



Digitaalisen turvallisuuden kansainvälinen vertailu

Valtiovarainministeriö

Helmikuu 2020

Julkinen

[KPMG Oy Ab](#)

Sisällys

Digitaalisen turvallisuuden kansainvälinen vertailu	1
Kansainvälisen vertailun yhteenveto	1
Kansainvälisen vertailun analyysi	3
Digitaalinen yhteiskunta ja digitaalisen turvallisuuden käsite	3
Lainsäädäntö	3
Johtaminen ja yhteistoiminta	4
Kansainvälinen toiminta	5
Talous ja teknologia	5
Kansalainen, henkilöstö ja osaaminen	6
Strategiset linjaukset ja toimintaympäristön uhka-arviot	7
Verrokkivaltioiden analysointi	9
Vertailussa käytetyt indeksit	9
Maakohtaiset analyysit	9
Alankomaat	10
Australia	12
Iso-Britannia	14
Israel	16
Ruotsi	18
Saksa	20
Venäjä	22
Viro	24
Suomi	25
Liite 1 - Maakohtaiset aineistot	1
Liite 2 – Lähteitä	49

Digitaalisen turvallisuuden kansainvälinen vertailu

Digitaalisen turvallisuuden kansainvälisessä vertailussa on koottu yhteen tietoa digitaalisen turvallisuuden ohjauksesta, tehtävistä, rakenteista, riskeistä ja resursseista valituissa maissa.

Digitaalinen turvallisuus kattaa tässä asiayhteydessä riskienhallinnan, jatkuvuudenhallinnan ja varautumisen, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan. Verrokkivaltioiksi valittiin Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Vertailun vuoksi myös Suomesta laadittiin vastaavanlainen yhteenveto.

Vertailutieto kerättiin verrokkivaltioiden julkisista dokumenteista perustuen kysymyksiin, jotka laadittiin yhdessä valtiovarainministeriön kanssa. Kysymykset käsittelivät lainsäädäntöä, strategisia linjauksia, toiminnan organisointia ja resursseja. Vertailussa hyödynnettiin kansainvälisiä vertailuja ja indeksejä, joissa on arvioitu verrokkimaiden kyberturvallisuutta ja muutosvalmiutta. Valtiovarainministeriö pyysi lisäksi kunkin verrokkivaltion Suomen edustustolta kommentteja maan yhteenvedosta. Raportissa on huomioitu edustustoilta saatu palaute.

Kansainvälisen vertailun yhteenveto

Digitaalisen turvallisuuden terminologia on verrokkivaltioissa kirjavaa. Käsitteet ”digitaalinen turvallisuus (digiturva)”, ”kyberturvallisuus” ja ”tietoturvallisuus” eivät ole täysin vakiintuneita Suomessakaan ja käsitteiden väliset erot vaikuttavat osin keinotekoisilta. Lainsäädäntö on vaihtelevaa, mutta EU-valtioiden tietosuoja-asetus (GDPR) ja tietoverkkodirektiivi (NIS) yhtenäistävät käytäntöjä. Uusi kyberturvallisuusasetus vahvistaa EU:n yhteisen viranomaisen (ENISA) kyberturvallisuuden koordinoijan ja neuvonantajan roolia ja määrittelee prosessien, palvelujen ja tuotteiden sertifiointijärjestelmän. Israel on määritellyt kyberturvallisuuden asiantuntijatehtävät, jotka edellyttävät henkilökohtaista sertifiointia ja Isossa-Britanniassa kyberturvallisuuden Cyber Essentials -sertifikaatin voivat yritysten ja ammattilaisten lisäksi hankkia myös yksityishenkilöt. Suomen Tietoturvamerkki on esimerkki mallista, jolla sertifiointia voitaisiin toteuttaa.

Digitaalista infrastruktuuria ei verrokkivaltioissa käsitellä erillisenä kokonaisuutena. Sen sijaan digitaalisen infrastruktuurin ajatellaan sisältyvän fyysisen maailman rakenteisiin, toimintoihin, palveluihin ja tuotteisiin ja sen turvaaminen olevan vastaavasti osa yleistä varautumista ja jatkuvuuden hallintaa. Energiahuolto ja tietoliikenteen toimivuus nähdään digitalisoituvan yhteiskunnan keskeisinä edellytyksinä.

Kyberturvallisuuden ohjauksessa suuntaus näyttää olevan kohti keskitettyjä malleja, jossa yhden ministeriön alaisuuteen on sijoitettu toimivaltainen viranomainen, joka ohjaa ja koordinoi mutta myös ohjeistaa ja kouluttaa sekä valvoo ja reagoi. Vahvasti hajautetussa mallissa toimijoiden välinen kommunikointi ja toimivaltakysymykset voivat muodostua haasteellisiksi.

Verrokkivaltioiden kyberturvallisuusstrategioiden uhka-arvioissa tunnistetaan strategiseksi riskiksi vieraiden valtioiden tai näiden tukemien ryhmittymien vihamielinen vaikuttaminen lähes poikkeuksetta. Kyberhyökkäyksiä pidetään merkittävänä uhkina mm. siksi, että niiden katsotaan voivan horjuttaa yhteiskunnan vakautta esimerkiksi hybridivaikuttamisen tai valeuutisten kautta. Hyökkäyksiin tarvittavaa teknologiaa on lisäksi helposti saatavilla ja hyökkääjän kiinnijäämisen riski on pieni. Digitaalisen toimintaympäristön turvallisuuden parantamiseksi tarvitaan konkreettisia, yhteiskunnan eri alueet kattavia toimenpiteitä, joiden toteutumista seurataan säännöllisesti esimerkiksi Ison-Britannian tavoin kyberturvallisuusstrategian avulla.

Verrokkimaissa kansallisen kyberturvallisuuden aktiivisina toimijoina tunnistetaan yleisesti julkishallinto, elinkeinoelämä, korkeakoulut ja tutkimuslaitokset sekä kansalaiset. Kaikkien toimijoiden yhteistyö tuottaa kattavamman digitaalisen turvallisuuden tilannekuvan. Uusien digitaalisten tuotteiden ja palveluiden kehittyminen kasvattaa koko kybertoimialaa ja tarjoaa uusia vientimahdollisuuksia. Israel ja Alankomaat ovat esimerkkejä valtioista, joissa toimialaa ja tutkimusta kehittämällä tavoitellaan kansantaloudellista hyötyä. Suomessa kansalaisten roolia ja vastuita aktiivisina yhteiskunnan turvallisuuden tekijöinä ei ole selkeästi määritetty, toisin kuin verrokkivaltioissa, joissa koko yhteiskunnan kattava kybertaitojen ja kyberosaamisen kehittäminen tehtävineen, tavoitteineen ja mittareineen on strateginen painopiste ja pää-tavoite.

Nopeasti kehittyvän digitaalisen toimintaympäristön muutokset edellyttävät nopeaa ja kansainvälisesti tehokasta havainnointi- ja reagoitokykyä. Kybertoimintaympäristö ja siihen kohdistuvat uhat, kuten kybervakoilu, -terrorismi tai muun kyberrikollisuus, eivät noudata valtioiden rajoja, joten uudenlainen erityisosaaminen, tiedonvaihto ja turvallisuusviranomaisten yhteistyö on välttämätöntä niin kansallisesti kuin kansainvälisestikin.

Johtopäätökset

Digitaalinen yhteiskunta ja digitaalisen turvallisuuden käsite	— Digitaalisen infrastruktuurin tulee olla osa palvelurakenteita ja digitaalisen turvallisuuden osa palvelukokonaisuutta. Palveluntarjoajan tulee vastata digitaalisen turvallisuuden vaatimuksiin ja taata turvallinen palvelun käyttö. — Suomen tulee systemaattisesti edellyttää digitaalisen turvallisuuden standardien ja kriteeristöjen noudattamista sekä varmistaa kansallisten kriteerien kansainvälinen yhteensopivuus. Kansallisia digitaalisen turvallisuuden vaatimuksia tulee käyttää täydentämään kansainvälisiä standardeja, ei korvaamaan niitä.
Lainsäädäntö	— Verrokkivaltioiden digitaalisen turvallisuuden osa-alueita koskeva lainsäädäntö ei ole kovin yhtenäinen. Kyberturvallisuuden merkitys on kuitenkin tunnistettu laajasti ja monissa maissa (mm. Ruotsi, Alankomaat, Saksa, Viro) ja lainsäädäntöä on pyritty kehittämään vastaamaan digitaalisen toimintaympäristön nopeita muutoksia. Saksassa viranomaisjärjestelmien ja verkkojen tietoturva on nostettu perustuslain tasolle. — Digitaaliseen turvallisuuteen liittyvän lainsäädännön on oltava kansainvälistä, mikä edellyttää Suomen aktiivista osallistumista EU:n säädösvalmisteluun. Suomen tulee seurata yhteiskunnan sääntelyn tarvetta ja reagoida nopeasti muutostarpeisiin esimerkiksi keinoälyn ja data-analytiikan käytön osalta. Lisäksi Suomen tulee ottaa käyttöön oppivien järjestelmien eettiset periaatteet sekä käytön valvonnan ohjeistus.
Johtaminen ja yhteistoiminta sekä kansainvälinen toiminta	— Verrokkivaltiot ovat siirtymässä kohti keskitettyä johtamista, jossa virastoja yhdistetään suuremmiksi kokonaisuuksiksi. Verrokkimaissa kansallisen kyberturvallisuuden aktiivisina toimijoina tunnistetaan yleisesti julkishallinto, elinkeinoelämä, korkeakoulut ja tutkimuslaitokset sekä kansalaiset. Esimerkiksi Ruotsissa on käynnissä kyberturvallisuuden hallinnan keskittäminen uudelle viranomaiselle. — Kansainvälinen yhteistoiminta edellyttää selkeitä vastuualueita ja rooleja. johtamisrakenteita kansainvälisen mukaisesti. Koordinointi- ja toteutusvastuut voidaan erottaa toisistaan, mutta vastuualueet tulee määrittää selkeästi toimivan kansallisen ja kansainvälisen yhteistyön takaamiseksi. Suomen tulee arvioida kriittisesti digiturvallisuuden nykyisiä johtamisrakenteita, vastuita ja rooleja sekä uudistaa niitä kansainvälisen kehityksen mukaisesti. Toimivaltakysymykset eivät saa olla digitaalisen turvallisuuden kehitystyön esteenä. — Suomen tulee lisätä yhteistoimintaa edellä mainittujen kyberturvallisuuden aktiivisten toimijoiden välillä myös muualla kuin elintärkeiden toimintojen turvaamisessa.
Talous ja teknologia	— Verrokkivaltioiden digiturvallisuuteen kohdistettujen investointien arvioiminen on kerätyn tiedon pohjalta mahdotonta. Verrokkivaltioiden osalta havaittiin kuitenkin tarve investointien tuottavuuden mittaamiseen.

	— Suomen tulee varmistaa, että digiturvallisuuden kehityshankkeiden tavoitteet hyödyttävät yhteiskuntaa ja ne ovat mitattavissa. Mittaustuloksia ja riskianalyysseja tulee soveltaa tulevien investointiohjelmien suunnittelussa. — Yhteiskunnan palveluissa käytettävälle teknologialle on asetettava digitaalisen turvallisuuden minimivaatimukset ja niiden toteutumista on valvottava.
Kansalainen, henkilöstö ja osaaminen	— Digitaalisen turvallisuuden osaamisen kehittäminen on mukana lähes kaikkien verrokkivaltioiden kyberturvallisuusstrategioissa. — Kaikilla yhteiskunnan osilla – hallinnolla, kansalaisilla ja yhteisöillä – tulee olla aktiivinen rooli kyberturvallisuuden toimijoina ja digi-turvallisuustaitojen kehittäminen tulee olla strateginen painopiste koko yhteiskunnan laajuisesti. — Digiturvataitojen takaamiseksi tulee valmistella henkilösertifiointi-menettely (vrt. Iso-Britannia, Australia, Israel) osaamisen todentamiseksi. Turvallisuuden kannalta kriittisimmille tehtäville on määriteltävä digiturvaosaamisen vähimmäisvaatimukset.
Strategiset linjaukset ja toimintaympäristön uhka-arviot	— Verrokkivaltioiden uhka-analyysit ovat pääsääntöisesti samankaltaisia keskenään, mutta kokonaisuus ei ole erityisen selkeä yhdelläkään tarkastellulla valtiolla. — Tiivistä yhteistyötä viranomaisten ja elinkeinoelämän välillä korostetaan lähes kaikkien verrokkivaltioiden strategioissa. — Suomen tulee kuvata digitaaliseen turvallisuuteen liittyvät uhat selkeästi kaikkien yhteiskunnan osien ymmärtämään muotoon. Uhkien vaikutusten pienentämiseen liittyvät strategiset linjaukset tulee avata toimeenpanosuunnitelmassa konkreettisiksi operatiivisiksi tehtäviksi. — Hallinnolle, kansalaisille ja yhteisöille on tarjottava tunnistettuihin digiturvallisuuden häiriötilanteisiin apua. Iso-Britannia on esimerkiksi perustanut kyberyksikön kaikkiin paikallisiin poliisiosastoihin.

Kansainvälisen vertailun analyysi



Digitaalinen yhteiskunta ja digitaalisen turvallisuuden käsite

Käsitteet ”digitaalinen turvallisuus (digiturva)”, ”kyberturvallisuus” ja ”tietoturvallisuus” eivät ole täysin vakiintuneita. Suomessakin ”digitaalinen turvallisuus” ja ”kyberturvallisuus” mielletään usein synonyymeiksi (vrt. kyberturvallisuusstrategia, Kyberturvallisuuskeskus), eikä kyberturvallisuuden ja tietoturval-lisuudenkaan määritelmät ole yksikäsitteisiä. Esimerkiksi Saksassa kyberturvallisuus kattaa kaikki tieto- ja viestintätekniikkaa koskevan tietoturvan näkökulmat. Käsitteiden erot vaikuttavat näin ollen osittain keinoitekoisilta. Ruotsin lisäksi digitaalisen turvallisuuden käsitettä ei juuri käytetä muissa verrokkivalti-oissa. Digitaalisen toimintaympäristön (digital domain) turvaamiseen tunnistetaan kyllä erilaisia näkökul-mia, mutta kokonaisuudesta puhuttaessa käytetään yleisimmin sateenvarjotermiä kyberturvallisuus. Verrokkimaiden kyberturvallisuuden määritelmät eivät ole täysin samanlaisia, mutta eivät kuitenkaan poikkea toisistaan merkittävästi.

Digitaalista infrastruktuuria ei ole yleensä määriteltä, eikä sitä verrokkivaltioiden varautumissuunni-telmissa käsitellä erillisenä kokonaisuutena. Sen sijaan digitaalisen infrastruktuurin ajatellaan sisältyvän fyysisen maailman rakenteisiin, toimintoihin, palveluihin ja tuotteisiin ja sen turvaaminen on vastaavasti osa yleistä varautumista ja toiminnan jatkuvuuden hallintaa. Kyberturvallisuus kattaa tyypillisesti digitaalisten palvelujen, tietojärjestelmien, laitteistojen ja tietoverkkojen toiminnan turvaamisen, uhkien arvi-oinnin ja häiriöistä toipumisen, joten sen voidaan ajatella olevan digitaalisen toimintaympäristön suojaa-mista.



Lainsäädäntö

Verrokkivaltioiden digitaalisen turvallisuuden osa-alueita koskeva lainsäädäntö ei yleisesti ottaen ole ko-vin yhtenäinen. Kyberrikollisuuteen, kriittisen infrastruktuurin suojaamiseen ja tietoliikenteen toimivuuteen otetaan kantaa, mutta lainsäädännön heikkouksia tai vahvuuksia on mahdotonta arvioida

syventymättä tarkemmin verrokkimaiden lainsäädäntöön ja oikeudenkäyttöön. Näin ollen verrokkivaltioiden säädösten ja normien heikkouksia tai vahvuuksia ei analysoitu. Voi kuitenkin todeta, että kyberturvallisuuden merkitys on tunnistettu laajasti ja mm. Ruotsissa, Alankomaissa, Saksassa ja Virossa lainsäädäntöä on pyritty kehittämään vastaamaan digitaalisen toimintaympäristön nopeita muutoksia.

Digitaalisen turvallisuuden lainsäädäntö on kirjavaa, mutta EU-valtioiden tietosuoja-asetus (General Data Protection Regulation, GDPR) ja tietoverkkodirektiivi (The Directive on Security of Network and Information Systems, NIS) yhtenäistävät käytäntöjä. Kesäkuussa 2019 voimaan tullut kyberturvallisuusasetus ([Cybersecurity Act](#)) täydentää NIS-direktiiviä. Asetuksessa EU:n yhteisen viranomaisen (ENISA) kyberturvallisuuden koordinoijan ja neuvonantajan roolia vahvistetaan ja lisäksi määritellään prosessien, palvelujen ja tuotteiden sertifiointijärjestelmä. Suomen Tietoturvamerkki on esimerkki mallista, jolla sertifiointia voitaisiin toteuttaa.

Suomessa digitaalista turvallisuutta koskeva lainsäädäntö on hajautettu, vaikka uusi tiedonhallintalaki kokoakin asioita yhteen. Verrokkivaltioissa erityisesti digitaaliseen toimintaympäristöön liittyvää lainsäädäntöä on laadittu mm. Ruotsissa (Brottsdatalog), Alankomaissa (Cybersecuritywet) ja Saksassa (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). Sekä Australiassa että Israelissa on oma tietosuojalainsäädäntönsä ja Venäjän tietosuojalainsäädäntöön sisältyy vaatimus tietojen säilyttämisestä venäläisillä palvelimilla. Suoranaisesti riskienhallintaa koskevaa lainsäädäntöä ei verrokkivaltioista löydy, mutta monien verrokkivaltioiden viranomaiset julkaisevat riskienhallintaa koskevaa ohjeistusta.



Johtaminen ja yhteistoiminta

Suomen digitaalisen turvallisuuden kehittäminen, koordinointi ja johtaminen on hajautettu ja hallinnossa toimijoita on paljon (mm. Kyberturvallisuuskeskus, Traficom, valtiovarainministeriö, Digi- ja väestötietovirasto, Huoltovarmuusk keskus ja valtioneuvoston tilannekeskus). Useimmissa verrokkivaltioissa kyberturvallisuutta ohjataan sen sijaan keskitetymin. Alankomaissa, Australiassa, Isossa-Britanniassa ja Saksassa kyberturvallisuuden ohjaus on keskitetty yhden ministeriön alaisuudessa toimivan turvallisuusviranomaisen yhteyteen. Alankomaiden NCSC-NL on oikeusministeriön alaisen turvallisuuden ja terrorismin torjunnan viraston (NCTV) osa, Isossa-Britanniassa päävastuussa on ulkoministeriön alaisen tiedusteluorganisaation, GCHQ:n alainen National Cyber Security Center (NCSC) ja Australian ACSC on sijoitettu puolustusministeriön alaiseen tiedusteluorganisaatioon (Australian Signals Directorate). Saksassa kyberturvallisuuden päävastuullinen on sisäasiainministeriön alainen Bundesamt für Sicherheit in der Informationstechnik.

Viime vuosina kyberturvallisuuden ohjauksa on edelleen keskitetty muissakin verrokkivaltioissa. Israelissa Cyber National Bureau ja National Cyber Security Authority yhdistettiin vuonna 2018 kansalliseksi kyberdirektoraatiksi ja Ruotsin MSB on saanut tehtäväksi yhdessä muiden turvallisuusviranomaisten kanssa uuden kyberturvallisuusviranomaisen perustamisen vuoden 2020 kuluessa. Koska ohjauksen keskittäminen näyttää olevan vallitseva trendi, voidaan olettaa tällaisen mallin antavan paremmat valmiudet digitaalisen turvallisuuden tehokkaaseen ohjaamiseen, parempaan havainnointikykyyn ja nopeampaan reagointiin nopeasti muuttuvassa digitaalisessa toimintaympäristössä. Hajautetussa mallissa digitaalisen turvallisuuden kehittämisen ja kehittymisen kokonaiskuvan muodostaminen on haastavaa.

EU-valtioissa tietosuoja hoitaa GDPR:n mukaisesti erillinen viranomainen. Sekä Israelissa että Australiassa on vastaavan kaltainen tietosuojaviranomainen. Resursoinnissa on merkittäviä eroja valtioiden välillä. Suomessa tietosuojavaltuutetun toimistossa on vakituisesti kolme henkilöä, Virossa yhdeksäntoista, Ruotsissa 75 ja Saksan liittovaltion virastossa 190. Verrokkivaltioista mm. Saksassa, Isossa-Britanniassa ja Ruotsissa tietosuojasta vastaava viranomainen tarjoaa myös ohjeita, neuvontaa ja koulutusta hallinnolle, yrityksille ja kansalaisille.

Verrokkivaltioissa on toimivaltaisten viranomaisten lisäksi erilaisia elinkeinoelämän ja tutkimusyhteisöjen tiedonvaihto- ja yhteistyöfoorumeita, joissa kyberturvallisuutta käsitellään ja kehitetään. Esimerkeinä yhteistyöfoorumeista ovat Alankomaiden ([Digital Trust Center](#) (DTC)), Australian [Joint Cyber Security Centre](#) (JCSC), Ison-Britannian [Cyber Security Information Sharing Partnership](#) (CiSP), Israelin [CyberSpark Initiative](#), Ruotsin [Näringslivet's Säkerhetsdelegation](#) (NSD) ja Saksan [Allianz für Cyber-Sicherheit](#).

Verrokkimaissa kansallisen kyberturvallisuuden aktiivisina toimijoina tunnustetaan yleisesti julkishallinto, elinkeinoelämä, oppilaitokset (erityisesti yliopistot ja korkeakoulut) ja kansalaiset. Suomessa julkisen ja yksityisen sektorin yhteistyöllä on pitkät perinteet – erityisesti huoltovarmuuskriittisten toimijoiden varautumisessa. Kansalaisia ei kuitenkaan ole Suomessa tunnustettu kansallisen kyberturvallisuuden

aktiivisiksi toimijoiksi toisin kuin verrokkivaltioissa, joissa myös yksityisten kansalaisten rooli ja tehtävät digitaalisen toimintaympäristön turvaamisessa on määritelty. Uudessa kyberturvallisuusstrategian osaamisen kehittämisen kohdassakin sivutaan kansalaisten roolia varsin pintapuolisesti: ”Julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta lisätään uusien palveluiden ja tuotteiden tietoturvasta” ([Kyberturvallisuusstrategia 2019](#)).

Tutkimus- ja koulutuslaitosten yhteistyö julkishallinnon ja elinkeinoelämän kanssa vaikuttaa pistemäiseltä, eikä digitaalisen turvallisuuden tutkimusta koordinoita toisin kuin esimerkiksi Israelissa tai Virossa. Suomessa kyberturvallisuuden koulutusohjelmia on muutamissa oppilaitoksissa (mm. Laurea AMK) ja Metropolia AMK). Kuitenkin vain Jyväskylän yliopistossa on erityinen kyberturvallisuuden maisteriohjelma. Verrokkivaltioista esimerkiksi Alankomaissa ja Isossa-Britanniassa on useita erilaisia maisteriohjelmia monissa yliopistoissa.

Jatkuvuudenhallinta ja varautuminen tarkoittaa verrokkivaltioissa yleensä fyysisen maailman kriisivalmiutta ja resilienssiä. Vaikka kyberturvallisuuden rooli osana kriittisen infrastruktuurin suojaamista on tunnistettu, se ei korostu kriisivalmiudesta vastaavien viranomaisten toimintamalleissa. Kriittisen infrastruktuurin suojaamista koordinoi erityisviranomainen: Australiassa CIC ja Isossa-Britanniassa CPNI. Toiminta on sisällytetty osaksi muun turvallisuusviranomaisen tehtäviä Alankomaissa (NCTV) ja Ruotsissa (MSB). Varautumisviranomaisten tehtävät poikkeavat toisistaan eri maissa jonkin verran, mutta tyypillisesti suojattavia kohteita ovat mm. valtionhallinto, energia-, ruoka- ja vesihuolto, kuljetuslogistiikka ja finanssiala (mm. vakuutustoiminta ja maksuliikenne). Kyberturvallisuuselementti on mukana kriittisen infrastruktuurin ICT-järjestelmien (esimerkiksi teollisuuden SCADA-järjestelmät, tai IoT-laitteet) kautta. Tavoitteiden ja hallintamallien erojen takia varautumisviranomaisten vertailu ei ole kovin tarkoituksenmukaista. Suomen Huoltovarmuuskeskukseen verrattuna voidaan kuitenkin todeta esimerkiksi Ruotsin MSB:n vuosibudjetti on yli 120 miljoonaa euroa ja virasto työllistää yli 1200 henkilöä.



Kansainvälinen toiminta

Kaikissa verrokkivaltioissa on tunnistettu digitaalisen toimintaympäristön haasteeksi se, ettei toiminta noudata valtioiden rajoja. Esimerkiksi pilvipalvelujen yleistymisen myötä on vaikea määritellä täsmällisesti, missä tietojärjestelmien tiedot sijaitsevat. Toisaalta myöskään kyberrikollisuus ei rajoitu yksittäisiin valtioihin vaan kohteena voivat olla yritykset, hallitukset tai yksityiset henkilöt globaalisti. Näin ollen kansainvälisen yhteistyön merkitystä korostetaan niin verrokkivaltioiden kuin Suomenkin strategioissa.

EU-valtioissa kansainvälinen yhteistyö on yhdenmukaisten käytäntöjen laatimista EU-lainsäädännön pohjalta (esimerkiksi NIS-direktiivi ja kyberturvallisuusasetus). Kuitenkin mm. Alankomaat, Ruotsi ja Israel hakevat kansainvälisen yhteistyön kautta kansantaloudellista etua: omien intressien kansainvälinen edistäminen ja uusien digitaalisten tuotteiden ja palveluiden tuotanto kehittää valtioiden omaa kyberturvallisuustoimialaa, tarjoaa uusia vientimahdollisuuksia ja parantaa kilpailukykyä. Toisaalta digitaalisen toimintaympäristön nopeasti muuttuvien haasteiden, kybervakoilun- tai -terrorismin tai muun kyberrikollisuuden torjunta edellyttävät nopeaa vastetta ja valtioilta tehokasta havainnointi- ja reagointikykyä, jonka saavuttamiseksi uudenlainen erityisosaaminen, tiedonvaihto ja turvallisuusviranomaisten yhteistyö on välttämätöntä myös kansainvälisesti.

Kansainvälien yhteistyön lisäksi useimmat verrokkivaltiot panostavat kyberpuolustukseen ja esimerkiksi Iso-Britannia, Israel, Venäjä ja Australia kehittävät kybertoimintaympäristöön myös hyökkäyksellistä kykyä. Kyberpuolustus on kansallisen turvallisuuden osa, joka on tyypillisesti puolustusvoimien vastuulla. Valtiot eivät julkaise kyberpuolustuksestaan yksityiskohtaisia tietoja. Suomen näkökulmasta digitaalisen turvallisuuden kehittämisessä ja kansainvälisessä toiminnassa on huomioitava eri valtioiden edellyttämät turvaluokitustasot esimerkiksi tiedustelu- ja turvallisuuspalveluiden välisessä tiedonvaihossa.



Talous ja teknologia

Verrokkivaltioiden digiturvallisuuteen liittyviä taloudellisen seurannan mittareita ei ole tunnistettu. Valtiot ovat laatineet budjetteja, mutta digitaalisen turvallisuuden investointien tuottamien hyötyjen mittaamiseen ei ole työkaluja. Selvityksessä käytetyssä tausta-aineistossa löytyy Alankomaiden turvaklusterin (The Hague Centre for Strategic Studies) tuottama vertailu, jossa kyberturvallisuuden investointien kustannukset on suhteutettu kansantuotteeseen. Vertailussa Alankomaat jää mm. USA:n, Ison-Britannian ja Australiasta, mutta vertailu ei kuitenkaan mittaa investointien tehokkuutta tai saavutettuja yhteiskunnallisia hyötyjä. Esimerkiksi Ison-Britannian, Alankomaiden ja Saksan kyberturvallisuusstrategioiden seurantaraporteissa arvioidaan, kuinka hyvin asetetut tavoitteet on saavutettu, mutta vaikutuksia

kyberturvallisuuden kypsyystasoon ei ole arvioitu. Australiassa kehitetyn kypsyysarviointimallin (Essential Eight Maturity model) kaltaista mittaristoa soveltamalla voitaisiin käyttää kyberturvainvestointien hyötyjen ja vaikutusten mittaamiseen.

Tutkimuksen ja kehityksen osalta valtiot, jotka ovat määrätietoisesti kehittäneet tieto- ja kyberturvallisuusosaamista, ovat onnistuneet kasvattamaan yksityisen sektorin toimijoiden kokoa ja lukumäärää. Esimerkiksi Israelin kyberturvallisuussektorin aloittavien yritysten rahoituksen [vuotuinen kasvu](#) on viiden vuoden ajan ollut yli 20 %. Israelissa toimi vuonna 2017 421 aktiivista kyberturvallisuusyritystä, kyberturvallisuustoimialan yritysten liikevaihto oli noin kolme miljardia dollaria ja kyberturvateknologian viennin arvioitiin olevan yli 5,5 miljardia dollaria ([lähde](#)). Lisäksi Be'er Shevaan on muodostettu kyberturvallisuusklusteri, johon kuuluu kansallisia ja kansainvälisiä yrityksiä, yliopistoja ja julkishallinnon organisaatioita.

Digiturvallisuuden menetelmien ja työkalujen kehittämisen lähtökohtana on tavallisesti yksityisen sektorin liiketoimintatavoitteet. Verrokkimailla, joilla on ennestään vahvaa kyberturvallisuusosaamista (mm. Australia, Iso-Britannia, Israel, Alankomaat) pitävät toimialan kehittämistä strategisesti tärkeänä alueena. Esimerkiksi Ison-Britannian NCSC:n järjestämässä Industry 100 -ohjelmassa yritysten työntekijät työskentelevät lyhyen määräajan NCSC:ssä, kehittämällä yhteistä turvallisuusosaamista ja luovat uusia asiantuntijaverkostoja.

Kyberturvallisuusasetus (EU 2019/881) määrittelee [ENISA](#) (Euroopan unionin kyberturvallisuusvirasto) tehtävät. Uutena kohtana asetus määrittelee eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän, jonka mukaisesti sertifioitujen ICT-tuotteiden ja palveluiden kyberturvallisuuden tasosta pyritään varmistumaan. Suomessa lanseerattu [Tietoturvamerkki](#) on esimerkki mallista, jossa sertifiointilla voi osoittaa tuotteen tai palvelun kyberturvallisuuden tason.

Viro on varmistanut valtion digitaalisten palvelujen jatkuvuuden Luxemburgin kanssa solmitulla [Data Embassy](#) -sopimuksella. Järjestelyssä Viro on hankkinut korkean turvatason palvelinkeskuskapasiteettia varmistusten säilyttämiseksi ja kriittisimpien digitaalisten palvelujen tuottamiseksi. Data Embassy varmistaa Viron hallinnon toiminnan tilanteessa, jossa valtion oman alueen käyttö ei ole mahdollista.

Venäjä investoi voimakkaasti kybertoimintakyvyn kehittämiseen, mutta sen tavoitteena on ensisijaisesti valtion etujen takaaminen. Keskeisenä tavoitteena on varmistaa valtiolle tärkeiden asioiden tuominen esiin globaaleissa informaatioverkostoissa. Kansallisten etujen turvaamiseksi Venäjällä on käynnissä ns. Runet-hanke, joka tähtää Internetin saarekekäyttöön ja tiedon kontrollointiin. Hanke ja siihen liittyvä lainsäädäntö edellyttävät tietoliikenneoperaattoreilta kykyä sulkea Venäjä tarvittaessa Internetin ulkopuolelle ja varmistaa kansallisen verkon toimivuus Internetistä irrotettuna. Venäjällä Internet-palveluja veloitetaan keräämään käyttäjien henkilötiedot venäläisille palvelimille, jotta valtio voi varmistaa käyttäjätietojen valvonnan tarvittaessa.



Kansalainen, henkilöstö ja osaaminen

Suurimmilla organisaatioilla on usein käytössään eniten resursseja digitaalisen turvallisuuden osa-alueiden kehittämiseksi. Pienet yritykset ja yksityishenkilöt voivat näin ollen joutua helpommin kyberrikollisuuden uhreiksi esimerkiksi henkilökohtaisten laitteiden haittaohjelmien, verkkoon liitettyjen turvattomien laitteiden tietomurtojen tai tietovarkauksien kautta. Yksityishenkilöihin kohdistuva kyberrikollisuus vähentää kansalaisten luottamusta digitaalisiin palveluihin ja tarjoaa rikollisille laajan hyökkäyspinnan niin julkisia kuin yksityisiäkin digitaalisten palvelujen tuottajia vastaan esimerkiksi palvelunestohyökkäyksiin valjastettuina verkostoina. Nopeasti muuttuvat ja kehittyvät digitaaliset tuotteet ja palvelut tuottavat mahdollisuuksia ja hyötyjä mutta myös uusia haavoittuvuuksia ja uhkia, joita voidaan käyttää rikollisiin tarkoituksiin.

Tietoisuuden ja osaamisen kehittäminen on verrokkivaltioissa tunnistettu digitaalisen toimintaympäristön turvaamisen tärkeäksi osatekijäksi. Osaamisen kehittämistä voidaan tarkastella sekä pitkän että lyhyen aikavälin tavoitteina. Pitkällä aikavälillä yksityishenkilöiden digitaalisen turvallisuuden osa-alueiden (yleisemmin tosin puhutaan kyberturvallisuustaidoista) kehittäminen alkaa jo kouluiässä, jossa tavoitteena on antaa kaikille perusvalmiudet toimia turvallisesti digitaalisessa toimintaympäristössä ja samalla herättää kiinnostusta kyberturvallisuusasioiden jatko-opintoihin. Verrokkivaltioista pisimmällä tässä asiassa on Israel, jossa kyberturvallisuuskoulutus alkaa jo kouluiässä ja myös varusmiespalvelus sisältää kyberturvallisuuteen liittyvää koulutusta. Isossa-Britanniassa on nykyisen kyberturvallisuusstrategian toimeenpanokaudella (2016-2021) ollut käynnissä CyberFirst ja Cyber Discovery -ohjelmat, joista ensin mainittu tarjoaa kyberturvallisuuteen liittyviä kursseja 11-17 -vuotiaille ja jälkimmäinen on verkossa

toteutettu 13-18 -vuotiaille suunnattu ohjelma, jonka kautta houkutellaan nuoria kyberturvallisuusosalalle. Ruotsin, Alankomaiden ja Viron digitalisaatiostrategioihin on kirjattu tavoitteeksi digitaalisen taitojen (mm. medialukutaito ja kyberturvallisuus) lisääminen ensimmäisen ja toisen asteen opetusohjelmiin, valmistamaan koululaisten ja opiskelijoiden osallistumista digitaalisessa yhteiskunnassa ja työelämässä toimimiseen.

Kaikissa verrokkivaltioissa on pulaa kyberturvallisuuden osaajista, vaikka yliopistoissa olisikin useita kyberturvallisuuteen liittyviä maisteriohjelmia (kuten esim. [Iso-Britannia](#), [Alankomaat](#) ja [Israel](#)). Parhaista osaajista kilpaillaan maailmanlaajuisesti ja osaajista kilpailevat niin julkinen kuin yksityinenkin sektori. EU-maiden yliopistojen yhteistyönä EIT Digital Master School järjestää [kyberturvallisuuden maisteriohjelman](#) asiantuntijoiden määrän kasvattamiseksi.

Verrokkivaltioiden strategiaan tavoitteisiin kuuluu poikkeuksetta kybertaitojen ja -osaamisen kehittäminen, mutta painotuksissa ja toteutuksissa on vaihtelua: Venäjän ja Israelin linjauksissa korostuu valtion turvallisuusintresseistä huolehtiminen, kun taas esimerkiksi Alankomaissa, Ruotsissa ja Isossa-Britanniassa myös yksityisten ihmisten turvallinen toiminta digitaalisessa toimintaympäristössä nähdään tärkeänä. Harjoittelu on strategian tasolla kytketty osaamisen ylläpitoon mm. Ruotsissa ja Isossa-Britanniassa; Australiassa korostetaan kansainvälistä yhteistyötä tietoisuuden lisäämisessä. Kyberturvallisuusosaamisen kehittäminen on mukana Suomenkin kyberturvallisuusstrategiassa vuodelta 2019, joskaan siinä tavoitteet eivät ole yhtä yksityiskohtaisia kuin esimerkiksi Ison-Britannian tai Australian strategioissa, eikä konkreettisia toimenpiteitä tai edistymisen mittareita ole määritetty. Ison-Britannian kyberturvallisuusstrategian tavoitteena on määritellä kaikkien yhteiskunnan osien – hallinnon, yksityishenkilöiden ja organisaatioiden – roolit kyberturvallisuuden toimijoina.

Digitaalisen turvallisuuden kulttuurin juurruttaminen yhteiskuntaan on pitkäkestoinen hanke. Alankomaiden [digitalisaatiostrategian](#) mukaan yli 55-vuotiaista kansalaista joka viidennellä on vain vähän kokemusta tietotekniikasta. Kybertaitojen osaamista edistetään koko yhteiskunnan laajuisesti: Australian [eSmart Libraries](#) tukee julkisten kirjastojen kyberturvallisuustyötä ja Saksassa BSI käyttää sosiaalista mediaa kyberturvallisuustietouden jakamiseen. Verrokkivaltioista ainakin Australiassa, Isossa-Britanniassa ja Israelissa on käytössä sertifiointijärjestelmä, joiden avulla voidaan osoittaa pätevyys kyberturvallisuusasioissa. Saksassa BSI selvittää kyberturvallisuuden kansallista tilaa toteuttamalla vuosittain laajan kyberturvallisuutta koskevan kyselytutkimuksen. Selvityksen tuloksia voi käyttää vertailukohteena, kun yritykset ja organisaatiot arvioivat oman kyberturvallisuutensa kypsyystasoa.

Australiassa on elinkeinoelämän tuella toteutettu kaksi kansallista sertifikaattia: [Certificate IV in Cyber Security](#) ja [Advanced Diploma of Cyber Security](#), joiden avulla tavoitellaan lisää kyberturvallisuusosaajia ja kyberosaamisen kehittymistä. Ison-Britannian NCSC:llä on laaja sertifiointiohjelma, joka kattaa myös yliopistojen koulutusohjelmia. Cyber Essentials -toimintamalli sisältää niin yksityishenkilöiden kuin yritystenkin kyberturvallisuussertifiointin, jota valtionhallinnon toimijat voivat edellyttää mm. julkisiin kilpailutuksiin osallistumisen ehtona. Israelissa edellytetään valtiolle kyberturvallisuustyötä tekevilta henkilöiltä kyberturvallisuusammattilaisten sertifikaattia, jolla osoitetaan ammatillinen pätevyys, eettisten periaatteiden noudattaminen ja luotettavuus. Sertifiointin piiriin kuuluu viisi toimintoa: kyberpuolustus, tunkeutumistestaus, tietoturvaloukkausten tutkinta (ns. forensikka), kyberturvallisuuden metodologiat ja kyberturvallisuusteknologiat. Isossa-Britanniassa kyberturvallisuuden sertifikaatin (Cyber Essentials) voivat yritysten ja ammattilaisten lisäksi hankkia myös yksityishenkilöt.



Strategiset linjaukset ja toimintaympäristön uhka-arviot

Kaikilla verrokkivaltioilla on julkisia, digitaaliseen turvallisuuteen liittyviä strategisia linjausasiakirjoja ja kaikkien tavoitteena on olla tavalla tai toisella kyberturvallisuuden edelläkävijä. Kyberturvallisuusstrategioissa määritellään erilaisia toimenpiteitä, joilla turvataan digitaalisen toimintaympäristön toimintaa. Tällaisia toimenpiteitä ovat esimerkiksi kansalaisten osaamisen kehittäminen, kansainvälinen yhteistyö kyberrikollisuuden torjumiseksi tai tietojärjestelmien ja -verkkojen teknisen tietoturvallisuuden parantaminen. Ruotsissa ja Alankomaissa on laadittu lisäksi digitalisaatiostrategiat, joissa kuvataan yhteiskunnan digitalisaatiolle asetettuja tavoitteita ja korostetaan kyberturvallisuuden integroimista kaikkeen yhteiskunnan toimintaan. Julkiselle hallinnolle on lisäksi tuotettu omat digitalisaatiostrategiat mm. Ruotsissa, Australiassa ja Alankomaissa. Julkishallinnon digitalisaation edistämistä koordinoi erillinen viranomainen ainakin Ruotsissa ([DIGG](#)) ja Isossa-Britanniassa ([Government Digital Services](#), GDS).

Verrokkivaltioiden kyberturvallisuusstrategiat poikkeavat toisistaan toimeenpanosuunnitelmien yksityiskohtaisuudessa. Ison-Britannian ja Australian strategioissa on määritetty kyberturvallisuuden kehittämiseksi yksityiskohtaisia tavoitteita, konkreettisia toimenpiteitä, joilla tavoitteisiin pyritään ja mittareita, joiden avulla seurataan tavoitteiden vuosittaista toteutumista. Ruotsin kyberturvallisuusstrategiassa

kuvataan tavoitteita yleisemmin, eikä strategiaan ole kirjattu konkreettista toimenpidesuunnitelmaa, tehtäviä, tai mittareita.

Muutamilla verrokkimailla kansallisen turvallisuuden strategioista on saatavilla julkinen versio. Ne käsittelevät laajemmin yleistä turvallisuutta ja kyberturvallisuutta arvioidaan uhkien, kuten esimerkiksi kybervakoilun ja kyberrikollisuuden näkökulmista. Viron kansallisen turvallisuuden strategia linjaa vain yleisesti kyberpuolustuskyvyn kehittämisen ja koordinoinnin osana valtion kokonaispuolustusta.

Verrokkivaltioiden kyberturvallisuusstrategiat sisältävät yleensä vähintään yleisen katsauksen digitaalisen (tai kyber-) toimintaympäristön uhkiin. Varsinaista kansallista riskiarviota tai vaikutusanalyysii ei strategioissa yleensä ole, koska valtion strategisen tason riskiarviot sisältävät yksityiskohtaisia tietoja valtioiden heikkouksista. Muutamat verrokkivaltiot (mm. Iso-Britannia ja Alankomaat) julkaisevat kansallisista riskiarvioistaan Suomen [kansallisen riskiarvion](#) (Sisäministeriön julkaisu 2019:5) kaltaisia yhteen-vetoja.

Verrokkivaltioiden kyberturvallisuusstrategioiden uhka-arvioissa tunnistetaan strategiseksi riskiksi vieraiden valtioiden tai näiden tukemien ryhmittymien vihamielinen vaikuttaminen lähes poikkeuksetta. Joissain uhka-arvioissa on jopa mainittu nimeltä valtiot, joiden katsotaan muodostavan suurimman kyberuhan ao. valtion turvallisuudelle (esimerkkeinä Venäjä, Kiina, Pohjois-Korea ja Iran). Kyberhyökkäystä pidetään merkittävinä uhkina mm. siksi, että niiden arvioidaan voivan horjuttaa yhteiskunnan vakautta esimerkiksi hybridivaikuttamisen tai valeuutisten kautta. Lisäksi hyökkäyksiin tarvittavaa teknologiaa on helposti saatavilla ja hyökkääjän kiinnijäämisen riski on pieni.

Suomen kansallisessa riskiarviossa strategisissa riskeissä tunnistetaan kyberhyökkäysten tai kybervai-kuttamisen merkitys mm. rahoitusjärjestelmälle, tietoliikenteelle tai logistiikan järjestelmille, mutta vieraiden valtioiden vihamielistä kybertoimintaa ei ole kirjoitettu riskiarvioon auki, eikä kyberturvallisuus-strategiassa valtiollisten toimijoiden tai näiden tukemien ryhmien edustamia kyberuhkia ole selkeästi kirjattu.

Digitaalista infrastruktuuria ei ole yleensä määritelty erikseen, mutta tietoliikenteen toimivuus ja energiahuolto nähdään digitalisoituvan yhteiskunnan keskeisinä edellytyksinä. Digitaalisen toimintaympäristön jatkuvuuden hallintaa toteutetaan yleensä osana yhteiskunnan ja elinkeinoelämän muuta varautumista. Varautumisesta tai toiminnan jatkuvuudesta julkaistaan yleiskuvauksia, mutta yksityiskohtien katsotaan kuuluvan kansallisen turvallisuuden piiriin. Kyberturvallisuusstrategioissa kybertoimintaympäristö saatetaan tunnistaa ensisijaiseksi vihamielisen vaikuttamisen kohteeksi. Usein sitä kuitenkin ajatellaan kanavana, jota kautta yhteiskunnan toimintaa voidaan horjuttaa hyökkäämällä kriittistä infrastruktuuria (esimerkiksi vesi-, ruoka- tai energiahuoltoa) vastaan tai pyrkimällä haittaamaan valtion päätöksentekoa hybridivaikuttamisen kautta. Suomessa valtioneuvoston päätöksessä [huoltovarmuuden tavoitteista](#) (1048/2018) mainitaan kyberturvallisuusuuhkiin varautuminen erityisesti kriittisen infrastruktuurin kohdalla. Digitaalisen yhteiskunnan kyberturvallisuuden kehittäminen ja sen huomioiminen varautumisessa tunnistetaan, mutta konkreettisia tavoitteita tai toimenpiteitä ei määritellä, eikä Suomen kyberturvallisuusstrategiakaan ota näihin kantaa.

Suomessa ei valtiontalouden tarkastusviraston (VTV) [tarkastuskertomuksen](#) 20/2018 mukaan ole koko valtiota koskevaa riskien- ja jatkuvuudenhallintaa. Vaikka virastoilla on käytettävissä ohjeistusta, ei ohjeita osata välttämättä soveltaa. VTV toteaa, että muiden valtioiden hyviä käytäntöjä voitaisiin soveltaa Suomeen. Verrokkivaltioilla ei ole yhteistä tai jaettua riskienhallintamallia, mutta useimmat valtiot julkaisevat riskienhallinnan ohjeita, jotka soveltuvat niin julkiselle kuin yksityisellekin sektorille. Ohjeistuksissa on sovellettu yleensä kansainvälistä riskienhallinnan standardia ISO/IEC 31000, joka esimerkiksi korvasi Australiassa aiemmin käytössä olleen kansallisen riskienhallintastandardin. Ruotsissa MSB julkaisee riskienhallintaa koskevaa ohjeistusta, mutta siitä huolimatta riskienhallinnan käsitteistö ei ole yhdenmukainen ja riskille on olemassa lukuisia erilaisia määritelmiä.

Tiivistä yhteistyötä viranomaisten ja elinkeinoelämän välillä korostetaan lähes kaikkien verrokkivaltioiden strategioissa. Osaamisen ja innovaatioiden kehittämiseksi yhteistyö tutkimus- ja koulutusorganisaatioiden kanssa nähdään tärkeäksi. Myös kansainvälisen yhteistyön merkitystä korostetaan, koska yleisesti tiedostetaan, etteivät kybertoimintaympäristö ja sitä kohtaavat uhkat noudata valtioiden rajoja. Tällöin yksittäisen valtion mahdollisuudet kyberrikollisuuden torjunnassa ovat rajoitetut. Jokainen valtio kehittää kuitenkin kyberturvallisuuden tilannetietoisuuttaan sekä kyberuhkien (esimerkiksi informaatiovaikuttaminen ja haittaohjelmat) tunnistamista, ehkäisemistä ja torjumista, mikä on esimerkiksi Saksassa eräs strategisista painopisteistä.

Verrokkivaltioiden analysointi

Vertailussa käytetyt indeksit

Jokaiselle maalle on laskettu vertausluku kolmesta indeksistä:

- ITUn Global Cybersecurity Index 2018 ([GCI](#))
- Viron National Cyber Security Index 2018 ([NCSI](#))
- KPMG:n Change Readiness Index 2019 ([CRI](#))

Verrokkimaiden sijoitus kussakin indeksissä on suhteutettu indeksissä mukana olevien valtioiden lukumäärään. Näin saatu indeksiluku voidaan tulkita prosenttiosuutena niistä maista, joiden sijoitus ao. indeksissä on heikompi kuin vertailtavan maan sijoitus. Indeksissä ensimmäisenä olevan maan indeksiluku on siten yksi (100 %) ja viimeisen nolla (0 %). Kunkin maan indeksiluvuista on laskettu keskiarvo, ja indeksilukujen keskiarvot on esitetty vertailussa pylväsdiagrammina. Indeksilukujen erot eivät ole kovin suuria, mikä kertoo siitä, että käytetyn tausta-aineiston perusteella digitaalisen turvallisuuden tilanne on verrokkivaltioissa melko hyvä.

Indeksilukujen taulukkoon on otettu mukaan myös valtion sijoitus EU:n The Digital Economy and Society Index 2018 ([DESI](#)), mutta sitä ei ole otettu mukaan indeksilukujen keskiarvoon kahdesta syystä: ensiksikään Australia, Israel ja Venäjä eivät ole mukana tässä indeksissä ja toiseksi DESI:ssä on selvästi vähemmän valtioita kuin muissa indekseissä, joten jo yhden sijan ero kahden valtion välillä tuottaa indeksilukuun muista indeksejä huomattavasti suuremman poikkeaman.

Indeksilukujen keskiarvojen perusteella kyberturvallisuuden kärkijoukkoon kuuluvat Iso-Britannia, Viro ja Alankomaat. Suomi, Saksa ja Australia muodostavat keskikastin, joskaan ryhmien väliset erot eivät ole kovin suuria. Sen sijaan Ruotsi, Israel ja Venäjä jäävät vertailussa selvemmin jälkeen muista verrokkivaltioista. Vaikka laskettu vertailuluku ei suoraan kerro valtion kyberturvallisuuden tasosta, näyttää kuitenkin siltä, että tiedon vapaampi jakaminen parantaa valtion sijoitusta eri vertailuindekseissä. Ruotsi on kuitenkin poikkeus tässä suhteessa, koska sen sijoitus on tiedon jakamisen avoimuudesta huolimatta alhainen, mitä voi pitää odottamattomana tuloksena.

Maakohtaiset analyysit

Alankomaat

Alankomaiden kyberturvallisuusstrategia ([CSA](#)) määrittelee termin **kyberturvallisuus** kaikkien niiden toimenpiteiden muodostamaksi kokonaisuudeksi, jolla 1) estetään ICT-häiriöiden, -vikojen tai käyttövirheiden aiheuttamat vahingot, 2) jonka avulla vaikutuksia vähennetään ja 3) jonka avulla häiriöistä toivutaan ja vahingot korjataan. Digitaaliseen turvallisuuteen ei ole käytössä yhtenäistä määritelmää, CSA:ssa digitaalinen turvallisuus käytetään kyberturvallisuuden synonyyminä, mutta toisissa yhteyksissä sillä tarkoitetaan digitaalisten prosessien ja järjestelmien luottamuksellisuutta, eheyttä ja saatavuutta, mikä on lähempänä suomalaista tietoturvan määritelmää.

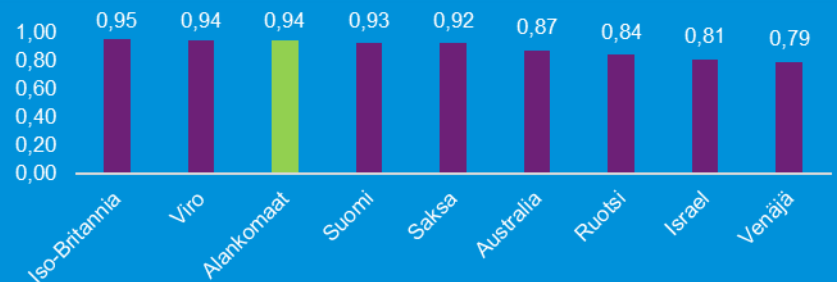
Alankomaiden kyberturvallisuuden ohjaus on keskitetty oikeusministeriön hallinnonalalle. Käytännön tehtävät on osoitettu kansalliselle turvallisuuden virastolle (National Coordinator for Security and Counterterrorism, [NCTV](#)) ja sen osana toimivalle kansalliselle kyberturvallisuusvirastolle (National Cyber Security Centre, [NCSC](#)). Puolustusvoimilla on vastuu kyberpuolustuksen järjestämisestä. Alankomailla on muiden EU-maiden tapaan oma tietosuojavirasto (Autoriteit Persoonsgegevens, [AP](#)). Näiden lisäksi on erilaisia yhteistyöfoorumia kuten esimerkiksi Cyber Security Council ([CSR](#)) ja Digital Trust Centre ([DTC](#)).

Alankomaiden NSCS julkaisee vuosittain kansallinen kyberturvallisuuden tilannekuvaraportin (Cyber Security Assessment Netherlands, [CSAN 2019](#)). Raportti käsittelee kyberturvallisuuden uhka-arviota, -painopistealueita ja häiriönsietokykyä. Lisäksi siinä arvioidaan näiden kyberturvallisuuden näkökulmien vaikutusta kansalliseen turvallisuuteen. Uhka-arvioissa vakavimmaksi tekijäksi on nostettu valtiotoimijoiden Alankomaihin kohdistama vihamielinen toiminta, kuten esimerkiksi kybervakoilu, sabotaasi ja tietojen manipulointi. Raportti mainitsee esimerkkeinä Venäjän, Kiinan

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	3	12	9	10
Indeksiluku	0,93	0,94	0,94	0,94

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + selkeät strategiset linjaukset digiturvallisuuden kehittämiseksi (National Cyber Security Agenda 2019)
- + laaja-alainen yhteistyö digiturvallisuuden toimijoiden välillä erityisesti tutkimuksen ja kehityksen alueella
- + keskitetty kyberturvallisuuden hallinta yhteen ministeriöön
- + Alankomaiden myöntämä AVG-sertifikaatti (GDPR-compliance)
- + useita kyberturvallisuuteen liittyviä koulutusohjelmia

Kehityskohteet

- digitaalisten tuotteiden ja palveluiden sekä hallinnon puutteellinen resilienssi
- digitaalisen resilienssin mittaaminen
- havainnointi- ja reagointikyvyn kehittäminen
- Alankomaiden hallinnon kyberturvallisuuden investoinnit

ja Iranin. Kybertoimintaympäristön häiriönsietokyvyn (resilienssin) ei koeta olevan kaikilta osin riittävä, eikä mittaamiseen tarvittavia menetelmiä ole. Lisäksi häiriönsietokyvyn tilannekuvaa pidetään puutteellisenä. Kolmantena merkittävänä uhkana nähdään Alankomaiden riippuvuus pienestä määrästä muiden maiden ohjelmisto-, laitteisto- ja palvelutoimittajista.

Alankomaiden yhteiskunta ja sen kriittiset prosessit on digitalisoitu erittäin kattavasti ja digitaalisen

toimintaympäristö on kompleksinen kokonaisuus. Tämä tuo mukanaan uusia haavoittuvuuksia, kun esimerkiksi kyberhyökkäyksissä käytettäviä työkaluja on helposti saatavilla, eikä vaihtoehtoisia toimintatapoja digitalisoitujen palvelujen häiriöiden varalle ole valmisteltu. Kun palvelutuotanto on erittäin verkostoitunutta ja toisaalta riippuvuus toimittajista on suuri, voi palveluverkostoon kohdistuva kyberhyökkäys aiheuttaa merkittäviä yhteiskunnallisia häiriöitä, joita

vastaan yksittäisten organisaatioiden voi olla vaikea suojautua.

Kyberturvallisuus on Alankomaissa kytkeyty digitalisaation viiteen painopistealueeseen (tutkimus ja innovaatiot, työn muutos ja jatkuva oppiminen, digitaalinen talous, kansalaisten ja organisaatioiden digitaalinen resilienssi, digiajan perusoikeudet eettiset periaatteet) yhdessä yksityisyyden suojan ja digitaalisten taitojen kanssa. Kyberturvallisuus turvaa keskeisten toimialojen (esim. ruoan ja energian tuotanto, avoin digitaalinen julkinen hallinto) häiriötöntä toimintaa, tukee kestävästä kasvua ja parantaa elämisen laatua (mm. digitaaliset terveyspalvelut).

Toisaalta kyberturvallisuus nähdään toimialana, jonka kehittäminen avaa työmarkkinoille uusia mahdollisuuksia, parantaa digitaalisen toimintaympäristön turvallisuutta ja tuottaa kansallisia kyberturvallisuusratkaisuja yhteiskunnan käyttöön parantaen digitaalista omavaraisuutta. Kybertoimialan kehittämisen arvioidaan lisäävän myönteistä kiinnostusta Alankomaita kohtaan laajemminkin.

Australia

Australian kyberturvallisuusstrategiassa ei määritellä termejä ”kyberturvallisuus” tai ”digitaalinen turvallisuus”. Parlamentin sivustolta löytyy yksinkertaistettu määritelmä, jonka mukaan kyberturvallisuus on Internetiin kytkettyjen tietojärjestelmien suojaamista, mikä on huomattavasti rajoittuneempi määritelmä kuin monessa muussa verrokkivaltiossa. Kyberturvallisuusstrategiassa kuitenkin käsitellään asiaa tätä määritelmää laajemmin.

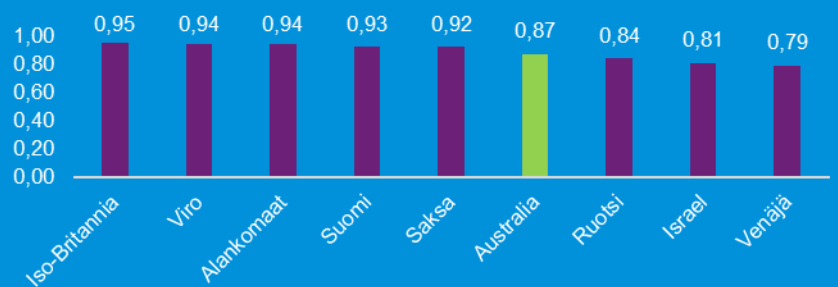
Australian puolustusministeriön hallinnonalaan kuuluva erillislaitos [Australian Signals Directorate](#) (ASD) vastaa mm. signaalitiedustelusta, aktiivisista kyberturvallisuuden vastatoimista (offensive cyber operations) datan ja järjestelmien analyysistä. ASD toimii lisäksi hallituksen neuvonantajana toimintaansa liittyvissä asioissa. ASD toimii tiiviissä yhteistyössä Australian puolustusvoimien kanssa. Vuonna 2014 perustettu kyberturvallisuuden keskus ([Australian Cyber Security Centre](#), ACSC) liitettiin vuonna 2018 ASD:n osaksi. Samalla myös Australian CERT-toiminto sisällytettiin ACSC:hen. Virasto tuottaa kyberturvallisuuden tilannekuvaa yhteistyössä julkishallinnon ja yritysten kanssa, kehittää yhteiskunnan kybertietoisuutta hallinnon, elinkeinoelämän ja kansalaisten yhteistyönä sekä tuottaa kyberturvallisuuteen liittyvää ohjeistusta koko julkishallinnon, yritysten ja kansalaisten tarpeisiin. Lisäksi ACSC valvoo ja seuraa maailmanlaajuisia kyberturvallisuustilannetta jatkuvasti.

Australia ei ole julkaissut kansallista riskiarviota, eikä esimerkiksi kyberturvallisuusstrategiassa ole riskejä käsittelevää osuutta. Kansallisessa turvallisuusstrategiassa ainoa digitaaliseen turvallisuuteen liittyvä strateginen riski on vihamielinen kybertoiminta, joka kattaa mm. identiteettivarkaudet, palvelunestohyökkäykset ja vakoilun. Kyberturvallisuusstrategia nostaa esiin järjestäytyneen rikollisuuden ja valtiolliset toimijat

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	n/a	10	33	14
Indeksiluku	-	0,95	0,76	0,91

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + riskiperusteinen kyberturvallisuuden arviointimalli, joka perustuu kansainväliseen ISO/IEC 31000 -standardikokonaisuuteen
- + Kypsyysmalli kyberturvallisuushäiriöiden hallintaan (Essential Eight Maturity Model)
- + kyberturvallisuusstrategiassa määritellään konkreettisia tavoitteita
- + strategiassa kuvattujen tavoitteiden toteutumisesta raportoidaan vuosittain

Kehityskohteet

- turvallisuusstrategioiden vaatimusten mukaisuuden toteutuminen

merkittävimpinä kyberturvallisuutta uhkaavina tekijöinä.

Kyberturvallisuusstrategiassa (2016) on määritetty viisi painopistealuetta: hallinnon ja yksityissektorin yhteistyö (national cyber partnership), vahva kyberpuolustus, kansainvälinen yhteistyö (global responsibility and influence), kasvu ja innovaatiot sekä kansallisen kyberturvallisuustietoisuuden, -osaamisen ja -kykyjen kehittäminen (cyber smart nation). Kuhunkin osa-alueeseen on kuvattu hallinnon

tavoitteet yleisesti. Esimerkiksi kasvun ja innovaatioiden kohdalla hallinnon tavoitteena on yhdessä elinkeinoelämän ja tutkimusyhteisön kanssa kohdentaa kyberturvallisuuden tutkimusta vastaamaan paremmin Australian kyberturvallisuushaasteisiin. Kyberpuolustuksen tavoitteina ovat mm. tukea pk-yritysten kyberturvallisuuden tason varmistumista, tukea julkishallinnon organisaatioita toimitusketjujen riskien hallinnassa ja vahvistaa Australian

kyberturvallisuusviraston (ACSC) kykyä reagoida kyberuhkiin ja -rikollisuuteen. Strategia sisältää myös toimeenpanosuunnitelman, jossa on määritelty painopistealueille tehtäviä konkreettisemmin, mutta kaikki tehtävät eivät ole yhtä yksityiskohtaisesti määriteltyjä kuin esimerkiksi Ison-Britannian vastaavassa strategiassa. Tehtäville on strategiassa määritelty toivotut tulokset, mutta ei toteutuskeinoja tai onnistumisen mittareita.

Uuden kyberturvallisuusstrategian (Australia's 2020 Cyber Security Strategy) valmistelua varten hallitus on syyskuussa 2019 julkaissut asiakirjan herättämään keskustelua strategisista tavoitteista. Asiakirjaa voivat kommentoida niin yritykset kuin yksityiset kansalaisetkin. Kehitettävänä alueina on tunnistettu julkishallinnon ja elinkeinoelämän kyberturvallisuus, digitaalisen kaupankäynnin turvaaminen, kyberrikollisuuden torjunta ja digitaalisen turvallisuuden tietoisuuden ja osaamisen kehittäminen koko yhteiskunnassa (cyber-aware community). Ukrainan sähkön kantaverkkoon kohdistunutta kyberhyökkäystä ja laajalle levinneitä kiristys- ja häirintäohjelmia (WannaCry, NotPetya) on käytetty esimerkkeinä uusista uhkista. Toisaalta EU:n NIS-direktiivi ja Ison-Britannian aktiivinen kyberpuolustus on nostettu esimerkeiksi kansainvälisen yhteistyön keinoista, joilla kansallista kyberturvallisuutta voidaan parantaa. Asiakirjan liitteenä on listattu edellisen strategiakauden saavutuksia, kuten esimerkiksi ACSC:n perustaminen, poliisin kyberturvallisuus-koulutuksen lisääminen ja valtion rahallinen tuki pienten yritysten kyberturvallisuuden arvioinnille (cyber security health check).

Australian kriittisen infrastruktuurin suojaamisen strategiassa digitaalista infrastruktuuria ei ole määritelty erikseen. Kriittiseen infrastruktuuriin luetaan fyysiset laitokset, toimitusketjut, tietoverkot ja ICT, joiden pitkäaikaiset häiriöt aiheuttavat vahinkoa Australian taloudelliselle hyvinvoinnille tai kansalliselle turvallisuudelle. Australian kriittisen infrastruktuurin

suojaamisen strategiassa linjataan kaksi päätavoitetta: 1) kriittisen infrastruktuurin omistajien ja käyttäjien toiminnan jatkuvuuteen vaikuttavien riskien tehokas hallinta ja 2) näiden toimijoiden toiminnan jatkuvuuden hallinnan parantaminen vastustuskykyä (resilienssiä) kehittämällä. Tavoitteiden saavuttamisen edellytyksinä ovat tiivis julkishallinnon ja liike-elämän välinen yhteistyö sekä kehittynyt ja kattava riskienhallinta. Yhteistyön perustana on tiedon jakamisen verkosto (The Trusted Information Sharing Network, TISN), jonka puitteissa kriittisen infrastruktuurin toimijat voivat vaihtaa luottamuksellisia tietoja resilienssin kehittämiseksi. TISN:ssä on sekä toimialoja leikkaavia asiantuntijaryhmiä että toimialakohtaisia (mm. energia, rahoitus ja kuljetukset) ryhmiä. Riskienhallintaa varten Australian hallitus on julkaissut riskienhallinnan viitekehyksen, joka noudattaa kansainvälistä riskienhallinnan standardia (ISO31000).

ACSC on julkaissut organisaatioiden käyttöön listan toimenpiteistä, joilla kyberturvallisuuden riskejä voidaan pienentää. Toteuttamalla mallin kahdeksan keskeisintä hallintakeinoa ([The Essential Eight](#)) saavutetaan perustaso, jolla monia yksinkertaisimpia kyberhyökkäyksiä tai -häiriöitä saadaan torjuttua. Mallissa on priorisoitu perustason jälkeen toteutettaviksi muitakin hallintakeinoja, joita soveltamalla kyberturvallisuuden riskejä voidaan edelleen pienentää. Malliin sisältyy lisäksi arviointikehikko (Essential Eight Maturity Model), jota organisaatiot voivat käyttää arvioidessaan omaa kyberturvallisuuden kypsyystasoaan.

Iso-Britannia

[Kansallisen kyberturvallisuusstrategian 2016-2021](#) mukaan **kyberturvallisuus** on tietojärjestelmien (laitteet, ohjelmistot ja infrastruktuuri), niiden sisältämien tietojen ja niiden tuottamien palveluiden suojaaminen luvattomalta käytöltä, vahingonteoilta tai väärinkäytöltä. Kyberturvallisuus kattaa lisäksi kansainvälisten toimijoiden tahallisesti tai tuottamuksellisesti aiheuttamat vahingot (esimerkiksi puutteellisten turvallisuuskäytäntöjen takia).

Ison-Britannian kyberturvallisuuden koordinointi on jossain määrin valtioneuvoston kansliaan verrattavissa olevan pääministerin toimiston (Cabinet Office) vastuulla, mutta operatiivisista tehtävistä vastaa GCHQ, jota ohjaa ulkoministeriö (Foreign Office). Kansallisen turvallisuusneuvosto ([National Security Council](#)) on neuvoa-antava elin, joka käsittelee kansalliseen turvallisuuteen liittyviä valtion tavoitteita ja koordinoi Ison-Britannian kokonaisturvallisuutta. Turvallisuuteen, puolustukseen ja ulkosuhteisiin liittyvien tiedustelutietojen analysoinnista vastaa [Joint Intelligence Committee](#). Turvallisuus- ja tiedusteluorganisaatioiden operatiivista toimintaa ja hallintoa arvioi parlamentaarinen [Intelligence and Security Committee](#).

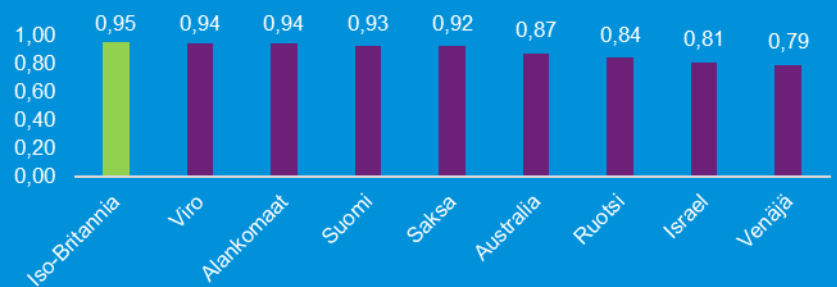
Kansallinen kyberturvallisuuskeskus ([NCSC](#)) on perustettu vuonna 2016, kun osa GCHQ:n toiminnoista, CERT-UK ja kansallisen infrastruktuurin suojaamisesta vastaava virasto ([Centre for Protection of National Infrastructure](#), CPNI) koottiin yhteen. NCSC:n päätehtäviä ovat kyberturvallisuuteen liittyvä ohjeistus ja koulutus, kyberuhkien torjunta, kybertoimintakyvyn ylläpito ja tietoverkkojen suojaaminen (sekä julkiset että yksityiset verkot). NCSC laatii kohdennettua ohjeistusta niin yksilöille ja perheille, pk-yrityksille, suuryrityksille, julkiselle sektorille ja kyberturvamammattilaisille.

Isossa-Britanniassa panostetaan erittäin laajasti koko yhteiskunnan kyberturvallisuuden tietoisuuden kehittämiseen ja koulutukseen.

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	5	1	14	8
Indeksiluku	0,86	1,00	0,90	0,95

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + laaja kansallinen sertifiointiohjelma (mm. Cyber Essentials, Certified security professionals)
- + kyberturvallisuusyksikkö kaikissa paikallisissa poliisiosastoissa
- + Iso-Britannia on aktiivinen kansainvälisessä yhteistyössä kyberrikollisuuden torjunnassa
- + resursointi
- + kyberturvallisuusstrategiassa konkreettisia tavoitteita, joiden edistymistä seurataan vuosittain
- + voimakas panostus kyberturvallisuuden koulutukseen ja tietoisuuden kasvattamiseen koko yhteiskunnassa

Kehityskohteet

- IoT-laitteiden turvallisuus yleisesti
- osaamisen kehittäminen (kansalainen, valtiohallinto)

NCSC koordinoi kyberturvallisuuden koulutusta. [CyberFirst](#)-ohjelmassa on 11-19-vuotiaille suunnattuja kursseja ja NCSC on sertifioinut useita eri yliopistojen kyberturvallisuuden [kandidaatti- ja maisteriohjelmia](#). [Industry 100](#) -ohjelmassa yritysten asiantuntijoita työskentelee NCSC:ssä lyhytaikaisen jakson. Ohjelman tarkoitus on kehittää NCSC:n omaa toimintaa tuomalla sinne uusia näkemyksiä. Toimialan hyötyinä on laajojen yhteistyöverkostojen syntyminen ja

tiedonvaihto muiden toimijoiden kanssa. Yhteistoiminnalla arvioidaan olevan sekä NCSC:ää että ohjelmaan liittyviä yrityksiä hyödyttäviä imagovaikutuksia.

NCSC:llä on kattava [sertifiointiohjelma](#), joka kattaa tuotteita (esim. salaustuotteet), palveluja (esim. konsultointi, tunkeutumistestaus) sekä osaamista ja taitoja (esim. kyberturvallisuuden maisteriohjelmat, asiantuntijoiden Cyber security professionals (CCP) -sertifikaatti). Lisäksi on laadittu [Cyber](#)

[Essentials](#) -ohjelma, joka tarjoaa välineet teknisen tietoturvan itsearviointiin, mutta myös kaksi eri tasoista sertifikaattia vaatimustenmukaisuuden todentamiseksi. Osassa valtionhallintoa Cyber Essentials -sertifikaatti on edellytyksenä esimerkiksi hankintakilpailutuksiin osallistumiselle.

National Risk Register vuodelta 2017 on salassa pidettävän kansallisen riskiarvion julkinen versio. Yhtenä sen osana ovat hyökkäykset yhteiskuntaa kohtaan ja kyberhyökkäykset on tunnistettu yhdeksi hyökkäyskanavaksi. Riskiarvion mukaan kybertoimintaympäristö ("cyberspace") on sekä talouden että yhteiskunnan oleellinen osa. Kyberhyökkäysten seurauksina on tunnistettu tiedon saatavuuden, luottamuksellisuuden tai eheyden menetys, palvelukatkot, taloudelliset vahingot tai mainehaitat. Äärimmäisessä tilanteessa seurauksena voi olla ihmishenkien menetys. Riskiraportissa suositellaan vastatoimiksi mm. havainnointikyvyn sekä osaamisen ja tietoisuuden kehittämistä.

Vuosille 2016-2021 laadittu kyberturvallisuusstrategiassa on kolme aluetta: kyberuhkilta suojautuminen ja niiden torjunta (Defend), hyökkäysten tunnistaminen, analysointi ja vastatoiminta (Deter) ja kybertoimialan kehittäminen ja tutkimus (Develop). Strategiassa merkittävimiksi uhkiksi on nostettu kyberrikollisuus ja valtioiden vihamielinen toiminta (kybervakoilu, kyberterrorismi ja muu vahinkojen tuottaminen). Vastaavasti merkittävimpiä haavoittuvuuksia ovat Internetiin liitettyjen turvattomien laitteiden määrän kasvu (erityisesti Internet of things, IoT), puutteellinen suojautuminen kyberuhkia vastaan, koulutuksen ja osaamisen puutteet ja se, että haittaohjelmien ja kyberhaittojen tuottamiseen tarvittavia resursseja on helposti saatavilla.

Strategiassa määritellään kullekin osa-alueelle tavoitela ja periaatteet näiden saavuttamiseksi (mm. kansalaisten yksityisyyden suojan turvaaminen, kyberhyökkäyksiin

vastaaminen ja koko yhteiskunnan osallistaminen). Strategian osana oleva toimeenpanosuunnitelma listaa kaikille kolmelle osa-alueelle strategisia tehtäviä (ks. esim. 5.2 "Building a more secure Internet", s. 35). Jokaisesta tehtävästä on kirjattu yleiskuvauksen lisäksi, täsmällisempi tavoite, konkreettiset keinot ja tehtävät tavoitteen saavuttamiseksi, sekä mittarit edistymisen seurantaan varten. Cabinet Officen vuosittain julkaisemassa seurantaraportissa kuvataan strategisten tavoitteiden toteutumista.

Strategiassa kuvataan yksityishenkilöiden, yritysten ja organisaatioiden sekä hallinnon roolit ja vastuut yhteiskunnan kyberturvallisuuden kehittämisessä ja ylläpitämisessä. Kansainvälisessä yhteistyössä on taustalla omien taloudellisten ja turvallisuusintressien vahvistaminen. Strategiassa sitoudutaan investoimaan viisivuotiskaudella 1,9 miljardia puntia kyberturvallisuuden kehittämiseen. Kahden uuden, kyberturvallisuustuotteiden ja -yritysten kehittämiseen keskittyvän innovaatiokeskuksen perustaminen on myös kirjattu strategiaan.

Israel

Israelissakaan ei käytetä käsitettä ”digitaalinen turvallisuus”. Yleensä termi kyberturvallisuus kattaa digitaalisen turvallisuuden osa-alueet. Israelin digitaalisen turvallisuuden osa-alueista saatiin koottua tietoja rajoitetusti. Virallisia, englanniksi käännettyjä dokumentteja oli käytettävissä vähän ja monet linkit kääntyivät suoraan pääministerin toimiston [pääsivulle](#).

Israelin strateginen ympäristö on riskialtis. Valtion on alusta alkaen panostanut sotilaalliseen toimintaan, terrorismin torjuntaan ja tiedustelutoimintaan, sekä puolustavaan että hyökkäyskykyyn.

Israeliin on myös syntynyt vahva globaali tietoturvaluusteknologian yritysklusteri, jonka liikevaihto 2017 oli kolmen miljardin dollarin luokkaa. Vertailun vuoksi Israelin kansantuote on yli 350 miljardia dollaria.

Israel panostaa kyberturvallisuuteen ja se on teknologisesti edellä niitä Lähi-Idän toimijoita, jotka se kokee uhakseen. Se on myös panostanut hyökkäyskykyyn. USA:n ja Israelin yhdessä toteuttamat tunnetut kyberhyökkäykset esim. Iranin uraanirikastamoja kohtaan ovat mitä ilmeisemmin olleet hyvin pitkälle Israelin ideoimia.

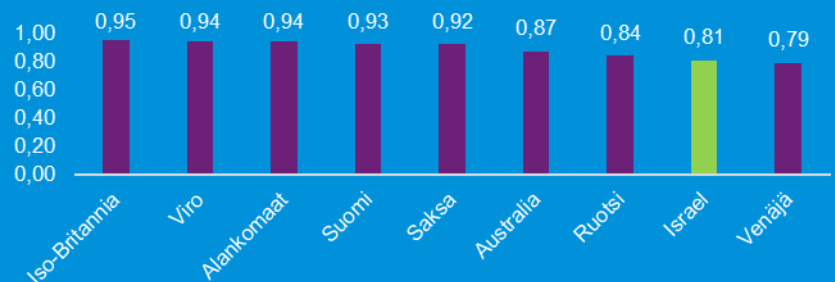
Valtionhallinnon ote maan tietoturvallisuuden kehittämiseen on tiukka. ”Kansallinen tietoturva-direktoraatti” on suoraan pääministerin alaisuudessa laajoilla valtuuksilla toimiva ylätason koordinoiva yksikkö. Parlamentilla on kyberpuolustuskomitea. Israelin kovaotteisen maineessa oleva salainen poliisi Israel Security Agency ja sen kyberosasto keskittyvät mm. vaikoilu- ja hyökkäysteknologioiden torjumiseen ja kehittämiseen. Oikeusministeriöllä on oma kyberrikollisuuteen keskittyvä jaostonsa. Puolustusministeriö vastaa osaltaan kyberturvallisuudesta sotilasoperaatioissa. Lisäksi on muuta sektorikohtaista kyberturvallisuustoimintaa.

Vuoden 2015 päätöksen mukaan valtionhallinnon yksiköiden on

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	n/a	39	25	25
Indeksiluku	-	0,78	0,82	0,83

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + kyberteollisuuden ekosysteemi (ks. TEAS)
- + kyberkriisinhallinnan kypsyyden arviointikehikko
- + kyberturvallisuusalan ammattilaisten sertifiointi (viisi ammattiryhmää, kaksi tasoa kustakin)

Kehityskohteet

- Kyberturvallisuuden osaamisen kehittäminen

siirtymääjan kuluessa täytettävä Israelin itselleen sovittaman ISO 27001 -standardin version vaatimukset. Valtionhallinnon sisäistä tietojärjestelmien turvallisuutta on näin hoidettu nojaamalla yleisempiin standardeihin, eikä ole keksitty pyörää uudelleen.

Jatkuvuuden hallintaa ja yleensä kyberkriisejä varten on olemassa kansallinen kyberkriisien hoidon konsepti. Siinä määritellään keskeiset käsitteet niin hallintoa kuin elinkeinoelämää varten ja se luo

pohjan yhteiselle valmiussuunnittelulle.

Tietosuoja on pääosin samalla tasolla kuin esim. EU:ssa, mutta myös sitä luonnehtii kriisitietoisuus. Toisin kuin tyypillisesti EU:ssa, useilla viranomaisilla on kuitenkin valtuudet esim. salakuunteluun, mikäli turvallisuus sitä vaatii. Israelin tietosuojalakeja ja niiden poikkeussäännöksiä pidetään myös vaikeaselkoisina.

Israelin kyberturvallisuusviranomaisilla on voimassa käytäntö, jolla

pyritään varmistamaan valtionhallinnon, tai sille palveluja tuottavien yritysten kyberturvallisuuden asiantuntijoiden ammatillinen osaaminen, eettiset periaatteet ja luotettavuus. Sertifiointimenettely kattaa viisi ammattiryhmää (kyberpuolustus, tunkeutumistestaus, tietoturvaloukkausten tutkinta (ns. forensiikka), kyberturvallisuuden metodologiat ja kyberturvallisuusteknologiat). Jokaisesta sertifikaatista on kaksi tasoa, mutta näiden tarkemmasta käytöstä ei löydy englanninkielistä lähdettä. Sertifikaatin saaminen edellyttää Israelin kansalaisuutta ja puhdasta rikosrekisteriä. ([lähde](#))

Ruotsi

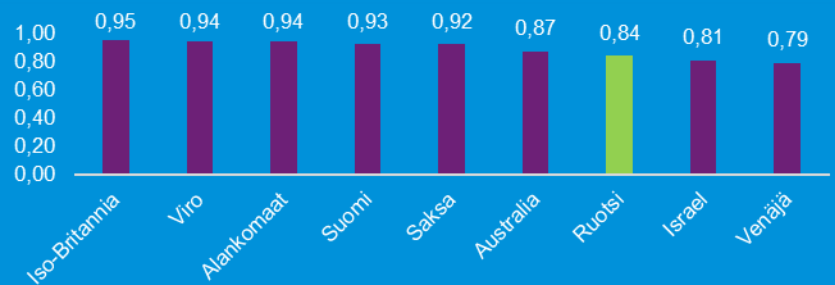
Digiturvallisuudelle ei ole yksikäsitteistä määritelmää, mutta se kattaa erilaisia yksityisen ja julkisen sektorin toimenpiteitä, joiden avulla taataan digitaalisten palveluiden luotettavuus, luodaan edellytykset sille, että palveluita halutaan käyttää ja varmistetaan digitaalisten järjestelmien turvallisuus. ([lähde](#))

Ruotsissa digitaalisen turvallisuuden vastuita on hajautettu laajasti valtion- ja aluehallintoon. Keskeisiä viranomaisia, joille on määrätty digitaaliseen turvallisuuteen liittyviä vastuita, ovat varautumisesta ja kriisinhallinnasta vastaava Myndigheten för samhällsskydd och beredskap (MSB), tietosuojaviranomaisen Datainspektionen ja valtionhallinnon digitalisointia koordinoiva DIGG. MSB:ssä teknisestä kyberturvallisuudesta vastaa erillinen osasto. Valtakunnallinen varautumisharjoitusten koordinoiti ja strategisten analyysien laatiminen on sijoitettu kriisivalmiuden ja siviilipuolustuksen osastolle. Ruotsin CERT-SE-toiminto on sijoitettu MSB:hen. Hallitus on antanut MSB:lle tehtäväksi yhdessä FRA:n, puolustusvoimien ja turvallisuuspoliisin kanssa valmistella uuden kyberturvallisuuskeskuksen perustamista vuonna 2020. Uuden viranomaisen on tarkoitus vahvistaa Ruotsin kykyä estää, havaita ja reagoida kyberturvallisuusuhkiin ja vähentää haavoittuvuuksia. Viraston on lisäksi tarkoitus tuottaa riskien, uhkien ja haavoittuvuuksien tilannekuvaa julkiselle sektorille ja yrityksille sekä toimia hallituksen neuvonantajana kyberturvallisuusasioissa. Uuden viranomaisen perustamisen voi katsoa perustuvan Ruotsin tieto- ja kyberturvallisuuden strategian (Skr. 2016/17:213) tavoitteisiin. Eri ministeriöiden näkemykset uuden viraston resursseista ja ohjauksesta eivät ole vielä täysin yhteneviä. Yhtenä haasteena on nähty itsenäistä toimivaltuutta käyttävät noin 220 virastoa, jotka vastaavat omasta kyberturvallisuudestaan ja tarvitsevat tehokkaampaa ja keskitettyä ohjausta ja tukea.

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	2	32	38	4
Indeksiluku	0,96	0,82	0,72	0,98

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + harjoitustoiminnan keskitetty koordinoiti
- + kattava yhteiskunnan digitalisaatiostrategia
- + uuden kyberturvallisuuskeskuksen perustaminen 2020
- + elintärkeiden toimintojen ylläpitäjien velvoite toimittaa jatkuvuussuunnitelmat MSB:hen

Kehityskohteet

- pitkälle viety vastuiden hajauttaminen hankaloittaa järjestelmällistä digitaalisen turvallisuuden kehittämistä
- tieto- ja kyberturvallisuuden integrointi osaksi valtionhallinnon organisaatioiden ydintoimintaa
- yhtenäistä kuvaa yhteiskunnan strategisista riskeistä ei ole julkaistu
- julkishallinnossa ei ole käytössä systemaattista riskien hallintamenettelyä

Tieto- ja kyberturvallisuuden strategiset tavoitteet ovat monelta osin saman kaltaisia kuin muissakin verrokivaltioissa. Strategian kuusi tavoitetta ovat: 1) tieto- ja kyberturvallisuuden järjestelmällinen kehittäminen, 2) tietoverkkojen, tuotteiden ja järjestelmien turvallisuuden parantaminen, 3) kyberhyökkäysten ja -häiriöiden havainnointi, torjunta ja hallinta, 4) IT-alaan liittyvän rikollisuuden torjunta, 5) osaamisen kehittäminen ja 6) kansainvälinen yhteistyö. Strategia ei sisällä

riskiarvioita, vaan siinä on kuvattu joitain tyypillisimpiä uhkia, kuten esimerkiksi erilaiset tietomurrot ja petokset. Valtiollisten ja valtioiden tukemien toimijoiden vihamielinen vaikuttaminen (kybervakoilu, kyberhyökkäykset, informaatiovaikuttaminen) voi vahingoittaa Ruotsin taloudellisia intressejä, kriittistä infrastruktuuria, Ruotsin puolustuskykyä tai yritystoimintaa. Kyberhyökkäysten vaikutusta verrataan suoraan aseelliseen vaikuttamiseen.

Ruotsin strategioissa suunnitelmassa on tunnistettu kaikkien toimijoiden (hallinto, yritykset, kansalaiset) yhteinen vastuu digitaalisesta turvallisuudesta. Yritysten merkitys teknologian kehittäjinä ja yhteiskunnallisesti tärkeiden toimintojen omistajina on tunnistettu. Julkishallinnon ja elinkeinoelämän vuoropuhelua pidetään tärkeänä ja sitä varten MSB on organisoinut sektorikohtaisia tiedonvaihtofoorumeita (Forum för informationsdelning, FIDI), kuten esimerkiksi FIDI Finans, FIDI Vård och Omsorg ja FIDI Supervisory Control And Data Acquisition (SCADA). Viranomaisyhteistyötä varten MSB ylläpitää SAMFI-työryhmää (Samverkansgruppen för informationssäkerhet), jossa ovat mukana keskushallinnon virastot, joilla on tietoturvallisuuteen liittyviä vastuita (mm. MSB, FRA, poliisi, Posti- ja telehallitus sekä puolustusvoimat). Julkishallinnon ja yksityissektorin yhteistyö perustuu kuitenkin vapaaehtoisuuteen, eikä yksityisen sektorin tehtäviä tai vastuita digitaalisen yhteiskunnan turvaamisessa ole kuvattu kovinkaan tarkasti.

Yritykset osallistuvat tiedonvaihtoon, tuottavat informaatiota kansalliseen tilannekuvaan ja huolehtivat omasta digitaalisesta turvallisuudestaan. Strategia määrittää viranomaisille tehtäviä ja korostaa viranomaisyhteistyön tärkeyttä. Julkishallinnon ja yksityissektorin yhteistyö (public-private partnership) perustuu vapaaehtoisuuteen. Yrityksille tai kansalaisille ei strategias- sa ole määritelty tieto- ja kyberturvallisuuteen liittyviä tehtäviä ja vastuita yhtä selvästi kuin viranomaisille. Toisaalta hallituksen strategiaan kirjaamat tavoitteet ovat melko yleisiä, eikä tulosten saavuttamiseksi ole esitetty konkreettisia toimenpiteitä tai aikatauluja. Strategian toteutumiselle ei ole asetettu mittareita.

Ruotsin digitalisaatiostrategiassa (N2017/03643/D) on kuvattu viisi painopistettä kestävä digitalisoidun yhteiskunnan saavuttamiseksi: digitaalinen osaaminen, digiturvallisuus, digitaaliset innovaatiot, johtaminen digitalisaation avulla ja

digitaalinen infrastruktuuri. Kullekin osa-alueelle on kirjattu hyvin yleinen tavoite (esim. D-kompetens: jokainen pystyy kehittämään ja soveltamaan omaa digitaalista osaamistaan ja D-infrastruktur: nopeat laajakaistayhteydet ja vakaat mobiilipalvelut ovat kaikkien saatavilla). Vaikka osatavoitteita on strategiassa kirjoitettu auki, on varsinaisia konkreettisia toimenpiteitä määritelty vain vähän, eikä aikatauluja tai mittareita löydy. Vaikuttaakin siltä, että Ruotsissa on laadittu kattavia ylätasoa suunnitelmia, mutta yhteisiä strategioiden toimeenpano-ohjelmia ei löydy.

Ruotsin varautumisen ja jatkuvuuden hallinnan harjoittelun valtakunnallinen koordinointi on keskitetty MSB:hen. Virasto ylläpitää julkista harjoituskalenteria, johon on kuvattu valtakunnalliset, alueelliset ja toimialakohtaiset harjoitukset. Yhteiskunnan elintärkeistä toiminoista vastaavien organisaatioiden tulee laatia jatkuvuussuunnitelmia ja MSB on laatinut [ohjeistusta](#) tukemaan julkishallinnon ja yritysten riskien ja toiminnan jatkuvuuden hallintaa. Ohjeet perustuvat kansainvälisiin standardeihin (ISO/IEC 22301 ja ISO/IEC 31000).

Saksa

Saksassa termiä **digiturvallisuus** (digitale Sicherheit) käytetään yleensä, kun tarkoitetaan kuluttajien tietoturvallista toimintaa digiympäristössä ja tietotekniikan parissa. Saksan korkeimman tietoturvaviranomaisen BSI:n käyttämässä terminologiassa **kyberturvallisuus** (Cyber-Sicherheit) ulottuu kaikkiin tieto- ja viestintätekniikkaa koskevan tietoturvan näkökohtiin. Kyberturvallisuus kattaa kaikki Internet-yhteyteen ja vastaaviin verkoihin liitetyt tietotekniikat ja sisältää viestinnän, sovellukset, prosessit ja niihin perustuvan prosessoidun tiedon.

Kyberturvallisuus on monesta muusta viranomaistoiminnasta poiketen keskitetty liittovaltion eikä osavaltioiden viranomaisille. Keskeinen valvontaviranomainen on Bundesamt für Sicherheit in der Informationstechnik (BSI) ja puolustushallinnon osalta puolustusministeriö (Ministerium für Verteidigung). Tietosuojassa kansallisen valvontaviranomaisen Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Bdfl) lisäksi jokaisessa 16 osavaltiossa on oma paikallisviranomainen.

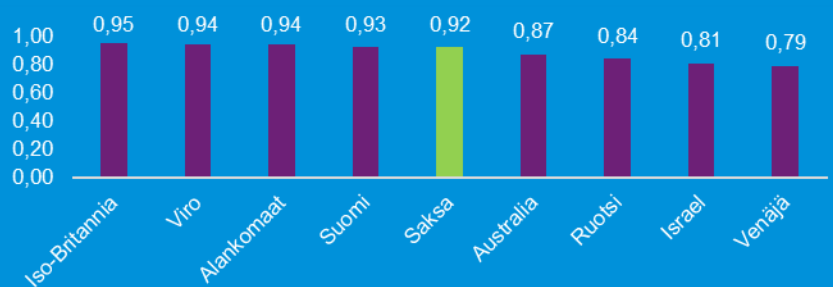
Saksassa julkishallinto osallistaa myös yksityissektoria kyberturvallisuuskeskusteluun ja kyberturvallisuustietoisuuden parantamiseen ja on perustanut tätä tarkoitusta varten yhteistoimintaelimiä, kuten Allianz für Cyber-Sicherheit ja Cyber-Sicherheitsrat.

Valtion ja liittovaltion viranomaisjärjestelmien ja verkkojen tietoturvasta säädetään Saksan perustuslaissa olkoonkin, että säädös johtuu ennemminkin Saksan liittovaltiorakenteesta kuin digitaalisen turvallisuuden tärkeydestä. Digiturvallisuuden vastuu on liittovaltion ja osavaltioiden välisellä sopimuksella annettu erillisten osavaltioiden vastuiden sijaan liittovaltiotason toimijalle (BSI), joka vahvistaa mm. tietotekniikkajärjestelmien välisen viestinnän tarvitsemat standardit ja turvallisuusvaatimukset. Perustuslain mukaisella

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	12	22	10	7
Indeksiluku	0,61	0,88	0,93	0,96

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + viranomaisjärjestelmien ja verkkojen tietoturva on nostettu perustuslain tasolle
- + laaja standardikokoelma digiturvallisuuden hallintaan (IT-Grundschutz)
- + kyberturvallisuuden strategia koskee myös kansalaisia ja talouselämää
- + kriittisen infrastruktuurin toimialoilla vahva yhteistyö julkishallinnon ja yksityisen sektorin välillä
- + kansalaisten digivalmiuksia tutkitaan vuosittain (digital index)
- + tietosuojaviranomaisilla merkittävät resurssit (laaja henkilöstö)

Kehityskohteet

- julkishallinto järjestää digitaalisia kansalaispalveluita niukasti
- liittovaltion ja osavaltioiden viranomaisten välinen yhteistyö on byrokraattista ja hierarkista, koordinointi syö resursseja

sopimuksella (IT-Staatsvertrag über die Errichtung des IT-Planungsrats) on myös perustettu liittovaltion ja osavaltioiden välinen IT-Planungsrat-niminen toimielin (2009), joka vastaa mm. valtiollisen e-hallintostrategiasta NEGSin (Nationale E-Government-Strategie Fortschreibung 2015). Strategiassa julkishallinnon yhdeksi rooliksi linjataan kriittisten hallinnollisten digi-infrastruktuurien suojelemisen digitaalisessa yhteiskunnassa.

Vuoden [2016 Kyberturvallisuusstrategiassa](#) on neljä painopistealuetta: turvallinen ja itseohjautuva (itsenäinen) toiminta digitalisoituneessa ympäristössä, valtion ja talouselämän välisen yhteistyön vahvistaminen, tehokas ja kestävä julkinen tietoverkkoturvallisuuden arkkitehtuuri sekä Saksan aktiivinen osallistuminen eurooppalaiseen ja kansainväliseen kyberturvallisuuspolitiikkaan. Kyberturvallisuusstrategiasta on johdettu

käytännönläheinen toimintasuunnitelma ja käytännön tavoitteita.

Saksassa on kehitetty tietoturvan hallintajärjestelmänä (ISMS) IT-Grundschutz, joka kattaa yhtäläisesti tekniset, organisatoriset, infrastruktuuriset ja henkilöstöön liittyvät näkökulmat. IT-Grundschutz tarjoaa järjestelmällisen lähestymistavan tietoturvaan ja on yhteensopiva ISO/IEC 27001 -standardin kanssa. Hallintajärjestelmää voi soveltaa julkisen sektorin lisäksi yksityissektorilla, jossa soveltaminen ei kuitenkaan ole pakollista.

Saksa on ollut edelläkävijä NIS-direktiivin kattaman kriittisen infrastruktuurin määrittelyssä. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) eli Kansallinen strategia kriittisen infrastruktuurin suojelemiseksi on vuodelta 2009. Kriittiseen infrastruktuuriin kuuluvat strategian mukaan: energiahuolto, tieto- ja viestintätekniikka, liikenne, juomavesi ja viemäröinti, terveydenhuolto, ravitsemus elintarvikehuolto, hätä- ja pelastuspalvelut, katastrofeihin varautuminen, parlamentti, liittohallitus, hallinto, oikeuslaitos, rahoitus- ja vakuutustoiminta sekä media (joukkoviestimet) ja kulttuuriperintö.

Venäjä

Venäjän keskeinen digiturvallisuutta määrittelevä dokumentti on Venäjän ulkoministeriön (Министерство иностранных дел Российской Федерации) julkaisema tietoturvallisuuskäsi vuodelta 2016 (Об утверждении Доктрины информационной безопасности Российской Федерации No 646). Puolustusministeriöllä ja liittovaltion turvallisuuspalvelulla (FSB) on vahva ja aktiivinen rooli julkaisun sisällön laatimisessa. Doktriinin mukaan tietoturvallisuus on yksityisten kansalaisten, yhteiskunnan ja valtion suojaamista sisäisiltä ja ulkoisilta turvallisuushilto. Venäjällä on myös tärkeä ”Digitaalisen talouden ohjelma” (Цифровая экономика Российской Федерации No 1632-p), joka käsittelee talouden modernisointia ja digitalisoitumista yleensä.

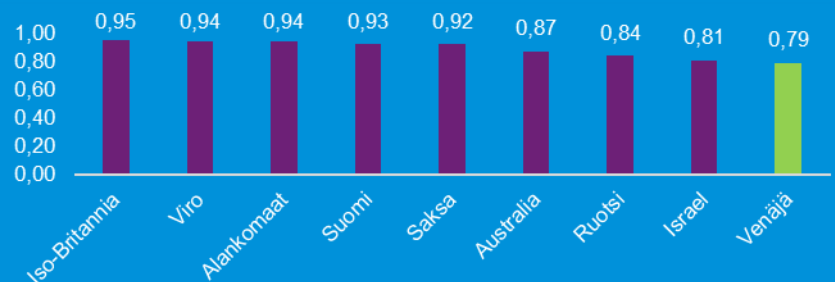
Tietoturvallisuuskäsiin linjauksen perusteella Venäjä näyttää kokevan, että se on avoimessa globaalissa viestintäympäristössä haitallisen ja valtion vakautta uhkaavan informaatiovaikuttamisen kohteena jatkuvasti. Tietoturvallisuuden linjauksissa Venäjä haluaa suojata kansalaistensa perinteisiä arvoja ja toisaalta vahvistaa omien tavoitteidensa saavuttamista kansainvälisessä toiminnassa esimerkiksi osallistumalla kansainväliseen tietoturvallisuuden lainsäädäntötyöhön ja turvallisuusjärjestelmien kehittämiseen. Lisäksi Venäjä panostaa merkittävästi puolustusvoimien kyberhyökkäyskyvyn kehittämiseen.

”Kyberturvallisuus”-termin sijaan englanniksi julkaistuissa dokumenteissa käytetään yleensä termiä ”tietoturvallisuus” (information security). Tietoturvallisuuden kehittämisen strategiset painopistealueet ovat kansallinen puolustus, valtion ja yleinen turvallisuus, talous, tutkimus, tiede ja koulutus sekä strateginen vakaus ja strategiset kumppanuudet. Strategisesti merkittävänä riskinä pidetään terrorismi- ja rikollisryhmien, ääriliikkeiden ja muiden valtioiden tiedustelu-

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	n/a	26	23	46
Indeksiluku	-	0,86	0,83	0,68

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + kyberomavaraisuuden johdonmukainen kehittäminen

Kehityskohteet

- Valtion ulkopuolelta tulevan informaatiovaikuttamisen vähentäminen

organisaatioiden vihamieliset pyrkimykset digitaalisessa toimintaympäristössä. Kohteina voivat olla esimerkiksi valtion poliittinen, sosiaalinen tai yhteiskunnallinen vakaus, alueellinen koskemattomuus tai valtion itsemääräämisoikeus. Venäjä ei muiden verrokkivaltioiden tapaan julkaise yksityiskohtaisia tietoja digitaalisen toimintaympäristönsä suojaamisesta.

Tietoturvallisuuden painopistealueille on kuvattu väljästi määriteltäviä tavoitteita, uhkien torjumiseksi.

Merkittäviksi uhkiksi on nostettu muiden valtioiden tai ääriyhtymien informaatiovaikuttaminen, tiedusteluorganisaatioiden teknologisten kykyjen kasvattaminen poliittisten ja sotilaallisten päämäärien saavuttamiseksi sekä rikollisuuden lisääntyminen digitaalisessa toimintaympäristössä erityisesti rahoitussektorilla. Strategisena riskinä nähdään lisäksi Venäjän teollisuuden riippuvuus ulkomaisista komponenteista, ohjelmistoista ja tietoteknisistä laitteista; kansallista

teknologiaa ei ole tarpeeksi saatavilla, eikä osaajia ole riittävästi.

Digitaalisen toimintaympäristön haasteet ovat näin ollen hyvin samankaltaisia kuin muissakin verrokivaltioissa. Muista verrokeista poiketen Venäjä kuitenkin nojaa digitaalisen turvallisuuden kehittämisessä vahvasti valtion keskusjoh-toiseen ohjaukseen. Esimerkiksi tutkimus- ja kehitystoimintaa ohjataan kehittämään kilpailukykyisiä kansallisia ratkaisuja, joilla riippuvuutta ulkopuolisista toimijoista voidaan vähentää.

Esimerkkinä Venäjän tietoverkkoihin liittyvien intressien turvaamisesta on ns. Runet-hanke, jonka tarkoituksena on mahdollistaa saarekekäyttö sellaisessa tilanteessa, jossa Venäjä haluaa irrottautua kansainvälisestä Internetistä, tai se joutuu muusta syystä eristetyksi kansainvälisistä tietoverkoista. Lainsäädännöllä (mm. Jarovaja-lakipaketti) veloitetaan palveluntarjoajia tallettamaan viestiliikennettä viranomaisten valvontaa varten ja tietoliikenneoperaattoreita veloitetaan avaamaan salattua tietoliikennettä tarvittaessa. Myös finanssisektorin turvallisuuteen on kiinnitetty erityistä huomiota.

Perinteisten tietojärjestelmien suojaamisesta puhutaan valtion strategisissa suunnitelmissa vähän. Operatiiviset tehtävät ovat hallinnonalojen kunkin yksikön tietohallinnon ja IT-järjestelmien vastuulla. Merkittävä hanke on kuitenkin hyökkäyksiä havaitseva, lähinnä Suomen HAVAROA vastaava GosSOPKA-järjestelmä.

Venäjä ei ole liittynyt kaikkiin kansainvälisiin sopimuksiin liittyen kuten esimerkiksi poliisin mahdollisuuteen tutkia kyberrikollisuutta maasta toiseen, mikä on linjassa strategisen itsemääräämisoikeuden varmistamisen kanssa.

Tietosuojaan liittyy vuodesta 2015 säädetty ns. tietojen lokalisatiolaki, joka edellyttää Internet-palveluja tarjoavien yritysten keräävän käyttäjien henkilötiedot myös venäläisille palvelimille. Tietojen siirtämistä edelleen kolmansiin maihin

ei ole kielletty, mutta käyttäjätietojen tulee säilyä Venäjän omassa kontrollissa.

Viro

Viron Kansallisessa kyberturvallisuusstrategiassa 2019–2022 kyberturvallisuus määritellään seuraavasti: kyberturvallisuus on tila, jossa tietoverkko ja tietojärjestelmät on suojattu siten, että uhkat eivät toteutuisi. Viron kyberturvallisuutta koskee myös toinen linjausdokumentti Viron Digitaalinen agenda 2020 (päivitetty vuonna 2018).

Kyberturvallisuuden politiikan yleisestä koordinoinnista vastaa talous- ja viestintäministeriö (vuoteen 2011 saakka puolustusministeriö). Cyber Security Council of the Security Committee of the Government tukee strategisen tason virastojen välistä yhteistyötä ja valvoo kyberturvallisuusstrategian tavoitteiden toteutumista. The Information System Authority (RIA) hoitaa ja suojaa valtion Internet-verkkoa ja varmistaa turvalliset e-vaalit.

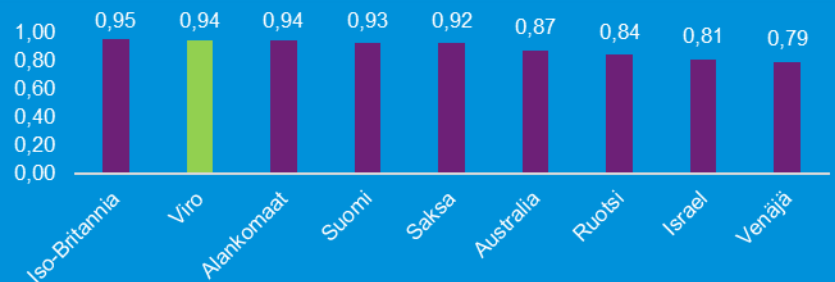
Viron kyberturvallisuusstrategia asettaa neljä tavoitetta: 1) Viro on kestävä digitaalinen yhteiskunta, joka luottaa vahvaan teknologiseen kestävyys- ja valmiuteen, 2) Viron kyberturvallisuusteollisuus on vahva, innovatiivinen, tutkimuskeskeinen ja globaalisti kilpailukykyinen, ja se kattaa kaikki Viron avaintaidot, 3) Viro on luotettava ja kykenevä kumppani kansainvälisesti ja 4) Viron kyberosaamisen taso on korkea yhteiskunnassa ja maa varmistaa riittävän ja tulevaisuuteen suuntautuvan kyberturvallisuuskäytön. Strategia on horisontaalinen eli se kattaa kaikki osallistuvat sidosryhmät Virossa: julkisen sektorin (sekä siviili että puolustus), välttämättömät palveluntarjoajat, alakohtaiset yrittäjät ja korkeakouluja. Strategian tarkoituksena on sopia ja luoda olosuhteet kattavan, systemaattisen ja osallistavan alakohtaisen politiikan toteuttamiselle.

Kyberpuolustuksen kehittämisessä on kolme painopistealuetta: 1) kriittinen infrastruktuuri ja elintärkeät palvelut, 2) kyberrikollisuuden torjunta sekä 3) kansallinen puolustus. Riittävän kyberturvallisuuden tason varmistamisella halutaan myös

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	8	5	2	21
Indeksiluku	0,75	0,98	0,99	0,86

Indeksien keskiarvo



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + yksityiskohtainen kyberturvallisuuslaki
- + vahva yhteistyö tietoturva- ja tietosuojaviranomaisten välillä
- + valtio hankkinut kriisitilanteiden varalta tallennustilaa Luxemburgista (Data Embassy)
- + sähköinen allekirjoitus ollut pitkään käytössä (digitaalinen Viro)
- + säännölliset kyberturvallisuusharjoitukset
- + valtion myöhäisen itsenäistymisen vuoksi tietojärjestelmät ja IT-arkkitehtuuri ovat uudempia kuin monessa muussa vertailuvaltiossa

Kehityskohteet

- tietoturva-asiantuntijoiden puute (ja mahdollinen muutto ulkomaille), riittämätön koulutusresurssointi
- kyberturvallisuuden erittäin voimakas riippuvuus EU:n rahoituksesta
- voimakas riippuvuus NATOn kyberkeskuksesta (The NATO Cooperative Cyber Defence Centre of Excellence)

houkutella ulkomaisia investointeja Viroon. Kyberturvallisuuspolitiikkojen täytäntöönpanossa talous- ja viestintäministeriöllä on kolme yhteistyökumppania: Cyber defence unit of the Defence League (vapaaehtoinen kyberturvallisuusjärjestö), International Centre for Defence Studies sekä Estonian Information System's Authority (EISA).

Viro on ottanut mallia Saksan IT-Grundschutzista, kun se on laatinut oman ISKE-tietoturvamallin. Virolla on myös RIHA-portaali, johon on

koottu listaus kaikista julkisista tietojärjestelmistä. Eesti.ee –portaali on kansallinen väylä Eestin julkisiin digipalveluihin sekä valtiolliseen julkiseen tietoon.

Viron kyberturvallisuuden omavaraisuus on hyvin riippuvainen sekä EU:n että Naton rahoituksesta.

Suomi

Käsitteet ”digitaalinen turvallisuus (digiturva)”, ”kyberturvallisuus” ja ”tietoturvallisuus” eivät ole täysin vakiintuneita. Tietoturvallisuudella voidaan tarkoittaa tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista ja kyberturvallisuus voidaan nähdä rajoittuvan tietoverkkoihin (erityisesti Internetiin) liitettyjen ICT-järjestelmien teknisenä suojaamisena. Kyberturvallisuus ymmärretään yleensä laajempaa kokonaisuutena, joka kattaa tiedon suojaamisen lisäksi myös toiminnan jatkuvuuden hallintaa häiriötilanteiden varalle.

Suomen digitaalisen turvallisuuden kehittäminen ja johtaminen on hajautettu ja hallinnossa toimijoita on paljon (mm. UM, VM, LVM, SM, Digi- ja väestötietovirasto, Kyberturvallisuuskeskus, Traficom, Huoltovarmuuskeskus). Hajautetussa mallissa digitaalisen turvallisuuden kehittämisen ja kehittymisen kokonaiskuvan muodostaminen on vaikeaa. Suomen viranomaisyhteistyö on kuitenkin varsin toimivaa ja julkisen ja yksityisen sektorin yhteistoiminta (public-private partnership) on organisoitu varsinkin yhteiskunnan elintärkeistä toiminnoista vastuussa olevien toimijoiden kesken (huoltovarmuusorganisaatio).

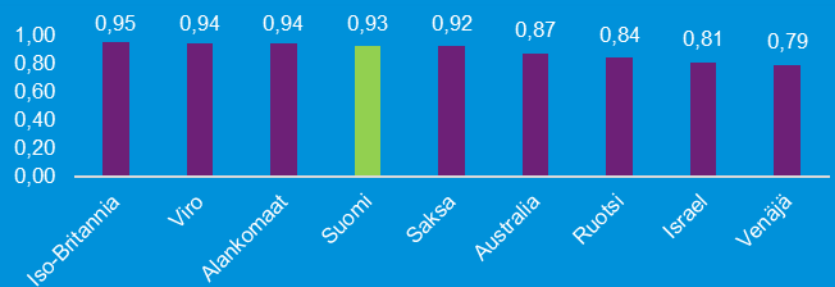
Kyberturvallisuuteen liittyvää tutkimusta tehdään, mutta kansallisesti ei ole linjattu tutkimuksen strategisia painopistealueita ja erityisiä kyberturvallisuuden koulutusohjelmia on korkeakouluissa melko vähän. Digitaalisen toimintaympäristön turvallisuuden kehitys on painottunut operatiiviseen toimintaan tunnettujen uhkien ja häiriötilanteiden hallitsemiseksi. Kansalaisten roolia digitaalisen toimintaympäristön aktiivisina turvallisuustoimijoina ei ole määritetty. Osaamisen kehittäminen on mainittu kyberturvallisuusstrategiassa, mutta tarkempia tavoitteita, tehtäviä tai mittareita ei strategiassa ole määritetty.

Vuonna 2019 julkaistu uusi kyberturvallisuusstrategia määrittelee kolme kyberturvallisuuden kehittämisen painopistettä: 1) kansainvälisen yhteistyön kehittäminen, 2)

Digitaalisen turvallisuuden indeksejä

	DESI	GCI	NCSI	CRI
	The Digital Economy & Society Index (n=28)	ITU Global Cybersecurity Index (n=175)	National Cyber Security Index (n=131)	KPMG Change Readiness Index (n=140)
Sijoitus	1	19	7	11
Indeksiluku	1,00	0,90	0,95	0,93

Indeksien keskiarvo (DESI ei mukana)



Valtion digitaalisen turvallisuuden vahvuudet ja kehityskohteet

Vahvuudet

- + toimiva viranomaisyhteistyö
- + EU-lainsäädännön toimeenpano

Kehityskohteet

- puutteellinen kokonaiskuva digitaalisen turvallisuuden kokonaistilasta
- myös muiden kuin elintärkeiden toimintojen digitaalisen turvallisuuden kehittäminen

johtamisen, suunnittelun ja varautumisen koordinaation kehittäminen ja 3) osaamisen kehittäminen. Strategia ei sisällä varsinaista uhkai riskiarviota, vaan ne todetaan kategorisesti. Erityisesti vieraiden valtioiden tai näiden tukemien toimijoiden uhkia (kyberterrorismi, -vakoilu, -sabotaasi) tai hybridivaihtamasta yhteiskunnan rakenteita tai päätöksentekokykyä vahingoittavana ilmiönä ei mainita lainkaan. Kansallisessa riskiarviossa (2018) tietoturva- ja kyberturvallisuus-

riskejä on käsitelty Yhteiskunnan turvallisuusstrategian (YTS 2017) näkökulmasta. Riskienhallinnan menettelyt vaihtelevat organisaatioittain ja Valtiontalouden tarkastusvirasto suosittelee raportissaan 20/2018 selvittämään riskien- ja jatkuvuuden hallinnan nostamista hallinnonalojen tai valtioneuvoston tasolle.

Vertailussa havaittiin, että Suomen harjoitustoimintaan liittyvät vastuut ovat hajautuneet usealle organisaatiolle. Vaikka harjoituksia

järjestetään aktiivisesti, kokonais-koordinoinnista tai -seurannasta vastaavaa tahoa ei ole nimetty.

Suomi haluaa kansainvälisessä yhteistyössä korostaa mm. avoimuutta, vapautta ja oikeusvaltioperiaatteita ja osaamisen kehittämisen katsotaan olevan kilpailukyvyn kannalta tärkeää. Kansainvälistä yhteistyötä ei kuitenkaan mielletä mahdollisuudeksi edistää Suomen taloudellisia etuja, eikä koulutuksen kasvattamista nähdä koko kyberturvallisuustoimialan mahdollistajana toisin kuin verrokkivaltioissa (esimerkiksi Alankomaat, Israel, Ruotsi) on tehty.

Kyberturvallisuusstrategia on yleisluontoinen ja sen toteuttaminen ja seuranta edellyttävät konkreettisen toimeenpano-ohjelman laatimista tehtävineen, aikatauluinen ja mittareineen. Digitaalisen toimintaympäristön kehittämisessä kustannus- ja tehokkuushyötyjä pyritään saavuttamaan ulkoistusten, pilvipalvelujen sekä tekoälyn ja oppivien järjestelmien kautta. Digitaalisen toimintaympäristön turvallisuuden kehittämisen kustannuksia ei kuitenkaan tunneta tarkasti, eikä tehtyjen toimenpiteiden vaikuttavuuden arvioimiseksi ole luotettavia mittareita. Digitaalisen turvallisuuden osa-alueiden kehittämisessä käytetään usein kansallisia viitekehyksiä (mm. KATAKRI) kansainvälisten standardien sijaan.

Liite 1 - Maakohtaiset aineistot

Perustiedot, hallinto ja resurssit

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Valtiomuoto	Perustuslaillinen monarkia	Perustuslaillinen monarkia (lähde)	Monarkia. Kuningatar on muodollisesti valtion pää, mutta käytännössä hallitus on vastuussa parlamentin alahuoneelle, jolla on käytännön valta. Hallitusta johtaa pääministeri.	Parlamentaarinen demokraattinen tasavalta (lähde)	Perustuslaillinen monarkia	Liittotasavalta (Bundesrepublik Deutschland) joka koostuu kuudestatoista tasavallasta (Bundesländer)	Venäjän federaatio on liittovaltio. Presidentin nimittämä pääministeri johtaa liittovaltion hallitusta.	Tasavalta	Tasavalta
Mihin merkittäviin liittoutumiin valtio kuuluu?	EU, Euro, Nato, YK	Kansainyhteisö (Commonwealth of Nations) (lähde), G20 (lähde), OECD (lähde), WTO (lähde), YK (lähde), MIKTA (Meksiko, Indonesia, Etelä-Korea, Turkki, Australia) (lähde), APEC (lähde), ASEAN-Australia yhteistyö (lähde), ASEAN Regional Forum (ARF) (lähde), East Asia Summit (EAS) (lähde)	EU (31.10.2019 asti), NATO, YK	YK (lähde)	EU, YK	Euroopan Unioni, Euroopan talous- ja rahaliitto (EMU, Euro), NATO, YK	YK, WTO Itsenäisten valtioiden yhteisö (IVY), johon kuuluvat useimmat NL:sta/Venäjältä eronneet muut valtiot Euraasian talousyhteisö, johon kuuluu osa IVY-maista Kollektiivinen turvallisuusjärjestö, eli IVY-maiden sotilasliitto Shanghaiin yhteistyöjärjestö (IVY-maita + Kiina)	Euroopan Unioni, NATO, YK, OECD, WTO	EU, Euro, YK, Naton rauhankumppanuusohjelma
Mitkä ovat suurimmat vientikohteet (valtiot)?	Saksa (\$89,9 miljardia), Belgia ja Luxemburg (\$67,6 miljardia), Iso-Britannia (\$47 miljardia), Ranska (\$29,8 miljardia), Italia (\$24,8 miljardia) (lähde)	Kiina (\$85 miljardia), Japani (\$34,6 miljardia), Etelä-Korea (\$18 miljardia), Intia (\$14,8 miljardia), Hong Kong (\$14,2 miljardia) (lähde)	Yhdysvallat (\$45,2 miljardia), Saksa (\$38,6 miljardia), Alankomaat (\$24,9 miljardia), Ranska (\$24,8 miljardia), Kiina (\$22 miljardia) (lähde)	Yhdysvallat (\$18,2 miljardia), Kiina (\$3,7 miljardia), Belgia ja Luxemburg (\$1,9 miljardia), Intia (\$1,9 miljardia), Saksa (\$1,8 miljardia) (lähde)	Saksa (\$16,1 miljardia), Tanska (\$10,4 miljardia), Norja (\$10,1 miljardia), Yhdysvallat (\$9,8 miljardia), Iso-Britannia (\$8,9) (lähde) (lähde)	2017: Yhdysvallat (\$112 miljardia), Ranska (\$104 miljardia), Kiina (\$95 miljardia), Iso-Britannia (\$90,3 miljardia), Alankomaat (\$84,5 miljardia) (Fakten zum Deutschen Aussehenhandel) (lähde)	Kiina (\$39 miljardia), Alankomaat (\$28 miljardia), Saksa (\$20 miljardia), Valko-Venäjä (\$19 miljardia), Yhdysvallat (\$15 miljardia) (lähde)	Suomi (\$1,8 miljardia), Ruotsi (\$1,7 miljardia), Venäjä (\$1,5 miljardia), Latvia (\$1,2 miljardia), Liettua (\$1 miljardi) (lähde)	Saksa (\$9 miljardia), Ruotsi (\$6,7 miljardia), Yhdysvallat (\$5,6 miljardia), Alankomaat (\$4,6 miljardia), Kiina (\$4 miljardia) (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Mitkä ovat suurimmat tuonnin lähteet (valtiot)?	Saksa (\$84,5 miljardia), Belgia ja Luxemburg (\$49,3 miljardia), Kiina (\$43,9 miljardia), Yhdysvallat (\$35,2 miljardia), Venäjä (\$27,7 miljardia) (lähde)	Kiina (\$47 miljardia), Yhdysvallat (\$20,5 miljardia), Etelä-Korea (\$18,7 miljardia), Japani (\$16,3 miljardia), Thaimaa (\$10,6 miljardia) (lähde)	Saksa (\$90,3 miljardia), Kiina (\$58,9 miljardia), Alankomaat (\$47 miljardia), Yhdysvallat (\$46,6 miljardia), Ranska (\$36 miljardia) (lähde)	Yhdysvallat (\$6,9 miljardia), Kiina (\$5,9 miljardia), Sveitsi (\$4,7 miljardia), Saksa (\$4,2 miljardia), Iso-Britannia (\$3,7 miljardia) (lähde)	Saksa (\$27,3 miljardia), Alankomaat (\$11,9 miljardia), Tanska (\$9,6 miljardia), Norja (\$9 miljardia), Belgia ja Luxemburg (\$7,6 miljardia) (lähde) (lähde)	2017: Kiina (\$109,2 miljardia), Alankomaat (\$89,9 miljardia), Ranska (\$69,1 miljardia), Yhdysvallat (\$61,6 miljardia), Italia (\$58,5 miljardia) (Fakten zum Deutschen Aussenhandel) (lähde)	Kiina (\$44 miljardia), Saksa (\$27 miljardia), Valko-Venäjä (\$13 miljardia), Yhdysvallat (\$11 miljardia), Italia (\$9 miljardia) (lähde)	Saksa (\$1,7 miljardia), Suomi (\$1,7 miljardia), Venäjä (\$1,7 miljardia), Kiina (\$1,5 miljardia), Liettua (\$1 miljardi) (lähde)	Saksa (\$10,7 miljardia), Venäjä (\$8,4 miljardia), Ruotsi (\$6,7 miljardia), Kiina (\$5 miljardia), Alankomaat (\$3,8 miljardia) (lähde)
Mikä on valtion väkiluku (miljoonaa asukasta)?	n. 17 miljoonaa (lähde)	25,3 miljoonaa asukasta (maaliskuu 2019) (lähde)	66,4 miljoonaa (2018) (lähde)	9,1 miljoonaa asukasta (2019) lähde	noin 10 miljoonaa (lähde)	2018: 83 miljoonaa (Statistisches Bundesamt)	147 milj. (2017)	noin 1,3 miljoonaa (lähde)	2018: noin 5.5 miljoonaa (lähde)
Ministeriöt, joilla on digiturvallisuuden liittyviä vastuita?	Digitaalisen toimintaympäristön ohjaus on keskitetty oikeusministeriöön (Ministerie van Justitie en Veiligheid). Elinkeinoministeriö (Ministerie van Economische Zaken en Klimaat) vastaa Alankomaiden digitalisatiosta. Kyberpuolustus kuuluu puolustusministeriön (Ministerie van Defensie) toimialaan.	Department of the Prime Minister and Cabinet, puolustusministeriö (Department of Defence, ulkoministeriö (Department of Foreign Affairs) (lähde) Department of Foreign Affairs (lähde)	Pääministerin kanslia (Cabinet Office) koordinoi kyberturvallisuuden hallintaa. GCHQ:n toiminta on ulkoministeriön vastuulla. Puolustusministeriö	Pääministerin kanslia (Prime Minister's Office)	Puolustusministeriö (kokonaismaanpuolustus, kriisivalmius, turvallisuuspoliittiset tiedustelukysymykset) Oikeusministeriö (lainsäädäntö, rikosasiat; Myndigheten för samhällsskydd och beredskap, (MSB) toimii oikeusministeriön ohjauksessa) Infrastruktuuriministeriö (fyysinen infrastruktuuri, digitalisaatio, IT, posti ja energia) Elinkeinoministeriöt (valtion yritykset, elinkeinoelämä, innovaatiot ja tutkimus) Regeringskansliet (valtionhallinnon digitalisaatio)	Bundesministerium für Innern, für Bau und Heimat (sisäasiainministeriö) Bundesministerium der Verteidigung (puolustusministeriö)	Venäjän tietoturvallisuusdoktriinin (tietoturvallisuuden strategiset linjaukset) mukaan presidentti määrittää tavoitteet tieto- ja viestintätekniikan käyttöön toteutuksessa ja ulkopoliittikan edistämiseksi. (lähde; analyysia täällä) Armeijalla/puolustusministeriöllä on merkittävä rooli, koska tietoturvadoktriinin painopiste on informaatiovaihtamisessa ja globaalissa, valtion turvallisuutta koskevassa kyberpuolustustoiminnassa. Digitalisaatio-, tietoliikenne- ja joukkoviestintäministeriöksi (digiministeriö) mm. rahoittaa FSB:n (ks. alla) rakentamaan tietoturvahyökäysten torjuntajärjestelmää GosSOPKA.	Ulkoministeriö - Ministry of Foreign Affairs Sisäministeriö - Ministry of Internal Affairs Talous- ja viestintäministeriö - Ministry of Economic Affairs and Communications Minister of Foreign Trade and Information Technology Puolustusministeriö Oikeusministeriö	Valtiovarainministeriö Liikenne- ja viestintäministeriö Ulkoministeriö Sisäministeriö Puolustusministeriö Valtioneuvoston kanslia
Muut viranomaiset, joilla on digiturvallisuuteen liittyviä vastuita?	NCTV, NCSC-NL	Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC), joka hyödyntää seuraavia viranomaisia:	Government Communications Headquarters (GCHQ) on ulkoministeriön alainen tiedustelu- ja kyberturvallisuusvirasto. Sen vastualueisiin kuuluvat	Israel National Cyber Directorate Knesset Subcommittee for Cyber Defense	Myndigheten för samhällsskydd och beredskap (MSB) on oikeusministeriön ohjauksessa toimiva valmiusvirasto. Sen tehtäviin kuuluvat mm.	Bundesamt für Sicherheit in der Informationstechnik (BSI) (ks. enemmän kyberturvallisuus-kohdassa)	Liittovaltion turvallisuuspalvelu (FSB) on digitaalisen turvallisuuden laaja ja aktiivinen vaikuttaja varsinkin sen jälkeen, kun siihen liitettiin Federal Agency	Kyberturvallisuusneuvosto (Cyber Security Council) : Tehtävänä on edistää sujuvaa yhteistyötä eri instituutioiden välillä ja valvoa kyberturvallisuusstrategian	Digi- ja väestötietovirasto (DVV) Traficom Kyberturvallisuuskeskus Valtori

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
		Defence Intelligence Organisation Australian Security Intelligence Organisation Australian Federal Police Australian Criminal Intelligence Commission Critical Infrastructure Centre Sisäasianministeriö (Department of Home Affairs) Data61 Joint Cyber Security Centres (JCSC) Defence Science and Technology (DST) Information Warfare Division (IWD) (lähde)	terrorismin torjunta, kyberturvallisuus, valtiolisten toimijoiden aiheuttamien uhkien torjunta, järjestäytyneen rikollisuuden torjunta ja maanpuolustuksen tuki. National Cyber Security Centre (NCSC) on GCHQ:n alainen vi-rasto, joka auttaa kyberhyökkäysten torjunnassa ja vastaa vakavien häiriöiden hallinnasta. NCSC antaa teknistä neuvontaa ja koordinoi poikkihallinnollisia toimenpiteitä. (lähde). NCSC sertifioi kaupallisia kyberturvallisuustuotteita ja –palveluita. (lähde) The National Security Secretariat koordinoi strategisia turvallisuus- ja tiedusteluhankkeita poikkihallinnollisesti.	Department of Emergency, Information Security and Cyber Israel National Cyber Event Readiness Team (CERT-IL) Israeli Security Agency (ISA) Technology and Cyber Division	siviilipuolustuksen kehittäminen ja tukeminen, osallistuminen valtakunnalliseen tietoturvatyöhön, valtakunnallisten varautumisharjoitusten koordinointi ja yhteiskunnan varautumisen kehittäminen. Datainspektionen on oikeusministeriön ohjauksessa toimiva Ruotsin tietosuojaviranomainen. DIGG on valtiovarainministeriön ohjauksessa toimiva viranomais, joka vastaa hallinnon digitalisaatiosta Försvarsmakten, puolustusvoimat; kyberpuolustus Försvarets radioanstalt (FRA), signaalitiedustelu Post- och telestyrelsen (PTS), tietoliikenne Polismyndigheten, Säkerhetspolisen, Försvarets materielverk (FMV) Aluehallinto (21 lääniä (län), 20 maakuntaa (landsting))	IT-Planungsrat (va-paasti suomennettuna IT-suunnitteluneuvosto) on Saksan perustuslain 91 c §:n mukainen Saksan liittovaltion ja osavaltioiden välinen yhteistoimintaelin (IT-Staatsvertrag über die Errichtung des IT-Planungsrats) vuonna 2009. IT-Planungsrat on mm. laatinut valtiolisen e-hallintostrategian NEGSin (Nationale E-Government-Strategie Fortschreibung 2015), joka linjaa julkishallinnon yhdeksi rooliksi kriittisten hallinnollisten digi-infrastruktuurien suojelemisen digitaalisessa yhteiskunnassa. Koordinierungsstelle für IT-Standards (Ko-SIT) koordinoi julkishallinnossa kehitettäviä IT-standardeja viranomaisten väliseen tietojenvaihtoon. Saksassa on myös sisäasiainministeriön alaisena Beauftragter der Bundesregierung für Informationstechnik – nimikkeellä oleva virkamies, jonka tehtävänä on edistää elinkeinoelämän, osavaltioiden ja Saksan liittovaltion välistä yhteistyötä informaatiotekniikkaan liittyvissä asioissa.	of Government Communications and Information, joka oli vastuussa mm. liittovaltion oman viestinnän turvaamisesta. FSB on virallisesti osa sotilasorganisaatiota, mutta vastaa suoraan presidentille. Venäjän keskuspankki hoitaa finanssisektorin tietoturvaa. Liittovaltion tasavallat ja muut hallinnolliset alueet hoitavat alueellisia asioita. CERT.GOV.RU vastaa Venäjän valtiollisista tietoverkoista ja koordinoi viranomaisten ja lainvalvonnän toimenpiteitä (lähde).	täytäntöönpanoa. (Secretary General of the Ministry of Economic Affairs) Ambassador at Large for Cyber Security - Suurlähettiläs vastaa Viron kyberturvallisuuden ulkopoliittikan kehittämisestä, varmistaa sen koordinoitun toteuttamisen, edustaa Viroa kansainvälisissä organisaatioissa ja osallistuu alan kansainväliiseen yhteistyöhön. (UM) Estonian Internal Security Service (SM) KAPO on vastuussa kansallista turvallisuutta uhkaavien hyökkäyksien havaitsemisesta ja estämisestä. Information System Authority tehtävänä on hallita ja suojata valtion Internet-verkkoa ja varmistaa turvalliset e-vaalit. Estonian Data Protection Inspectoriate toimialat: tietosuojavalvottu, alustava tuomioistuim, audittoja ja lisenssinantaja, koulutaja ja konsultti, oikeudellisten käytäntöjen suunnittelija, poliittinen neuvonantaja, lainvalvontavirasto	Huoltovarmuuskeskus
Mikä on valtion digiturvallisuuden kehittämiseen käytetty rahamäärä?	NCSC:n budjetti vuodelle 2019 oli noin 8,75 miljoonaa euroa. (lähde) Valtionhallinnon kyberturvallisuusinvestoinneista ei löydy	Australia julkaisi 2016 kyberturvallisuusstrategian vuosille 2016-2020. Näille neljälle vuodelle Australia on varannut 230 miljoonaa Australian dollaria (141	UK käyttää 1,9 miljardia puntia (n. 2,1 miljardia euroa) viiden vuoden aikana kyberturvallisuuden kehittämiseen. 836 miljoonan punnan (n.	Puolustukseen ja yhteiskunnan kriisivarautumiseen on vuodelle 2019 budjetoitu yhteensä noin 56 miljardia kruunua (hieman yli	BSI:n budjetti vuonna 2018 117,9 miljoonaa euroa	Venäjän on arvioitu käyttävän noin 300 M€ vuodessa pelkästään kyberhyökkäyskyvyn parantamiseen, ja tähän palkattuja asiantuntijoita on tuhat (lähde).	2014–2020 tuetaan Viron tietoyhteiskunnan kehittämistä 181 760 000 eurolla, johon lisätään Viron yhteisrahoitus 24 928 235 euroa.	Valtion ICT-toiminnan kokonaismenot vuonna 2016 olivat yhteensä noin 780 miljoonaa euroa (lähde). Julkisen hallinnon ICT:n ohjaus ja kehittäminen	

Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	täsmällisiä lukuja viranomaislähteistä. Erään raportin mukaan Alankomaissa hallinto investoi kyberturvaan kansantuotteeseen suhteutettuna vähemmän kuin esimerkiksi Iso-Britannia, Ranska, Yhdysvallat tai Australia. (lähde; ei viranomaislähde)	miljoonaa euroa) toteuttaakseen strategiasa asetetut kehitystoimenpiteet. Australia käyttää vuonna 2016 julkaiseman kyberturvastrategian kehitystavoitteiden toteuttamiseen yhteensä 230 miljoonaa AUD vuosina 2016-2020. (lähde)	940 miljoonaa euroa) kehitysohjelma. (lähde)	5,2 miljardia euroa) (lähde). MSB: vuosibudjetti 2019 oli noin 1,3 miljardia kruunua (noin 121 miljoonaa euroa) (lähde) Datainspektionen: vuoden 2019 budjetti oli noin 94 miljoonaa kruunua (noin 8,8 miljoonaa euroa). (lähde) DIGG: budjetti vuodelle 2019 oli noin 99 miljoonaa kruunua (noin 9,2 miljoonaa euroa) (lähde).			Information Security Authority (RIA) toimii täytäntöönpanoyksikönä. (lähde)	vuodelle 2020 budjetoitu 42,7 miljoonaa euroa (lähde).
Kuinka monta henkilöä työskentelee digiturvallisuuden parissa?	AP: 167 henkilöä (2018) (lähde)		GCHQ: yhteensä noin 6000 henkilöä (2017) (lähde) National Security Secretariat (NSS): 120 henkilöä (2017) (lähde) ICO: 601 henkilöä (2018-2019) (lähde)		MSB: keskimääräinen henkilöstömäärä 2018 vuosikertomuksen mukaan oli 1240 henkilöä (lähde). Virastossa on kuusi osastoa, mutta osastokohtaisia henkilöstömääriä ei ole saatavilla. Datainspektionen: keskimääräinen henkilöstömäärä 2018 vuosikertomuksen mukaan oli 75 henkilöä. (lähde) DIGG: keskimääräinen henkilöstömäärä 2018 vuosikertomuksen mukaan oli 39 henkilöä (lähde). FRA: noin 800 henkilöä (lähde)	BSI yli 900 asiantuntijaa, päämaja Bonn	Ks. edellä.	

Strateginen riskienhallinta

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Riskienhallintaa ohjaava lainsäädäntö		Public Governance, Performance and Accountability Act 2013 (lähde) Laissa säädetään australialaisten organisaatioiden sisäisten riskienhallintaohjelmien laatimisesta.	Civil Contingencies Act Financial Services and Markets Act 2000 (FSMA) (finanssisektoria koskeva)			Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) 17.7.2015, joka on lakiteknisesti BSI-G-lain sekä usean muun lain muutos. Linkki vie alkuperäiseen Saksan säädöskokoelmassa julkaistua muutostekstiin, mutta muutos on mm. myös osana ajantasaista BSI-G-lakitekstiä. Ei kattavaa yleislainsäädäntöä vaan tiettyjä aloja koskevaa erityislainsäädäntöä, ks. tarkemmin raportin kohta tietoturva.	Valtion sisäisistä digitalisointistrategioista nousevia kattavia ja yleisiä riskienhallintasuunnitelmia tai niiden tueksi laadittua lainsäädäntöä ei tunnustettu. Venäjän tietoturvallisuudessa keskeisinä elementteinä ovat globaali vaikuttaminen ja valtion keskusjohtoinen kontrolli valtion etujen suojaamiseksi.	Emergency Act (lähde) Information System Authority antaa valtakunnallista tukea merkittävässä/laaja-alaisissa kyberhäiriöissä. National Defence Act (lähde) Cyber Security Act (lähde)	Euroopan parlamentin ja neuvoston päätös unionin pelastuspalvelumekanismista (N:o 1313/2013/EU)
Riskienhallintaa koskevat strategiset linjaukset	Digitalisaatiostrategiassa ei arvioida riskejä, mutta energia-tuotannon osalta todetaan, että digitalisaation myötä järjestelmien väliset yhteydet muodostavat uusia haavoittuvuuksia ja lisäävät huoltovarmuusriskejä (security of supply). Kansallisessa riskiarviossa riskejä arvioidaan kuuden kansallisen turvallisuussintresin kautta: alueellinen turvallisuus (security)	Australian kansallisessa turvallisuusstrategia 2013: Australian kansallisen turvallisuuden tavoitteena on suojella ja vahvistaa suvereniteettia varmistaa väestön turvallisuus ja vastustuskyky turvata omaisuus, infrastruktuuri ja institutiot edistää suotuisaa kansainvälistä ympäristöä Tärkeimmät prioriteetit seuraaville viidelle	Kansallisen tason riskit on ryhmitelty kolmeen luokkaan (Tier 1, 2 ja 3). Tier 1 -tason riskejä ovat kyberhyökkäykset, kansainväliset sotilaalliset kriisit, kansainvälinen terrorismi, suur-onnettomuudet ja luonnonkatastrofit. (The National Security Strategy , 2010) (lähde) (lähde) Turvallisuusstrategia (kohta 4.03) listaa kahdeksan kansallista turvallisuustehtävää: Kansallisten riskien ja mahdollisuuksien	Oikeusministeriö on julkaissut rahanpesua koskevan kansallisen riskiarvion. (lähde)			Tietoturvallisuuskokiriin mukaan suurimmat digitaalisen toimintaympäristön (information space; информационное пространство) uhat liittyvät muiden valtioiden Venäjään kohdistamaan vihamieliseen toimintaan, terrorismiin ja ääriliikkeiden toimintaan sekä lisääntyvään kyberrikollisuuteen.	ks. Jatkuvuudenhallinta (Viro)	VM on valmistellut valtionhallinnon riskienhallintapolitiikkamalli, jonka pohjalta valtiovarain controller-toiminto on antanut suosituksen mallin käytöstä. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	fyysinen turvallisuus (safety) talouden turvallisuus (security) ekologinen turvallisuus (security) sosiaalinen ja poliittinen tasapaino kansainvälinen laillisuusperiaate Kyberuhkista arviossa tunnistetaan erityisesti digitaalinen sabotaasi, kybervakoilu, kyberrikollisuus ja Internetin toiminnan häirintä. Kyberuhkista johtuvat häiriöt nähdään sekä ensisijaisina tavoitteina että välineinä, joilla vaikutetaan fyysiseen toimintaympäristöön. Kyberympäristön riskit on sijoitettu alueellisen turvallisuuden ja sosiaalisen ja poliittisen tasapainon teemojen alle.	vuodelle strategian laatimisesta ovat tehostettu alueellinen sitoutuminen turvallisuuden ja hyvinvoinnin tukemiseen "Aasian vuosisadalla" integroitu kyberpolitiikka ja -toiminnot turvaamaan digitaalisten verkostojen puolustuksen parantamiseksi tehokkaat kumppanuudet innovatiivisten ja tehokkaiden kansallisen turvallisuuden tulosten saattamiseksi (lähde)	tunnistaminen ja seuranta Häiriöiden juurisyiden selvittäminen Riskien hallinta ja mahdollisuuksien hyödyntäminen Valtiota ja sen intressejä uhkaavien tekijöiden hallinta kansallisen lainsäädännön ja kansainvälisten normien avulla Suojautuminen valtiollisten ja ei-valtiollisten toimijoiden aiheuttamilta fyysisiltä tai digitaalisilta häiriöiltä valtion alueella, sen rajoilla ja kansainvälisesti Konfliktien ratkaisu vakauden tukemiseksi Varautuminen erilaisiin vakaviin häiriötilanteisiin (emergency) ja häiriöiden hallinta nopeaa toipumista ja elintärkeiden palvelujen ylläpitoa varten Yhteistoiminnan ja kumppanuuksien hyödyntäminen toiminnan tehostamiseksi						
Mitkä ovat valtion strategiset digiturvallisuuteen liittyvät riskit?	Alankomaiden kansallinen kyberturvallisuusarvio (Cyber Security Assessment Netherlands, CSAN 2019) nostaa esiin seuraavat kyberturvallisuuden kohdistuvat riskit: valtiollisten toimijoiden aiheuttamat uhat (kyberhyökkäykset,	Tunnistettujen kansallisten turvallisuusriskit ovat vakoilu ja ulkomainen puuttuminen epävakaus kehittyvissä ja hauraisissa valtioissa pahantahtoinen kybertoiminta	Kansallinen riskiarvio (The National Risk Assessment, NRA) ei ole julkisesti saatavilla. Siitä on laadittu julkinen versio (The National Risk Registry, NRR), jossa yhteiskunnan riskejä käsitellään yleisellä tasolla. Kyberturvallisuus on käsitelty riskikisterissä. Tuorein		Ruotsin strategisten riskien hallintaa käsitellään tieto- ja kyberturvallisuusstrategiassa. Tyhjentävää listaa tunnistetuista riskeistä ei strategiaan ole kirjattu, mutta MSB:n julkaisussa vuodelta 2012 on listattu 24 keskus- ja aluehallinnon tunnistamaa riskiä. Digitaaliseen turvallisuuteen		Informaatiodoktriinissa yhtenä merkittävänä riskikokonaisuutena pidetään ulkopuolelta tulevaa vihamielistä vaikutusta, jolla pyritään haittaamaan valtion itsemääräämisoikeutta, alueellista koskemattomuutta tai valtion poliittista	Tärkeä kehityksen este on asiantuntijoiden puute, mikä hidastaa kasvua koko ICT-alalla. Ei ole riittävästi alan asiantuntijoita ja mahdollinen ongelma, että alan asiantuntijat muuttavat Viirasta muualle. Riittämätön kokonaisjohtaminen.	Erillisinä häiriötilanteina on tunnistettu informaatiovaikutaminen sekä viestintäverkkojen ja -palveluiden vakavat häiriöt. Monissa uhkamalleissa (mm. finanssiala ja logistiikka) kyber-, tietoturva- ja tietosuojariskit (esim. kyberhyökkäykset, tietoverkkotiedustelu) ovat mukana, mutta

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	kybervakoilu, kybersabotaasi) digitaalisille palveluille ja prosesseille ei ole vaihtoehtoisia (analogisia) toimintatapoja riippuvuus pienestä määrästä palvelujen toimittajia kyberhyökkäyksiä varten tarvittavan teknologian helppo saataisuus digitaaliset tuotteet ja palvelut, joiden turvataso on huono digitaalisen infrastruktuurin pirstaleisuudesta johtuva monimutkaisuus	joukkotuhoukseiden leviäminen vakava ja järjestäytynyt rikollisuus valtiollinen konflikti tai pakkotila, joka vaikuttaa Australian intresseihin terrorismi ja väkivaltaiset ääriilikkeet Näistä riskeistä monet sisältävät digiturvallisuuteen liittyviä elementtejä. (lähde)	versio on vuodelta 2017.		liittyviä riskejä ovat listalla mm. sähköisen viestinnän häiriöt, maksuliikennejärjestelmien häiriöt ja kyberhyökkäykset.		tai sosiaalista vaikutusta (lähde).	Riittämätön tietoisuus verkkouhkien ja vaaratilanteiden vaikutuksista sekä infrastruktuurien riippuvuuksista Kyberturvallisuuden takaamista ei pidetä henkilökohtaisena vastuuna tai organisaation toimintarisikinä. (lähde)	niitä ei ole käsitelty erikseen. (lähde)
Kuka arvioi valtion strategisia riskejä? Riskienhallinnan hallintorakenteet	NCTV on osoittanut kansallisen riskiarvion tekemisen yhteistyöverkoston (National Network of Safety and Security Analysts, ANV) tehtäväksi.	Australian Government (lähde)	Valtion kriittiset riskit kuvataan kansallisessa riskiarviossa (National Risk Assessment NRA – ei saatavilla julkisesti). Cabinet Officeen sijoittuva Civil Contingencies Secretariat päivittää arviota vuosittain. (lähde)		Ruotsin hallitus on määrännyt valmiusviraston (Myndigheten för samhällsskydd och beredskap, MSB) ylläpitämään yleiskuvaa riskeistä, jotka kohdistuvat kansalliseen toimintakykyyn. (lähde)	Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) Bundesministerium des Innern, für Bau und Heimat (BMI) Bundesamt für Sicherheit in der Informationstechnik (BSI)	FSB:llä on vahva rooli. Ks. lisäksi hallintorakenteen yhteydessä mainitut doktriinin mukaiset informaatioturvallisuuteen vaikuttavat organisaatiot.	Tasavallan hallituksen turvallisuuskomitea (Security Committee of the Government of the Republic). Hallituksen turvallisuuskomitea analysoi ja arvioi kansallisen turvallisuuden tilannetta ja koordinoi viranomaisten toimintaa kansallisen puolustuksen suunnittelussa, kehittämisessä ja järjestämisessä. Komitean puheenjohtajana toimii pääministeri, ja sen jäseniä ovat puolustusministeri, talous- ja infrastruktuuriministeri, yritys- ja IT ministeri, valtiovarainministeri, ulkoministeri, sisäministeri, ja oikeusministeri. (lähde) Viro järjestää kyberturvallisuuden yhteinäisesti samoilla rakennetkaisuilla rauhan ja sodan aikana.	Kansallisen riskiarvion julkaisee sisäministeriö. Siihen kootaan uhkamalleja ja riskiarvioita eri hallinnonaloilta. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
								Kyberpuolustus on osana kansallista puolustusjärjestelmää ja sitä järjestetään yhteistyössä virastojen kanssa sekä harjoitetaan säännöllisesti. (National Security Concept)	
Kuka ylläpitää kokonaiskuvaa valtion riskeistä?	Oikeusministeriö ja sen alaiset laitokset (NCTV ja NCSC). NCTV on julkaissut valtion riskeistä yläta-son yhteenvedon .	Australian Govern-ment (lähde)	Cabinet Office (Minis-ter for Government Resilience and Effi-ciency) National Security Counselin alakomitea (Threats, Hazards, Resilience and Con-tingencies - THRC) vastaa korkeimman riskitason uhkien, häi-riöiden ja jatkuvuuden suunnittelun, valmis-telun ja toipumistoi-menpiteiden strategi-sesta johtamisesta (lähde; Table 3) Cabinet Officeen si-joittuva Civil Contin-gencies Secretariat päivittää arviota vuo-sittain. (lähde)		MSB toimittaa halli-tukselle vuosittain kansallisen riskiar-vion, jossa kuvataan haasteita ja nimetään kehitysehdotuksia. Vuoden 2019 arvion yksi kehityssuositus on integroida tieto- ja kyberturvallisuustyö tiiviimmin osaksi vi-ranomaisten ydintoi-mintaa. Keskitettyä yleiskuvaa riskeistä on ylläpidetty vuo-desta 2011 lähtien (lähde) .			Kyberpuolustus osana kansallista puolustusjärjestelmää ja sitä järjestetään yhteistyössä virastojen kanssa sekä harjoite-taan säännöllisesti. (National Security Concept)	Sisäministeriö koos-taa Euroopan parla-mentin ja neuvoston päätöksen unionin pe-lastuspalvelumekanis-mista (N: o 1313/2013/EU) nojalla kansallisen riskiarvion kolmen vuoden vä-lein. (lähde)
Mikä on yksityis-sektorin rooli val-tion riskienhallin-nassa?	Nimetyt yksityissek-torin johtohenkilöt ja tiedeyhteisöjen edus-tajat osallistuvat kan-sallisen riskiarvion tuottamiseen. (lähde)					Antaa lausuntoja laki-esityksiin ja osallistuu muutenkin yhteiskun-nalliseen keskus-te-luun.			
Kuinka riskienhal-lintaprosessi on ohjeistettu?	Oikeusministeriö on laatinut ohjeen , jossa käsitellään mm. ris-kien arviointia kansal-lisen turvallisuusstra-tegian näkökulmasta. NCTV on julkaissut linjauksen siitä, miten valtion riskeihin vasta-taan. Linjauksessa ko-rostuvat osaamisen kehittäminen ja yh-teistyö niin	The Commonwealth Risk Management Policy julkaistiin 2014. Kyseinen poli-tiikka edellyttää toi-menpiteitä vastuuväl-voillisilta viranomai-silta. Riskienhallinta-politiikan implemen-toinnista on annettu ohjeistus. (lähde) Riskienhallinnan stan-dardina käytetään AS/NZS ISO	NCSC ylläpitää sivus-toa , jolla kuvataan ris-kienhallinnan perus-toiminnot ja kybertur-vallisuuden riskienhal-lintakeinoja.		MSB ylläpitää tietoturvallisuutta koske-vaa sivustoa , jossa annetaan yleisiä oh-jeita riskien hallinnan toteuttamiseksi (lähde) . Ohjeessa kä-sitellään riskien tun-nistamista ja analy-sointia (mm. toimin-taympäristön ana-lyysi, riskianalyysi ja kuiluanalyysi). Ohjeis-tuksessa viitataan	Hallinnon taloudelli-sen tehokkuuden liit-tovaltion komissaari (Der Bundesbeauftragte für Wirtschaftlichkeit in der Verwaltung BWW) on julkaissut 2017 ehdotuksen siitä, miten liittoval-tion viranomaiset voi-vat systemaattisesti käsitellä riskejä, jotka voivat vaarantaa	Information System Authority järjestää valtakunnallisia ratkai-suita silloin kun on ta-pahtunut merkittäviä tai laaja-alaisia ky-berhäiriöitä. (Emer-gency Act) Hätätilanteita koordi-noi RIA:n Incident Re-sponse Department. CERT osallistaa tarvit-taessa RIA: n muiden kyberturvallisuus-	Ohje riskienhallintaan (VM 22/2017) kuvaa ISO31000-standardiin perustuvan riskien ar-viointimenettelyn val-tionhallintoa varten.	

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	kansallisesti kuin kansainvälisestikin.	31000:2009, joka korvasi aiemmin käytetyn kansallisen standardin. (lähde)			kansainvälisiin standardeihin ISO/IEC 27001 (tietoturvallisuuden hallintajärjestelmä), ISO/IEC 27005 (tietoturvariskien hallinta) ja ISO/IEC 31000 (riskienhallinta). MSB on lisäksi julkaissut yhteiskunnan toiminnan kannalta tärkeille yksityisille ja julkishallinnon toimijoille ohjeen toimintojen suojaamisesta. Ohje sisältää mallit riskien ja jatkuvuuden hallintaan. Riskienhallintaan liittyvät toimintamalli vaihtelevat valtion organisaatioissa. Yhtenevää tapaa riskienhallintaan ei ole. Riskienhallintaan liittyviä termejä käytetään vaihtelevasti. Jatkuvuuteen ja varautumiseen liittyvät riskit on määritetty ja kuvattu Säkerhetspolitik-sivustolla, jota ylläpitää varautumisviranomainen (MSB).	niiden tehokkaan, asianmukaisen ja taloudellisen suorituskäytännön. BVVV:n kehittämä malli riskienhallintamatriisille yhdistää kattavan riskienhallinnan sisäisen valvonnan ja hallintajärjestelmät erilaiset vaikutussuhteet BVVV-malli ei vaadi yhdenmukaista riskienhallintaa koko liittovaltion hallinnolle. Eri viranomaiset voivat mukauttaa mallia omiin olosuhteisiinsa ja vaatimuksiinsa ja kehittää siten oman riskienhallintajärjestelmänsä.	osaston työntekijöitä ja muita Emergency Response Plan:ssa lueteltuja viranomaisia (lähde).		
Miten digiturvallisuuden osa-alueet on huomioitu riskienhallinnassa?	NCSC:n julkaisuissa käytetään termiä ”kyberturvallisuus” sateenvarjoterminä, joka kattaa useimmat digitaalisen turvallisuuden osa-alueet.	Kyberturvallisuus kattaa useimmat digiturvallisuuteen liittyvistä käsitteistä.	National Risk Registry (NRR) (2017) kansallisen riskiarvion (National Risk Assessment) käsittelee kyberturvallisuutta yhtenä kokonaisuutena.		ks. seuraava kohta			Kriisinhallintalaki (Emergency Act) määrittää elektronisen turvallisuuden elintärkeäksi varmistettavaksi palveluksi (§41).	
Miten riskiarvioita käytetään valtion digiturvallisuuden kehittämisessä?	Kansallisessa riskiarviossa vuodelta 2019 kriittisimpien riskien joukossa ovat digitaalinen sabotaasi, kriittisen infrastruktuurin häiriöt ja hybridioperaatiot.	Australia on havainnut kyberturvallisuuden merkittäväksi kehityskohteeksi ja asettanut tämän merkittäväksi kehityskohteeksi kansallisessa	National Risk Registry (NRR) (2017) kansallisen riskiarvion (National Risk Assessment) listaa toimenpiteitä, joilla kehitetään valtionhallinnon, yritysten ja kansalaisten		Systemaattinen riskien hallinta ei näy Ruotsin digitalisaatiostrategiassa, jossa todetaan vain hyvin yleisellä tasolla riskien hallinnan tärkeys.	Ks. IT-Grundschutz .			

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
		turvallisuusstrategiassa. (lähde)(*) Kyberturvallisuusstrategiassa on asetettu monta kehityskohdetta, jonka edistymistä seurataan. (lähde)	kyberturvallisuutta. Tällaisia ovat mm. strategian päivitys, Cyber Essentials -koulutus ja sertifiointi (lähde) ja kansallisen kyberturvallisuusviranomaisen (NCSC) perustaminen 2016.						

Jatkuvuudenhallinta

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Jatkuvuudenhallintaa ohjaava lainsäädäntö		Security of Critical Infrastructure Act 2018 (lähde) Security of Critical Infrastructure Rules 2018 (lähde)	The Civil Contingencies Act 2004 velvoittaa kriisinhallinnan keskeisiä toimijoita (Category 1 responders) julkisen riskirekisterin (Community Risk Register) ylläpitoon. Näiden toimijoiden on myös varmistettava toimintansa jatkuvuus kriisitilanteissa. (lähde)		MSB:n tehtävät määritellään asetuksessa Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap. Lääninhallituksille kuuluvat varautumistehtävät on määrätty asetuksella Förordning (2017:868) med länsstyrelseinstruktion. Kuntien ja maakuntien toimenpiteet vakavien häiriöiden ja korotetun valmiuden varalle on määritelty laissa 2006:544 (Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap) Lakiin perustuvia tai hallinnon antamia varautumistehtäviä on lukuisilla viranomaisilla.	Liittovaltiolla on kriisinhallintaa (väestönsuojelua ja katastrofiapua) koskeva laki Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz - ZSKG) 25.3.1997. Lakia on muutettu vuonna 2009, jolloin siihen kirjattiin 18 §:ään väestönsuojelua koskeva pakollinen riskianalyysi. Tämän lisäksi jokaisella osavalttiolla on oma lainsäädäntönsä, joka löytyy Väestönsuojelu- ja katastrofisuojelevirasto Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK:n) ylläpitämältä koontisivustolta verkosta. Osavaltioiden lainsäädäntö kattaa kriisien ennaltaehkäisyn sekä suurien ihmismäärien, eläinten, ympäristön, huomattavan omaisuuden sekä väestön elintärkeiden toimintojen turvaamisen ja suojelun kriisitilanteissa. (Esim. Baijerin katastrofisuojelelaki Bayerisches Katastrophenschutzgesetz BayKSG 24.7.1996 BayRS 1 §)	Ajankohtainen, keskeinen ja kiinnostusta globaalistakin herättänyt hanke on "Itsenäinen Runet"-hanke (laki 01.05.2019/90-FZ "On amendments to the federal law on communications" sekä "On information, information technologies and information protection").	Data Embassy Under Public International Law: Sopimus tieto- ja tietojärjestelmien ylläpidosta Viron tasavallan ja Luxemburgin suurherttuakunnan välillä. (Eesti Vabariigi ja Luksemburgi Suurhertsogiiriigi vaheline andmete ja infosüsteemide majutamise kokkulepe) (lähde) Emergency Act määrittää oikeusperustan kriisinhallinnalle, mukaan lukien hätätilanteiden valmistelu ja reagointi, sekä varmistaa elintärkeiden palvelujen jatkuvan toiminnan. (Emergency Act (n 35) § 1 (1)) State of Emergency Act Kyberturvallisuuslaki (Cybersecurity Act) Electronic Identification and Trust Services for Electronic Transactions Act RIA valvoo palveluntarjoajille asetettujen vaatimusten noudattamista. Agreement on housing data and information systems between the Republic of Estonia and the Grand Duchy of Luxembourg (16/05/2018) Emergency Act (Cyber Security)	Valmiuslaki (1552/2011) Laki huoltovarmuuden turvaamisesta (1390/1992) Laki valtioneuvoston tilannekeskuksesta (300/2017)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
								Strategy 2019-2022: lähde Cyber Security Act (Cyber Security Strategy 2019-2022: lähde)	
Varautumisen ja jatkuvuuden hallinnan strategiset linjaukset		Critical Infrastructure Resilience Strategy: Plan (lähde) Critical Infrastructure Resilience Strategy: Policy Statement (lähde) Critical Infrastructure Resilience Strategy		Israel National Cyber Directorate (INCD) on julkaissut konseptin, jonka avulla organisaatiot voivat kehittää omia kybervarautumissuunnitelmiaan (National Concept for Crisis Preparedness and Management). Ohjeen tavoitteena on määritellä siviili- ja kybertoimintaympäristön varautumisen ja kriisinhallinnan periaatteet ja toimintatavat.	Tieto- ja kyberturvallisuusstrategia edellyttää, että yhteiskunnallisesti tärkeiden toimijoiden tulee laatia jatkuvuus- ja varautumissuunnitelmia kyberuhkien varalle.	Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) eli Kansallinen strategia kriittisen infrastruktuurin suojelemiseksi vuodelta 2009. Kriittiseen infrastruktuuriin kuuluvat strategian mukaan: - energiahuolto - tieto- ja viestintäteknikka - liikenne - juomavesi ja viemärintä - terveydenhuolto, ravitsemus elintarvikehuolto - häätä- ja pelastuspalvelut, katastrofeihin varautuminen - parlamentti, hallitus, hallinto, oikeuslaitos - rahoitus- ja vakuutus-toiminta - media (joukkoviestimet) ja kulttuuriperintö	Runet-hankkeen tarkoituksena on mahdollistaa Venäjän Internetin kontrolli ja toiminta muusta maailmasta riippumatta, mikä edellyttää tietoliikenneoperaattoreilta ja keskeisten järjestelmien rakentajilta pitävyyttä infrastruktuuriin ja tietoon, joka on käytettävissä, vaikka Venäjä erottaa tai päättää irtautua muun maailman Internetistä. Tietoverkkojen ja kriittisen digitaalisen infrastruktuurin toiminnan takaamisessa painotetaan erityisesti valtiolliseen infrastruktuuriin.	Data suurlähetystö on Viron hallituksen pilven jatko, mikä tarkoittaa, että Viron valtio omistaa palvelinresursseja rajojensa ulkopuolella. (lähde) Viro on määritellyt toimintoja valtion digitaalisen jatkuvuuden varmistamiseksi tilanteissa, jossa se on menettänyt hallintonsa alueestaan. (National Security Concept 2017) Varmistaa elintärkeiden palvelujen jatkuvuus ja merkittävien häiriöiden estäminen (Cyber Security Strategy 2019-2022 (lähde)).	Yhteiskunnan turvallisuusstrategia 2017 (YTS)
Mitkä ovat valtion jatkuvuuden hallinnan painopisteet?	Kriittisen infrastruktuurin tärkeimpiä prosesseja (A-tärkeysluokka) ovat energian tuotanto ja jakelu, juomaveden saanti, turvallisuus (lähde). Digitaalinen turvallisuus ei suoranaisesti kuulu kriittisen infrastruktuurin prosesseihin,	Kriittisen infrastruktuurin osa-alueet ovat pankki- ja rahoitustoiminta, hallinto, viestintä, energia, ruoka ja päivittäistavarat, terveys, kuljetukset ja vesihuolto.	Yhteiskunnan häiriönsietokyky (resilience) koostuu infrastruktuurin ja yhteisöjen kestävydestä sekä organisaatioiden jatkuvuuden hallinnan tehokkuudesta. Yritysten toiminnan jatkuvuuden varmistaminen on keskeinen osa koko	Kansallinen kyberkonsepti määrittelee siviiliyhteiskunnan kybertoimintaympäristön puolustamisen perusteet (varautuminen ja kriisinhallinta). Ohjeessa määritellään yhteiset käsitteet ja se ohjaa jatkuvuuden ja varautumisen hallintajärjestelmien	MSB:ssä on kyberturvallisuuden ja viestintäyhteisöjen turvaamisen osasto (Avdelningen för cybersäkerhet och säkra kommunikationer). Kriisivarautuminen ja siviilipuolustus on organisoitu omaksi osastokseen samoin	Väestönsuojelu sekä valtionhallinnon toiminnan jatkuvuuden varmistaminen		Viro valvoo kyberavaruuttaan ja tarkkailee tietoturva-vaatimusten soveltamista hallituksen ja elintärkeiden palveluntarjoajien tietojärjestelmiin. (National Security Concept)	Yhteiskunnan elintärkeiden toimintojen turvaaminen.

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	mutta kansallisessa riskiarviossa kyberuhkien kytkentä kriittiseen infrastruktuuriin on tunnistettu niin fyysisessä kuin digitaalisessa toimintaympäristössä. Digitalisaatiostrategiassa nostetaan kyberturvallisuuden merkitys digitaalisen yhteiskunnan häiriönsietokyvylle (resilience). Valtiotoimijoiden aiheuttamia uhkia pidetään suurina, eikä häiriönsietokyky ole riittävä kaikilla toimialoilla. Digitaalisille palveluille ei ole käytännössä lainkaan vaihtoehtoisia toimintatapoja. (lähde)		yhteiskunnan varautumista. (lähde)	rakentamista organisaatioissa. (lähde)	kuin pelastustoiminta. (lähde). Lainsäädännössä tai strategioissa ei ole erikseen määritelty digitaalisen yhteiskunnan varautumista vaan se sisältyy osana Ruotsin kokonaispuolustuksen konseptiin. (lähde)				
Kuka on vastuussa varautumisesta ja jatkuvuuden hallinnasta?	National Coordinator for Security and Counterterrorism (NCTV) vastaa terrorismin torjunnasta, kyberturvallisuudesta, kansallisesta turvallisuudesta ja kriisinhallinnasta. NCTV keskittyy yhteiskuntaa kohtaavien häiriöiden estämiseen ja häiriöiden vaikutusten minimointiin. (lähde) NCTV pitää yllä oris.nl -sivustoa, josta löytyy ohjeita erilaisen häiriötilanteiden varalle. National Cyber Security Centre (NCSC) mm. tukee elintärkeiden palvelujen tarjoajien ja julkishallinnon organisaatioiden jatkuvuuden kehittämistä. Se mm.	Sisäasiainministeriö (Department of Home Affairs) on Australian hallinnon johtava viranomainen kriittisessä infrastruktuurissa. Sisäasiainministeriö on vastuussa Critical Infrastructure Centrestä ja Trusted Information Sharing Networkista (TISN). (lähde) Kriittisen infrastruktuurin vastuut on määritelty kriittisen turvallisuuden strategiassa (lähde; liite B)	The Cabinet Office on julkaissut BS25999-standardiin perustuvan ohjeen (Business Continuity Management Toolkit) tukemaan yritysten ja organisaatioiden jatkuvuuden hallintaa. The National Security Secretariat kehittää valtion kykyä sietää häiriöitä ja toipua niistä. Virasto vastaa Iso-Britannian kyberturvallisuuden strategiasta johtamisesta. Local resiliency forums (LRF) ovat alueellisia ja poikkihallinnollisia varautumisorganisaatioita. Niitä on yhteensä 42 Englannissa, Walesissa, Skotlannissa ja Pohjois-Irlannissa. LRF:llä ei ole	National Preparedness Center, joka on osa INCD:tä. (lähde) Ministry of Financen alaisuuteen on perustettu The Cyber and Finance Continuity Center (FC3) vuonna 2017. FC3 vastaa rahoitusalan palveluiden (financial services) jatkuvuudesta ja häiriönsietokyvyn vahvistamisesta. (lähde)	Hallitus määrittää vuosittain annettavalla ohjeella MSB:n tavoitteet, raportointivelvoitteet ja resursit. MSB:n johtajan nimittää Ruotsin hallitus. MSB vastaa onnettomuuksiin ja kriiseihin varautumisesta, tietojen ja kyberturvallisuudesta sekä siviilipuolustuksesta. Se toimii myös Ruotsin yhteyspisteenä muiden maiden vastaavien toimijoiden ja toimintojen kanssa. MSB:n tehtäviin kuuluu laajasti muiden viranomaisten ja yritysten tukeminen varautumiseen liittyvissä asioissa (lähde). Kukin lääninhallitus (länsstyrelsen) hoitaa	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), jonka organisaatiokaaviosta näkyvät viraston toimialueet. Viraston tehtävinä on: hoitaa liittohallituksen pelastuspalvelun tehtävät koordinoida kriittisten infrastruktuurien suojaamista laatia yhteenveto, arvioida ja esitellä laaja valikoima tietolähteitä yhtenäisestä riskitilanteesta koordinoida liittovaltion viestintää osavaltioiden ja kuntien, yksityisen sektorin ja kansalaisten kanssa ennakkovalmistelusta		Puolustusministeriö (MOD) on kyberpuolustuksen koordinoiva viranomainen kansallisesti puolustettavalla alueella. Cyber Command (land forces of the Ministry of Defence) päätehtävänä on suorittaa operaatioita kyberavaruudessa. (lähde) Cyber Command structure The Estonian Internal Security Service (Kaitsepolitsei, KAPO) on tärkeä toimija tietoverkkouhkien havaitsemisessa ja estämisessä. (Annual review 2018)	

Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
koordinoi IT-häiriöiden selvittämistä. NCTV:n alaisuudessa toimii National Crisis Centre (NCC), joka koordinoi valtakunnallisten kriisien hoitamista ja sen yhteistyöverkosto kattaa julkishallinnon lisäksi muut yhteiskunnalliset ja yksityisen sektorin toimijat. NCC:llä on 24/7 palvelutointo, joka toimii kriisitilanteissa tiedottamisen keskuksena. NCC:n toiminnassa ei erikseen korosteta digitaalisen toimintaympäristön kriisinhallintaa.		toimeenpanovaltaa, mutta niiden velvollisuuksiin kuuluu alueellisen riskiarvion ja kaminen ja alueellinen varautuminen erilaisiin kriiseihin. (lähde)		varautumista omalla maantieteellisellä alueellaan. Yhteiskuntasuunnittelun avulla pyritään vähentämään yhteiskunnan haavoittuvuuksia (lähde).	ja ajankohtaisista uhista tukea liittovaltion joukkojen ja muiden julkisten ja yksityisten resurssien hallintaa laaja-alaisissa hätätilanteissa koordinoida väestön suojaamista joukkotuhosilta järjestää pelastuspalvelun johtamiskoulutusta koordinoida siviiliturvallisuuden alalla kansallista Euroopan yhdentymisprosessia koordinoida liittovaltion, osavaltioiden, palokuntien ja yksityisten avustusrakennusten tehtäviä kansainvälisissä humanitaarisissa tehtävissä ja siviili-sotilaallisessa yhteistyössä. Bundesamt für Sicherheit in der Informationstechnik (BSI) vastaa oman toimivaltansa osalta jatkuvuudenhallinnasta. BBK ja BSI ovat julkaisseet yhteisen verkkosivuston (kooste näiden kahden viraston aiheeseen KRITIS-toimintaan liittyvistä sivuista) jatkuvuudenhallinnasta.			
Mikä on yksityissektorin rooli valtion jatkuvuudenhallinnassa?	Digital Trust Center (DTC) on NCTV:n, NCSC:n, keskuskaupakamarin (the Dutch Chamber of Commerce), teollisuustyönantajien (Confederation of Netherlands Industry and	Organisaatiot mukaan lukien yksityinen sektori voivat osallistua TISN:n kautta tiedon jakamiseen kriittisten infrastruktuurin haavoittuvuuksista ja riskien arviointi- ja	Suuri osa valtion kriittisestä infrastruktuurista on yksityisessä omistuksessa. (lähde) Yksityissektorin merkitys valtion kyberturvallisuuden ja jatkuvuuden hallinnan	Toimialoitain voidaan asettaa kansallista kyberturvallisuuden tilaa korkeampi hälytystila, mutta ei matalampaa. Kansallinen taso velvoittaa kaikkia toimijoita osallistumaan	MSB tekee omalla vastuualueellaan yhteistyötä myös yksityissektorin toimijoiden kanssa. (lähde)	Osallistuu mm. LÜKEX-kriisinhallintaharjoituksiin sekä käytännön toimintaohjeiden valmisteluun julkishallinnon kanssa, esim. (Schutz Kritischer Infrastrukturen –		Huoltovarmuusorganisaatioon osallistuu sektori- ja poolitoiminnan kautta huoltovarmuuskriittisiä yrityksiä. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	Employers, VNO-NCW) ja muiden järjestöjen ylläpitämä yhteisö, jonka tehtävänä on mm. jakaa yrityksille NCSC:n tuottamaa kyberturvallisuuden uhkakuva ja ylläpitää kyberturvallisuuteen liittyvien asioiden tiedonjakoalustaa. (lähde)	hallinnointitekniikoista. (lähde)	kehittämisessä nähdään tärkeäksi, koska NCSC:llä ei ole toimeenpanovaltaa edes NIS-direktiiviin liittyvissä asioissa. (lähde; kohta 84)	yhteiskunnan kyberpuolustukseen. Jokaisen organisaation vastuulla on luoda kriisinhallinnan menettelyt omien kyberuhkamalliensa ja riskiarvioidensa perusteella. Menettelyissä on huomioitava osaaminen, resurssit, teknologiat, organisaation ulkopuolinen tuki ja harjoittelu. (lähde)		Risiko- und Krisenmanagement Leitfaden für Unternehmen und Behörden UP KRITIS (Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland) Yksityissektori voi liittyä jäseneksi UP KRITIS -yhteenliittymään. Osallistuminen on ilmaista ja vapaaehtoisia. UP KRITIS on julkisen ja yksityisen sektorin yhteistyöelin elintärkeiden infrastruktuurien ylläpitäjien (KRITIS), alan järjestöjen ja asianomaisten valtion viranomaisien välillä. UP KRITIS -toiminta kattaa KRITIS-lainsäädännön yhdeksästä ryhmästä kahdeksan. Ks. ylempänä kriittisen infrastruktuurin osa-alueiden luettelo. UP KRITISin organisaatiomallista ilmenee yhteenliittymän toimintatavat. UP KRITIS Grundlagen und Ziele -dokumenttiin vuodelta 2014 on kirjattu yhteenliittymän tavoitteet ja toiminnan perusta.			
Kuka määrittelee valtion kriittiset digitaaliset resurssit ja tietovarannot?	NCTV ylläpitää listaa kriittisen infrastruktuurin prosesseista . Jokainen ministeriö on velvollinen tunnistamaan ja luokittelemaan omat kriittiset prosessinsa. Suoranaisesti digitaalisen turvallisuuden	Critical Infrastructure Centre tunnistaa kriittisimmän infrastruktuurin ja sisäasianministeriö määrittää kriittisen infrastruktuurin suojattavat kohteet. (lähde) (lähde)	Centre for the Protection of National Infrastructure (CPNI) jakaa kansallisen infrastruktuurin kolmeentoista sektoriin, joihin kuuluvat mm. tiedonvälitys (ml. tietoliikenne), energia, rahoitus, puolustus ja hallinto.	INCD	Digitalisaatiostrategiassa (osatavoite D-infrastruktuur) korostetaan tietoliikenteen ja erityisesti laajakais-tayhteyksien merkitystä. Sekä ”kovan” (kaapelointi, mastot, jne.) että ”pehmeän” (mm. lait, standardit	BSI		Kriittisen tietoinfrastruktuurin suojauksen (CIIP) tehtävänä on ylläpitää maan tärkeiden tieto- ja viestintäjärjestelmien ongelmatonta toimintaa. The Information System Authority (RIA)	

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	teemaan liittyviä prosesseja ovat Internet ja tietoliikenne, henkilö- ja yritystietorekisterit, tietorekisterien väliset kytkennät sekä sähköinen viestintä ja kansalaisten tiedonsaanti.		Kriittisiä digitaalisia resursseja tai tietovarantoja ei ole erikseen nimetty.		ja protokollat) digitaalisen infrastruktuurin elementit on mainittu tässä strategiassa.			järjestää kansallisella tasolla Viron valtion toiminnalle välttämättömien julkisen ja yksityisen sektorin verkkojen ja tietojärjestelmien suojausta (lähde) Yhteiskunnalle välttämättömät palvelut määritellään kyberturvallisuuden laissa, alajaksossa 3 Cybersecurity Act .	
Kuka on vastuussa kriittisten digitaalisten resurssien jatkuvuudesta?	NCSC Dutch Continuity Board (DCB) on teleyritysten operatiivinen yhteistyöverkosto, joka pyrkii torjumaan ja vähentämään ICT-palveluihin kohdistuvia uhkia (esim. DDoS-hyökkäykset).	Australian Cyber Security Centre (lähde)	Kriittisen infrastruktuurin (Critical National Infrastructure) turvaaminen kuuluu Cabinet Officen toimivaltaan. (lähde) Centre for Protecting National Infrastructure (CPNI) on MI5:n alainen viranomainen, jonka tehtävänä on vähentää yhteiskunnan haavoittuvuuksia. (lähde) Valtion tärkeimpien julkisten ja yksityisten palvelujen turvaaminen on keskeinen turvallisuusstrategian osa. Turvallisuuden ja häiriönkeston (resilience) sektorikohtaiset periaatteet ja vastuut on kuvattu Cabinet Officen julkaisemassa dokumentissa Public Summary of Sector Security and Resilience Plans .						
Mitä viitekehyksiä käytetään?	Julkishallinnon jatkuvuudenhallinnan viitekehyksiä ei tunnistettu.	Strategies to Mitigate Cyber Security Incidents (lähde) Australian Government Information Security Manual (lähde)	BS 25999-1:2006 (Business Continuity Management. Code of Practice) BS 25999-2:2007 (Specification for Business Continuity Management)	Government Plans, 2017-2018 (lähde)	EU-direktiivien pohjalta on laadittu kansallinen lainsäädäntö, jonka perusteella on annettu viranomaisille varautumiseen liittyviä tehtäviä. Lainsäädännössä tai strategisissa linjauksissa ei	Pelastuspalvelun ja katastrofiavun liittovaltion virasto (BBK) on kehittänyt menetelmän väestönsuojelun riskianalyysiin. Riskianalyysin menetelmä julkaistiin sisäasiainministeriön			Toiminnan jatkuvuuden hallinta (VAHTI 2/2016; pohjautuu ISO22301-standardiin) ICT-varautumisen vaatimukset (VAHTI

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
		National Plan to Combat Cyber Crime (lähde)			nimetä käytettäviä jatkuvuuden hallinnan viitekehyksiä. MSB:n jatkuvuudenhallinnan ohje perustuu ISO22301-standardiin.	Saksan liittopäiville antamissa lakisääteissä raporteissa vuonna 2010 ja 2011. Viitekehystä on testattu useissa pilotti-projekteissa ja näiden pohjalta päivitetty. Menetelmä liitteineen (työkaluineen löytyy) BKK:n verkkosivuilta . Ks. myös Risikoanalyse im Bevölkerungsschutz - Ein Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz Menetelmä on kehitetty kansainvälisten tieteellisten havaintojen perusteella ja se perustuu kansainväliseen riskinhallintastandardiin ISO 31000 ja 31010. Menetelmää tarkistetaan ja kehitetään jatkuvasti. Menetelmällä voidaan kaikilla hallinnollisilla tasoilla suorittaa riskianalysit kullakin vastuualueella, joiden tulokset ovat perustana päätöksenteolle riskien- ja kriisinhallinnassa. Jatkuva vaihto liittovaltion ja osavaltioiden välillä BKK:n verkostojen kautta tukee vuorovaikutusta ja näkemysten jakamista. (lähde)			2/2012; perustuu kansallisiin viitekehyksiin)
Kuka ylläpitää valtion tason tilannekuvaa?	NCTV seuraa sekä fyysisen että digitaalisen toimintaympäristön uhkia, riskejä ja haavoittuvuuksia.	Australian Cyber Security Centre. ACSC:llä on computer emergency response team (CERT). (lähde)	GCHQ (lähde) CPNI arvioi kriittisen infrastruktuurin uhkia (lähde)	INCD:n johtaja päättää kansallisen kyberhälytystilan tassist. (lähde)	MSB:llä on tehtävä ylläpitää tilannekuvaa sekä ennaltaehkäisevästi että tietoturvaongelmien selvittelyn	ZSKG:n 18 §: n 1 momentin 2 lauseen nojalla liittovaltion sisäministeriö raportoi vuodesta lähtien 2010 Saksan liittopäiville riskianalysien		The Information System Authority	Laajavaikutteisten häiriötilanteiden hallinnan ja poikkeusolojen tilannekuvasta vastaa valtioneuvoston kansliaan sijoit-

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
					koordinoimiseksi. ("Handling serious IT incidents")	tuloksista. Raportit julkaistaan riskianalyseineen Saksan liittopäivien verkkosivuilla. Vuodesta 2012 seuraaville riskeille on tehty riskianalyysi, ja tulokset on julkaistu vastaavissa Bundestag-raporteissa: 2012: "Erittäin korkea sulamisvesi vuoristo-alueilta" ja "Pandemia Virus Modi-SARS" 2013: "Talvimyrsky" 2014: "Myrskyn nousu" 2015: "Radioaktiivisten aineiden vapauttaminen ydinvoimalaitokselta" 2016: "Kemiallisten aineiden vapauttaminen" 2017: "Aiempien riskianalyysien huomioon ottaminen" 2018: "Kuivuus" Lähde: BKK			tettu valtioneuvoston tilannekeskus. (lähde) Kyberturvallisuuskeskuksella on useita tilannekuvatuotteita organisaatioiden ja kansalaisten käyttöön. (lähde)
Kuka koordinoi valtion harjoitustoimintaa?	NCSC harjoittelee itse IT-häiriöiden varalle ja se osallistuu muiden toimijoiden järjestämiin kansallisiin harjoituksiin. (lähde)	Kriittisen infrastruktuurin toimijoille on tarjolla kansallinen harjoitusohjelma (National exercise program) kyberturvallisuustapahtumien hallinnan tueksi. Ohjelmassa käsitellään mm. strategista päätöksentekoa, operatiivista ja teknistä osaamista sekä viestintää. (lähde)	Cabinet Office ja National security and intelligence julkaisevat ohjeita varautumisharjoitusten järjestäjille. Valtion tason harjoituksia ei koordinoita, mutta Civil Contingencies Act velvoittaa kriisinhallintayksiköitä (Category 1 responders) järjestämään henkilöstöilleen koulutusta ja harjoituksia. Central Government Emergency Response Training (CGERT) koulutusohjelma antaa osallistujille tiedot, taidot ja		MSB:n tehtävänä on järjestää vastuualueensa mukaisia, poikahallinnollisia harjoituksia niin valtakunnallisesti kuin alueellisesti (lähde). Varautumisvelvolliset viranomaiset toimittavat harjoitusohjelmansa MSB:lle, joka kokoaa ne kansalliseen harjoitusohjelmakalenteriin (lähde). Esimerkkinä 2020 MSB:n ja Ruotsin puolustusvoimien järjestämä kokonaispuolustus-	BBK järjestää säännöllisesti ns. Länder- und Ressortübergreifende Krisenmanagementübung (Exercise) eli LÜKEX –kriisinhallintaharjoituksia eri aiheista. (lähde) Velvollisuus järjestää kyseisiä harjoituksia perustuu Zivilschutz und Katastrophenhilfegesetz (ZSKG) 14 §:ään. Vuoden 2011 LÜKEX-harjoituksessa testattiin massiivista kyberhyökkäystä, joka		Valtion harjoitustoimintaa järjestävät valtion viranomaiset, jotka kuuluvat puolustusministeriön ja sisäministeriön toimivaltaan. (lähde)	Puolustusministeriö, turvallisuuskomitea (KYHA) Digi- ja väestötietovirasto (TAISTO) Huoltovarmuuskeskus, Digipooli (TIETO) AVI, Pelastusopisto (alueelliset valmiusharjoitukset) Turvallisuuskomitea (VALHA) Kyberturvallisuuskeskus (FINEST)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
			valmiudet toimia kansallisesti strategisen tason kriisinhallinta-tehtävissä. (lähde)		harjoitus (Totalförsvarsövning 2020). Regeringskansliet järjestää vuosittain useita harjoituksia, joissa hallinto harjoittelee esimerkiksi kriisien, epidemioiden tai terrorismin varalle (lähde).	kohdistui kriittisen infrastruktuurin (KRITIS) yrityksiin sekä julkishallintoon. Harjoituksen aikana testattiin tietoturvan alan tietojenvaihto liittotahallituksen ja liittovaltioiden välillä onnistuneesti ensimmäistä kertaa määritellyillä raportointikanavilla, mikä käynnisti hallinnollisen CERT-verkon perustamisen. (lähde)			
Miten jatkuvuuden hallinnan vaikuttavuutta mitataan?		Australian National Audit Office (ANAO) tekee mm. kyberturvallisuuden häiriönsietokykyyn (cyber resilience) liittyviä tarkastuksia.			MSB:n tehtävänä on tuottaa (tilata) sen vastuualueeseen kuuluvia tutkimus- ja kehityshankkeita sekä varmistaa näiden laatu. Hallitus linjaa vuosittain MSB:n toiminnan painopisteet ja tavoitteet ohjauskirjeellä . MSB:n vuosittain julkaisemassa toimintakertomuksessa kuvataan, miten vaatimukset ovat toteutuneet, mutta varautumisen kypsyystasoa ei toimintakertomuksessa varsinaisesti käsitellä. MSB:n vastuulla on Ruotsin kansallisten, alueellisten ja kansainvälisten harjoitusten järjestäminen ja koordinointi poikkihallinnollisesti. Harjoituksista kerätään kokemuksia säännönmukaisen prosessin kautta. Varautumisen toteutumista yhteiskunnassa seurataan NAFS-foorumissa , joka kokoontuu kerran vuodessa. Harjoitustoiminnassa ei				

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
					käsitellä digitaalista turvallisuutta erikseen.				

Tietoturvallisuus

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Tietoturvaa ohjaava lainsäädäntö		ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	The Protection of Privacy Law (PPL), 5741-1981 (lähde ; ei viranomaislähde) määrittelee tietoturvallisuusvaatimuksia kolmen eri turvatason tietovarannoille (basic, medium ja high security level databases).	Ruotsissa ei ole yhteistä tietoturvaa koskevaa lainsäädäntöä. Alan normit on hajautettu lainsäädäntöön. Järjestelmien ja organisaatioiden omaa tietoturvaa koskevaa velvoittavaa lainsäädäntöä julkishallinnolle on ollut vähemmän kuin Suomessa. Suomen valtionhallintoa koskevaa tietoturva-asetusta vastaa lähinnä Offentlighets- och sekretesslag. Se ei määrittele tiedon luokittelua tai luokkien käsittelyä tarkemmin. Vuonna 2019 voimaan tullut turvallisuslaki (Säkerhetskyddlag) määrittelee tiedon turvaluokittelukriteerejä yleisesti, mutta ei aseta edelleenkaan käsittelyvaatimuksia. Laki koskee periaatteessa muutakin Ruotsin turvallisuu-teen vaikuttavaa toimintaa, eikä vain valtionhallintoa. Elinkeinoelämän tietoturvaa säädellään lainsäädännöllä hajautetusti.	Saksan perustuslain (Grundgesetz GG) 91 c § Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) 14.8.2009 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) 17.7.2015, joka on lakiteknisesti BSIG-lain sekä usean muun lain muutos. Linkki vie alkuperäiseen Saksan säädöskokoelmassa julkaistun muutos-tekstiin, mutta muutos on mm. myös osana ajantasaista BSIG-lakitekstiä. Lisäksi erityislainsäädäntöä kuten Telekommunikationsgesetz (TKG) (Telekommunikaatiolaki) 22.6.2004, Telemediengesetz (Telemedialaki) (TMG) 26.2.2007, Kreditwesengesetz (Luottolaitoslaki) (KWG) 10.7.1961, Wertpapierhandelsgesetz (Arvopaperikauppalaki) (WpHG) 27.6.1994 Saksassa on valmis-teilla ns. IT-Sicherheitsgesetz 2.0 jolla pyritään nostamaan tietoturva-vaatimuksia, ks. lähde	Jarovaja-lakipaketti (Закон Яровой); 374-FZ ja 375-FZ täydentävät aiempia terrorismin vastaisia lakeja ja säättävät mm. teleoperaattoreiden velvollisuuksista tallettaa viestintää koskevia tietoja ja sallia viranomaisille tarvittaessa pääsy salattuun viestiliikenteeseen. Venäjän rikoslain tietoturvaa koskeva kohta: Статья 28. Невиновное причинение вреда International Code of Conduct for Information Security (lähde) on Venäjän ja Kiinan aloitteesta solmittu sopimus, joka pyrkii turvaamaan valtiot ulkoiselta informaatiovaikuttamiselta. YK:n yleiskokous hyväksyi joulukuussa 2018 kaksi Venäjän päätöslauselmaehdotusta ("Developments in the field of information and telecommunications in the context of international security" ja "Countering the use of information and communications technologies for criminal purposes"), joiden tarkoituksena on suojata valtion sensitiivisiä tietoja ja tarjota konkreettisia keinoja kyberrikollisuuden torjuntaan (lähde; ei viranomaislähde).	Valtioneuvoston asetus (nro. 273 of 12 August 2004) määrittelee, että ISKE-standardi on pakollinen valtioneuvoston ja paikallishallinnon organisaatioille, jotka käsittelevät tietokantoja / rekistereitä 12. (lähde) Public Information Act (Avaliku teabe seadus) Tietoturvalisuu-teen liittyvät tietyt teot on kriminalisoitu Rikoslais-ssa. • \$206 Interference with computer data • \$207 Hinder- ing of functioning of computer systems • \$208 Dissemination of spyware, malware or computer viruses • \$216 Preparation of computer-related crime • \$217 Illegal obtaining of access to computer systems Tietojärjestelmien tiedonvaihtokerros X-tee on tekninen ja organisatorinen ympäristö, joka mahdollistaa turvallisen Internet-pohjaisen tiedonvaihdon tietojärjestelmien välillä. (lähde) X-tietä käytetään valtakunnallisesti Viron tiedonvaihtokerroksessa X-tee ja Suomi.fi-tiedonvaihtokerrospalvelussa. (lähde)	Laki julkisen hallinnon tiedonhallinnasta (906/2019) Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvalisuu- den arvioinnista (1406/2011) Laki tietoturvalisuu- den arviointilaitok- sista (1405/2011) Valtioneuvoston ase- tus tietoturvalisuu- desta valtionhallin- nossa (681/2010)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
								RIHA toimii luettelona valtion tietojärjestelmälle. Samalla se on menettelyllinen ja hallinnollinen ympäristö, jonka avulla varmistetaan valtion tietojärjestelmän kattava ja tasapainoinen kehitys. (lähde) Virossa yksityissektorilla on mahdollisuus liittyä X-teen. ISKE on Viron julkiselle sektorille kehitetty tietoturvastandardi. ISKE:n valmistelu ja kehittäminen perustuvat saksalaiseen tietoturvastandardiin - IT Baseline Protection Manual (IT- Grundschutz). Ministeriöt, virastot + rekisterit yhdistetty IS-> ovat velvoitettu suorittamaan IT-auditointi: • H-taso: joka 2 vuosi • M-taso: joka 3 vuosi • L-taso: joka 4 vuosi (lähde) Ohjekirja (lähde) ISKE auditointimanuaali (lähde)	
Mitkä ovat lain-säädännön merkittävimmät havainnot digitaalisen turvallisuuden näkökulmasta?		ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)		Ruotsissa viranomaisilla on pakollinen raportointivelvollisuus IT-poikkeamista keskitetysti MSB:lle. Ruotsissa ei ole tietoturvasojen, VAHTIn tai Katakrin kaltaisia hallinnon asettamia yksityiskohtaisia määrittelyjä julkishallinnon tai elinkeinoelämän tietoturvalle, tai kattavia velvoitteita tai	Valtion ja liittovaltion viranomaisjärjestelmien ja verkkojen tietoturva on nostettu perustuslain tasolle. Perustuslain 91 c §:ssä säädetään Saksan liittovaltion ja osavaltioiden tietoteknisistä järjestelmistä. Pykälän 2 momentin mukaan liittovaltio ja osavaltiot voivat sopimuksella vahvistaa tietotekniikka-	Venäjän kyberturvallisuuden politiikan mukaan valtion velvollisuus on suojata sekä infrastruktuuria että informaatiota (lähde) (lähde; ei viranomaislähde). Venäjä ei ole allekirjoittanut Euroopan neuvoston “Convention on Cybercrime” -sopimusta. Venäjän mielestä sopimuksen		

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
					hankkeita niiden nou- dattamiseksi ja tar- kastamiseksi.	järjestelmiensä väli- seen viestintään tar- vittavat standardit ja turvallisuusvaatimuk- set.	alekirjoittaminen vaa- rantavan kansallista itseäänäämisoi- keutta (lähde). Venäjä ei osallistu ETYJ:n hankkeeseen, jossa kehitetään kan- sainvälistä kyberhyök- käysten ennakko- roitusjärjestelmää (lähde).		
Tietoturvaa kos- kevat strategiset linjaukset		Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Iso-Britannia)			Strategiset tietoturva- linjaukset on koottu sisäasiainministeriön julkaisemaan Umsetzungsplan Bund 2017 - Leitlinie für Informationssicherhei t in der Bundesverwaltung . (UP Bund 2017) -do- kumenttiin. Umsetzungsplan (to- teutus suunnitelma) sisältää vuoden 2016 kyberturvallisuusstra- tegian käytännön si- tovat ja yhtenäiset soveltamisohjeet. Sitä sovelletaan kaik- kiin ministeriöihin ja liittovaltion viranomai- siin.	Venäjän digitaalisen talouden ohjelman (Digital Economy of the Russian Federa- tion) (lähde) mukaan vakavimmat digitaali- sen talouden kehitty- misen esteet ovat kansallisen ja kan- sainvälisen kyberrikol- lisuuden lisääntyminen, ulkopuolisten toimijoiden lisäänty- nyt toimintakyky ja ICT-turvallisuusasian- tuntijoiden puute. (lähde , analyysi tällä). Ohjelma mää- rittelee järjestelmien omistajille ja valtiolli- sille toimijoille pakolli- sia tehtäviä: kriittisen digitaalisen infrastruktuuriin (criti- cal information infra- structure) turvallisuus- den ja vakaan toimin- nan parantaminen kyberuhkien havaitse- misen ja torjumisen keinojen kehittämi- nen ja häiriöiden seu- rausten eliminointi kansalaisten ja alueit- ten suojaaminen kriit- tisen infrastruktuuriin kohdistuvien ky- berhyökkäysten seu- rauksilta ICT-rikollisuuden tor- junta ja rikolliseen		Suomen tietoturvali- suusstrategian (2016) tavoitteina ovat: 1) Suomessa on digi- taaliset liiketoimin- nan kannalta kilpailu- kykyinen ja edistyk- sellinen lainsäädäntö 2) EU:n sisämarkkinat toimivat nykyistä luo- tettavammin 3) suomalaiset yrityk- set hyötyvät kansain- välisistä standar- deista ja markkinoilla on saatavilla digitaali- sia hyödykkeitä, joi- den tietoturva on si- säänrakennettua 4) tietoturva ja sii- hen liittyvää osaa- mista tutkitaan, mita- taan, seurataan ja ke- hitetään 5) Viranomaiset autta- vat yhteisöjä ja kansa- laisia tietoturvan pa- rantamisessa (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
							toimintaan vastaaminen (vrt. Venäjän tietoturvallisuuskoktriini, 2016) Venäjän digitalisaatio-, tietoliikenne- ja joukkoviestintäministeriö (digiministeriö) muokkaa kansallisen digitaalisen talouden ohjelman toteuttamiseen varataan yli biljoona ruplaa vuoteen 2024 asti. Noin 1,6 miljardia ruplaa käytetään digitaalisen toimintaympäristön regulaation toteuttamiseen, yli 413 miljardia ruplaa informaatioinfrastruktuuriin, noin 140 miljardia ruplaa digitaalisen talouden henkilöstöön ("Human Reserves for the Digital Economy"), yli 280 miljardia digitaaliin teknologioihin ja noin 226 miljardia digitaalisen hallinnon kehittämiseen. Tietoturvallisuuteen on varattu noin 18 miljardia ruplaa (lähde). Venäjä on tehnyt vuodesta 1998 lähtien YK:n yleiskokoukselle ICT-järjestelmien turvallisuuteen liittyviä ehdotuksia. 2011 Venäjä alkoi yhdessä Kiinan kanssa kehittää kansainvälistä tietoturvallisuuden toimintatapaa (International Code of Conduct for Information Security) (lähde). Fundamentals of the state policy of the Russian Federation in the field of international information		

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
							security for the period until 2020		
Mitkä ovat valtion tietoturvan painopisteet?	ks. Kyberturvallisuus (Alankomaat)	ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Israel)	Ruotsin digitalisointi-strategia asettaa vaatimuksia tietoturvan kehittämiselle. Painopistealueita ovat mm. digitaalinen identiteetti, viranomaisten oma tietoturva, kansalaisten sekä pienten ja keskisuurten yritysten tietoturva ja kuntien tietoturva. (lähde)	UP Bund 2017 -dokumentin mukaan valtion tietoturvan painopistealueina ovat mm. tietoturvan hallintajärjestelmien implementointi BSI-standardien pohjalta, tietoturvan minimistason varmistaminen, liittovaltion viranomaisten käyttämien tietojärjestelmien suojaaminen oikeudettomilta hyökkäyksiltä ja tiedon häviämiseltä sekä virka- ja liikesalaisuuksien suojaaminen.	Ks. Strateginen riskienhallinta (Venäjä)		Suomen tietoturvallisuusstrategia (2016) painottaa Suomen digitaalisen talouden kilpailukyvyyn parantamista ja vientiedellytysten varmistamista. (lähde)
Kuka on päävastuussa valtion tietoturvallisuuden kehittämisestä?	Alankomaiden kyberturvallisuuskeskus (NCSC) vastaa kyberturvallisuudesta. Terminologiassa "kyberturvallisuus" kattaa digitaalisen turvallisuuden osa-alueista sekä tieto- että kyberturvallisuuden.	ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Israel)	Ruotsissa tietoturvan kehittämistä hoitavat eri toimijat varsin itsenäisesti yhteistyöhön perustuen. Keskitettyä pakottavaa lakiin perustuvaa ohjausta on vähän. Ruotsissa samat tahot säilyttävät tehtävänsä myös kriisikaikoina. Oikeusministeriön alla toimiva Myndigheten för samhällsskydd och beredskap (MSB) vastaa yleisemmin tietoturvasasioista, ei vain jatkuvuuden ja kriisivalmiuden näkökulmasta. Toiminta-ala kattaa myös aluehallinnon ja elinkeinoelämän. MSB ei voi kriisitilanteessakaan käyttää muita, vaan valta pysyy hajautettuna, kuten normaalioloissakin. (lähde)	Tietotekniikan liittovaltion turvallisuusviraston on tarkoitus saada uusia valtuuksia ja tulla yhä enemmän hakkerointiviranomaiseksi. Tämä on kirjattu sisäministeriön lakiesitykseen. Viraston tulisi hakkeroida vaarallisia järjestelmiä ja poistaa tietoja etäyhteyden kautta. Sisäministeri Horst Seehofer haluaa rakentaa liittovaltion tietoturvaviraston hakkerointiviranomaiseksi. Tulevaisuudessa BSI:n ei pitäisi enää puolustaa ja neuvoa itseään puolustavasti, vaan aggressiivisesti tunkeutua IT-järjestelmiin. Sen pitäisi olla "tietoturvalaki 2.0" -sivustolla, jos se menee sisäministeriöön. Sisäasiainministeriö on antanut 27.3.2019 uuden lakiehdotuk-	Ks. Perustiedot, hallinto ja resurssit (Venäjä)		Varsinaista päävastuullista on vaikea nimetä, koska vastuita on hajautettu monelle toimijalle (VM, LVM, PLM, Digi- ja viestintävirasto, Traficom, Kyberturvallisuuskeskus, Turvallisuuskomitea).

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						sen, jolla BSI:lle annettaisiin nykyistä huomattavasti laajemmat valtuudet puuttua			
Mikä on yksityissektorin rooli valtion tietoturvasuuden kehittämisessä?	ks. Kyberturvallisuus (Alankomaat)	ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Israel)		Antaa mm. lausuntoja lakiesityksiin ja osallistuu julkiseen keskusteluun. Myös mukana Allianz für Cyber-Sicherheitin sekä Cyber-Sicherheitsratin toiminnassa.	Tietoliikenneoperaattoreille on säädetty velvoitteita tukea viranomaisia.		
Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?	ks. Kyberturvallisuus (Alankomaat)	ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Israel)	MSB:n Avdelningen för cybersäkerhet och säkra kommunikationer ylläpitää sivustoa Informationssakerhet.se , joka on valtion pääasiallinen kanava tiedottaa verkossa koko yhteiskunnan tietoturvan kehittämisestä. Osaston vastuulla on koordinoita häiriöitä ja ongelmatilanteita kansallisella tasolla kansainvälisen Computer emergency response team (CERT) -yhteistyön ja FIRST- ja TF-CSIRT-yhteistyön puitteissa. Samverkansgruppen för informationssäkerhet (SAMFI) on yhteistyöverkosto, joka toimii MSB:n alaisuudessa ja kehittää tietoturvaan liittyvien organisaatioiden yhteistoimintaa. Lisäksi MSB ylläpitää toimialakohtaisia Forum för informationsdelning (FIDI) -foorumia. Regeringskansliet edistää ja koordinoi omalta osaltaan koko	Ks. Kyberturvallisuus	Kansallisen turvallisuuspalvelun (Federal Security Service, FSS) alaisuuteen on perustettu kansallinen koordinaatiokeskus (National Coordination Center, NCC), joka käsittelee ICT-häiriöitä ja suojaa kansallisia tietoresursseja. Ensisijainen vastuu kyberhyökkäysten havaitsemisesta ja torjumisesta on siten FSS:llä (lähde). Venäjän keskuspankki perusti rahoitussektorin CERT-toiminnon (FinCERT) vuonna 2015. FSB:n perustaman National Coordination Center for Computer Incidents (NCCTC) on NCC:n toimivaltainen osa, joka vastaa mm. Internetin .RU -toimialueesta (domain). Sillä on oikeus estää pääsy verkkosivustolle . Venäjän viranomaiset käyttävät suljettua valtionhallinnon verkkoa (RSNet).	Kansallisen turvallisuusviranomaisena (NSA), Se ohjaa kansallista toimintaa ja vastaa muun muassa kansainvälisten tietoturvasopimusten valmistelusta. Traficom NCSA-toiminto vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsitteelyyn liittyvistä turvallisuusasioista. (lähde) Kyberturvallisuuskeskuksen CERT-toiminnon tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturvaasioista. (lähde) Ministeriöt vastaavat tietoturvasuudesta omilla hallinnaloillaan.	

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
					maan tietoturvan kehittämistä erityisesti valtionhallinnon näkökulmasta. Ruotsin puolustusministeriö (Försvarsdepartementet), on aktiivinen tietoturva-asioissa. Ministeriön alla toimiva Försvarets radioanstalt (FRA) tekee signaalitiedustelua ja sillä on oikeus tarkkailla ja kuunnella kaikkea Ruotsin läpi kulkevaa Internet-liikennettä pääasiassa terrorismin ja järjestäytyneen rikollisuuden torjumiseksi.				
Miten tietoturvaa valvotaan ja arvioidaan?	ks. Kyberturvallisuus (Alankomaat)	ks. Kyberturvallisuus (Australia)	Ks. Kyberturvallisuus (Iso-Britannia)	Ks. Kyberturvallisuus (Israel)	MSB:lle on syyskuussa 2019 annettu tehtäväksi laatia rakenne, jonka avulla seurataan julkishallinnon tieto- ja kyberturvallisuustyötä (lähde)	BSI valvoo valtionhallinnon organisaatioiden tietoturvaa. BSI:n yksikkö Nationales IT-Lagezentrum (Kansallinen IT-tilannekeskus) on liittovaltion virastojen, kriittisten infrastruktuurien ja yhteistyökumppaneiden käytettävissä päivittäin 24 tuntia vuorokaudessa. IT-tilannekeskus analysoi päivittäin yli 80 avoimen ja luottamuksellisen lähteen tietoturvaa. Lisäksi se tarkkailee julkisen hallinnon verkkoja ja kumppaniverkkoja sekä liittovaltion hallintoviranomaisten 100 tärkeimmän verkkosivuston saavutettavuutta. Nämä tiedot kootaan kuukausiraporttiin. Kansallinen IT-tilannekeskus ylläpitää yhteyksiä kansallisiin ja kansainvälisiin kumppaneihin CERT-Bundin kautta.	FSS:n/NCC:n GosSOPKA-ohjelman tarkoitus on kytkeä yritykset havainnointijärjestelmään, jonka tarkoituksena on estää ja torjua tietomurtoja (lähde). Järjestelmän on kehittänyt FSB ja vuonna 2015 julkaistun kuvauksen mukaan järjestelmä jatkautuu käsittelykeskuksiin (response center), jotka hajautetaan alueellisesti ja eri ministeriöihin. Venäjä on ottamassa käyttöön kriittisen infrastruktuurin lainsäädäntöä, joka velvoittaa toimijoita jakamaan tietoa GosSOPKA-järjestelmässä (lähde).		Venäjä on virallisesti ottanut käyttöön kansalliset ja toimialakohtaiset kyberturvallisuuden viitekehykset julkishallinnon virastojen toiminnan arvioinnissa ja

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						Kansallinen IT-tilanne-keskus tarjoaa johtoraportteja, taustatietoja IT-tietoturvatapahtumista ja haavoittuvuustietoja / varoituksia kansalliselle kyberpuolustuskeskukselle (Nationales Cyber-Abwehrzentrum). Kyberpuolustuskeskus tekee mm. pitkäaikaisia tilanneanalyyskejä. (lähde) Liittovaltion viranomaisten on nimetty tietoturvas- taava (IT-Grundschtz- zissa käytetty termi Informationssicherheitsbeauftragter). Teh- tävään valittavan hen- kilön kelpoisuusvaati- muksia ja tehtäviä ku- vataan BSI-standardin 200-2 luvussa 4.4.	hyväksynnässä (Re- solution of the Gov- ernment of the Rus- sian Federation No.608, June 26, 1995 "On certification of information protec- tion tools", lähde)		
Raportoidut tieto- turvapoikkeamat	ks. Kyberturvallisuus (Alankomaat)		Ks. Kyberturvallisuus (Iso-Britannia)		MSB:lle raportoitin vuonna 2018 yh- teensä 297 vakavaa tietoturvatapahtumaa (lähde)	BSI on kehittänyt IT- Grundschtz -tietotur- van hallintamallin. Siitä julkaistiin päivi- tetty versio loka- kuussa 2017. BSI- standardit ovat olen- nainen osa IT- Grundschtz -mene- telmää. Ne antavat suosituksia menetel- mistä, prosesseista ja menettelyistä sekä lä- hestymistavoista ja toimista tietoturvan eri näkökohtia varten. Valtion virastojen ja yritysten käyttäjät sekä valmistajat tai palveluntarjoajat voi- vat käyttää BSI-stan- dardeja liiketoiminta- prosessiensa ja tie- tonsa turvallisuuden parantamiseksi.	Venäläiset yritykset ovat menettäneet yli 116 miljardia ruplaa (noin 2 miljardia USD) vuonna 2017. Venä- jän keskuspankin mu- kaan venäläisten pankkien myöntä- mien maksukorttien käyttö luvattomissa maksutapahtumissa ylitti 1,3 miljardia rup- laa vuonna 2018 (lähde).		2018: "HÄIRIÖMÄÄ- RÄT: VAKAVIA 41 MERKITTÄVIÄ YH- TEENSÄ 67" (lähde) Teleyritysten käsitte- lemiä tietoturvahäiriö- tapauksia vuonna 2018 yli 310.000 ja merkittäviä tietoturva- loukkauksia yksi- toista. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						BSI-standardi 200-1 määrittelee yleiset vaatimukset tietoturvan hallintajärjestelmälle (ISMS). Se on yhteensopiva ISO 27001 -standardin kanssa ja ottaa huomioon muiden ISO-standardien, kuten ISO 27002, suositukset. BSI-standardi 200-2 muodostaa perustan BSI-menetelmälle tietoturvan hallintajärjestelmän (ISMS) rakentamiseksi. BSI-standardi 200-3 sisältää riskienhallintamenetelmät. BSI:n vuosittain julkaisemassa Die Lage der IT_Sicherheit in Deutschland -raportissa on useita Saksan tietoturvaan liittyviä tilastoja ja analyyskejä, jotka koskevat sekä julkishallintoa että yksityissektoria. Mutta raportissa ei ole yksiselitteistä tietoa siitä, kuinka paljon tietoturvapoikkeamia raportoidaan viranomaiselle vuosittain.			

Kyberturvallisuus

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Kyberturvallisuutta ohjaava lainsäädäntö	Cybersecurity Notification Obligation Act (Wet gegevensverwerking en meldplicht cybersecurity, Wgmc) korvautuu lähiaikoina uudella lailla (Cybersecuritywet, Csw) Computer Crime Act III (Wet Computercriminaliteit III) Network and Information Systems Security Act (Wet beveiliging netwerken informatiesystemen, Wbni) on NIS-direktiivin kansallinen versio. Se on tullut voimaan 9.11.2018. Intelligence and Security Services Act 2017	Telecommunications and Other Legislation Amendment Act No. 111 of 2017 (lähde) Cybercrime Legislation Amendment Act 2012, No. 120 (lähde)	Investigatory Powers Act 2016 kokoaa yhteen tietoliikennetiedustelua ja viranomaisten oikeuksia määrittävän lainsäädännön. Human Rights Act 1998	Regulation of Security in Public Bodies Law, 5758-1998 (lähde)	Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktiivi)	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) 14.8.2009 Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG) 5.9.2005, viimeksi muutettu vuonna 2013	Kriittisen infrastruktuurin turvaaminen: laki No. 187 (2017) "On the Security of the Critical Information Infrastructure of the Russian Federation." Laki 194 (2017) mm. määrittelee rangaistuksia infraan kohdistuvista hyökkäyksistä.	Cyber Security Act (lähde) Public Information Act (Avaliku teabe seadus) Emergency Act (lähde) Information System Authority järjestää valtakunnallisia ratkaisuita silloin kun on tapahtunut merkittäviä/laajajalajaisia kyberhäiriöitä. Regulation: Requirements for risk analysis of network and information systems and description of security measures. Unofficial translation (lähde) Regulation: Riigi infosüsteemi haldussüsteem (lähde)	Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) NIS-direktiivi
Kyberturvallisuutta koskevat strategiset linjaukset	Kansallisessa kyberturvallisuusohjelmassa on tunnistettu seuraavat linjaukset: Strategiasta voidaan lisäksi nostaa esiin seuraavat periaatteet: kyberturvallisuus on osa valtion kokonais-turvallisuutta kyberturvallisuuden perusta on julkisen ja yksityisen sektorin yhteistyö hallitus edustaa yhteisiä intressejä, kannustaa vastuunottoon ja näyttää esimerkkiä omalla toiminnallaan osaamisen kehittämisen ja tiedon		Kansallinen kyberturvallisuusstrategia 2016-2021	Israelilla ei ole julkisista lähteistä löytyvää kyberturvallisuusstrategiaa. Hallituksen periaatepäätös 3611 on käytännössä vastannut tällaista strategiaa. (Lehto et al, 2018) (lähde; epävirallinen)	Kyberturvallisuutta käsitellään Ruotsin strategioissa rinnan tietoturvan kanssa. Kun mennään yksityiskohtiin, hankkeita ja päämääriä ei erotella erikseen tietoturva- tai kyberturvahankkeiksi.	Saksan sisäasiainministeriö on julkaissut vuonna 2011 ensimmäisen kyberturvallisuusstrategian, jota on päivitetty vuonna 2016 (Cyber-Sicherheitsstrategie für Deutschland 2016).	Ks. Tietoturvallisuus (Venäjä)	Kansallinen kyberturvallisuusstrategia 2019–2022 (lähde) In English: (lähde) Digital Agenda 2020 Viroon on luotu hyvin toimiva ja turvallinen ympäristö ICT-ratkaisujen laajalle käytölle Tietoyhteiskunnan kehittäminen Kyberturvallisuuden varmistaminen	Kyberturvallisuusstrategian (2019) strategiset linjaukset ovat: 1) kansainvälisen yhteistyön kehittäminen (kybertoimintaympäristön rajatonta turvaamista) 2) kyberturvallisuuden johtamisen, suunnittelun ja varustamisen parempi koordinaatio 3) kyberturvallisuuden osaamisen kehittäminen (arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina) (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	jakaminen ovat kriittisiä tekijöitä kyberturvallisuuden kehittämisessä kyberturvallisuus tulee saada osaksi jokapäiväistä toimintaa julkisella sektorilla, yrityksissä ja kansalaisten parissa (mainstreaming) valtioiden rajat eivät rajoita digitaalista toimintaympäristöä digitalisoituvassa ympäristössä turvallisuuden, vapauden ja talouskasvun tarpeet voivat tuottaa ristiriitaisia vaatimuksia (lähde) (lähde) Kansainvälisen kybertoimintaympäristön uhkia, haasteita ja Alankomaiden tavoitteita tässä ympäristössä on linjattu erillisessä strategiassa. Siinä tunnistetaan kansainvälisen yhteistyön merkitys mm. kyberrikollisuuden torjunnassa, Internetin hallinnoinnissa ja sen kestävässä kehityksessä sekä online-ympäristön oikeuksien ja vapauksien turvaamisessa. (lähde)								
Mitkä ovat kyberturvallisuuden painopisteet?	Oikeus- ja turvallisuusministeriö (Ministry of Justice and Security) on julkaissut elokuussa 2018 kansallisen kyberturvallisuusohjelman (National Cyber Security Agenda, NCSA), jossa listataan	Australian kyberturvastategiassa 2016-2020 on nimetty seuraavat painopistealueet: kansallinen yhteistyö kyberturva-asioissa vahva kyberpuolustus globaali vastuu ja vaikuttaminen	Kyberturvallisuudessa on sekä puolustuksellinen että hyökkäyssellinen ulottuvuus. Defend, Deter, Develop. Kyberturvallisuusstrategia nostaa esiin seuraavat keskeiset haavoittuvuudet:	Vuoden 2017 strategian kolme osiota ovat operaatiot, rakenne ja kyvykkyyden luominen (Lehto et al, 2018)	Kyberturvallisuusstrategiassa (Nationell strategi för samhällets informations- och cybersäkerhet) tärkeimpinä tavoitteina mainitaan tietoverkkojen, tuotteiden ja järjestelmien turvallisuuden parantaminen sekä kyberhyökkäysten ja muiden it-	BSI:n käyttämässä terminologiassa kyberturvallisuus (Cyber-Sicherheit) ulottuu kaikkiin tieto- ja viestintätekniikkaa koskevan tietoturvan näkökohtiin. Kyberturvallisuus kattaa kaikki Internet-yhteyteen ja vastaaviin verkkoihin liitetty tietotekniikat	Ks. Tietoturvallisuus (Venäjä)	Päätavoitteet: uuden tietoturvastandardin kehittäminen kansallisen kyberturvallisuuskeskuksen perustaminen järjestelmällinen ennaltaehkäisy (lähde)	Kybertoimintaympäristöä suojataan kasvattamalla kynnystä erityyppisiin kyberhyökkäyksiin muun muassa parantamalla kyberhyökkäysten havainnointi- ja attributiokykyä sekä kykyä vastatoimiin.

Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
seitsemän keskeistä tavoitetta: Alankomailla on riittävät digitaaliset kyvyt kyberuhkien havaitsemiseen, torjuntaan ja vaikutusten vähentämiseen Alankomaat osallistuu kansainvälisen digitaalisen toimintaympäristön turvallisuus-toimintaan Alankomaat on laitteiden ja ohjelmistojen digitaalisen turvallisuuden edelläkävijä Alankomailla on häiriönkestävät (resilientit) digitaaliset prosessit ja toimintavarma [digitaalinen] infrastruktuuri Alankomaat pystyy onnistuneesti torjumaan kyberrikollisuutta Alankomaat on kyberturvallisuuden osaamisen kehittämisen suunnannäyttäjä Alankomaiden kyberturvallisuutta kehitetään julkisen ja yksityisen sektorin tiiviissä yhteistyössä (public-private-partnership) Strategian painopiste-alueille on asetettu yksityiskohtaisia tehtäviä, tavoitteita ja mittareita.	kasvu ja innovaatiot kyberturvassa kyberosaamisen kasvattaminen Aloitteita katselmoidaan ja päivitetään vuosittain ja strategia katselmoidaan ja päivitetään neljän vuoden välein. (lähde) International Cyber Engagement Strategy on kolmivuotinen, kattava ja koordinoitu kansainvälisen kyberasioiden suunnitelma, joka ottaa kantaa digitaalisen kaupankäynnin, kyberrikollisuuden, kansainvälisen turvallisuuden ja kyberavaruuden asioihin. (lähde)	laitteiden Internet (Internet of Things, IoT; ml. teollinen IoT) lisää laitteiden lukumäärää ja tarjoaa laajan hyökkäyspinnan kyberhyökkäysten onnistuminen johtuu usein kohteen heikosta suojautumisesta eikä niinkään hyökkääjän taitavuudesta koulutuksessa ja osaamisessa on puutteita niin hallinnossa kuin yksityisellä sektorilla käytössä on vanhentuneita tietojärjestelmiä eikä järjestelmiä päivitetä kyberhyökkäysten toteuttaminen on helppoa, koska resursseja on helposti saatavilla Strategian liitteessä 3 kuvataan kolmesta strategista tavoitetta, joiden toteutumista seurataan vuosittain. (lähde)		häiriöiden ennaltaehkäisy, havainnointi ja häiriöihin reagointi. (lähde)	ja sisältää viestinnän, sovellukset, prosessit ja niihin perustuvan prosessoidun tiedon. (lähde) Kyberturvallisuusstrategian painopisteet on jaettu neljään toiminta-alueeseen: Turvallinen ja itseohjautuva (itsenäinen) toiminta digitalisoituneessa ympäristössä digitaalisten taitojen minimivaatimusten määrittäminen kaikille verkon käyttäjille huolimattoman toiminnan välttäminen digiympäristössä edellytysten luominen turvalliselle toiminnalle verkossa ja verkkoviestinnälle turvallinen digitaalinen identifiointi / henkilöllisyys tietoturvallisuussertifiointien ja hyväksymisten vahvistaminen digitalisoinnin turvallisuuden edistäminen tietoturvallisuustutkimuksen tukeminen Valtion ja talouselämän välisen yhteistyön vahvistaminen kriittisen infrastruktuurin vahvistaminen saksalaisten yritysten suojaaminen kyberuhkia vastaan saksalaisen IT-teollisuuden vahvistaminen			Kyberturvallisuuden kansallista kehittämistä koordinoi kyberturvallisuusjohtaja. Määritetään elintärkeiden toimintojen edellyttämä digitaalinen infrastruktuuri. Viranomaisten kyberturvallisuusyhteistyötä kehitetään erityisesti kyberpuolustus- ja kansallista turvallisuutta vaarantavien kyberuhkien torjunnassa. Digitaalisen turvallisuuden osa-alueisiin kytkeytyviä koulutusohjelmia vahvistetaan. Kyberturvallisuuden tutkimusta, kehitystä ja testausta vahvistetaan. Julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta lisätään uusien palveluiden ja tuotteiden tietoturvasta. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						laillisen yhteistyön edistäminen palveluntuottajien välillä yksityisten tietoturva- palveluiden tarjoajien osallistaminen turvallisen yhteisen alustan luominen esim. kyberuhkia koskevan tiedon jakamiseen Tehokas ja kestävä julkinen tietoverkkoturvallisuuden arkkitehtuuri kansallisen kyberpuolustuskeskuksen (Cyber-Abwehrzentrum) kehittäminen paikallisen analysointi- ja reagointikyvyyn vahvistaminen kyberturvallisuusasioissa lainvalvonnan tehostaminen kyberrikoksissa kybervakoilun ja kybersabotoinnin tehokas vastustaminen ulkomailta Saksaan kohdistuvien kyberhyökkäysten ennakkoarvointusjärjestelmän perustaminen Zentrale Stelle für Informationstechnik im Sicherheitstsbereich (ZITIS) perustaminen sotilaallisen puolustuskäytön vahvistaminen kyberturvallisuudessa CERT (Computer Emergency Response Teams) – rakenteiden vahvistaminen			

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						liittovaltion hallinnon turvaaminen tietoturvaratkaisuilla liittovaltion ja osavaltioiden välisen yhteistyön tiivistäminen taloudellisten resursien kasvattaminen ja henkilöstön kehittäminen kyberturvallisuusasioissa hallinnon kaikilla tasoilla: kunnat, osavaltiot ja liittovaltio Saksan aktiivinen osallistuminen eurooppalaiseen ja kansainväliseen kyberturvallisuuspolitiikkaan Toimivan eurooppalaisen tietoturvallisuuspolitiikan aktiivinen edistäminen NATOn kyberpuolustuspolitiikan kehittäminen kansainvälisen kyberturvallisuuden aktiivinen edistäminen kahdensivulaisen ja alueellisen tuen ja yhteistyön rakentaminen kyberkyvykkyyksissä (Cyber Capacity Building) kansainvälisen lainvalvonnan vahvistaminen			
Kuka on päävastuussa kyberturvallisuuden kehittämisestä? Kyberturvallisuuden hallintorakenteet	The National Cyber Security Centre (NCSC) on vastuussa digitaalisen turvallisuuden ohjauksesta. Kyberturvallisuus on yläkäsite, joka kattaa lähes kaikki digitaalisen turvallisuuden osa-alueet. Kyberturvallisuuden ohjaus on keskitetty oikeus- ja	Australian Signals Directorate (ASD) (lähde) Australian Cyber Security Centre (ACSC) on osa ASD:tä (lähde)	National Cyber Security Centre (NCSC): tiedon jakaminen, systeemisten haavoittuvuuksien käsittely, keskeisten kansallisten kyberturvallisuuskeskustusten johtajuus (lähde)	Israel National Cyber Directorate on aloittanut toimintansa vuonna 2018, kun kahden erillisen viraston (Cyber National Bureau ja National Cyber Security Authority) toiminnot yhdistettiin. Virasto vastaa keskitetysti kaikista siviili-	Ruotsin malli on varsin hajautettu. MSB:llä on merkittävä rooli erilaisissa varautumiseen ja kyberturvallisuuteen liittyvissä asioissa. MSB:n alakohtaisissa Forum för informationsdelning (FIDI) –foorumeissa tulevat esiin sektorikohtaiset	Vuoden 2011 alkupe- räisen kyberturvallisuusstrategian pohjalta Saksaan perustettiin		Kyberturvallisuuden politiikan yleisestä koordinoinnista vastaa talous- ja viestintäministeriö. Se oli puolustusministeriön vastuulla vuoteen 2011 saakka Cyber Security Council of the Security Committee of the Government tukee	Varsinaista päävastuullista on vaikea nimetä, koska vastuita on hajautettu monelle toimijalle (UM, VM, LVM, PLM, Digi- ja väestötietovirasto, Traficom, Kyberturvallisuuskeskus, Turvallisuuskomitea).

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	turvallisuusministeriöön ja sen alaisiin laitoksiin (erityisesti NCTV ja NCSC).			yhteiskunnan kyberpuolustuksen toiminoista, kuten politiikkojen määrittelystä, teknologian kehittämisestä ja operatiivisesta kybertoimintaympäristön suojaamisesta. (lähde) (Lehto et al, 2017)	kybertarpeet, jotka koskettavat fyysistä infrastruktuuria. Myös monilla muilla viranomaisilla on tähän liittyviä tehtäviä. (lähde)			strategisen tason virastojen välistä yhteistyötä ja valvoo kyberturvallisuusstrategian tavoitteiden toteutumista. (lähde) The Information System Authority (RIA) hoitaa ja suojaa valtion Internet-verkkoa ja varmistaa turvalliset e-vaalit. (lähde) Rakenne	
Mikä on yksityissektorin rooli valtion kyberturvallisuuden kehittämisessä?	<u>Kyberagendassa</u> on nostettu julkisen ja yksityisen sektorin yhteistyö (public-private partnership) yhdeksi seitsemästä painopistealueesta. Vuonna 2018 perustetun yhteistyöelimen (De Cybersecurity Alliantie, CS Alliantie) puitteissa voidaan toteuttaa julkisen ja yksityisen sektorin yhteistyönä (public private partnership) lyhyitä, enintään 9 kk kestäviä, kyberturvallisuutta kehittäviä hankkeita (esim. eettisen turvallisuustestauksen TIBER-NL – mallin laajentaminen rahoitussektorilta muille kriittisille toimialoille). (lähde)	Yksityissektorilta voidaan ilmoittaa kyberrikollisuuteen liittyviä seikkoja Australian Cybercrime Online Reporting Networkiin (ACORN). (lähde) Joint Cyber Security Centres (JCSC) on Australian kyberstrategian toteuttamisen perustettu tuomaan yhteen liiketoimintaa, tiedeyhteisöä sekä liittovaltion, osavaltioiden ja territorioiden virastoja yhteistyöhön (lähde)	Yritysten ja organisaatioiden ovat vastuussa omista kyberturvallisuuden riskeistään ja verkkojensa turvaamisesta. NCSC tarjoaa neuvoja, ohjeita ja maksuttomia työkaluja yritysten kyberturvallisuuden kehittämiseen. (lähde) <u>Cyber Essentials Scheme</u> on NCSC:n ja elinkeinoelämän tuottama koulutus- ja neuvontaohjelma, jonka avulla yritykset ja kansalaiset voivat suojautua tavallisimmilta kyberuhkilta. Vuodesta 2014 alkaen valtionhallinnon kilpailutuksiin osallistuvilla yrityksillä tulee olla Cyber Essentials -sertifikaatti. (lähde)	CyberSpark Initiative on Israelin kybertoimialan katto-organisaatio, jonka puitteissa hallinto, yritykset, tutkimuslaitokset ja yksittäiset asiantuntijat kehittävät kyberturvallisuuden ekosysteemiä. (lähde) Kyberturvallisuuden ekosysteemin kautta suojataan yhteiskuntaa ja tuotetaan teknologiaa vientituotteeksi. (Lehto et al, 2018)	Svensk Näringsliv on ruotsalaisten yritysten etujärjestö, joka julkaisee raportteja ja järjestää kyberturvallisuuteen liittyviä tilaisuuksia. Näringslivets Säkerhetsdelegation – Nätverket för lönsam riskhantering (NSD) on elinkeinoelämän oma yhteistyöverkosto, joka kehittää myös tietoturva.	Saksassa toimii vuonna 2012 perustettu riippumaton <u>Cyber-Sicherheitsrat</u> (kyberturvallisuusneuvosto), jonka jäseninä on keskikokoisia ja suuria yrityksiä, kriittisen infrastruktuurin alalla toimivia yrityksiä, useita osavaltioita (esim. Nordrhein-Westfalen, Niedersachsen), suurimpia kaupunkeja (esim. Frankfurt-am-Main) sekä poliittisia päättäjiä ja asiantuntijoita kyberturvallisuuden toimialalla. Jäsensensä välityksellä neuvosto edustaa yli kolmea miljoonaa työntekijää Saksassa sekä melkein kahta miljoonaa muiden yhdistysten ja järjestöjen jäsentä. Neuvoston tehtävänä on: lisätä yhteistyötä poliittikkojen, julkishallinnon, liike-elämän ja tieteen välillä kyberturvallisuuden parantamiseksi, esittää aloitteita ja projekteja kyberturvallisuustietoisuuden kasvattamiseksi,		Työryhmä: julkisen ja yksityisen sektorin yhteistyön edistäminen. (lähde) Viron henkilöllisyshallinnon ja henkilöllisyssyödistysten ala perustuu julkisen ja yksityisen sektorin yhteistyöhön. Yksityissektorilta osallistuvat: palveluntarjoajat viestintäoperaattorit henkilöllisyssyödistysten valmistaja (Valge raamat)	Turvallisuusviranomaisten ja elinkeinoelämän kriittisten toimijoiden digitaalisten palvelujen käyttö ja kehittäminen turvataan kaupallisia palveluja hyödyntävillä ja niitä täydentävillä ratkaisuilla. (lähde)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						kehittää kansallinen kyberturvallisuusverkosto toimimaan eu-rooppalaisessa ja kansainvälisessä ympäristössä, tarjota tietoa, keskustelufoorumi ja verkostoitumismahdollisuuksia järjestön jäsenille. Tehtäviään neuvosto hoitaa järjestämällä jäsenilleen mm. keskustelu- ja koulutustilaisuuksia sekä opintomatkoja ulkomaisiin kohteisiin, antamalla lausuntoja lainsäädäntöhankkeisiin, konsulttoimalla poliittisia päättäjiä, tukemalla kyberturvallisuutta koskevaa tieteellistä julkaisu toimintaa sekä järjestämällä kyberturvallisuustietoutta lisääviä kampanjoita. Ks. lisäksi Allianz für Cyber-Sicherheit eli Kyberturvallisuusliitto seuraava kohta.			
Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?	Kyberturvallisuuden ohjaus on Alankomaissa keskitetty Oikeus- ja turvallisuusministeriöön ja sen alaisiin laitoksiin (NCTV ja NCSC). NCSC:n toimintaa ohjaa Operational Framework NCSC-NL, jossa määritellään viraston päätehtävät ja keskeiset yhteistyötahot. NCTV vastaa Alankomaiden yhteiskunnan suojaamisesta hallinnon, tutkimusyhteisön ja yksityis-	ASD toimii koko Australian hallituksen sekä puolustusvoimien tukena tiedusteluun, kyberturvaan sekä kyberhyökkäyksiin liittyvissä asioissa. ACSC ajaa kybervastustuskäytäntöä maanlaajuisesti sisältäen myös kriittisen infrastruktuurin ja järjestelmät liittovaltion, osavaltioiden, paikallisten hallintojen sekä yksityissektorin osalta. Työntekijöitä on monesta	Hallinnon turvallisuusvastuut on kuvattu dokumentissa Government Security: Roles and Responsibilities. Cyber Security Operations Centre varmistaa armeijan toimintakykyä kyberhyökkäysten varalle (lähde) NCSC on julkaissut hallinnolle kyberturvallisuuden minimivaatimukset. Dokumentissa on kymmenen kohtaa, joissa määritellään lyhyesti ministeriöiltä	Israel National Cyber Directoraten (INCD) tehtävänä on neuvota pääministeriä, hallitusta ja sen komiteoita. Vastuussa kyberturvallisuusstrategiasta. CERT-IL -toiminta on osa INCD:tä. Israeli Defence Forces (IDF) vastaa sotilaallisesta kyberturvallisuudesta ja se kehittää myös kyberhyökkäyskykyä. (lähde)	Ruotsin puolustusministeriö (Försvarsdepartementet) on aktiivinen kyberasioissa. Försvarets radioanstalt (FRA) on Ruotsin puolustusministeriön alainen siviiliorganisaatio, joka suorittaa signaalitiedustelua. FRA saa tiedustella kaikkea Ruotsin läpi kulkevaa viestiliikennettä, esimerkiksi puheluja, Internet-selailua ja sähköposteja. Pää tarkoituksena on terrorismin ja järjestä-	Kyberturvallisuuteen liittyviä tehtäviä on jaettu eri hallinnonaloilla olevien viranomaisten kesken: Sisäasiainministeriön alaisen Bundesamt für Sicherheit in der Informationstechnik eli Tietotekniikan turvallisuusviraston (BSI) tehtävänä on edistää informaatioteknologian turvallisuutta. Tehtävät ja vastuut sekä toimivalta on säädetty laissa Gesetz über das Bundesamt für	Digitaalisen turvallisuuden (information security) järjestelmän rakenteen määrittelee presidentti (lähde). Venäjän Internetin valvonta voitaneen nähdä kyberturvallisuutena. Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) toimii Internetin valvonta- ja kontrolliviranomaisena. (lähde).	Estonian Information Security Association (EISA) has been established to coordinate effective cooperation between private sector, academia and the state. (Cyber Security Strategy 2019-2022)	Ks. Tietoturvaluus (Suomi)

Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
sektorin kanssa yhteistyössä. Päätehtävät ovat kyberturvallisuuden varmistaminen, terrorismin torjunta ja Alankomaiden suojaaminen valtiollisten toimijoiden uhkaa vastaan. (lähde) NCSC arvioi digitaalisen toimintaympäristön riskejä ja trendejä. Virasto jakaa tietoa ja tarjoaa asiantuntija-apua ja neuvontaa. Se on mm. julkaissut ohjeen toimialakohtaisen yhteistyöelimen (ISAC) perustamisesta. Virastossa on 24/7 toimintavalmius kriisien varalle. (lähde) Kyberturvallisuusneuvoston (Cyber Security Council, CSR) jäsenet edustavat sekä julkishallinnon että elinkeinoelämän johtoa sekä tiedeyhteisön edustajia. CSR vahvistaa Alankomaiden kyberturvallisuutta strategisen tason toimilla. (lähde) NCSC toimii lisäksi NIS-direktiivin mukaisena CSIRT-organisaationa. (lähde) Kyberpuolustuksen järjestäminen on puolustusministeriön vastuulla. Aluehallinnolle ei löydy erityisiä digitaalisen turvallisuuteen liittyviä velvoitteita tai vastuita.	Australian julkishallinnon organisaatiosta. (lähde) Special Adviser to the Prime Minister on Cyber Security johtaa kyberstrategian kehitystä, asettaa selkeitä tavoitteita sekä prioriteetteja julkishallinnon organisaatioille ja valvoo näiden toteutumista. (lähde) Ambassador for Cyber Affairs on vastuussa kansainvälisesti Cyber Engagement Strategyn implementoinnista. (lähde)	vaadittavat kyberturvallisuuden toimenpiteet. (lähde)	Israeli Security Agency (ISA) Information technology ja Cyber divisioonat kehittävät ja tuottavat työkaluja mm. vakoi- lun ja terrorismin torjunnan käyttöön. Se mitä ilmeisimmin oli avainroolissa esim. Iranin uraanirikastamoja vastaan tehdyissä kyberiskuissa, vaikka kampanja on julkisuudessa esitelty lähinnä amerikkalaisvetoisena. (lähde), jossa esitellään Stuxnetin kaltainen hanke jo vuosia ennen kampanjaa)	tyneen rikollisuuden torjuminen. (lähde) Puolustusministeriön alla armeijalla on omaa kyberpuolustustoimintaa, johon osallistuu myös Försvars Materiel Administration (FMV). FRA, MSB, puolustusvoimat ja turvallisuuspoliisi (Säkerhetsspolisen) ovat saaneet hallitukselta 26.9.2019 tehtäväksi valmistella kansallisen kyberturvallisuuskeskuksen perustamista 19.12.2019 mennessä. (lähde)	Sicherheit in der Informationstechnik (BSI-Gesetz – BSIg), erityisesti sen 3 §:ssä. Tietotekniikan turvallisuusviraston 15.4.2019 alkaen voimassa olevassa orga- nisaatiokaaviossa näkyvät hyvin viranomaisen eri tehtäväalueet. Viraston alaisuudessa ja yhteistyössä viraston kanssa toimii useita eri aliorganisaatioita, joiden tehtävät näytävät osittain päällekkäisiltä: Vuoden 2011 alkupe- räisen kyberturvalli- suusstrategian pohjalta on perustettu Kansallinen kyber- puolustuskeskus (Cyber-Abwehrzentrum, NCAZ tai Cyber-AZ). Kyberpuolustuskeskus on Saksan turval- lisuusvirastojen yh- teistyöelin liittovaltion tasolla. Sen tarkoituksena on torjua sähköi- siä hyökkäyksiä Sak- san liittotasavallan ja sen talouden IT-infra- struktuureihin. Cyber- AZ yhdistää kaikki ke- rätyt tiedot turvalli- suusviranomaisten tietoinfrastruktuurei- hin kohdistuvista tie- toturvahyökkäyksistä. (lähde) CERT-Bund (Compu- ter Emergency Res- ponde Team für Bun- desbehörden) eli liit- tohallituksen IT-hätä- valmiusryhmä, on keskeinen yhteys- piste ennaltaehkäise- ville ja reagoiville toi- menpiteille			

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						tietojärjestelmien tietoturvaan liittyvissä vaaratilanteissa. (lähde) Nationales IT-Lagezentrum (Kansallinen IT-tilannekeskus) perustettiin vuonna 2005 toteuttamaan liittohallituksen hyväksymää Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI) eli tietoinfrastruktuurien suojaamista koskevaa kansallista suunnitelmaa. Viranomaisen tehtävänä on 1) tapahtumien tunnistaminen, kirjaaminen ja arviointi, 2) Ilmoittaminen, hälyttäminen ja varoittaminen sekä 3) IT-tietoturvahäiriöihin reagoiminen (lähde). IT-Krisenreaktionszentrum (IT-kriisikeskus) on perustettu vuoden 2005 NPSI-suunnitelman pohjalta. IT-kriisikeskusten tehtävänä on varmistaa nopea reagointi vakaviin vaaratilanteisiin, mahdollistaa oikea-aikaiset vastatoimet ja siten minimoida vahinkojen määrä. Tehtävän täyttämistä varten IT-tietoturvatapahtumat analysoidaan, arvioidaan ja välitetään asianomaisille viranomaisille. Lisäksi IT-kriisikeskus koordinoi yhteistyötä sekä paikallisten että toimialakohtaisten kriisinhalintajärjestöjen kanssa. Jos kriisi ylittää			

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						paikalliset vastuut ja vaikuttaa suurempiin osiin liittohallintoa, IT-kriisikeskus hoitaa koordinoitua (lähde). Vuonna 2012 perustettu Allianz für Cyber-Sicherheit eli Kyberturvallisuusliitto tarjoaa laajan valikoiman tietoverkkoturvallisuustietoja yritysten, hallitusten, tutkimuksen ja tieteen sekä muiden instituutioiden kanssa. Liiton toiminta keskittyy pieniin ja keskisuuriin yrityksiin. Kriittisen infrastruktuurin piirissä toimivien yritysten on mahdollista liittyä järjestön jäseneksi ns. INSI-statuksella (Institutionen im besonderen staatlichen Interesse). INSI-jäsenille jaetaan mm. enemmän luottamuksellista tietoa ja ne ovat ennakkovaroitusjärjestelmän piirissä. Liitolla on miltei 2900 jäsentä (15.10.2019) ja jäsenmäärä on kasvussa. Liitto tarjoaa mm. koulutusta, asiantuntijapalveluita ja tietopalveluita parantamaan tietoturvallisuuden tasoa. (lähde)			
Miten kyberturvallisuutta valvotaan ja arvioidaan?	Kaikkiin seitsemään kyberturvallisuusohjelmassa (NCSA) listattuun tavoitteeseen on kytketty tavoitteet (objectives) ja toimenpiteet (measures), joilla tavoitteisiin pyritään. Toimenpiteille ei ole määritely	ACSC pitää yllä tilanne- ja uhkakuva. (lähde) Strategiatasolla asetettujen tavoitteiden saavuttamista seurataan vuosittain. (lähde) Uuden 2020 strategian laatimisprosessissa on julkaistu	Toukokuussa 2019 julkaistu seurantaportti luettelee kansallisen kyberturvallisuusstrategian mukaisia saavutuksia kolmella strategisella painopistealueella (Defend, Deter, Develop). Tällaisia ovat esimerkiksi:			BSI julkaisee vuosittain Saksan kyberturvallisuuden tilannekatsausta eli Die Lage der IT-Sicherheit in Deutschland -nimistä julkaisua, jonka uusin versio kuvaa tilannetta kevääseen 2019 saakka.		Estonian Computer Emergency Response Team CERT-EE on organisaatio, joka vastaa .ee-tietokoneverkkojen tietoturvahäiriöiden hallinnasta. Se on myös kansallinen yhteyspiste kansainväliselle	

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	konkreettisia mitta-reita. van Tilburgin yliopisto julkaisi marraskuussa 2015 katsauksen eräiden verokkivaltioiden kyberturvallisuuden rakenteisiin. Vertailussa olivat mukana Kanada, Viro, Saksa, Alankomaat ja Iso-Britannia. Operational Framework NCSC-NL Version March 21, 2019 Alankomaiden tilastokeskus (Het Centraal Bureau voor de Statistiek, CBS), julkaisee vuosittain (holanniksi; tuorein julkaisu vuodelta 2019) Cyber Security Monitor -katsauksen. Siitä löytyy monipuolisia tilastoja kyberrikollisuudesta, haavoittuvuuksista ja toteutetuista kyberturvallisuustoimenpiteistä. (lähde) (lähde; julkaisun yleiskuvaus englanniksi)	arvio nykytilasta ja lista kysymyksiä, joihin pyydetään yritysten, yhteisöjen, oppilaitosten ja kansalaisten näkemyksiä uuden strategian laatimiseksi. (lähde) Australian valtionhallinnon organisaatioiden tulee noudattaa Protective Security Policy Framework -määräyksiä. Määräykset eivät suoraan velvoita valtionyhtiöitä (government business enterprises) tai yksityisyrityksiä. Australian National Audit Office (ANAO) tekee mm. kyberturvallisuuden suorituskykyyn liittyviä tarkastuksia (ks. esim. Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities)	NCSC:n perustaminen rakennettu kansainvälinen verkosto, joka tunnistaa valtiollisten toimijoiden kyberhyökkäyksiä ja reagoi niihin tietojenkäsittelyn koulutuksen kehitysohjelma käynnistämisen (84 miljoonaa punta; noin 94 miljoonaa euroa) Raportti kuvaa yksityiskohtaisemmin kolmentoista strategisen tavoitteen (SO1-SO13) toteutumista.			BSI järjestää vuosittain kyberturvallisuutta koskevan laajan kyselytutkimuksen yhteistyössä Allianz für Cyber-Sicherheitin kanssa. Uusin tutkimusraportti vuodelta 2018 on julkaistu keuhällä 2019. Tutkimusta on tehty vuodesta 2014 eteenpäin. Tutkimusraportteja voi hyödyntää esim. kyberturvallisuuden perustason arviointiin organisaatioissa.		tietoturvaan liittyvälle yhteistyölle. (lähde)	
Raportoidut kyberturvallisuustapahtumat	Vuosittain julkaistavassa Cyber Security Assessment –raportissa on liitteenä tilastotietoja NCSC:lle raportoiduista kyberturvallisuustapahtumista. CSAN 2019 mukaan virastolle oli raportointijaksolla ilmoitettu 358 tapausta, joista 26 % oli erilaisia tiedon kalastelu-yrityksiä, 15 % haittaohjelmia, 21 % luvaton käyttöä ja tunkeutumista (intrusion), 11 % palvelunestohyökkäyksiä,	ACSC ylläpitää tilastoja haittaohjelmatarunnoista, palveluiden haavoittuvuuksista, avoimista palveluista ja muista kyberturvallisuushavainnoista (lähde).	Tutkimuksen mukaan noin kolmannes yrityksistä on ollut kyberhyökkäyksen tai tietomurron kohteena vuonna 2018. Kohdeena olleiden yritysten osuus on laskeutunut parin vuoden aikana, mutta yksittäiseen yritykseen kohdistuu nyt useampia hyökkäyksiä. Phishing-tyyppiset tiedon kalastelu-yritykset ovat tyypillisimpiä hyökkäysten toteutustapoja.	CERT-IL ei julkaise tilastoja kyberturvallisuustapahtumista (ainakaan englanniksi). INCD on julkaissut kyberturvallisuutta koskevan yleiskatsauksen. (lähde)				17 440 (2018) (lähde)	Ks. Tietoturvaluus (Suomi)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	21 % petoksia ja loput 6 % muita ilmoituksia. Alankomaiden tilastokeskus (Centraal Bureau voor de Statistiek, CBS) julkaisemien tietojen mukaan 8,5 % yli 12-vuotiaista Internetin käyttäjistä oli joutunut kyberrikoksen uhriksi vuonna 2018. (lähde)								

Tietosuoja

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
Tietosuojaa ohjaava lainsäädäntö	Algemene verordening gegevensbescherming (AVG) on Alankomaiden kansallinen versio GDPR:stä. General Administrative Law Act (Algemene wet bestuursrecht) The Freedom of Information Act (Wet openbaarheid van bestuur)	Privacy Act No. 119 (lähde) (lähde)	Data Protection Act 2018 on GDPR:ään perustuva tietosuojalaki, mutta siihen on tehty kansallisia laajennuksia. Freedom of Information Act Privacy and Electronic Communications Regulations Re-use of Public Sector Information Regulations Investigatory Powers Act 2016 INSPIRE Regulations eIDAS Regulation NIS Regulations 2018 Environmental Information Regulations	The Protection of Privacy Law (PPL), 5741-1981 (lähde; ei viranomaislähde) Protection of Privacy Regulations (Data Security) 5777-2017 (lähde)	EU-direktiivin (GDPR) pohjalta on muodostettu kansallinen tietosuojalaki (Brottsdotalag (2018:1177)). Direktiivin vaatimuksia on täydennetty erityislilla (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).	GDPR Bundesdatenschutzgesetz (BDSG) 30.6.2017, epävirallinen käännös englanniksi laissa säädetty kansallinen liikkumavara: lapsen ikäraja 16 vuotta (GDPR:n mukainen, ei mainintaa ikärajasta kansallisessa BDSG:ssä)	Venäjän Henkilötietolaki 152-FZ vuodelta 2006 ja sitä täydentävät oikeuslähteet vastaavat suunnilleen Suomen ja EU:n vastaavaa lainsäädäntöä (GDPR). Henkilötietojen käsittelyä säätelevä ns. tietojen lokalisatiolaki 242-FZ on vuodelta 2015. Lain rikkomisesta säädettyjä sanktioita on kiristetty vuonna 2019. (lähde)	Eesti Vabariigi põhiseadus - Henkilötietojen suoja taataan 26 §:llä (perhe- ja yksityiselämän suoja), 19 §:llä (oikeus itsensä toteuttamiseen) ja 44 §: n 3 momentilla (oikeus tutustua viranomaisten keräämiin henkilötietoihin). Pääsy julkiseen tietoon taataan 44 §: n 2 momentilla. Public Information Act (Avaliku teabe seadus) – Pääsy julkiselle tiedolle ja sen rajoitukset, julkisen tiedon uudelleenkäyttö sekä julkisen sektorin tietokantojen ylläpito ja valvonta. Personal Data Protection Act (Isikuandmete kaitse seadus) – henkilötietojen suoja ja valvontaa sekä Data Protection Inspectoriate (AKI) statusta. Electronic Communications Act (Elektroonilise side seadus) – Sähköisen suoramarkkinoinnin valvonta ja viestintä yritysten henkilötietojen rikkomusten seuranta (lähde) Kansallinen liikkumavara: Viron oikeusjärjestelmät eivät mahdollista tietosuojasetuksen mukaisia hallinnollisia sakkojen määräämistä julkisorganisaatioille. Virossa sakon määrä	EU:n tietosuojaa-asetus (GDPR) (EU) 2016/679 Tietosuojalaki (1050/2018) Laki yksityisyyden suojasta työelämässä (759/2004) Laki sähköisen viestinnän palveluista (917/2014)

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
								valvontaviranomainen rikkomusmenettelyn puitteissa, edellyttäen että kyseisten jäsenvaltioiden sääntöjen tällaisella soveltamisella on vastaava vaikutus kuin valvontaviranomaisten määräämillä hallinnollisilla saakoilla (lähde). Lapsen ikäraja: 13 (§8 of the Personal Data Protection Act)	
Mitkä ovat lainsäädännön merkittävimmät havainnot digitaalisen turvallisuuden näkökulmasta?				Lainsäädäntöä voi pitää pääosin riittävänä modernista eurooppalaisesta näkökulmasta, mutta viranomaisilla on suuret valtuudet murtaa se tarvittaessa. (lähde)	Ruotsin perustuslaki sisältää määräyksen yksityisyyden suojasta ja mainitsee erikseen yksityiselämän koskemattomuuden automaattisen tietojenkäsittelyn yhteydessä. Tietosuoja on siten nostettu osin perustuslain tasolle. Ruotsissa ei ole erillistä lakia yksityisyyden suojasta työelämässä, mutta se on valmisteilla (2019) (Hur står det till med den personliga integriteten?).	BDSG sisältää myös rikosoikeudellisia sanktioita (vankeusrangaistus) tiettyjen säännösten vastaisesta toiminnasta, Rekisterinpitäjien ja käsittelijöiden on noudatettava henkilötietojen käsittelyssä BSI:n antamia teknisiä ohjeistuksia ja suosituksia (BDSG 64 §)	Ns. lokalisaatiolaki 242-FZ vuodelta 2014 ("On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks") vaatii, että Internet-palvelut keräävät käyttäjien henkilötiedot venäläisille palvelimille. Tietojen siirtämistä edelleen myöhemmin kolmansiin maihin ei ole suoraan kielletty, mutta käyttäjätietojen tulee pysyä Venäjällä viranomaisten kontrolloitavissa. (lähde). Määräyksiä on analysoitu täällä ja täällä ja täällä)		
Mitkä ovat valtion tietosuojan painopisteet? Tietosuojaa koskevat strategiset linjaukset	GDPR:n vaatimusten toteuttaminen (valvonta ja neuvonta, tiedottaminen tietosuoja-asetuksen tulkinnoista ja vuosikertomukset, kansainvälinen yhteistyö) (lähde)	Lainsäädännön pohjautuvat 13 tietosuoja-periaatetta, jotka ohjaavat kaikkien organisaatioiden tietosuojatoimintaa. (lähde) Corporate Plan 2019-2020 ohjaa tietosuojan strategisia painopisteitä:	Yritysten tietosuojavelvoitteiden valvonta (lähde) Freedom Of Information Act (FOIA) ja Environmental Information Regulations (EIR) lainsäädännön vaatimustenmukaisuuden parantaminen. (lähde)	Tietosuojalainsäädäntö jakaa suojattavat tiedot (tietokannat) neljään suojausluokkaan tietojen arkaluonteisuuden, kohteiden määrän ja tietojen käyttäjien määrän perusteella. (lähde)		Kansalaisten henkilötietojen suojaaminen lähde Ks. alempana Standard-Datenschutzmodell.		Viranomaisen (AKI) on tehostettava valmiuksia suorittaa tehtävänsä. Erityisesti on kiinnitettävä huomiota siihen, että virastossa on riittävästi virkamiehiä, joilla on riittävä asiantuntemus erityisesti tieto- ja viestintätekniikasta. Lisäksi AKI:n on varmistettava valmiutensa	

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
		Edistää australialaisten tietosuojaa internetissä Vaikuttaa ja ylläpitää "privacy and information access" -viitekehyksiä Kannustaa ja tukea proaktiivista julkishallinnon hallussa pitämän tiedon vapauttamista Nykyaikainen lähestymistapa sääteltyyn (lähde)	Valmistautuminen sopimuksettomaan brexitiin (lähde)					koordinoida julkisen tiedon suojaamista. Lakimuutoksia on tuettava myös teknisillä ratkaisuilla, joiden avulla AKI voi siirtyä sähköiseen menettelyyn. (lähde) Oikeusministeriön kehityssuunnitelma 2019–2022 (lähde)	
Kuka on päävastuussa tietosuojan kehittämisestä?	The Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) vastaa EUn tietosuojadirektiivin toteutumisesta. Tehtäviin kuuluvat valvonta, neuvonta, tiedottaminen ja koulutus. Virasto huolehtii myös GDPR:n kansainvälisistä velvoitteista ja se on Euroopan tietosuojaneuvoston (The European Data Protection Board) jäsen. (lähde)	Office of the Australia Information Commissioner (OAIC) tietosuojan valvontaviranomainen Australiassa. (lähde)	Information Commissioner's Office (ICO)	The Privacy Protection Authority valvoo tietosuojan toteutumista Israelissa. (lähde)	Datainspektionen on viranomainen, joka vastaa tietosuojan toteutumisesta ja henkilötietojen käsittelyn oikeasta käsittelystä (valvonta, seuranta ja tiedottaminen). (lähde). Virastossa työskentelee noin 80 henkilöä (lähde). Datainspektionen järjestää vastuualueeseensa liittyvää koulutusta ja se tukee kansalaisia, yksityisiä yrityksiä ja viranomaisia. Virasto ei tarjoa teknistä tietoturvatukea. Datainspektionen ohjeistaa organisaatioiden tietosuojavastavia mm. järjestämällä koulutustilaisuuksia.	Kansallinen valvontaviranomainen Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). Viranomainen on mm. julkaissut GDPR:n ja kansallisen tietosuojalain kommentaarin Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterung (säädöstekstit selityksineen) kesäkuussa 2019.	Federal Service for Supervision of Communications, Information Technologies and Mass Media ("Roskomnadzor"). Sitä ohjaa digitalisatio-, tietoliikenne- ja joukkoviestintäministeriö (digiministeriö).	Oikeusministeriö (Justiitsministerium) – Estonian Data Protection Inspectoriate	
Mikä on yksityissektorin rooli valtion tietosuojan kehittämisessä?	Alankomaiden AP on itsenäinen ja riippumaton ja puolueeton viranomainen. Se tukee, valvoo ja opastaa niin julkishallinnon organisaatiota, yksityisyrityksiä kuin kansalaisiakin. (lähde) AP:ltä voi hakea tuoteelle, palvelulle tai		Valtionhallinto ja yritykset rahoittavat Get Safe Online -sivustoa, josta löytyy ohjeita ja neuvoja erilaisten digitaalisen toimintaympäristön uhkien tunnistamiseksi ja torjumiseksi (esim. identiteettivarkaudet, phishing ja yksityisyys-	Tietokannan omistajan (database controller) täytyy ilmoittaa tietokanta hallinnon ylläpitämään rekisteriin, mm. jos tietokannassa on useamman kuin 10.000 henkilön tiedot, tai tietokanta sisältää sensitiivisiä tietoja.		Yritysten on noudatettava GDPR:ää sekä kansallista tietosuojalakia BDSG:tä. BDSG 38 §:n mukaan yli 10 hengen yritysten on nimitettävä tietosuojavastava. Saksan parlamentti on kuitenkin hyväksynyt 28.6.2019 lainmuu-			

Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
prosessille AVG-sertifikaattia, joilla tiedon käsittelijä tai omistaja voi osoittaa GDPR:n mukaisen tietosuojan toteutumisen. (lähde)		den suoja). (lähde) (lähde)	Myös viranomaisten tietokannat on ilmoitettu em. rekisteriin.		toksen, jolla tietosuojavastaavan nimitysmistä edellyttävän henkilöstön minimimäärä nostetaan 20 henkilöön. Tietosuojavastaavilla on Saksassa oma edunvalvontajärjestö Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), joka edustaa yhteensä noin 1750 sekä julkissektorin että yksityissektorin palveluksessa työskentelevää tietosuojavastaavaa, ulkoistettua tietosuojavastaavaa ja yritysjäsentä. Järjestö on toimialan vanhin edunvalvontajärjestö maailmanlaajuisesti ja se on perustettu vuonna 1989. Järjestön tavoitteena on tuoda esille tietosuojavastaavien työtä sekä parantaa tietosuojatietoisuutta. Järjestöllä on 11 alueellista ryhmää sekä yhdeksän työryhmää. Järjestö on myös laatinut tietosuojavastaavien 'tehtävänkuvan' Das berufliche Leitbild der Datenschutzbeauftragten - Code of Practice for Data Protection Officers, jonka neljäs versio on julkaistu vuonna 2018 GDPR:n voimaantulon jälkeen. Organisaation toiminnasta voi lukea lisää (ei viranomaislähde). Tietosuojavastaavan ei tarvitse olla yrityksen oma työntekijä oletettavasti siksi,			

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						että henkilöstöltään pienissäkin organisaatioissa vaaditaan tietosuojavastaavan nimitystä, joten Saksaan on syntynyt ulkoistettujen tietosuojavastaavien ammattikunta. Lokakuuhun 2019 mennessä BvD:hen oli liittynyt 169 ulkoistettua tietosuojavastaavaa (lähde ; ei viranomaislähde)			
Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?	Oikeus- ja turvallisuusministeriö nimitää tietosuojaviraston johtoryhmän. (lähde)	Australian Information Commissioner and Privacy Commissioner johtaa OAIC:tä	Information Commissioner's Office (ICO) on GDPR:n mukainen tietosuojaviranomainen.	The Privacy Protection Authority on tietosuojaviranomainen. (lähde)	Muille viranomaisille ei ole osoitettu tietosuojan toteuttamiseen liittyviä vastuuta tai toimivaltaa. Jokainen viranomainen vastaa omalta osaltaan tietosuojavelvoitteiden toteutumisesta.	Saksan kansallinen valvontaviranomainen on Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) eli tietosuoja- ja tiedonvälitysvapausvaltuutettu. BfDI:n toimistossa on henkilökuntaa noin 190 virkamiestä, joista osa on Bonnissa, osa Berliinissä. Tämän lisäksi jokaisella 16 osavalttiolla on oma paikallinen Landesbeauftragter ja valtuutetun virasto. BfDI:n viraston yhteydessä mutta erillisenä organisaationa toimii lisäksi Die Zentrale Anlaufstelle (ZAST) eli keskitetty yhteyspiste. Sen tehtävänä on koordinoida rajat ylittävää yhteistyötä muiden Euroopan unionin jäsenvaltioiden, Euroopan tietosuojalautakunnan (EDSA) ja Euroopan komission sekä Saksan osavaltioiden paikallisten tietosuojaviranomaisten välillä. ZAST:lla ei ole valvon-		Päävastuu on tietosuojavaltuutetulla.	Tietosuojavaltuutetun toimisto Ministeriöt vastaavat tietosuojasta omilla hallinonaloillaan

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
						taan liittyvää toimivaltaa. Kansallinen valvontaviranomainen sekä osavaltioiden tietosuojavaltuutetut pitivät kaksi kertaa vuodessa ns. Die Datenschutzkonferenz (DSK) eli tietosuoja-konferenssin. Sen tehtävänä on ylläpitää ja suojata tietosuojan peruseriaatteita, saavuttaa eurooppalainen ja kansallinen tietosuojalaki yhdenmukaisesti ja työskennellä yhdessä sen edelleen kehittämiseksi. Tämä tapahtuu erityisesti päätöslauselmien, päätösten, ohjeiden, standardoinnin, lausuntojen, lehdistötiedotteiden ja määräysten avulla.			
Miten tietosuojaa valvotaan ja arvioidaan?	Autoriteit Persoonsgegevens (AP) valvoo tietosuojan toteutumista GDPR:n ja sananvapauslain puitteissa. Virasto julkaisee toiminnastaan vuosikertomuksen. (lähde)	OAIC valvoo tietosuojan toteutumista (lähde) Corporate Planissa arvioidaan OAIC:n asettamien strategisten tavoitteiden toteutumista. (lähde)	ICO:n vuosiraportissa raportoidaan merkittävimmät saavutukset. Kaudella 2018-2019 tällaisia olivat mm. GDPR:n toteuttaminen, kansainvälisen toiminnan kehittäminen ja kyberturvallisuuden lisääminen. Virasto raportoi toiminnastaan ohjaavalle ministeriölle (Department for Digital, Culture Media and Sport) (lähde)	Privacy Protection Authorityn tehtävänä on valvoa tietosuojan toteutumista sekä raportoida vuosittain aktiviteeteistaan. (lähde)	Datainspektionen valvoo ja seuraa tietosuojaan liittyvien lakien ja ohjeiden noudattamista. Valvontaa tehdään sekä kyselyjen avulla että tekemällä organisaatioihin tarkastuskäyntejä.	BfDI neuvoo ja valvoo liittovaltion viranomaisia (liittovaltion viranomaisia, liittovaltion ministeriöitä). Yksityisellä sektorilla BfDI neuvoo ja valvoo vain tietoliikenne- ja postipalveluyrityksiä, sekä yksityisiä yrityksiä, jotka kuuluvat turvallisuusarkistuksen piiriin.		Tietosuojavaltaviranomainen suorittaa henkilötietojen suojaamista koskevia vaatimustenmukaisuus- ja valmiustarkastuksia. (lähde) Auditointiohje (Isikuandmete kaitse auditi läbiviimise juhend) Viron tietosuojaviranomaisen verkkosivuilla on nähtävissä 7 varoitusta tietoturvallisuuden rikkomisesta, jotka Viron tietosuojaviranomainen on antanut. (2019) (lähde)	
Raportoidut tietosuojaloukkaukset	Vuonna 2018 raportitiin 20881 tietosuojaloukkausta (data breach). 29 % näistä kohdistui terveys- ja hyvinvointisektorille.	OIAC julkaisee neljännesvuosittain tilastoja tietosuojaloukkauksista (lähde). Vuoden 2019 toisella neljänneksellä virastolle oli	Q4 2018 - 2019 aikana raportitiin yhteensä 686 kybertietosuojaloukkausta (cyber personal data breach: esim. luvaton		Vuonna 2018 tietosuojaviranomaiselle tehtiin yhteensä 72 ilmoitusta, joista 67 liittyi GDPR:ään ja viisi	Saksan valtiollisten viranomaisten pitää noudattaa toiminnassaan tietosuojalainsäädännön lisäksi tietosuojamallia		462 (2018) (lähde)	Traficomien vastaanottamia ilmoituksia henkilötietojen tietoturvaloukkauksista vuonna 2018 481 kpl, joista 17 oli tietovuotoja ja

	Alankomaat	Australia	Iso-Britannia	Israel	Ruotsi	Saksa	Venäjä	Viro	Suomi
	26 % rahoitussektorille ja 17 % julkishallintoon. (lähde)	tehty 245 ilmoitusta, joista 62 % oli pahanthautoisia tai rikollisia tapauksia, 34 % inhimillisiä virheitä ja 4 % järjestelmien vikoja. (lähde)	käyttö ja phishing). Samalla jaksolla raportoitiin 2577 muuta tietosuojaloukkausta (mm. henkilötietojen paljastaminen suullisesti ja sähköpostin lähettäminen väärälle vastaanottajalle) (lähde)		Ruotsin tietosuojala- kiin. (lähde)	Standard-Datenschutzmodellia . Mallin hyväksyivät kansallinen tietosuojaja ilmaisunvapausvaltuutettu sekä osavaltioiden valvontaviranomaiset 25-26.4.2018. Malli perustuu saata- vuuden, luottamuk- sellisuuden, eheyden ja läpinäkyvyyden to- teuttamiseen teknis- ten ja organisatoris- ten toimintojen ja suoatoimenpiteiden avulla. Malli muodos- taa yhtenäisen, avoi- men ja ymmärrettä- vän kehyksen tieto- suojaviranomaisten työlle ja se tukee or- ganisaatioiden ja yri- tysten henkilötietojen käsittelyjen menette- lyä. BfDI:n vuoden 2017-2018 toiminta- kertomuksen mukaan valvontaviranomai- selle raportoitiin 25.5.-31-12.2018 väli- senä aikana yhteensä 7293 tietosuojalouk- kausta (sivu 17).			lopun tietojen hallin- nan virheitä (lähde).

Liite 2 – Lähteitä

- Bischoff, P (2019) [Surveillance States: Which countries best protect privacy of their citizens?](#), [Accessed 16 Oct 2019], Comparitech, 15 October 2019
- Kettunen, P, Sandberg, S, Fredriksson, C (2016) Eurooppalaiset hallintojärjestelmät vertailussa, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 37/2016, Valtioneuvoston kanslia 20.9.2016
- OECD (2019) [ICT value added \(indicator\)](#). [Accessed on 11 Oct 2019]

Alankomaat

- Cyber Security Assessment Netherlands, CSAN 2019 (Cyber-+Security-+Assessment-+Netherlands-+2019.pdf), 2019
- Dutch Digitalisation Strategy - Getting the Netherlands ready for the digital future (Dutch+Digitalisation+strategy+def.pdf), 2018
- National Cyber Security Agenda – A cyber secure Netherlands (CSAgenda_EN_def_web_tcm32-339827.pdf)
- National Risk Assessment - The National Network of Safety and Security Analysts (Dutch National Risk Assessment 2019_tcm32-408907.pdf), 2019
- Quantitative Analysis of Dutch Research and Innovation in Key Technologies (Dutch+Research+and+Innovation+in+Key+Technologies.pdf), 2018
- Resilient critical infrastructure (Factsheet Critical Infrastructure ENG 2018_tcm32-240750.pdf), 2018
- Working Worldwide for the Security of the Netherlands - An Integrated International Security Strategy 2018-2022 (NL_International_Integrated_Security_Strategy_2018_2022.pdf)

Australia

- Australia's Cyber Security Strategy - Enabling innovation, growth & prosperity (PMC-Cyber-Strategy.pdf), 2016
- Australia's International Cyber Engagement Strategy (DFAT AICES_AccPDF.pdf), 2017
- Critical Infrastructure Resilience strategy: PLAN (CriticalInfrastructureResilienceStrategyPlan.PDF), 2015
- Essential Eight Maturity Model (PROTECT - Essential Eight Maturity Model (July 2019)_0.pdf), heinäkuu 2019
- National Emergency Risk Assessment Guidelines (handbook-10-national-emergency-risk-assessment-guidelines.pdf), 2015
- Risk Management Policy Framework (risk-management-policy-framework-544f3b1beeb16.pdf), 2014
- Vision 2025 (digital-transformation-strategy.pdf), 2018

Iso-Britannia

- A Strong Britain in an Age of Uncertainty: The National Security Strategy
- Expecting the unexpected - Business continuity in an uncertain world (expecting-the-unexpected.pdf), 2003
- Cyber Essentials (ECSCBriefingIntroCyberEssentials.pdf)
- Digital Strategy 2018-2020: Doing Development in a Digital World (DFID-Digital-Strategy-23-01-18a.pdf), 2018
- National Cyber Security Strategy 2016-2021 (UK_NCSSL_2016.pdf), 2016
- National Risk Register Of Civil Emergencies (UK_National_Risk_Register_2017.pdf), 2017
- National Security Strategy and Strategic Defence and Security Review 2015 (52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf), 2015

Israel

- Advancing National Cyberspace Capabilities Resolution No. 3611 of the Government (Israel_2011_Advancing National Cyberspace Capabilities.pdf), 2011
- Cyber Defense Methodology for an Organization Ver. 1.0 (Cyber1.0_english_617_A4_0.pdf), 2017
- Organizational Preparedness for a Cyber Crisis (Cyber crisis_575941_eng final 28.11.pdf)

Ruotsi

- För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (digitaliseringsstrategin_slutlig_170518-2.pdf), 2017

- Nationell risk- och förmågebedömning 2019 (msb1392_nationell-risk-o-formagebedomning_2019_web.pdf), 2019
- Nationell strategi för samhällets informations- och cybersäkerhet (skr-201617-213-bilaga-uppdatering-om-genomforandet.pdf), 2018 (alkuperäinen strategia ja sen päivitys)
- Nationell säkerhetsstrategi (nationell-sakerhetsstrategi.pdf), 2017

Saksa

- Cyber Security Strategy for Germany (110309_Br_A4_Cybersicherheit_EN_bf_pgr.indd.pdf), 2011
- Cyber-Sicherheitsstrategie für Deutschland 2016 (Cyber-Sicherheitsstrategie für Deutschland 2016.pdf), 2016
- Umsetzungsplan Bund 2017 Leitlinie für Informationssicherheit in der Bundesverwaltung (up-bund-2017.pdf), 2017
- IT-Grundschutz-Kompendium 2019 (IT_Grundschutz_Kompendium_Edition2019.pdf), 2019
- Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (KRITIS Strategie.pdf), 2009
- Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement Leitfaden für Unternehmen und Behörden (kritis-leitfaden.pdf), 2011
- Risikoanalyse im Bevölkerungsschutz Ein Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz (PiB_16_Risikoanalyse_im_Bevoelkerungsschutz.pdf), 2019
- Nationale E-Government-Strategie Fortschreibung 2015 (NEGS Fortschreibung.pdf), 2015
- Digitalisierung gestalten - Umsetzungsstrategie der Bundesregierung (digitalisierung-gestalten-download-bpa-data.pdf), 2019
- Die Lage der IT-Sicherheit in Deutschland 2019 (Lagebericht2019.pdf), 2019
- Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen Betrachtungszeitraum 2018 (Cyber-Sicherheits-Umfrage 2018.pdf), 2018
- Das Standard-Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (SDM-Methode_V1.1.pdf), 2018
- Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterung (INFO1.pdf), 2019
- Das berufliche Leitbild der Datenschutzbeauftragten Code of Practice for Data Protection Officers (BvD-Berufsbild_Auflage-4_dt_en.pdf), 2018

Venäjä

- [Digital Economy of the Russian Federation No 1632](#) [Accessed 7 Feb 2020], 2017
- Doctrine of Information Security of the Russian Federation No 646 (Ukaz_Prezidenta_Rossiiskoi_Federatsii_ot_05122016.pdf) (Russian original), 2016
- [Doctrine of Information Security of the Russian Federation](#) (Doctrine of Information Security of the Russian Federation.pdf), 2016 (epävirallinen käännös)
- Hacks, leaks and disruptions - Russian cyber strategies, (CP_148.pdf), CHAILLOT PAPER N° 148, 2018, European Union Institute for Security Studies
- Military Doctrine of the Russian Federation (Military Doctrine of the Russian Federation - RU.pdf)
- National Security Strategy of the Russian Federation No 683 (National Security Strategy of the Russian Federation - RU.pdf), 2015
- [Objectives of the Russian Armed Forces](#) [Accessed 3 Feb 2020]

Viro

- Digital Agenda 2020 for Estonia - Updated 2018 (summary) (digitalagenda2020_final.pdf), 2018
- Küberturvalisuse strateegia 2019-2022 (kuberturvalisuse_strateegia_2019-2022.pdf)
- National Defence Strategy Estonia (national_defence_strategy.pdf), 2011
- Estonian Internal Security Service Annual Review 2018 (AnnualRevies2018.pdf)

Suomi

- Kansallinen riskiarvio 2018, Sisäministeriön julkaisuja 2019:5
- Lehto, M, Limnell, J, Innola, E, Pöyhönen, Rusi, T, J, Salminen, M (2017) Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Valtioneuvoston kanslia 17.2.2017

- Lehto, M, Limnell, J, Kokkomäki, T, Pöyhönen, J, Salminen, M (2018) Kyberturvallisuuden strateginen johtaminen Suomessa, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, Valtioneuvoston kanslia 29.3.2018
- Suomen kyberturvallisuusstrategia 2019, VnP 3.10.2019, Turvallisuuskomitea
- Suomen tietoturvallisuusstrategia 2016, Liikenne- ja viestintäministeriön julkaisuja 7/2016
- Tuloksellisuustarkastuskertomus - valtionhallinnon riskienhallinta ja toimintojen jatkuvuus, 20/2018, Valtiontalouden tarkastusvirasto, Dnro 263/54/2017
- Yhteiskunnan turvallisuusstrategia 2017, VnP 2.11.2017, Turvallisuuskomitea



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.