trusted Information Sharing Network (TISN)	kriittinen infrastruktuuri	• Australian Government's primary engagement mechanism with industry on critical infrastructure • understanding threat, vulnerability and consequence to better manage risk • increasing awareness and understanding of cross-sector dependencies and the impacts of a disruption to any critical infrastructure sector • enhancing communication channels and networks between industry and all levels of government • identifying gaps and implementing appropriate mitigation strategies within each sector • informing future policies and programs to support critical infrastructure resilience
National Intelligence Community (NIC)		• comprises of ASD, Australian Geospatial-Intelligence Organisation (AGO), Australian Secret Intelligence Service (ASIS), Australian Security Intelligence Organisation (ASIO), Defence Intelli-

Foorumi	Teema	Keskeiset tavoitteet
		gence Organisation (DIO), Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Department of Home Affairs • collect, analyse and disseminate intelligence information and advice in accordance with Australia's interests and national security priorities • has a mandate to integrate the intelligence functions of government, and provide more opportunities for collaboration, coordination and cooperation to address the increasing complexity of Australia's geostrategic environment, the rapid pace of technological change and broadening scope of security and intelligence challenges

ISO-BRITANNIA

Taulukko 11: Iso-Britannia – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Government Communications Headquarters (GCHQ)	hallitus	• Counter Terrorism - Stopping terrorist attacks in the UK and against our interests overseas • Cyber Security - Making the UK the safest place to live and do business online • Strategic Advantage - Managing the threats from hostile states, promoting the UK's prosperity and shaping the international environment • Serious & Organised Crime - Reducing the social and financial harm that serious and organised crime causes to the UK • Support to Defence - Protecting Defence personnel and assets and supporting an integrated approach to war fighting
Information Commissioner's Office (ICO)	Department for Digital, Culture Media and Sport	• uphold information rights in the public interest • promoting openness by public bodies • data privacy for individuals
Government Digital Service (GDS)	Cabinet Office	• provide vital information and services for users through GOV.UK • support government's response to COVID-19 by providing digital leadership and tools to enable services to be rapidly built and deployed • maintain, iterate and improve the services and tools we provide to the rest of government • increase the use of shared platforms and components across government • support departments by strengthening their digital capability and providing direct support for major digital projects • enhance government's digital capability through the GDS Academy

Toimija	Ohjaus	Keskeiset tehtävät
The National Cyber Security Centre (NCSC)	GCHQ	• supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public • understands cyber security, and distils this knowledge into practical guidance that we make available to all • responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK • uses industry and academic expertise to nurture the UK's cyber security capability • reduces risks to the UK by securing public and private sector networks
Centre for the Protection of National Infrastructure (CPNI)	Cabinet Office	• national technical authority for physical and personnel protective security • protect national security by helping to reduce the vulnerabilities from threats such as terrorism, espionage and sabotage • works with partners in government, police, industry and academia
The National Crime Agency (NCA)	Cabinet Office	• serious and organised crime • focus on critical cyber incidents • prevent young people from slipping into cyber crime
Office for Artificial Intelligence	Department for Digital, Culture, Media & Sport and the Department for Business, Energy & Industrial Strategy	•

Taulukko 12: Iso-Britannia – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
National Security Council (NSC)	kansallinen turvallisuus	• main forum for collective discussion of the government’s objectives for national security • ensure that ministers consider national security in the round and in a strategic way

Foorumi	Teema	Keskeiset tavoitteet
National Security Secretariat	kansallinen turvallisuus	• providing policy advice to the National Security Council • coordinating and developing foreign and defence policy across government • coordinating policy, ethical and legal issues across the intelligence community • developing effective protective security policies and capabilities for government • improving the UK's resilience to respond to and recover from emergencies • providing strategic leadership for cyber security in the UK
Joint Intelligence Organisation (JIO)	kansallinen turvallisuus	• support the work of the Joint Intelligence Committee and National Security Council • provide authoritative, all-source assessment for the Prime Minister, the National Security Council (NSC) and senior policy makers • evaluate emerging technology, economic and health security, climate change and horizon scanning • overseen by the Intelligence and Security Committee of Parliament

ISRAEL

Taulukko 13: Israel – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Israel National Cyber Directorate (INCD)	Prime Minister's office (2018)	• defending Israel's national cyberspace and for establishing and advancing Israel's cyber power • to prevent and handle cyberattacks and to strengthen emergency response capabilities • advances innovative cyber solutions and forward-looking technological solutions • formulates strategies and policies in the national and international arenas • develops its cyber manpower • provides incident handling services and guidance for civilian entities and critical infrastructures
The Privacy Protection Authority (PPA)	Ministry of Justice	• outline the Israeli data protection policy • build trust in the digital economy • promoting individual's control on personal identifiable data • promoting processes of privacy by design across the economy
Government ICT Authority	PrimeMinister's Office	• creation, development and operation of secure technological solutions and infrastructure • promoting "ask only once" vision, Open government, and access to public databases • government cloud and API and government API Management Platform • set standards and improve the level of service provided by government bodies to public • hosting on the government server farm • guides and directs ministries in cyber defence matters • a cross-organization infrastructure (G2G network) and service to share and transfer secured data and emails • B2G network network facilitates contact between the government and the business sector (banks, credit companies, etc.) • government issue of verification certificates • protect all systems and infrastructures against complex cyber attacks; building advanced defense capabilities
Israeli Security Agency (ISA)	Prime Minister's office	• developing new and innovative systems and infrastructures in the field of intelligence/operational technology • initiating, developing, and producing advanced technological tools for intelligence collection

Toimija	Ohjaus	Keskeiset tehtävät
Israel National Cyber Event Readiness Team (CERT-IL)	INCD	• handles cyber incidents in the civilian cyber sphere • responding to cyber incidents • promoting preventive activities • creating tailor made partnerships and coordination between industries, government and international partners when dealing with and responding to cyber incidents • enhancing information sharing • preparing and issuing alerts to the public

Taulukko 14: Israel – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
CyberSpark		• cyber research (Israeli SMEs, multinational corporations, university)
National Security Council	kansallinen turvallisuus	• Prime Minister's political security headquarters • integrate the views and positions of various governmental and security bodies • wide spectrum of professionals (military, security, intelligence professionals, diplomats, technology, law and the economy, researchers)

RUOTSI

Taulukko 15: Ruotsi – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Myndigheten för samhälls-skydd och beredskap (MSB)	Justitiedepartemen-tet	• support and develop civil defence • preparedness for accidents, crises, and war; coordinate the municipalities at national level • organizing training and exercises • identify and analyze serious vulnerabilities, threats and risks in society; overall planning of necessary counter-measures • develop and strengthen society's ability to prevent and deal with incidents involving hazardous substances (e.g. flammable material, chemicals, radioactive material) • participate in Sweden's international humanitarian activities • order and coordinate research and development work for protection against accidents, crisis preparedness and civil defense; NIS-contact point • manage and develop secure communications systems (Rakel, SGSI) • support and coordinate society's information security work; preventive advice and support to government agencies, municipalities, regions, companies, and organizations • participate in national and international ISO/CEN/SIS standardization committees (e.g. crisis management, information security, fire) lähde; lähde (MSB)
Integritetsskydds myndi-gheten (IMY)	Justitiedepartemen-tet	• review and enforce the application of data protection rules • provide guidance and support to authorities, companies, organizations and the general public • support uniform application of data protection rules within the EU (GDPR) • issue permits and carry out supervision regarding camera surveillance, debt collection activities and credit in-formation • monitor and report on developments in the field of privacy

Toimija	Ohjaus	Keskeiset tehtävät
Myndigheten för digital förvaltning (DIGG)	Infrastrukturdepartementet	• coordinate and support the digitisation of the administration • responsible for the shared digital infrastructure • provide the government with information on public administration and the digitisation of society • monitoring, analysing and describing developments • electronic identification and signature services • support electronic procurement • promote use of open data and re-use of public administration documents • promote accessibility of digital services
Försvarets radioanstalt (FRA)	Försvarsdepartementet	• support the protection of society's important activities against attacks carried out by state or state-aided organizations • cyber defense

Taulukko 16: Ruotsi – digitaalisen turvallisuuden muita toimijoita

Toimija	Ohjaus	Keskeiset tehtävät
Nationellt center för cybersäkerhet (CFCS)	MSB, FRA, Säpo, Försvarsmakt	• coordinate the work to prevent, detect and manage cyber-attacks and other IT incidents • compile joint analyses and promote overall situational awareness regarding threats and vulnerabilities • provide advice and support on threats, vulnerabilities and risks • coordinate work in the event of cyberincidents, including cyberattacks
CERT-SE	MSB	• disseminating information, coordinating actions and participating in work required to remedy or mitigate the effects of cyber incidents • cooperate with authorities with specific responsibilities in the field of information security • act as Sweden's point of contact with corresponding functions in other countries and develop cooperation and exchange of information with them
National Centre for Security in Control Systems for Critical Infrastructure (NCS3)	MSB, FOI	• securing the functionality and security of industrial information and control systems through research and development • cyber-physical model of the societal impact of cyber incidents • increase the competence and capability to manage industrial information and control systems from an IT-security perspective
Research institute of Sweden (RISE)	independent, state-owned research institute	• Sweden’s research institute and innovation partner • international collaboration programmes with industry, academia and the public sector • mission is to work for sustainable growth by strengthening the competitiveness and capacity for renewal of Swedish industry
Myndigheten för psygologiskt försvar (MPF)	Justitiedepartementet	• lead the coordination and development of Sweden’s psychological defence in collaboration with public authorities and other stakeholders in society • offer support to government agencies, municipalities, regions, the business sector, and organisations, as well as contribute to strengthening the resilience of our population • works both preventively and operationally and fulfils its tasks both in peacetime and in the event of war • contributes to creating resilience and a willingness to defend the country

Taulukko 17: Ruotsi – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
Forum för informations-delning om informations-säkerhet (FIDI)	sektorikohtainen tiedonvaihto	• public-private collaboration fora • increase information security among all participating actors through information exchange, analysis of the surrounding world • production of common information material • e.g. FIDI-SCADA, FIDI-Vård och omsorg, FIDI-Drift, FIDI-Telekom, FIDI-Finans lähde
Cybersäkerhetsrådet	tietoturvallisuus	• Information on development trends in the field of information security, i.e. protection of information and security of information systems • Views on the focus, prioritization and implementation of MSB's work in the area • Quality assurance and credibility of MSB's work by being properly composed and linked to vital societal functions • To contribute to the dissemination of information about MSB's work with information security in the outside world lähde

SAKSA

Taulukko 18: Saksa – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bundesministerium des Innern und für Heimat	• central IT security service provider for the federal government • investigates security risks associated with the use of IT and develops preventive security measures • provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions • IT security testing and assessment of IT systems, including their development, in co-operation with industry • advises manufacturers, distributors and users of information technology • analyses development and trends in information technology
IT-Planungsrat	poikkihallinnollinen komitea	• the central political steering committee between the federal and state governments (information technology and the digitization of administrative services) • promotes and develops common IT solutions • provide the federal and state governments with a binding basis for joint federal digitization activities • coordinating body for the network linking the IT networks of the federal and state governments • coordination of federal cooperation on information technology issues • definition of overarching IT interoperability and security standards
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	Bundesministerium des Innern und für Heimat	• develops and tests cyber-related strategies, technical solutions and tools and coordinates joint projects for the security authorities • application-oriented research coordinated with various authorities • provides comprehensive advice to the security authorities on technical issues and strategies (previously distributed among almost 40 different authorities at the federal and state levels) • contributes to effective danger prevention and prosecution by the competent authorities and helps to protect citizens
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BDfI)	independent authority	• data protection and privacy (GDPR)

Toimija	Ohjaus	Keskeiset tehtävät
Federal IT Cooperation (FITKO) 1.1.2020 →	IT-Planungsrat	• organisational and technical support for the IT Planning Council (IT-Planungsrat) • hub for federal activities relating to the digitalisation of the administrative system • formulating and implementing the federal IT strategy • designing and developing the federal IT architecture • coordinating and providing operational management for the products and projects of the IT Planning Council • managing the digitalisation budget
Koordinierungsstelle für IT-Standards (KoSIT)	IT-Planungsrat	• coordinates the development and operation of IT standards for data exchange in the public administration • supports adopting subject-independent and interdisciplinary IT-interoperability and IT-security standards and steering e-government projects
Nationales Cyber-Abwehrzentrum, Cyber-AZ (NCAZ)	BKA	• a joint, cross-authority and cross-institutional platform (not an independent authority) • exchange relevant information quickly between the authorities and partners • coordinate protective measures to ensure cyber security in Germany • founded in 2011 as part of the implementation of the Federal Government's Cyber Security Strategy (CSS) • brings cybersecurity expertise in federal agencies and ensure effective and efficient collaboration among all government agencies to coordinate protection and response to IT incidents • cooperation platform among governmental agencies (e.g. Federal Police, Federal Intelligence Service, etc.)
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	Bundesministerium des Innern und für Heimat	• crisis management; Joint Reporting and Situation Center • review and development of emergency planning with federal and state authorities • physical protection of critical infrastructure • civil-military cooperation • identification of research needs and preparation of framework plans, ABC protection / provision in the field of science, technology and medicine • design and procurement of supplementary civil protection equipment for the federal states • execution and evaluation of exercises, (e.g. country-wide crisis management exercise LÜKEX) • scientific supervision of research projects as well as their evaluation and implementation • conducting studies and investigations, seminars, exercises and other events for civil-military cooperation

Taulukko 19: Saksa – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
Competence Network Trusted Cloud (Trusted Cloud)		• create transparency and build trust in cloud technologies • provide orientational knowledge such as checklists and guidelines • serves as an exchange platform for interested parties, as a form of transferring knowledge and as a way of jointly developing requirements • membership available to individuals, companies, organisations, and commercial and public institutions

VENÄJÄ

Taulukko 20: Venäjä– digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Federal Security Service (FSB)	The President of the Russian Federation	• implement government policy in the national security of the Russian Federation • counterterrorism, organized crime • counter-intelligence and intelligence • the protection and defence of the state border of the Russian Federation • the protection of internal sea waters, the territorial sea, the exclusive economic zone, the continental shelf and their natural resources • ensuring the information security of Russia • exercising the basic functions of the federal security services
Ministry of Digital Development, Communications and Mass Media (Mintsifry Rossii)	The President of the Russian Federation	• telecommunications, including the allocation and conversion of the radio frequency spectrum, and postal communications • information technology, including creation of government information resources and promotion of access to such resources • personal data processing and Internet governance
Federal Service for Supervision of Communications, Information Technologies and Mass Media (Роскомнадзор, "Roskomnadzor")	Ministry of Digital Development, Communications and Mass Media	• overseeing the media, including the electronic media, and mass communications, information technology and telecommunications • overseeing compliance with the law protecting the confidentiality of personal data being processed • organising the work of the radio-frequency service

Taulukko 21: Venäjä – digitaalisen turvallisuuden muita toimijoita

Toimija	Ohjaus	Keskeiset tehtävät
Security Council of the Russian Federation (Совет безопасности Российской Федерации, СБРФ)	The President of the Russian Federation	• preparation of the annual report of the President of the Russian Federation to the Supreme Council on ensuring the security to protect the vital interests of individuals, society and the state from external and internal threats • organizing work of interdepartmental commissions for formulating draft decisions of the President of the Russian Federation • developing proposals to ensure the protection of the constitutional order, State sovereignty and territorial integrity of the Russian Federation
National computer incident response & coordination center (CERT.GOV.RU)		• responsible for governmental networks of Russian Federation • incident response assistance and consultation • incident response coordination • alerts and warnings about critical security threats • gathering and analysis data concerning incidents in state information-telecommunication networks
RU-CERT		• computer incident prevention and response service for all users when the incident in question is related to resources located on the territory of Russian Federation • provide assistance in contacting russian incident response teams, abuse services, and law enforcement agencies
Federal Communications Agency	Ministry of Digital Development, Communications and Mass Media	• executive authority responsible for managing state property and providing state services in the sphere of telecommunications and postal communications • creation, development and use of telecommunications networks, communications satellite networks and television and radio broadcasting networks
Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters (EMERCOM)		• elaboration and fulfillment of the state policy in the field of civil defence, protection of the population and territories against emergencies, provision of fire safety and safety of people on water bodies • organization of preparation and approval of drafts of regulative and legal acts in the field of civil defence protection of the population and territories against emergencies, provision of fire safety and safety of people on water bodies • management of the field of civil defence, protection of the population and territories against emergencies, provision of fire safety and safety of people on water bodies, management of activity of federal executive authorities within the framework of the Single State Disaster Management System • legal regulation to prevent, forecast and mitigate the consequences of emergencies and fires, introduction of special, permissive, supervisory and control functions in matters related to the competence of the Emergencies Ministry of Russia

	• organization of activities and carrying out of efforts in the matters related to the civil defence, emergency response to emergencies, protection of the population and territories against emergency situations and fires, provision of safety of people on water bodies, carrying out emergency humanitarian response operations, including operations abroad

VIRO

Taulukko 22: Viro – digitaalisen turvallisuuden keskitetyt toimijat

Toimija	Ohjaus	Keskeiset tehtävät
Security Committee of the Government of the Republic	hallitus	• analyses and assesses the national security situation • coordinates the activities of the authorities of executive power in planning, developing and organising national defence • chaired by the Prime Minister • secretary of the commission is the director of national security and defence coordination
Cyber Security Council	Security Committee	• contribute to smooth cooperation between various institutions • ensure the implementation of the objectives of Estonia's Cyber Security Strategy • chaired by the secretary general of the Ministry of Economic Affairs and Communications
The Information System Authority (RIA)	Ministry of Economic Affairs and Communications	• coordinate the development and administration of information systems ensuring the interoperability of the state's information system • organize activities related to information security • handle security incidents in Estonian computer networks • developing cyber security strategies and policies • coordinate the safe implementation of IT infrastructures important for the state supervision • monitor the Estonian computer network and solve cyber incidents
Estonian Data Protection Inspectoriate (AKI)	Ministry of Justice	• data protection and privacy (GDPR)
State Infocommunication Foundation (RIKS)	Ministry of Economic Affairs and Communications	• provides communication-related services for public institutions and other state-budgeted institutions • provides operative, radio and maritime communications, and telephone services • offers the service of hosting equipment in contemporary server spaces • offers space for radio mast equipment

Toimija	Ohjaus	Keskeiset tehtävät
Estonian Computer Emergency Response Team (CERT-EE)	RIA	• monitoring of the state of information security in Estonia by using received reports and collecting information about information security incidents • preventing security incidents and reducing security risks, mainly by raising awareness and through communication work • assisting institutions regarding security incidents and advising them if they want law enforcement agencies to start an incident investigation
Critical Information Infrastructure Protection (CIIP)	RIA	• maintain a trouble-free functioning of the country's essential information and communication systems • development of security measures • development of instructions and sample materials • raising cyber security awareness
Estonian Foreign Intelligence Service (Välisluuramet)	Ministry of Defence	• collect, analyse and report information on Estonia's external security threats • responsible for the security of the state's classified networks • carry out counterintelligence for the protection of Estonian diplomats and military personnel posted abroad • National Security Authority
e-governance academy (eGA)	non-profit foundation	• assists public sector and civil society organisations in making digital transformation happen • e-government and digital transformation policy planning and implementation • analyse information, create knowledge about e-governance and digital transformation, and transfer Estonian and international best practices to governments and other stakeholders around the world

Taulukko 23: Viro – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
Estonian Defence League's Cyber Unit	kyberpuolustus	• development of cooperation among qualified volunteer IT specialists • raising the level of cyber security for critical information infrastructure through the dissemination of knowledge and training • creation of a network which facilitates public private partnership and enhances preparedness in operating during a crisis situation • education and training in information security • participation in international cyber security training events
Cooperative Cyber Defence Centre of Excellence (CCDCOE)	NATO	• support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defence research, training and exercises

SUOMI

Taulukko 24: Suomi – Toimijat, joilla on yleisiä digitaalisen turvallisuuden vastuita

Toimija	Ohjaus	Keskeiset tehtävät
Valtioneuvoston kanslia		• VNTIKE • valtionhallinnon varautumisen koordinointi • ministeriöiden ohjeistus
Ulkoministeriö		• NSA
Sisäministeriö		• sisäinen turvallisuus
Puolustusministeriö		• kyberpuolustus
Valtiovarainministeriö		• julkisen hallinnon tiedonhallinnan, palvelujen ja palvelutuotannon varautumisen, valmiuden ja turvallisuuden yleinen ohjaus • DVV:n ja Valtorin tehtävät ja tulosohjaus
Liikenne- ja viestintäministeriö		• Traficomin ohjaus
Työ- ja elinkeinoministeriö		• HVK:n ohjaus
Liikenne- ja viestintävirasto (Traficom)	liikenne- ja viestintäministeriö	• liikenteen ja viestinnän lupa-, rekisteröinti- ja hyväksyntä- sekä turvallisuusviranomainen • autoilijan palvelut • liikennejärjestelmäpalvelut • digitaaliset yhteydet • Kyberturvallisuuskeskus
Kyberturvallisuuskeskus (KTK)	Traficom	• CERT-FI • tietojärjestelmien arvioinnit ja hyväksynnät • salaustuotteiden arvioinnit ja hyväksynnät • kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta • tuottaa kyberturvallisuuden tilannekuvaa
Tiedonhallintalautakunta	valtiovarainministeriö	• edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista • valvoa valtion virastojen ja laitosten sekä kuntien ja kuntayhtymien tiedonhallintalain noudattamista arvioimalla
Digi- ja väestötietovirasto (DVV)	valtiovarainministeriö	• edistää yhteiskunnan digitalisaatiota • turvaa tietojen saatavuutta • tarjoaa palveluja asiakkaiden elämäntapahtumiin • VAHTI-toiminta
Tietosuojavaltuutetun toimisto (TSV)	oikeusministeriö	• kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista
Valtion tieto- ja viestintätekniikkakeskus (Valtori)	valtiovarainministeriö	• tuottaa valtionhallinnon toimialariippumattomat ict-palvelut

		• tuottaa korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja ja integraatiopalveluja
Suomen Erillisverkot Oy	sisäministeriö	• valtion kokonaan omistama erityistehtäväyhtiö • turvaverkon operaattori; turvallisuuden kannalta tärkeiden viranomaisten ja valtion ylimmän johdon viestintä • Krivat-palvelu • VIRVE-palvelut • turvapilvi ja konesali

Taulukko 25: Suomi – digitaalisen turvallisuuden muita toimijoita

Toimija	Ohjaus	Keskeiset tehtävät
Huoltovarmuuskeskus (HVK)	työ- ja elinkeinoministeriö	• sopimuksellisten varautumisjärjestelyjen tekeminen yritysten kanssa • tilannetietoisuuden ylläpito ml. toimintaympäristön analyysi, skenaario- ja ennakointityö • kriittisten teknisten järjestelmien toimivuuden varmistaminen • keskushallintotason poikkihallinnollinen valmiusyhteistyö • harjoitukset, koulutus, tiedotus ja ohjeistaminen
Kansaneläkelaitos (Kela)	eduskunta	• suomalaisten sosiaaliturva eri elämäntilanteissa • etuushakemusten käsittely ja ratkaisu • koordinoi ja tukee Kanta-palvelujen käyttöönottoja sekä huolehtii palvelun käytön aikaisesta asiakasyhteistyöstä • vastaa Kanta-palvelujen ylläpidosta ja teknisestä kehittämisestä, tietojärjestelmiin liittyvästä taustatuesta ja tukipalveluista, kansallisen koodistopalvelun teknisestä rakentamisesta ja yhteistestauksen koordinoinnista
Suojelupoliisi (Supo)	sisäministeriö	• hankkii, analysoi ja raportoi tiedustelutietoa päätöksenteon tueksi • torjuu terrorismia • estää vakoilua • seuraa ja arvioi kotimaisten ääriliikkeiden muodostamaa uhkaa • tekee turvallisuusselvityksiä kansallisen turvallisuuden tai erittäin tärkeän yksityisen edun kannalta merkittäviin tehtäviin valittavista ihmisistä
Keskusrikospoliisi (KRP)	sisäministeriö	• tutkii vakavaa, järjestäytynyttä ja ammattimaista rikollisuutta • kehittää rikostorjuntaa, eli esitutkintaa ja rikostiedustelua, sekä rikostutkintamenetelmiä • rikostekninen laboratorio • Poliisin kyberrikostorjuntakeskus • rahanpesun selvittelykeskus sekä PTR- rikostiedustelu- ja analyysikeskus
Hansel		• julkishallinnon yhteisankintayksikkö

Suomen Kuntaliitto		• tietoturvavastaavien verkosto • tietosuojavastaavien verkosto
kuntien omistamat ICT-palveluyhtiöt		• (mm. 2M IT, Istekki, LapIT) • omistajien ICT-palvelut (ICT-hankinnat, tietoturva, järjestelmänhallinta, …)
Digiturvan strateginen johtoryhmä	valtiovarainministeriö	•

Taulukko 26: Suomi – kansallisia yhteistoimintafoorumeita

Foorumi	Teema	Keskeiset tavoitteet
VAHTI	digitaalinen turvallisuus	• edistää julkisen hallinnon digitaalista turvallisuutta • koordinoi palvelutuotannosta vastaavien organisaatioiden yhteistyötä • käsittelee tiedonhallintalautakunnan antamia suosituksia • julkisen hallinnon toiminnan ja ICT-palveluiden turvaaminen • uuden teknologian turvallisen käyttöönoton mahdollistaminen • kansalaisten ja sidosryhmien luottamuksen säilyttäminen julkiseen hallintoon • yhteistyön kehittäminen kansallisesti ja kansainvälisesti myös elinkeinoelämän kanssa
Kuntaliiton tietoturvavastaavat	tietoturva	• tiedonvaihto • verkostoituminen
Kuntaliiton tietosuojavastaavat	tietosuoja	• tiedonvaihto • verkostoituminen
Turvallisuuskomitea	kokonaisturvallisuus	• avustaa valtioneuvostoa ja ministeriöitä laajoissa kokonaisturvallisuuteen liittyvissä asioissa

			• seuraa Suomen turvallisuusympäristön ja yhteiskunnan kehitystä sekä yhteensovittaa kokonaisturvallisuuteen liittyvää ennakoivaa varautumista
VIRT	digitaalinen turvallisuus		• viranomaisten yhteistyö häiriötilanteessa
ISAC-ryhmät	digitaalinen turvallisuus		• eri toimijoiden yhteistyö häiriötilanteissa ja niihin varautumisessa