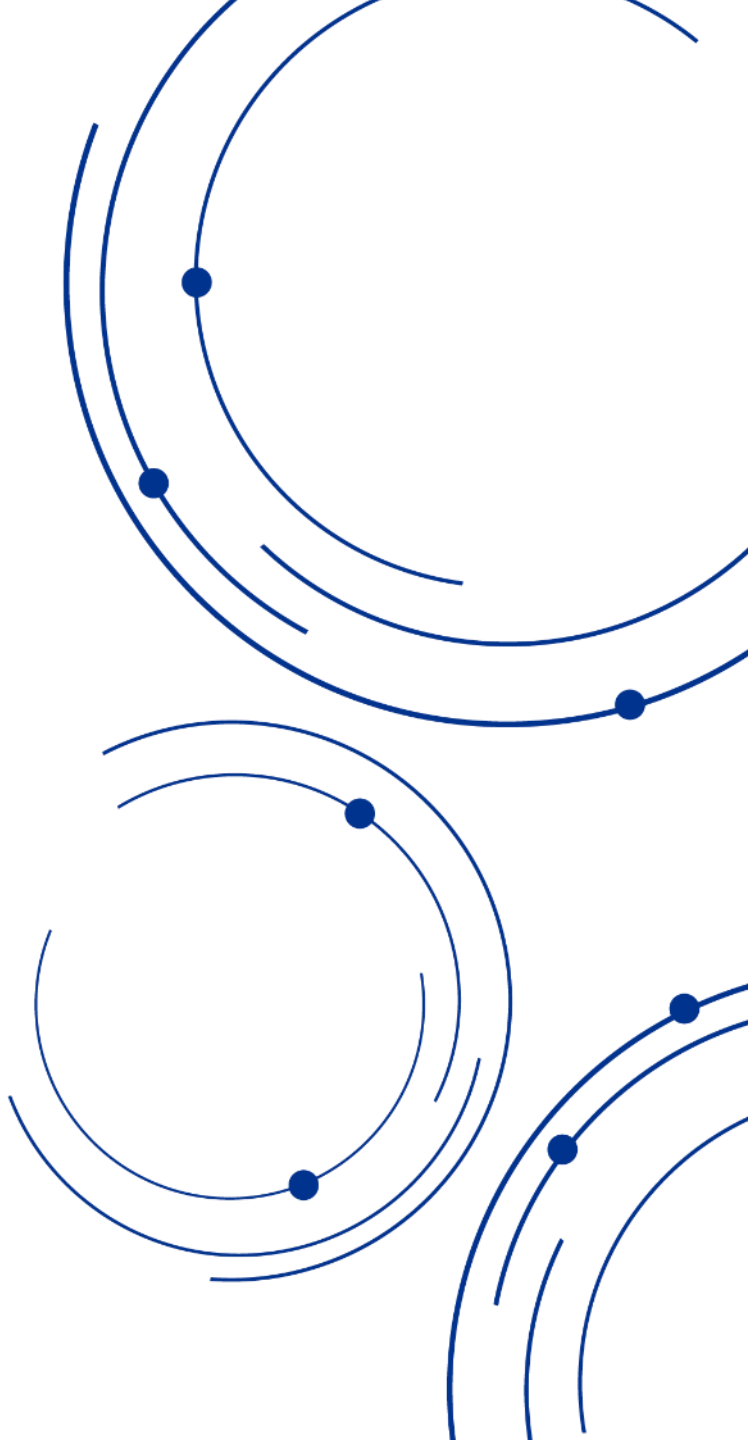
Digitaalisen turvallisuuden kansainvälisen vertailun yhteenveto



KPMG

Kv-vertailun lähtökohta

Digitaalisen turvallisuuden kansainvälinen vertailu

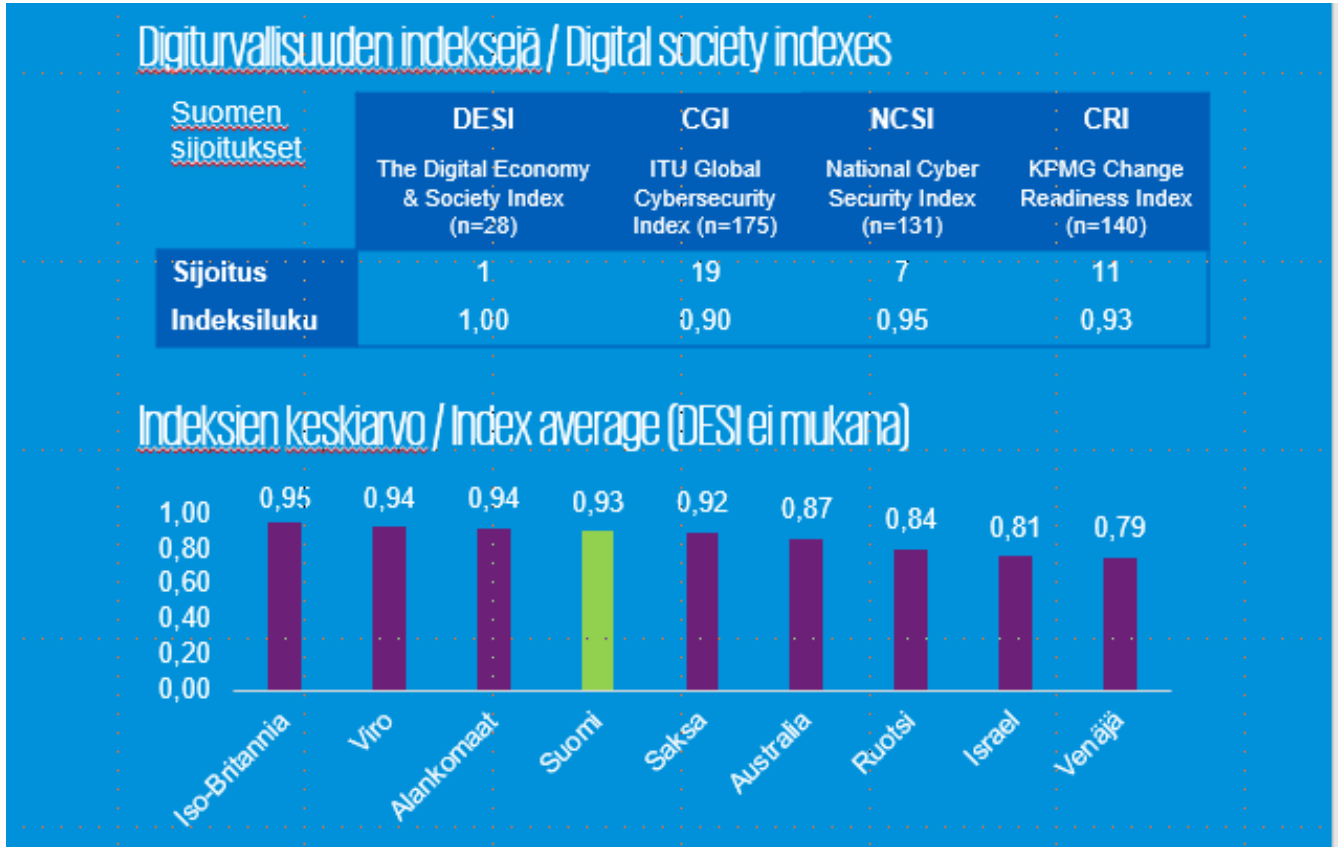
- Digitaalisen turvallisuuden kansainvälisessä vertailussa on koottu yhteen tietoa digitaalisen turvallisuuden ohjauksesta, tehtävistä, rakenteista, riskeistä ja resursseista valituissa maissa.
- Digitaalinen turvallisuus kattaa tässä asiayhteydessä riskienhallinnan, jatkuvuudenhallinnan ja varautumisen, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan.
- Verrokkivaltioksi valittiin Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Digitaalisen turvallisuuden kansainvälinen vertailu

- 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.



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.

Kunkin maan indeksiluvuista on laskettu keskiarvo, ja indeksilukujen keskiarvot on esitetty vertailussa pylväsdiagrammina.

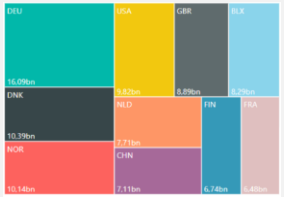
© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Verrokkivaltion ja sen digiturvallisuuteen liittyvän kokonaisuuden kuvaus

Poliittinen asema

Verrokkivaltion valtiosäännön kuvaus sekä digitaalisten oikeuksien avaaminen. Verrokkivaltion voimasuhteiden kuvaus kaupankäynnin ja liittoumien kautta.

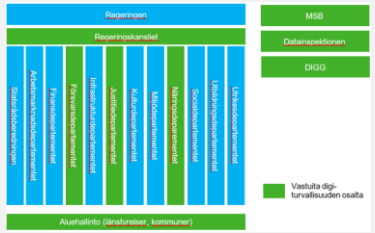


Poliittisen aseman osalta avataan lukijalle taustatietoa siitä, miten verrokkivaltio sijoittuu suhteessa muihin valtioihin. Lisäksi lukija saa ymmärryksen siitä, mitkä voimat ohjaavat valtion kehitystä.

Hallintorakenne

Verrokkivaltion hallinnon yleiskuva sekä digiturvallisuuden ohjaukseen liittyvien ministeriöiden ja virastojen tunnistaminen verrokkivaltiossa.

Digiturvallisuuden ohjauksen keskittyneisyyden tai hajautuneisuuden kuvaus.



Hallintorakenteen avulla lukija hahmottaa valtionhallinnon laajuuden ja sen, mihin osaan eri digitaalisen turvallisuuden elementtien ohjaus on sijoitettu. Lisäksi luvussa avataan yleisesti digitaalisen toiminnan suojaamista valtiotasolla.

Riskienhallinta

- Ohjausperiaatteet riskienhallintaan
- Merkittävät riskit ja uhat
- Hallintorakenteen tarkempi kuvaus

Jatkuvuudenhallinta

- Valmius- ja jatkuvuudenhallinnan ohjeistus
- Merkittävät harjoitukset
- Hallintorakenteiden tarkempi kuvaus

Tietoturva

- Tietoturvan hallintaan liittyvä ohjeistus
- Raportoidut tietoturvapoikkeamat
- Hallintorakenteiden tarkempi kuvaus

Kyberturvallisuus

- Strategiset linjaukset
- Hallintorakenteiden tarkempi kuvaus

Tietosuoja

- Tietosuojaan liittyvä lainsäädäntö ja ohjeistus
- Raportoidut tietosuojaloukkaukset
- Hallintorakenteiden tarkempi kuvaus

Digiturvallisuuden osa-alueiden osalta lukijalle avataan verrokkivaltion toimintaa kysymysten kautta. Kysymykset liittyvät tapahtumiin, teknologioihin, akateemiseen keskusteluun, sekä rakenteisiin, joilla digiturvallisuutta ohjataan.

Kehityshankkeet, innovaatiot sekä yleinen digiturvallisuuden valmius ja arkkitehtuuri

Verrokkivaltion kehityshankkeiden ja innovaatioiden kuvaus sekä valtion muutos- ja innovaatiokyvyn arviointi (EU:n osalta DESI-indeksi). Digiturvallisuuden osalta käytetään kansainvälisiä vertailuja (ITU CGI ja NCSI)

Selvityksessä kuvataan verrokkimaan merkittävät kehityshankkeet ja innovaatiot digiturvallisuuden saralla sekä avataan digiturvallisuuden tasoa suhteessa muihin maihin. Lukija saa kuvan valtion tahtotilasta ja tulevaisuuden painopisteistä.

Budjetointi ja resursointi

Verrokkivaltion digiturvallisuuden osa-alueisiin käyttämän rahamäärän avaaminen julkiseen budjettiin ja kansaiväliseen vertailudataan perustuen.

Budjetoinnin ja resursoinnin kautta lukijalle avataan verrokkivaltion tämän hetken panostuksia digiturvallisuuteen. Vertailuaineistona käytetään pääasiassa julkisia indeksejä ja OECD:n dataa.

Document Classification: KPMG Confidential

Digiturvallisuuden osa-alueiden sisältö

Riskienhallinta

Riskienhallintaa ohjaava lainsäädäntö

- Lainsäädännön merkittävimmät vahvuudet ja heikkoudet digitaalisen turvallisuuden näkökulmasta?

Riskienhallintaa koskevat strategiset linjaukset

- Mitkä ovat valtion strategiset digiturvallisuuteen liittyvät riskit?
- Kuka arvioi valtion strategisia riskejä?

Riskienhallinnan hallintorakenteet

- Kuka ylläpitää kokonaiskuvaa valtion riskeistä?
- Mikä on yksityissektorin rooli valtion riskienhallinnassa?
- Kuinka riskienhallintaprosessi on ohjeistettu?

Strateginen riskienhallinta

- Miten digiturvallisuuden osa-alueet on huomioitu riskienhallinnassa?
- Miten riskiarvioita käytetään valtion digiturvallisuuden kehittämisessä?

Jatkuvuudenhallinta

Varautumista ja jatkuvuuden hallintaa ohjaava lainsäädäntö

- Lainsäädännön merkittävimmät vahvuudet ja heikkoudet digitaalisen turvallisuuden näkökulmasta?

Varautumisen ja jatkuvuuden hallinnan strategiset linjaukset

- Mitkä ovat valtion jatkuvuuden hallinnan painopisteet?

Jatkuvuudenhallinnan hallintorakenteet

- Kuka on vastuussa varautumisesta ja jatkuvuuden hallinnasta?
- Mikä on yksityissektorin rooli valtion jatkuvuudenhallinnassa?
- Kuka määrittelee valtion kriittiset digitaaliset resurssit ja tietovarannot?
- Kuka on vastuussa kriittisten digitaalisten resurssien jatkuvuudesta?
- Mitä viitekehyksiä käytetään?
- Kuka ylläpitää valtion tason tilannekuvaa?
- Kuka koordinoi valtion harjoitustoimintaa?
- Miten jatkuvuuden hallinnan vaikuttavuutta mitataan?

Tietoturva

Tietoturvaa ohjaava lainsäädäntö

- Lainsäädännön merkittävimmät vahvuudet ja heikkoudet digitaalisen turvallisuuden näkökulmasta?

Tietoturvaa koskevat strategiset linjaukset

- Mitkä ovat valtion tietoturvan painopisteet?

Tietoturvan hallintorakenteet

- Kuka on päävastuussa valtion tietoturvallisuuden kehittämisestä?
- Mikä on yksityissektorin rooli valtion tietoturvallisuuden kehittämisessä?
- Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?
- Miten tietoturvaa valvotaan ja arvioidaan?

Raportoidut tietoturva-poikkeamat

Kyberturvallisuus

Kyberturvallisuutta ohjaava lainsäädäntö

- Lainsäädännön merkittävimmät vahvuudet ja heikkoudet digitaalisen turvallisuuden näkökulmasta?

Kyberturvallisuutta koskevat strategiset linjaukset

- Mitkä ovat kyberturvallisuuden painopisteet?

Kyberturvallisuuden hallintorakenteet

- Kuka on päävastuussa kyberturvallisuuden kehittämisestä?
- Mikä on yksityissektorin rooli valtion kyberturvallisuuden kehittämisessä?
- Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?
- Miten kyberturvallisuutta valvotaan ja arvioidaan?

Raportoidut kyberturvallisuus-tapahtumat

Tietosuoja

Tietosuojaa ohjaava lainsäädäntö

- Lainsäädännön merkittävimmät vahvuudet ja heikkoudet digitaalisen turvallisuuden näkökulmasta?

Tietosuojaa koskevat strategiset linjaukset

- Mitkä ovat valtion tietosuojan painopisteet?

Tietosuojan hallintorakenteet

- Kuka on päävastuussa tietosuojan kehittämisestä?
- Mikä on yksityissektorin rooli valtion tietosuojan kehittämisessä?
- Miten vastuut, toimivalta ja toteutus on jaettu viranomaisten kesken?
- Miten tietosuojaa valvotaan ja arvioidaan?

Raportoidut tietosuoja-loukkaukset

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

Maakohtaiset yhteenvedot

Maakohtainen yhteenveto - Alankomaat

Digitaalinen yhteiskunta

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. Digitaaliselle turvallisuudelle ei ole käytössä yhtenäistä määritelmää, CSA:ssa digitaalista turvallisuutta käytetään kyberturvallisuuden synonyyminä, mutta toisissa yhteyksissä sillä tarkoitetaan digitaalisten prosessien ja järjestelmien luottamuksellisuutta, eheyttä ja saatavuutta, mikä on lähempänä suomalaista tietoturvallisuuden määritelmää.

Johtaminen ja yhteistoiminta

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 yhteistyöfoorumeita kuten esimerkiksi Cyber Security Council (CSR) ja Digital Trust Centre (DTC).

Tilannekuva ja toimintaympäristön uhat

Alankomaiden NSCS julkaisee vuosittain kansallinen kyberturvallisuuden tilannekuvaraportin (Cyber Security Assessment Netherlands, CSAN 2019). Raportti käsittelee kyberturvallisuuden uhka-arviota, -painopistealueita ja häiriönsietokykyä. Uhka-arvioissa vakavimmaksi tekijäksi on nostettu valtiotoimijoiden Alankomaihin kohdistama vihamielinen toiminta, kuten esimerkiksi kybervakoilu, sabotaasi ja tietojen manipulointi. Raportti mainitsee esimerkkeinä Venäjän, Kiinan ja Iranin. Kybertoimintaympäristön häiriönsietokyvyn (resilienssin) ei koeta olevan kaikilta osin riittävä, eikä mittaamiseen tarvittavia menetelmiä ole. Lisäksi häiriönsietokyvyn tilannekuvaa pidetään puutteellisena. Kolmantena merkittävänä uhkana nähdään Alankomaiden riippuvuus pienestä määrästä muiden maiden ohjelmisto-, laitteisto- ja palvelutoimittajista.

Digitaalisen turvallisuuden kehityskohteet

Kyberturvallisuus on Alankomaissa kytketty 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 kestävää kasvua ja parantaa elämisen laatua (mm. digitaaliset terveyspalvelut).

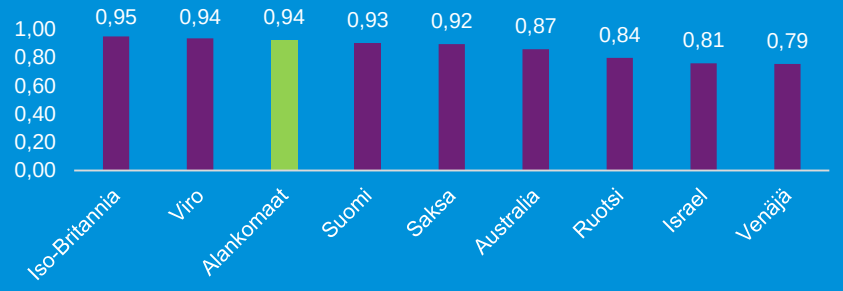
Toisaalta kyberturvallisuus nähdään toimialana, jonka kehittäminen avaa työmarkkinoille uusia mahdollisuuksia, parantaa digitaalisen toimintaympäristön turvallisuutta ja tuottaa kansallisia kyberturvallisuusratkaisuja yhteiskunnan käyttöön parantaen digitaalista omavaraisuutta. Kybertoimialan kehittämisen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

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average



Digiturvallisuuden vahvuuden 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 resiliessi
- digitaalisen resilienssin mittaaminen
- havainnointi- ja reagointikyvyn kehittäminen
- Alankomaiden hallinnon kyberturvallisuuden investoinnit

Maakohtainen yhteenveto - Australia

Digitaalinen yhteiskunta

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

Johtaminen ja yhteistoiminta

Australian puolustusministeriön hallinnonalaan kuuluva erillislaitos Australian Signals Directorate (ASD) vastaa mm. signaalitiedustelusta, aktiivisista kyberturvallisuuden vastatoimista (offensive cyber operations) datan ja järjestelmien analyyseista. 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 maailmanlaajuista kyberturvallisuustilannetta jatkuvasti.

Tilannekuva ja toimintaympäristön uhat

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 merkittävimpinä kyberturvallisuutta uhkaavina tekijöinä. Riskienhallintaa varten Australian hallitus on julkaissut riskienhallinnan viitekehyksen, joka noudattaa kansainvälistä riskienhallinnan standardia (ISO31000).

Digitaalisen turvallisuuden kehityskohteet

Kehitettävinä 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 kiristyshaittaohjelmia (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.

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.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average

Digiturvallisuuden vahvuuden 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 vaatimustenmukaisuuden toteutuminen

Maakohtainen yhteenveto - Iso-Britannia

Digitaalinen yhteiskunta

Kyberturvallisuusstrategian 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).

Johtaminen ja yhteistoiminta

Ison-Britannian kyberturvallisuuden koordinointi on pääministerin toimiston (Cabinet Office) vastuulla, mutta operatiivisista tehtävistä vastaa ulkoministeriön ohjaama GCHQ. 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 kyberturva-ammattilaisille.

Tilannekuva ja toimintaympäristön uhat

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. strategioiden havainnointikyvyn sekä osaamisen ja tietoisuuden kehittämistä.

Digitaalisen turvallisuuden kehityskohteet

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

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average

Digiturvallisuuden vahvuuden 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)

Maakohtainen yhteenveto - Israel

Digitaalinen yhteiskunta

Israelissa kyberturvallisuus kattaa digitaalisen turvallisuuden osa-alueet. Tietosuojaa arvioidaan henkilötietoja sisältävien tietokantojen kolmiportaiseen asteikkoon perustuvan luokittelun kautta (high, medium, basic).

Johtaminen ja yhteistoiminta

Valtionhallinnon ote maan tietoturvallisuuden kehittämiseen on tiukka. ”Kansallinen tietoturvavirasto” on suoraan pääministerin laajoilla valtuuksilla toimiva ylätason koordinoiva yksikkö, minkä lisäksi parlamentilla on kyberpuolustuskomitea. Israelin salainen poliisi (Israel Security Agency) ja sen kyberosasto keskittyvät mm. vakoilu- ja hyökkäysteknologioiden torjumiseen ja kehittämiseen. Oikeusministeriöllä on oma kyberrikollisuuteen keskittyvä jaostonsa. Lisäksi on muuta sektorikohtaista kyberturvallisuustoimintaa. Vuonna 2018 toimintansa aloitti Israelin kansallinen kyberdirektoraatti (Israel National Cyber Directorate), kun kaksi aiemmin erillisenä viranomaisen toiminutta kyberturvallisuusvirastoa yhdistettiin. Virasto vastaa keskitetysti kaikista siviiliyhteiskunnan kyberpuolustuksen toiminnoista, kuten politiikkojen määrittelystä, teknologian kehittämisestä ja operatiivisesta kybertoimintaympäristön suojaamisesta.

Tilannekuva ja toimintaympäristön uhat

Israelin poliittinen ympäristö on haastava ja Israel kokee olevansa jatkuvasti sotatilassa. Koko yhteiskunta panostaa merkittävästi sotilaalliseen toimintaan, terrorismin torjuntaan ja tiedustelutoimintaan. Kyberturvallisuuden osaajia pyritään valikoimaan hallinnon tehtäviin jo koulutuspolun alkuvaiheessa, mutta tästä huolimatta osaamisvajetta pidetään ongelmana. Israel rakentaa sekä puolustavaa että hyökkäyksellistä toimintakykyä.

Digitaalisen turvallisuuden kehityskohteet

Israeli on systemaattisesti kehittänyt vahvaa globaalia tietoturvallisuusteknologiaa tuottavaa yritysklusteria, jonka liikevaihto 2017 oli kolmen miljardin dollarin luokkaa. Be’er Shevaan perustetu klusteri kokoaa yhteen kansallisia ja kansainvälisiä yrityksiä, oppilaitoksia ja hallinnon osia.

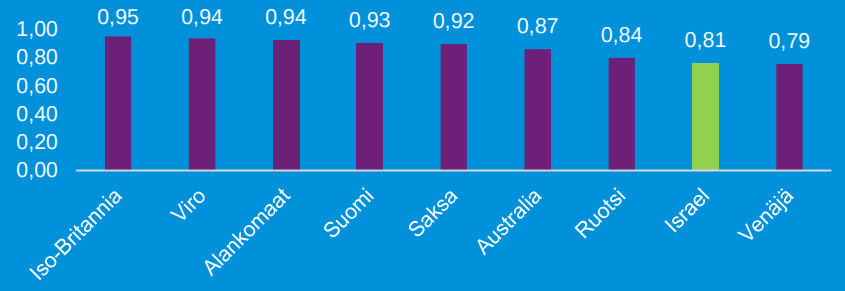
Israelin kokemat turvallisuusuhkat ja sen geopoliittinen asema ovat kyberturvallisuuteen panostamisen taustalla. Israel on teknologisesti selvästi edellä niitä Lähi-Idän valtioita ja toimijoita, jotka se kokee uhkikseen, joten myös hyökkäyksellistä kyberympäristön toimintakykyä on kehitetty. Tunnettuja, Iranin uraanirikastamoja vastaan kohdistettuja kyberhyökkäyksiä pidetään melko yleisesti Israelin ideoimina.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average



Digiturvallisuuden vahvuuden ja kehityskohteet

Vahvuudet

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

Kehityskohteet

- ei avointa tiedon jakamista (englanniksi)

Maakohtainen yhteenveto - Ruotsi

Digitaalinen yhteiskunta

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.

Johtaminen ja yhteistoiminta

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), tietosuojaviranomainen Datainspektionen ja valtionhallinnon digitalisointia koordinoiva DIGG. MSB:ssä teknisestä kyberturvallisuudesta vastaa erillinen osasto. Valtakunnallinen varautumisharjoitusten koordinointi 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 signaalitiedustelulaitoksen (FRA), puolustusvoimien ja turvallisuuspoliisin kanssa valmistella uuden kyberturvallisuuskeskuksen perustamista vuonna 2020. Uuden viranomaisen on tarkoitus vahvistaa Ruotsin kykyä estää ja havaita kyberturvallisuusuhkia, reagoida niihin sekä vähentää haavoittuvuuksia. Viraston on lisäksi tarkoitus tuottaa riskien, uhkien ja haavoittuvuuksien tilannekuvaa julkiselle sektorille ja yrityksille ja toimia hallituksen neuvonantajana kyberturvallisuusasioissa.

Tilannekuva ja toimintaympäristön uhat

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.

Digitaalisen turvallisuuden kehityskohteet

Ruotsin strategisissa suunnitelmissa 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). Viranomaisyhteistyötä varten MSB ylläpitää SAMFI-työryhmää (Samverkansgruppen för informationssäkerhet), jossa ovat mukana keskushallinnon virastot, joilla on tietoturvallisuuteen liittyviä. Julkishallinnon ja yksityissektorin yhteistyö perustuu kuitenkin vapaaehtoisuuteen, eikä yksityisen sektorin tehtäviä tai vastuita digitaalisen yhteiskunnan turvaamisessa ole kuvattu kovinkaan tarkasti.

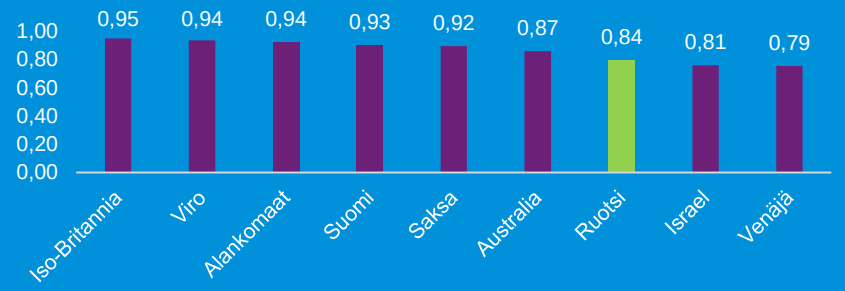
Ruotsin digitalisaatiostrategiassa (N2017/03643/D) on kuvattu viisi painopistettä kestävän digitalisoidun yhteiskunnan saavuttamiseksi: digitaalinen osaaminen, digiturvallisuus, digitaaliset innovaatiot, johtaminen digitalisaation avulla ja digitaalinen infrastruktuuri. Kullekin osa-alueelle on kirjattu 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.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average



Digiturvallisuuden vahvuuden ja kehityskohteet

Vahvuudet

+ harjoitustoiminnan keskitetty koordinointi
+ 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

Maakohtainen yhteenveto - Saksa

Digitaalinen yhteiskunta

Saksassa termiä digiturvallisuus (digitale Sicherheit) käytetään yleensä, kun tarkoitetaan kuluttajien tietoturvallista toimintaa digitaalisessa toimintaympäristössä ja tietotekniikan parissa. Saksan korkeimman tietoturvaviranomaisen BSI:n käyttämässä terminologiassa kyberturvallisuus (Cyber-Sicherheit) ulottuu kaikkiin tieto- ja viestintätekniikkaa koskevan tietoturvan näkökohtiin. Kyberturvallisuus kattaa kaiken Internetiin ja vastaaviin verkkoihin liitetyn tietotekniikan. Se sisältää myös viestinnän, sovellukset, prosessit ja niihin perustuvan prosessoidun tiedon.

Johtaminen ja yhteistoiminta

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 (BdfI) lisäksi jokaisessa 16 osavaltiossa on oma paikallisviranomainen.

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

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, mutta yksityissektorilla sen soveltaminen ei 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.

Digitaalisen turvallisuuden kehityskohteet

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.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average

Digiturvallisuuden vahvuuden 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 hierarkkista, koordinointi syö resursseja

Maakohtainen yhteenveto - Venäjä

Digitaalinen yhteiskunta sekä johtaminen ja yhteistoiminta

Venäjän kekskeinen digiturvallisuutta määrittelevä dokumenttin on Venäjän ulkoministeriön (Министерство иностранных дел Российской Федерации) julkaisema tietoturvallisuusdoktriini. Sen mukaan tietoturvallisuus on yksityisten kansalaisten, yhteiskunnan ja valtion suojaamista sisäisiltä ja ulkoisilta turvallisuusuhilta. Erilaiset valtionhallinnon organisaatiot ja paikallisviranomaiset käyttävät mm. lainsäädäntöä, teknologioita, analyyttisia ja organisatorisia keinoja sekä tiedustelua ja vastatiedustelua uhkien ennustamiseksi, havaitsemiseksi ja torjumiseksi sekä vaikutusten vähentämiseksi. Venäjällä on myös tärkeä ”Digitaalisen talouden ohjelma”, joka käsittelee talouden modernisoimista ja digitalisoitumista yleensä.

Tilannekuva ja toimintaympäristön uhat

Tietoturvallisuusdoktriinin mukaan muiden valtioiden informaatiovaikuttaminen ja teknologisten kykyjen kasvattaminen ovat Venäjälle merkittäviä poliittisia ja sotilaallisia uhkia, joilla valtion vakautta ja itsemääräämisoikeutta pyritään horjuttamaan. Terroristiryhmittymien ja ääriliikkeiden vihamielinen toiminta digitaalisessa toimintaympäristössä sekä kyberrikollisuuden vaikutukset erityisesti luotto- ja rahoitussektorilla katsotaan olevan lisääntymässä. Doktriinin mukaan Venäjän riippuvuus ulkomaisista ICT-teknologioista asettaa Venäjän sosio-ekonomisen kehityksen riippuvaiseksi muiden valtioiden tarvoitteista.

Digitaalisen turvallisuuden kehityskohteet

Venäjä on määritellyt tietoturvallisuudelle strategisia tavoitteita mm. puolustuksen, valtion turvallisuuden, vakauden, itsemääräämisoikeuden ja alueellisen koskemattomuuden sekä talouden näkökulmista. Tavoitteissa korostetaan erityisesti ulkopuolelta tulevien uhkien ennakointia, tunnistamista ja torjumista. Esimerkkinä tilannekuvan kehittämisestä on hyökkäyksiä havaitseva, lähinnä Suomen HAVAROa vastaava GosSOPKA-järjestelmä. Tutkimusta ja kehitystä kohdennetaan Venäjän omien teknologioiden kehittämiseen vähentämään riippuvuutta muista valtioista.

Venäjän ”Itsenäinen Runet”-hankkeen tarkoituksen on varmistaa Venäjän sisäisen tietoverkon toimivuus kriisitilanteessa. Lainsäädännöllä pyritään varmistamaan, että tietoliikenneoperaattorit pystyvät takaamaan Venäjän sisäisen verkon toiminnan, vaikka se erotettaisiin muusta maailmasta kriisitilanteessa joko valtion omien tarpeiden tai ulkopuolisten tekijöiden perusteella.

Tietosuojaan liittyy vaatimus, jonka mukaan Internet-palveluista kerättävät käyttäjien henkilötiedot on talletettava myös venäläisille palvelimille. Tietojen siirtämistä edelleen kolmansiin maihin ei ole kielletty, mutta käyttäjätietojen on kuitenkin pysyttävä Venäjällä, jossa valtio voi kontrolloida niitä tarpeen mukaan.

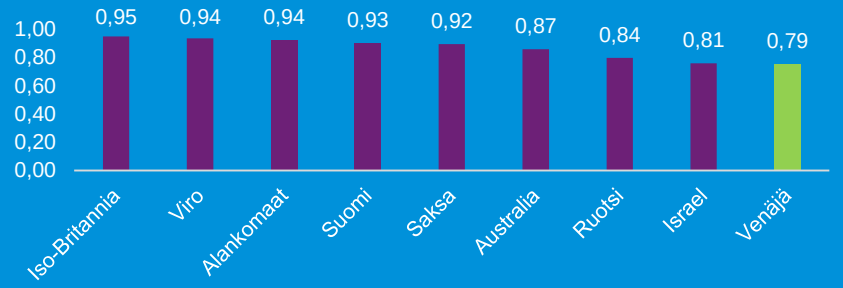
Venäjä ei ole liittynyt kaikkiin kansainvälisiin sopimuksiin kuten esimerkiksi poliisin mahdollisuuteen tutkia kyberrikollisuutta maasta toiseen. Venäjä vaikuttaa pelkäävän, että se vaarantaisi valtion kansallisen itsemääräämisoikeutta.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average



Digiturvallisuuden vahvuuden ja kehityskohteet

Vahvuudet

+ kyberomavaraisuuden johdonmukainen kehittäminen
+ tietoturvallisuuden strategisten tavoitteiden määrittely

Kehityskohteet

- merkittävä riippuvuus muiden valtioiden tuottamista teknologioista
- tunnistetut tietoturvallisuuden uhkat pääasiassa ulkpuolelta tulevia

Maakohtainen yhteenveto - Viro

Digitaalinen yhteiskunta

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).

Johtaminen ja yhteistoiminta

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.

Tilannekuva ja toimintaympäristön uhat

Viro on varautunut valtion digitaalisen jatkuvuuden toiminnan jatkamiseen tilanteessa, jossa valtio on menettänyt alueensa maantieteellisen hallinnan. Virolla on Luxemburgin kanssa sopimus tieto- ja tietojärjestelmien säilyttämisestä (ns. Data Embassy) laaja-alaisen kyberhyökkäyksen, luonnonkatastrofin tai tavanomaisesta datakeskukseen kohdistuvan tavanomaisen hyökkäyksen varalle.

Digitaalisen turvallisuuden kehityskohteet

Viron kyberturvallisuusstrategia asettaa neljä tavoitetta: 1) Viro on kestävä digitaalinen yhteiskunta, joka luottaa vahvaan teknologiseen kestävyyteen 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 kyberturvallisuuskyvykkyyden. 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 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).

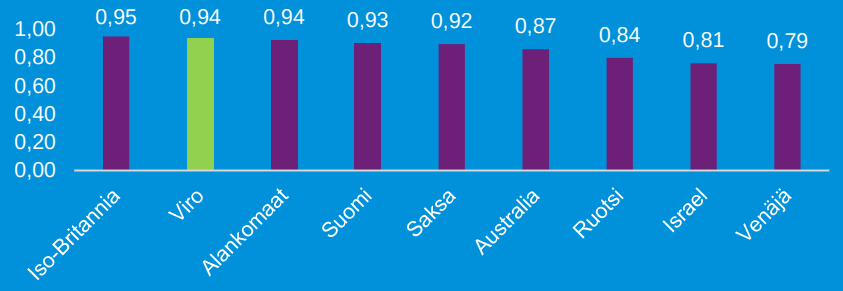
Viro on ottanut mallia Saksan IT-Grundschutzista, kun se on laatinut oman ISKE-tietoturvamallin. Virolla on myös RIHA-portaali, johon on koottu listaus kaikista julkisista tietojärjestelmistä. Eesti.ee –portaali on kansallinen väylä Viron julkisiin digipalveluihin sekä valtiolliseen julkiseen tietoon.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Digiturvallisuuden indeksejä / Digital society indexes

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

Indeksien keskiarvo / Index average



Digiturvallisuuden vahvuuden 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 koulutusresursointi
- kyberturvallisuuden erittäin voimakas riippuvuus EU:n rahoituksesta
- voimakas riippuvuus NATOn kyberkeskuksesta (The NATO Cooperative Cyber Defence Centre of Excellence)

KPMG

Kv-vertailun yhteenveto

Yhteenveto KV-vertailun johtopäätöksistä ja suosituksista

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.
Lainsäädäntö	• Verrokkivaltioiden digitaalisen turvallisuuden osa-alueita koskeva lainsäädäntö ei ole kovin yhtenäinen. Kyberturvallisuuden merkitys on kuitenkin tunnistettu laajasti ja monissa maissa ja lainsäädäntöä on pyritty kehittämään vastaamaan digitaalisen toimintaympäristön nopeita muutoksia. • 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.
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. • Kansainvälinen yhteistoiminta edellyttää selkeitä vastuualueita ja rooleja. Suomen tulee arvioida digiturvallisuuden johtamisrakenteita, vastuita ja rooleja sekä uudistaa niitä vastaamaan kansainvälistä kehitystä. Koordinointi- ja toteutusvastuut voidaan jakaa osiin, mutta vastuualueet tulee määrittää selkeästi toimivan kansallisen ja kansainvälisen yhteistyön takaamiseksi. Suomen tulee lisätä yhteistoimintaa edellä mainittujen kyberturvallisuuden aktiivisten toimijoiden välillä.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Yhteenveto KV-vertailun johtopäätöksistä ja suosituksista

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 riskianalyyseja 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 digiturvallisuustaitojen kehittäminen tulee olla strateginen painopiste koko yhteiskunnan laajuisesti.
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.

© 2019 KPMG Oy Ab, a Finnish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential