Digitaalinen puolustuskyky osana kokonaisturvallisuutta

Kyberturvallisuuden kehitys Suomessa vuosina 2010–2024

Poliittisen historian

Pro gradu -tutkielma

Laatija(t):

Riku Yamaguchi

16.5.2026

Turku

Pro gradu -tutkielma

Oppiaine: Poliittinen historia
Tekijä(t): Riku Yamaguchi
Otsikko: *Digitaalinen puolustuskyky osana kokonaisturvallisuutta* – Kyberturvallisuuden kehitys Suomessa vuosina 2010–2024
Sivumäärä: 105 sivua
Päivämäärä: 16.5.2026

Tiivistelmä

Kyberturvallisuus on erottamaton osa suomalaisen yhteiskunnan turvallisuutta. Sen tuomat uhkakuvat ovat kuitenkin verrattain uusia, ja aihe on noussut keskeiseksi osaksi kansallista kokonaisturvallisuutta nopeasti ja vaivihkaa. Tämä pro gradu -tutkielma tutkii, miten kyberturvallisuus vakiintui osaksi suomalaisen yhteiskunnan turvallisuusajattelua vuosina 2010–2024, ja miten Suomen valtionjohto ja -hallinto on siihen suhtautunut. Lisäksi siinä tarkastellaan, mitkä tekijät ja toimijat ovat tähän kokonaisuuteen vaikuttaneet ja millaisten hallinnollisten vaiheiden läpi prosessi on kulkenut.

Tutkielmassa hyödynnetään valtionhallinnon turvallisuutta ja kyberturvallisuutta käsitteleviä linjaavia asiakirjakokonaisuuksia, kuten kyberturvallisuusstrategioita, puolustusselontekoja, ulko- ja turvallisuuspoliittisia selontekoja sekä yhteiskunnan turvallisuusstrategioita. Aineistoa on täydennetty tarkasteluajanjakson hallitusohjelmilla sekä muilla aihetta käsittelevillä asiakirjoilla. Tutkielmassa hyödynnetään historiantutkimuksen perusmenetelmiä sekä turvallistamisteoriaa.

Tutkimustulokset osoittavat, että kyberturvallisuus vakiintui ja institutionalisoitui osaksi kansallista kokonaisturvallisuutta ensi kädessä ulkoisten ja sisäisten shokkien seurauksena. Kyberturvailmiöihin suhtautuminen on ollut reaktiivista ja iteratiivisesti opettelevaa. Suomen kyberturvallisuuden tila on tarkastelujakson aikana ollut kansainvälisesti verrattuna varsin hyvä, ja sen kybertoimintaympäristöä voidaan pitää turvallisena. Tästä huolimatta poliittista tahtoa, strategista johtajuutta ja siten riittäviä resursseja kyberturvallisuuden kehittämiseen on löytynyt lähtökohtaisesti vasta valitettavien kyberturvailmiöiden jälkeen.

Merkittävimmät kyberturvallisuuden turvallistajat olivat alan asiantuntijat, turvallisuusviranomaiset, Puolustusvoimat ja Suomen valtionhallinnon virkakunta. Poliittisten päättäjien kiinnostus aiheeseen oli vaihtelevaa. Eniten Suomen kybertoimintaympäristön kehitykseen ovat vaikuttaneet teknologisen kehityksen myötä kiihtyvä digitalisaatio sekä muuttunut turvallisuusympäristö, jossa vihamielisen kybervaikuttamisen nähdään olevan todennäköinen uhka Suomen turvallisuudelle.

Avainsanat: Kyberturvallisuus, kokonaisturvallisuus, tieto- ja viestintäyhteydet, turvallistaminen, resilienssi, kriisinkestävyys, digitalisaatio

Sisällysluettelo

1 Johdanto

Suomen valtioneuvosto linjasi ajankohtaisselonteossaan 13.4.2022, että Suomen ja Euroopan toiminta- ja turvallisuusympäristö on muuttunut perustavanlaatuisella tavalla. Tämän muutoksen aiheutti Itämeren alueen, ja laajemmin koko itäisen Euroopan, turvallisuustilanteen muuttuminen, jonka katalysaattorina voidaan pitää aikaisemmin samana vuonna Venäjän Ukrainassa aloittamaa hyökkäyssotaa 24.2.2022. Selonteossa arvioitiin, miten tämä muutos tulisi vaikuttamaan suomalaisen yhteiskunnan kokonaisturvallisuuteen eritellen tarkasteltaviksi muun muassa kriisinsietokyvyn, huoltovarmuuden ja sisäisen turvallisuuden ohella monia muita osa-alueita.[1] Yksi näistä mainituista osa-alueista – kyberturvallisuus – on kuitenkin luonteeltaan erityinen, sillä se on vaivihkaa noussut digitalisoituneen yhteiskunnan kriittiseksi tukipilariksi, jonka häiriöt heijastuvat herkästi kaikkiin muihin yhteiskunnan turvallisuuden osa-alueisiin.

Digitalisaatiolla tarkoitetaan yleisellä tasolla sitä, miten teknologisen kehityksen myötä digitaalitekniikka tulee yhä keskeisemmäksi osaksi jokapäiväistä arkielämäämme. Sen alku voidaan sijoittaa Suomessa 1980-luvulle, jolloin kotitietokoneet alkoivat yleistymään kotitalouksissa. Myöhemmin tärkeitä kehitysaskelia sille ovat olleet internet, mobiili-internet sekä sosiaalinen media.[2] Digitalisaatio on edennyt suomalaisessa yhteiskunnassa pitkälle. Tämä todetaan myös vuonna 2024 julkaistussa Suomen kyberturvallisuusstrategiassa. Sen mukaan yhä suurempi osa yhteiskunnan jokapäiväisistä toiminnoista ja palveluista sijoittuu digitaaliseen ympäristöön.[3] Huolimatta siitä, että digitalisaatio on kehittänyt suomalaisten elämänlaatua ja parantanut palveluita, on se kiistattomasti myös heikentänyt turvallisuuttamme luomalla uusia potentiaalisia uhkakuvia sekä hyökkäysvektoreita[4].

Vaikka Suomi on kansainvälisesti ollut pitkään kyberturvallisuuden sekä laajemmin ICT-kyvykkyyden kärkipäässä, huoli kyberturvallisuudesta nousi merkittävällä tavalla päättäjien ja valtionhallinnon yleiseen tietoisuuteen vasta 2010-luvun alkupuolella. ”Kyberturvallisuus” mainittiin terminä ensimmäisen kerran julkishallinnon ohjaavassa asiakirjassa vasta Yhteiskunnan turvallisuusstrategiassa vuonna 2010. Hallitusohjelmassa se esiintyi

[1] Valtioneuvoston Ajankohtaisselonteko turvallisuusympäristön muutoksesta, 13.4.2022, 1.
[2] Koiranen et al. 2016, 24–25.
[3] Valtioneuvoston kanslia 2024, 17.
[4] Hyökkäysvektoreilla tarkoitetaan kyberturvallisuudessa välillistä ”hyökkäyksen kantajaa”, jonka kautta tietojärjestelmään tai- verkkoon on mahdollista hyökätä.

ensimmäisen kerran Jyrki Kataisen hallituksen ohjelmassa vuonna 2011 ja eduskunnan istunnoissa 2012.[5]

Aalto yliopiston kyberturvallisuuden työelämäprofessori, Jarno Limnéll, on tutkinut kyber-käsitteen ilmestymisen ajankohtaa valtionhallinnon asiakirjoissa, ja sijoittaa sen läpimurron sekä hallinnollisen institutionalisoitumisen vuoteen 2013, jolloin julkaistiin Suomen ensimmäinen kyberturvallisuusstrategia. Seuraavana vuonna osana mainittua strategiaa perustettiin kyberturvallisuuskeskus.[6] Tätä seuranneiden reilun kymmenen vuoden aikana kyberturvallisuus on vaivihkaa hivuttautunut keskeiseksi osa-alueeksi turvallisuuskysymysten ytimeen.

1.1 Tutkimustehtävä ja aikaisempi tutkimus

Tutkimukseni kohteena on suomalaisen kyberturvallisuuden kehittyminen marginaalisesta turvallisuuden osa-alueesta keskeiseksi ja tärkeäksi osaksi suomalaisen yhteiskunnan kriisinkestävyyttä eli resilienssiä. Olen rajannut tarkasteltavan ajanjakson vuosiin 2010–2024. Aikarajausta perustelen noina vuosina Suomeen vaikuttaneilla tapahtumilla sekä käytettävissä olevalla aineistolla. Valitsin vuoden 2010 tutkimukseni aikarajauksen aloitusvuodeksi, jolloin ”kyberturvallisuus” ensimmäisen kerran esiintyi *Yhteiskunnan turvallisuusstrategiassa*, joka on valtioneuvoston strateginen asiakirja. Siinä kuvataan kokonaisturvallisuuden toimintamallia eli, miten yhteiskunnan elintärkeistä toiminnoista huolehditaan.[7] Seuranneina vuosina aihe nousi ensimmäisen kerran keskustelun aiheeksi eduskunnassa 2012, jolloin Suomen ensimmäistä kyberturvallisuusstrategia oli valmisteilla ja herätti mielenkiintoa Arkadianmäellä.

Tutkimusajanjakso loppuu vuoteen 2024, sillä vuosina 2022–2024 julkaistiin merkittäviä kansallisia ja kansainvälisiä digitalisaatioon ja kyberturvallisuuteen liittyviä linjaavia asiakirjoja, jolloin on varsin turvallista todeta, että kyberturvallisuus on institutionalisoitunut Suomalaiseen turvallisuusajatteluun. Tältä väliltä valitsemani asiakirjat toimivat kohtuullisen hyvin vertailun kohteena tarkasteltaessa eroja tavoissa puhua kyberturvallisuudesta

[5] PTK 132/2012 vp, J. Jääskeläinen, 18.12.2012 <https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiakirjat&docid=PTK+132/2012+ke+p+4> [Luettu 29.1.2025]; Limnéll 2014, 13.
[6] Limnéll 2014, 3, 16; Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös, 2013, 1–2.
[7] Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös, 1–2.

valtionhallinnon tasolla. Valtioneuvosto julkaisi Suomen digitaalisen kompassin 2022[8], joka on Suomen digitalisaatiokehitystä vuoteen 2030 saakka ohjaava kansallinen strateginen etenemissuunnitelma. Lisäksi se julkaisi vuonna 2024 kyberturvallisuusjohtajan johdolla Suomen neljännen kyberturvallisuusstrategian, joka on yhteensopiva vuonna 2022 julkaistun EU:n NIS2-kyberturvallisuusdirektiivin kanssa.[9] Lisäksi helmikuussa 2022 alkanut Venäjän hyökkäys Ukrainaan herätti Suomen sekä laajemmin Euroopan siihen, että alueellinen turvallisuustilanne oli muuttunut perustavanlaatuisesti. Myös Ukrainan sodan alussa osana hyökkäystä Venäjä hyödynsi kyberoperaatioita, joidenka vaikutukset jäivät kuitenkin vähäisemmiksi kuin arvioitiin Ukrainan kehittyneen kyberkyvykkyyden ansiosta, jota se oli vuoden 2014 jälkeen vaivihkaa, mutta määrätietoisesti, kehittänyt yhdessä liittolaistensa ja yksityisten toimijoiden kanssa.[10]

Tutkielmassa selvitän, miten Suomen valtionhallinto on suhtautunut kyberturvallisuuteen kansallisen turvallisuuden osa-alueena, ja miten tämä ymmärrys on muuttunut ja kehittynyt vuosina 2010–2024. Näin ollen tarkoituksena on muodostaa kokonaiskuvaa siitä, mitkä tapahtumat, päätökset ja toimijat vaikuttivat tähän muutokseen. Koska tarkoituksena on etenkin ymmärtää, miten Suomen valtiojohdon ja -hallinnon käsitys kyberturvallisuuden merkityksestä kehittyi, tutkielmassa hyödynnetään valtioneuvoston virallisia ja linjaavia asiakirjoja, kuten strategioita ja toimeenpano-ohjelmia.

Ensimmäisessä tutkimuskysymyksessäni selvitän, mikä on kyberturvallisuuden painoarvo tarkasteluaikavälin alussa ja lopussa sekä miten se on muuttunut niiden välissä. Millä tavalla siitä puhutaan keskeisissä valtioneuvoston työskentelyä ohjaavissa dokumenteissa verrattuna esimerkiksi muihin keskeisiin turvallisuuden osa-alueisiin. Lisäksi tutkielmassa tarkastelen kuinka usein ’kyberturvallisuus’ käsitteenä esiintyy, millaisiin käsitteisiin sitä yhdistetään ja mikä kyberturvallisuuden ja muiden turvallisuuden käsitteiden välinen merkityssuhde on. Samanaikaisesti tarkastelen myös kyberturvallisuuden semanttisen merkityksen kehitystä.

Toisessa tutkimuskysymyksessäni tarkastelen, miten primääriaineistossani on suhtauduttu kullakin käsittelemälläni ajanjaksolla senhetkiseen suomalaisen yhteiskunnan kybertoimintaympäristön tilaan ja täsmällisemmin sen turvallisuuteen. Pyrin vastaamaan

---

[8] Valtioneuvoston selonteko: Suomen digitaalinen kompassi 2022, passim.
[9] Suomen Kyberturvallisuusstrategia 2024, passim; Euroopan parlamentin ja neuvoston direktiivi 8 EU) 2022/2555. Euroopan unionin virallinen lehti, 2022.
[10] “Cyber War and Ukraine”. Center for Strategic and International Studies, 16.6.2022 <https://www.csis.org/analysis/cyber-war-and-ukraine> [luettu 31.1.2025].

siihen, mihin suuntaan suomalaisen yhteiskunnan kyberturvallisuutta on valtionhallinnossa haluttu viedä ja miten. Millaisia tavoitteita sille on asetettu tulevaisuuteen, ja mitä niillä on haluttu saavuttaa. Lisäksi tarkastelen, miten niiden saavuttamista on seurattu ja arvioitu. Toisaalta keskityn myös siihen, millaisia mahdollisuuksia suomalaisen kyberosaamisen kehittämisessä on nähty.

Kolmannessa tutkimuskysymyksessäni tutkin sitä, mistä kyberturvallisuuden turvallistamisen ajurit ovat lähtöisin. Oliko hallinnollisessa turvallistamisessa kyse sisäisestä muutosvoimasta, vai onko toiminta pikemminkin enemmän reaktiivista ja ympäristön tapahtumiin sopeutuvaa. Tarkoituksena on tehdä näkyväksi, mitkä tapahtumat saivat suomalaisen valtiojohdon reagoimaan ja puuttumaan suomalaisen kybertoimintaympäristön tilaan.

Poliittisen historian tulokulmasta kyberturvallisuus on sikäli kiinnostava ja hedelmällinen aihe, sillä siitä ei vielä ole ehditty tekemään tutkimusta. Aihe on kuitenkin tällä hetkellä, ja tulee vastaisuudessakin olemaan, kansallisen turvallisuuden kannalta äärimmäisen tärkeä, sillä teknologiset läpimurrot tulevat muuttamaan yhteiskunnan kyberturvallisuuden tilannekuvaa nopeasti. Toisaalta se on myös oiva esimerkki yhteiskunnallisen muutoksen tuomista haasteista, joihin yhteiskuntien ja valtioiden on sopeuduttava. Ilma- ja kybersodankäynnin dosentti Martti Lehto sekä informaatioteknologian professori Pekka Neittaanmäki ennustavat teoksessaan *Cyber Security: Power and Technology*, että sodankäynnissä on päässyt valloilleen uusi paradigma, jossa perinteinen sodan ja rauhan selkeä mustavalkoisuus hämärtyy, ja sen korvaa hybridivaikuttamisesta koostuva harmaan sävyjen alue, joka on jotain sodan ja rauhan väliltä. Kyberhyökkäykset muodostavat keskeinen osan hybridivaikuttamisesta, ja yhteiskunnan kyky torjua niitä tulee olemaan keskeinen osa sen resilienssiä.[11] Venäjän hyökkäys Ukrainaan 2022 oli otollinen esimerkki siitä, miten kyberoperaatioita voidaan käyttää perinteisten sotilaallisten toimien tukena. Venäjä hyökkäsi järjestelmällisesti Ukrainan yhteiskunnan kriittistä infrastruktuuria vastaan kaatamalla palvelunestohyökkäyksillä asevoimien ja pankkien verkkosivuja, tuhoamalla tärkeitä tietoja haittaohjelmilla sekä hyökkäämällä Ukrainan satelliittilaajakaistaan tavoitteenaan rampauttaa Ukrainan asevoimien johtamisjärjestelmä.[12]

Digitalisoitunut suomalainen yhteiskunta on haavoittuvainen kyberuhkille hyvin monella tavoin, minkä takia sen suojaaminen lähtee valtiohallinnon korkeimmalta tasolta ja jatkuu

---

[11] Lehto 2018, 1–5.
[12] ”Ukrainan infrastruktuuri kyberhyökkäyksen kohteena”. Upseeriliitto, 2/2022. <https://upseeriliitto.fi/verkkolehti/ukrainan-infrastruktuuri-kyberhyokkaysten-kohteena/>.

yksilön vastuulle saakka läpäisten yhteiskunnan eri kerrokset kauttaaltaan. Kyse on samalla kansallisesta turvallisuudesta, sillä terveydenhuollon, tietoliikenteen, finanssialan, sähköverkon sekä viranomaisten toiminta ovat kaikki riippuvaisia kybertoimintaympäristön häiriöttömyydestä.[13] Aihe on siis keskeinen poliittisen historian näkökulmasta.

Kyberturvallisuudesta on tehty kattava määrä tutkimusta tietotekniikan ja tietojenkäsittelytieteen aloilla sekä valtioneuvosto on erinäisillä strategioilla ja raporteilla koostanut aiheesta tilannekuvaa, mutta historiantutkimuksellista tutkimusta aiheen kehityksestä Suomessa ei ole aikaisemmin tehty. Valtiohallinnon, Suomen päättäjien tai eduskunnan suhtautumisesta kyberturvallisuuteen ei myöskään ole tehty tutkimusta. Liikenne- ja viestintävirasto Traficomin alainen kyberturvallisuuskeskus on listannut verkkosivuilleen kourallisen artikkeleita liittyen Suomeakin koskettaneisiin kyber- ja tietoturvailmiöihin.

Jarno Limnéll on tutkinut ”kyber” -alkuisten sanojen ensiesiintymistä tutkielmassaan *Kyber rantautui Suomeen*. Hänen tutkimusajanjaksonsa alkaa 1980-luvulta ja päättyy vuoteen 2014, jolloin tutkimus julkaistiin. Tämän pro gradu -tutkielman ja Limnéllin tutkimuksen tarkastelemat ajankohdat sijoittuvat toisiinsa nähden hieman limittäisesti.[14] Tämä antaa myös omalle tutkimukselleni hyvän pohjan ymmärtää ”kyberin” historiaa sekä kattavan katsauksen alan potentiaaliseen lähdemateriaaliin.

Limnéll on myös julkaissut tutkimuksen kansanedustajien suhtautumisesta kyberturvallisuuteen: *Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta* vuonna 2016. Tutkimus auttaa ymmärtämään, miten Eduskunnassa, joka käyttää Suomessa lainsäädäntövaltaa, ymmärrettiin kyberturvallisuuden senhetkinen tilanne.[15] Limnéll on myös kirjoittanut yhdessä alan muiden ammattilaisten kanssa teoksen *Kyberturvallisuus*, joka lähestyy kyberturvallisuutta käytännönläheisemmästä, arkisesta näkökulmasta. Teos analysoi julkaisuvuotenaan 2014 digitaalisen maailman turvallisuutta sekä tulevaisuutta. Limnéll on henkilökohtaisesti turvallisuustematiikalla uraa politiikassakin rakentanut entinen upseeri. Hän on omalta osaltaan ollut mukana turvallistamassa Suomalaista kybertoimintaympäristöä sekä luonut pohjaa aiheen tutkimusperinteelle.

[13] Järvinen 2018, 63.
[14] Limnéll 2014, 1.
[15] Limnéll 2016, passim.

Vuonna 2018 julkaistu Martti Lehdon ja Pekka Neittaanmäen teos *Cyber Security: Power and Technology* käsittelee sitä, kuinka kybermaailma on tuonut sodankäyntiin ja voimankäyttöön uuden ulottuvuuden, jossa tiedolla ja osaamisella on keskeinen rooli. Laajemmin teos käsittelee, miten merkittävä rooli kyberturvallisuudella ja -ominaisuuksilla tulee olemaan valtioiden puolustuksessa tulevaisuudessa.[16] Käytän teosta havainnollistamaan, miten alan johtavat tämänhetkiset asiantuntijat näkevät kyberturvallisuuden turvallisuuspoliittisen puolen.

Kyberturvallisuudella on oma vakiintunut termistönsä, ja tutkimuksen kannalta on merkittävää, että näitä termejä käytetään säännönmukaisesti ja oikein, jotta saadaan varmuus siitä, mistä tosiasiallisesti puhutaan. Aihe on myös siitä haastava, että arkipuheessa esimerkiksi sanoja ”kyberturvallisuus” ja ”tietoturvallisuus” käytetään toistensa synonyymeinä, vaikka ne eivät semanttisesti merkitse samaa. Toisaalta monien termien määritelmät ja merkitykset voivat olla limittäisiä. Merkitykseltään oikean termistön käyttämiseksi hyödynnän tutkimuksessani sanastokeskuksen julkaisemaa sanastokokoelmaa *Kyberturvallisuuden sanasto*. Sanasto on julkaistu 2018, ja sen tarkoituksena on määritellä kyberturvallisuuteen liittyvä käsitteistö sekä kansallista että kansainvälistä viestintää varten.[17]

Taustoitukseen käytän myös suomalaisen tietoturvatutkijan ja entisen F-Securen tutkimusjohtajan Mikko Hyppösen vuonna 2021 ja 2022 julkaisemia teoksia *Internet* ja *If it's smart, it's vulnerable*. *Internet* on alan ammattilaisen kirjoittama pohtiva teos siitä, miten digitalisaatio sekä verkkorikollisuus on kehittynyt viimeisen 30 vuoden aikana. Hyppönen käy teoksessaan läpi haittaohjelmien sekä verkkohuijauksien historiaa. Hyppönen tuo ilmi, kuinka verkkorikollisuus on kehittynyt tietoteknisesti näppärien nuorten kiusanteosta järjestäytyneeksi rikollisuudeksi sekä hybridisodankäynnin työkaluksi.[18] Teoksessa *If it's smart, it's vulnerable* Hyppönen käsittelee internetin hyötyjä ja haittoja, haittaohjelmien historiaa, aiheeseen liittyvän lainsäädännön kehitystä, huoltovarmuutta, yksityisyyttä, ”kybersodankäyntiä” ja tulevaisuuden skenaarioita.[19]

[16] Lehto 2018, 1–5.
[17] Sanastokeskus 2018, 3.
[18] Hyppönen 2021, passim.
[19] Hyppönen 2022, passim.

Tampereen yliopiston tietojenkäsittelytieteen emeritusprofessori, Pertti Järvinen, on kirjoittanut samasta aiheesta teoksen kolme vuotta aikaisemmin *Kyberuhka ja somesotaa*. Järvinen keskittyy enemmän kyberuhkiin ja niiden merkitykseen kansallisen turvallisuuden näkökulmasta. Nämä teokset tuovat tutkielmassani tarkastelluille asiakirjoille kontekstia ja helpottavat niiden tarkastelua niiden sen aikaisessa ajanjaksossa. Toisaalta Hyppösen vuosikymmenien kaltainen asiantuntijuus auttaa myös syventämään joidenkin tapahtumien taustoja ja tuomaan näkökulmia, joita lyhyemmän aikaa alaa seurannut ihminen ei välttämättä ymmärtäisi nostaa käsittelyyn.

Aihepiiristä on kirjoitettu myös pro gradu -tutkimuksia. Tuovi Helin Turun yliopistosta on kirjoittanut valtio-opin pro gradu -tutkielman samaa aihepiiriä käsittelevästä tematiikasta: hän tarkasteli, miten kybertoimintaympäristön uhkia ja riskejä käsiteltiin Suomen turvallisuuspoliittisissa dokumenteissa. Hänen tutkimusaikavälinsä on omaani kapeampi, ulottuen vuosiin 2013–2023.[20] Mikko Soikkeli Jyväskylän yliopiston informaatioteknologian tiedekunnasta puolestaan on kirjoittanut oman tutkielmansa siitä, miten lainsäädäntö velvoittaa ja ohjaa valtionhallinnon viranomaisia tieto- ja kyberturvallisuuden osalta.[21] Lisäksi Riikka Tanner kirjoitti pro gradu -tutkielman tapaustutkimuksena Suomen tiedustelulainsäädännön uudistamisesta vuosina 2015–2019. Hänkin hyödynsi tutkielmassaan turvallistamisteoriaa, mikä osaltaan myös vaikutti tämän tutkielman metodologisiin valintoihin.[22]

1.2 Metodi

Yhdistelen tutkielmassa historian tutkimuksen ja laadullisen tutkimuksen metodeja sekä lainaan valtio-opin turvallistamisteoriaa tavoitteessani tehdä näkyväksi suomalaisen kyberturvallisuuden kehityskulkua. Tarkoituksenani on koostaa historiantutkimuksellinen kuva ilmiöstä samalla analysoiden sitä turvallisuuden ja turvallistamisen tutkimuksen näkökulmasta.

Historiantutkimuksessa lähtökohtana on lähteiden pohjalta todellisuutta reflektoivan tulkinnan rekonstruoiminen. Sen ikuisena haasteena on absoluuttisen ja objektiivisen totuuden saavuttamattomuus. Kyse on tulkinnoista, sillä tapahtumahistoriallisten faktojen

[20] Helin 2025, 1–3.
[21] Soikkeli 2021, 1–3.
[22] Tanner 2019, 1–4.

selvittämisenkään jälkeen aikalaisten ja osallisten tulkinta ”totuudesta” voi olla hyvin erilainen. Esimerkiksi historian julkiset esitykset, joita valtiolliset tahot ylläpitävät, voivat erota kansanomaisista tulkinnoista. Nämäkään eivät välttämättä ole yhteneväisiä, kuten Suomen sisällissodan tapauksessa.[23] Historiantutkimuksellinen tarkastelutapa auttaa tutkijaa ennakoimaan ja tunnistamaan tällaisia haasteita pyrkimyksissä mahdollisimman uskottavan ja eheän tulkinnan koostamisessa. Historian perusmenetelminä voidaan pitää lähdekritiikkiä, tutkimuskohteen kontekstualisointia ja kirjoittaessa tehtävää teoreettista päättelyä.[24]

Lähdekritiikki on yksi keskisimmistä historiallisen tutkimuksen menetelmistä. Se jakautuu sisäiseen ja ulkoiseen lähdekritiikkiin. Sisäinen lähdekritiikki tarkoittaa kirjallisen jäljen syntyjäljen arviointia. Nykytutkimuksessa jäljen totuusarvon selvittämisen sijaan olennaisempaa on pohtia, miksi kyseinen lähde kuvaa tapahtunutta juuri sillä tavalla. Toisin sanoen painopiste on lähteen laatijan tavoitteissa. Tutkielmassa käsiteltävien strategioiden tarkastelu tästä näkökulmasta on arvokasta, sillä ne ovat linjaavia valtiollisia asiakirjoja, joilla pyritään vaikuttamaan valtionhallinnon ja sitä kautta laajemmin koko yhteiskunnan toimintaan. Ulkoinen lähdekritiikki puolestaan tarkastelee lähteen synty-ympäristön tarkastelua ja arvioi, millaisessa valossa esimerkiksi aikaisempi tutkimus sen ymmärtää – onko lähde juuri sitä, mitä se esittää olevansa, vaiko väärennös. Ulkoinen lähdekritiikki jää todennäköisesti pienempään rooliin, sillä lähtökohtaisesti on oletettavissa, että Suomen valtionhallinnolla ei ole intressejä väärentää oman sisäistä kehittämistä ohjaavaa asiakirjaa.[25]

Kontekstualisointi tarkoittaa puolestaan lähteiden ja tutkimuskohteen asettamista osaksi tutkittavan aikakauden yhteiskuntaa ja kulttuuria.[26] Kontekstualisoinnin keskeisenä haasteena tulee olemaan tutkimusajankohdan läheinen ajallinen etäisyys nykypäivästä. Näin monien senhetkisten tekijöiden erottaminen tämänpäiväisistä on erityisen tärkeää – etenkin, kun turvallisuuspoliittiset linjaukset ja päätökset ovat riippuvaisia senhetkisistä realiteeteista. Tärkeää onkin tarkastella tutkittavaa ilmiötä useasta eri näkökulmasta.[27]

Kolmas tässä tutkielmassa käytetty historiantutkimuksen perusmenetelmä on kirjoittamalla tapahtuva päättely. Käytännössä tämä tarkoittaa lähteiden ja tutkijan välisestä vuoropuhelusta,

[23] Ylikangas 2015, 13–15; Kalela 2000, 38–39.
[24] Tepora 2022, passim.
[25] Ibid., s.n.
[26] Ibid., s.n.
[27] Ibid., s.n.

kirjoittamisprosessista nousevasta hermeneuttisesta ymmärryksestä ja analyysityössä hyödynnettävistä tutkimusteorioista muodostuvaa kokonaisuutta. Kirjoittaminen ei ole pelkkä esitystekninen työkalu, vaan tapa, jolla päätelmät syntyvät ja primääriaineisto sovitetaan yhteen aiemman tutkimuksen sekä teoreettisen viitekehyksen kanssa. Kirjoittamisen kautta tulee ilmi tutkijan omat ennakkokäsitykset ja lähtökohdat sekä rajoitteet. Koska käyttävä aineisto on harvoin aukoton, täytyy tutkijan usein päätellä asioita – tämä prosessi tulee näkyväksi kirjoittamalla.[28]

Tutkija itse on altis oman aikansa synnyttämille ennakkokäsityksille, maailmankatsomukselle ja ymmärrykselle maailmasta.[29] Omien ennakkoasenteiden tunnistaminen on yhtä tärkeää kuin tutkielmassa käytettävien lähteiden syntykontekstin, tarkoituksen ja luonteen ymmärtäminen. Tässäkin tutkielmassa hyödyntämääni primääriaineistoa tulee tarkastella kriittisesti. Ne palvelevat syntyaikansa elämää, minkä takia niiden syntyyn vaikuttaneita tekijöitä sekä seurauksia tulee myös arvioida niiden rinnalla.[30]

Oman haasteensa tässä tutkielmassa aiheuttaa tutkimuskohteen ajallinen läheisyys. Ajallinen, maantieteellinen ja kulttuurinen läheisyys saattavat auttaa ymmärtämään tarkasteltavaa ilmiötä paremmin. Toisaalta tämä voi myös altistaa kyseenalaistamattomuudelle sekä päättelyharhoille, minkä lisäksi historia on monesti osoittanut, että etenkin turvallisuuspoliittisten päätösten todelliset realiteetit ovat paljastuneet vasta myöhemmin ”pölyn laskeuduttua”. Myös tieto- ja viestintätekniikan olemus äärimmäisen nopeasti kehittyvänä alana altistaa anakronismille – laskentateho, muistiteknologia sekä tietoverkot ovat kehittyneet räjähdysmäisesti viime vuosina nopeudella, jonka ennustaminen vain kymmeniäkin vuosia sitten on ollut lähes mahdotonta. Lähimenneisyyttä tutkittaessa kaikki tarpeelliset tiedonlähteet eivät ole välttämättä vielä saatavilla – arkistojen salassapitorajoitukset vaikeuttavat merkittävästi lähihistorian tutkimista.[31]

Lisäksi hyödynnän aineistoni analysoimiseen laadullista sisällönanalyysiä johtuen sen joustavuudesta sekä monipuolisuudesta, minkä takia sitä on mahdollista käyttää muiden teoreettisten viitekehyksien rinnalla.[32] Pyrin vastaamaan asettamaani tutkimuskysymykseen

[28] Tepora 2022, s.n.
[29] Kalela 2000, 40–42.
[30] Ylikangas 2015, 49–53.
[31] Lähteenkorva ja Pekkarinen 2000, 195.
[32] Tuomi ja Sarajärvi 2002 s.n.

valtionhallinnon toimintaa ohjaavien virallisten selontekojen, strategioiden ja raporttien kautta, minkä takia sisällönanalyysi soveltuu hyvin tutkielmassa hyödynnettäväksi tutkimusmetodiksi. Hyödynnän sitä analyysin ohella myös aineiston keruuprosessissa.

Laadullisen tutkimuksen asiantuntijoiden, Jouni Tuomin sekä Anneli Sarajärven, mukaan sisällönanalyysissä tekstistä etsitään merkityksiä. He argumentoivat, että historiallisessa analyysissa ja osassa sisällönanalyysilla toteutettuja tutkimuksia kyse on maailmansuhteesta, jossa ihminen tarkastelee todellisuutta ikään kuin ulkopuolelta. Tämän takia totuus on näin ollen sen tuottamista, miten tutkittavan ilmiön kokonaisuus ja aikalaiset näyttäytyvät tutkijalle sekä nykyihmiselle.[33] Tämä jaettu ymmärrys siitä, että tuotettava tutkimustieto on loppujen lopuksi tulkinta siitä, mitä on tapahtunut, sopii hyvin yhteen historiantutkimuksellisiin lähtökohtiin.

Tuomen ja Sarajärven mukaan laadullisessa tutkimuksessa usein keskenään sekaisin menevät *sisällön erittely*, eli dokumenttien kvantitatiivinen analyysi, ja *sisällönanalyysi*, dokumenttien sisällön sanallinen kuvailu.[34] Tässä tutkielmassa käytän juuri *sisällönanalyysiä*, sillä tärkeämpää on ymmärtää millaisissa konteksteissa ja asiayhteyksissä kyberturvallisuudesta on puhuttu, jotta selviää, millä tavalla sen paino- ja merkitysarvo on ajan saatossa kehittynyt. Hyödynnän myös sisällön erittelyä analyysini tukena, sillä frekvenssillä, jolla aihe esiintyy, on myös merkitystä.

Lähestyn tutkielmaa *aineistolähtöisen- ja teoriaohjaavan analyysin* kautta. Aineistolähtöisessä analyysissä pyritään rakentamaan tarkasteltavasta lähdeaineistosta teoreettinen kokonaisuus. Teoriaohjaavassa analyysissä puolestaan teoria on tutkimuksen apuna, mutta analyysi ei pohjaudu siihen suoraan. Näin ollen käyttämäni metodi muistuttaa läheisesti *abduktiivista päättelyä*, jossa tutkijan ajattelua ohjaa vaihtelevasti aineistolähteisyys ja valmiit mallit.[35]

Tässä tutkielmassa lähtökohtana on historiantutkimuksen rinnalla kansainvälisten suhteiden tutkimuksen Kööpenhaminan koulukunnan turvallistamisteoria (securitization), sillä se tarjoaa laajasti hyväksytyn ja skaalautuvan viitekehyksen turvallisuuden tutkimiseen ja tarkasteluun.

---

[33] Tuomi ja Sarajärvi 2002, 117–118.
[34] Ibid., 119–121.
[35] Ibid., 117–118.

Koulukunnan keskeiset tutkijat Barry Buzan, Ole Wæver ja Jaap De Wilde ottivat osaa 1980–1990-lukujen vaihteessa alalla syntyneeseen debattiin, jossa kansainväliselle toimikentälle nousi uusia turvallisuusagendoja, kuten ilmastonmuutos ja terrorismi. Tämä keskustelu haastoi perinteistä näkemystä, jossa turvallisuus oli tutkimusalana sotilaallis-valtiollisen sektorin yksinoikeus.[36] He argumentoivat, että turvallisuus ei ole objektiivinen olotila vaan sosiaalinen konstruktio, jolla jokin ilmiö tai aihe voidaan nostaa normaalina pidettävän yhteiskunnallisen menettelyn ja politiikan ulkopuolelle. Tämän *turvallistamiseksi* kutsutun menettelyn jälkeen kyseisen aiheen käsittelyyn voidaan kohdistaa toimia, joita muulloin ei voitaisi pitää yhteiskunnallisessa menettelyssä hyväksyttävinä tai sopivina.

Koulukunta sai alkunsa Buzanin vuonna 1991 julkaiseman teoksen, *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*, ja sen pohjalta käynnistyneen debatin seurauksena. Teoksessa Buzan tarkastelee ja kartoittaa, omien sanojensa mukaan filosofiselta pohjalta, miten turvallisuuden laajennettu, kiistelty konsepti rakentuu: mitä sillä tarkoitetaan ja miten sitä sovelletaan tiettyihin turvallisuuspolitiikan kohteisiin, kuten ihmisiin ja valtioihin sekä mitkä ovat turvallisuuden *viitekohteet*.[37] Buzan ei laadi turvallisuudelle kaiken kattavaa määritelmää, mutta pyrkii kuitenkin standardoimaan sitä semanttisesti siten, että alalla olisi yhtenäisempi ymmärrys siitä, mitä turvallisuudella tarkoitetaan: pohjimmaisena ajatuksena turvallisuudesta keskusteltaessa kyse on uhkien poissaolon tavoittelusta.[38]

Buzan ja Wæver tarjoavat myös analyyttisen työkalun tarkastelemaan, miten aiheita *turvallistetaan* ja käsittelevät aihetta teoksissa: *Security: A New Framework for* Analysis ja *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era* sekä artikkelissa "Securitization and rityritization" R. D. Lipschutzin toimittamassa teoksessa *On Security*. He myös samalla osallistuvat kansainvälisten suhteiden tutkimusalalla vallinneeseen keskusteluun turvallisuuden laajentamisesta perinteisen sotilaallis-valtiollisen käsityksen ulkopuolelle. Buzan erottaa viisi osa-aluetta, eli sektoria, joille turvallisuus heidän mukaansa on laajentunut: sotilaallisen, poliittisen, taloudellisen, yhteiskunnallisen ja ympäristöllisen. Sektorit ovat objektiivisten tilojen tai ilmiöiden sijaan niille ominaisten

---

[36] Buzan 1991, 29, 34; Wæver 1995, 20–23.
[37] Buzan 1991, 34–35.
[38] Buzan 1991, 37; Buzan et al. 1998, 195.

viitekohteiden rakenteiden määrittelemiä linssejä tai diskursseja, joiden läpi käsiteltävää kokonaisuutta tarkastellaan.[39]

Turvallisuus on Wæverin mukaan *puheteko* (speech act), eli toisin sanoen se ei ole objektiivinen olosuhde, vaan sosiaalinen konstruktio, joka luodaan lausumalla ”turvallisuus”. Yleensä lausuja on valtiollinen taho tai yhteiskunnallisen eliitin edustaja.[40] Wæver, Buzan ja de Wilde argumentoivat vuoden 1998 teoksessa turvallisuuden perimmäisen olemuksen olevan jäljitettävissä sen tutkimusta perinteisesti hallinneen sotilaallis-poliittisen lähtökohtaan, johtuen muun muassa alan turvallisuuteen vakiinnuttaneista mielleyhtymistä ja konnotaatioista. Waever et al. painottavat, että loppujen lopuksi puhuessamme turvallisuudesta, puhumme selviytymisestä. Tästä johdettuna he määrittelevät, että turvallisuusongelmat ovat luonteeltaan *eksistentiaalisisa uhkia* (existential threat), jotka kohdistuvat tärkeänä pidettyyn *viitekohteeseen* (referent object). *Viitekohde* on perinteisesti, mutta ei välttämättä yksinomaan, ollut valtio, hallinto, alue tai yhteiskunta. Sotilaallis-valtiollisessa perinteessä turvallisuutta konseptina on hyödynnetty legitimoimaan voimankäyttöä tai ottamaan käyttöön muita yhteiskunnallisesta normista poikkeavia valtaoikeuksia *viitekohdetta* uhkaavan *eksistentiaalisen uhkan* torjumiseksi.[41]

Teoriassa kaikki julkiset aiheet voidaan sijoittaa lineaariselle janalle, jonka toisessa päässä on ei-poliittiset, arkiset aiheet ja toisessa turvallistetut aiheet. Buzan, Wæver ja de Wilde havainnollistavat *turvallistamista* politisaation, eli asioiden nostamisen politikoinnin piiriin, äärimmäiseksi muodoksi. ”Turvallisuuden” lausuminen tekona ei kuitenkaan yksinomaan riitä *turvallistamiseen*. Tämä on vasta *turvallistamisteko* (securitizing move).[42] Sen tutkiminen on kuitenkin suhteellisen suorasukaista tarkastelemalla diskursseja ja poliittisia rakenteita: *”Milloin argumentin retorinen ja semioottinen rakenne onnistuu vakuuttamaan kuulijakuntansa hyväksymään sääntörikkomuksia, joita ei muutoin katsottaisi sormien lävitse?”*[43]

Toisin sanoen *turvallistamisteko* muuttuu *turvallistamiseksi* vasta, kun *yleisö* (audience) hyväksyy diskurssissa argumentoidun uhkan muodostavan *eksistentiaalisen uhkan* tärkeäksi

---

39 Waver 1995, 22, 27–28. Hansen ja Nissenbaum 2009, 1157.
40 Wæver 1995, 26, 31.
41 Wæver 1995; Buzan, et al, 21.
42 Wæver 1995, 23–25.
43 Ibid., 25.

koetulle ja siten suojelemisen arvoiselle *viitekohteelle*, jolloin tämä hyväksyy yhteiskunnallisista normeista poikkeavien vallankäyttöoikeuksien käyttöönoton. Lisäksi näillä yhteisistä säännöistä poikkeavilla toimilla tulee olla riittävän painavat vaikutukset kyseisen toimintaympäristön senhetkiseen tilanteeseen.[44] Tähän vaikuttavat kaksi tekijää, joita nimitetään *fasilitoiviksi olosuhteiksi* (facilitaiting conditions): *turvallistavan puheteon* lausujan sosiaalinen auktoriteetti "puhua" turvallisuutta uskottavasti ja *turvallistettavan* aiheen koettu uskottavuus.[45]

Kansainvälisten suhteiden tutkija Lene Hansen ja informaatiotieteen tutkija Helen Nissenbaum argumentoivat artikkelissaan "Digital Disaster, Cyber Security, and the Copenhagen School", että koulukunta sopii kyberturvallisuuden syntymisen ja kehittymisen analysointiin juuri sen takia, miten se käsittää turvallisuuden diskursiivisena modaliteettina, jolla on erityinen retorinen rakenne sekä poliittisia vaikutuksia.[46] Kyberturvallisuus on tutkielman aikana kehittynyt vakiintumattomasta jargonista jokapäiväisen turvallisuuden peruspilariksi.

Näin ollen analysoin turvallistamisteorian pohjalta, miten kyberturvallisuutta on turvallistettu tunnistamalla turvallistavien toimijoiden, *turvallistamistekojen, viitekohteiden,* onnistuneen ja epäonnistuneen turvallistamisen kautta. Yhdistäen teoriaa historiantutkimuksen menetelmiin jäljitän kyberturvallisuuden nousua keskeiseksi turvallisuuden osa-alueeksi. Johtuen ilmiön ajallisesta uutuudesta siihen linkittyy myös olennaisesti lähihistorian tutkimus. Tämän takia kiinnitän tutkielmassani huomiota haasteisiin, jotka liittyvät ajallisesti läheiseen tutkimusjaksoon.

Tutkielman työstämiseen on hyödynnetty generatiivista tekoälyä. Alkuvaiheessa sitä hyödynnettiin aineistonhakuun ja sen tiivistämiseen. Sitä on hyödynnetty lisäksi ideoinnissa, faktantarkistuksessa ja muotoilussa. Loppuvaiheessa sitä on käytetty ajatteluprosessin logiikan tarkistamiseen, oikolukuun sekä muihin ulkoasuun liittyviin korjauksiin. Käytetyt kielimallit olivat Claude Sonnet 4.6, Claude Opus 4.6, Claude Opus 4.7, ChatGPT 4o, Google Gemini 2.0 ja NotebookLM.

---

[44] Wæver 1995., 25–26, 31.
[45] Ibid., 33.
[46] Hansen ja Nissenbaum 2009, 1156.

1.3 Aineisto

Primääriaineisto koostuu 21:stä valtiohallinnon asiakirjasta, jotka on julkaistu vuosina 2010–2024. Niihin sisältyy myös asiakirjoja, joiden julkaisuvuosi asettuu kyseisen rajauksen ulkopuolelle, mutta vaikuttavat sisällöltään merkittävällä tavalla tähän. Jaan tutkielmassa käytettävän primääriaineiston kolmeen yläkategoriaan: Suomen kokonaisturvallisuutta käsitteleviin asiakirjoihin, suoraan suomalaisen yhteiskunnan kyberturvallisuuden tavoitetilaa ja sen toteutumista arvioiviin asiakirjoihin sekä muihin aihealueeseen liittyviin asiakirjoihin, kuten hallitusohjelmiin ja valtiopäiväaineistoon, joita ei kuitenkaan voi temaattisesti yhdistää omaksi kokonaisuudekseen.

Ensimmäisen kategorian muodostavat kokonaisturvallisuuden[47] kehitystä arvioivat selonteot ja asiakirjat. Näitä ovat muun muassa yhteiskunnan turvallisuusstrategiat vuosilta 2010 ja 2017, joissa käsitellään yhteiskunnan varautumisen perusperiaatteita ja kokonaisturvallisuuden toimintamallia. Lisäksi tähän ryhmään kuuluvat turvallisuus- ja puolustuspoliittinen selonteko vuodelta 2012 ja tästä kahteen erilliseen julkaisusarjaan jakautuneet puolustusselonteot vuosilta 2017, 2021 ja 2024 sekä ulko- ja turvallisuuspoliittisia selontekoja vuosilta 2016, 2020 ja 2024. Kyseiset julkaisut ovat selontekoja eduskunnalle, joissa esitellään Suomen turvallisuus- ja puolustuspolitiikkaan liittyviä teemoja muodostaen suuntaviivat Suomen politiikan painopisteille. Hyödynnän ensimmäisen kategorian aineistoa tutkiessani, miten kyberturvallisuuden merkitys on muuttunut painoarvoltaan merkittävissä valtiohallinnon asiakirjoissa. Strategiat ovat sisällöiltään runsaita, ja tarkastelen niitä arvioidakseni, miten kyberturvallisuus suhteutuu muihin turvallisuuskysymyksiin tutkimusajanjaksolla.

Toisen kategorian muodostavat Suomen kyberturvallisuusstrategiat vuosilta 2013, 2019 ja 2024 sekä niiden toimeenpanostrategiat ja muuta niiden ohessa julkaistut asiakirjat. Näitä ovat muun muassa vuoden 2014 *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma*, Suomen kyberturvallisuuden nykytilaa, tavoitetilaa ja tarvittavia toimenpiteitä tavoitetilan saavuttamiseksi arvoiva vuonna 2017 julkaistu asiakirja. Toisen kategorian aineisto on kerätty tarkempaa laadullista, kronologisesti etenevää tarkastelua varten, jonka pohjalta tehdään

[47] Kokonaisturvallisuudella tarkoitetaan yhteiskunnan elintärkeiden toimintojen turvaamista, joiksi nykyymmärryksen mukana luetaan johtaminen; kansainvälinen ja EU-toiminta; sisäinen turvallisuus; talous, infrastruktuuri ja huoltovarmuus; väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys.

näkyväksi, miten suomalaisen yhteiskunnan kyberturvallisuuden kehityskulkua on kuvattu sitä nimenomaisesti tarkastelevissa asiakirjoissa. Tämän luokan aineistot käsittelevät tyypillisesti strategisella, mutta varsin yksityiskohtaisella tasolla kyberturvallisuuden toivottua tavoitetilaa sekä toimenpiteitä siihen pääsemiseksi. Toimeenpano-ohjelmat sisältävät monesti pitkiäkin listoja tarvittavista toimenpiteistä.

Kolmas kategoria koostuu temaattisesti heterogeenisesti kokonaisuudesta, jotka sisällöltään kuitenkin tukee kahta aikaisempaa kategoriaa sekä auttavat täydentämään näitä ja asettamaan tutkimuskysymystä laajempaan yhteiskunnalliseen kontekstiin. Näitä aineistoja ovat muun muassa Jyrki Kataisen hallituksen hallitusohjelma ja *Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)*. Tähän kokonaisuuteen on koottu tutkielman kannalta merkittävät kyberturvallisuuden kehityskulkua täydentävät aineistot, joita ei voida sitoa temaattisesti kahteen aikaisempaan kategoriaan, mutta joiden sisällön hyödyntäminen on tutkittavan aiheen kannalta oleellista.

Tutkielmassa käytettävä sekundääriaineisto puolestaan koostuu kyberturvallisuutta käsittelevästä tutkimusaineistosta sekä viranomaisten dokumentaatiosta, joka käsittelee kyberturvallisuuden kehitystä. Tähän kuuluvat muun muassa julkisen hallinnon sisäiset selvitykset, kuten Valtiontalouden tarkastusviraston (VTV) tuloksellisuuskertomukset, jotka käsittelevät kyberturvallisuuden toteutumista. Samaan joukkoon kuuluvat myös tutkielman tarkasteluaikana vallassa olleiden hallitusten ohjelmakirjaukset, joita hyödynnän yleisen kybertietoisuuden tarkasteluun sekä toisaalta turvallisuuspoliittisen ”ajan hengen” arviointiin.

1.4 Katsaus Suomen poliittiseen ilmapiiriin ja hallituspohjiin 2010–2024

Tutkimuksen tarkastelujakso kattaa neljät eduskuntavaalit ja kuusi eri hallitusta. Jokainen näistä hallituksista on johtanut Suomea niin sanotun poliittisen ajan hengen, puoluepoliittisen tausta sekä toimintaympäristön hengen mukaisesti. Näin ollen niiden toimintaa tulee ymmärtää aikalaisten oman kontekstin kautta. Vuosien 2010–2024 välille mahtuu poliittiselta taustaltaan monia eri hallituksia, ja niiden tausta vaihtelee kirjavasti vasemmistovoittoisista oikeistovoittoisiin. Perinteisesti oikeistopuolueille turvallistaminen ja turvallisuusaiheisiin identifioituminen on ollut helpompaa, mikä toimii tässäkin tutkielmassa kirjoittajan tietynlaisena ennakkovääristymänä. Tätä toisaalta tukee osa tutkielman tuloksista, kuten Suomen tiedustelulainsäädäntöprosessi käynnistäminen Sipilän keskustaoikeistolaisen hallituksen kaudella. Toisaalta akateeminen kirjallisuus aiheesta tuntuu olevan ristiriitaista, ja Suomen lähihistoriasta löytyy vasemmistohallitusten tekemiä merkittäviä turvallisuuspoliittisia päätöksiä, kuten F-35 hävittäjien hankinta.[48]

Tämän tutkielman tarkasteluajanjakson alkaessa 16.12.2010 julkaistusta *Yhteiskunnan turvallisuusstrategiasta* Suomen istuva hallitus oli Mari Kiviniemen johtama keskustaoikeistolainen hallitus. Hallituksen ohjelma oli lyhyt, eikä hallituksen lyhyessä ohjelmassa ollut lainkaan mainintoja digitalisaatiosta, tieto- tai kyberturvallisuudesta. Hallituksen päämäärä oli kuitenkin palautua vuoden 2008 finanssikriisin aiheuttamasta taantumasta.[49]

Kiviniemeä seurasi Jyrki Kataisen sinipunahallitus, joka oli ensimmäinen hallitus, jonka ohjelmassa kyberturvallisuus esiintyi. Hallituksen painopisteet olivat kuitenkin, ajan hengen mukaisesti, vähemmän turvallisuuspolitiikassa. Ohjelman kolme kärkeä olivat huono-osaisuuden vähentäminen, julkisen talouden vakauttaminen ja kestävän talouskasvun, työllisyyden ja kilpailukyvyn vahvistaminen. Kataisen hallituksen aikana laitettiin vireille ja julkaistiin Suomen ensimmäinen kyberturvallisuusstrategia.[50] Kataisen hallitusta seurasi sen pohjalta perustettu Alexander Stubbin hallitus, joka kerkesi toimia noin vuoden. Hallituksen teemat olivat pitkälti samat kuin Kataisen hallituksella. Lisäksi vain kymmenen sivuisessa ohjelmassa kyberstrategian määrätietoista toimeenpanoa kirjattiin jatkettavan tavoitteena maailmanlaajuisen edelläkävijyyden saavuttaminen kyberuhkiin varautumisessa.[51]

Stubbin hallitusta seurasi keskustaoikeistolainen Juha Sipilän hallitus vuonna 2015. Osana hallituksen strategiaa kyber-alkuiset sanat esiintyvät kolme kertaa. Hallituksen aikana Suomen ja koko Euroopan turvallisuusympäristö muuttui merkittävästi: vuoden 2015 pakolaiskriisi osui suoraan hallituksen alkukauteen, kybertoimintaympäristön uhkat alkoivat realisoitua ja tämän myötä myös Suomen ensimmäiset tiedustelulait säädettiin. Ohjelman kärkiteemoja olivat työllisyys ja kilpailukyky; osaaminen ja koulutus; hyvinvointi; biotalous ja vihreä siirtymä; sekä digitalisaatio.[52]

---

[48] Raunio & Wagner 2020, passim; Fertl 2023, passim; “Tällainen on Suomen uusi hävittäjä F-35”. *Yle Uutiset.* 10.12.2021. <https://yle.fi/a/3-12224296>. [luettu: 10.5.2026].
[49] Suomi ehyenä kasvun, työllisyyden ja kestävyyden uralle, 2010, 1.
[50] Pääministeri Jyrki Kataisen hallituksen ohjelma 2011, 7, 22–23; Suomen kyberturvallisuusstrategia 2013.
[51] Pääministeri Alexander Stubbin hallituksen ohjelma 2014, 5, passim.
[52] Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen strateginen ohjelma 2015, 7, 8, 9, 35, passim.

Sote-uudistukseen loppumetreillään kaatunutta Sipilän hallitusta seurasi Antti Rinteen lyhytikäiseksi jäänyt ”vihreä kansanrintama”. Hallitus laati pitkän ohjelman, jossa kyberturvallisuus esiintyi temaattisesti 18 kertaa. Antti Rinteen erottua 10.12.2019 Sanna Marinista tuli hallituksen uusi pääministeri, ja ohjelma käytännössä jäi voimaan. Hallituksen teemoina olivat kestävä ilmastopolitiikka, aktiivinen kansainvälinen osallistuminen, oikeusvaltioperiaate, elinvoiman vahvistaminen, tasa-arvon lisääminen työmarkkinoilla sekä osaamiseen, koulutukseen ja innovaatioihin panostaminen.[53] Marinin hallituksen aikaa värittivät moninaiset kriisit, kuten Covid-19 koronaviruspandemia sekä Venäjän aloittama hyökkäyssota Ukrainassa. Suomen historian kannalta yksi merkittävimmistä kyberturvallisuuspoikkeamista tapahtui tällä hallituskaudella, kun psykoterapiakeskus Vastaamon potilaskertomukset anastettiin.

Viimeisin tutkielman tarkasteluajanjaksolla toiminut Suomen hallitus on Petteri Orpon oikeistohallitus. Orpon hallituksen aika tehtiin uusin päivitys kyberturvallisuusstrategiaan vuonna 2024. Hallitusohjelmassa oli talouden tasapainottamisen lisäksi voimakkaana teemana kriisinkestävyys ja sopeutuminen uuteen turvallisuusympäristöön. Kyberturvallisuus ilmeenkin ohjelmassa voimakkaitten – 35 kertaa.[54] Tutkimusaineisto kuitenkin osoittaa, että läpi koko tarkasteltavan ajanjakson, varmasti vilpittömistä pyrkimyksistä huolimatta, valtioneuvosto ei ole onnistunut sitoutumaan tarvittavalla tavalla itse asettamiinsa tavoitteisiin suomalaisen kybertoimintaympäristön turvaamiseksi. Tämä näkyy muun muassa riittämättömänä resurssointina sekä määrätiedottomina hankkeina. Tästä huolimatta on kuitenkin todettava, että Suomi on silti yksi maailman kyberturvallisimmista maista, esimerkiksi NCSI-indeksin perusteella.[55]

---

[53] Osallistava ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta 2019, passim.
[54] Vahva ja välittävä Suomi. Pääministeri Petteri Orpon hallituksen ohjelma 2023, 3–8, passim.
[55] National Cyber Security Indexin verkkosivut. <https://ncsi.ega.ee/ncsi-index/?order=-ncsi>. [luettu: 10.5.2026].

2 Jargonista kansallisen turvallisuuden kysymykseksi

2.1 Kyberturvallisuus debytoi *Yhteiskunnan turvallisuusstrategiassa* ja Jyrki Kataisen hallitusohjelmassa

Vuonna 2010 julkaistu yhteiskunnan turvallisuusstrategia oli ensimmäinen valtioneuvoston strateginen periaatepäätös, jossa kyberturvallisuuteen liittyvät riskit tunnistetaan turvallisuusympäristöön kohdistuvina uhkamalleina. Turvallisuusstrategian päämääränä oli antaa perusteet Suomen ulko-, turvallisuus- ja puolustuspolitiikan tärkeimpien tehtävien, eli ”itsenäisyyden, alueellisen koskemattomuuden ja perusarvojen turvaamisen, väestön turvallisuuden ja hyvinvoinnin edistämisen sekä yhteiskunnan toimivuuden ylläpitämisen - -” saavuttamiseksi.[56] Siinä muun muassa tunnistetaan ”elintärkeitä toimintoja vaarantavat uhkamallit ja niihin liittyvät mahdolliset häiriötilanteet”, joihin luetellaan ensimmäisen kerran myös ” tietoliikenteen ja tietojärjestelmien vakavat häiriöt – kyberuhkat”.[57]

Strategiassa *uhkamalleilla* viitataan turvallisuusympäristön mahdollisiin häiriöihin, jotka koskevat kansallista turvallisuutta eli valtiota, yhteiskuntaa ja väestöä. Strategiassa näiden uhkien globaalit ja yksilöihin vaikuttavat näkökulmat on rajattu käsittelyn ulkopuolelle, vaikka ne tunnistetaan. Kyberturvallisuuden uhkamallit on nostettu samaan ryhmään kuin ”poliittinen, taloudellinen ja sotilaallinen painostus” sekä ”sotilaallinen voiman käyttö”, mikä voidaan Kööpenhaminan koulukunnan turvallistamisteorian pohjalta tulkita *turvallistamisteoksi*.[58] Turvallistavasta puheteosta vaikuttavan ja onnistuneen tekee – teoriaan pohjaten – konteksti, jossa se mainitaan. Yhteiskunnan turvallisuusstrategia on merkittävä Suomen valtiojohdon linjaava asiakirja, joka määrittelee suomalaisen yhteiskunnan kansallisen turvallisuuden turvallisuuspoliittiset painopisteet sekä toimii ohjausasiakirjana koko julkishallinnolle valtuuttaen tämän edistämään siinä mainittuja asiakohtia.[59]

Strategiassa on eritelty oma alalukunsa kyberturvallisuuden uhkamalleille, vaikka termi ”kyberturvallisuus” ei itsessään asiakirjassa esiinny. Tarkemmin asiakokonaisuudesta puhutaan ”tietoliikenteen ja tietojärjestelmien vakavina häiriöinä, eli kyberuhkina”.

---

[56] Yhteiskunnan turvallisuusstrategia 2010, 3, 5.
[57] Ibid., 14.
[58] Ibid., 14.
[59] Buzan, et al., 1998, 25; Yhteiskunnan turvallisuusstrategia 2010, 5.

Strategiassa niitä käytetään kuvaamaan ”uhkaa, joka liittyy toisistaan riippuvaisiin verkostoihin, sisältäen erilaiset tieto- ja tiedonsiirtoverkot, internetin, puhelinverkot, tietokonejärjestelmät sekä kriittisen tuotannon sulautetut prosessorit ja kontrollointilaitteet”.[60] Vuonna 2018 julkaistu *Kyberturvallisuuden sanasto* määrittelee kybertoimintaympäristön seuraavalla tavalla: ”Kybertoimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet[61].” Tämän pohjalta voidaan todeta, että strategiassa kyberuhkilla tarkoitetaan kybertoimintaympäristöön kohdistuvia uhkia.

Alalle myöhemmin vakiintuneen sanaston puuttuminen sekä pääasiallisesti kybertoimintaympäristöä uhkaavien toimijoiden paikallistaminen verkkorikollisiin sekä terrorismiin heijastelee senhetkisen turvallisuustilanteen realiteetteja. Suomen ei todeta olevan vihamielisen valtiollisen vaikuttamisen kohteena, toisin kuin myöhemmin turvallistavan retoriikan nostaessa päätään. Valtiolliset toimijat ja näiden kyvykkyys sekä kriittiseen infrastruktuuriin kohdistuvien tietoteknisten uhkien vaikutukset kuitenkin tunnistetaan sekä tunnustetaan, mutta niiden potentiaalista uhkaa ei pidetä merkittävänä. Asiakirjassa on lisäksi tunnistettu haasteita, jotka ulottuvat myös nyky-Suomen kybertoimintaympäristön turvaamiseen, kuten teknologian nopea kehitys, digitalisaation myötä kasvava hyökkäyspinta-ala sekä kansalaisten kyvykkyys suojautua kyberuhkilta, mitkä ovat aitoja ja realisoituvia uhkia.[62]

Strategiassa asetetaan tavoitetila tieto- ja viestintäjärjestelmien varassa oleville kriittisille toiminnoille. Mielenkiintoisesti tavoitetilan muotoilussa todetaan, että suomalaisen yhteiskunnan kriittisistä toiminnoista osa on riippuvaisia tieto- ja viestintäjärjestelmien toiminnasta.[63] Tämä eroaa merkittävällä tavalla nykypäivän retoriikasta, jossa puhutaan laajemmin koko digitaalisen yhteiskunnan toimintojen suojaamisesta[64]. Strategiaa tarkastellessa on vaarana syyllistyä liialliseen anakronismiin – niin yhteiskunnan rakenteeseen liittyvät, teknologiset kuin turvallisuuspoliittiset realiteetit ovat olleet strategian laatimisen aikaan hyvin erilaiset. Tavoitetilana asiakirjassa on varmistaa, että valtionhallinto,

---

[60] Yhteiskunnan turvallisuusstrategia 2010, 89.
[61] Kyberturvallisuuden sanasto 2018, 21.
[62] Yhteiskunnan turvallisuusstrategia 2010, 66–67.
[63] Ibid., 35–36.
[64] Suomen kyberturvallisuusstrategia 2024, 10.

elinkeinoelämä, koko julkinen sektori ja kansalaiset voivat luottaa tieto- ja viestintäverkkojen toimivuuteen. Toisaalta osa tavoitetilaan tähtäävistä toimenpiteistä jää jopa strategian tasolla väljiksi: kirjaukset ” viestintäverkkojen tietoturvallisuudesta huolehditaan” ja ”järjestelmien rakentamista ja niiden ylläpitoa sekä palveluiden toimivuutta koskevien määräysten noudattamista valvotaan” jättävät vastuun näiden linjauksien toteutumisesta toimeenpanevien hallinnonaloille.[65] Painopiste on dokumentissa jätetty teknisten järjestelmien ja prosessien varmistamiseen ja turvaamiseen, mutta huomionarvoista on henkilöstön, kansalaisten ja muiden toimijoiden osaamisen sekä ymmärryksen kasvattamisen huomioimatta jättäminen.

Suhteessa nykypäivään erilainen aiheen painoarvo korostuu strategiassa myöhemmin luvussa ”Elintärkeät toiminnot ja niiden turvaaminen”, jossa kyberturvallisuus on sijoitettu alaluvun ”Talouden ja infrastruktuurin toimivuus” alle esimerkiksi ”Sisäisen turvallisuuden” tai ”Suomen puolustuskyvyn” sijaan. Tämä voi hyvin olla myös muotoilutekninen valinta, mutta se toisaalta antaa aiheesta ymmärrettävän sellaisen kuvan, että aihe jää vain infrastruktuurin ylläpitämiseen liittyväksi tekniseksi osa-alueeksi. Tämä myös korostuu tarkastelemalla asiakirjaa laajemmin: sana ”kyber” mainitaan leipätekstissä ainoastaan kahteen otteeseen.[66] Verrattuna esimerkiksi *Yhteiskunnan turvallisuusstrategiaan 2025*, jossa se mainitaan kokonaisuudessa 53 kertaa, ero on huomattava. Tähän vaikuttaa myös kyber-alkuisten sanojen vakiintumattomuus vuonna 2010, mutta samaa aihetta eksplisiittisesti sekä implisiittisesti käsittelevät aiheet esiintyvät jokaisessa osa-alueessa myöhemmissä turvallisuusstrategioissa.[67]

Talouden ja infrastruktuurin linjauksia toimeenpanevien strategisten tehtävien alle on määrätty kunkin hallinnonalan vastuut. Liikenne- ja viestintäministeriö vastaa sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistamisesta ja valtiovarainministeriö valtionhallinnon IT-toimintojen ja tietoturvallisuuden sekä valtionhallinnolle yhteisten palvelujärjestelmien turvaamisesta. Molemmissa vastuunjaoissa on eritelty toimenpiteitä, joilla strategiassa asetetut päämäärät saavutetaan.[68]

---

[65] Yhteiskunnan turvallisuusstrategia 2010, 35.
[66] Ibid., 2, passim.
[67] Yhteiskunnan turvallisuusstrategia 2025, passim
[68] Yhteiskunnan turvallisuusstrategia 2010, 41–42.

Painopiste on sähköisten tieto- ja viestintäjärjestelmien kohdalla elintärkeiden toimintojen lamaantumisen estämisessä, yhteiskunnan sähköisen viestinnän ja palveluiden turvallisuuden varmistamisessa sekä maan ulkopuolelta kohdistuvien uhkien torjumisessa. Toimenpiteet on strategisessa dokumentissa jätetty ylätason tavoitteiksi todennäköisesti, jotta hallinnonalat voivat itse määritellä tarkemmat toimenpiteet niiden saavuttamiseksi. Lisäksi mainitaan, että viestintäviraston toimintaa tullaan kehittämään tieto- ja viestintäjärjestelmien turvallisuutta ja toiminnan jatkuvuutta varmistavana turvallisuusviranomaisena, joka ennakoi Suomen kybertoimintaympäristön vastuun siirtämistä nykyisen liikenne- ja viestintäviraston, eli Traficomin, ja myöhemmin 2014 perustetun kyberturvallisuuskeskuksen alle.[69]

Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen valiokunta (utva) päättivät 8.3.2011 käynnistää kansallisen kyberstrategian laatimisen osana Yhteiskunnan turvallisuusstrategian toimeenpanoa. Tämä oli merkittävä päätös, sillä Limnéllin mukaan itse kyberturvallisuusstrategian julkaiseminen vuonna 2013 merkitsi kyber-käsitteen läpimurtoa ja hallinnollista institutionalisoitumista.[70]

Pääministeri Jyrki Kataisen valtioneuvoston hallitusohjelma vuodelta 2011 on ensimmäinen laatuaan, jossa esiintyy termi ”kyber-”. Laajemmin ohjelma kertoo suomalaisen valtiovallan päätöksenteon heräämisestä kysymyksen pariin, mitä kuvastaa kirjaus: ”Tietoverkkojen toimintavarmuus on välttämätöntä modernin tietoyhteiskunnan toiminnalle. Hallitus laatii kansallista tietoverkkoturvallisuutta koskevan kyberstrategian ja osallistuu aktiivisesti alan kansainväliseen yhteistyöhön. Tavoitteena on, että Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä”.[71] Ohjelmassa on monta mielenkiintoista linjausta suomalaisen yhteiskunnan kyberturvallisuuden kehityksen osalta.

Ensiksi kirjauksessa puhutaan Suomesta modernina tietoyhteiskuntana, joka kuvastaa konkreettista tunnustusta suomalaisen yhteiskunnan luonteesta. Huoltovarmuuskeskuksen mukaan tietoyhteiskunta on verkottunut yhteiskunta, jossa keskinäiset riippuvuudet ovat kasvaneet, ja jossa tehokkaan ja optimoidun verkostotalouden pohjana on nopeasti kehittyvä tieto- ja viestintäteknologia. Kuvatunlainen yhteiskunta on myös erityisen häiriöherkkä

---

[69] Yhteiskunnan turvallisuusstrategia 2010, 41; Suomen kyberturvallisuusstrategia 2013, 7.
[70] ”Tietoverkkoturvallisuuden valmiudet”. Valtioneuvoston verkkosivut. < https://valtioneuvosto.fi/-/beredskapen-i-fraga-om-datanatssakerheten>. [luettu 29.6.2025].
[71] Pääministeri Jyrki Kataisen hallituksen ohjelma 2011, 22.

uudenlaisille uhkille, kuten kyberhyökkäyksille.[72] Tämä heijastelee myös tietynlaista ymmärrystä valtiojohdon tasolla suomalaisen yhteiskunnan luonteen ja toimintaympäristön muutoksesta, vaikka toisaalta ymmärrystä aiheesta oli vuodelta 2003 ensimmäisestä poikkihallinnollisesta kansallisesta tietoturvastrategiasta *Tietoturvalliseen tietoyhteiskuntaan*[73].

Toisena, ja ehkä kyberturvallisuuden kannalta keskeisimpänä, mainintana ohjelmassa esiintyy päätös kyberstrategian laatimisesta, jonka käynnistys päätettiin tasavallan presidentin ja utvan yhteiskokouksessa. Huomionarvoista on, että kyberstrategia yhdistettiin ohjelmassa tietoverkkorikollisuuteen sekä järjestäytyneeseen rikollisuuteen, eikä esimerkiksi valtiolliseen vaikuttamiseen. Ohjelmassa on myös huomioitu uusien turvallisuushaasteiden joukossa tietoverkkoihin kohdistuvat hyökkäykset, joihin liitetään terrorismi. Tätä eroa myöhempiin vuosiin vertailtaessa huomataan selkeä trendi alueellisen turvallisuustilanteen heikkenemisestä, kun esimerkiksi ulko- ja turvallisuusselonteossa ilmaistaan suoraan 2024, että Suomeen kohdistuu vihamielistä, valtiollista hybridivaikuttamista.[74] Lisäksi tietoturvallisuuden kohdalla painotetaan strategista autonomiaa ja mainitaan kriittisten tietosisältöjen tietoturvallisuuden ratkaistavan kotimaisin keinoin.[75]

Kolmantena ohjelmassa asetetaan kunnianhimoinen tavoite: ”-- Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä.” Vaikka Suomessa on ollut pitkään alan osaamista, ei Suomi vuonna 2011 ollut kyberturvallisuuden johtavia maita sen kehittämisessä. Yhdysvallat julkaisi 2003 maailman ensimmäisen kansallisen kyberturvallisuusstrategian syyskuun 11. päivän iskujen jälkimainingeissa.[76] Strategia ei myöskään ollut ensimmäinen laatuaan Euroopassakaan, sillä Viro julkaisi vuonna 2007 kansallisen tietoverkkoturvallisuusstrategian, kun se oli joutunut Venäjän laajamittaisen palvelunestohyökkäyksen kohteeksi.[77] Myös länsinaapurissa oltiin samoihin aikoihin siirrytty päivittämään tiedustelulainsäädäntöä sellaiseen malliin, että se sallisi puolustusvoimien signaalitiedustelun seurata radiotaajuuksien lisäksi verkossa kulkevaa ulkomaantiedustelua.

[72] “Tietoyhteiskunta”. Huoltovarmuuskeskuksen verkkosivut. <https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta>. [luettu 28.6.2025].
[73] Limnéll 2014, 9.
[74] Suomen ulko- ja turvallisuuspoliittinen selonteko 2024, 10.
[75] Pääministeri Jyrki Kataisen hallituksen ohjelma 2011, 22, 28,
[76] The National Strategy to Secure Cyberspace 2003, passim.
[77] ”Verkkokelmit eivät keinoja kaihda – Suomen tie kohti parempaa tietoverkkoturvallisuutta”. Agendan verkkosivut. < https://agenda.fi/fi/julkaisu/verkkokelmit-eivat-keinoja-kaihda-suomen-tie-kohti-parempaa-tietoverkkoturvallisuutta/#virolainen-huippuosaaminen>. [luettu 29.6.2025].

FRA-nimisen lain (Försvarets Radioanstalt)[78] hyväksyminen 19.6.2008 ja siihen liittyvät päivitykset aiheuttivat tyrmistystä Suomessa, sillä tämä tarkoitti sitä, että Ruotsin kautta kulkevat Suomen ulkkomaanyhteydet olivat nyt ruotsalaisten kuunneltavissa.[79]

Suomi oli vuonna 2013 yksi Euroopan viimeisimpiä valtioita, joissa ei ollut sotilas- tai siviilitiedustelulainsäädäntöä, ja Ruotsin FRA-laki aiheutti voimakasta kritiikkiä, etenkin vasemmistopuolueissa, joiden kansanedustajat ilkkuivat ruotsalaisille näiden ”salakuuntelulaista”.[80] Tämä asetelma kuitenkin kääntyi päälaelleen, kun ruotsalaiset vinkkasivat suomalaisille virkaveljilleen, että venäläiset olivat kuunnelleet

2.2 Kyberturvallisuus vakiintuu ulko- ja turvallisuuspolitiikkaan

Turvallisuus- ja puolustuspoliittiset selonteot ovat Limnéllin mukaan vakiintunut käytäntö, jossa valtioneuvosto koostaa turvallisuus- ja puolustuspoliittiset linjauksensa kerran vaalikaudessa eduskunnalle (ja suomalaiselle yhteiskunnalle) arvioitaviksi.[81] Limnéllin mukaan ja vuoden 2012 selontekoa tarkastellessa huomataan kyber-käsitteen esiintyvän siinä ”voimallisesti”. Sisällysluetteloa tarkastellessa selviää, että ”Kokonaisturvallisuuden toimeenpanon kehittämisen linjaukset” -nimisen luvun alla ”Kansallinen kyberturvallisuus” esiintyy omana alalukunaan. Huomattavana erona esimerkiksi kahden vuoden takaiseen Yhteiskunnan turvallisuusstrategiaan, selonteossa kyberturvallisuuteen liittyvät aihekokonaisuudet esiintyvät laajemmin ja kokonaisvaltaisemmin eri osa-alueiden yhteydessä, kuten muuttuneen toimintaympäristön, sodankäynnin, Naton sekä kokonaisturvallisuuden.[82]

Limnéll avaa, että selonteossa käytetystä käsitteistöstä on havaittavissa kyber-etuliitteisten sanojen vakiintuminen valtiohallintoon: ”Selonteossa esiintyvät käsitteet kybertoimintaympäristö, kyberhyökkäys, kybertila, kyberuhka, kyberturvallisuus kyberhyökkääjä” ja monet muut. Hän huomauttaa myös, että selonteossa kyberuhkat ja -hyökkäykset yhdistetään laaja-alaisiin turvallisuuskysymyksiin. Lisäksi teknologian kehittymisen ennustetaan johtavan myös muiden kuin valtiollisten valtiollisten toimijoiden

[78] Lain kritisoijat kutsuivat lakia pilkkaavasti nimillä ”Lag 1984” ja ”Lex Orwell”.
[79] Järvinen 2018, 155–158.
[80] Ibid. 2018, 157.
[81] Limnéll 2014, 10.
[82] Limnéll 2014, 14; Suomen turvallisuus- ja puolustuspolitiikka 2012, 3.

vahingollisten vaikuttamisyritysten määrän lisääntyvän.[83] Tämä on merkittävä kirjaus ja tulkinnallinen sunnanmuutos, sillä Kataisen hallitusohjelmassa ja Yhteiskunnan turvallisuusstrategiassa kybertoimintaympäristön häiriöt yhdistettiin tietoverkkorikollisuuteen ja terrorismiin.

Selonteko on retoriikaltaan vuoden 2010 Yhteiskunnan turvallisuusstrategiaan verrattuna erilainen. Tiivistelmässä mainitaan, että Suomen toimintaympäristö on muuttunut muun muassa teknologisen kehityksen ansiosta, vaikka sillä viitataan enemmän globaaliin tilanteeseen. Venäjä luonnollisesti mainitaan yhtenä merkittävimmistä tekijöistä, mutta lähtökohtana on aktiivinen poliittinen dialogi, viranomaisyhteistyö ja Venäjän integroituminen yleiseurooppalaiseen kehitykseen, kansainväliseen yhteistyöhön ja maailmantalouden rakenteisin. Suomen suhtautuminen Venäjään on toiveikas ja valtioiden välisiä suhteita lähentävä.[84] Entisen Suomen Venäjä-Suurlähettilään teoksessa *Sotaa ja rauhaa. Venäjä, Yhdysvallat ja Suomi uuden suurvaltakilpailun aikakaudella* Hautala kuvaa lännen suhtautumista Venäjään kylmän sodan jälkeen jopa turhan toiveikkaana optimismina. Hänen mukaansa Venäjän haluttiin nähdä siirtyvän kohti demokratiaa, oikeusvaltiota ja läntisen mallin markkinataloutta. Positiivisen kehityskulun kannalta myönteiset viestit, kuten 2010 allekirjoitettu ydinaseiden rajoitussopimus New START, nähtiin liian optimistisesti, kun Georgian sodan kaltaisiin varoitussignaaleihin ei suhtauduttu tarpeeksi vakavasti.[85] Tässä kontekstissa selonteon linjausta on mahdollista ymmärtää osana Suomen ja lännen toiveikkuutta Venäjän suuntaan.

Selonteon tiivistelmässä mainitaan myös keskinäisriippuvuuden lisääntymisen ja toimintaympäristön teknistymisen tuoneen esiin yhteiskuntien uudenlaisia haavoittuvaisuuksia. Siinä myös ymmärretään kyberturvallisuuden merkitys yhteiskunnan kriittisen infrastruktuurin toimivuudelle. Samassa yhteydessä yhteiskunnan elintärkeiden toimintojen turvaamisen jatkuvuuden takaamiseksi todetaan kokonaisvaltaisen turvallisuusajattelun ja yhteistoiminnan olevan avainasemassa. Kappaleessa täydennetään, että lähivuosien painopisteen olevan tietoyhteiskunnalle välttämättömän kybertoimintaympäristön turvaamisessa.[86]

---

[83] Limnéll 2014, 14; Suomen turvallisuus- ja puolustuspolitiikka 2012, 8.
[84] Suomen turvallisuus- ja puolustuspolitiikka 2012, 8–9.
[85] Hautala 2024, 54–58.
[86] Suomen turvallisuus- ja puolustuspolitiikka 2012, 11–12.

Seuraavan kerran kyberturvallisuudesta puhutaan selonteon ensimmäisessä luvun alaluvussa ”keskinäisriippuvuus ja turvallisuuden jakamattomuus” Laaja-alaisten turvallisuuskysymysten merkityksen yhteydessä. Maailmanlaajuisen keskinäisriippuvuuden kasvun myötä valtioiden ulkoisen ja sisäisen turvallisuuden mainitaan nivoutuvat yhä tiiviimmin yhteen. Kyberhyökkäysten mainitaan voivan aiheuttaa nopeasti eteneviä, vakavia kriisejä, joiden ehkäisy ja estäminen edellyttävät laaja-alaista varautumista. ”Kybertilan” tai kybertoimintaympäristön häiriöiden mainitaan olevan kriittinen uhkatekijä.[87] Muutos tavasta puhua kyberturvallisuudesta korostaa valtionhallinnon heräämistä aiheen painoarvoon kansallisessa sekä kansainvälisessä viitekehyksessä. Valitut kuvaavat adjektiivit, kuten ”kriittinen” ja ”vakava” ovat silmäänpistävä ero aikaisemmin tarkastelluista dokumenteista.

Tässä vaiheessa myös tunnistetaan, että laajoissa tietoverkoissa uhkaavien toimijoiden erottaminen valtiollisten ja ei-valtiollisten toimijoiden välillä alkaa olla vaikeaa, mikä saattaa viitata siihen, että valtiolliset toimijat saattavat käyttää omien operaatioidensa toteuttajina verkkorikollisia tai muita ulkopuolisia toimijoita, joita on hankala yhdistää valtiollisiin toimijoihin.[88] Esimerkiksi Pohjois-Korean, Venäjän ja Kiinan tiedetään käyttävän erilaisten hakkeriryhmien palveluksia. Omat haasteensa aiheuttaa myös potentiaaliset lavastettu hyökkäykset, (eng. *false flag*) joissa tarkoituksella naamioidaan hyökkäys- tai vakoiluoperaatiot toisen valtion tai tahon tekemiksi.[89]

Toisin kuin Yhteiskunnan turvallisuusstrategiassa 2010, selonteossa todetaan, että ”Kybertoimintaympäristössä on siirrytty uuteen aikakauteen, jossa haittaohjelmien avulla teollisuusautomaation ja ohjelmoitavan logiikan kautta kyetään vaikuttamaan kaikkiin yhteiskunnan elintärkeisiin toimintoihin.” Samalla mainitaan, että myös Suomi on joutunut kyberoperaatioiden kohteeksi niin sisäisesti kuin ulkoisestikin.[90] Nämä ovat varsin merkittäviä ilmaisuja ja *turvallistamistekoja*, joilla kybertoimintaympäristön haasteita nostetaan turvallisuuskysymyksiksi. Valtionhallinto näiden lausujana omaa myös vaikutusvaltaa, mikä puhuu turvallistamisen onnistumisen puolesta. Julkaisijana on valtioneuvoston kanslia, joka on ministeriö, ja sen päätehtävänä on auttaa pääministeriä

---

[87] Suomen turvallisuus- ja puolustuspolitiikka 2012, 21–22.
[88] Ibid., 22.
[89] Järvinen 2018, 18.
[90] Suomen turvallisuus- ja puolustuspolitiikka 2012, 22.

valtioneuvoston johtamisessa sekä sovittamaan hallituksen ja eduskunnan väliset työtehtävät.[91] Toki selonteko on luonteeltaan virallisesti tiedoksianto eduskunnalle sekä sen myötä laajemmin koko suomalaiselle yhteiskunnalle, minkä takia on argumentoitavissa, että valtioneuvoston silmissä aihe nähdään jo turvallisuuskysymyksenä.

Alaluvussa ”Sotilaalliset voimavarat ja asevalvonta” puhutaan sodankäynnin muuttumisesta. Sodankäynnin luonteen muutoksen lisäksi keskeisiä painopisteitä ovat laajentuneet sodankäynnin muodot, jotka ulottuvat sotilaallisten lisäksi erilaisiin epäsymmetrisiin keinoihin, kuten informaatio- ja kybersodankäynnin muotoihin. Lisäksi teknologian ennustetaan luovan uusia mahdollisuuksia sodankäyntiin, ja mainitaan, että ”erityisesti tietojärjestelmien käytöllä on myös huomattavia seurannaisvaikutuksia, kuten järjestelmien haavoittuvuus sekä muodostuvat kustannukset.” Merkittävää on myös se, että vaikutusten tunnistetaan kohdistuvan asevoimien lisäksi koko yhteiskuntaan.[92] Sen lisäksi, että selonteossa ymmärretään koko yhteiskunnan olevan haavoittuvainen kybertoimintaympäristön muutoksille, kappaleessa eritellään myös sen kannalta kaksi keskeistä *viitekohdetta*: asevoimat ja yhteiskunta. Kööpenhaminan turvallistamisteorian mukaisesti on siis tunnistettavissa turvallistava teko, turvallistettava aihe ja sen viitekohde. Seuraavissa selonteon luvuissa nähdään, miten turvallistava teko etenee onnistuneeksi turvallistamiseksi ja millaisia poikkeuksellisia toimenpiteitä esitettyjen uusien haasteiden torjumiseksi esitetään.

Globaalisti merkittävien toimijoiden, kuten sotilaallisten suurvaltojen ja Naton, toimintaa sekä ajankohtaisia fokusalueita tarkastellaan selonteossa. Yhdysvaltain, Kiinan ja Naton kohdalla sotilaalliseksi painopisteeksi mainitaan muiden uusien aluevaltauksien ohella kyberturvallisuus.[93] Suomen lähialueen turvallisuuskehitystä arvioivassa luvussa sen tilannetta luonnehditaan kuitenkin hyväksi. Siinä puhutaan alueellisen yhteistyön vakiintumisesta ja pitkäjänteisestä yhteistyöstä, johon kohdistuvia uhkia myös arvioidaan. Näiksi listataan rajat ylittävän järjestäytyneet rikollisuuden ja laittoman maahanmuuton ohella kyberuhkat.[94] Näin ollen lähtökohtaisesti Suomeen kohdistuvien uhkien ei kuitenkaan arvioida tulevan Itämeren ympäristöstä. Norjan entinen ulkoministeri Thorvald Stoltenberg

[91] “Valtioneuvoston kanslia”. Valtioneuvoston verkkosivut. <https://valtioneuvosto.fi/valtioneuvoston-kanslia>. [luettu 1.7.2025].
[92] Turvallisuus- ja puolustuspolitiikka 2012, 36–37.
[93] Ibid., 38–39, 58.
[94] Ibid., 62.

julkaisi raportin vuonna 2009, jossa esiteltiin toimia, joilla pohjoismaiden ulko- ja turvallisuuspoliittista yhteistyötä voitaisiin kehittää. Raportin seitsemäs nosto oli pohjoismaisen osaamisverkoston perustaminen Pohjoismaihin kohdistuvien kyberhyökkäysten torjumiseksi.[95] Kyberturvallisuuden turvallistamista eivät siis aja vain kotimaiset voimat, sillä etenkin lähialueensa naapureihin läheisesti verkottunut, mutta kansainväliseenkin toimintaympäristöön kuuluva Suomi ja suomalainen yhteiskunta ovat riippuvaisia niissä tapahtuvissa muutoksissa.

Selonteossa tarkastellaan kyberturvallisuutta omana asiakokonaisuutenaan kokonaisturvallisuuden toimeenpanon kehittämisen linjauksia käsittelevässä alaluvussa. Siinä kyberuhkien sanotaan muodostavan laaja-alaisen ja merkittävän haasteen kokonaisturvallisuudelle kybertoimintaympäristöön kohdistuvien uhkien muuttuessa vaikutuksiltaan vaarallisemmiksi koko yhteiskunnan kannalta.[96] Aikaisemmin tarkasteltuihin dokumentteihin verrattaessa, retoriset muutokset ovat hyvin selkeitä. Ilmaisut ”laaja-alainen” ja ”merkittävä haaste” sekä ”vaikutuksiltaan vaaralliset” reflektoivat todellisia kyberturvallisuuden uhkakuvia, mutta ovat myös voimallisia julkilausumia, joilla kybertoimintaympäristön uhkakuvia rakennetaan sosiaalisesti.

Samassa alaluvussa esitetään myös useita toimenpiteitä, joilla tavoiteltu kyberturvallisuuden tila saavutetaan. Kybertoimintaympäristö on sikäli mielenkiintoinen luonteeltaan, että 2012 ja pitkään sen jälkeenkin valtiot ovat joutuneet reagoimaan kyberuhkiin pitkälti *ad hoc* -perusteella, sillä harvoilla valtioilla oli olemassa valmiita linjauksia menettelyistä. Jarno Limnéll on listannut artikkelissaan ”Developing Political Response Framework to Cyber Hostilities” viisi muuttujaa, joita päättäjät voivat ymmärtää näiden reagoidessa kyberhyökkäyksiin. Hänen mukaansa painopiste valtionhallinnossa keskittyy liiaksi työkaluihin ja tekniikkaan strategioiden ja linjausten kustannuksella.[97] Tämä on myös haaste, joka myöhemmissä luvuissa toistuu vakiintuen suomalaisen kybertoimintaympäristön krooniseksi haasteeksi.

Selonteossa ymmärretään kybertoimintaympäristön kansainvälinen luonne, ja tiedostetaan, että Suomen kyky vastata erilaisiin kyberuhkiin on ”- - vahvasti sidoksissa kansainväliseen

---

[95] Turvallisuus- ja puolustuspolitiikka 2012., 66.
[96] Ibid., 94.
[97] Limnéll 2018, 32.

yhteistyöhön.”[98] Tämä oli myös vuonna 2015 YK:n hallinnollisten asiantuntijoiden lopputulema luonteeltaan rajat ylittävien ja globaalien kyberuhkien torjumiseksi – valtioiden tulisi yhteistyössä estää kybertoimintaympäristölle vahingollista toimintaa.[99]

Toisena kansallisen kyberturvallisuuden varmistamisen toimenpiteiksi vaaditaan kaikkien hallinnonalojen verkostoyhteistyö, valtioneuvoston tilannekuvatoiminta sekä kyberkoordinaatiokeskuksen perustaminen. Lisäksi mainitaan seuraavana vuonna 2013 valmistuva kansallinen kyberturvallisuusstrategia sekä sen toimeenpano-ohjelma. Näiden avulla muodostetaan kansallisen kyberturvallisuusstrategian linjaukset sekä toimeenpannaan sen vaatimat toimenpiteet.[100] Tämä on linjassa vuosia myöhemmin Limnéllin kirjoittaman suosituksen kanssa kansallisen ”kyberpolitiikan” linjausten laatimisesta. Turvallistamisteorian näkökulmasta Suomen valtiohallinnon vaatimat poikkeustoimet kyberturvallisuuteen puuttumiseen eivät kuitenkaan selonteon perusteella ole erityisen äärimmäisiä. Seuraavassa alaluvussa tarkastellaan tarkemmin itse strategiaa sekä sen toimeenpano-ohjelmaa.

2.3 Suomen ensimmäinen kyberturvallisuusstrategia luo raamit kansallisen kyberturvallisuuden tahtotilalle

Suomen ensimmäinen kansallinen kyberturvallisuusstrategia julkaistiin 24.1.2013, ja siinä määriteltiin Suomen kyberturvallisuuden visio, sen johtamisen ja koordinoinnin toimintamalli sekä strategiset linjaukset. Sen pisti alulle tasavallan presidentin ja ulko- ja turvallisuuspoliittisen valiokunnan välinen kokous, josta käytetään nimeä TP-UTVA.[101] Lisäksi osana strategiaa julkaistiin myös sen taustamuistio, jossa määriteltiin tarvittavat toimet sen toteuttamiseksi. Käytännön tasolla strategiaa toimeenpantiin sen toimeenpano-ohjelmalla, joka julkaistiin vuosi strategian ilmestymisen jälkeen.[102]

Kyberturvallisuusstrategian laatiminen itsessään kielii onnistuneen turvallistamisen käynnistymisestä. Strategia itsessään ei ole turvallistajan tavoitteiden päätepiste, mutta se

---

[98] Turvallisuus- ja puolustuspolitiikka 2012, 94.
[99] Limnéll 2018, 38.
[100] Turvallisuus- ja puolustuspolitiikka 2012, 94–95.
[101] TPAK, pyyntö 14.4.2011.
[102] Suomen kyberturvallisuusstrategia 2013, passim; Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, passim.

kertoo siitä, että kyberturvallisuus on saanut riittävästi hyväksyntää *yleisöltä* tullakseen institutionalisoiduksi. Wæverin mukaan *eksistentiaalinen uhk*a voi olla uniikki ja kertaluontoinen tai toistuva ja pysyväluontoinen. Toistuvan uhkan ratkaisemiseksi tyypillisesti kehitetään prosesseja, jotka institutionalisoituvat.[103] Vaikka vahingonteon keinot ovat muuttuneet, kybertoimintaympäristöön kohdistuvien uhkien vaikutukset yhteiskuntaan eivät ole uusia, kun puhutaan kansallisesta turvallisuudesta. Esimerkiksi modernille yhteiskunnalle korvaamattomien sähköverkkojen toimivuuden kannalta ei ole merkitystä sammutetaanko ne kyberhyökkäyksellä vai perinteisellä kineettisellä hyökkäyksellä. Kybertoimintaympäristön toimintavarmuuden turvallistamiseen haetaan myös näin ollen legitimiteettiä jo turvallisuuden piiriin kuuluvista aiheista.

Strategian johdannossa todetaan teknologisen kehityksen myötä suomalaisen yhteiskunnan muuttuneen riippuvaisemmaksi sitä ylläpitävien tietoteknisten järjestelmien toimivuudesta, mikä puolestaan asettaa uudenlaisia vaatimuksia jokapäiväisen arjen turvaamiseksi. Kyberuhkien muuttumista aiempaa vaarallisemmaksi korostetaan, ja niiden roolia myös sotilaallisen, poliittisen ja taloudellisen voimankäytön keinoina painotetaan. Toisaalta kyberturvallisuus nähdään Suomessa myös voimavarana ja mahdollisuutena: luotettavan kybertoimintaympäristön uskotaan tekevän Suomesta houkuttelevan investointikohteen, sekä kansallisen kyberturvallisuuden ja alan yritysten menestyksen nähdään olevan yhteydessä keskenään.[104]

Strategiassa Suomi visioidaan tulevaisuuden kyberturvallisuuden kärkimaaksi. Siinä tunnistetaan, että vahvan osaamisperustan, pitkään vallinneen julkisen ja yksityisen sektorin välisen luottamuksen ja hallinnonalojen välisen yhteistyön ansiosta seuraavat kunnianhimoiset tavoitteet voitaisiin saavuttaa. Suomen kyberturvallisuuden visiona on, että: 1. ”Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.” 2. ”Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.” 3. ”Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.”[105]

---

[103] Buzan, et al. 1998, 27–28.
[104] Suomen kyberturvallisuusstrategia 2013, 2.
[105] Ibid., 3.

Strategiassa ei tarkalleen avata, mitä kybertoimintaympäristön muuttuminen vaarallisemmaksi tarkoittaa. Kyseessä on valtiohallinnon asiakirja, joka on ensisijaisesti kohdistettu valtioneuvostolle, jolloin todennäköisesti oletetaan, että kansliapäälliköille, alivaltiosihteereille ja muulle virkakunnalle, jotka strategiaa toimeenpanevat, ei tarvitse eritellä erikseen, mitä yhteiskunnan elintärkeiden toimintojen häiriötilat tarkoittavat.[106] Kyberturvallisuutta popularisoivat teokset kuvaavat näitä uhkia konkreettisemmin sekä dramaattisemmin. Järvinen esittää hypoteettisen uhkakuvan, jossa Suomi halvaantuu 48:ssa tunnissa ilman sähköä täysin liikenteen, terveydenhuollon ja laajemmin koko yhteiskunnan murentuessa.[107] Vaikka tällainen uhkakuva Suomessa ja pohjoismaissa on epätodennäköinen, huhtikuussa 2025 Iberian niemimaalla sattunut sähkökatko olisi Pohjolassa kohtalokas keskellä kylmää talvea.[108] Toisaalta linjauksia ja toimenpiteitä ei perustella pelkästään uhkaperustaisesti, sillä strategiassa nähdään myös kybertoimintaympäristön onnistuneen turvallistamisen seurauksena taloudellisia ja poliittisia hyötyjä koko yhteiskunnalle.

Strategiassa kybertoimintaympäristössä tapahtuvia muutoksia kuvataan nopeina ja vaikutuksiltaan vaikeasti ennakoitaviksi. Tähän kohdistuviin uhkiin varautuminen ja torjuminen edellyttää strategian mukaan yhteiskunnan kaikilta toimijoilta nopeampaa, läpinäkyvämpää ja paremmin koordinoitua toimintaa. Kyberturvallisuuden johtamisen ylimmäksi tahoksi osoitetaan valtioneuvosto, jonka tehtävinä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä resursseista ja toimintaedellytyksistä päättäminen. Näin ollen kukin ministeriö ja niiden hallinnonala vastaa kyberturvallisuudesta. Kansallinen kyberuhkien sietokyky, eli kyberresilienssi, määritellään kykynä ennakoida ja varautua uhkiin sekä säilyttää toimintakyky häiriötilanteissa ja palautua näistä normaalitilaan.[109]

Suomen kyberturvallisuuden toimintamallin esitettiin rakentuvan kahdeksan periaatteen varaan. Niiden pohjalta vastuu kyberturvallisuuden toimeenpanosta asetettiin tapahtuvan hallinnonalakohtaisesti kunkin ministeriön johdolla. Tämä linjaus myöhemmin kostautui, sillä se toisaalta vaikeutti poikkihallinnollisten tavoitteiden saavuttamista.[110] Se myös liitettiin

---

[106] Suomen kyberturvallisuusstrategia 2013, 1.
[107] Järvinen 2018, 87–95.
[108] ” Raportti: Iberian niemimaan valtavan sähkökatkon taustalla oli monta tekijää”. *Yle Uutiset*. 20.3.2026. < https://yle.fi/a/74-20216413>. [luettu: 12.5.2026].
[109] Suomen kyberturvallisuusstrategia 2013, 3.
[110] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 23–24.

kiinteästi osaksi *Yhteiskunnan turvallisuusstrategiaan*, ja siten osaksi kokonaisturvallisuutta. Siinä myös painotettiin ketterää yhteistoimintaa ja vastuunjakoa, mikä toteutui osittain. Tehokas tiedonvaihto ja yhteisen tilannekuvan muodostaminen ovat haasteita, jotka vielä vuosikymmen myöhemmin vaativat edistämistoimia.[111] Lainsäädännön kehittäminen oli myös yksi periaatteista, joka katsottiin tärkeäksi. Lisäksi kansainvälinen yhteistyö- ja kehitystoiminta ja kansallinen osaamisen kehittäminen ja TKI-toiminta koettiin avaimiksi kyberturvallisuusalan osaamisen kotiuttamiseksi kansainvälisen kilpailukyvyn muodossa.[112]

Suomi haki voimakkaasti uusia avaimia kasvuun finanssikriisin, ja sitä seurannen eurokriisin, myötä. Tämä näkyi voimakkaasti Kataisen, Stubbin, Sipilän ja oikeastaan lähes jokaisen 2000-luvulla toimineen hallituksen ohjelmasta.[113] Huolenaihe on näin vielä vuonna 2026 ajankohtainen. Suomen talous ei ole kasvanut lähes kahteenkymmeneen vuoteen.[114] Tämä asetelma toistui myös vuosien 2019 ja 2024 strategioissa. Taloudellisen potentiaalin peräänkuuluttaminen on sikäli mielenkiintoinen, sillä se on ainoa toistuvasti esiintyvä ei eksplisiittisesti turvallisuuteen liittyvä teema. On kuitenkin argumentoitavissa, että tämä pikemminkin kuvaa valtionjohdon toiveikkuutta mahdollisista ”pikavoitoista”, sillä merkittäviä investointeja esimerkiksi kyberturvallisuusekosysteemien rakentamiseen ei lopulta tehty.

Luvussa neljä esitettiin strategian ydin, eli kymmenen linjausta, joita oli 10 kappaletta. Näiden linjausten tehtävä oli määrittää Suomen kyberpolitiikan painopisteet seuraavaan kansalliseen kyberturvallisuusstrategiaan saakka vuonna 2019. Linjaukset määrättiin toteutettavaksi strategian toimeenpano-ohjelmassa.

Paperilla strategiset linjaukset ovat todella ansiokkaat:

1. Viranomaisten ja julkisen sektorin tehokas yhteistoimintamalli
2. Elinkeinoelämän aktivoiminen ja osaamisen kehittäminen
3. Elintärkeiden toimintojen turvaaminen kyberuhkilta
4. Poliisin riittävien toimintaedellytysten varmistaminen

[111] Suomen kyberturvallisuusstrategia 2024, 33.
[112] Kyberturvallisuusstrategia 2013, 5.
[113] Pääministeri Jyrki Kataisen hallituksen ohjelma 2011, passim; Pääministeri Alexander Stubbin hallituksen ohjelma 2014, passim; Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen strateginen ohjelma 2015.
[114] Pohjola 2025, 6.

5. Puolustusvoimien vastuuttaminen kyberpuolustuksesta
6. Kansainvälisen toiminnan vahvistaminen
7. Yhteiskunnallisen kyberosaamisen vahvistaminen
8. Lainsäädännön ajantasaistaminen
9. Yhteiskunnallisten vastuiden selkeä määritteleminen
10. Strategian toimeenpanon valvonta

Painopiste toki oli olemassa olevien prosessien kehittämisessä, kuten suomalaisen yhteiskunnan julkisen ja yksityisen sekä kolmannen sektorin voimavarojen sekä toimijoiden yhteensovittamisessa sekä ymmärryksen ja osaamisen kasvattamisessa.[115] Toisaalta viranomaisille pyritään allokoimaan resursseja kybertoimintaympäristön turvaamista varten: kyberturvallisuuskeskuksen perustaminen sekä poliisin resurssien ja kyvykkyyden kasvattaminen on kirjattu linjauksiin neljä ja viisi. Kyse oli nimenomaan resurssien uudelleenallokoinnista, ei uusien määrärahojen lisäämisestä, mikä aiheutti merkittäviä ongelmia tavoitteiden saavuttamiseen.[116]

Linjauksiin neljä ja viisi oli kirjattu, että poliisin riittävistä toimivaltuuksista kybertoimintaympäristössä huolehditaan ja puolustusvoimille laaditaan puolustusministeriön johdolla toimivaltuussäännöstö, joka mahdollistaa kokonaisvaltaisen kyberpuolustuskyvyn luomisen.[117] Lisäksi linjauksessa kahdeksan esitettiin, että kybertoimintaympäristöön ja -turvallisuuteen vaikuttavaa lainsäädäntöä kartoitetaan uudelleen tarkoituksen löytää kehittämistarpeita hallinnonalojen ja elinkeinoelämän yhteistyönä. Tämän tarkoituksena oli luoda juridiset edellytykset kyberuhkia torjuville toimenpiteille. Konkreettisena esimerkkinä mainitaan tiedon luovuttamiseen, vaihtamiseen ja keräämiseen liittyvät lainsäädännölliset esteet. Lisäksi kansainvälisen yhteistyön lisääminen ja tiivistäminen kyberturvallisuuden parantamiseksi mainittiin useaan otteeseen, mikä on myös alan asiantuntijoiden mukaan tärkeää. Kansainväliselle yhteistyölle on osoitettu myös oma alalukunsa strategian taustamuistiossa.[118]

---

[115] Suomen kyberturvallisuusstrategia 2013, 7.
[116] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2017, 26.
[117] Suomen kyberturvallisuusstrategia 2013, 8–9.
[118] Ibid., 8–10, 16; Limnéll 2014, 84

Kyberturvallisuusstrategian taustamuistiossa tunnistetaan kyberoperaatioita pidettävän sen laatimisen aikaan toistaiseksi ”pehmeiksi toimiksi”. Tämän takia niiden käyttökynnystä pidetään myös matalampana.[119] Saman huomion ovat tehneet useat tutkijat, sillä vielä 2015 kansainvälisessä lainsäädännössä kyberoperaatioita pidettiin niin sanottuna harmaana alueena ja sellaisen ne ymmärrettiin pitkään.[120] Toisaalta kybertoimintaympäristön kehityksen luomat, Suomen kaltaiseen kehittyneeseen tietoyhteiskuntaa kohdistuvat, vakavat vaarat tunnustetaan, ja niiden ennustetaan lisääntyvän. Myös Stuxnet-verkkomato[121] jolla Yhdysvallat onnistui hidastamaan Iranin ydinaseohjelmaa arvioiden mukaan yhdestä kolmeen vuotta, mainittiin kyberturvallisuuden osalta uuden aikakauden lähtölaukauksena. Se osoitti, että kybertyökalujen potentiaalin myös fyysistä tuhoa aiheuttavissa iskuissa, joiden uskottiin olevan mahdollisia vain perinteisin kineettisin iskuin.[122]

Alaluku *Kybertilannetietoisuus ja Kyberturvallisuuskeskuksen* perustaminen käsitteli uuden kyberturvallisuuskeskuksen perustamista sekä sen vastuita. Se rakentui sen hetkisen CERT-FI toiminnon sekä kehitteillä olevan GOV-CERT toiminnon yhdistämisellä, minkä lisäksi sen tukena toimii verkosto, johon kuuluvat tarvittavat viranomaistahot, yritykset ja muut alan keskeiset toimijat. Keskuksen tehtäviksi lueteltiin: 1. Kyberturvallisuustilannekuvan muodostaminen ja jakaminen. 2. Kyberuhkien riskianalyysin kokoaminen ja ylläpito yhdessä eri hallinnonalojen kanssa. 3. Toimivaltaisten viranomaisten ja yksityisen sektorin toimijoiden tukeminen laajojen kyberhäiriötilanteiden hallinnassa. 4. Yhteistyön tehostaminen ja osaamisen kehittämisen tukeminen. Keskuksen tulosohjauksesta vastaisi liikenne- ja viestintäministeriö, minkä lisäksi sen tulosohjauksen varmistamiseksi määrättiin perustettavaksi kyberturvallisuustyöryhmä.[123]

Elinkeinoelämää ja poliisin roolia käsittelevät luvut jäivät vastuiden allokointia lukuun ottamatta väljiksi. Tämä antoi yksittäisille hallinnonaloille ja toimijoille paljon vapautta, mutta myös vastuuta toteuttaa strategian linjaukset riittävällä tavalla. Esimerkiksi elinkeinoelämää käsittelevässä alaluvussa todettiin kyberuhkiin varautumisen toteutuvan

[119] Suomen kyberturvallisuusstrategia 2013, 17.
[120] Limnéll 2018, 35–38; Lehto ja Neittaanmäki 2018.
[121] Stuxnet oli vuonna 2010 Yhdysvaltojen tiedustelupalvelun NSA:n kehittämä haittaohjelma, jolla soluttauduttiin Iranin ydinlaitoksiin, joissa rikastettiin uraania ydinvoimalan polttoainesauvoihin tarvittavaksi U-235-isotooppiksi. Haittaohjelmassa onnistuttiin hajottamaan rikastusprosessissa käytettävät sentifiguurit. Myöhemmin haittaohjelma levisi muiden toimijoiden käyttöön aiheuttaen tuhoa globaalisti – myös Yhdysvalloissa.
[122] Suomen kyberturvallisuusstrategia 2013, 17–18; Järvinen 2018, 38–40.
[123] Ibid., 23–24.

yksittäisissä organisaatioissa käytännössä perinteisen tietoturvallisuuden keinojen avulla. Keinot näiden valvomiseksi ja mahdollistamiseksi jäivät kuitenkin varsin laihoiksi.[124] Puolustusvoimien roolia ja kyberpuolustuskykyä käsittelevä alaluku tarjosi enemmän konkreettisia linjauksia kyberturvallisuuden kehittämiseen. Puolustusvoimille haluttiin luoda uskottava suorituskyky kyberpuolustuksen luomiseen yhteistyöllä muiden viranomaisten, yritysten ja yliopistojen kanssa sekä hankkeilla ja kansallisilla että kansainvälisillä harjoituksilla lainsäädännön muutoksien kautta.[125] Näin ollen strategiassa ei esitetty valtioneuvostolle tai sen toimialoille poikkeuksellisia toimivaltuuksia edes mahdollisissa kriisitilanteissa.

Lainsäädäntö on eduskunnan ja hallituksen yksi tärkeimmistä keinoista käyttää valtaa Suomen kaltaisessa oikeusvaltiossa.[126] Tämän myötä kyberturvallisuutta koskevaa säätelyä käsittelevän luvun sisältö tulee sen kehityksen tarkastelun kannalta olemaan avainasemassa. Strategiassa tunnistetaan kyberturvallisuuden haastava luonne oikeudellisesti uutena ilmiönä, eikä kyberuhkatilanteita kattavaa valtioita sitovaa valtiosopimusta vuonna 2013 ole. Juridisesti kyberturvailmiöiden termistöstä ei ole vielä selvyyttä, saati konsensusta.[127] Tarve kansallisen lainsäädännön päivittämiselle vastaamaan kyberturvallisuuden luomia uhkia nähdään keskeisenä. Samalla ymmärretään myös, että Suomi on sitoutunut kansainväliseen oikeuteen ja sopimuksiin, eikä sen nähdä pystyvän yksinään kansallisella lainsäädännöllä luomaan turvallista kybertoimintaympäristöä – oma lainsäädäntö tulee yhtenäistää kansainväliseen, minkä lisäksi tähän tulee myös pyrkiä vaikuttamaan. Lähtökohtana lainsäädännön uudistamisessa on viranomaisten riittävien toimintavaltuuksien varmistaminen siten, että ne sisältyvät heidän normaaleihin toimivaltuuksiinsa erottamatta sitä muista turvallisuuteen liittyvistä elementeistä. Tämän lisäksi lainsäädäntöä tulee tarkastella myös kyberturvallisuutta parantavien keinojen esteitä ja rajoituksia purkamisen näkökulmasta.[128]

Huolimatta siitä, että taustamuistiossa on strategian toimeenpanon edellyttäville toimenpiteille oma alalukunsa, konkreettisten toimenpiteiden määrä jää vähäiseksi. Konkreettisin ja strategian ylivoimaisesti tärkein linjaus ja toimenpide oli kyberturvallisuuskeskuksen

[124] Suomen Kyberturvallisuusstrategia 2013, 25–26.
[125] Ibid., 28–29.
[126] “Oikeusvaltio Suomi”. Oikeusministeriön verkkosivut. < https://oikeusministerio.fi/oikeusvaltio-suomi>. [Luettu 16.7.2025].
[127] Suomen kyberturvallisuusstrategia 2013, 33–34.
[128] Ibid., 34–35.

perustaminen. Keskuksen tehtäviä eriteltiin kattavasti, mutta sen lisäksi muissa luvuissa mainitsemattomia toimenpiteitä ei lueteltu. Poikkeuksena tähän oli kirjaus vaatimuksesta raportoida kyberhäiriötapauksessa käynnistetyt toimenpiteet sekä laatia jälkianalyysin tapahtuneesta.[129] Myöhemmin samana kesäkuuna julki tulleet Edward Snowdenin paljastukset sekä lokakuussa ulkoministeriön järjestelmistä löytynyt vakoiluohjelma yhdessä kyberturvallisuusstrategian kanssa toimivat lähtölaukauksena Suomen tiedustelulainsäädännön uudistamiselle, joka tuli päätökseensä kuitenkin vasta 2019.[130]

Kyberturvallisuusstrategian laatimista voidaan pitää merkittävänä virstanpylväänä Suomen kybertoimintaympäristön turvallistamisprosessissa. Se vakiinnutti aiheen osaksi valtionhallinnon turvallisuusajattelua ja käynnisti sen institutionalisoimisen. Strategian toimeenpanoa vaikeuttivat epäselväksi jäänyt kyberturvallisuuden kansallinen johtajuus sekä heikko poliittinen sitoutuminen, ja sen myötä puutteelliseksi jäänyt resurssointi.[131] Kyberturvallisuusstrategian laatimisen voi katsoa lähteneen liikkeelle puolustusministeriön hallinnonalalta, jossa asiaa myös valmisteltiin. Hallinnonalat saivat osallistua strategian laatimiseen varsin aktiivisesti, minkä takia on arvioitavissa, että niiden sitoutuminen ja toimijuus heijastuu strategian linjauksista – esimerkiksi puolustus- ja sisäministeriöiden hallinnonalat saivat merkittäviä vastuita ja toimivaltuuksia. Strategia oli myös voimakkaasti virkakunnan valmistelema, eikä sillä ollut voimakasta poliittista taustavoimaa, mikä heijastelee Parlamenttisampo-palvelusta haettuja puheenvuoroja vuosilta 2012–2014. Suurin osa puheenvuoroista käsitteli vasta valmistunutta strategiaa, eikä se herättänyt erityistä polemiikkia; suhtautumista aiheeseen kuvastaa parhaiten ”varsin samanmielinen hyrinä”.[132]

2.4 Kyberturvallisuusstrategian toimeenpano

Reilu vuosi Suomen ensimmäisen kyberturvallisuusstrategian ilmestymisen jälkeen, julkaistiin sen toimeenpano-ohjelma, jossa esitetään 74 toimenpidettä kyberturvallisuuden

---

[129] Suomen kyberturvallisuusstrategia 2013, 37.

[130] Järvinen 2018, 155, 162; “Tiedustelulainsäädännön hankkeet käynnistettiin”. Valtioneuvoston verkkosivut. < https://valtioneuvosto.fi/-/1410869/tiedustelulainsaadannon-hankkeet-kaynnistettiin> [luettu 17.7.2025]; ”Tietoturvailmiöt, jotka muuttivat maailmaa”. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvailmiot-jotka-muuttivat-maailmaa> [luettu 17.7.2025].

[131] Kybersuojauksen järjestäminen 2017, 5–6.

[132] ”Puheenvuorot 2000–2014”. Parlamenttisampon verkkosivut. < https://parlamenttisampo.fi/fi/speeches-2000-2014/faceted-search/by_year> [luettu.13.5.2026].

parantamiseksi. Sen on laatinut vuotta aikaisemmin perustettu Turvallisuuskomitea[133], minkä lisäksi siihen on koottu lausuntopyynnöllä esityksiä yhteensä 54 toimijalta. Ohjelman johdannossa tunnistetaan myös, että julkaistu strategia linjasi pitkälti viranomaisten toiminnasta, vaikka suuri osa digitaalisista palveluista tuotetaan yksityisellä sektorilla. Itse asiakirja on jaettu kahteen osaan: ohjelmaan sekä sen käytännön esityksiin. Lisäksi se sisältää yhteenvetotaulukon jokaisesta esityksestä. Tähän on listattu itse toimenpiteet, niiden toimeenpanosta vastaava hallinnonala, arvio lainsäädännön muutostarpeesta sekä strategian linjaus, johon toimenpide liittyy.[134]

74 esitettyä toimeenpanoa jakautuvat seitsemän yläkategorian alle. Ne ovat ”Kriittiset toiminnot ja järjestelmät”, ”Viranomaisten osaaminen ja kyvykkyyksien kehittäminen”, ”Tilannekuva”, ”Tiedonhankinta ja tutkinta kybertoimintaympäristössä”, ”Osaamisen kehittäminen”, ”Hyvinvointipalveluiden kehittäminen” ja ”Yritysten toimintaedellytykset ja jatkuvuuden hallinta”. Keskeisiksi kehittämiskohteiksi ohjelmassa on eritelty ”kyberturvallisuuskeskus, valtion ympärivuorokautinen tietoturvatoiminta, salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (SATU), poliisin toimintakyky kyberrikollisuuden torjunnassa, kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen sekä tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen”.[135]

Kriittisien toimintojen ja järjestelmien turvaamiseksi käynnistettiin hallinnon turvallisuusverkkohanke (TUVE) ja toimialariippumattomien ICT-tehtävien (TORI) kehitystoiminta. TORI- ja TUVE-hankkeisiin kuului useita muita ala-hankkeita, kuten ICT-toimintojen ja palveluiden priorisointiin perustuvan järjestelmäluokituksen ja kokonaispriorisoinnin tuottaminen hätätilanteissa, tieto- ja viestintäjärjestelmien energian saatavuuden riskikartoitus sekä tietojärjestelmien ja niiden alustojen sekä tietoliikennelaitteistojen ja -ohjelmistojen haavoittuvuuksien hallinnan kehittäminen.[136] Kuitenkin tarkemmin näitä toimenpiteitä tarkastelemalla huomataan, että harvalla niistä oli toimeenpanosuunnitelmaan julkaisuvaiheessa edes aikataulua, ja lupaavasta sisällöstä

---

[133] Turvallisuuskomitea on poikkihallinnollinen pysyvä yhteistyöelin, joka toimii puolustusministeriön yhteydessä. Ennen vuotta 2013 samankaltaisesta toiminnallisuudesta vastasi Turvallisuus- ja puolustusasiain komitea.
[134] Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 1–3, 18–22.
[135] Ibid., 1.
[136] Ibid., 25–26.

huolimatta niiden käynnistymisaikataulu on epämääräinen. Toisaalta on huomioitava, että jokaiselle toimenpiteelle oli määrätty vastuutaho, joka vastaa niiden toimeenpanosta. Kaikki edellä mainitut toimet sijoitettiin valtiovarainministeriön hallinnonalalle.

Viranomaisten osaamisen ja kyvykkyyksien kehittämiseksi toimenpiteitä oli enemmän: yhteensä 21 kappaletta. Näitä olivat muun muassa valtioneuvoston tietoturvaverkoston virallistaminen ministeriöiden tieto- ja kyberturvallisuuden viralliseksi yhteistyöryhmäksi, kansallisen kryptolaboratorion perustaminen kansallisen salaustekniikan osaamisen kehittämiseksi sekä useat erilaiset hallinnonalakohtaiset hankkeet, koulutukset näiden toimintojen kehittämiseksi ja nykytilan kartoittamiseksi kyberuhkien varalta.[137] Toimenpiteillä vastattiin suoraan aikaisemmin ohjelmassa esitettyihin tavoitteisiin: muun muassa ulkoministeriö sai tehtäväkseen tuottaa selvitys kyberympäristöä koskevasta kansainvälisoikeudellisesta sääntelystä, mikä vastasi suoraan kyberturvallisuuteen liittyviin juridisiin haasteisiin. Lisäksi erilaiset hallinnonalakohtaiset standardoimistyöt sekä kyberturvallisuuden arviointikriteeristön luominen kieli selkeästä tahtotilasta institutionalisoida ja sisäänrakennuttaa kyberturvallisuutta suomalaisen yhteiskunnan hallintoprosesseihin.

Tilannekuvan kehittämiseksi ohjelmassa ehdotettiin vain kolmea keskeistä toimenpidettä: Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeen (SECICT) käynnistämistä, kyberturvallisuuskeskuksen perustamista sekä puolustusvoimien kyberturvallisuustilannekuvan luomista. Kyberturvallisuuskeskuksen perustaminen vastuutettiin viestintävirastolle[138] ja liikenne- ja viestintäministeriölle. Jokaiseen näistä toimenpiteistä kuului tai niihin liittyi vaikutuksiltaan merkittäviä toimia. SECICT oli laaja ja poikkihallinnollinen hanke, jonka tavoitteena oli yhtenäistää kyberturvallisuuden yhteistoimintaa ja selkeyttää häiriötilanteiden hallinnan toimintamalleja. Tämän lisäksi siihen kuului kolme muuta hanketta, joissa parannettiin tietoverkkojen tilannekuvaa mahdollisten haittaohjelmien havaitsemiseksi, kehitettiin huoltovarmuuskriittisten organisaatioiden kykyä varautua tietoturvauhkiin sekä pilotoitiin kyberturvallisuuden kehittämis- ja auditointityökalua.[139]

---

[137] Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 28–34.
[138] Viestintävirasto liittyi osaksi Liikenne- ja viestintävirastoa.
[139] Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 34–36.

Tiedonhankintaa ja kyberympäristön tutkintaa koskeva osio oli myös lyhyt, mutta siihen kuului useita kolme merkittävää toimenpidettä, joista kaksi edellytti muutoksia lainsäädäntöön. Ensimmäinen näistä käsitteli kansallisen lainsäädännön kehittämistä, jotta turvallisuusviranomaiset kykenisivät vastaamaan kybertoimintaympäristön uhkiin tehokkaammin parantamalla tiedonhankintakykyä. Etenkin tämä toimenpide, joka käynnistettiin TP-UTVAssa 7.11.2013[140], tarkoitti jyrkkää muutosta suomalaisten turvallisuusviranomaisten valtuuksiin tiedonhankinnan ja tiedustelun saralla. Puolustusministeriö asetti 13.12.2014 työryhmän arvioimaan ja muokkaamaan Suomen lainsäädäntöä siten, että viranomaisilla olisi riittävät tiedonhankintaoikeudet tietoverkoissa esiintyvien uhkien torjumiseksi.[141] Toinen lainsäädäntöön vaikuttavista toimenpiteistä on kybervalvonnan ja kybertiedustelun jatkovalmistelu. Se kytkeytyy voimakkaasti edellä mainittuun lainsäädäntöhankkeeseen ja sen määritellään toteutuvan hankkeen mahdollistamissa rajoissa. Kolmantena toimenpiteenä poliisihallitus nimettiin edistämään useita toimia, jotka parantavat kyberrikosten tutkintaa muun muassa selvittämällä esitutkintaviranomaisten toimivaltuuksia sekä lisäämällä tiedonhankinnan ja tilannekuvan luomisen kyvykkyyksiä.[142]

Työryhmän asettaminen tiedonhankintalainsäädännön laatimiseksi oli äärimmäisen konkreettinen ja toisaalta painava toimenpide, joka aiheutti myös laaja-alaista poliittista keskustelua yksityisyyden suojasta ja viranomaisten tiedonsaantioikeuksista. Mikko Kurttila kirjoitta pro gradu -tutkielmansa *Mitä tiedustelusta kirjoitettiin? – Suojelupoliisi ja tiedonhankintalakityöryhmä mediassa 2013–2015* lakihankkeesta käydystä keskustelusta. Kurttilan mukaan lakihankkeen työryhmä aiheutti mediassa varsin voimakkaitakin mielipiteitä.[143] Kurttila argumentoi, että keskustelun hedelmällisyyttä vaikeutti ymmärryksen puute debatin aiheesta. Tämä johtui Kurttilan mukaan siitä, että tiedonhankintalain kaltaista tiedustelulakia ei Suomessa tähän mennessä ollut olemassa, joten keskusteluun osallistujilla näin ollen oli vajavainen ymmärrys, esimerkiksi valmiin lain implikaatioista.[144]

---

[140] TP-UTVA tarkoittaa Tasavallan Presidentin ja valtioneuvoston ulko- ja turvallisuuspoliittisen ministeriövaliokunnan yhteistä kokousta.
[141] Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 39–40.
[142] Ibid., 41.
[143] Kurttila 2015, 2.
[144] Ibid., 71–72.

Kurttila argumentoi, että juuri valtiojohto kannatti tiedustelulainsäädännön säätämistä, kun puolestaan tutkijat, jotkin elinkeinoelämän edustajat ja valtioneuvoston virkahenkilöt osallistuivat debattiin hanketta kritisoivin puheenvuoroin.[145] Tätä tuki Helsingin Sanomissa julkaistu Anna-Liisa Kauhasen artikkeli ”Tiedustelulakien laadinta haastaa Suomen, vaikka tiedustelulle on vankka poliittisen johdon tuki”, jossa punnittiin lakihankkeen taustamuuttujia sekä vaikutusta yksityisyyden suojaan ja kansalaisten oikeuksiin. Artikkelissa mainittiin, että työryhmän julkaisema mietintö ei ollut yksimielinen, vaan liikenne- ja viestintäministeriö jätti eriävän mielipiteen. Aihe aiheutti myös merkittävää yhteiskunnallista kiinnostusta, mistä kertoo lausuntokierroksella saatujen lausuntojen määrä, joka oli 74 kappaletta. Toisaalta tiedustelulainsäädännön säätämistä kannattaneisiin toimijoihin nostettiin senaikainen tasavallan presidentti Sauli Niinistö sekä istuva hallitus.[146]

Lakihanke oli sikäli myös merkittävä, että vuonna 2015 valmistuneessa tiedonhankintalakityöryhmän mietinnössä arvioitiin, että se edellyttäisi perustuslain muuttamista, sillä ”tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta ei näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, pelkästään vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua ehkä lukuun ottamatta”.[147] Sipilän hallituksen eri ministerit ottivat voimakkaasti kantaa lainsäädännön puolesta: viestintäministeri Anne Berner sanoi turvallisuusviranomaisten tarvitsevan digiajassa ajanmukaiset työkalut ja painotti tiedustelulakien olevan välttämättömyys. Tiedustelulait löytyvät myös Juha Sipilän hallitusohjelmasta. Lisäksi suojelupoliisin päällikkö Antti Pelttari ja puolustusvoimien tiedustelupäällikkö Harri Ohra-aho ottivat kantaa tiedustelulakien puolesta.[148]

Tässä vaiheessa ei siis tarvinnut enää arvailla, kuka turvallistaa suomalaista kyberturvallisuutta. Tasavallan presidentti, supon päällikön ja puolustusvoimien tiedustelupäällikön puheenvuorot lausuttiin merkittävästä vaikutus- ja arvovallan asemasta, mikä Waeverin mukaan on tärkeä tekijä arvioitaessa turvallistamisteon tai puheteon onnistumista.[149] Suomalaisen kybertoimintaympäristön turvallistaminen on tässä vaiheessa

---

[145] Kurttila 2015, 72.
[146] Helsingin Sanomat, 30.9.2015, ” Tiedustelulakien laadinta haastaa Suomen, vaikka tiedustelulle on vankka poliittisen johdon tuki”.
[147] ”Suomalaisen tiedustelulainsäädännön suuntaviivoja – Tiedonhankintalakityöryhmän mietintö”, Edlilexin verkkosivut. < https://www.edilex.fi/ministerioiden_julkaisut/14652>.
[148] Helsingin Sanomat, 2.10.2015, ” Tiedustelulait vaativat perustuslain muuttamisen”. <https://www.hs.fi/suomi/art-2000002856691.html>; Helsingin Sanomat, 8.10.2015, ” Kansallisesta turvallisuudesta ei tule tinkiä”. <https://www.hs.fi/mielipide/art-2000002858053.html>.
[149] Wæver 1998, 31.

siten konkreettinen valinta, jonka suomalainen valtiovalta haluaa tehdä. Tämä korostuu myös oikeus- ja työministeri Jari Lindströmin lausunnossa: ”Maailmantilanne on muuttunut”.[150]

2.5 Kyberturvallisuus rakentuu VAHTIn kasteen alla

Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) toimintakertomuksessa vuodelta 2015 arvioitiin Suomen kyberturvallisuuden tilaa. Vuonna 2004 perustettu VAHTI käsittelee kaikki merkittävät valtionhallinnon kyberturvallisuuden ja tietoturvallisuuden linjaukset, ja se toiminnallaan edistää valtakunnan tieto- ja kyberturvallisuuden tilaa.[151] VAHTI:n toimintakertomuksen mukaan Suomen tieto- ja kyberturvallisuuden tilanne pysyi lähes samalla tasolla edelliseen vuoteen verrattuna. Se myös mainitsi tähän syyksi vuosina 2010–2015 tehdyt aktiiviset tietoturvallisuusasetukseen liittyvät kehitystyöt, jotka olivat tasoittuneet vuonna 2015. Vuosittaisessa seurannassa vuonna 2015 päästiin 100 prosenttiin neljässä mittarissa: (valtionhallinnon) organisaation osa- tai kokoaikaisen tietoturvavastaavan löytyminen, vakavista tietoturvapoikkeamista raportoiminen johdolle, huonotasoisten salasanojen käytön esto ja tietoturvapoikkeamien käsittelyn organisointi tai vastuuttaminen.[152]

Tietoturvallisuuden hallintaa ja johtamista valtioneuvossa mittaavien mittareiden valossa luvut olivat kokonaisuudessa parantuneet käytännössä kaikilla osa-alueilla vuoteen 2011 verrattaessa. Tästä huolimatta toimintakertomuksessa suositeltiin organisaatioita jatkamaan valmius-, tietoturva- ja jatkuvuussuunnittelun kehittämistä ja toteuttamista sekä huolehtia rekisteriselosteiden ajantasaisuudesta ja saatavuudesta. Lisäksi painotettiin tärkeäksi osa-alueeksi riskien ja jatkuvuudenhallinnan sekä varautumisen toteuttamista ja kehittämistä niin normaalioloissa kuin häiriötilanteissakin. Etenkin johtuen valtion- ja julkishallinnon prosessien digitalisoitumisen kiihtyvästä kehittymisestä, minkä arvioitiin kasvattavan potentiaalista hyökkäyspinta-alaa. Kehityskohteiksi mainittiin seurannan pohjalta johtaminen, kokonaisvaltaisuus, ennaltaehkäisy, varautuminen sekä tiedon ja sen arvon suojaaminen.[153]

Vuosina 2012–2015 erityistoimia vaatineiden ja kohdistettujen hyökkäysten määrä pysyi samana, mutta 2014 ja 2015 järjestelmien käyttöä estäneiden haittaohjelmien

[150] Helsingin Sanomat, 2.10.2015, ” Tiedustelulait vaativat perustuslain muuttamisen”.
[151] ”Valtionhallinnon tietoturvallisuuden johtoryhmä”. <https://vm.fi/hanke?tunnus=VM047:00/2007> [luettu 25.1.2026]; VAHTI:n toimintakertomus vuodelta 2015, 5.
[152] VAHTI:n toimintakertomus vuodelta 2015, 31.
[153] Ibid., 33–35.

raportointimäärät olivat nousseet. Vuonna 2015 vastanneista organisaatioista 36 % oli ollut haittaohjelmien takia järjestelmiä tai niiden osia haittaohjelmien takia. Edelliseen vuoteen verrattuna kyseessä oli 26 prosenttiyksikön kasvu. Lisäksi huomautetaan, että kansainvälisten selvitysten mukaan piiloon jäävien hyökkäysten osuuden arvioitiin olevan kasvussa. Yleisimmät järjestelmiin ja työasemiin vaikuttaneet tietoturvapoikkeamat olivat haittaohjelmat. Toiseksi yleisimmiksi listattiin palvelunestohyökkäykset, jonka jälkeen huijausviestit ja haavoittuvuudet.[154]

Toimintakertomus arvioi myös kyberturvallisuusstrategian täytäntöönpanon tilannetta. VAHTI ja Turvallisuuskomitea nimettiin strategiassa korostetuiksi toimielimiksi. VAHTI ilmoitti seuranneensa säännöllisesti kyberturvallisuusstrategian toimeenpanoa hallinnonaloilla. Osana seurannan tehostamista toimielimet valmistelivat kyberturvallisuuden seurannan kysymyssarjan, joilla on mitattu organisaatioiden kypsyystasoa asteikolla 0–5. Kyselyn perusteella selviää, että useimmissa mittareissa tavallisin vastaajien kypsyystaso asteikolla on 2.[155]

VAHTI:n toimintakertomus vuodelta 2015 antoi perspektiiviä kansallisessa kyberturvallisuusstrategian toimeenpano-ohjelmassa esitettyihin toimenpiteisiin. Sen perusteella suomalaisen valtiohallinnon kyberturvallisuuden kypsyystaso osoittautui verrattain alhaiseksi. Vaikka tarkastelussa on huomioitava, että toimintakertomus on julkaistu vain noin vuosi toimeenpano-ohjelman julkistamisen jälkeen, eikä toimenpiteiden – etenkään pitkäaikaisten hankkeiden ja lakimuutosten – vaikuttavuus näin lyhyellä aikavälillä välttämättä näy kybermaturiteetin arvioinnissa, kertovat tulokset kuitenkin eri todellisuutta niiden lähtötasosta.

Tarkastelussa on myös huomioitava, että toimintakertomuksessa tarkasteltu kohderyhmä koostui valtion virastoista, jotka ovat suoraan valtiohallinnon tulosohjattavia organisaatioita. Vuonna 2015 merkittävä osan suomalaisesta julkishallinnosta muodostui kunnista, joiden vastuulla olivat myös sosiaali- ja terveyspalvelut. Kunnat ovat itsenäisiä julkishallinnollisia yksiköitä, joissa ylintä päätösvaltaa käyttävät kunnanvaltuustot. Näin ollen valtioneuvosto ei voi ohjata niitä suoraan. Lisäksi suomalainen kuntasektori on hyvin hajanainen – kyberturvallisuuteen käytettävissä olevat resurssit ovat varsin heterogeenisiä. Vuonna 2021

[154] VAHTI:n toimintakertomus vuodelta 2015, 36–37.
[155] Ibid., 2015, 41–45.

Digi- ja väestötietoviraston teettämässä kyselytutkimuksessa selvisi, että 75 prosenttia vastanneista kunnista ilmoitti, että organisaatiolla oli riittämättömät resurssit huolehtia organisaation digitaalisesta turvallisuudesta. Vuonna 2015 oli hyvin todennäköistä, että kyberturvallisuuden lähtötaso on ollut varsin heikko.[156]

[156] Kuntien digitaalisen turvallisuuden selvitys 2021, 9–10.

3 Toimintaympäristön muutos herättää Suomen unesta

3.1 Muuttunut toimintaympäristö kirjoittaa kyberin turvallisuuspoliittisiin asiakirjoihin

Luvussa käsitellään kolmea Suomen valtioneuvoston laatimaa linjaavaa asiakirjaa: ulko- ja turvallisuuspoliittista ja puolustuspoliittista selontekoa sekä yhteiskunnan turvallisuusstrategiaa. Käsittelen näitä lähteitä, sillä Buzan käsittelee turvallisuutta kolmella tasolla: yksilöllisellä, kansallisella (valtiollisen) sekä kansainvälisellä.[157] Yhteiskunnan turvallisuusstrategian keskiössä on kansalaisten, ja siten yksilöiden, turvallisuus. Puolustuspoliittinen selonteko edustaa selkeinten valtion turvallisuutta ja ulko- ja turvallisuuspoliittinen selonteko puolestaan kansainvälistä – tosin Suomen näkökulmasta.

Valtioneuvoston kanslia päivitti ulko- ja turvallisuuspoliittista selontekoaan kesäkuussa 2016. Siinä määritettiin Suomen ulko- ja turvallisuuspolitiikan painopisteaiheiksi 2020-luvun puoliväliin ulottuvalle ajalle monia eri aiheita Itämeren alueen turvallisuuskysymyksistä ihmisoikeuksiin. Tiivistelmässä kyberturvallisuuteen aiheellisesti läheisin turvallisuuden painopisteaihe oli kriisinkestokyvyn vahvistaminen.[158] Kyber-alkuisia sanoja selonteossa esiintyy yhteensä seitsemän kappaletta. Verrattuna neljän vuoden takaiseen aiempaan selontekoon kyberturvallisuuteen liittyvät maininnat olivat vähentyneet merkittävästi. Asiaa saattoi osaltaan selittää kyberturvallisuudelle osoitetut omat strategiat, minkä takia aihetta ei katsottu tarpeen käsitellä tarkemmin strategisesti ylätason asiakirjassa.

Kyberturvallisuus mainitaan ensimmäisen kerran luvussa neljä, joka käsittelee ulko- ja turvallisuuspolitiikan toimintaympäristöä. Alaluvussa *4.1 Maailmanlaajuiset kehityssuunnat* sen ennustetaan kasvavan keskeisemmäksi osaksi ulko- ja turvallisuuspolitiikkaa. Ennuste pitää paikkansa, mutta tuntuu sivujuonteelta osana muita maailmanlaajuisia ilmiöitä. Tästä huolimatta kyberturvallisuuden rooli tunnistettiin.[159] Samassa kontekstissa mainittiin digitalisaatio potentiaalisen voimavarana sekä sosiaalinen media sekä tämän rajat ylittävä muutosvaikutus.[160] Maailmalta oli kantautunut uhkaavia varoitusmerkkejä Euroopan

[157] Wæver 1995, 3.
[158] Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2016, 3.
[159] Ibid., 12.
[160] Ibid., 12.

turvallisuustilanteen heikkenemisestä. Lähi-itää ravistellut arabikevät johti alueelliseen epävakauteen, joka puolestaan lietsoi verisiä sisällissotia, jotka Euroopan näkökulmasta eskaloituivat pakolaiskriisinä vuosina 2014–2015.

Alaluvussa *4.3 Valtiot ja muut kansainväliset toimijat* kyberturvallisuus mainittiin esimerkkinä sodan kuvan monimutkaistumisesta. Selonteossa oli myös ymmärretty epätavanomaisten vaikuttamiskeinojen välitön ja häilyvä luonne, jolloin niillä on mahdollista aiheuttaa epävarmuutta ja -vakautta. Näin sisäisen ja ulkoisen turvallisuuden raja hämärtyy. Jo vuonna 2016 Venäjän nähtiin hylänneen yhteistyöhön perustuvan turvallisuuden ja alkaneen haastaa Euroopan turvallisuusjärjestystä. Maan johdon katsottiin olevan halukas käyttämään sotilaallista voimaa tavoitteidensa edistämiseksi, ja tämän implisiittisesti vihjattiin aiheuttavan Suomen turvallisuusnäkymille huolenaiheita.[161]

Seuraavan kerran kyberturvallisuus otettiin esille painopisteiden ja tavoitteiden alla osana suhteiden kehittämistä sotilasliitto Natoon. Yhteistyön lisäämisen Naton kanssa kyberpuolustuksen alalla katsottiin olevan tärkeää.[162] Osana ulkoisen ja sisäisen turvallisuuden yhteyden korostamista kyberturvallisuus tekee merkittävimmän esiintymisensä, jossa sille on osoitettu kaksi kappaletta. Sitä käsiteltiin kuitenkin lähinnä ei-valtiollisessa kontekstissa. Se hahmotetaan osana kokonaisturvallisuusajattelua, jossa Suomi vahvistaa kykyjä tunnistaa hybridivaikuttamista ja sen vaatimaa suorituskykyä ja siten parantaa kyberturvallisuutta. Suomen mainitaan myös selvittävän mahdollisuuksia edistää EU:n hybridiuhkien osaamiskeskuksen perustamista. Lisäksi osana kybersuorituskyvyn vahvistamista kansainvälisen yhteistyön nähdään olevan vahvassa osassa kybertoimintaympäristön sekä digitalisaation valjastamisessa kansallisiksi kilpailueduiksi.[163]

Kaiken kaikkiaan kybertoimintaympäristöön kohdistuvat uhat tunnistettiin selonteossa, mutta tässä vaiheessa kehityskulkua niiden vaikutusten ei arvioitu olevan ulko- ja turvallisuuspolitiikan painopistealueita. Toisin kuin vuoden 2012 turvallisuus- ja puolustuspoliittisessa selonteossa niille ei ole omistettu omaa lukuaan tai edes alalukuaan. Siihen on saattanut vaikuttaa omalta osaltaan muutokset Euroopan turvallisuusympäristössä, kuten vuonna 2014 turvallisuuspoliittista miljöötä järisyttänyt Krimin valtaus ja Itä-Ukrainan

[161] Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2016, 16.
[162] Ibid., 26.
[163] Ibid., 27–28.

konflikti. Toisaalta näissäkin Venäjän hybridivaikuttaminen oli keskeisessä asemassa, ja oli omiaan vauhdittamaan Ukrainan omaa kybersuorituskykyä, joka kantoi hedelmää kahdeksan vuotta myöhemmin alkaneessa täysimittaisessa hyökkäyssodassa.

Vuoden 2013 kyberturvallisuusstrategiassa asetettu tavoite ”Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” ei välity selonteosta erityisen voimallisena tahtotilana, mikä enteilee vuotta myöhemmin valmistuneen Suomen kyberturvallisuuden tilaa arvioivan selvityksen johtopäätöksien lopputulemaa.[164] Vuonna 2016 kybertoimintaympäristöä, ja etenkin tavallisten kansalaisten IoT-laitteiden[165] verkkoa, ravistellut Mirai-haittaohjelma havaittiin ensimmäisen kerran. Haittaohjelma on tänäkin päivänä merkittävä tietoturvaongelma, jota valtiolliset ja ei-valtiolliset hyödyntävät esimerkiksi palvelunestohyökkäysten toteuttamiseen.[166] Turvallistamisteorian suhdetta kyberturvallisuuteen tutkinut Marek Górka argumentoi, että kybertoimintaympäristön turvallisuuden luotettava arvioiminen on vaikeaa. Alan toimijoilla on voimakas insentiivi pitää oma kyberkyvykkyytensä piilossa estääkseen vastapuolen kehittämästä keinoja torjua haavoittuvuuksia. Tämä aiheuttaa myös haasteita turvallistamistekojen argumentoinnille – on haastavaa perustella kansalaisia hyväksymään heidän oikeuksiaan rajoittavia toimenpiteitä ilman konkreettista uhkakuvaa.[167]

Tästä huolimatta selonteon pohjalta voi päätellä, että kyberturvallisuutta ei pidetty ulko- ja turvallisuuspoliittisesti merkittävänä tematiikkana, sillä merkittäviinkään kyberturvapoikkeamiin reagoiminen ei heijastu selonteosta. Vaikka kybertoimintaympäristön vähäistä käsittelyä selonteossa voidaan perustella sillä, että aihepiiri oli katettu vuoden 2013 erillisstrategiassa, selonteosta välittyy silti vaikutelma, ettei sen laatijoilla ole täyttä ymmärrystä kyberturvallisuuden merkityksestä ulko- ja turvallisuuspolitiikalle. Tämä varmistui muutaman vuoden myöhemmin julkaistuissa asiakirjoissa, joissa kyberturvallisuuden tila arvioitiin riittämättömäksi.[168] Peilaten myös Suomen poliittiseen tilanteeseen, vallassa olleen oikeisto-hallituksen huomio kului Euroopan turvapaikkakriisin

---

[164] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 2.
[165] IoT:lla viitataan tässä ”esineiden internetiin” eli järjestelmiin, jotka perustuvat teknisten laitteiden suorittamaan automaattiseen tiedonsiirtoon sekä niiden etäseurantaan- ja ohjaukseen internetin välityksellä.
[166] ”Miraissa on tulevaisuus”. Traficomin verkkosivut. < https://traficom.fi/fi/ajankohtaista/blogit/miraissa-tulevaisuus>.
[167] Górka 2023, 273–275.
[168] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, passim.

selvittämiseen, mikä saattoi osittain selittää poliittisen sitoutumisen vajavaisuutta. Toisaalta Sipilän hallituskauden aikana saatiin vietyä maaliin Suomen uudet tiedustelulait ja perustettua Helsinkiin Euroopan hybridiuhkien torjunnan osaamiskeskuksen, mitkä konkreettisesti edistivät Suomen kybertoimintaympäristön turvaamista.[169]

Vuosi ulko- ja turvallisuuspoliittisen selonteon julkaisemisen jälkeen julkaistiin valtioneuvoston puolustusselonteko. Puolustusselonteossa määritellään Suomen puolustuspoliittiset linjaukset puolustuskyvyn ylläpidolle, kehittämiselle ja käytölle. Se jakaantui kolmeen osaan: sotilaallisen toimintaympäristön, puolustuksen nykytilan sekä puolustuskyvyn ylläpidon ja kehittämisen arviointiin. Kyber-alkuiset sanat esiintyivät ulko- ja turvallisuuspoliittista selontekoon verrattuna voimallisemmin – yhteensä 19 kertaa.[170]

Kybersuorituskyky mainittiin selonteossa jo tiivistelmässä osana puolustusvoimien suorituskykyä. Vuonna 2014 pääministerinä toimiessaan Alexander Stubb peräänkuulutti kybertoimintojen tunnustamista osana asevoimien perinteisiä puolustushaaroja kansainvälisiin viitekohteisiin vedoten.[171] Tämä on merkittävä ero ulko- ja turvallisuuspoliittiseen selontekoon, sekä liittää kybertoimintaympäristön turvaamisen keskeiseksi osaksi Suomen puolustuspolitiikan painopisteitä.[172] Kyberturvallisuus mainitaan heti ensimmäisessä käsittelyluvussa, jossa tarkastellaan sotilaallisen toimintaympäristön trendejä. Luku alkoi toteamalla Suomen lähialueen turvallisuustilanteen heikentyneen Krimin valtauksen ja Itä-Ukrainan konfliktin seurauksena, minkä puolestaan nähdään lisänneen jännitteitä ja epävarmuutta Itämerellä sekä laajemminkin. Osana samaa lukua kybertoimintaympäristön merkityksen todettiin kasvavan.[173]

Kyberkeinojen käyttö poliittisten päämäärien saavuttamiseksi tunnistettiin, ja yhteiskunnan elintärkeiden toimintojen katsottiin olevan alttiita kybervaikuttamiselle. Tämän lisäksi todettiin, että Suomen kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan oli jo kohdistettu kyber- ja

---

169 ” Eurooppalainen hybridiuhkien osaamiskeskus perustettiin Helsinkiin”. Valtioneuvoston verkkosivut. < https://valtioneuvosto.fi/-/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin?_101_INSTANCE_3wyslLo1Z0ni_groupId=10616> [luettu 13.5.2026].
170 Valtioneuvoston puolustusselonteko 2017, 3–4.
171 Limnéll 2014, 4.
172 Valtioneuvoston puolustusselonteko 2017, 6.
173 Ibid., 8–9.

informaatiovaikuttamista.[174] Suomen valtion puolustuspoliittisten painopisteiden asettaman asiakirjan kautta lausutaan kyberturvallisuuden näin ollen aiheuttavan Suomen valtiolle merkittävän uhkan, johon puolustusvoimien tulee lähitulevaisuudessa vastata. Mahdollisesti asiakirjan merkittävin turvallistamisteko löytyy luvun lopusta, jossa Suomen puolustamisen edellytyksiksi luetellaan perinteisten maa-, meri- ja ilmatoimintaympäristöjen lisäksi kyvykkyys turvata kybertoimintaympäristöä.[175]

Kyberturvallisuuden mainitseminen perinteisten sotilaallisen turvallisuuden toimintaympäristöjen rinnalla loi mielikuvaa siitä, että selonteon lukija ymmärtää aiheen osana Suomen puolustusvoimien, valtion, sekä viime kädessä kansan, elinehtona. Viimeistään tässä vaiheessa kyberturvallisuus voidaan ymmärtää siirretyksi turvallisuuskysymysten luokkaan. Toisin sanoen selonteossa käytännössä myönnetään, vaikka tätä ei suoranaisesti lausuttu julki, että kybertoimintaympäristön häiriöiden nähdään olevan niin vakava riski tärkeäksi pitämillemme viitekohteille, että näiden suojaamiseksi kansalaisten on tarvittaessa hyväksyttävä oikeuksiensa kaventuminen. Tällöin Wæverin et al. ymmärtämällä tavalla käytännössä onnistuneen turvallistamisteon kriteerit täyttyvät. [176] Toisaalta selonteosta ei selvinnyt, miten valtioneuvosto ja Puolustusvoimat tulisivat käytännössä lisäämään turvallisuutta. Viimeinen luku, joka käsitteli puolustusvoimien resursseja, esitti turvallisuusympäristön muutoksen edellyttämään valmiuden parantamiseen lisäresursseja. Näin ollen toistaiseksi suomalainen veronmaksaja joutui tyytymään 55 miljoonan euron ylimääräiseen kuluerään kyberpuolustuksen, sekä monen muun maanpuolustuksen kannalta välttämättömän toimen, varmistamiseksi.

Osana alalukua *4.3 Puolustusjärjestelmän käytön ja ylläpidon painopisteet* eriteltiin, että selontekokauden puolustusjärjestelmän ylläpidon ja kehittämisen painopisteet ovat: ”kaikkien puolustushaarojen valmius”, ”käytöstä poistuvien suorituskykyjen korvaaminen” ja ”tiedustelu, kyberpuolustus ja kaukovaikuttaminen”.[177] Aihetta linjattiin tarkemmin alaluvussa *4.3.4 Puolustusjärjestelmän yhteiset suorituskyvyt*. Puolustusvoimat sitoutui jatkamaan kyberpuolustuksen kehittämistä kansallisen kyberturvallisuusstrategian mukaisesti sekä ”rakentamaan kyvyn kybertilannekuvan muodostamiseen, kyberoperaatioiden

---

[174] Valtioneuvoston puolustusselonteko 2017., 9.
[175]Ibid., 10.
[176] Wæver 1995, 7.
[177] Valtioneuvoston puolustusselonteko 2017, 19.

suunnitteluun ja toimeenpanoon sekä omien järjestelmien suojaamiseen ja valvontaan kybertoimintaympäristössä”.[178] Verrattuna ulko- ja turvallisuuspoliittiseen selontekoon, puolustusselonteosta välittyi, että puolustusministeriön hallinnonala oli selkeämmin perillä kybertoimintaympäristön häiriöiden vaikutuksista sekä heidän omiin että koko yhteiskunnan toimintoihin. Tämä on sikäli yllättävää ottaen huomioon, että vain kolme vuotta aikaisemmin ulkoasiainhallintoon oli kohdistunut Venäjään linkittynyt tietoverkkovakoilu.[179]

Samana vuonna julkaistiin *Yhteiskunnan turvallisuusstrategia 2017*. Siinä päivitettiin vuonna 2010 asetetut varautumisen kansalliset periaatteet ja kokonaisturvallisuuden yhteistoimintamalli. Vuodesta 2010 eroten päivitetyssä yhteiskunnan turvallisuusstrategiassa puhutaan elintärkeiden toimintojen lisäksi kokonaisturvallisuudesta[180], joka käsittää aiemmin käsiteltyjä toimintoja osana laajempaa yhteistoimintamallia. Tähän laajempaan yhteistoimintamalliin tunnistetaan kuuluvan valtiollisten toimijoiden lisäksi muu julkinen hallinto, elinkeinoelämä, yliopistot ja tutkimuslaitokset, järjestöt, yhteisöt ja yksilöt.[181] Kokonaisturvallisuuden mainitaan kehittyneen ensisijaisesti yhteistoimintamalliksi, jossa ”-- toimijat jakavat ja analysoivat turvallisuutta koskevaa tietoa sekä suunnittelevat, harjoittelevat ja toimivat yhdessä.” Yhteistyö perustuu lakisääteisiin tehtäviin, yhteistyösopimukseen sekä *Yhteiskunnan turvallisuusstrategiaan*. Vuoden 2017 strategiassa painopiste laajennetaan valtioneuvostotasolta, jolle se aiemmin painottui, kattamaan laajalti koko yhteiskuntaa.[182]

Kyberalkuiset sanat esiintyivät vuoden 2017 turvallisuusstrategiassa 13 kertaa. Kokonaisturvallisuuden käytännön jalkautuksen mainittiin toteutettavan hallinnonalakohtaisissa tai poikkihallinnollisissa strategioissa, toimeenpano-ohjelmissa ja muissa asiakirjoissa. Näistä esimerkkeinä nostettiin Suomen kyberturvallisuusstrategia sekä sen toimeenpano-ohjelma. Yhteiskunnan elintärkeät toiminnot uudelleenjärjesteltiin seitsemään kokonaisuuteen: johtamiseen; kansainväliseen ja EU-toimintaan; puolustuskykyyn; sisäiseen turvallisuuteen; talouteen, infrastruktuuriin ja huoltovarmuuteen; väestön toimintakykyyn ja palveluihin sekä henkiseen kriisinkestävyyteen.[183]

---

178 Valtioneuvoston puolustusselonteko 2017, 23.
179 ” Venäjän verkkovakoojat iskivät Suomeen satelliittien avulla – Hyökkäys ulkoministeriöön oli osa laajaa kampanjaa”. *Yle Uutiset*. 13.1.2016. < https://yle.fi/a/3-8589628>. [luettu 13.5.2026].
180 Määriteltiin ensi kerran tavoitetilaksi valtioneuvoston periaatepäätöksessä kokonaisturvallisuudesta (5.12.2012). Kokonaisturvallisuuden hallintaan eli yhteiskunnan elintärkeiden toimintojen ylläpi- tämiseen kuuluvat uhkiin varautuminen, häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen.
181 Yhteiskunnan turvallisuusstrategia 2017, 5; Yhteiskunnan turvallisuusstrategia 2010, 1.
182 Yhteiskunnan turvallisuusstrategia 2017, 5–6; Yhteiskunnan turvallisuusstrategia 2010, 1–2.
183 Yhteiskunnan turvallisuusstrategia 2017, 4, 7–8.

Alaluvussa *3.5 Talous, infrastruktuuri ja huoltovarmuus* puhuttiin suoraan kyberturvallisuudesta, ja käsiteltiin aihetta osana kokonaisturvallisuutta. Se antoi monipuolisemman katsauksen tieto- ja viestintätekniikan roolista osana infrastruktuuria ja huoltovarmuutta verrattuna vuoden 2010 strategiaan. Merkittävin ero oli yhteiskunnan muiden toimijoiden, kuten elinkeinoelämän, yhteisöjen ja kansalaisten, huomioiminen häiriötilanteiden vaikutuksissa sekä kansainvälisten velvoitteiden tunnistaminen. Lisäksi talouden, infrastruktuurin ja huoltovarmuuden tiedostettiin olevan riippuvaisia teknologioista, joiden varaan nämä rakentuvat.[184] Tämä osoittaa kyberturvallisuuden koko yhteiskunnan kattavan vaikutuksen ymmärrystä.

Kyberturvallisuutta ei kaksiosaisen strategian ensimmäisessä osiossa näiden nostojen lisäksi mainittu eksplisiittisesti osana yhteiskunnan elintärkeitä toimintoja. Kyberistä puhuttiin muutaman kerran strategian toisessa osiossa, jossa käsiteltiin hallinnonalojen strategisia tehtäviä, eli nimitettiin vastuulliset ministeriöt kullekin osa-alueelle.[185] Yksittäiset turvallisuusaiheet oli kuitenkin jätetty ensimmäisessä osassa laveammalle tarkastelulle kuin esimerkiksi puolustuspoliittisessa selonteossa.

Osio 27. *Julkisen hallinnon ICT-infrastruktuurin ja digitaalisten palvelujen turvaaminen* oli koko strategian yksi merkittävimmistä kirjauksista senaikaisen kyberturvallisuusymmärryksen käsittämiseksi. Siinä kirjattiin valtiovarainministeriön ja valtioneuvoston kanslian hallinnonalalle kuuluvan yhteiskunnan elintärkeiden toimintojen vaatiman tietohallinnon, ICT-ohjauksen, tieto- ja kyberturvallisuuden ohjauksen sekä julkisen hallinnon digitaalisten palveluiden ja tiedon turvaaminen. Mielenkiintoisesti kirjauksessa tavoitetasoksi määriteltiin, että elintärkeiden toimintojen kannalta välttämättömien digitaalisten palveluiden ja tietojen toimivuuden sekä oikeellisuuden tulisi olla varmistettu vain julkisen hallinnon tasolla – ei koko yhteiskunnan.[186]

Toisaalta itse toimintamallia käsittelevässä kappaleessa tarkennettiin, että julkisen hallinnon tuottamat yhteiskunnan elintärkeiden toimintojen palvelut perustuvat julkisen hallinnon ja elinkeinoelämän välisiin sopimuksiin. Seuraavat kappaleet keskittyvät valtiovarainministeriön

---

[184] Yhteiskunnan turvallisuusstrategia 2017, 20–21; Yhteiskunnan turvallisuusstrategia 2010, 35–36.
[185] Yhteiskunnan turvallisuusstrategia 2017, 27–29.
[186] Ibid., 2017, 59–60.

rooliin julkisen hallinnon ICT-infrastruktuurin, digitaalisten palvelujen kokonaisarkkitehtuurin, näiden yhteentoimivuuden ohjaamisen sekä tietoturvallisuuden yleisten periaatteiden laatimiseen. Tämän pohjalta todettiin myös, että ministeriö määrittelisi vähimmäiskriteerit edellä mainituille palveluille julkisessa hallinnossa. Tämän lisäksi keskeiset vastuulliset viranomaiset tunnistettiin. Merkittävä ero esimerkiksi vuoden 2025 yhteiskunnan turvallisuusstrategiaan löytyi kybertoimintaympäristön kattavuudesta – seitsemän vuotta myöhemmin asia muotoillaan seuraavalla tavalla: ”[kyberturvallisuuden] yhteistoiminnan tavoitteena on varmistaa kaikissa oloissa yhteiskunnan keskeisten toimijoiden tiivis yhteistyö varautumisessa”.[187]

Peilaten VAHTI:n arvioon kyberturvallisuuden tilasta julkisella sektorilla, on ymmärrettävää, että painopiste on ollut julkishallinnon kriisinkestävyyden edistämisessä. Tästä huolimatta, kuten viranomaiset itsekin ovat tunnistaneet, valtaisa osa Suomen elintärkeiden toimintojen kriittisestä infrastruktuurista on yksityisen sektorin hallinnoimaa. Puute nostetaan myös esille Suomen kybertoimintaympäristön tilaa arvioivissa asiakirjoissa, joita vuonna 2017 teetettiin. Merkittävänä haasteena strategian kohdalla oli sen koherentti johtaminen – sen ohjelmakohtia toteutettiin siiloissa vailla riittävän yhtenäistä ohjaus- ja seurantarakennetta. Samalla jälkiviisaana voi hieman liioitellen pohtia, enteilikö tämä esimerkiksi vuoden 2020 psykoterapiakeskus Vastaamon tai vuoden 2024 Helsingin kaupungin tietomurtoja.

Toisaalta tämä ei tunnu niin kaukaa haetulta tarkastellessa, miten voimahuollon, sosiaali- ja terveydenhuollon tietojärjestelmien toimivuuden ja elintarvikehuollon osa-alueiden kybertoimintaympäristön mahdollisista häiriötilanteista puhuttiin. Ne kyllä tunnistettiin uhkakuviksi, mutta niiden todellisen luonteen ymmärtäminen vaikutti vajavaiselta. Valitettavan usein tarvittaviin toimiin saadaan rahoitus ja riittävä poliittinen tahto vasta, kun vahinko on kerennyt tapahtua. Vuonna 2017 WannaCry -niminen kiristysohjelma alkoi leviämään sadoille tuhansille haavoittuvaisille tietokoneille ja lukitsemaan ne. Vaikka haittaohjelmalle löydettiin niin sanottu tappokytkin, se kerkesi aiheuttaa merkittävää vahinko ja vauriota kansainvälisesti julkisten hallintojen organisaatioissa. Esimerkiksi Yhdistyneiden kuningaskuntien terveydenhuoltojärjestelmän ICT-järjestelmät, jotka koostuivat suuresta määrästä päivittämättömiä Windows-käyttöjärjestelmää hyödyntäviä tietokoneita, joutuivat

[187] Yhteiskunnan turvallisuusstrategia 2017, 59–60; Yhteiskunnan turvallisuusstrategia 2025, 109.

haittaohjelman uhriksi. Tämä johti joidenkin teho-osastojen sulkemiseen, mikä johti suoraan ihmisten henkien vaarantumiseen.[188]

3.2 Kyberturvallisuusstrategia reputtaa ensimmäisen kokeensa

Vuonna 2017 maailmalta saatiin hälyttäviä uutisia kybertoimintaympäristössä tehtyjen hyökkäysten yhteiskunnallisista vaikutuksista. Venäjä hyökkäsi tuolloin Ukrainan yhteiskuntaa vastaan useilla eri kyberhyökkäyksillä. Kohteina oli useita eri pankkeja, kansallinen sähköverkko ja yksityisiä yrityksiä. Kyseessä oli tarkoituksenmukainen hyökkäys Ukrainan yhteiskunnan jokapäiväistä toimintaa ylläpitävää infrastruktuuria vastaan, ja kohteiksi joutui useita toimintoja, jotka Suomi itse luokitteli jo vuoden 2017 *Yhteiskunnan turvallisuusstrategiassa* elintärkeiksi toiminnoiksi.[189] Sama Ukrainan yhteiskuntaa ravistellut kiristysohjelma aiheutti tanskalaiselle rahtilaivajätti Maerskille yli 300 miljoonan Yhdysvaltain dollarin tappiot saastuttaen 45 000 tietokonetta ja 4 000 palvelinta, mikä johti 76:n globaalin sataman terminaalin sulkeutumiseen.[190] Kyberturvallisuuden pettämisen vaikutukset eivät enää olleet tieteisfiktiivistä satuilua.

Vuoden 2017 helmikuussa julkaistiin hankeselvitys, jossa arvioitiin vuoden 2013 kyberturvallisuusstrategiassa esitettyjä tavoitteita suhteessa senhetkiseen suomalaisen yhteiskunnan kyberturvallisuuden tilaan. Hankkeen tavoitteena oli selvittää kokonaisvaltaisesti, miltä osin strategiassa asetettu tavoite ”Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” on saavutettu sekä millaiset tavoitteet tulisi aseetta tälle vuonna 2020.[191]

Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi -nimisen selvityksen lopputuleman mukaan Suomi ei yltänyt vuonna 2013

---

[188] ”Tietoturvailmiöt, jotka muuttivat maailmaa”. Traficomin verkkosivut. < https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvailmiot-jotka-muuttivat-maailmaa>; “What Is WannaCry Ransomware? Does WannaCry Still Exist?”, Fortinetin verkkosivut. < https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack>.

[189] Reuters, 27.7.2017, ” Ukrainian banks, electricity firm hit by fresh cyber attack”. < https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ/> [luettu 22.3.2026]; BBC, 26.7.2017, “Ukraine braces for further cyber-attacks”. < https://www.bbc.com/news/technology-40706093> [luettu 22.3.2026].

[190] “Notpetya ransomware attack on Maersk - key learnings”. LRGA:n verkkosivut. < https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/>.

[191] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 2.

asetettuihin tavoitteisiin, mutta ne olisivat vielä saavutettavissa. Etenkin merkittävää oli tutkimuksessa määritelty tavoitetila, jonka mukaan ”-- vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaa kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti”.[192] Tavoite oli kunnianhimoinen, mutta erittäin tarkoituksenmukainen olettaen, että kansallisena tahtotilana pidetään edelleen maailmanlaajuisen edelläkävijyyden saavuttamista kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.[193]Selvitys eritteli tiivistelmässään useita kehittämiskohteita, joita joissain tämän tutkielman aikaisemmissa luvuissakin on käsitelty, jotka eritellään vielä tämän luvun lopussa.

Kyberturvallisuuden megatrendeiksi selvityksen[194] laatimisen aikaan – vuonna 2016 – eriteltiin kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhkat, yrityksen sisäpiiri hyökkäyskanavana, liiketoiminnan tuhoamiseen tähtäävät hyökkäykset sekä henkilötietojen varastaminen. IoT-laitteiden, kuten älypuhelinten, tablettien ja muiden internetiin yhdistettävien laitteiden laaja-alaisen yleistymisen nähtiin kasvattaneen potentiaalista hyökkäyspinta-alaa, minkä lisäksi kyberhyökkääjien kyvykkyyksien nähtiin kasvaneen. Samaan aikaan myös yrityksiin kohdistuneiden hyökkäysten määrän raportointiin olleen kasvussa. Erään lähteen mukaan jopa 21 % yrityksistä olisi menettänyt vuoden 2014 aikana luottamuksellisia tietoja, ja yritysten sisäpiiriläiset olivat näissä useimmiten epäiltyinä. Nämä molemmat trendit olivat johdonmukaisia aikaisemmassa kappaleessa käsiteltyjen kyberhyökkäystapausten valossa.[195]

Merkittävimmiksi kyberuhkiksi puolestaan nostettiin älypuhelimiin ja IoT-laitteisiin kohdistuvat hyökkäykset, web-hyökkäykset, sosiaalisen median, kohdistetut hyökkäykset, tietovuodot ja yksityisyyden suoja sekä pilvipalvelut.[196] Henkilökohtaisiin älypuhelimiin ja IoT-laitteisiin sekä sosiaaliseen kohdistuneiden hyökkäysten lisääntyminen tunnistettiin valtiohallinnon puolesta viimeistään tässä vaiheessa, ja nosti kyberturvallisuuden häiriötilanteet koskemaan myös yksilöitä. Samalla yksityisen sektorin huomattiin

[192] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 2.
[193] Ibid., 2–3.
[194] Eräs käytetyistä lähteistä oli Kasperysky -nimisen venäläisen tietoturvayhtiön laatima. Yhtiön tuotteet ja palvelut on Ukrainan sodan jälkeen kielletty esimerkiksi Yhdysvalloissa, ja Saksan turvallisuusviranomaiset varoittivat sen palveluiden käyttämisestä.
[195]Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 12–13.
[196] Ibid., 13–17.

havahtuneen jo tähän trendiin – AT&T:n mukaan haavoittuvuuksien etsimiseen tähtäävät skannaukset päätelaitteissa ovat lisääntyneet 458 %, ja kybertoimintaympäristössä yritykset ja kyberhyökkääjät käyvät kiihtyvää kilpajuoksua haavoittuvuuksien etsimisessä ja tukkimisessa.[197]

Älypuhelinten tietoturva ja sosiaalisen median avulla kohdistetut hyökkäykset yksityishenkilöitä kohtaan tähdensivät laajemmin nopeasti konkretisoitunutta aspektia; henkilökohtaista yksityisyyden ja omaisuuden suojan merkittävää heikentymistä. Tieto- ja viestintäteknologian ripeä kehitys, ja sen uiminen kiistämättömäksi osaksi jokapäiväistä elämää on viimeisen 10–15 vuoden aikana tuonut kybertoimintaympäristön turvallisuushaasteet kosketeltavan lähelle tavallista suomalaista. Lisäksi yksilön, yhteiskunnan ja valtion kyberturvallisuuden voi huomata tässä vaiheessa jo liittyneen toisiinsa niin saumattomasti, että niiden käsittely erillisinä itsenäisinä kokonaisuuksina tuntui kyseenalaiselta.[198] Turvallistamisen näkökulmasta päästään merkittävään haasteeseen, jota myös Marek Gorka on tarkastellut artikkelissaan ”Conceptualising securitisation in the field of cyber security policy” – millaisena turvallisuusongelmana kyberturvallisuutta pitäisi käsitellä? Onko vastuu valtiohallinnon, palveluntarjoajien ja muiden alan erityisasiantuntijoilla, vai pitäisikö sen olla monialaisemmin säädelty kokonaisuus?[199]

Huolimatta taustalla vaikuttavista mahdollisista motiiveista, tämä julkaisu oli valtionneuvoston tasolla myös yksi ensimmäisistä, joka laaja-alaisesti ja kattavasti pyrki turvallistamaan kyberturvallisuutta myös yksilöiden perspektiivistä. Aihe oli turvallistettavana kokonaisuutena sikäli haastava, että tietoteknisiä haavoittuvuuksia koskevan keskustelun seuraaminen edellyttää tavan kansalaiselta varsin kattavaa ymmärrystä ICT-järjestelmistä ja ohjelmista. Vaikka toteutuneiden uhkakuvien realiteetit olivat varmasti selvempiä kuin itse niihin johtaneet vaiheet, aiheuttivat esimerkiksi Suomen ensimmäisen tiedustelulainsäädännön säätäminen (709/2019) ja (590/2019) merkittävääkin poliittista polemiikkia vuosina 2015–2019. Valtiohallinnon pääviestinä pidettiin tuolloin kansallisen turvallisuuden varmistamista, vaikka sillä oli myös myönteisiä vaikutuksia yksilöiden

---

[197] [197]Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 14.
[198] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 15–17.
[199] Górka 2023, 271–272.

kybertoimintaympäristön turvallisuuteen.[200] Toisaalta paradoksaalisesti nämä lait omalta osaltaan heikensivät yksityisyydenturvaa, viestisalaisuutta ja yleistä yksityiselämän suojaa.

Pilvipalveluiden lisääntyminen yritysten ja muiden organisaatioiden käyttämänä infrastruktuurina oli huomattu. Pilvipohjaisia SaaS-, PaaS- tai IaaS-palveluja ei itsessään pidetty turvallisuushaasteena, mutta käytännössä ne muodostivat uuden palvelukerroksen, mikä puolestaan kasvatti hyökkäyspinta-alaa. Etenkin sen vuoksi, että monet yritykset säilyttivät liiketoiminnan kannalta kriittistä dataa. Pilvipohjainen arkkitehtuuri nähtiin erityisen alttiiksi palvelunestohyökkäyksille sekä niihin usein liitetyille tietovuotohyökkäyksille.[201] Vaikka Euroopan turvallisuustilanne oli jo alkanut muuttua Krimin valtauksen, Yhdysvaltain uuden, transatlanttisista suhteista piittaamattoman, hallinnon sekä vuoden 2015 pakolaiskriisin myötä, näkyi asiakirjassa kuitenkin verrattain vahva luottamus sääntöperusteiselle kansainväliselle järjestykselle. Tämä oli silminnähden selvää, kun tilannetta verrataan vuosikymmen myöhempään aikaan, jolloin strateginen autonomia hallitsee turvallisuusajatteluamme. Vuosien 2025–2026 vaihteessa Suomessa käytiin huolestunut keskustelu siitä, että Suomen vaalitietojärjestelmää oltiin siirtämässä Amazon Web Services -palveluun.[202]

Vuonna 2015 terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne- ja kuljetustoimiala olivat viisi useimmiten kyberhyökkäysten kohteena olleita toimialoja. Kyberuhkien aiheuttajiksi tunnistettiin neljä erillistä ryhmittymää: sisäpiiriläiset, kybervandaalit, kybervakoilijat ja kyberterroristit ja -sotilaat. Näistä eniten tuhoa arveltiin aiheuttaneen sisäpiiriläiset ja kybervakoilijat. Sisäpiiriläisten roolia selittää kyseisen ryhmän suuri koko ja toisaalta väärinkäytösten helppous, sillä usein rikkomukset liittyvät käyttäjätunnushallinnan hyväksikäyttämiseen. Yhdysvaltain hallitus piti vuonna 2015 kybervakoilua merkittävänä ja kasvavana uhkana valtion turvallisuudelle. Ja hyvästä syystä, sillä jo tuolloin kybervakoilijat onnistuivat osoittamaan, että kyberhyökkäyksillä voi olla hyvinkin tuhoisia seurauksia – Sonyn ja TV5Mondeen kohdistuneen hyökkäykset rampauttivat yritysten palvelut viikoiksi, ja OPM-tietomurto puolestaan johti 21,5 miljoonan

---

[200] Helsingin Sanomat, 30.9.2017, ”Tiedustelulakien laadinta haastaa Suomen, vaikka tiedustelulla on vakka poliittisen johdon tuki”.
[201] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 18.
[202] Helsingin Sanomat, 10.3.2026, ”Supon päällikkö: Kannattaisi vielä harkita vaalitietojen siirtämistä Amazonin pilveen”. < https://www.hs.fi/politiikka/art-2000011871700.html>; Yle Uutiset, 20.2.2026, ”Suomi voi ajatua kaaokseen, jos yhdysvaltalainen jätti ei noudata sopimuksiaan”. < https://yle.fi/a/74-20210924>.

ihmisen biometristen sekä muiden henkilötietojen vuotamiseen. Yhdysvallat syytti hyökkäyksestä julkisesti Kiinaa.[203]

Selvitys tarkasteli myös Suomen kyberturvallisuuden nykytilaa julkisella sektorilla, ja arvioi oliko vuoden 2013 kyberturvallisuusstrategian visiona esitetty tavoitetila saavutettu, ja oliko kyberturvallisuutta kehitetty strategiassa esitettyjen linjausten mukaisesti. Sen perusteella Suomi ei saavuttanut strategiassa asetettuja tavoitteita. Tämän lisäksi strategiaa kritisoitiin liian yleisluontoiseksi, minkä katsottiin johtuvan poikkihallinnollisen valmistelun aiheuttamista kompromisseista. Lisäksi sen toimeenpano jätettiin jo valmisteluvaiheessa toteutettavaksi siilomaisesti toimiviin hallinnonaloihin, mikä ei tukenut poikkihallinnollisten yhteistyörakenteiden syntymistä. Myös liiallista valtiohallintokeskeisyyttä kritisoitiin, ja elinkeinoelämän katsottiin jääneen liiaksi marginaaliin. Strategian keskeisimmäksi onnistumiseksi mainitaan Keskusrikosrikospoliisin kyberyksikön perustaminen ja Kyberturvallisuuskeskuksen perustaminen.[204]

Kokonaisuutta tarkastellessa Suomen tilannetta pidettiin kohtuullisena verrattuna alan edelläkävijöihin. Suomi oli Euroopan 17. valtio, joka oli laatinut kansallisen kyberturvallisuusstrategian. Sen arvioitiin sijoittuvan kärkikymmenikköön eri kyberturvallisuuden mittareilla. Toisaalta selvityksessä muistutetaan, että Suomi pyrkii olemaan edelläkävijä nimenomaan kyberuhkiin varautumisessa, eikä esimerkiksi offensiivisissa kyvyissä. Lisäksi kyberturvallisuusstrategian ja sen toimeenpano-ohjelman on nähty vaikuttavan kaikkien hallinnonalojen toimintaan, minkä koetaan lisänneen kybertietoisuutta.[205]

Haasteina nähtiin Suomen valtiohallinnon, ja etenkin valtioneuvoston, siiloutuneisuus hallinnonaloittain. Toisin kuin ideaalitilanteessa, poikkihallinnollinen, yhteinen kyberosaamisen ja -kyvykkyyden kasvattaminen koko suomalaisessa julkisessa hallinnossa ei onnistunut parhaalla mahdollisella tavalla. Lisäksi monen viraston mainittiin kärsineen puhtaasti aiheen ymmärtämättömyydestä. Tämä näkyi muun muassa siten, että kyberturvallisuutta pidettiin mutkikkaana, vaivalloisena ja ainoastaan kyseisen hallinnon alan

[203] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 18–21; Ilta Sanomat, 24.9.2015, ” Valkoisen talon jättimäinen vahinko: 5,6 miljoonan sormenjäljet vietiin”.
[204] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 23–24.
[205] Ibid., 25–26.

ICT-sektoria koskevana asiana, minkä takia aihe sijoitettiin monesti prioriteettilistalla alhaiselle tasolle. Haastatteluissa nousi myös suoraan esille, että kyberturvallisuutta ei saatu implementoitua kansalliseen kokonaisturvallisuuteen sisäänrakennettuna, eivätkä he tunnistaneet Suomessa olevan pitkän aikavälin poliittista tahtotilaa tai johtamismallia kyberturvallisen digiyhteiskunnan rakentamiseksi. Merkittäväksi haasteeksi tuolloin raportoitiin myös riittämätön resurssointi kyberturvallisuudelle määritettyjen tehtävien suorittamiseksi, mikä johti näiden tehtävien tekemiseen virkatyön ohessa.[206]

Myös itse toimenpideohjelmaa ja sen syntykontekstia taustoitettiin sekä arvioitiin selvityksessä. Ohjelma koostui tehtävistä ja vastuista strategian tavoitteiden toimeenpanemiseksi, jotka hallinnonalat saivat osin itse määritellä itselleen, minkä takia se ei muodosta yhtenäistä ja selkeää koko ohjelman läpileikkaavaa linjaa. Toisaalta hallinnonalat olivat haastattelujen perusteella sellaisessa uskossa, että ohjelman toimeenpanoon oltaisiin ollut allokoimassa ylimääräisä määrärahoja, mikä ei lopulta pitänytkään paikkansa. Tämän myötä osa ohjelmassa esitetyistä toimenpiteistä oli jo lähtökohtaisesti epärealistisia, minkä takia sen onnistumisen arvioinnin mainitaan olevan haastavaa suorittaa jälkikäteen. Sillä myöskin mainittiin olevan vaihteleva painoarvo ministeriöittäin.[207]

Tämä indikoi, että vuonna 2016 Suomen kyberturvallisuuden johtaminen valtiojohdon tasolla oli hajanaista ja siten varsin vajavaista, sillä esimerkiksi viimeisimmässä *Yhteiskunnan turvallisuusstrategiassa* linjattiin, että kokonaisturvallisuutta käytännön tasolla toteutettaisiin hallinnonalakohtaisissa tai poikkihallinnollisissa strategioissa ja muissa vastaavissa asiakirjoissa.[208] Toisin sanoen Suomen kokonaisturvallisuuden kyberturvallisuuden elementtejä ohjattiin strategialla, joka oli jo laatimisvaiheessaan ongelmallinen. Tämä johti tilanteeseen, jossa ei ollut selkeyttä siitä, mikä oli ”kriittistä”. Haastatteluiden pohjalta suositeltiin, että toimiva johtamisjärjestely rakennetaan aina valtionhallinnon ylimmälle tasolle saakka; eri toimijoiden välisen kyberturvallisuusfoorumin luomista sekä ketteryyden lisäämistä eri sisäisten sekä ulkoisten yhteistyötahojen välille. Myös vuonna 2017 tehty

---

[206] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 26–27.
[207]Yhteiskunnan turvallisuusstrategia 2017, 27.
[208]Ibid., 7.

VTV:n selvitys kybersuojauksen toteuttamisesta huomautti operatiivisen johtajuuden olemattomuudesta.[209]

Tilannekuva Suomen kybertoimintaympäristöstä vuonna oli 2016 pirstaleinen, ja sen kokonaisuuden hahmottaminen oli hankalaa, sillä se perustui eri tahojen keskenään jakamasta tiedosta rakentuvaan tilkkutäkkimäiseen kokonaisuuteen. Lisäksi sen muodostamista nähtiin hankaloittavan toimivaltuuksien puute sekä kykenemättömyys tehokkaaseen tiedonjakoon yhteiskunnan eri toimijoiden välillä. Strategisella tasolla tilanteen olisi linjausten perusteella pitänyt parantua, mutta käytännön nähtiin laahaavan perässä.[210] Selvitystä varten haastateltavat asiantuntijat arvioivat, että esimerkiksi yksityiseltä sektorilta saatava tilannekuvan eri toimialojen kyberturvallisuudesta olisi vapaaehtoisuuteen perustuvan tiedonvaihtokäytännön takia epätäydellinen, eikä vastannut sektorin tosiasiallista tilaa. Kolmannen sektorin tilasta, jonka muodostavat yhdistykset, säätiöt ja järjestöt käsittelevät sekä keräävät suuria määriä henkilötietoja, ei mainittu mitään, mikä osaltaan indikoi vielä heikommasta tilannekuvasta näiden toimijoiden suhteen.[211] Samalla tavoin myös kybertoimintaympäristön uhkien havainnointikyvyn mainittiin olevan puutteellinen, mutta tarkempaa arviota sille ei osattu antaa, sillä suomalainen yhteiskunta ei ollut joutunut vakavien kyberhyökkäysten kohteeksi. Kehitysehdotuksiksi ehdotettiin laajempia viranomaisten toimivaltuuksia sekä julkisen ja yksityisen sektorin välistä yhteistyötä.[212]

Seuraavissa alaluvuissa analysoitiin poliisin ja puolustusvoimien kyvykkyyttä sekä toimivalmiuksia valvoa kybertoimintaympäristöä. Haastateltavat uskoivat poliisin tarvitsevan nykyistä laajemmat toimivaltuuden kansallisten ja rajat ylittävien kyberrikosten torjumiseen. Selvityksessä sanoitettiin selkeästi ja painokkaasti muutos, joka oli myös vuoden 2016 puolustusselonteosta huomattavissa: Suomen sotilaalliseen puolustamiseen kuuluisi nyt maa-alueen, vesialueen ja ilmatilan lisäksi kansallisen kybertilan valvominen sekä koskemattomuuden turvaaminen. Tämä kyvykkyys muodostuisi tiedustelusta, vaikuttamisesta sekä suojautumisesta. Haastateltavat näkivät puolustusvoimien kyberkyvykkyyksien kehittämisen välttämättömänä Suomen suvereniteetin sekä alueellisen koskemattomuuden

[209] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 27–29; Kybersuojauksen järjestäminen 2017, 5.
[210] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 29.
[211] Ibid., 30.
[212] Ibid., 30–31.

varjelemiseksi. Tämän valossa aikaisemmin mainittua tiedustelulakihanketta puollettiin, sillä sotilastiedustelua käsittelevän lainsäädännön puuttuminen nähtiin merkittävänä puutteena viranomaisten toimivaltuuksissa. Toisaalta tammikuussa 2015 toimintansa aloittanut puolustusvoimien kyberosaston perustamista, jonka tehtävänä on suojata tietoverkkoja- ja palveluita sekä kehittää kyberpuolustusta, pidettiin huomattavana edistysaskeleena.[213]

Vaikka itse haastateltavat eivät sitä välttämättä tietoisesti tehneet, he osallistuivat kybertoimintaympäristön ja laajemmin myös digitalisoituvan yhteiskunnan toimirakenteiden turvallistamiseen. Heidän asiantuntijuutensa perustuva huoli kanavoitiin selvityksen kautta Suomen valtiojohdolle, joka arvioi viitekohteelle kohdistuvan uhkan todennäköisyyttä sekä vakavuutta ja siten tarpeellisia toimenpiteitä. Ratkaisuiksi havaittuun uhkaan ehdotettiin monialaisia ja -vaikutteisia toimenpiteitä. Esimerkiksi tehokkaamman yhteistyön ja viestinnän tehostamista valtiollisten toimijoiden välillä. Toisissa tapauksissa, kuten puolustusvoimien ja poliisin, viranomaisten toimivaltuuksien kasvattamista kannatetaan, mikä toisaalta eittämättä kaventaa kansalaisten yksityisyyden suojaa. Näin palaamme monesti turvallisuuspolitiikan parissa käydyn keskustelun äärelle: onko yksityisyyden kaventuminen lisääntyneen turvallisuuden väärti, ja tarkentaaksemme, on aiheellista terävöittää, keiden turvallisuudesta tällöin puhutaan. Yksityisyyteen ja tietoturvaan erikoistunut immateriaalioikeuden ja teknologiaoikeuden professori Daniel J. Solove argumentoi, että etenkin syyskuun 11. päivän terrori-iskun jälkeen länsimaisessa turvallisuusajattelussa turvallisuus otti yliotteen kansalaisten oikeudesta yksityisyyteen. Tämä on johtanut Soloven mukaan harhakuvaan, jossa ajatellaan, että nämä kaksi tekijää sulkevat toisensa pois – saadaksemme lisää turvallisuutta on meidän luovuttava yksityisyydestä.[214]

Kyberoiosaamisen- ja ymmärryksen parantamiseen keskittynyt luku oli kattava, ja nosti turvallistamisen perspektiivistä mielenkiintoisen näkökulman – huippuosaajien tarpeen lisäksi, myös tavallisten kansalaisten kyberosaamisen kasvattaminen nähtiin tärkeänä ominaisuutena.[215] Yhä verkottuneempi IoT-laitteiden yhteiskunta tekisi myös yksittäisten ihmisten kehnosta kyberosaamisesta kaikkia koskevan turvallisuusongelman.[216] Toisaalta

---

[213] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 32–33.
[214] Solove 2011, 2.
[215] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 34
[216] Hyppönen 2022, 116.

kyse on myös samalla yksilöiden turvallisuudesta. On kiistatonta, että jokaisen kansalaisen kyberosaamisen kehittäminen lisäisi myös heidän henkilökohtaista turvallisuuttaan. Samaan aikaan ihmisten kyberosaamisen kasvattaminen parantaisi myös eri toimijoiden organisatorista kyberturvallisuutta, sillä puhdas ymmärtämättömyys sen merkityksestä aiheuttaa haasteita riittävän kansallisen kybersuorituskyvyn ylläpitämiseksi, mikä esimerkiksi yksityisellä sektorilla konkretisoituu rahallisena tappiona.[217] Tämän pohjalta voidaan kyseenalaistaa nollasummapelimäinen ajattelu, jossa turvallisuus ja yksityisyys ovat toistensa vaihtoehtoja.

Lainsäädäntöä käsittelevä osuus puolestaan kuvasti hyvin sitä ongelmaa, jonka nopeasti kehittyvä teknologia liberaalille perustuslakiin pohjautuvalle yhteiskunnalle aiheuttaa. Lainsäädäntö, joka pitkälti määrittelee viitekehykset, joiden rajoissa voimme toimia, muuttuu – suhteessa teknologiseen kehitykseen – hitaasti ja kankeasti. Tämä aiheuttaa haasteita etenkin sellaisissa tilanteissa, joissa toimivaltuuksia tarvittaisiin antamaan raamit viranomaistoiminnalle, joita tarvitaan jo tai pahimmassa tapauksessa olisi tarvittu vuosia aiemmin. Tämän takia juuri tiedustelulainsäädännön olemattomuus nousi kerta toisensa jälkeen haastatteluissa esiin kriittisenä kehityskohteena. Toisaalta raportti toi esiin, että tietoturvallisuuden säätelyllä oli Suomessa puolestaan pidemmät perineet, minkä ansiosta perusasiat toimivat, mikä mahdollisti myös niiden päälle rakentamisen. Vaikka haastateltavat yleisesti kokivat, että suomalaiset viranomaiset tarvitsivat laajempia toimivaltuuksia kyberuhkien torjumiseen, haastatteluissa näkyi moraalista tasapainottelua turvallisuuden ja yksityisyyden välillä.[218]

Suomalaisen kybertoimintaympäristön senhetkistä tilaa arvioivan osion viimeinen luku käsitteli haasteita ja kehityskohteita, ja siksi sitä voidaan pitää yhtenä julkaisun tärkeimmistä anneista. Merkittävimmiksi haasteiksi nimettiin riittävä resursointi, ja näiden oikeanlainen kohdistaminen; havainnointikyvyn kehittäminen ja kehittyneiden hyökkäysten analysointikyky sekä tasapaino kansalaisten yksityisyyden, anonymiteetin ja havainnoinitkyvyn välillä. Samaan aikaan peräänkuulutettiin riittävää kansallisen kryptografian hallintaa ja digitaalisten järjestelmien kehittämistä *Security by Design*[219] -

---

[217] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 34

[218] Ibid., 35–37.

[219] Ohjelmistokehitysperiaate, jossa turvallisuuselementit sisäänrakennetaan järjestelmiin, eikä niin sanotusti liimata päälle.

ajattelun mukaisesti. Riittämätön resursointi nähtiin merkittävänä haasteena myös VTV:n selvityksessä – sen mukaan valtion talousarvion laadintaprosessissa ei ollut tunnistettavissa menettelyjä, jotka olisivat varmistaneet riittävän määrärahojen kohdistumisen kybersuojauksen toteuttamiseen. Tämän pelättiin johtavan siihen, että kyberturvallisuuden tila määräytyisi käytettävissä olevien resurssien perusteella, eikä riskienhallinnan näkökulmasta.[220]

Selvityksen neljännessä osiossa käsiteltiin Suomen kyberturvallisuuden nykytilaa yksityisellä sektorilla. Yritysten kyberturvallisuuden nähtiin olevan yleisesti hyvällä tasolla. Kriittisen infrastruktuurin yritysten tekemän yhteistyön kotimaisten viranomaisten sekä kansainvälisten toimijoiden kanssa pidettiin tärkeänä asiana varautumisen ja ennakoinnin näkökulmasta. Linjausten toteutumisen haasteina puolestaan pidettiin edistyksellisten uhkien torjumista, kuten teollisuusvakoilua ja valtiollisten toimijoiden aiheuttamien uhkien tunnistamista. Yrityskenttä oli, ja on edelleen, myös hyvin heterogeeninen ryhmä – suuryrityksillä on resursseja ja siten mahdollisuus varautua kybertoimintaympäristön uhkiin, kun taas pienemmillä yrityksillä varautumisessa voi olla suuriakin puutteita. Myös kuntataustaisten yritysten nähtiin olleen jäljessä kehityksestä. Näiden haasteiden pelättiin monistuvan, sillä moni toimiala on vahvasti ketjuttunut, minkä takia yhden yrityksen heikko kyberturvallisuus voi aiheuttaa koko alihankintaketjulle merkittäviä haasteita.[221]

Tutkimuksen pohjalta tutkimusryhmä suositteli kymmenen jatkotoimenpidettä yrityssektorille, ja niissä korostuivat strategisen johtamisen ja tilannekuvan vahvistaminen sekä kansallisen ja kansainvälisen yhteistyön tiivistäminen. Keskeisiä prioriteetteja ovat tiedustelulainsäädännön voimaansaattaminen riittävine toimivaltuuksineen, julkisen ja yksityisen sektorin kumppanuuden kehittäminen sekä kriittisen infrastruktuurin toimijoiden ohjaaminen proaktiivisempaan kyberturvallisuuden hallintaan. Erityisesti pk-yritysten osallistuminen toimialayhteistyöhön sekä systeemiajattelun vahvistaminen, jossa verkoston jokainen solmu kantaa vastuun omasta osastaan ja jatkuva tiedonvaihto muodostaa toiminnan ytimen, nousevat esiin kehittämiskohteina.

---

[220] Kybersuojauksen järjestäminen 2017, 22.
Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 46.

Selvityksen pohjalta tutkimusryhmä esitti 12 kokonaisuuden toimenpide-ehdotuksen Suomen kyberturvallisuusstrategiassa asetetun vision tavoittamiseksi. Näitä olivat:

1. Kyberturvallisuuden valtakunnallisen strategisen johtajuuden selkeyttäminen ja vahvistaminen
2. Poliittisen sitoutumisen lisääminen kyberasioiden edistämiseksi sekä tahtotilan määrittelemiseksi
3. Kansainvälisen toiminnan lisääminen ja yhteistyön tiivistäminen
4. Kattavamman tilannetietoisuuden muodostaminen niin uhkista kuin yhteistyön mahdollisuuksista
5. Elintärkeiden toimintojen turvaaminen
6. Lainsäädännön yhteensovittaminen kyberturvallisuuden vaatimusten mukaiseksi
7. Riittävien resursoinnin varmistaminen
8. Kyberturvallisuuden realisointi kilpailueduksi
9. Osaamisen ja tutkimuksen lisääminen
10. Yleisen tietoisuuden lisääminen
11. Kyberturvallisuuden semanttinen ymmärtäminen osana kansallista kokonaisturvallisuutta
12. Toimenpiteiden seuranta ja kyberturvallisuuden tilan säännönmukainen arviointi[222]

Selvityksellä nähtiin olevan niin merkittävä painoarvo, että kyberturvallisuuden koordinointia ohjaava Turvallisuuskomitea joutui päivittämään kyberturvallisuuden toimeenpano-ohjelmaa laatimalla vuodet 2017–2020 kattavan ohjelman.[223] Päivitetyn ohjelman lähtökohtana oli sitoa yhteiskunnan muut toimijat tiiviimmin osaksi kyberturvallisuuden kehittämistä, ottaa huomioon kyberturvallisuuden toimintaympäristön muutos sekä vahvistaa poliittista sitoutumista kyberturvallisuuteen. Tätä lähdettiin toimeenpanemaan uudelleenjärjestelemällä alkuperäiset 74 toimenpidettä 22 uuteen. Johtuen Turvallisuuskomitean luonteesta yhteensovittavana elimenä, sillä ei ollut vallankäytöllistä mandaattia toimeenpanna esimerkiksi poikkihallinnollisia tavoitteita, mikä heijastui uusissa toimenpiteissä.[224]

[222] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 67–75.
[223] Kybersuojauksen järjestäminen 2017, 19; Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017, passim.
[224] Kybersuojauksen järjestäminen 2017, 19; Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017, 4,

3.3 Suomen kansallista kyberturvallisuuden tahtotilaa uudelleenkalibroidaan 2020-luvulle

Vuoden 2017 arvio Suomen kyberturvallisuuden nykytilasta ja VTV:n tarkastusarvio antoivat selkeät suuntaviivat tuleville vuosille, mihin vuonna 2019 päivitetyllä kyberturvallisuusstrategialla valtioneuvosto pyrki vastaamaan. Strategian päivittämistarpeeksi mainittiin vaikuttaneen toimintaympäristön merkittävät muutokset sekä kansallisessa toiminnassa havaitut kehittämiskohteet. Vuoden 2017 selvityksessä nostetut teemat, kuten kyberturvallisuuden myönteisten mahdollisuudet, muuttuvat ja kehittyvät uhkat, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja, tunnistettiin monipuolisesti ja kattavasti. Johdannon toisen kappaleen alaviitteistä on huomattavissa, että uuden strategian laatijat olivat tutustuneet kattavasti Suomen kyberturvallisuudesta laadittuihin asiakirjoihin.[225]

Tästä huolimatta strategian johdannosta lähtien on kuitenkin aistittavissa, että samanlainen ambitiotaso ei toistu suhteessa vuoden 2013 strategiaan. Sen toinen virke on muotoiltu seuraavalla tavalla: ”Strategian tarkoituksena on myös tukea luotettavien digitaalisten palveluiden saatavuuden ja liiketoiminnan kehittämistä”. Tästä ilmaisumuodosta on tulkittavissa, että kyseisiin tavoitteisiin ei välttämättä päästä, sillä strategian kaltaisissa asiakirjoissa sanamuotoihin ja semanttisiin merkityksiin kiinnitetään paljon huomiota, ja niiden tarkoituksenmukaisuutta arvioidaan tarkasti; etenkin johdantoteksteissä. Sama pätee myös seuraavaan virkkeeseen: ” Suomen tavoite on edelleen olla kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa.”, joka osaltaan indikoi, että asetettuun tavoitteeseen ei päästy, ja toisaalta kyberturvallisuuden kirkkainta kärkeä ei enää tavoitella, vaan määrittelemätön ”kärkijoukko” riittää.[226]

Itse strategia oli vuoden 2013 laadittua strategiaa sisällöltään ja sivumäärältään merkittävästi lyhyempi. Toisaalta se itse täsmensi, että sillä oli rajapintoja aikaisempaan strategiaan, vuoden 2017 Yhteiskunnan turvallisuusstrategiaan sekä sen mainittiin olevan osa EU:n kyberturvallisuusstrategian toimeenpanoa, joka itseasiassa alkoi NIS-direktiivin myötä sanelemaan voimakkaasti jäsenvaltioidensa, sekä Suomen kyberturvallisuuden

[225] Suomen kyberturvallisuusstrategia 2019, 4.
[226] Ibid.., 4.

toimeenpanoa.[227] Ohjelma koostui kolmesta strategisesta linjauksesta: 1) kansainvälisen yhteistyön kehittämisestä; 2) kyberturvallisuuden johtamisen, suunnittelun ja varautumisen paremmasta koordinaatiosta sekä 3) kyberturvallisuuden osaamisen kehittämisestä. Jokainen näistä toimenpiteistä mainittiin vuoden 2017 kyberturvallisuuden senhetkistä tilaa arvioivassa selvityksessä.[228]

Strategian ensimmäinen luku käsitteli kansainvälisen yhteistyön kehittämistä. Sen mukaan kansainvälinen yhteistyö oli elintärkeä osa Suomen kyberturvallisuuden varmistamista niin teknisellä kuin poliittisellakin tasolla. Luvussa linjattiin, että Suomi haluaa vaalia ja säilyttää ”- - universaalin, vapaan ja vakaan internetin ja mahdollistaa sen turvallisen käytön.”, eikä halua rajoittaa sen vapautta ja avoimuutta. Suomen linjattiin korostavan kaikessa kyberturvallisuuden yhteistyössä oikeusvaltioperiaatetta, demokratiaa ja läpinäkyvyyttä.[229] Turvallisen kybertoimintaympäristön nähtiin siis edistävän yksilön perusoikeuksia ja -vapauksia. Näkökulma on varsin erilainen verrattuna vuoden 2017 puolustusselontekoon, jossa kyberturvallisuus miellettiin osaksi Suomen puolustusvoimien eri haaroja ja erottamattomaksi osaksi asevoimien suorituskykyä.[230] Linjaus on myös ristiriidassa vuoden 2017 kyberturvallisuuden tilan selvityksen asiantuntijalausuntojen kanssa, joissa kyberturvallisuuden lisääminen nähtiin, ainakin jossain määrin ja havainnointikyvyn osalta, yksityisyyden vapautta heikentävänä tekijänä.[231] Tässä Suomen valtionjohdon voidaan tulkita tekevän moraalisesti yksioikoisen – mutta käytännönläheisen – päätöksen, jossa niin sanottujen hyväntahtoisten toimijoiden, eli tässä tapauksessa viranomaisten, toimivaltaa kasvatetaan. Tämän nähdään lisäävän kansalaisten yksityisyyden suojaa, koska siten pystytään puuttumaan kybertoimintaympäristössä kansalaisiin kohdistuviin uhkiin tehokkaammin, mikä nousi myös uhkakuvaksi aikaisemmin.[232]

Linjaus oli johdonmukainen eri selvitysten kehitysehdotuksiin nähden: vuoden 2017 selvityksessä kansainvälisen yhteistyön kehittämistä suositeltiin sekä yhteistyön että

---

[227] Suomen kyberturvallisuusstrategia 2019, 4; “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”. EUR-Lex. < https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng> [luettu: 14.5.2026].
[228] Suomen kyberturvallisuusstrategia 2019, 2; Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 67–75.
[229] Suomen kyberturvallisuusstrategia 2019, 5.
[230] Valtioneuvoston puolustusselonteko 2017, 10.
[231] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 36.
[232]Ibid., 33–34.

edunvalvonnan ja vaikuttamisen näkökulmasta. Lisäksi samassa luvussa linjattiin myös havainnointi- ja attribuutiokykyjen[233] kehittämisestä sekä suvereenin kyberkyvykkyyden nostamisesta. Nämä olivat relevantteja ja tärkeitä kehityskohteita, jotka mainittiin myös vuoden 2017 selvityksessä sekä VTV:n *Kybersuojauksen järjestämisen tarkastuskertomuksessa*, mutta niiden mainitseminen kansainvälisyyttä käsittelevän luvun loppupuolella on jokseenkin kummallista.[234] Asiaa olisi perustellusti voinut käsitellä omana linjauksenaan, mutta näin jätettiin tekemättä.

Toista linjausta voidaan pitää koko strategian tärkeimpänä, sillä se pyrki vastaamaan suomalaisen kybertoimintaympäristön kriittisimpään haasteeseen: kyberturvallisuuden johtamiseen. Tämä aihe nousi molemmissa selvityksissä merkittävimmäksi puutteeksi, johon kaivattiin kipeästi muutosta, joten siihen puuttuminen oli jopa odotettavissa.[235] Strategian myötä käynnistettyä kansallista kyberturvallisuuden kehittämisohjelmaa huomioimatta, sisällölliset vastaukset kyberturvallisuuden johtajuuden haasteisiin jäivät ohuiksi. Konkreettisena toimenpiteenä edistämään kyberturvallisuuden johtamista liikenne- ja viestintäministeriöön perustettiin kyberturvallisuusjohtajan tehtävä. Hänen vastuulleen asetettiin kyberturvallisuuden kansallisen kehittämisen koordinoiminen, minkä linjattiin tapahtuvan kehitystyön, suunnittelun ja varautumistoiminnan yhteensovittamisen kautta. Tehtävän perustamisella ei kuitenkaan muutettu ministeriöiden ja toimivaltaisten viranomaisten kyberturvallisuuteen liittyviä vastuista ja toimivaltuuksia. Ministeriöiden mainittiin aiemmassa selvityksessä edistävän kyberturvallisuutta siilomaisesti omilla hallinnonaloillaan, minkä nähtiin aiheuttavan haasteita kansalliselle koordinaatiolle, johtuen toimivaltaan ja mandaattiin liittyvistä epäselvyyksistä.[236] Lisäksi tämän ohella mainittiin, että kyberturvallisuuden kehittämisohjelman laatimisessa tulisi huolehtia siitä, että sen laatimiseen osallistuvat alan teollisuuden, tutkimuslaitosten sekä julkisen sektorin kriittisistä toiminnoista ja palveluista vastaavien avainorganisaatioiden edustajat. Lisäksi itse johtamista ja yhteistyötä linjattiin kehitettäväksi operatiivisella tasolla.

---

[233] Attribuutiolla, eli syyksilukemisella, tarkoitetaan vihamielisen kyberoperaation toteuttajan tunnistamista, paikantamista ja yksilöimistä.
[234] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 33–34, 69; Suomen kyberturvallisuusstrategia 2019, 5; Kybersuojauksen järjestäminen 2017, 6–7.
[235] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 67; Kybersuojauksen järjestäminen 2017, 6.
[236] Suomen kyberturvallisuusstrategia 2019 6; Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 24–26.

Toinen tärkeä, mutta varsin lyhyesti mainittu nosto luvussa oli maininta taloudellisten voimavarojen ja yhteistoiminnan huomioiminen riittävällä tarkkuudella kullakin hallinnonalalla osana tuloksellista kyberturvallisuuden suunnittelua. Resursointi oli yksi avain haasteista siinä, miksi vuonna 2014 laadittu kyberturvallisuusstrategian toimeenpano-ohjelman tietyt tavoitteet epäonnistuivat täysin – ne olivat täysin epärealistisia suhteessa budjetoituihin resursseihin. Lisäksi riittämätön määrärahojen resurssointi kyberturvallisuuden edistämiseen oli aihe, jonka VTV nosti esiin katsauksessaan, ja josta se lausui kehittämisehdotuksen.[237] Tämän syvemmälle strategiassa ei kuitenkaan päästä, jolloin merkittävä vastuu kyberturvallisuuden edistämiseen korvamerkittävistä määrärahoista jää linjattavaksi kansallisen kyberturvallisuuden kehittämisohjelmalle.[238] Kaksi vuotta myöhemmin julkaistussa kehittämisohjelmassa toimia mainittiin edistettävän pääasiassa valtion budjettiraamien sekä olemassa olevien määrärahojen puitteissa, ja tätä tarkoitusta varten kohdistettavat määrärahalisäykset tai muut budjettivaikutuksia vaativat toimenpiteet päätettäisiin erikseen valtiontalouden kehyksissä ja vuosittaisissa talousarvioissa.[239]

Viimeinen luku vuoden 2019 strategiassa käsitteli kyberturvallisuuden osaamisen kehittämistä, mikä osaltaan esiintyi myös voimallisesti eri viranomaisten tekemissä kyberturvallisuuden puitteita arvioivissa asiakirjoissa. Strategiassa painopisteet olivat osaamistarpeen tunnistamisessa sekä koulutuksen ja tutkimuksen vahvistamisessa. Luvussa ymmärrettiin, että kansallinen kyberturvallisuus rakentuu viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, ja että jokainen näistä toimijoista vaikuttaa siihen aktiivisesti. Näin ollen todetaan, että kansallisesti olisi varmistettava, että jokaisella suomalaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä. Lisäksi tunnistettiin, että olisi varmistettava, että alan kotimaisia huippuosaajia sekä korkean tason osaajia löytyy sekä elinkeinoelämästä että julkiselta sektorilta. Tämän koettiin olevan myös tärkeää osa suomalaista TKI-toimintaa, ja siten kansallisen kilpailukyvyn kannalta merkittävää.[240]

[237] Kybersuojauksen järjestäminen 2017, 8, 15.
[238] Suomen kyberturvallisuusstrategia 2019, 6–7.
[239] Kyberturvallisuuden kehittämisohjelma 2021, 20.
[240] Suomen kyberturvallisuusstrategia 2019, 8–9.

Vaikka Suomassa arvioitiin vuosina 2016–2019 olleen varsin hyvä osaamistaso kyberturvallisuuden suhteen, useampi selvitys suositteli tuolloin osaamiseen panostamista merkittävällä tavalla kansainvälisen kyberin edelläkävijyyden saavuttamiseksi. Tämä koski myös tarvittavan osaamisen parempaa tunnistamista, mihin itse asiassa uudessa strategiassa suoraan viitattiin. Vuonna 2017 osaavan henkilöstön puute ja siitä johtuvat rekrytointivaikeudet olivat kyberturvallisuusalan keskeinen haaste. Lisäksi kritisoitiin myös sitä, että Suomessa ei ollut strategista kokoavaa näkemystä alan koulutuksen ja tutkimuksen kehittämisestä. Tätä myöskin peräänkuulutettiin vuonna 2016 julkaistussa *Kyberosaaminen Suomessa* -tutkimuksessa, jossa tarkasteltiin suomalaisen kyberosaamisen nykytilaa ja tulevaisuuden näkymiä.[241]

Kaiken kaikkiaan strategia oli lyhyt ja sisällöltään yllättävän laiha. Etenkin, jos huomioidaan sitä edeltävinä vuosina julkaistut selvitykset, tutkimukset ja toimenpide-ehdotukset liittyen kyberturvallisuuden tilaan. Vielä yllättävämpää on vuonna 2013 asetettuihin tavoitteisiin ja kunnianhimoon verrattuna matala ambitiotaso. Tämä konkretisoitui tarkastellessa alaluvun 3.2 lopussa listattuja toimenpidesuosituksia. Poliittisen sitoutumisen puute olisi saamansa kritiikin perusteella kuulunut sisällyttää strategiaa, sillä se oli yksi kritisoiduimmista puutteista Suomen kybertoimintaympäristön turvaamisessa vuosina 2013–2019. Tätä peräänkuulutettiin myös lausuntopalvelussa, jossa eri sidosryhmiltä pyydettiin lausuntoja strategiasta noin puoli vuotta ennen sen julkaisua.[242] Strategisen johtamisen siirtämisellä liikenne- ja viestintäministeriöön ei myöskään ratkaistu valtioneuvostossa vallitsevaa mandaattiin ja toimivaltaan perustuvaa ongelmaa.

Yleisesti ottaen edellisen myötä voidaan arvioida, että vuoden 2019 kyberturvallisuusstrategia oli kokonaisuutena hillitty, realistisempi ja paikoin puutteellinen päivitys vuonna 2013 aloitettuun kyberturvallisuuden strategiaohjelmaan. Merkittävimmät puutteet koskivat poliittista sitoutumista ja riittävää resursointia, mutta strategiasta oli löydettävissä muitakin puutteita. Esimerkiksi tilannetietoisuuden kehittäminen löytyi sekä vuoden 2017 kyberturvallisuuden tilaa arvioivasta tutkimuksesta, että VTV:n

[241] Suomen kyberturvallisuusstrategia 2019, 8–9; Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 70–71; Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen 2016, 2,

[242] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 68; ”Lausuntopyyntö Suomen kyberturvallisuusstrategiasta 2019”. Lausuntopalvelun verkkosivut. < https://www.lausuntopalvelu.fi/FI/Proposal/ParticipationNonJsShowReport?proposalId=56ab7d09-1859-4815-a19a-1ef624eea034> [luettu 24.4.2026].

tuloksellisuustarkastuskertomuksesta nostettuna kehityskohteena, mutta jäi käsittelemättä strategiassa riittävällä tavalla.[243] Verrattain laiha vuoden 2019 kansallinen kyberturvallisuusstrategia nosti useita kysymyksiä. Miksi ambitiotaso laski, vaikka kuusi vuotta aiemmin ja vielä vuonna 2017 Suomella oli tahtotila saavuttaa kansainvälinen edelläkävijän asema kyberturvallisuudessa? Yksi selitys oli mahdollinen vuonna 2017 tehty ensimmäisen kyberstrategian toimeenpano-ohjelman päivitys, mutta toisaalta tämä kuitenkin ulottui vain vuoteen 2020 saakka ja käsitteli pitkälti samoja sisältöjä kiinnittäen huomiota eniten strategisen johtamisen ja yhteiskunnan digitalisoitujen elintärkeiden toimintojen turvaamiseen.[244]

Turvallistamisteorian näkökulmasta voidaan argumentoida, että kyberturvallisuus oli onnistuttu jo institutionalisoimaan osaksi suomalaisen yhteiskunnan turvallisuuskäsitystä. Toisaalta tämä argumentti ontuu, sillä kyberturvallisuus ilmiönä on pysyväluonteinen ja jatkuvasti muuttuva. Lisäksi vuosina 2016–2017 maailma koki monta vakavaa ”kyberturvakriisiä”, kuten Mirain ja WannaCryn kaltaisten haittaohjelmien nouseminen uutisotsikoihin saakka. Päinvastoin kyberturvallisuuden rooli tuntui kasvavan osana kansallisesta kokonaisturvallisuudesta käytyä keskustelussa. Toisaalta oli myös mahdollista, että vuoden 2013 tavoitteet nähtiin kuuden vuoden jälkeen epärealistisina, ja strategialla pyrittiin keskittymään keskeisimpiin kyberturvallisuuden haasteisiin. Tätä puolsi esimerkiksi puolustusministeriön lausunto, jossa todetaan, että: ”strategisten linjausten toimeenpanon kannalta on hyvä, että kyberturvallisuusstrategiasta on tehty lyhyt ja ytimekäs.”[245]

Samaan aikaan tuli päätökseensä, vuoden 2014 kyberturvallisuusstrategian toimeenpano-ohjelman myötä käynnistetty, tiedustelulainsäädäntöhanke, jonka tuloksena eduskunta hyväksyi siviilitiedustelulain (709/2019) ja sotilastiedustelulain (590/2019).[246] Hanke aiheutti mittavaa yhteiskunnallista poliittista keskustelua, sillä se edellytti Suomen perustuslain 10

---

[243] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 70; Kybersuojauksen järjestäminen 2017, 7, 69.
[244] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017, 2–3.
[245] ”Lausuntopyyntö Suomen kyberturvallisuusstrategiasta 2019”. Lausuntopalvelun verkkosivut. < https://www.lausuntopalvelu.fi/FI/Proposal/ParticipationNonJsShowReport?proposalId=56ab7d09-1859-4815-a19a-1ef624eea034> [luettu 25.4.2026].
[246] “Siviilitiedustelulainsäädännön valmistelu”, Sisäministeriön verkkosivut. <https://intermin.fi/tiedustelu> [luettu: 25.4.2026]; ”Sotilastiedustelu”, Edsukunnan verkkosivut. <https://www2.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/tiedustelulait/Sivut/sotilastiedustelu.aspx>. [luettu: 25.4.2026].

§:ään muutoksia, ja hyväksyttiin merkittävällä enemmistöllä 178–13.[247] Lakien myötä Suojelupoliisin ja puolustusvoimien pääesikunnan tiedusteluosaston oli jatkossa mahdollista hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka ei ollut rikos tai tapahtui ulkomailla. Samaan aikaan se herätti kritiikkiä oikeusoppineiden keskuudessa – oikeustieteen professorit Martin Scheinin ja Juha Lavapuro jarruttivat lakien voimaantuloa, sillä he tulkitsivat niiden rikkovat suomalaisten viestintäsalaisuutta sekä muita oikeuksia, perustuslakimuutoksesta huolimatta. Tästä huolimatta, lakeja valmistelemassa olleet, puolustus- tai hallintovaliokunnat, suostuivat vain osaan professoreiden vaatimista muutoksista, ja valiokuntien kansanedustajat tuntuivat uskovan tiedusteluviranomaisia oikeusoppineiden sijaan.[248]

Kyberturvallisuusstrategia valmistui poliittisesti hankalaan aikaan. Vuonna huhtikuussa 2019 järjestettiin eduskuntavaalit, jota ennen Juha Sipilän keskusta-oikeistolainen hallitus lopulta ilmoitti erostaan toimikautensa loppumetreillä tämän valmisteleman sosiaali- ja terveydenhuollon uudistuksen kaatuessa sote-valiokunnassa.[249] Sote-uudistus myös ajoi esimerkiksi edellä mainittujen tiedustelulakien valmistelun edelle: tiedustelulakeja käsitelleiden valiokuntien työ oli lain suhteen keskeytynyt keväällä 2018, sillä niiden työ oli ruuhkautunut uudistuksen takia.[250] Lisäksi vuoden 2019 eduskuntavaaleissa muodostuneen hallituksen Antti Rinteen hallitus oli lyhytikäinen, sillä pääministeri erosi vain 188 päivän jälkeen. Täten on myös argumentoitavissa, että poliittinen tahtotila ja sitoutuminen ei ollut parhaalla mahdollisella tasolla kyberturvallisuuden edistämisen kannalta. Heikosta poliittisesta sitoutumisesta tai kiinnostuksesta kertoo myös se, että vuonna 2019 eduskunnan täysistunnoissa kyberturvallisuuteen liittyviä puheenvuoroja esiintyi vain 24 kappaletta, mikä oli vuotta 2015 lukuun ottamatta alhaisin lukema kyberturvallisuusstrategian laatimisen jälkeen.[251]

---

[247] Helsingin Sanomat, 3.10.2018. ”Eduskunta hyväksyi perustuslain muutoksen kiireellisenä äänin 178–13 – HS kokosi vastaukset viiteen kysymykseen tiedustelu-laeista”.
[248] Helsingin Sanomat, 14.2.2019 ” Mistä tiedustelulakisotkussa oikein on kysymys? Twiittaavat perustuslakiprofessorit saivat eduskunnan puhemiehen vetämään hätäjarrusta näiden huomioiden vuoksi”.
[249] “Sote kaatui ja hallitus erosi – Yle seurasi dramaattisen päivän hetki hetkeltä, tässä herkkupalat“. Yle Uutiset, 8.3.2019. < https://yle.fi/a/3-10679132>. [luettu 27.4.2026]; ” Perustuslakimuistio vaatii parempaa sote-esitystä – sote-valiokunnan jäsen: ’Veretseisauttavaa tekstiä!’”. Yle Uutiset, 5.3.2019. < https://yle.fi/a/3-10673210>.
[250] ”Tiedustelulaki jäänyt soten ja maakuntauudistuksen jalkoihin”. Kuntalehti, 9.5.2018. < https://www.kuntalehti.fi/paeaetoeksenteko/tiedustelulaki-jaeaenyt-soten-ja-maakuntauudistuksen-jalkoihin/192611>.
[251] ”Puheenvuorot 2015–2024”. Parlamenttisampi. <https://parlamenttisampo.fi/fi/speeches-2015-/faceted-search/by_year> [luettu: 15.5.2026].

4 Digitalisaatio kiihtyy koronapandemian, Ukrainan sodan ja eurooppalaisen turvallisuuden *status quon* murtuessa 2019–2024

4.1 Yhteiskuntaamme kohdistuva vahingollinen vaikuttaminen on lisääntynyt

Vuonna 2020 maailma oli muuttunut neljässä vuodessa turvallisuuspoliittisesti perustavanlaatuisella tavalla. Maailmanlaajuinen koronaviruspandemia pysäytti ja sulki maailman sekä osaltaan kiihdytti digitalisaatiota, sillä moni yhteiskunnallinen toiminto siirtyi digitaalisesti järjestettäväksi. Lähes kaikkialla maailmassa, Suomi mukaan lukien, koulutus, työnteko, harrastukset ja kaikki muut sosiaaliset toiminnot siirrettiin tieto- ja viestintäyhteyksin toteutettaviksi. Käytännössä koko yhteiskunta suljettiin tehohoidon kestävyyden varmistamiseksi, Suomi otti käyttöön valmiuslain ja lopulta päätyi sulkemaan Uudenmaan maakunnan muusta Suomesta maaliskuun lopulla.[252] Myös neljä vuotta kestänyt Donald Trumpin hallinto oli omalta osaltaan nakertanut pohjaa transatlanttisilta suhteilta. Trump esimerkiksi väläytteli puolustusliitto Naton viidennen artiklan ehdollistamista ja teki hyvin jyrkän linjanmuutoksen edeltäjänsä – Barack Obaman – hallinnon kauppapolitiikkaan ottaen merkantilistisen ”Amerikka ensin” -linjan.[253]

Tämän heijastui myös vuonna 2020 päivitetystä Suomen ulko- ja turvallisuuspoliittisessa selonteossa. Havahtuminen Euroopan strategisen autonomian olemattomuuteen, koronapandemian aiheuttama uhka valtakunnalliselle terveydenhuoltojärjestelmälle sekä digitalisaation mahdollisuuksien hyödyntäminen esiintyivät suoraan sen tiivistelmässä. Suomen ulko- ja turvallisuuspolitiikan linjattiin perustuvan ennustettavuuden ja vakauden lisäksi hyviin kahdenvälisiin suhteisiin, yhteistoimintaan ja vaikuttamiseen EU:ssa sekä sääntöpohjaiseen kansainväliseen järjestelmään. Kyberturvallisuutta kuljetettiin läpi selonteon, ja kyber-alkuiset sanat esiintyvät siinä 12 kertaa. Lisäksi digitalisaation hyödyntäminen löytyi strategiasta omana alalukunaan.[254]

Kyberturvallisuus mainittiin selonteossa ensimmäisen kerran osana globaaleja haasteita ja muutosilmiöitä määrältään lisääntyneen hybridivaikuttamisen yhteydessä. Selonteossa todettiin suoraan, että Suomen ja Euroopan turvallisuusympäristö oli ”voimakkaassa

[252] Yle Uutiset, ”Näin kaikki eteni 265 päivää sitten, kun Uusimaa laitettiin säppiin – kolme aitiopaikalla ollutta kertoo ennennäkemättömästä operaatiosta“. <https://yle.fi/a/3-11692794>. [Luettu: 27.4.2026].
[253] Dimitrova 2020.
[254] Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2020, 10, passim.

muutoksessa", johon vaikuttivat niin globaalit haasteet, kuten ilmastonmuutos ja pandemiat, mutta myös suurvaltojen muuttuneet keskinäiset suhteet. Kiina oli noussut haastamaan Yhdysvaltojen globaalia johtoasemaa. Ulko- ja turvallisuuspoliittisen toimintaympäristön muutosten nopeus ja globaali luonne tunnistettiin. Kybervaikuttaminen mainittiin selonteossa poliittisen, diplomaattisen, taloudellisen ja sotilaallisten keinojen rinnalla. Kyseinen ilmaisu löytyi merkitysarvoltaan identtisesti vuoden 2016 valtioneuvoston ulko- ja turvallisuuspoliittisesta selonteosta.[255] Tämän voi tulkita tarkoittavan sitä, että kyberturvallisuus on institutionalisoitunut osaksi Suomen ulko- ja turvallisuuspoliittisia linjauksia. Toisaalta käytännössä ulkoasultaan identtinen muotoilu on myös tulkittavissa päälle liimattuna pakollisena mainintana. Selonteon jälkimmäiset osioista selviää, että näin ei kuitenkaan asian laita ollut.

Alaluvussa *3.3 Kehityssuunnat Suomen ja Euroopan lähialueilla* Suomen ja Euroopan lähialueiden turvallisuustilanteen todettiin olevan epävakaa ja vaikeasti ennakoitava. Jännitteiden nähtiin lisääntyneen myös Suomen lähialueilla, mihin mainitaan suoraan vaikuttaneen kybertoimintaympäristön merkityksen kasvaminen. Selonteosta oli huomattavissa, että hybridi- ja kybervaikuttamista ymmärrettiin metodeina paremmin kuin aikaisemmissa selonteoissa.[256] Tämä ei toisaalta ollut yllättävää, koska viimeistään vuonna 2020 länsimaisessa tiedusteluyhteisössä vallitsi konsensus siitä, että Venäjä todella oli yrittänyt vaikuttaa Yhdysvaltojen vuoden 2016 presidentinvaaleihin, sillä Yhdysvaltain senaatin tiedustelukomitean virallinen loppuraportti arvioi Venäjän yrittäneen käyttää vuosina 2014–2017 kattavia toimenpiteitä paikallishallinto- ja osavaltiotasoilla.[257] Vuonna 2020 koko suomalainen yhteiskunta sai järkyttyä, kun valtakunnan tuhoisin ja järkyttävin tietomurto paljastui. Pyskoterapiakeskus Vastaamon potilastietokanta murrettiin, ja hyökkääjä alkoi kiristämään sekä yritystä että suoraan sen yksittäisiä potilaita lunnasmaksuilla uhaten julkaista ihmisten arkaluontoisia potilastietokertomuksia. Tilanne johti siihen, että noin 33 000 suomalaisen potilastietokertomukset vuosivat TOR-verkossa.[258]

---

[255] Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2016, 16. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2020, 12–14.
[256] Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2020, 14.
[257] Merkittävä osa tiedoista käytetyssä lähteessä on redaktoitu, joten Venäjän todellista vaikuttamisen mittakaavaa on vaikeaa arvioida.
[258] Report of the Select Committee on Intelligence, United States Senate, on Russian active measures, campaigns and interference in the 2016 U.S. election 2019, 3; Kortesoja 2022, 9–10.

Tapaus Vastaamo osoitti, kuinka vakavia seurauksia kyberturvallisuuden laiminlyönti pahimmillaan aiheuttaa niin yhteiskunnallisella kuin yksilölliselläkin tasolla. Tietomurto oli kansainväliselläkin tasolla poikkeuksellinen julmuudellaan ja häikäilemättömyydellään, sillä kohteena oli tavallisten ihmisten äärimmäisen sensitiivisiä tietoja, joiden julkitulo johti lukemattomiin henkilökohtaisiin tragedioihin. Mediassa on raportoitu, että osa tietomurron uhreista päätyivät lopulta riistämään henkensä hoitokertomuksien tultua julki, ja tapauksesta tehtiin yhteensä yli 25 000 rikosilmoitusta.[259] Sanoin kuvaamattoman tragedian lisäksi Vastaamo oli tietoturvailmiönä huolestuttava, sillä rikoksen tekijä oli yksityishenkilö, jota alan ammattilaiset kuitenkin luonnehtivat amatööriksi. Alkaessaan kiristää psykoterapiakeskusta sekä tämän asiakkaita, hyökkääjä alkoi julkaista potilastietokertomuksia pienissä ryppäissä, mutta tuli vahingossa julkaisseeksi varmuuskopion kaikista varastetuista potilastiedoista.[260] Vaikka myöhemmin kävi ilmi, että hyökkääjällä oli pitkä historia verkkorikollisuuden parissa, tapaus nosti kysymyksiä siitä, miten vakavasti salassa pidettäviä henkilötietoja tai niihin rinnastettavia aineistoja Suomessa säilytetään digitaalisesti. Jos yksityishenkilöt kykenevät tämänlaiseen vahinkoon, mihin valtiolliset toimijat, joilla on pääsy loputtomiin resursseihin, kykenevät?

Toisin kuin edeltäjässään, vuoden 2020 ulko- ja turvallisuuspoliittisessa selonteossa kyberturvallisuutta käsiteltiin kattavasti osana Suomen ulko- ja turvallisuuspolitiikkaa. Lähtien alan termistön sujuvasta käytöstä turvallisen kybertoimintaympäristön merkityksen sisäistämiseen, on selkeästi havaittavissa, että ”kyber” oli uinut valtiollisiin linjaaviin asiakirjoihin. Toisin sanoen ymmärrys aiheesta tuntuu lisääntyneet myös Suomen ulko- ja turvallisuuspolitiikasta päättävien tahojen keskuudessa, jotka kyseisen selonteon kohdalla ovat Suomen ulkoasiainhallinnon ja valtioneuvoston kanslian virkamiehiä, eduskunnan valiokuntien jäseniä sekä loppu kädessä itse valtioneuvosto.

Tästä huolimatta pisimmän korren turvallisuutta käsittelevistä selontekoista veti vuoden 2021 Valtioneuvoston selonteko, jossa kyber-alkuiset sanat esiintyvät peräti 57 kertaa. Tematiikka esiintyi pelkästään selonteon tiivistelmässä neljä kertaa. Tämä on varsin vakuuttavaa, sillä molemmat selonteot ovat sivumäärältään saman pituisia. Lisäksi kyberpuolustusta käsiteltiin

[259] Kortesoja 2022, 9–10; Ilta-Sanomat, ” Vastaamo-uhrien juristi: Ihmisiä on päätynyt itse-murhaan tieto-murron ja kiristyksen takia”. <https://www.is.fi/digitoday/art-2000010265713.html>. [luettu: 30.4.2026].
[260] Avoimien lähteiden tiedustelun erikoismies, vieraana Veli-Pekka Kivimäki, 2020, 03:00–08:58. Herrasmieshakkerit. < https://herrasmieshakkerit.fi/>. [kuunneltu 2.5.2026].

siinä osana puolustuskykyä perinteisten maa-, meri- ja ilmapuolustuksen rinnalla.[261] Toisaalta kyberturvallisuutta käsiteltiin samalla tavalla jo vuoden 2017 puolustusselonteossa. Tiivistelmässä puolustusvalmiuden vaatimusten linjattiin ulottuvan perinteisten ulottuvuuksien ohella myös kyber-, avaruus- ja informaatiotoimintaympäristöihin. Kyberpuolustuksen kehittämiseen sitouduttiin siten, että sillä voitaisiin jatkossa turvata paremmin niin puolustusvoimien omat kuin myös muiden puolustuskykyyn suoraan vaikuttavat järjestelmät. Myös digitalisaation vaikutuksen puolustuksen toimintaympäristölle mainittiin kasvavan, minkä takia puolustushallinto suuntaviivattiin kehittämään osaamistaan, innovaatio- ja ennakointikykyään sekä varmistamaan riittävät resurssit suorituskykyjen ja tutkimusyhteistyön vahvistamiseksi.[262]

Samalla tavoin kuin edellisen vuoden ulko- ja turvallisuuspoliittisesta selonteosta, myös puolustusselonteossa käytetystä kielestä ja sanavalinnoista pystyi päättelemään, että verrattuna edellisen vuosikymmeneen, Suomen puolustuksen toimintaympäristö oli epävarma. Itse selonteossa sitä kuvattiin jännitteiseksi ja vaikeasti ennakoitavaksi. Ero vuoden 2017 selontekoon on huomattava, ja se näkyy jo asiakirjan tiivistelmän toisella rivillä, jossa toimintaympäristöä kuvataan seuraavalla tavalla: ” Yhteiskuntaamme kohdistuva vahingollinen vaikuttaminen on lisääntynyt ja sen keinovalikoima on laaja.”[263] Vuonna 2017 tilannetta ei nähty yhtä akuuttina, ja Suomeen kohdistuvan voimankäytön mahdollisuuden sanottiin olevan olemassa, mutta ei aktiivinen.[264] Näitä kahta selontekoa tarkastellessa rinnakkain, on huomattavissa, että puolustusselonteoissa kybertoimintaympäristö oli huomioitu paljon laajemmin ja kattavammin.

Suomen puolustuksen toimintaympäristön kontekstissa vahingollisen vaikuttamisen, sisältäen kyberhyökkäykset, mainittiin lisääntyneen ja monimuotoistuneen osana koko alueen heikentynyttä turvallisuustilannetta. Lisäksi teknologian kehityksen ja digitalisaation ennustettiin mahdollistavan uudenlaisia vaikuttamiskeinoja, jotka voisivat pahimmillaan vaarantaa yhteiskunnan elintärkeitä toimintoja ja uhata kriittistä infrastruktuuria. Lisäksi lähialueen valtioiden mainittiin reagoineen tähän muutokseen ryhtymällä parantamaan asevoimiensa valmiutta, materialistista suorituskykyä, lisäämällä puolustusmäärärahoja sekä

---

[261] Valtioneuvoston puolustusselonteko 2021, passim, 6.
[262] Ibid., 8–9.
[263] Ibid., 8.
[264] Ibid., 10.

syventämällä puolustusyhteistyötä.[265] Käytännössä heikentynyt ja volatiilimpi turvallisuusympäristö kannustaa kutakin sen toimijaa parantamaan omaa turvallisuuttaan, mikä toisaalta, niin sanotun turvallisuusdilemman[266] takia, johtaa lopulta kiihtyneeseen asevarusteluun. Näin – toki jo valmiiksi turvallistettua – kyberturvallisuutta pyritään turvallistamaan myös puolustusministeriön hallinnonalalta, joka tosin tuntuu olevan aiheesta paremmin perillä.

Ulko- ja turvallisuuspoliittinen selonteko hahmotti muuttunutta turvallisuusympäristöä hybridivaikuttamisen näkökulmasta. Puolustusselonteossa ilmiötä lähestytään sotilaallisesta näkökulmasta, jota selonteossa kuvataan ”laaja-alaiseksi vaikuttamiseksi”. Hybridivaikuttamisen keinojen lisäksi siihen lasketaan kuuluvan avoin sotilaallinen voimankäyttö. Käytännössä vaikuttaja pyrkii suunnitelmallisesti luomaan itselleen edullisemmat olosuhteet horjuttamalla kohdevaltion puolustuskykyä esimerkiksi aiheuttamalla epävarmuutta yhteiskunnassa tai heikentämällä tämän puolustuskykyä.[267] Teknologisen kehityksen, mainiten juuri digitalisaation, tekoälyn, koneautomaation ja sensoriteknologian, nähtiin vaikuttavan suoraan puolustuksen kaikkiin toimintaympäristöihin, toki korostuen eniten kyber-, avaruus- ja informaatiopuolustuksessa. Tämän lisäksi järjestelmien kyberhäiriöiden sietokyky nostetaan kriittiseksi osaamisalueeksi, johon Puolustusvoimat näkee tarpeelliseksi jatkettavan panostaa.[268] Näin ollen on tulkittavissa, että Suomen kyberturvallisuuden, ja etenkin kyberpuolustuksen, kehittämisen yksi merkittävimpiä katalyyttejä oli muiden valtioiden luoma ulkoinen paine, joista yksilöitävissä oli selkeästi Venäjä.

Kyberulottuvuutta käsiteltiin kattavasti myös puolustuksen sen hetkistä tilaa arvioivassa luvussa. Selonteon mukaan kaksi vuotta aikaisemmin säädetty sotilastiedustelulaki toimivaltuuksineen oli parantanut tiedustelujärjestelmän kykyä muodostaa tilannekuvaa sekä antaa ennakkovaroituksia. Lisäksi kybersuorituskyvyn mainittiin olevan osa nykyaikaista laaja-alaisen vaikuttamisen keinovalikoimaa, johonka liittyvä kehitys oli ollut nopeaa. Tämän takia puolustusvoimien selostettiin kehittäneen kyvykkyyttä muodostaa kybertilannekuvaa,

---

[265] Valtioneuvoston puolustusselonteko 2017, 12.
[266] Turvallisuusdilemma tarkoittaa tilannetta, jossa valtion, oman turvallisuuden nimissä, tekemät investoinnit asevoimiinsa heikentävät sen naapurivaltioiden turvallisuutta tai sen tuntua, mikä saa nämä tekemään samoin. Tämä johtuu siitä, että asevoimien kyvykkyyksien kasvattaminen puolustustarkoituksessa käytännössä myös lisää niiden offensiivista kyvykkyyttä.
[267] Valtioneuvoston puolustusselonteko 2021, 17.
[268] Ibid., 14–16.

omien järjestelmien suojaamista sekä puolustuksellisten kyberoperaatioiden suunnittelua ja toimeenpanoa.[269]

Suomen puolustuspoliittisia perusteita määriteltäessä kyberturvallisuuden kansallinen johtajuus vaikutti selkeytyneen vuodesta 2017. Liikenne- ja viestintäministeriön katsotaan koordinoivan kansallista kyberturvallisuutta puolustusvoimien vastatessa sen sotilaallisesta kyberpuolustuksesta. Samalla puolustusjärjestelmän kybertilannekuvan parantamisen ja kyberuhkien torjumisen nähtiin edellyttävän tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä. Näitä viranomaisyhteistyön kehittämistarpeita linjattiin myös selvitettäväksi tulevaisuudessa. Kybertoimintaympäristön uhkia ja niihin liitettäviä kansallisia kehittämistoimia mainittiin arvioitavan vuoden 2019 kyberturvallisuusstrategian kehittämisohjelmassa, jonka pohjalta myös käynnistettäisiin selvitystyö. Työ jatkaisi vuonna 2017 aloitettua kyberturvallisuuden toteutumisen arviointityötä ja käynnistäisi tarvittavat kehittämistoimenpiteet kyberpuolustuksen saattamiseksi riittävälle tasolle.[270]

Kyberturvallisuutta käsiteltiin selonteossa kattavasti myös osana alalukunaan kuuluen osaksi koko puolustusjärjestelmän ylläpidon kehittämisen painopisteisiin. Siinä lyhyesti avattiin, miten sodankäynnin kenttä on moninaistunut, ja kuinka esimerkiksi digitalisaatio on syventänyt sitä. Luvun tärkein sisältö on kuitenkin Puolustusvoimien roolin selkeä määrittely kyberpuolustuksen näkökulmasta, joka on suojata Suomen puolustuskykyyn suoraan vaikuttavien järjestelmien kyberturvallisuus sekä maanpuolustukseen ja puolustusjärjestelmiin kohdistuva tietoverkkotiedustelu sekä kyberhyökkäykset. Varsinkin, jos hyökkääjän epäillään olevan valtiollinen toimija. Tämä tavoite pyritään lunastamaan nostamalla kyberhyökkäysten kynnystä, havaitsemalla uhkat ajoissa ja seuraamalla kybertoimintaympäristön muutoksia reaaliajassa.[271]

Kyberturvallisuuden voitiin arvioida olleen melko institutionalisoitunut ja sisäänrakennettu osa Suomen puolustuksen päälinjoja jo vuoden 2017 puolustusselonteon pohjalta. Vuoden 2021 versio kuitenkin osoittaa, että etenkin puolustusministeriön hallinnonalalla oli selkeästi tarve vahvemmin sisäänkirjoittaa ja tuoda kyberturvallisuutta osaksi puolustuskyvyn

[269] Valtioneuvoston puolustusselonteko 2021, 21–22.
[270] Kyberturvallisuuden kehittämisohjelma 2021, 24–25.
[271] Ibid., 32–33.

peruspilareihin. Samalla se vahvisti jatkuvilla viittauksilla kyberturvallisuuden kehittämisen tarpeisiin, että esimerkiksi vuoden 2019 kyberturvallisuusstrategia oli vaikutuksiltaan riittämätön, ja että Suomen kybertoimintaympäristön turvaaminen edellyttäisi jatkotoimenpiteitä.

Kyberin vahvaa esiintymistä selonteossa selittää myös 3.9.2019 valmistunut puolustusministeriön asettaman työryhmän valmistelema *Kyberpuolustuksen kehittämisen strategiset linjaukset*. Asiakirjassa laadittiin kyberpuolustuksen strategiset linjaukset tarpeellisen suorituskyvyn rakentamisen tueksi. Dokumentissa käsiteltiin yhteensä viittä erillistä osa-aluetta: osaamista, teknologiaa, yritystoimintaa, tutkimusta, kansainvälistä yhteistoimintaa ja kyberpuolustusta osana kansallista kyberturvallisuutta. Kyseisen linjauksen valmistumiseen vaikuttivat myös 1.6.2019 voimaan tulleet uudet tiedustelulainsäädännöt, jotka mahdollistivat kyberturvallisuuden tiedustelusuorituskykyjen kokonaisvaltaisen vahvistamisen. Linjapaperissa listattiin selkeästi, mitä asioita näillä osa-alueilla tulisi edistää ja miksi.[272]

4.2 Uutta strategiaa toimeenpannaan, mutta kuka sitä johtaa?

Vuoden 2019 kyberturvallisuusstrategiaa edistettiin vuonna 2025 laaditun VTV:n tuloksellisuustarkastuksen kertomuksen mukaan neljässä eri hankekokonaisuudessa:

- Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma vuosina (2020–2023, VM)
- Kyberturvallisuuden kehittämisohjelma (2021, LVM)
- Digitaalinen turvallisuus 2030-ohjelma (2021, HVK)
- Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla -työryhmän selvitys (2021)[273]

Strategian toimeenpano oli kuitenkin sirpaleista, eikä sen toteutumista seurattu tai arvioitu kokonaisuutena. Tämän lisäksi jopa näiden yksittäisten hankkeiden seurantaa kritisoitiin hajanaiseksi ja jopa vaillinaiseksi. Edellä mainitut hankekokonaisuudet toteutettiin joko valtiovarainministeriön tai liikenne- ja viestintäministeriön hallinnonalojen vastuulla. Kokonaisuutta vaikeutti vielä se, että vuoden 2019 kyberturvallisuusstrategian valmistelusta

[272] Kyberpuolustuksen kehittämisen strategiset linjaukset 2019, 3–5, passim.
[273] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 11–12.

vastasi puolustusministeriön yhteydessä toimiva Turvallisuuskomitea. Tämän jälkeen kuitenkin vastuu strategisesta koordinoinnista siirrettiin strategiassa tehdyn linjauksen mukaisesti liikenne- ja viestintäministeriöön perustetulle kyberturvallisuusjohtajalle ja tämän toimistolle.[274]

Valtiovarainministeriövetoinen Haukka oli toimeenpanosuunnitelma, johon koottiin 19 tehtävää, joiden avulla oli tarkoitus kehittää keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Siinä toteutettiin vuonna 2020 annetun julkisen hallinnon digitaalista turvallisuutta koskevan valtioneuvoston periaatepäätöksen asettamia linjauksia. Itse periaatepäätöksen tavoitteena oli suojata koko yhteiskuntaa digitaalisessa toimintaympäristössä kokonaisturvallisuuden viitekehyksessä. Käytännössä tätä lähdettiin toteuttamaan poikkihallinnollisen koordinaatioryhmän johdolla allokoiden hankkeelle yhteensä 3 660 000 euroa, mikä oli harvinainen konkreettinen rahallinen määre, joka kyberturvallisuuden kehittämiseen on korvamerkitty.[275]

19 toimenpidettä jaettiin yhdeksän laajemman kokonaisuuden alle, jotka määriteltiin periaatepäätöksessä:

1. Julkisen hallinnon digitaalisen turvallisuuden ja kansainvälinen yhteistoimintamalli
2. Julkisen hallinnon digitaalisen turvallisuuden riskien hallinta
3. Kunnille tarkoitetut yhteiset, digitaalista turvallisuutta edistävät palvelut
4. Digitaalisen identiteetin hallinta
5. Kansalaisten ja henkilöstön osaamisen kehittäminen
6. Julkisen hallinnon digitaalisen turvallisuuden asiantuntijapalvelut
7. Julkisen hallinnon palveluiden ja palvelutuotannon digitaalisen turvallisuuden arviointi
8. Julkisen hallinnon tarvitseman digitaalisen infrastruktuurin suojaaminen
9. Julkisen hallinnon autonomisten ja oppivien järjestelmien sekä palveluiden turvallinen kehittäminen

[274] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 4, 12–13.
[275] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) 2020, 3; Julkisen hallinnon digitaalinen turvallisuus 2020, 3, 9; Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 12.

Osa määritetyistä toimenpiteistä löytyi Suomen nykytilaa, tavoitetilaa ja tarvittavia toimenpiteitä tavoitetilan saavuttamiseksi kartoittavasta arviosta vuodelta 2017 – esimerkiksi ensimmäisen kokonaisuuden alta löytyy *1.1 Julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä* -niminen alaluku. Tämä käytännössä vastasi sisällöltään kehityskohdetta, joka löytyi jo vuoden 2017 asiakirjasta luvusta *6.2.1 Strateginen johtaminen*. Käytännön toimenpiteenä ongelman ratkaisemiseksi hankkeen myötä valtiovarainministeriö asetti digitaalisen turvallisuuden strategisen johtoryhmän, joka koostuisi suuresta osasta ministeriöitä, turvallisuuden kannalta keskeisistä virastoista sekä muun yhteiskunnan toimijoista, kuten kunnista ja korkeakouluista. Ryhmän tehtäviksi määritettiin koordinoida julkisen hallinnon digitaalisen turvallisuuden strategista riskiarvioita, luoda sille yhteiset toimintamallit ja monitoroida sen tilannetta. Lisäksi sen tehtävänä olisi valvoa Haukka-toimeenpanosuunnitelman ja kuntien digitaalisen tulevaisuuden tiekartan toteutumista.[276]

Tässä välissä on tärkeää huomata, että Haukka-toimeenpanosuunnitelmassa tarkasteltiin kyberturvallisuutta pitkälti julkisen hallinnon digitaalisen turvallisuuden kautta. Yksityisen ja kolmannen sektorin voimakkaampi kytkeminen osaksi kansallista kyberturvallisuutta jätti toivomisen varaa. Vielä tätäkin tärkeämpi kehityskohde jää mainitsematta; asiakirjassa ei lainkaan käsitellä poliittisen sitoutumisen vahvistamista, mikä oli merkittävä ongelma jo vuoden 2013 strategiassa, sen toimeenpano-ohjelmassa ja etenkin vuoden 2019 strategiassa.[277]. Toisaalta samaan hengenvetoon on todettava, että toimeenpanosuunnitelma otti järkevämmän suunnan kyberturvallisuuden kehittämiselle. Siinä keskityttiin hallittavaan ja seurattavaan kokonaisuuteen edistäen samalla konkreettisin toimenpitein kyberturvallisuutta.

Haukka vahvisti tiettyjä yhteiskunnan kyberturvallisuuden heikkoja puolia, kuten kunnallisen puolen kyberturvallisuutta omistaen sille yhden kokonaisuuden yhdeksästä kehittämisen osa-alueesta. Lisäksi siinä oli myös oma osansa, jossa arvioitiin tietoturvallisuuden ja digitaalisten palveluiden valmiuteen ja varautumiseen liittyvien säädösten päivitystarpeita. Toimeenpanosuunnitelmassa myös asetettiin käyntiin konkreettisia toimia, jotka tarjosivat

---

[276] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) 2020, 11; Julkisen hallinnon digitaalinen turvallisuus 2020, 14; Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 67.
[277] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) 2020, 8–9; Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 68.

ratkaisuja julkisen hallinnon digitaalisen infrastruktuurin suojaamiseksi, kuten yhteisen julkisen hallinnon turvallisuusarkkitehtuurin laatiminen.[278]

Haukka-hankkeen loppuraportissa arvioitiin toimeenpanosuunnitelman onnistumisia ja epäonnistumisia. Siinä Haukkaa pidettiin päällisin puolin onnistuneena, ja sen katsottiin parantaneen julkisen hallinnon digitaalista turvallisuutta. Tämän lisäksi hankkeen myötä NIS2-direktiivin kansallisen täytäntöönpanon edellytysten nähtiin parantuneen. Etenkin Haukan pitkäjänteisyyttä ja konkretiaan tähtääviä toimenpiteitä pidettiin yleisesti positiivisina, mutta VTV:n erillinen arvio peräänkuulutti toimien laajamittaista monistettavuutta ja monistamista, jotta aitoa vaikuttavuutta saataisiin materialisoitua. Tämä oli myös haaste, jonka loppuraportti tunnisti ja listasi kehitystä vaativaksi kohteeksi. [279]

Loppuraportissa myös käsiteltiin toimeenpanosuunnitelmaa laajemmin sen geopoliittisen toimintaympäristön kontekstissa, joita tahdittivat koronapandemia ja Venäjän vuonna 2022 aloittama hyökkäyssota Ukrainaan. Toimintaympäristön muutoksen myötä suunnitelmaa myös tarkasteltiin ja muokattiin paremmin vastaamaan uuden toimintaympäristön vaatimuksia. Tämän lisäksi Haukan rinnalla käynnistettiin muita hankkeita, työryhmiä ja linjavalmistelua, joissa siinä kirjattuja tavoitteita edistettiin samanaikaisesti.

Vuoden 2019 kyberturvallisuusstrategiaa oli myös tarkoitus edistää vuonna 2021 julkaistussa liikenne- ja viestintäministeriön *Kyberturvallisuuden kehittämisohjelmassa*. Ohjelman tiivistelmässä heti toisessa virkkeessä todettiin ohjelman lähestyvän kyberturvallisuutta mahdollisuuksien näkökulmasta. Suomeen haluttiin luoda kyberturvallisuuden ekosysteemi. Tämä oli hieman ristiriidassa vuoden 2017 tarkastusselvityksen tulosten pohjalta, sillä tuolloin merkittäviksi kehityskohdiksi tunnistettuja haasteita ei ollut vuoteen 2021 mennessä korjattu. Etenkin, kun heti tämän jälkeen esitettiin ohjelman ensisijaiseksi tavoitteeksi: ”- - luoda suomeen kyberturvallisuuden ekosysteemi, joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja - -”, ja vasta tämän jälkeen vahvistaa digitaalisen yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristön eri uhkilta.[280]

---

[278] Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) 2020, 26–27.
[279] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 12–13; Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) 2020, 4.
[280] Kyberturvallisuuden kehittämisohjelma 2021, 3, 10.

Tämä ekosysteemi pyrittiin luomaan neljän ydinteeman kautta: huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus ja tehokkaat kansalliset kyberkyvykkyydet.[281] Kaikki nämä teemat löytyivät myös jonkinlaisessa muodossa vuoden 2017 arviointiselvityksestä. Painopiste oli kuitenkin selkeästi siirtynyt varautumis- ja huoltovarmuusnäkökulmasta lähemmäs elinvoiman ja talouskasvun realisoimista. Samalla tavoin kuin vuoden 2013 kyberturvallisuusstrategian toimeenpano-ohjelmassa, kehittämisohjelmassa laadittiin asetetuille tavoitteille kehittämistoimenpiteitä, jotka koottiin toimeenpanosuunnitelmaan. Näitä toimenpiteitä oli yhteensä 46 kappaletta, ja ne on koottu 12 tavoitekokonaisuuden alle. Niille oli myös asetettu omat vastuutahot ja mittarit, mutta haasteeksi saattaa edelleen jäädä käytännön toteuttaminen. Vaikka yksi ohjelman neljästä päätavoitteesta oli kiinteämmän yhteistyön tekeminen, keskityttiin tässä enemmän julkisen sektorin ja elinkeinoelämän välisen yhteistyön tiivistämiseen. Haasteena olivat edelleen epäselvät toimivaltuudet, jotka VTV:n tarkastuskertomuksen mukaan ovat toisaalta parantuneet.[282]

Toisaalta ohjelma tunnisti yhteiskunnan toimintaympäristössä tapahtuneita muutoksia sekä ymmärtää, että kyberturvallisuuden tulee olla sisäänrakennettu osa suomalaista digitaalista yhteiskuntaa. Ohjelman kehittämisjänne on pitkä – se käsittää vuodet 2021–2030 ja ulottuu jopa tutkimusajankohdan jälkeiselle ajanjaksolle. Korvamerkittyjä määrärahoja ohjelman toimeenpanolle vuosiksi 2022–2025 esitettiin 5,9 miljoonaa euroa, mikä on parannus aikaisempiin ohjelmiin.[283]

On huomionarvoista, että ohjelmassa myös eriteltiin, mitkä asiakirjat sen laadinnassa on otettu huomioon. Sen laatimisessa on hyödynnetty pitkälti kaikki merkittäviä julkisen hallinnon kyberturvallisuutta käsitteleviä julkaisuja, kuten *Kyberturvallisuusstrategia 2019*, *yhteiskunnan turvallisuusstrategia 2017* ja *Puolustusselonteko 2017*, mutta siinä ei tarkasteltu vuoden 2017 kyberturvallisuuden arviointiselvitystä.[284] On argumentoitavissa, että neljän vuoden takaisia selvityksiä ei haluttu hyödyntää tässä toimeenpano-ohjelmassa, mutta toisaalta näihin puutteisiin ei ollut löydetty ratkaisua. Ohjelman päivitettyä vuoteen 2020 ulottuvaa toimeenpano-ohjelmaa ei myöskään huomioitu. Näin ollen kyberturvallisuuden

[281] Kyberturvallisuuden kehittämisohjelma 2021, passim, 10.
[282] Kyberturvallisuuden kehittämisohjelma 2021, 13–15, Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 21–22.
[283] Kyberturvallisuuden kehittämisohjelma 2021, 7–10.
[284] Ibid., 42–43.

kehittämisestä tuntuu uupuvan pitkäjänteisyys. Verratessa tätä eduskunnan täysistuntojen kyber-aiheisiin puheenvuoroihin, jotka vuosina 2019–2022 määrällisesti lähes kymmenkertaistuivat, on tulkittavissa, että vasta vuoden 2020 Vastaamon tietomurto sai päättäjät – olosuhteiden sanelemien ehtojen edessä – todella heräämään ja sitoutumaan suomalaisen kyberturvallisuuden edistämiseen.

Tästä konkreettisin esimerkki oli vuoden vaiheessa 2020–2021 laadittu työryhmän selvitys *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (TITUKRI)*. Se tehtiin suorana vastauksena tietomurtoon, mikä puhuu laajemmin organisaatioiden reaktiivisuudesta kyberturvallisuuden parissa toimiessa proaktiivisuuden sijaan. TITUKRIn johdannossa todetaan, että Suomessa edelleen oli tietojärjestelmiä, joiden tietoturvan, -suojan ja valvonnan taso ei ollut riittävällä tasolla peilaten EU:n tietosuojalainsäädäntöön ja toimialojen omiin erityislainsäädäntöihin. Kaiken lisäksi, kuten Vastaamon tietomurto osoitti, osa näistä riittävällä tavalla suojaamattomista järjestelmistä löytyi edelleen yhteiskunnan toiminnan kannalta kriittisiltä toimialoilta. Työryhmän selvityksessä asetettiin 37 tavoitetta, joilla pyrittiin varmistamaan suomalaisen yhteiskunnan kriittisten palveluiden, kuten sähkön ja juomaveden jakelu sekä terveydenhuollon palvelut, tietoturvallisuus ja -suojaus.[285]

Edellä mainituilla 37 tavoitteella, jotka perustuivat myös liikenne- ja viestintäministeriön johtaman poikkihallinnollisen työryhmän selvitykseen *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla*, oli tarkoitus täyttää yhteensä kahdeksan vaatimusta riittävän tietoturvan ja suoja saavuttamiseksi. Näiden mukaan oli varmistettava, että:

1. Lainsäädännössä on riittävät tietoturva- ja tietosuojavaatimukset ja -velvoitteet, joita toimialoilla noudatetaan, sekä säännökset antaa tarkempia määräyksiä tietoturvan ja tietosuojan toteuttamisesta.
2. Toimijoilla on riittävä tietämys ja osaaminen velvoitteiden noudattamisessa.
3. Viranomaisilla on riittävät toimivaltuudet valvoa tietoturvan ja tietosuojan toteutumista ja tehdä sektorirajat ylittävää yhteistyötä.
4. Viranomaisilla on riittävä osaaminen ja uskallus käyttää niille lainsäädännössä annettua toimivaltaa ja ohjata toimialaansa.

---

[285] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (TITUKRI), 2–13.

5. Viranomaisilla on riittävät tosiasialliset aineelliset ja henkilöresurssit käyttää toimivaltaansa.
6. Jokainen toimija kantaa itse vastuun oman toimintansa tietoturvasta ja tietosuojasta.
7. Pidetään yllä yhteistä tietoturvaa ja tietosuojaa koskevan toimintaympäristön tilannekuvaa ml. säännöllisellä koordinaatiolla, tiedonvaihdolla ja tilannekatsauksilla.
8. Käynnistetään toimet kansalaisten digiturvaosaamisen vahvistamiseksi eri toimijoiden laajana yhteistyönä.

Jälleen kerran on havaittavissa, että toimenpiteet eivät ole sisällöiltään uusia – päinvastoin. Tarkoituksenmukainen ja ajantasainen lainsäädäntö, riittävä osaaminen, resurssit ja selkeät toimivaltuudet ovat esiintyneet suomalaisen kybertoimintaympäristön arviointien kehityskohteina käytännössä jatkuvasti.[286]

2020-luvun alku oli Suomessa sekä koko maailmassa poikkeuksellinen. Koronavirus-pandemia, joka suurilta osin sulki käytännössä yhteiskuntien normaalin toiminnan pakottaen suurimman osan organisaatioista etätyöskentelyyn, -opiskeluun tai -asiointiin. Suomen valtionhallinnolla, muiden ohella, oli täysi työ tilanteen hallinnan säilyttämiseksi, sillä esimerkiksi tehohoitopaikkojen määrän riittävyys oli aito huolenaihe. Tapaus-Vastaamo toisaalta pakotti viranomaiset havahtumaan kansallisen kyberturvallisuuden riittämättömyyteen, mutta pandemia ei hellittänyt seuraavanakaan vuonna, vaan Suomessa sen eri aallot koettelivat terveydenhuollon kantokykyä alkukevääseen 2022 saakka. Näin vastuu kyberturvallisuuden kehittämisestä tuntuu jääneen virkamieskunnalle, jotka edistävät sitä resurssien ja osaamisen puitteissa. Tämän myötä ei ole yllättävää, että vuonna 2024 Helsingin kaupunki ja vuonna 2026 koko valtioneuvosto joutuivat vakavien tietomurtojen kohteiksi.[287]

---

[286] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (TITUKRI), 13–14.

[287] “P2024-01 Helsingin kaupungin tietomurto 2024". Onnettomuustutkintakeskuksen verkkosivut. < https://turvallisuustutkinta.fi/fi/index/tutkintaselostukset/poikkeuksellisettapahtumat/p2024-01helsinginkaupungintietomurto2024.html>. [luettu: 15.5.2026.]; ”Valtorin mobiilihallinnan tietomurto koskettaa valtioneuvostoa”. Valtioneuvoston verkkosivut. < https://valtioneuvosto.fi/-/valtorin-mobiilihallinnan-tietomurto-koskettaa-valtioneuvostoa>. [luettu 15.5.2026].

4.3 Venäjän ja lännen vastakkainasettelu näkyy Suomen lähialueilla erityisesti laaja-alaisena vaikuttamisena - -

Suomen ulko- ja turvallisuuspoliittinen selonteko vuodelta 2024 kuvasti konkreettisesti omaa aikaansa, joka oli jyrkkä, mutta jossain määrin ennustettavissa ollut eskalaatio Itämeren turvallisuusympäristössä. Venäjä aloitti hyökkäyssodan Ukrainaan 24.2.2022, ja tämä pakotti Suomen ja Ruotsin hylkäämään sotilaallisen puolueettomuuden nojaavan puolustuspolitiikkansa ja hakemaan Nato-jäsenyyttä. Varsin mutkikkaan prosessin jälkeen, jossa erinäiset Naton jäsenmaat jarruttivat Suomen ja Ruotsin jäsenyyksiä, Suomesta tuli Nato-maa 4.4.2023 lähes vuoden kestäneen hakuprosessin jälkeen.[288] Lisäksi lähenevät Yhdysvaltojen presidentinvaalit kiristivät tunnelmaa, sillä aikaisemmalla kaudellaan 2016–2020 transatlanttisia suhteita heikentänyt Donald Trump oli jälleen nousemassa vallan kahvaan.[289]

Tämä tarkoitti merkittävää muutosta, joka näkyi selonteon tiivistelmän ensimmäisessä virkkeessä, jossa todettiin Suomen ulko- ja turvallisuuspolitiikan pohjautuvan arvopohjaiseen realismiin. Arvopohjainen realismi oli Suomen vastavalitun tasavallan presidentin – Alexander Stubbin – lanseeraama käsite, jolla hän tarkoittaa Suomen pyrkivän edistämään arvojensa mukaisia ideoita, kuten vapautta, demokratiaa, ihmisoikeuksia ja perusoikeuksia, mutta pystyä käymään dialogia myös valtioiden ja toimijoiden kanssa, jotka eivät tätä näkemystä jaa.[290] Aistittavissa oli eräänlainen doktriininmuutos; Suomea uhkasivat nyt, vuoteen 2020 verrattuna, akuutimmat, eksistentiaalisemmat ja monilla tavoin konkreettisemmat uhkat. Heti Ukrainan hyökkäyssodan alettua sen hetkinen Suomen tasavallan presidentti Sauli Niinistö lausui: ”Nyt naamiot on riisuttu, vain sodan kylmät kasvot näkyvät”.[291] Venäjä oli osoittanut, että se tahtoessaan hyökkäisi naapurivaltionsa kimppuun, eikä kyseessä ollut enää hypoteettinen tilanne.

Kyberturvallisuus nousi, hieman itsestäänselvästikin, selonteossa merkittävämpään asemaan johtuen muuttuneesta ulko- ja turvallisuuspolitiikan toimintaympäristöstä. Venäjä oli, ja on

---

[288] ”Suomen Nato-jäsenyys”. Ulkoministeriön verkkosivut. <https://um.fi/suomen-nato-jasenyys>. [luettu: 8.5.2026].
[289] Nielsen & Dimitrova 2021, 1.
[290] Suomen ulko- ja turvallisuuspoliittinen selonteko 2024, 3;” Tätä tarkoittaa Stubbin ’arvopohjainen realismi’”. *Yle Uutiset*, 14.6.2024. < https://yle.fi/a/74-20093832/64-3-235009>. [luettu: 8.5.2026].
[291] ” Presidentti Sauli Niinistö: ’Nyt naamiot on riisuttu, vain sodan kylmät kasvot näkyvät’ – näin Suomen johto tuomitsi Venäjän hyökkäyksen”. *Yle Uutiset*, 24.2.2022. < https://yle.fi/a/3-12331829>. [luettu: 8.5.2026.]

tänäkin päivänä, johtava hybridi- ja kybervaikuttamisen roistovaltio. Kuten tämän tutkielman aikana on osoitettu, sillä on ollut läpi 2010–2020-luvun merkittäviä kyberkyvykkyyksiä, joita se on käyttänyt laaja-alaiseen vaikuttamiseen osana oman edun ajamista yrittäen esimerkiksi vaikuttaa Yhdysvaltojen vaalituloksiin tai käyttäen niitä suoraan osana sodankäyntiä Ukrainassa.[292] Mahdollisesti tästä johtuen, kyber-alkuiset sanat esiintyvät selonteossa 22 kertaa, joka tarkoittaa lähes kaksinkertaista esiintymistiheyttä verrattuna vuoden 2020 selontekoon.[293]

Kun vuonna 2020 puhuttiin kyberturvallisuuden merkityksen kasvamisesta, vuonna 2024 sen nähtiin olevan vakiintunut vihamielisten valtioiden voimankäytön väline, jolta tulisi suojautua. Vuonna 2020 todettiin vapaan, avoimen ja turvallisen kybertoimintaympäristön varmistamisen olevan tärkeää, neljä vuotta myöhemmin puheen sävy oli muuttunut asteen vakavammaksi. Turvaton kybertoimintaympäristö tarkoitti valtiollisen suvereniteetin menettämistä, minkä lisäksi arvopohjaisen realismin edistämisen keinovalikoimaan oli ilmestynyt liuta kyber-alkuisia sanoja, kuten kyberdiplomatia, -puolustus, -rikostorjunta ja -politiikka. [294] Lisäksi otettiin myös rohkeampi loikka sanoittaessa omaa toimijuutta kansainvälisessä kybertoimintaympäristössä; Suomen linjattiin vahvistavan kykyään varautua ja vastata vihamieliseen kybertoimintaan kyberdiplomatian sekä -politiikan kautta. Viranomaisten rinnalle nostettiin myös muun yhteiskunnan toimijoiden merkitys osana kansallista kybervarautumista ja -resilienssiä.[295]

Näin kyberturvallisuus terminä turvallistettiin myös ulko- ja turvallisuuspoliittiseen selontekoon tämän suuntautuessa yhä enemmän puolustusselonteon kanssa yhteneväisemmäksi. Toisaalta Niinistön sanojen mukaisesti ”naamareiden putoamaisen” myötä myös Suomi pystyi virallisissa linjaavissa asiakirjoissaan sanoittamaan konkreettisemmin sitä eksistentiaalista uhkaa, joka ei itsessään ollut kybertoimintaympäristön turvattomuus, vaan tämän kautta syntyvä hyökkäysvektori suoraan suomalaisten jokapäiväiseen elämään. Suomalaisille perinteisen vihollisen keinovalikoiman

[292] *King's College London.* Lukasz Olejnik's story, 24.5.2025. "Russian cyber and information warfare and its impact on the EU and UK". < https://www.kcl.ac.uk/russian-cyber-and-information-warfare-and-its-impact-on-the-eu-and-uk>. [luettu: 8.5.2026].
[293] Suomen ulko- ja turvallisuuspoliittinen selonteko 2024, passim; Suomen ulko- ja turvallisuuspoliittinen selonteko 2020, passim.
[294] Suomen ulko- ja turvallisuuspoliittinen selonteko 2024, 18,20, 26; Suomen ulko- ja turvallisuuspoliittinen selonteko 2020, 14, 17–18, 33, 37.
[295] Suomen ulko- ja turvallisuuspoliittinen selonteko 2024, 27.

uusimman ”lelun” torjuminen ei tässä vaiheessa enää vaatinut ylimääräistä vakuuttelua. Saman tuloksen huomasi suomalaisten Nato-kannassa, sillä vielä tammikuussa 2022 vain 30 prosenttia suomalaisista kannatti liittymistä, kun luku oli kasvanut maaliskuussa 53 prosenttiin.[296]

Päivitetty puolustusselonteko vuodelta 2024 oli kolme vuotta aikaisemmin julkaistuun versioon nähden pituudeltaan lähes kaksinkertainen. Tähän todennäköisesti vaikutti yleinen turvallisuusympäristön muutos sekä Suomen Nato-jäsenyys, joka edellytti reippaan määrän uusia linjauksia. Tästä huolimatta kyber-alkuisia sanoja esiintyi selonteossa peräti 95 kertaa, eikä aihe jäänyt Venäjän, Ukrainan sodan tai muiden ”akuutimpien” aiheiden alle piiloon. Samalla tavoin kuin vuoden 2021 strategiassa kybertoimintaympäristö liitetään osaksi maa-, meri-, ilma- ja avaruuspuolustuksen toimintaympäristöä, joiden nähdään yhä enemmän kytkeytyvän toisiinsa. Etenkin Ukrainan sota on osoittanut, että nämä viisi toimintaympäristöä ovat nykysodankäynnissä erottamattomia toisistaan. Maavoimia tarvitaan edelleen maa-alueiden hallintaan, mutta niitä vastaan hyökkääminen tai puolustaminen on osoittautunut äärimmäisen tehokkaaksi drooni-teknologialla, joka puolestaan perustuu kyber- ja avaruuskyvykkyyteen.[297]

Suomen puolustuksen toimintaympäristöä luonnehdittiin uudessa selonteossa epävakaaksi ja vaikeasti ennakoitavaksi. Venäjän ja lännen välisen konfliktin nähtiin kiristyneen, mikä edellytti Suomea kehittämään kyvykkyyttä sietää ja vastustaa vihamielistä vaikuttamista. Tämän vaikuttamisen nähtiin tulevan ennen kaikkea Kremlinistä, vaikka myös Kiinan tunnistettiin harjoittavan samalaista monialaista etujen ajamista.[298] Kyberpuolustusta käsittelevä luku oli myös kattavampi ja samalla pudotti pois informaatio- ja avaruuspuolustuksen käsittelyn, jotka sisällytettiin kolme vuotta aiemmin esiintyneessä selonteossa kyberpuolustuksen kanssa samaan osuuteen. Lisäksi linja kyberturvallisuuden roolin suhteen oli hyvin samanlainen kuin ulko- ja turvallisuuspoliittisessa selonteossa, jossa turvallinen kybertoimintaympäristö tarkoitti kansallista suvereniteettia.[299]

---

[296] ”Suomalaisten Nato-kanta kääntyi jyrkästi – muutos lienee pysyvä ja pakottaa päättäjät ulos kuorestaan, tutkijat uskovat”. Yle Uutiset, 1.3.2022. < https://yle.fi/a/3-12337319>. [luettu: 8.5.2026].
[297] ” Asiantuntijalta jäitä hattuun Venäjän ’Starlink-katastrofissa’”. Ilta-Sanomat, 26.2.2026. <https://www.is.fi/ulkomaat/art-2000011841279.html>. [luettu:8.5.2026]; Heider 2024, 409–410.
[298] Suomen puolustusselonteko 2024, 8–13.
[299] Ibid., 6–7, 10.

Samalla tavoin kuin jo vuoden 2021 puolustusselonteossa, vuoden 2024 päivityksessä painopiste oli juuri valtiollisten toimijoiden vihamielisen vaikuttamisen ja vahingonteon torjuminen. Vaikkei asiaa suoraan todettukaan, on selvää, että uskottavaa ja kyvykästä puolustusta ylläpidettiin johtuen Suomen geopoliittisesta sijainnista Venäjän rajanaapurina. Tämä on etenkin selvää, jos Suomen länsinaapureiden puolustuspolitiikkaa on seurannut kylmän sodan jälkeisellä ajalla. Toisaalta myös Yhteiskunnan turvallisuusstrategioista ja puolustusselonteoista 2010-luvun alkupuolelta on aistittavissa valtionjohdon usko siihen, että myös Moskovassa oltaisiin, ainakin jossain määrin, osallistuttu yhteiseen kansainväliseen sääntöpohjaiseen järjestykseen.

Vuoden 2024 selonteossa linjattiin, että Puolustusvoimien on kyettävä käynnistämään puolustuksen edellyttämät kyberoperaatiot ja muut tarvittavat vastatoimet ennakoivasti. Tätä linjausta täydennettiin vielä vaatimalla, että Puolustusvoimien toimintaa on kyettävä kybervaikuttamisella tukemaan kaikissa tilanteissa.[300] Tätä linjausta tarkasteltaessa on ymmärrettävä, että Puolustusvoimissa, kuten monien muidenkin maiden asevoimissa, Ukrainan sotaa on seurattu todella likeltä, sillä se antaa osviittaa siitä, miltä moderni totaalinen sodankäynti tulee todennäköisesti näyttämään. Venäjä on iskenyt sodan aikana raskaasti Ukrainan siviiliväestöä vastaan pyrkien murtamaan tämän kansakunnan resilienssin. Osana tätä se on käyttänyt perinteistä kineettistä voimaa, mutta myös voimakkaita kyberfyysisiä vaikuttamiskeinoja hyökäten usein talviaikaan Ukrainan energiainfrastruktuuria vastaan yrittäen tehdä Ilkka Remeksen fiktionaalisesta jännitysromaanista[301] realismia. Ukrainalaiset ovat kuitenkin onnistuneet vastustamaan näitä hyökkäyksiä.[302] Suomen osalta linjaus kuulostaa siltä, että pahimpaan, eli samankaltaiseen tilanteeseen, oltaisiin varautumassa kuin, mitä Ukrainan siviiliväestö on joutunut kestämään. Tämän puolesta puhuu myös seuraava kappale, jossa kyberuhkien havaitseminen ja muutosten seuraaminen reaaliaikaisesti katsottiin edellyttävän asevelvollisten ja vapaaehtoisten henkilöiden käytettävyyttä kyberpuolustuksen tehtävissä.[303]

Molemmissa vuoden 2024 selonteoissa puhuttiin valtiollisesta suvereniteetista kybertoimintaympäristössä. Puolustusselonteossa linjattiin, että se on määriteltävä ja kyettävä

[300] Suomen puolustusselonteko 2024., 69–70.
[301] Ilkka Remeksen *Jäätyvä helvetin* miljöö sijoittuu kuvitteelliseen Suomeen, jonka sähköverkko lamaantuu kesken ankaria talvipakkasia.
[302] Humphreys 2024, 1; Aebi, et al. 2024, 17.
[303] Puolustusselonteko 2024, 70.

turvaamaan. Tämän tulkittiin edellyttävään asiaan kuuluvan säädöspohjan kehittämistä. Tällä pyritään kehittää viranomaisten kykyä tukea toisiaan sekä avustaa muita yhteiskunnan kriittisen infrastruktuurin parissa toimivia tahoja varautumaan ja palautumaan mahdollisista kriiseistä. Lisäksi uutena aiheena nostettiin kyberpuolustusdoktriinin laatiminen, jossa kuvattaisiin, miten Suomi vastaisi vihamielisen valtion kybervaikuttamiseen strategisella tasolla. Doktriini ei ole vielä valmistunut, mutta sen linjattiin valmistuvan Petteri Orpon hallituskauden aikana.[304]

Selonteossa argumentoidaan, että käytännössä muuttunut turvallisuusympäristö vaatii lainsäädännön kehittämistä ja muuttamista riittävän kyberpuolustuksen mahdollistamiseksi. Muutoksia haluttiin Puolustusvoimien juridiseen toimivaltaan, tiiviimmän viranomaistyön lisäämiseen sekä itsenäisempään Puolustusvoimien operatiiviseen kybermandaattiin. Käytännössä tämä tarkoittaa todennäköisesti muutoksia 2019 säädettyihin tiedustelulakeihin. Lisäksi muutoksia kaavailtiin asevelvollisuuteen, Nato-yhteensopivuuteen sekä valmiuslakiin.[305] On myös muistettava, että puolustusselonteossa näkökulmana on kansallinen ja sotilaallinen kyberpuolustus eikä kyberturvallisuus. Näiden ero on se, että kyberpuolustuksesta puhuttaessa tarkoitetaan yhteiskunnan kybertoimintaympäristön toimintojen puolustamista, jotka ylläpitävät Suomen puolustuskykyä. Se myös vastaa ensisijaisesti valtiollisten kyberuhkien torjumisesta.[306]

4.4 Uusi kyberturvallisuusstrategia vastaa muuttuneen turvallisuusympäristön vaatimuksiin

Kolmannen ja viimeisimmän 10.10.2024 julkaistun kyberturvallisuusstrategian taustalla oli tarve uudistaa strategiaa sellaiseksi, että se vastaisi muuttuneen toimintaympäristön haasteisiin. Strategia huomioi myös EU:n NIS-2 kyberturvallisuusdirektiivin kautta jäsenvaltioilleen asettamat vaatimukset, ja otti uuden tulokulman kyberturvallisuusstrategioihin ulottamalla sen tavoitetilan vuoteen 2035. Strategian keskiössä oli kokonaisturvallisuuden ja voimakkaasti digitalisoituvan suomalaisen yhteiskunnan sovittaminen muuttuneeseen geopolitiikan tilaan. Siinä asetettiin kyberturvallisuudelle tavoitetila, kuvattiin yleisesti muuttunutta toimintaympäristöä, läpikäytiin kyberturvallisuuden

[304] Puolustusminiteriö 2024, 2, Puolustusselonteko 2024, 70–71.
[305] Puolustusselonteko 2024, 98.
[306] Ibid 2024, 69–70, 111, 113.

sen hetkinen tilanne, esitettiin kyberturvallisuuden edistämisen kärjet ja linjattiin näiden toimeenpano.[307]

Vuoden 2019 strategiassa tällaista rakennetta ei ollut. Siihen kuului vain johdanto ja kolme strategista linjausta. Strategiaa itsessään toteutettiin käytännön tasolla kyberturvallisuuden kehittämisohjelmalla, mutta siinäkään ei rakenteellisesti määritelty kansallisen kyberturvallisuuden tahtotilaa tai analysoitu toimintaympäristön muutosta. Toisaalta vuoden 2013 strategian toimeenpano-ohjelma oli rakenteeltaan hyvin samanlainen ja lähes yhtä kattava. Sen merkittävin ongelma oli kuitenkin epärealistinen tavoitteenasettelu tarkasteltaessa esimerkiksi eri hallinonalojen välisiä toimivaltuuksia.[308]

Strategiaa kuvailtiin esipuheessaan ”rohkeaksi ja kunnianhimoiseksi”. Toisaalta tämän kanssa on epäsuhdassa virke, joka esiintyi pian sen jälkeen, jossa todettiin suurimman osan sen hetkisestä kyberturvallisuuden sääntelystä ja politiikkatoimista tulevan EU:sta. Asetettaessa strategia rinnakkain vuoden 2019 varsin kunnianhimottoman päivityskerran kanssa toteamus pitää kyllä paikkansa. Strategian myötä Suomen kyberpolitiikkaa lähdettiin muuttamaan merkittävästi: vastedes se tulisi perustumaan kyberpuolustusdoktriiniin, ja uhkiin ryhdyttäisiin varautumaan proaktiivisesti turvautuen tarvittaessa myös attribuutioon ja vastatoimiin. Merkittävää on myös se, että johdannossa tunnistetaan sama haaste, joka on ollut myös osa tämän tutkielman hypoteesia – yhteiskunnallinen keskustelu ja ymmärrys kyberturvallisuudesta on rajautunut perinteisesti tekniseen näkökulmaan, eikä sitä ole osattu ymmärtää osana valtion kokonaisturvallisuutta. Strategian lähtökohdissa kuitenkin painotetaan sitä, että siinä käsitellään nimenomaan kansallista kyberturvallisuutta, jolla tarkoitetaan:

> *” - - niitä toimia joiden seurauksena digitaalinen yhteiskunta kykenee varautumaan, tunnistamaan, torjumaan ja kestämään sähköisten ja verkotettujen järjestelmien häiriöitä ja niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin, toipumaan niistä sekä varmistamaan kansallisen turvallisuuden, maanpuolustuksen ja huoltovarmuuden toimintaedellytykset.*”[309]

[307] Suomen kyberturvallisuusstrategia 2024, 3, 6.
[308] Suomen kyberturvallisuusstrategia 2019, 3; Kyberturvallisuuden kehittämisohjelma 2021, 3; Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 1.
[309] Suomen kyberturvallisuusstrategia 2024, 6–10.

Suomen kansallisen kyberturvallisuuden tavoitetila määritettiin rakentuvan neljän pilarin päälle, ja nämä olivat: 1. Osaaminen, teknologia ja TKI-toiminta; 2. Varautuminen; 3. Yhteistoiminta; sekä 4. Reagointi ja vastatoimet. Tässä tavoitetilassa kyberturvallisuus olisi sisäänrakennettu osa kokonaisturvallisuutta, ja jossa digitalisoitunut yhteiskunta on toimintavarma ja luotettava. Teknologisia mahdollisuuksia hyödynnettäisiin kilpailuedun saamiseksi unohtamatta kybertoimintaympäristön uhkia. Kyky havaita, tunnistaa, torjua ja kestää kyberhäiriötilanteita, sekä toipua niistä päämäärätietoisesti, olisi ratkaisevaa. Suomi edistäisi kyberturvallisuuttaan aktiivisesti ja määrätietoisesti tiiviin kansallisen ja kansainvälisen yhteistoiminnan sekä tiedonvaihdon kautta. Lopuksi tämä kaikki sidottaisiin yhteen varmistamalla riittävät resurssit ja niiden tehokas käyttö. [310]

Toimintaympäristöä arvioivassa luvussa tunnistettiin samat muutosvoimat, joiden on myös tässä tutkielmassa arvioitu vaikuttaneen kyberturvallisuuden kehitykseen. Toimintaympäristön tulkittiin myös muuttuneen merkittävästi vuodesta 2019, jolloin viimeksi kyberturvallisuusstrategiaa päivitettiin. Toimintaympäristössä tunnistettiin kahdeksan eri trendiä. Niistä merkittävimmät olivat yleisluontoisempi niin sanottujen monikriisien[311] aikakauden tunnistaminen; Suomeen kohdistuvan vihamielisen kybertoiminnan lisääntyminen; teknologisen murroksen aiheuttama kyberturvallisuuden vastuun siirtyminen kaikille; ja kansallisen yhteistoimintamallin kehittäminen.[312]

Nykytilan arviossa Suomen kansallisen kybertoimintaympäristö saa hyvän arvosanan. Yhteiskunnan digitalisaation katsottiin olleen kansainvälisillä standardeilla pitkällä. Suomalaisten tekninen osaaminen ja ymmärrys kyberturvallisuudesta oli jopa kiitettävällä tasolla. Parhaimmat pisteet sai kansainväliselläkin mittarilla vahva yksityisen ja julkisen sektorin välinen yhteistyö.[313] Suomen kansallisen kyberturvallisuuden tavoitteiden taso oli vuosien varrella muuttunut realistisemmaksi suhteessa sen todelliseen kyvykkyyteen, resursseihin ja poliittiseen sitoutumiseen. Vuonna 2013 asetetut tavoitteet toteutuivat jokseenkin, sillä Suomi oli toistaiseksi onnistunut suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkia vastaan. Lisäksi kansalaisilla, viranomaisilla ja yrityksillä oli ollut

[310] Suomen puolustusselonteko, 12.
[311] Englanniksi *Polycrisis*, jolla tarkoitetaan rinnakkain esiintyvien kriisien kasautumisen kautta syntyvää epävakauttava, joka on yhteisvaikutkseltaan suurempi kuin kuin niiden osien summa.
[312] Suomen kyberturvallisuusstrategia 2024, 13–16.
[313] Ibid 2024, 17.

mahdollisuus hyödyntää turvallista kybertoimintaympäristöä, joitain poikkeuksia lukuunottamatta, kansallisesti että kansainvälisesti. Suomi ei kuitenkaan ollut vuonna 2016 saati 2024 maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.[314] On selvää, että Suomi jää Yhdysvaltojen, Iso-Britannian, Venäjän ja Kiinan kaltaisista suurvalloista, sillä niillä on käytössä täysin eri luokan kapasiteetti tutkia, kehittää ja innovoida alan uran uurtavaa teknologiaa.

Nykyajasta hieman anakronistisesti tarkastellen on mielenkiintoista katsoa näitä tavoitteita, sillä parin viime vuoden aikana tässä keskustelussa on tapahtunut hyvin jyrkkä muutos. Valovuosien kehitys tekoälyn ja mikrosirujen saralla on muuttanut pelikenttää merkittävästi. Tähän TKI-kehitykseen pystyy vain kourallinen jättiluokan IT-taloja. Lisäksi Suomen koko julkinen sektori sekä merkittävä osa yksityistä sektoria on "hirttäytynyt" Microsoftin palveluihin, joka on yhdysvaltalainen suuryritys. Trumpin toisen presidentinkauden aiheuttama transatlanttisten suhteiden heikkeneminen on aiheuttanut huolta eri organisaatioiden digitaalisesta strategisesta autonomiasta, eli siitä, ovatko käyttämämme digitaaliset järjestelmät todella loppukäyttäjien hallussa, ja keillä kaikilla todellisuudessa on pääsy esimerkiksi pilvipalveluissa säilytettävä tietoon. Strateginen autonomia terminä esiintyy uusimmassa strategiassa vain kerran, ja sekin puhuttaessa EU:n strategisesta autonomiasta.[315]

Strategian ensimmäinen pilari – osaaminen, teknologia ja TKI – käsitteli ja asetti osittain samoja teemoja kuin aikaisemmatkin strategiat, kuten yleistä kyberturvallisuusosaamisen vahvistamista ja sitä kautta elinvoiman sekä kilpailukyvyn lisäämistä. Uusia elementtejä olivat kansalaisten kyberturvallisuusvastuun peräänkuuluttaminen, kyberturvallisuuden kriittisen tietopääoman suojaaminen ja salausteknologian omavaraisuus, disruptiivisten teknologioiden[316] käyttöönotto edellyttäen kaikissa laitteissa sisäänrakennettua turvallisuutta. Tänä päivänä vahvasti esillä oleva narratiivi ICT-omavaraisuudesta on jokseenkin haistettavissa strategiasta. Etenkin niiden toimintojen suhteen, joita pidetään kansallisen turvallisuuden suhteen kriittisinä. Toinen mielenkiintoinen nosto oli kyberturvallisuusvastuun nostaminen kansalaistaidoiksi, sillä tämä oli ensimmäinen maininta, joka käsitteli tavallisten

[314] Suomen kyberturvallisuusstrategia 2013, 3.
[315] Suomen kyberturvallisuusstrategia 2024, 33.
[316] Disruptiolla tarkoitetaan ilmiötä, jossa uuteen teknologiaan perustuva keksintö haastaa perinteiset toimintatavat. Esimerkiksi transformer-arkkitehtuuriin perustuvat suuret kielimallit.

suomalaisten toimijuutta kybertoimintaympäristössä muustakin kuin ”uhrin” tai viitekohteen näkökulmasta.

Silmäänpistävää strategiassa oli kvanttiteknologian läpimurtoon valmistautuminen: kvanttilaskennan disruptiivista vaikutusta 2020-luvun salaustekniikalle pidettiin keskeisenä, mistä kertoivat useat maininnat ja oma alaluku aiheelle. Valtiot ovat alkaneet jo keräämään salattua dataa, jonka he toivovat pystyvänsä murtamaan niin sanotun *Q-päivän*[317] koitettua, millä tarkoitetaan sitä hetkeä, kun kvanttitietokoneet saavuttavat riittävän laskennallisen tehon mitätöidäkseen nykyisen salausstandardit tehden niistä hyödyttömiä.[318] Q-päivää ei ole vielä saavutettu, mutta sen sijaan vaivihkaa transformer-arkkitehtuurin perustuvat suuret kielimallit ovat lyöneet itsensä läpi, ja vuonna 2026 generatiivinen tekoäly on ujuttanut itsensä osaksi ihmisten jokapäiväistä elämää. Teknologian kehitys on ollut niin nopeaa, että alan ammattilaistenkin on haastavaa pysyä kehityksen kulussa mukana. Tällä hetkellä arvioidaan, että esimerkiksi agenttisen tekoälyn[319] kehitys saattaa muuttaa merkittävästi joidenkin ammattien työnkuvaa sekä täysin korvata osan. Vauhti on ollut niin huimaa, että olemassa olevien yhteiskunnallisten ”suojakaiteiden” pelätään pettävän.[320]

Tekoälyn disruptiivisen vaikutuksen voidaan siis argumentoida olleen paljon merkittävämpi, ainakin toistaiseksi, mutta sen käsittely strategiassa jäi paljon pienempään osaan. Toisaalta juuri tämä taas puoltaa epävarman ja heikosti ennustettavan toimintaympäristön puolesta. Epävarmuuteen tehokkain vastalääke on varautuminen useisiin erilaisiin mahdollisiin skenaarioihin, mikä osittain on varmasti taustalla myös strategian toisessa pilarissa – varautumisessa. Kyberturvallisuuden varautumisen näkökulmasta tavoiteltiin tilannetta, jossa yhteiskunnan elintärkeät toiminnot, kriittinen infrastruktuuri, julkiset palvelut sekä huoltovarmuuskriittiset toimijat olisivat kybersietoisia. Lisäksi yksilöiden, yritysten, yhteisöjen ja viranomaisten haluttiin varautuvan yhdessä kyberuhkiin. Tämän varautumisen tulisi perustua jaettuun kokonaisvaltaiseen tilanneymmärrykseen ja pitkäjänteiseen

---

[317] Q-päivä tulee todennäköisesti olemaan yhden päivän sijaan ajanjakso, jolloin perinteiseen salaustekniikkaan perustuvista järjestelmistä tulee kvanttitietokoneille haavoittuvaisia.
[318] Mascelli & Rodden 2025, 1, 6.
[319] Agenttisella tekoälyllä tai tekoälyagenteilla tarkoitetaan tekoälyjärjestelmiä, jotka kykenevät suorittamaan itsenäisesti niille asetettuja tehtäviä. Tällaiseen tekoälyjärjestelmään saattaa kuulua useita eri AI-agentteja, jotka pystyvät kommunikoimaan keskenään.
[320] Radanliev, et al. 2025; ”Koodarin kuolema?”: *Helsingin Sanomat*. 4.5.2025. <https://www.hs.fi/visio/art-2000011176878.html>.

resurssointiin. Kyvykkyyttä reagoida ja toimia yhdessä harjoiteltaisiin monipuolisesti. Tästä varautumismallista pyrittiin myös rakentamaan kansainvälisesti tunnettua vientituotetta.[321]

Kolmas strategian pilari omistettiin kokonaan yhteistoiminnalle, joka oli myös Suomen kyberturvallisuuden tilaa vuonna 2017 arvioineen selvityskokonaisuuden kehittämiskohde. Selvityksen johtopäätöksissä kannustettiin edistämään Suomen kyberturvallisuuden kannalta myönteisiä asioita, minkä lisäksi elinkeinoelämän kyberturvallisuutta arvioivassa osassa kehotettiin vahvistamaan yksityisen ja julkisen sektorin välistä yhteistyötä.[322] Kolmannen pilarin toimenpiteet vastaavat pitkälti näihin ehdotuksiin: tavoitteeksi asetettiin proaktiivinen kansainvälinen kybertoimintaympäristöä koskeva yhteistyö, minkä lisäksi kyberturvallisuuden, -rikostorjunnan ja -puolustuksen yhteistoimintaan katsottiin olevan hyödyllistä osallistua. Tämän todettiin olevan erityisen tärkeää EU:n ja Naton viitekehyksessä. Kansallisen yhteistoiminnan puolella yksityisen ja julkisen sektorin välisen yhteistyön ja luottamuksen tiivistämistä pidetään tärkeänä. Tältä pohjalta pyrkimys oli myös päästä kehittämään ja tarjoamaan yhteisiä kyberturvallisuuspalveluja. Lopuksi vielä painotetaan, että viranomaisten välillä yhteistoiminnassa tarvittavan tiedon on liikuttava saumattomasti.[323]

Neljäs ja viimeinen pilari on entuudestaan tuntemattomampi. Suomi ei ole ainakaan julkisesti halunnut linjata, että sen kyberpuolustukseen kuuluu myös vastatoimet vihamieliseen kybervaikuttamiseen. Osa-alueen strategiset tavoitteet ovat: koko yhteiskunnan toimijoiden selkeiden roolien ja toimivaltuuksien asettaminen sekä kyky reagoida oikea-aikaisesti ja oikealla tavalla kyberhäiriöihin; perustaa reagointi ja vastatoimet kattavaan tilanneymmärrykseen; torjua järjestäytynyttä sekä vakavaa kyberrikollisuutta; ja laatia kansalliset toimintaperiaatteet valtiollisiin ja valtion turvallisuutta vaarantaviin uhkiin vastaamiseksi lanseeraamalla kyberpuolustusdoktriini.[324] Toisaalta Suomen maanpuolustuspoliittisen linjan mukaista on ylläpitää uskottavaa asevoimien kyvykkyyttä, jolla Suomeen kohdistuvaa sotilaallisen voimakäytön kannattavuutta ennaltaehkäistään. Viimekädessä Suomi kuitenkin ”- - puolustaa aluettaan, väestöään ja yhteiskuntaansa hyödyntäen kaikkia

---

[321] Suomen kyberturvallisuusstrategia 2024, 27.
[322] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 45, 68.
[323] Suomen kyberturvallisuusstrategia 2024, 31.
[324] Ibid., 35.

voimavarojaan ja yhteistyössä liittolaisten kanssa - -.”[325]

Tässä kontekstissa toisaalta olisi kummallista, jos samanlainen linjaus ei pätisi, sillä kansainvälisen oikeuden mukaan valtioilla on oikeus puolustaa suvereniteettiaan, johon myös kybertoimintaympäristö kuuluu. Mahdollisiksi vastatoimenpiteiksi luetellaan muun muassa tehostettu kansainvälinen tiedonvaihto, pakotteet ja aktiviinen kyberpuolustus. Kyberpuolustus on osa-alueena perinteisiä sodankäynnin ulottuvuuksia mutkikkaampi, sillä siinä oman kyvykkyyden piilottaminen vihollisilta korostuu – kyberkyvykkyyksiä on haastavampi esitellä pelotteen samalla tavalla kuin ohjuksia. Käytännössä tämä edellyttäisi, ”oman käden” paljastamista, mikä antaisi vastapuolelle mahdollisuuden käänteismallintaa mahdollinen valttikortti.[326]

VTV tunnisti kuitenkin strategiassa merkittäviä puutteita lähtien sen toimeenpanosta. Yhteisestä toimeenpanosuunnitelmasta huolimatta kenelläkään ei ole kokonaisvastuuta strategian toteutuksesta, koska kyberturvallisuusjohtajalla ei siihen ole toimivaltuuksia. VTV nostaa huolenaiheeksi myös tässä tutkielmassa nousseen ilmiön, jossa samat tavoitteet siirretään strategiasta ja toimeenpanosuunnitelmasta toiseen. Hämmästyttävästi, tätä pidettiin jopa ”pitkäjänteisenä kehittämisenä”, mikä toki joidenkin tavoitteiden kohdalla saattoi pitää paikkansa niiden luonteesta johtuen. Ongelmaksi muodostuivat ne tavoitteet, joiden toteuttamisessa epäonnistuttiin, ja joita siirrettiin seuraavaan strategiaan.[327]

Viimeisin käsiteltävä osuus vuoden 2024 strategiasta koski resursointia, toimeenpanoa ja seurantaa. Vuoden 2019 strategiassa riittävien resurssien varmistaminen mainittiin ohimennen ja ainoastaan kriittisten toimintojen osalta. Kyberturvallisuuden kehittämisohjelmassa rahoituksen määrää tarkennettiin ainakin vuosille 2022–2025, jolloin ohjelman toteutuksen arvioitiin edellyttävän 5,9 miljoonaa euroa. Vuonna 2024 ohjelman 45 toimenpiteestä 18 oli VTV:n tarkastuskertomuksen mukaan toteutettu kokonaan tai osittain, ja 21 oli aloitettu, mutta niiden jatko oli joko osittain tai täysin siirtynyt osaksi vuoden 2024 kyberturvallisuusstrategian toimeenpanosuunnitelmaa. Loput kuusi toimenpidettä oli lopetettu joko rahoituksen puutteen tai jonkun muun syyn takia. VTV näki vuonna 2025 merkittäviä puutteita kyberturvallisuuden rahoituksessa laajemminkin. Vuoden 2019 strategian hajanainen

---

[325] Suomen puolustusselonteko 2024, 59–60.
[326] Haggman 2018, 69.
[327] Suomen kyberturvallisuusstrategia 2024, 9–12, 15–16.

toteuttaminen johti myös resurssien siiloutumiseen, ja esimerkiksi HVK:n *Digitaalinen turvallisuus 2030* hankkeen rahoitusta jouduttiin vuonna 2025 supistamaan 20 miljoonasta 15 miljoonaan euroon.[328]

Strategiassa riittävälle resursoinnille oli osoitettu oma osionsa, ja siihen tunnuttiin suhtautuvan vakavasti. Siinä esimerkiksi todettiin, että strategian laatimishetkellä kyberturvallisuuden resursointi oli tarpeisiin nähden riittämätöntä pelkästään sen hetkisen tilan ylläpitämiseksi. Strategian toimenpiteiden toimeenpano tulisi edellyttämään lisäresursseja. Samalla arvioitiin, että Suomen valtionhallinto käyttäisi noin 300 miljoona euroa vuodessa kyberturvallisuuden varmistamiseen. Tämä ei sisältänyt aluehallinnon, hyvinvointialueiden ja paikallishallinnon käyttämiä resursseja, joiden seuraaminen on epävarmempaa. Elinkeinoelämän, jolla on huomattava rooli Suomen kriittisen infrastruktuurin kyberturvallisuuden varmistamisesta, arvioitiin käyttävän vuosittain noin kolme miljardia euroa kyberturvallisuuteen. Samaan aikaan tunnistettiin Suomen valtiontalouden merkittävät haasteet yhdistettynä teknologiseen korjausvelkaan, kyberturvallisuusalan omaamisvajeeseen sekä EU:n lisääntyvään sääntelyyn. Strategisten tavoitteiden toteuttamiseksi kyberturvallisuuteen katsottiin olevan välttämätöntä suunnata resursseja.[329]

Valitettavasti vakuuttavista kirjauksista huolimatta, uusimman strategiapäivityksen toimenpidesuunnitelma ei sisältänyt ylimääräisiä resursseja toteutukseen tai kehittämiseen. Jokainen eri toimenpiteistä vastaava hallinnonala tekisi omat esityksensä määrärahatarpeistaan. Tämä käytännössä kuitenkin herkästi johtaa VTV:n mukaan siihen, että kehittämisrahoitusta on vaikeaa koordinoida ja priorisoida poikkihallinnollisesti. Tämä on varsin hälyttävää huomioiden, että joulukuussa 2024 julkaistu strategian toimeenpanosuunnitelma esittää lähes 50 prosentille toimenpiteistä lisäresursseja toteutuakseen. Suunnitelman toimenpiteet on jaettu kahteen ”koriin”, joista ensimmäinen on varattu kriittisille, pikaista toimintaa vaativille aiheille. Näistä toimenpiteistä noin 60 % edellyttää lisäresursseja, ja koko strategian toimeenpanosuunnitelman vaatima lisärahoitustarve on 90 miljoonaa euroa. Suhteessa valtionhallinnon käyttämään 300 miljoonaan euroon tämä kasvattaisi kuluerää lähes kolmanneksella. VTV:n tekemän haastattelututkimuksen mukaan 54 prosenttia viranomaisorganisaatioiden edustajista oli sitä

[328] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 13–14.
[329] Suomen kyberturvallisuusstrategia 2024, 40–41.

mieltä, että heidän organisaationsa resurssit eivät riittäneet kyberturvallisuuden hallintaan ja kehittämiseen.[330]

NIS2 EU:n kyberturvallisuusdirektiivin esiintyminen strategiassa aiheuttaa kummastusta. Se tuntuu olevan kyberturvallisuutta ajava voima, johon Suomen tulee taipuva, vaikka kansallinen tahtotila ylläpitää kansainvälisesti korkeaa kyberturvallisuuden tasoa. Liitteenä löytyä kyberturvallisuuden kansallinen yhteistoimintamalli tuntuu lähes NIS2 sanelemalta kuin sisäisesti kumpuavalta, vaikka mallin määrittelemistä on peräänkuulutettu jo ensimmäisestä strategiasta lähtien. Tämänlaisen sisäisen yhteistoimintamallin ohjesäännön tulisi tulla sisältäpäin, eikä olla ulkoisen toimijan ”pakotettavana”.[331]

Huolimatta siitä, että Suomen kyberturvallisuus on kansainvälisillä indikaattoreilla hyvällä tolalla, kaikkien kyberturvallisuusstrategioiden toimeenpano, viimeisin mukaan lukien, antaa aihetta huoleen. Poliittinen sitoutuminen turvallisen kybertoimintaympäristön täytäntöön vaikuttaa vajavaiselta riippumatta hallituspohjasta ja taloudellisesta tilanteesta. Vuonna 2023 aloittanut Petteri Orpon oikeistolainen hallitus on pyrkinyt tasapainottamaan Suomen valtiontaloutta voimakkaasti. Vaikka kyberturvallisuus on huomioitu hallitusohjelmassa verrattain kattavasti, löytyen omana alalukunaan osana ulko- ja turvallisuuspolitiikkaa, on todennäköisesti turha odottaa valtioneuvoston kehysriihistä allokoitavan riittävästi määrärahoja kyberturvallisuusstrategiassa asetetun kansallisen tahtotilan saavuttamiseksi.[332]

[330] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 17–20.
[331] Suomen kyberturvallisuusstrategia 2024, 3, 51–52.
[332] Vahva ja välittävä Suomi 2023, 10, passim.

5 Johtopäätökset

Kyberturvallisuus on tänä päivänä keskeinen osa Suomen valtiollista, yhteiskunnallista ja kansallista suvereniteettia. Suomi on vuonna 2026 yksi maailman digitalisoituneimmista yhteiskunnista, mikä tarkoittaa sitä, että kyberturvallisuus yksi sen kriittisistä kulmakivistä. Vuosina 2010–2024 Suomen toimintaympäristö on muuttunut pikaisella tahdilla; turvallisuusympäristön muutoksen lisäksi teknologian vuolas kehitys on tuonut esiin valtioon, yhteiskuntaan ja yksilöihin kohdistuvia uhkia, joita ei vielä vuosikymmen sitten osattu edes kuvitella. Kyberturvallisuus on tutkielman tarkastelujakson aikana kehittynyt varsin kapeasta teknologiapainoitteisesta erikoisasiantuntijoiden alasta kaikkia ja kaikkea koskettavaksi turvallisuuskysymykseksi.

Suomen kyberturvallisuuden turvallistaminen ei ole ollut strategisesti ja proaktiivisesti johdettu selkeä, vaan pitkälti reaktiivinen, iteratiivisesti opetteleva prosessi, jolle olisi reilua kuitenkin antaa tyydyttävä arvosana. Sitä turvallistivat pääasiassa kyberturvallisuuden alan asiantuntijat ja tutkijat, puolustusministeriön hallinnonala sekä valtionhallinnon virkakunta. Viimeisimmässä joukossa korostuivat etenkin puolustus-, valtiovarain- ja liikenne- ja viestintäministeriön hallinnonalojen ICT-asiantuntijat. Kyberturvallisuuden etenemiseen eniten vaikuttivat teknologisen kehityksen ja geopolitiikan aiheuttama turvallisuus- ja toimintaympäristön muutos, mikä pakotti valtionhallinnon reagoimaan tilanteeseen enemmän pakon sanelemana kuin sisäisestä proaktiivisuudesta kummuten. Tästä esimerkkeinä toimivat muun muassa Edward Snowdenin tekemät paljastukset, ulkoministeriössä peräti neljä vuotta jatkunut tietoverkkovakoilutapaus ja Vastaamon tietomurto. Oli kyse sitten suomalaisesta sinisilmäisyydestä vai poliittisen tahdon riittämättömyydestä, Suomi on joutunut, hyvistä lähtökohdista huolimatta, vahvistamaan kyberturvallisuuttaan jälkijunassa kyberturvallisuusilmiöihin reagoiden. Suomi oli esimerkiksi yksi viimeisimpiä Euroopan maita, joilla ei ollut sotilas- tai siviilitiedustelulakeja.

Alun käynnistysvaikeuksien jälkeen kyberturvallisuuden kehittämiseen saatiin lupaavaa vauhtia hallitusohjelmakirjauksella, ensimmäisellä kyberturvallisuusstrategialla sekä tämän toimeenpano-ohjelmalla. Ilmassa oli jopa jonkinlaista toiveikkuutta, sillä Suomesta kuitenkin tunnistettiin löytyvän kyberturvallisuuden kansainvälistä osaamista, mistä etenkin poliitikot toivoivat talouskasvua kiihdyttävää veturia. Toisaalta vuoden 2013 strategiaa ja sen toimeenpano-ohjelmaa tarkastellessa on argumentoitavissa, että niiden tavoitteet olivat käytettävissä olevien resurssien sekä hallintorakenteiden asettamien realiteettien kanssa ristiriidassa. Tämä konkretisoitui vuonna 2017 tehdyissä selvityksissä kyberturvallisuuden tilasta sekä niiden myötä tehdyssä toimeenpano-ohjelman korjauksessa sekä muissa tutkimuksissa, kuten *Kyberturvallisuuden strateginen johtaminen*. Silloin havahduttiin siihen, että merkittävä osa tavoitteista oli jo niiden asettamisvaiheessa tuomittuja epäonnistumaan.

Vaikka ulkoiset tekijät vaikuttivat kyberturvallisuuden kehitykseen sitä kiihdyttävällä tavalla, veivät myös merkittävät ulkoiset kriisit paljon päättäjien ”kaistanleveyttä”, jolloin kyberturvallisuus jäi esimerkiksi Euroopan pakolaiskriisin ja koronapandemian jalkoihin. Vaikka aiheen vakavuus ja tärkeys jossain määrin tunnistettiin, kyberturvallisuuden kehitystä vaivasi todellinen poliittisen sitoutumisen puute, mikä osittain johtui myös aihealueen teknisestä ulottuvuudesta ja sen reaalimaailman vaikutusten kokemisesta etäisinä. Suomen yskivä talous oli myös jokaisen finanssikriisin jälkeisen hallituksen tärkein prioriteetti mikä osaltaan selittä sitä, miksi kyberturvallisuuteen ei ollut varaa allokoida riittäviä määrärahoja.

Poliittisen sitoutumisen puute heijastui toiseen kyberturvallisuuden merkittävään valuvikaan: olemattomaan strategiseen johtamiseen koko yhteiskunnan tasolla. Toisaalta valtionhallinto yritti korjata tilannetta vuoden 2019 strategiassa perustamalla kyberturvallisuusjohtajan toimiston vastamaan kansallisesta kyberturvallisuuden koordinaatiosta ja yhteensovittamisesta. Toimistolla ei kuitenkaan ole erityistä toimivaltaa tai tulos- ja kehittämisvastuuta, minkä lisäksi kyberturvallisuuden kansallisen johtamisen ja koordinoinnin malli on tänäkin päivänä varsin hajanainen.[333]

Vuosina 2014–2020 kyberturvallisuutta alettiin lähestyä jossain määrin realistisemmasta näkökulmasta, ja tuolloin laaditut yhteiskunnanturvallisuusstrategia, ulko- ja turvallisuuspoliittinen selonteko sekä puolustusselonteko alkoivat huomioimaan kybertoimintaympäristöstä kumpuavia uhkia. Näistä kolmesta puolustusselonteko käsitteli kyberturvallisuutta laaja-alaisimmin, sillä puolustusministeriö ja tämän hallinnonala, jonka yhteydessä myös Turvallisuuskomitea toimii, ajoi kyberturvallisuuden vahvistamista voimakkaasti. Strategisen johtamisen kehittämisestä huolimatta vuoden 2019 strategian toimeenpano oli hajanaista, eikä sen toteutumista VTV:n mukaan seurattu kokonaisuutena.[334] Toisaalta seuraavana vuonna alkanut koronapandemia vei huomion kyberturvallisuuden

[333] Kyberturvallisuuden hallinnan tila valtionhallinnossa 2025, 6, 12.
[334] Ibid., 12.

kehityksestä joksikin aikaa, kunnes 21.10.2020 ilmi tullut Vastaamon tietomurto käänsi koko yhteiskunnan katseen hetkeksi kohti kyberturvallisuutta ja tämän laiminlyönnin ikävämpiä seurauksia. Näin kävi siitäkin huolimatta, että tämänlaiset riskit oli tiedostettu vuosia aikaisemmin, ja joista alan erityisasiantuntijat, kuten Jarno Limnéll sekä Pertti Järvinen, olivat varoittaneet.

Rauhasta vuonna 2012 Nobel-palkittu unioni joutui havahtumaan siihen, että hitaasti, mutta varmasti, sotilaallinen voimankäyttö ja etupiiriajattelu tekivät paluun ruususen unta nukkuvalle mantereelle. Vaikka siihen ei haluttu uskoa, Suomessa tätä vastenmielistä todellisuutta osattiin jossain määrin ennakoida, mikä näkyi vuoden 2016 ja 2017 selonteoissa sekä Suomen viljelemässä ”Nato-optiossa”. Tästä huolimatta Venäjän aloittama hyökkäyssota 24.2.2022 löi silti monen ällikällä. Ukrainan kokemukset osoittivat, että kyberkyvykkyydestä oli tullut erottamaton osa modernia totaalista sodankäyntiä.

Vuonna 2024 ulko- ja turvallisuuspoliittinen selonteko sekä puolustusselonteko uusittiin kuvastamaan uutta realismin värittämää maailmaa. Myös kyberturvallisuusstrategia uusittiin vastaamaan muuttuneeseen turvallisuusympäristöön. Kansallisen kyberturvallisuuden lähtökohtia yhtenäistettiin puolustuspolitiikan ja kyberpuolustuksen kanssa. Tehokkaan puolustuksen lisäksi päivitetyssä strategiassa osoitettiin valmiutta ja halukkuutta myös reagoida ja vastata Suomeen kohdistuviin kyberhyökkäyksiin. Suomalaisen kybertoimintaympäristön uhkaksi attribuoitiin pääasiallisesti Venäjä sekä muita valtiollisia toimijoita. Näin suomalaisen kyberturvallisuusympäristön turvallisuus oli kansallisen suvereniteetin asia, jolloin sen puolustaminen nähtiin myös kansainvälisen lainsäädännön puitteissa oikeutettuna.

Omat haasteensa uusimman kyberturvallisuusstrategian toimeenpanolle toi riittämättömien varojen ikuisuusongelma. Orpon hallituksen keskeisin teema on ollut talouden tasapainottaminen, mikä on edellyttänyt reippaita menoleikkauksia, eikä kyberturvallisuuteen, Vastaamoista tai WannaCrysta huolimatta, tuntunut edelleenkään löytyvän riittäviä resursseja. Vaikka vuoden 2024 strategia eritteli resurssipuutteen kehittäväksi osa-alueeksi, senkin toimeenpano kärsi puutteellisesta rahoituksesta. Huolimatta siitä, että strategiaa oli tarkoitus toimeenpanna yhteisen toimeenpanosuunnitelman kautta, ja sen tueksi ryhdyttiin laatimaan kyberpuolustusta määrittävää kyberdoktriinia, tuntui sen tahtotila edelleen ohuelta. Tätä tukee vuoden 2026 ilmi tullut tieto, että ulkoasiainhallinnon tietojärjestelmiin oli murtauduttu –

jälleen. Tällä kertaa murto kosketti myös koko muuta valtioneuvostoa. Myös vuonna 2024 ilmi tullut Helsingin kaupunkiin kohdistunut tietomurto vahvistaa tätä johtopäätöstä.

Alan asiantuntijat, turvallisuusviranomaiset, Puolustusvoimat ja Suomen valtionhallinnon virkakunta pyrkivät turvallistamaan Suomen kybertoimintaympäristöä aktiivisesti vuosina 2010–2024 pyrkien vastaamaan muuttuvaan turvallisuusympäristöön sekä teknologiseen kehitykseen. Kataisen hallitusohjelmassa kyber-alkuiset sanat esiintyivät kaksi kertaa, kun Orpon vastaavassa osumia oli 35 kappaletta. Sama toistui kaikissa primaariaineiston asiakirjoissa.[335] Tämä näyttäytyi aineistossa aihepiirin esiintymisenä yhä useammin yhteiskunnan turvallisuutta käsittelevissä asiakirjoissa ja kansanedustajien puheissa, sekä sen yhdistämisenä alati voimakkaammin turvallisuus- ja puolustuspoliittisiin teemoihin. Kansanedustajien eduskunnan täysistunnossa pitämiä kyberiin liittyviä puheita tarkastellessa on huomattavissa, että kiinnostus aiheeseen pariin herää aina yhteydessä johonkin ulkoiseen tapahtumaan, kuten ensimmäisen kyberturvallisuusstrategian laatimiseen vuonna 2013, tiedustelulainsäädäntöön vuonna 2017 tai Vastaamoon ja Ukrainan sotaan vuosina 2021–2022.[336]

Suomen valtiohallinto tunnisti vuonna 2024 kyberturvallisuuden yhteiskunnalle aiheuttamat riskit ja mahdollisuudet monin verroin kattavammin, ja se oli myös joutunut kokemaan, mitä kybertoimintaympäristön vakavat häiriötilat myös aiheuttivat digitalisoituneelle tietoyhteiskunnalle. Tässä toimintaympäristössä kyberturvallisuuden tavoitetilaksi asetettiin yhteiskunnan toimintavarmuuden ja luotettavuuden varmistaminen. Kunnianhimoinen tahtotila kansainvälisestä edelläkävijyydestä vaihdettiin maadoitetumpaan, mutta kiistämättä tärkeämpään tavoitteeseen. ”Kyber” ei ollut enää vain tieto- ja viestintätekniikan ammattilaisten murhe, vaan vastuu koski koko yhteiskuntaa lähtien pääministeristä päättyen tavalliseen suomalaiseen, joka kytki laitteensa internetiin. Digitalisaation edetessä kyberturvallisuuden merkitys osana jokapäiväistä turvallisuuttamme tulee kasvamaan, mikä tulee edellyttämään viimeisimmän strategian määrätietoista ja yhtenäistä toteuttamista.

[335] Tarkat tiedot kyber-alkuisten sanojen esiintymisestä aineistossa löytyvät liitteestä 1.
[336] Tarkat tiedot kyber-alkuisten sanojen esiintymisestä eduskunnan täysistunnoissa löytyvät liitteestä 2.

6 Lähteet:

Primääriaineisto:

Turvallisuuskomitea. Kansallisen kyberturvallisuuden toimeenpano-ohjelma. Helsinki: 2014.

Turvallisuuskomitean sihteeristö. Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Forssa: Forssa print, 2013.

Turvallisuuskomitea. Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. Helsinki: Turvallisuuskomitean sihteeristö, 2019.

Valtioneuvoston kanslia. Suomen kyberturvallisuusstrategia 2024–2035. Valtioneuvoston kanslian julkaisuja 2024:11. Helsinki: Valtioneuvoston kanslia, 2024.

Valtioneuvoston kanslia. Suomen turvallisuus- ja puolustuspolitiikka. Valtioneuvoston selonteko. Helsinki: Valtioneuvoston kanslia, 2012.

Valtioneuvoston kanslia. Valtioneuvoston puolustusselonteko. Valtioneuvoston kanslian julkaisusarja 5/2017. Helsinki, Lönnberg & Promo, 2017.

Puolustusministeriö. Valtioneuvoston puolustusselonteko. Valtioneuvoston julkaisuja 2021:78. Helsinki: PunaMusta Oy, 2021.

Puolustusministeriö. Valtioneuvoston puolustusselonteko. Valtioneuvoston julkaisuja 2024:5. Helsinki: Grany Oy, 2024.

Valtioneuvoston kanslia. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko. Valtioneuvoston kanslian julkaisuja 7/2016. Helsinki: Lönnberg Print & Promo, 2016.

Ulkoministeriö. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko. Valtioneuvoston julkaisuja 2020:30. Helsinki: PunaMusta Oy, 2020.

Ulkoministeriö. Ulko- ja turvallisuuspoliittinen selonteko. Valtioneuvoston julkaisuja 2024:33. Helsinki: Valtioneuvosto, 2024.

Puolustusministeriö. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. Helsinki: Vammalan kirjapaino, 2010.

Turvallisuuskomitea. Yhteiskunnan turvallisuusstrategia 2017. Valtioneuvoston periaatepäätös 2.11.2017. Helsinki, Lönnberg Print, 2017.

Valtiovarainministeriö. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka). Helsinki, Valtiovarainministeriö, 2020.

Valtiovarainministeriö. Haukka-hankkeen loppuraportti. Helsinki: Valtiovarainministeriö, 2023.

Sanastokeskus TSK ry. *Kyberturvallisuuden sanasto*. Helsinki: Sanastokeskus, 2018.

VAHTI:n toimintakertomus vuodelta 2015. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 1/2016. Helsinki: Valtiovarainministeriö, 2016.

Valtioneuvosto, 2011. <https://valtioneuvosto.fi/-/beredskapen-i-fraga-om-datanatssakerheten>.

Valtioneuvoston kanslia. Pääministeri Jyrki Kataisen hallituksen ohjelma. Helsinki, Valtioneuvoston kanslia, 2011.

Valtioneuvoston kanslia. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Helsinki: Valtioneuvoston kanslia, 2017.

Liikenne- ja viestintäministeriö. Kyberturvallisuuden kehittämisohjelma. Liikenne- ja viestintäministeriön julkaisuja 2021:7. Helsinki: Liikenne- ja viestintäministeriö, 2021.

Valtiopäiväaineisto:

Valtiopäivät 2012, pöytäkirjat.

Tutkimuskirjallisuus:

Raunio, Tapio & Wagner, Wolfgang: "The Party Politics of Foreign and Security Policy". *Foreign Policy Analysis* 16 (4), 2020, 515–531. <https://doi.org/10.1093/fpa/oraa018>

Fertl, Duroyan: "Nordic left discuss security policy in the aftermath of Russia's invasion of Ukraine". *Links – International Journal of Socialist Renewal* 24.8.2023. <https://links.org.au/nordic-left-discuss-security-policy-aftermath-russias-invasion-ukraine> [luettu 10.5.2026)].

Center for Strategic and International Studies, 2022 <https://www.csis.org/>.

Dimitroca Anna, ” The State of the Transatlantic Relationship in the Trump Era”. *Schuman Papers n°545 : The State of the Transatlantic Relationship in the Trump Era*, 2020. < https://www.robert-schuman.eu/en/european-issues/0545-the-state-of-the-transatlantic-relationship-in-the-trump-era>.

Hyppönen, Mikko. *If It's Smart, It's Vulnerable*. John Wiley & Sons, Inc., 2022.

Järvinen, Pertti. *Kyberuhkia ja Somesotaa – Digiaikana sinäkin olet etulinjassa*. Jyväskylä: Docendo: 2018.

Koiranen, Ilkka; Räsänen, Pekka & Södegård, Caj: Mitä digitalisaatio tarkoittaa kansalaisen näkökulmasta? Talous ja yhteiskunta, 3/2016, s. 24–29. Palkansaajien tutkimuslaitos.

Lehto, Martti, and Pekka Neittaanmäki. *Cyber Security : Power and Technology*. Cham, Switzerland: Springer, 2018.

Lehto, Martti. Ukrainan Infrastruktuuri kyberhyökkäysten kohteena. Upseeriliitto, 2/2022 < https://upseeriliitto.fi/verkkolehti/ukrainan-infrastruktuuri-kyberhyokkaysten-kohteena/>.

Lehto, Martti. ”The Modern Strategies in the Cyber Warfare”. *Cyber Security: Power and Technology*, toim. Martti Lehto ja Pekka Neittaanmäki. Cham: Springer, 2018, 3–20.

Haggman, Andreas. ”Cyber Deterrence Thery and Prectice”. *Cyber Security: Power and Technology*, toim. Martti Lehto ja Pekka Neittaanmäki. Cham: Springer, 2018, 63–83.

Limnéll, Jarno. “Framework to Cyber Hostilities”. *Cyber Security: Power and Technology*, toim. Martti Lehto ja Pekka Neittaanmäki. Cham: Springer, 2018, 31–48.

Limnéll, Jarno. ”Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta”. *Aalto-yliopiston julkaisusarja TIEDE + TEKNOLOGIA,* 1/2016, https://urn.fi/URN:ISBN:978-952-60-6687-5.

Limnéll, Jarno. Kyber rantautui Suomeen. Helsinki, Unigrafia Oy, 2014.

Sanastokeskus TSK ry. *Kyberturvallisuuden sanasto*. Helsinki, Huoltovarmuuskeskus, 2018. Saatavilla verkossa: https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf. [haettu 20.3.2024]

Solove, Daniel J. *Nothing to Hide : The False Tradeoff between Privacy and Security*. 1st ed. Yale University Press, 2011.

Valtioneuvosto. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös. Helsinki, Grano Oy, 2025.

Krajčovič, Peter. “Perspective Chapter: The Risks and Opportunites Associated with Social Media during the COVID-19 Pandemic and the War in Ukraine”. *Social Media*. IntechOpen, 2024, 77–96.

Valtiontalouden tarkastusvirasto. Tuloksellisuustarkastuskertomus. Kybersuojauksen järjestäminen. Valtiontalouden tarkastusviraston tarkastuskertomukset 16/2017. Helsinki, 2017.

Valtiontalouden tarkastusvirasto. Tuloksellisuuskertomus. Kyberturvallisuuden hallinnan tila valtionhallinnossa. Valtiontalouden tarkastusviraston tarkastuskertomukset 8/2025. Helsinki, 2025.

Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. U.S. Government Publishing Office, 2019.

Kortesoja, Matti. “Tapaus vastaamo – Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista.” *Tutkimus & kritiikki, 1/2022*, 9–32. < https://doi.org/10.55294/tk.113346>.

Valtiovarainministeriö. Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 2020:23. Helsinki, Valtiovarainministeriö, 2025.

Nielsen, Kristian L., and Anna Dimitrova. “Trump, Trust and the Transatlantic Relationship.” *Policy Studies* [ABINGDON], vol. 42, nos. 5–6, November 2021, 699–719, https://doi.org/10.1080/01442872.2021.1979501.

King’s College London, 2025. < https://www.kcl.ac.uk/>.

Heider, Andre, “Heider, Andre, “27 Countering Unmanned Aircraft Systems”. *De Gruyter Handbook of Drone Warfare*. Toimittanut James Patton Rogers. Walter de Gruyter GmbH, 2024. 399–420.

Humphreys, Brian E. *Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience*. Congressional Research Service. 2024

Mascelli, Jillian ja Megan Rodden. *"Harvest Now, Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks*. FEDS Working Paper 2025-093. Washington D.C.: Federal Reserve, 2025. <https://www.federalreserve.gov/econres/feds/harvest-now-decrypt-later-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm\>

Radanliev, Petar, Omar Santos ja Uchenna Daniel Ani. "Generative AI Cybersecurity and Resilience". *Frontiers in Artificial Intelligence*, 2025. <10.3389/frai.2025.1568360>.

Vahva ja välittävä Suomi. Pääministeri Petteri Orpon hallituksen ohjelma 20.6.2023. Valtioneuvoston julkaisuja 2023:58. Helsinki, PunaMusta Oy, 2023.

Suomi ehyenä kasvun, työllisyyden ja kestävyyden uralle. Mari Kiviniemen hallituksen ohjelma. Helsinki, 2010.

Pääministeri Alexander Stubbin hallituksen ohjelma. Valtioneuvoston kanslian julkaisuja 11/2014. Helsinki, 2014.

Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen ohjelma. Hallituksen julkaisusarja 10/2025. Helsinki, Edita Prima, 2015.

Osallistava ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta. Pääministeri Antti Rinteen hallituksen ohjelma 6.6.2019. Valtioneuvoston kansilian julkaisuja 2019:23. Helsinki, 2019.

Helin, Tuovi. *Uhkan ja riskin rajamailla: Kyberturvallisuuden politiikka Suomessa*. Valtio-opin pro gradu -tutkielma. Turku: Turun yliopisto, 2025.

Soikkeli, Mikko. *Lainsäädäntö tieto- ja kyberturvallisuuden perustana – valtionhallinnon viranomaisen näkökulma*. Kyberturvallisuuden pro gradu -tutkielma. Jyväskylä: Jyväskylän yliopisto 2021.

Kurttila, Mikko. *Suojelupoliisi ja tiedonhankintalakityöryhmä mediassa 2013–2015*. Hallintotieteiden pro gradu -tutkielma. Tampere: Tampereen yliopisto, 2015.

Tanner, Riikka. *Suomen kyberturvallisuusstrategia ja tiedustelulakiuudistus. Turvallisuusongelmia vai turvallistamisongelmia?* Politiikan tutkimuksen pro gradu -tutkielma. Tampere, Tampereen yliopisto, 2019.

Pohjola, Matti. *Miksi Suomen talous ei kasva?* Sitran muistio. Vantaa: Grano Oy, 2025.

Turvallisuus- ja puolustusasiain komitea: ”Kansallista kyber-strategiaa valmistelevan työryhmän asettaminen.” Pyyntö 14.4.2011, FI.PLM.2011-1308.

Buzan, Barry et al. *Security : A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

Wæver, Ole. “Securitization and Desecuritization”. Lipschutz, Ronnie D. *On Security*. Columbia University Press, 1995.

Hansen, Lene, and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International studies quarterly* 53.4 (2009): 1155–1175.

Górka, Marek. “Conceptualising Securitisation in the Field of Cyber Security Policy.” *Journal of Modern Science*, vol. 53, no. 4, 2023, 263–90. <https://doi.org/10.13166/jms/176103>.

Tepora, Tuomas, Mirkka Danielsbacka ja Matti O. Hannikainen. ”Johdanto: Tutkimuksen työkalut”. *Avaimia menneisyyteen: opas historiantutkimuksen menetelmiin,* toim. Mirkka Danielsbacka, Matti O. Hannikainen ja Tuomas Tepora. Helsinki: Gaudeamus, 2022, 7–19.

Buzan, Barry. *People, States & Fear : An Agenda for International Security Studies in the Post-Cold War Era*. 2nd ed., Colchester: ECPR Press, 2007.

Hautala, Mikko. *Sotaa ja rauhaa: Venäjä, Yhdysvallat ja Suomi uuden suurvaltakilpailun aikakaudella*. Helsinki: Otava, 2024.

Ylikangas, Heikki, ja kustantaja Art House. *Mitä on historia ja millaista sen tutkiminen*. Helsinki: Art House, 2015.

Kalela, Jorma. *Historiantutkimus ja historia*. Helsinki: Gaudeamus Oy, 2000.

Lähteenkorva, Pekka & Jussi Pekkarinen. ”Suomen lähihistorian tärkeimmät ulkopoliittiset arkistolähteet”. *Lähihistoria: teoriaan, metodologiaan ja lähteisiin liittyviä ongelmia*. Toim. Timo Soikkanen. Turku: Turun yliopisto, 1995.

Tuomi, Jouni & Anneli Sarajärvi. *Laadullinen tutkimus ja sisällönanalyysi*. Uudistettu laitos., Helsinki: Kustannusosakeyhtiö Tammi, 2018.

Aebi, Simon & Andri Hauri, Jurgena Kamberaj. *Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication*. Risk and Resilience Report. Zürich: Center for Security Studies (CSS), 2024.

Digi- ja väestövirasto. *Kuntien digitaalisen turvallisuuden selvitys*. Helsinki: Digi- ja väestövirasto, 2021.

Valtioneuvosto. *Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (TITUKRI)*. Helsinki: Valtioneuvosto, 2021.

Puolustusministeriö. *Kyberpuolustuksen kehittämisen strategiset linjaukset*. Helsinki: Puolustusministeriö, 2019.

Valtioneuvosto. *Suomen digitaalinen kompassi*. Valtioneuvoston selonteko. Helsinki: Valtioneuvosto, 2022.

Muut lähteet:

Agenda, 2025. < https://agenda.fi/fi/julkaisu/verkkokelmit-eivat-keinoja-kaihda-suomen-tie-kohti-parempaa-tietoverkkoturvallisuutta/#virolainen-huippuosaaminen>.

BBC, 2017. <https://www.bbc.com/>.

Edliex, 2015. <https://www.edilex.fi/>.

Eduskunta, 2026. <https://www2.eduskunta.fi/FI>.

Fortinet, 2025. <https://www.fortinet.com>.

Helsingin Sanomat, 2015. <https://www.hs.fi/>.

Helsingin Sanomat, 2018. <https://www.hs.fi/>.

Helsingin Sanomat, 2025. <https://www.hs.fi/>.

Herrasmieshakkerit <https://herrasmieshakkerit.fi/>. *Avoimien lähteiden tiedustelun erikoismies, vieraana Veli-Pekka Kivimäki*, 2020.

Huoltovarmuuskeskus, 2025. <https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta>.

Ilta-Sanomat, 2024. < https://www.is.fi/>.

Ilta-Sanomat, 2026. < https://www.is.fi/>.

Kuntalehti, 2018. <https://www.kuntalehti.fi/>.

Kyberturvallisuuskeskus 2025, <https://www.kyberturvallisuuskeskus.fi/fi>.

Lausuntopalvelu.fi, 2026. <https://www.lausuntopalvelu.fi/FI>.

Oikeusminiteriö, 2025. <https://oikeusministerio.fi/etusivu>.

Reuters, 2017. <https://www.reuters.com/>.

Sisäministeriö, 2026. <https://intermin.fi/tiedustelu>.

The White House. The National Strategy to Secure Cyberspace. Washington DC, The White House, 2003.

Traficomin kyberturvallisuuskeskus, 2022. <https://www.kyberturvallisuuskeskus.fi/fi>.

Valtioneuvosto, 2015. <https://valtioneuvosto.fi/etusivu>.

Valtioneuvosto, 2017. <https://valtioneuvosto.fi/etusivu>.

Valtioneuvosto, 2025. <https://valtioneuvosto.fi/valtioneuvoston-kanslia>.
Valtioneuvosto, 2026. <https://valtioneuvosto.fi/valtioneuvoston-kanslia>.
Yle Uutiset, 2016. < https://yle.fi/>.
Yle Uutiset, 2019. < https://yle.fi/>.
Yle Uutiset, 2022. < https://yle.fi/>.
Yle Uutiset, 2024. < https://yle.fi/>.
National Cyber Security Index, 2026. <https://ncsi.ega.ee/>.
Parlamenttisampon verkkosivut, 2026. <https://parlamenttisampo.fi/fi>.
EUR-Lex, 2026. < https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng>.
Onnettomuusttutkintakeskus, 2025. < https://turvallisuustutkinta.fi/fi/index.html>.

Liitteet

6.1 Liite 1: Kyber-alkuisten sanojen esiintyminen aineistossa

Asiakirja	Määrä
Hallituksen ohjelmat	
Jyrki Kataisen hallitusohjelma	2
Alexander Stubbin hallitusohjelma	2
Juha Sipilän hallitusohjelma	3
Antti Rinteen ja Sanna Marinin hallitusohjelma	18
Petteri Orpon hallitusohjelma	35
Ulko- ja turvallisuuspoliittiset selonteot	
Turvallisuus- ja puolustuspolitiikka 2012[337]	39
Ulko- ja turvallisuuspoliittinen selonteko 2016	8
Ulko- ja turvallisuuspoliittinen selonteko 2020	12
Ulko- ja turvallisuuspoliittinen selonteko 2024	26
Puolustuspoliittiset selonteot	
Turvallisuus- ja puolustuspolitiikka 2012	39
Puolustusselonteko 2017	18
Puolustusselonteko 2021	57
Puolustusselonteko 2024	95
Yhteiskunnan turvallisuusstrategiat	
Yhteiskunnan turvallisuusstrategia 2010	5
Yhteiskunnan turvallisuusstrategia 2017	13
Yhteiskunnan turvallisuusstrategia 2025[338]	42

[337] Turvallisuus- ja puolustuspolitiikka 2012 jakautui ulko- ja turvallisuuspoliittiseksi selonteoksi ja puolustusselonteoksi
[338] Ei ollut osa primääriaineistoa, mutta havainnollistaa nousujohteista trendiä kyberturvallisuuden esiintymisen suhteen.

6.2 Liite 2: Kyber-alkuisten sanojen esiintyminen eduskunnan täysistunnoissa