FI.PLM.2013-312
429/80.01.99/2011

SUOMEN KYBERTURVALLISUUSSTRATEGIAN TAUSTAMUISTIO

SISÄLLYS

1. JOHDANTO 3
2 KYBERTOIMINTAYMPÄRISTÖ JA KYBERUHKA 3
3. KYBERTURVALLISUUDEN JOHTAMISEN PERIAATTEET JA HÄIRIÖTILANTEIDEN HALLINTA 5
3.1 Kyberturvallisuuden johtamisen yleiset periaatteet 5
3.2 Yhteiskuntaa uhkaavien häiriötilanteiden hallinta 8
4. YHTEISKUNNAN ELINTÄRKEIDEN TOIMINTOJEN TURVAAMINEN KYBERUHKIA VASTAAN 8
4.1 Kybertilannetietoisuus ja Kyberturvallisuuskeskuksen perustaminen 8
4.2 Elinkeinoelämän toimintaedellytysten turvaaminen ja huoltovarmuus 10
4.3 Kyberrikollisuuden torjunta 12
4.4 Kyberpuolustuskyky 13
4.5 Kansainvälinen yhteistyö 14
4.6 Tutkimuksen ja osaamisen kehittäminen sekä harjoitustoiminta 16
5. KYBERTURVALLISUUTTA KOSKEVA SÄÄNTELY 18
5.1 Kyberturvallisuuteen liittyvä sääntely kansainvälisellä ja kansallisella tasolla 18
5.2 Lainsäädännön kehittäminen 20
6. KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO 21
6.1 Strategian toimeenpanon periaatteet 21
6.2 Toimeenpanon edellyttämiä toimenpiteitä 22
6.3 Toimeenpanon resursointi 23
6.4 Toimeenpano-ohjelma ja tuloksellisuuden mittaaminen 23
LIITE 1 KYBERTURVALLISUUSSTRATEGIAN JATKUVAN KEHITTÄMISEN PROSESSI 24

1. JOHDANTO

Tämä taustamuistio on laadittu osana Suomen kyberturvallisuusstrategiaa. Taustamuistion keskeinen tavoite on lisätä kyberturvallisuuden toimijoiden ymmärrystä kybertoimintaympäristöstä ja sen myötä auttaa heitä oman kyberturvallisuutensa kehittämisessä. Taustamuistio syventää varsinaista strategiaa ja kuvaa yksityiskohtaisemmin kansallisen kyberturvallisuuden toimintamallimme sekä kybertoimintaympäristön ja varautumisen perusteeksi kuvatun uhkamallin. Taustamuistiossa avataan strategisten linjausten edellyttämiä toimenpiteitä sekä kyberturvallisuuteen liittyvää kansallista ja kansainvälistä sääntelyä. Muistion lopussa esitetään eri hallinnonalojen ja muiden toimijoiden toimeenpano-ohjelmien laatimisen perusteet.

2. KYBERTOIMINTAYMPÄRISTÖ JA KYBERUHKA

Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja – kerroksisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansallisia turvallisuusviranomaisten, muun julkishallinnon ja yritysmaailman kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä. Globaali kybertoimintaympäristö yhdistää valtioita, yrityksiä ja kansalaisia reaaliaikaisemmin ja entistä läheisemmiksi. Tämä kehitys on lisännyt merkittävästi hyvinvointia, mutta tuonut mukanaan myös aivan uudenlaisia riskejä. Tietoteknisten laitteiden ja järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen tai vakavat kyberhyökkäykset voivat aiheuttaa erittäin kielteisiä vaikutuksia julkisiin palveluihin, liike-elämään ja hallintoon ja siten koko yhteiskunnan toimintaan.

Kyberhyökkäyksillä voidaan tuottaa suuria häiriöitä ja jopa lamauttaa osia kriittisestä infrastruktuurista ja yhteiskunnan elintärkeistä toiminnoista. Valtio tai organisaatio voidaan painostaa poliittisiin, sotilaallisiin tai taloudellisiin myönnytyksiin. Suurvallat ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin.

Toistaiseksi kyberoperaatiot on tulkittu niin sanotuiksi pehmeiksi toimiksi, minkä vuoksi niiden käyttökynnyksen voidaan arvella olevan alempi kuin perinteisten sotilasoperaatioiden. Lisääntyvä kyberaktivismi, -rikollisuus ja -vakoilu osoittavat sekä valtiollisten että ei-valtiollisten toimijoiden toiminnan kasvua. Kybertoimintaympäristö onkin muuttanut perinteisiä kansainvälisiä valta-asetelmia. Se antaa pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen.

Edellä kuvattu kybertoimintaympäristön kehitys vaikuttaa myös Suomeen. Suomi on yksi kehittyneimmistä tietoyhteiskunnista, jonka toiminnat ovat riippuvaisia erilaisista sähköisistä verkoista ja niiden antamista palveluista. Suomi on jo joutunut kyberoperaatioiden kohteeksi, joissa painopiste on ollut kyberaktivismissa, -rikollisuudessa ja -vakoilussa. Kybertoimintaympäristössä tapahtuva kansainvälinen kehitys lisää uusien uhkien mahdollisuutta meitä vastaan. Julkishallintoon ja elinkeinoelämään kohdistuu jatkuvia järjestelmähaavoittuvuuksien hyväksi-

käyttö- tai murtoyrityksiä. Hyökkäysten ammattimaisuus näkyy siinä, että hyökkäyskohde on valittu ja tiedusteltu tarkasti. Hyökkäyksiin käytetään enenemässä määrin pitkälle kehittyneitä haittaohjelmia ja hyökkäystekniikoita.

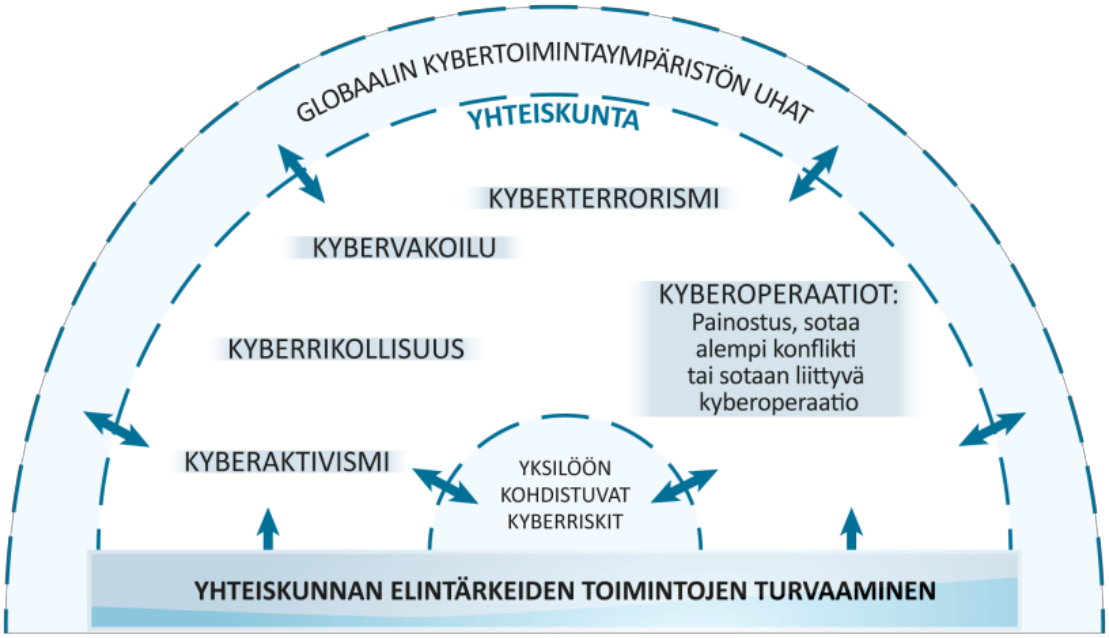
Kybermaailman avoimuus mahdollistaa hyökkäykset eri puolilta maailmaa käyttäen hyväksi järjestelmien haavoittuvuuksia. Näitä haavoittuvuuksia on niin ihmisten toiminnassa, organisaatioiden toimintaprosesseissa kuin käytettävässä informaatioteknologiassa. Monimutkaisia ja kehittyneitä haittaohjelmia vastaan on vaikea suojautua. Hyökkääjiä on vaikea tunnistaa tai löytää heidän olinpaikkojaan. Tietotekniikan levittäytyminen yhä laajemmin teollisuustuotanto- ja ohjausjärjestelmiin ovat luoneet uusia haavoittuvuuksia ja mahdollisia hyökkäyskohteita kybertoimintaympäristössä.

Vuosi 2010 oli kyberturvallisuuden osalta uuden aikakauden alku, kun Stuxnet -verkkomato löydettiin. Sen avulla toteutettiin Iranin ydinlaitoksiin kohdistunut hyökkäys, jossa Stuxnet vaurioitti uraanin rikastamiseen tarkoitettuja sentrifugeja ja siten viivästytti jopa vuosia Iranin rikastushanketta. Stuxnetin koodin kehittäminen on vaatinut suurta taitoa ja huomattavia resursseja. Tämä haittaohjelma osoitti, että kybertyökaluilla voidaan aiheuttaa myös fyysistä tuhoa sähköisissä laitteissa ja järjestelmissä. Tässä uudessa vaiheessa teollisuusautomaatio ja ohjelmoitava logiikka ovat entistä useammin kyberiskujen ensimmäisenä kohteena, kun lopullisena tavoitteena on vaikuttaa yhteiskunnan elintärkeisiin toimintoihin.

Kyberuhkamalli tarkoittaa kuvausta kyberuhkien aiheuttamista häiriöistä, uhkan vaikutusmekanismista, lähteestä, kohteesta ja vaikutuksesta kohteeseen. Uhkat voivat kohdistua suoraan tai välillisesti yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria ja/tai kansalaisia vastaan maan rajojen sisältä tai ulkopuolelta.

Kyberuhkamallissa kyberuhkia ovat:

- Kyberaktivismi (kybervandalismi, haktivismi)
- Kyberrikollisuus
- Kybervakoilu
- Kyberterrorismi
- Kyberoperaatiot; painostus, sotaa alempi konflikti tai sotaan liittyvä kyberoperaatio



KUVIO 1 Suomen kyberuhkamalli

Yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat uhkat voivat esiintyä itsenäisinä, samanaikaisina tai toistensa jatkumoina. Uhkien eskaloitumisen nopeus ja ajallinen kesto vaihtelevat, mutta hyvin usein vaikuttavuus toteutuu lyhyessä ajassa. Kybertoimintaympäristön luonteen vuoksi uhkien syitä, niiden taustalla olevia toimijoita, täsmällisiä kohteita ja tavoitteita, ilmenemisen laajuutta tai vaikutusten seurannaisvaikutuksia on vaikea ennustaa. Kyberuhkiin voi liittyä myös muita uhkia. Esimerkiksi terrorismissa voidaan fyysistä tuhoa aiheuttaviin iskuihin liittää erilaisia operaatioita kybertoimintaympäristössä.

3. KYBERTURVALLISUUDEN JOHTAMISEN PERIAATTEET JA HÄIRIÖTILANTEIDEN HALLINTA

3.1 Kyberturvallisuuden johtamisen yleiset periaatteet

Kyberturvallisuuden johtamisen ylimmän tason muodostaa valtioneuvosto. Pääministeri johtaa valtioneuvoston toimintaa ja huolehtii valtioneuvostolle kuuluvien asioiden valmistelun ja käsittelyn yhteensovittamisesta. Asioita käsitellään ja sovitetaan valmistelevasti yhteen pääministerin johtamissa valtioneuvoston ministerivaliokunnissa sekä tarvittaessa hallituksen iltakoulussa ja neuvottelussa. Valtioneuvoston tehtävänä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen.

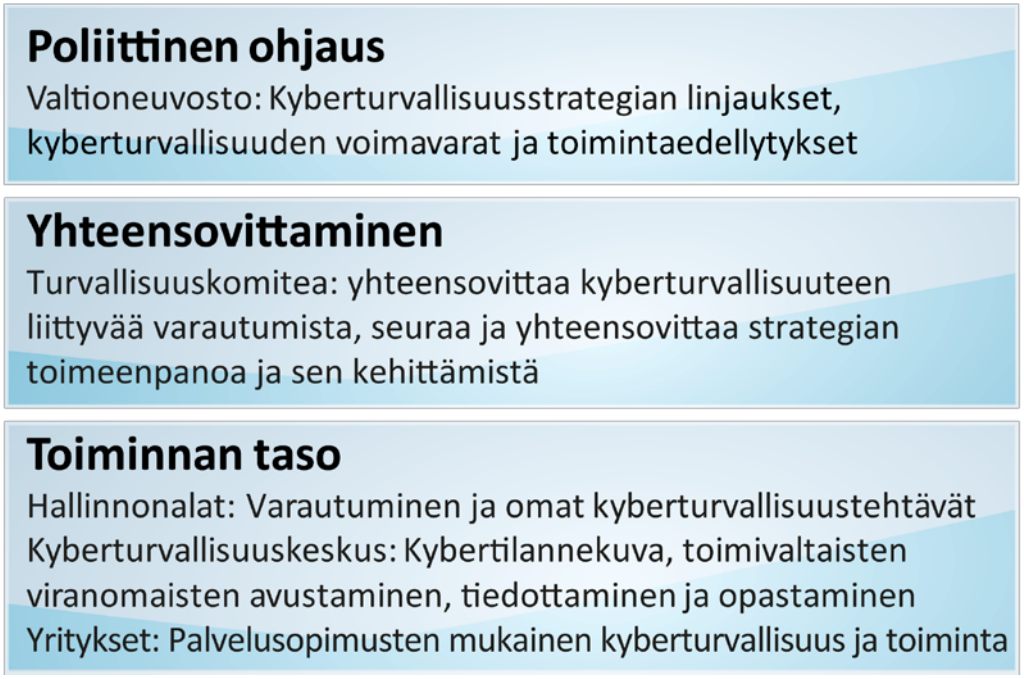
Yhteiskunnan turvallisuusstrategian perusperiaatteiden mukaisesti toimivaltaiset viranomaiset vastaavat häiriötilanteiden hallinnasta ja siihen liittyvästä varautumisesta. Kukin ministeriö vastaa oman toimialansa lainsäädännön valmistelusta ja johtaa vastuualueensa toimintaa sekä tarpeen mukaan osallistuu ministeriöiden yhteistoimintaan. Kyberturvallisuusstrategialla ei

muuteta Yhteiskunnan turvallisuusstrategiassa määritettyjä tehtäviä, joiden mukaan liikenne- ja viestintäministeriö vastaa sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistamisesta ja valtiovarainministeriö valtionhallinnon IT-toimintojen ja tietoturvallisuuden sekä valtionhallinnolle yhteisten palvelujärjestelmien turvaamisesta.

Perustettava Turvallisuuskomitea koordinoi kyberturvallisuuden varautumista ja seuraa kyberturvallisuusstrategian toimeenpanoa sekä tekee esityksiä sen jatkokehittämisestä. Turvallisuuskomitea toimii kiinteässä yhteistyössä muiden yhteistyöelinten kanssa, jotka yhteensovittavat kyberturvallisuuteen liittyviä asioita omiin tehtäviinsä liittyen.

Perustettava Kyberturvallisuuskeskus tukee ja avustaa kyberturvallisuuden toimijoita omien, vastuulleen kuuluvien tehtäviensä mukaisesti. Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) tukee valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa. VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuutta koskevat asiat.

Häiriötilanteiden johtamisen tehokkuus perustuu ennakoivien toimien onnistumiseen. Normaaliolojen kyberturvallisuuden järjestelyt vaikuttavat ratkaisevasti siihen, kuinka kyberuhkatilanteista voidaan selviytyä poikkeusoloissa. Varautumisvelvoite kyberuhkia vastaan on jokaisella hallinnon alalla ja huoltovarmuuskriittisillä yrityksillä ja organisaatioilla. Yritykset suunnittelevat kyberuhkiin varautumisen osana muuta jatkuvuudenhallintaa.



KUVIO 2 Kyberturvallisuuden johtamisen periaatteet

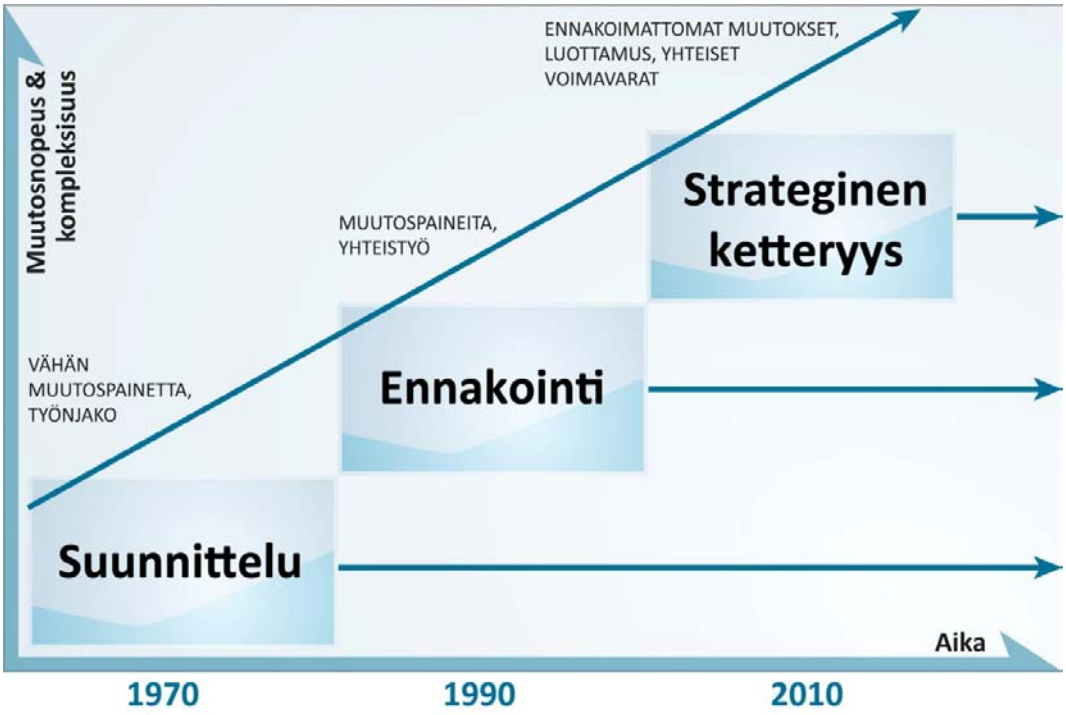
Kyberuhkien torjunta vaatii hyvää suunnittelua ja ennakointia. Uusi toimintaympäristömme edellyttääkin kaikilta osapuolilta vahvaa osaamista sekä nopeaa, oikean suuntaista ja yhdenmukaista reagointia eli strategista ketteryyttä. Kyberturvallisuuden johtamisessa ilmentyy stra-

tegisen ketteryyden kaikki kolme tekijää, joita ovat strateginen herkkyys, johdon yhtenäisyys sekä resurssien joustava käyttö.

Strateginen herkkyys edellyttää kykyä nopeaan tilannekuvan muodostamiseen ja tilannetietoisuuden luomiseen. Johdon yhtenäisyys edellyttää jaettua tilannetietoisuutta, koordinoitua ja verkostoitunutta johtamista sekä kokonaisuuden edun optimointia. Resurssien joustava käyttö vaatii riittävää kyberosaamista sekä kykyä nopeaan vastatoimenpiteiden ja taloudellisten resurssien allokointiin. Kybertoimintaympäristössä tulee päästä irti osa-optimoinnista sekä siiloutuneiden rakenteiden aiheuttamasta kankeudesta.

Kybertoimintaympäristön muutosnopeus ja kompleksisuus edellyttävät siis uudenlaista, vahvaan koordinaatioon ja yhteisiin pelisääntöihin perustuvaa verkostomaista toimintamallia (kuvio 3). Toiminnassa on kyettävä yhdistämään keskittämisen ja hajauttamisen edut, jotka ovat vahva koordinaatio ja asianomistajuuden myötä syntyvä reagointinopeus.

Suomella on lähtökohtaisesti moniin muihin maihin nähden erinomaiset mahdollisuudet nousta kyberturvallisuuden ja sen edellyttämän uuden toimintamallin edelläkävijäksi maailmassa. Kiistämättömiä vahvuuksiamme ovat vahva osaaminen, yhteistyön perinne sekä julkisen hallinnon sisällä että julkisen ja yksityisen sektorin välillä, sekä hyvin määritellyt toimintamallit ja turvallisuusvastuut eri toimijoiden kesken (YTS).



KUVIO 3 Strateginen ketteryys

3.2 Yhteiskuntaa uhkaavien häiriötilanteiden hallinta

Yhteiskunnan haavoittuvuuden lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti. Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta.

Kyberhäiriötilanteiden hallinnassa noudatetaan laillisuusperiaatetta ja voimassaolevaa toimialajakoa. Samoja häiriötilanteen hallinnan periaatteita noudatetaan sekä normaali- että poikkeusoloissa. Viranomaisten vastuujako ja yhteistyöelimien toimintamallit säilytetään normaaliolojen mukaisina. Tilanteita johdetaan ennakoivasti ja käyttöön otetaan heti riittävät voimavarat. Toimivaltainen viranomainen johtaa operatiivista toimintaa ja poikkihallinnolliset yhteistyöelimet tukevat vastuuviranomaista. Toimintaa johtava taho vastaa myös viestinnästä. Muut viranomaiset, yritykset ja järjestöt osallistuvat toimintaan tilanteen hallinnan edellyttämässä laajuudessa. Operatiivisten toimien ohella häiriötilanteiden hallinnan yhteydessä korostuu tiedonkulun varmistaminen toimijoiden välillä sekä valtiojohdon riittävä informointi.

Häiriötilanteiden hallinta organisoidaan ja toteutetaan yhteiskunnan turvallisuusstrategiassa esitetyllä tavalla. Sen mukaisesti vastuuviranomainen käynnistää häiriötilanteen hallintaan liittyvät toimenpiteet, informoi tilanteesta tarvittavassa laajuudessa muita viranomaisia ja toimijoita sekä kytkee toimintaan muut häiriötilanteen hallinnan edellyttämät toimijat. Kyberturvallisuuden häiriötilanteiden hallinta voidaan jakaa neljään kokonaisuuteen, joita ovat varautuminen, tilannekuvan muodostaminen, torjunta ja palautuminen.

4. YHTEISKUNNAN ELINTÄRKEIDEN TOIMINTOJEN TURVAAMINEN KYBERUHKIA VASTAAN

4.1 Kybertilannetietoisuus ja Kyberturvallisuuskeskuksen perustaminen

Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä. Perustetaan Kyberturvallisuuskeskus, jota tukemaan kootaan tiiviissä yhteistyössä toimiva verkosto.

Valtionjohto ja viranomaisten päätöksenteko edellyttävät riittävää tilannetietoisuutta ja että eri toimijoilla on käytettävissään luotettava ja ajantasainen kyberturvallisuuden tilannekuva yhteiskunnan elintärkeiden toimintojen ja kriittisen infrastruktuurin tilasta sekä niihin kohdistuvista häiriöistä. Kyberturvallisuuden reaaliaikainen skaalautuva tilannekuva muodostuu teknisen valvonnan ja seurannan lisäksi myös havainnoista, tiedustelusta sekä muusta tiedonhankinnasta ja aikaisemmista kokemuksista koostuvasta analyysistä.

Kansallinen Kyberturvallisuuskeskus perustetaan palvelemaan viranomaisia, elinkeinoelämää, ja muita toimijoita kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Palveluiden järjestelyistä ja Kyberturvallisuuskeskuksen toimintatavoista sovitaan osana kyberturvallisuusstrategian yhdistettyä toimeenpanosuunnitelmaa. Keskeisin palvelu on kybertilannekuvan luominen, ylläpitäminen ja jakaminen kiinteässä yhteistyössä keskusta tukevan verkoston kanssa. Kyberturvallisuuskeskus muodostetaan nykymuotoisen CERT-FI toiminnon sekä kehitteillä olevan GOV-CERT toiminnon yhdistämisellä ja varaamalla sen tehtävien toteuttamiseen tarvittavat lisäresurssit. Kyberturvallisuuskeskusta tukee toiminnallinen verkosto, johon osallistuvat kaikki tarvittavat viranomaistahot, yritykset sekä muut erikseen sovittavat toimijat, joiden tehtävänä on varautua ja reagoida kyberturvallisuuden loukkauksiin.

Kyberturvallisuuskeskuksen perustamisessa otetaan huomioon myös muut samansuuntaiset hankkeet tilannekuvajärjestelyiden virtaviivaistamiseksi ja tehostamiseksi. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä linjaa valtionhallinnon ympärivuorokautisen tietoturvallisuuden havainnointi- ja toimintakyvyn toteuttamisen. Tämän toiminnon suunnittelu ja toteuttaminen yhteensovitetaan Kyberturvallisuuskeskuksen toiminnan kanssa. Lisäksi tilannekuvan muodostamisessa otetaan huomioon valtionhallinnon tietoturvallisuuden kehittämisen yhteishankkeet, kuten turvallisuusverkkohanke (TUVE).

Kyberturvallisuuskeskuksen tehtävät:

1. Kyberturvallisuustilannekuvan muodostaminen ja jakaminen
2. Kyberuhkien riskianalyysin kokoaminen ja ylläpito yhdessä eri hallinnonalojen ja toimijoiden kanssa
3. Toimivaltaisten viranomaisten ja yksityisen sektorin toimijoiden tukeminen laajojen kyberhäiriötilanteiden hallinnassa
4. Yhteistyön tehostaminen ja osaamisen kehittämisen tukeminen

Kyberturvallisuuskeskuksen keskeisimmät palvelut ovat yhteiskunnan kyberturvallisuuden tilannekuvan luominen, kokoaminen, ylläpitäminen ja sen jakaminen tarvitsijoille. Tilannekuvan luominen edellyttää kykyä tarvittavien tietojen keräämiseen ja analysoimiseen sekä eri tarvitsijoiden tietopyyntöjen toteuttamiseen. Kyberturvallisuuskeskuksen yhteistyössä verkoston kanssa tuottama kokonaistilannekuva sisältää sekä teknisen tilannekuvan, että myös arvion kyberloukkausten kokonaisvaikutuksesta yhteiskunnan elintärkeille toiminnoille. Kyberturvallisuuskeskus sopii eri toimijoiden kanssa heidän toimintaansa liittyvistä tietotarpeista. Ylläpitohenkilöstölle suunnattua tiedotusta haavoittuvuuksista kehitetään yhä automaattisemmaksi. Sen sijaan viranomaisille ja päätöksentekijöille tehtävää tilannekuvaa kehitetään nykyistä enemmän yhteiskunnan elintärkeisiin toimintoihin kohdistuvien vaikutusten arvioinnin suuntaan.

Kyberhäiriötilanteen vahinkojen rajaus kuuluu niille viranomaisille ja yrityksille, joita häiriö koskee. Kyberturvallisuuskeskus voi laajoissa, monia viranomaisia tai yrityksiä samanaikaisesti koskevissa kyberhäiriötilanteissa tukea johtovastuussa olevaa viranomaista. Kyberturvallisuuskeskus tuottaa muodostamaansa kyberturvallisuuden kokonaistilannekuvaan perustuvaa ar-

viota kyberturvallisuuden yleistilanteesta. Tämän tilannekatsauksen avulla on tarkoitus tukea hallinnonaloja niiden omassa kybervarautumisessa ja sen suunnittelussa.

Kyberturvallisuuskeskus seuraa kyberturvallisuusuhkia ja analysoi sekä tekee ennusteita niiden vaikutuksesta Suomeen yhteistyössä kansainvälisten yhteistyökumppaneidensa kanssa. Perustuen toteuttamaansa seurantaan, Yhteiskunnan turvallisuusstrategian uhkamalleihin, kyberuhkamalliin ja reaaliaikaiseen kansalliseen valvontatietoon Kyberturvallisuuskeskus varoittaa yhteiskunnan elintärkeiden toimintojen kannalta tärkeitä yrityksiä ja viranomaisia Suomea uhkaavista uusista kyberuhkan muodoista ja kohonneista kyberuhkan tasoista sekä pyydettäessä avustaa näihin uhkiin varautumisessa.

Valtionjohdon tilannekuvan tuottaa valtioneuvoston tilannekeskus (VNTIKE). Sen ja perustettavan Kyberturvallisuuskeskuksen välinen tiivis yhteistyö lisää poikkihallinnollista havainnointi- ja analyysikykyä, jonka perusteella pystytään kokoamaan yhteinen kokonaistilannekuva. Yhteisen tilannetietoisuuden sekä -ymmärryksen avulla uhkiin kyetään reagoimaan tarkoituksenmukaisesti poliittisella ja operatiivisella tasolla.

Kyberturvallisuuskeskuksen tulosohjauksesta vastaa liikenne- ja viestintäministeriö. Keskuksen tulosohjauksen varmistamiseksi perustetaan erillinen kyberturvallisuustyöryhmä, jossa ovat edustettuina kaikki Kyberturvallisuuskeskuksen palveluiden tuottajat ja käyttäjät sekä resursoijat. Tässä työryhmässä edustajina toimivien henkilöiden tulee olla asiantuntijoita, joilla on laa- ja-alainen ymmärrys edustamiensa tahojen varautumisesta, kyberturvallisuuden tilasta ja tarpeista.

4.2 Elinkeinoelämän toimintaedellytysten turvaaminen ja huoltovarmuus

Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja – häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

Tavoitteena on turvata yhteiskunnan kannalta tärkeimpien yritysten toiminnan jatkuvuus myös kyberhäiriötilanteiden aikana. Elinkeinoelämän jatkuvuudenhallinnan suunnittelua tuetaan, kun sillä voi olla vaikutuksia elintärkeisiin toimintoihin ja turvallisen kyberympäristön luomiseen. Elinkeinoelämän toimintaedellytysten varmistamisessa Huoltovarmuusorganisaatiolla on keskeinen rooli. Varautumistoimenpiteillä turvataan yhteiskunnan toimivuuden kannalta välttämätön infrastruktuuri ja kriittisen tuotannon jatkuminen kaikissa tilanteissa.

Yhteiskunnan kriittiset tuotantoprosessit ovat entistä riippuvaisempia automaatiojärjestelmistä. Automaatiojärjestelmien kehityssykli on hidasta ja ne liittyvät nopeasti kehittyviin tietoteknisiin ratkaisuihin. Kriittisen infrastruktuurin jatkuvuudenhallinnassa on huolehdittava myös automaatiojärjestelmien tietoturvasta. Yhteydet fyysisessä maailmassa toimivien laitteiden ja tietoverkkojen välillä on suunniteltava siten, että yksinkertaisella kyberhyökkäyksellä ei voida keskeyttää laitoksen tai yksikön toimintaa. Yhteiskunnan kriittisten toimintojen kannalta on

keskeistä rajata automaatiojärjestelmien, kuten esimerkiksi kiinteistöautomaation, etäkäytön ja etäluennan haavoittuvuudet minimiin.

Nykyisin valtaosa kriittisestä infrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa. Yritysten edellytyksiä huolehtia liiketoimintansa jatkuvuudesta kyberuhkatilanteissa parannetaan ja siten lisätään luottamusta niiden tuottamien hyödykkeiden saatavuuden jatkuvuuteen.

Huoltovarmuusorganisaatio on verkosto, joka ylläpitää ja kehittää Suomessa huoltovarmuutta julkisen sekä yksityisen sektorin kumppanuusperiaatteella. Huoltovarmuus rakentuu toimivien markkinoiden ja kilpailukykyisen talouden varaan. Yhteiskunnan taloudellisia ja teknisiä perustoimintoja varaudutaan ylläpitämään markkinaehtoista toimintaa täydentävillä huoltovarmuustoimenpiteillä myös erilaisissa häiriötilanteissa ja poikkeusoloissa.

Suomen huoltovarmuuden kannalta tärkeitä yritysten liiketoiminnan jatkuvuutta turvaavia toimenpiteitä kartoitetaan ja toteutetaan osana huoltovarmuuspäätöstä ja sen toimeenpanoa. Varautuminen kyberuhkiin toteutuu yksittäisessä organisaatiossa käytännössä useimmiten perinteisen tietoturvallisuuden keinojen, menetelmien ja rakenteiden avulla. Yritysten tulisi kehittää kykyään arvioida kyberhyökkäysten riskejä, niiden vaikutuksia sekä tarvittavia toimenpiteitä. Eri toimintoketjujen ja verkostojen toimintavarmuuden arviointimenetelmiä ja arviointia tehostetaan sekä tietoisuutta verkostojen toiminnasta ja toimintavarmuudesta lisätään. Turvaaminen kyberuhkia vastaan edellyttää toimijoilta samanlaisia tai keskenään yhteen sovitettuja suojaamiskäytäntöjä. Huoltovarmuusorganisaatio tuottaa huoltovarmuuden kannalta kriittisten yritysten käyttöön työkaluja, jotka helpottavat yrityksiä niiden tehdessä toimintaansa liittyviä riskikartoituksia ja niiden kehittäessä oman toimintansa jatkuvuuden hallintaa.

Suomi voi olla hyvän kyberturvallisuutensa ansiosta myös houkutteleva investointikohde. Julkisen sektorin tehtävä on luoda turvallinen ja tehokas toimintaympäristö, mutta uusien liiketoimintamallien, tuotteiden ja palveluiden kehittäminen on yritysten vastuulla. Tavoitteena on kansainvälisen tason kyberturvallisuusklusterin aikaansaaminen. Vahvat kansainväliset yhteydet varmistavat riittävän osaamispohjan ja mahdollistavat kansainvälisesti verkostoituneen liiketoiminnan.

Erilaisissa kansallisissa kehityshankkeissa, joita hoidetaan mm. Tekesin (Teknologian ja innovaatioiden kehittämiskeskus) ja TIVIT:n (Tieto- ja viestintäteollisuuden tutkimus) kanssa tulee painopistettä siirtää selkeästi kyberympäristön suojaamista tukevan uuden liiketoiminnan ja tutkimuksen suuntaan. Esimerkiksi vuonna 2013 toimintansa aloittavan Pilvipalveluiden kehittämislaboratorion yhden painopistealueen tulee kohdistua uusien kyberympäristön suojaamispalveluiden kehittämiseen.

Yritystoiminnan turvallisuudesta huolehditaan torjumalla laitonta taloudellista tiedustelua ja kybervakoilua sekä vähentämällä tietopääomariskejä. Kotimaisen tietoturvallisuussektorin vahvistamiseksi valtionhallinto lisää panostuksia tutkimukseen, tuotekehitykseen ja koulutuk-

seen sekä toimenpiteitä hallinnon virastojen sisäiseen kehittämiseen. Kansallinen tietoturvallisuusviranomainen saavuttaa kansainvälisesti tunnustetun kansainvälisiä tietoturvasertifiointeja myöntävän viranomaisen aseman.

4.3 Kyberrikollisuuden torjunta

Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

Poliisin on pystyttävä tunnistamaan ja torjumaan tietoverkossa tapahtuva terrorististen ja muiden yhteiskuntajärjestystä vaarantavien rikosten valmistelu, rahoitus, johtaminen sekä kyettävä selvittämään epäillyt rikokset.

Tietoverkkorikollisuudesta on tullut hyvin kattava rikollisuuden osa-alue ja sen vaikutukset kohdistuvat niin valtioihin, yksityisiin kansalaisiin kuin liiketoimintaan. Tietoverkko on sekä rikollisille edullisempi, että myös riski-hyöty ja riski-vahinko – suhteessa entistä houkuttelevampi ympäristö toteuttaa rikoksia, joilla on taloudellinen tai terroristinen tavoite. Tietoverkkojen ja -järjestelmien haavoittuvuuksia käyttävät hyväkseen myös perinteinen järjestäytynyt rikollisuus. Verkossa tehtävillä hyökkäyksillä voidaan vaarantaa yhteiskunnan kriittistä infrastruktuuria ja toteuttaa terroristi-iskuja. Terroristitekojen lisäksi myös perinteisiä rikoksia, kuten petoksia, lasten seksuaalista hyväksikäyttöä ja teollisuusvakoilua tehdään myös yhä enemmän kybertoimintaympäristössä.

Rikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa toimivaltaisena viranomaisena toimii pääsääntöisesti poliisi yhteistyössä muiden lainvalvontaviranomaisten kanssa. Tietojärjestelmiin kohdistuva rikollisuus on usein valtioiden rajat ylittävää, ja sen tutkinta edellyttää monesti kansainvälistä poliisi- ja oikeudellista yhteistyötä. Oikeudellista yhteistyötä tarvitaan muun muassa todisteiden hankkimiseksi tai rikoksesta epäillyn luovuttamiseksi.

Huolehditaan, että poliisilla on riittävä toimivalta sekä osaaminen ja riittävät tiedonsaantioikeudet tunnistaa kybertoimintaympäristöön liittyviä rikollisuusilmiöitä, ennalta ehkäistä tietoverkkorikoksia, paljastaa kybertoimintaympäristössä toimivia rikollisia ja selvittää näitä rikoksia. Samoin varmistetaan, että poliisilla on riittävä toimivalta sekä osaaminen ja riittävät tiedonsaantioikeudet tunnistaa ja torjua tietoverkossa tapahtuva terroristien ja muiden yhteiskuntajärjestystä vaarantavien rikosten valmistelu, rahoitus, johtaminen ja niihin liittyvä propagandistinen tiedottaminen ja mielipiteenmuokkaus sekä kyky selvittää epäillyt rikokset.

Poliisille luodaan taito, kyky ja riittävät oikeudelliset mahdollisuudet vaihtaa tietoja ja tehdä yhteistyötä eri lainvalvontaviranomaisten kanssa rikosten ennalta ehkäisemiseksi, paljastamiseksi ja selvittämiseksi. Poliisi panostaa tietoverkkorikollisuuden torjuntaan osana järjestäytyneen rikollisuuden torjuntaa. Poliisi kehittää ja vahvistaa kansallisia tietoverkkorikollisuuden torjuntamenetelmiä mm. lisäämällä eri poliisilaitosten yhteistyötä ja nopeita valmiuksia.

Keskusrikospoliisi pitää Poliisihallituksen määräyksen mukaisesti yllä tilannekuvaa kansainvälisestä ja järjestäytyneestä rikollisuudesta. Tämän lisäksi keskusrikospoliisi ylläpitää kokonaisrikollisuuden tilannekuvaa yhteistyössä paikallispoliisin kanssa. Tilannekuvan muodostamisessa hyödynnetään PTR -rikostiedustelu- ja analyysikeskusta. Suojelupoliisi ylläpitää toimialansa tilannekuvaa.

Poliisilla tulee olla osaava ja motivoitunut henkilöstö, joka hoitaa vaativien tietoverkkorikosten taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin oikeusvarmalla tavalla. Kyberrikollisuuden torjunnassa ja tutkinnassa tarvittavaa viranomaisten, syyttäjien ja tuomareiden osaamista parannetaan kehittämällä tarvittavaa alan koulutusta.

4.4 Kyberpuolustuskyky

Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

Kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Tavoitteena on, että suorituskyky mitoitetaan sellaiseksi, että se mahdollisimman tehokkaasti tukee puolustusvoimien toimintaa alueellisen koskemattomuuden turvaamiseksi ja maan puolustamiseksi. Kyberpuolustus toteutetaan kokonaisuutena, joka sisältää puolustusvoimien, muiden viranomaisten sekä yhteiskunnan muut suorituskyvyt.

Uskottava suorituskyky rakennetaan yhteistyössä muiden viranomaisten, yritysten sekä yliopistojen kanssa. Normaaliaikoina suorituskykyä kehitetään verkostoitumalla, tiedonvaihdolla, yhteisillä hankkeilla sekä osallistumalla kansallisiin ja kansainvälisiin työryhmiin ja harjoituksiin. Poikkeusoloissa tai erilaisissa häiriötilanteissa toiminnan perusratkaisut eivät muutu. Kyberuhkiin varaudutaan ja uhkia hallitaan kehittämällä ja ylläpitämällä erilaisia suojaus- ja vaikuttamiskeinoja ja lisäksi luodaan tarvittava toipumiskyky kyberhyökkäyksistä.

Kybervaikuttamista voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä sekä vakavassa kriisissä yhtenä vaikuttamiskeinona muiden perinteisten sotilaallisten voimakeinojen rinnalla. Puolustusvoimat suojaa omat järjestelmänsä ja verkkonsa sekä luo ja ylläpitää kykyä tiedusteluun ja vaikuttamiseen kybertoimintaympäristössä. Suorituskykyjen kehittäminen perustuu laadittuihin suorituskykyvaatimuksiin ja käytettävissä oleviin resursseihin.

Kyberuhkien syntyminen on kyettävä havaitsemaan ajoissa ja kybermaailman ilmiöitä ja tapahtumia on kyettävä seuraamaan reaaliajassa. Tämä edellyttää kybertilannekuvan muodostamista ennakkovaroituksen ja valmistautumisajan tuottamiseksi sekä vaikuttamisen toteuttamiseksi. Puolustusvoimien kybertilannekuvaa muodostettaessa toimitaan yhteistyössä perustettavan kansallisen Kyberturvallisuuskeskuksen kanssa.

Tiedustelun suorituskyvyillä tuotetaan tietoa kybertoimintaympäristön toimijoiden järjestelmien sekä verkkojen kokoonpanoista ja haavoittuvuuksista sekä arviota toimijoiden kyvyistä toteuttaa kyberoperaatioita. Kybertiedustelun tavoitteena on luoda suojautumisen ja vaikuttamisen edellyttämä tilannetietoisuus ja tiedustelutieto.

Kyberpuolustuksen suorituskykyä kehitetään kansallisella tasolla yhteistyössä muiden viranomaisten, elinkeinoelämän, tiedeyhteisön ja muiden toimijoiden kanssa. Kansallisen toiminnan koordinointi, yhteisen valtakunnallisen tilannekuvan muodostaminen sekä yhteistoiminnan edellytysten ylläpitäminen edellyttävät säännöllistä tiedonvaihtoa eri toimijoiden kesken.

Kansainvälistä kyberpuolustukseen liittyvää yhteistyötä tiivistetään edelleen keskeisten toimijoiden kanssa. Yhteistoiminta perustuu kahdenvälisiin sopimuksiin sekä monikansalliseen yhteistyöhön. Kansainvälisen yhteistoiminnan tavoitteena on mahdollistaa säännöllinen tiedonvaihto eri toimijoiden kesken erityisesti oman suorituskyvyn kehittämiseksi ja toimintamallien yhtenäistämiseksi.

Puolustusvoimat antaa kyberuhkien aiheuttamissa häiriötilanteissa virka-apua muille viranomaisille. Tarvittaessa puolustusvoimat saa tukea muilta viranomaisilta omia kyberpuolustustehtäviä toteuttaessaan. Puolustusvoimien kykyä tukea muita viranomaisia kyberhäiriötilanteissa kehitetään.

Kybersuorituskykyyn liittyvät toimintamahdollisuudet ja toimivaltuudet edellyttävät perusteellista jatkotarkastelua. Tässä työssä tulee arvioida olemassa olevan kansainvälisen oikeuden ja kansallisen sääntelyn soveltuvuus ja riittävyys sekä kyberpuolustuskyvyn edellyttämät mahdollisten säädösmuutosten tarpeet.

Puolustusvoimille luodaan maanpuolustus-, virka-apu-, aluevalvonta- sekä kriisinhallintatehtävien toteuttamiseksi tarpeelliset toimivaltuudet, osaaminen ja riittävät tiedonsaantioikeudet.

4.5 Kansainvälinen yhteistyö

Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.

Kyberturvallisuustoiminnassa toteutetaan kansallisella tasolla aktiivista eri toimijoiden välistä yhteistoimintaa tavoitteena jaettu tilannetietoisuus, tehokas häiriöiden hallinta ja uhkien torjunta. Kyberturvallisuuden laaja-alaisen luonteen vuoksi kansainvälisen yhteistyön merkitys korostuu entisestään. Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa.

Kyberturvallisuuden kansainvälistä yhteistyötä tehdään monella tasolla ja foorumilla, pohjoismaissa, Euroopan neuvostossa, Euroopan unionissa ja kansainvälisten organisaatioiden, kuten NATO, ETYJ ja YK, kesken. Kyberuhat ylittävät kansalliset rajat ja siksi kansainvälinen yhteistyö eri kansainvälisillä foorumeilla on välttämätöntä. Yhteistyö antaa mahdollisuuden vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä. Lisäksi toiminta antaa perusteita kansal-

lisen kyberturvallisuuden kehittämiseen osana globaalia kyberturvallisuutta sekä lisää kyberpuolustuksen yhteensopivuutta ja yhteen toimivuutta.

Yhteistyö jakaantuu toimintaan eri organisaatioiden kanssa sekä kahdenväliseen yhteistyöhön. Organisaatioiden osalta Euroopassa keskeisimmät kyberturvallisuuden toimijat ovat EU ja NATO, joiden kanssa kehitettävä yhteistyö on luonteeltaan ensisijaisesti tilannetiedon vaihtoa, yhteistyötä yhteisten suorituskykyjen kehittämisessä sekä koulutus- ja harjoitustoiminnassa.

Perinteinen pohjoismainen yhteistyö antaa mahdollisuuden myös kyberturvallisuuden edistämiseen. Vuoden 2009 ulkoministerikokouksessa sovittiin pohjoismaiden välisen kyberturvallisuusyhteistyön tiivistämisestä. Perustetun asiantuntijaryhmän suositusten mukaisesti on valmisteilla pohjoismainen viranomaisten yhteistyöverkosto ja sitä tukeva turvallinen tietoverkko.

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (ns. Budapestin sopimus) vuodelta 2001 on kaiken kyberrikollisuuden torjunnan kehittämisen perusta. Myös Euroopan unioni on Suomelle erittäin tärkeä foorumi kyberturvallisuutta kehitettäessä. EU valmistelee parhaillaan omaa kyberturvallisuusstrategiaa. Tällä hetkellä EU on keskittynyt ohjeissaan ja direktiiveissään tietoverkkorikollisuuden torjuntaan, kriittisen informaatioinfrastruktuurin suojelemiseen sekä sähköistä viestintää, tietoturvaa ja tietosuojaa koskevaan lainsäädäntötyöhön.

Suomi jatkaa kiinteää yhteistyötä eurooppalaisten yhteistyöorganisaatioiden kanssa, kuten Euroopan verkko- ja tietoturvavirasto (European Network and Information Security Agency, ENISA), Euroopan unionin poliisivirasto (Europol), Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (Body of European Regulators for Electronic Communications, BEREC), Euroopan kriittisen infrastruktuurin suojaamista käsittelevä jäsenvaltiofoorumi (European Forum for Member States, EFMS) sekä ICT-järjestelmien sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuuselin (European Public-Private Partnership for resilience, EP3R).

Kyberpuolustusta kehitettäessä yhteistyötä jatketaan EU:n Sotilasesikunnan (EUMS), Euroopan Puolustusviraston (EDA) ja NATO:n kanssa. NATO tulee tekemään yhteistyötä kumppanimaiden kanssa uusiin turvallisuushaasteisiin vastaamiseksi, NATO-johtoisten operaatioiden tukemiseksi sekä tilannetietoisuuden parantamiseksi.

Euroopan turvallisuus- ja yhteistyöjärjestö ETYJ:n piirissä pyritään kehittämään luottamusta lisääviä toimia kyberkonfliktien estämiseksi avoimuutta, yhteistyötä ja vakautta lisäten. Tavoitteena on, että työ täydentää muiden kansainvälisten järjestöjen työtä ja se perustuu ETYJ:n kokonaisvaltaiselle turvallisuuskäsitykselle.

YK:n tietoyhteiskunta-huippukokouksen (WSIS, World Summit on the Information Society) loppuasiakirjoissa jäsenmaat sitoutuvat kasvattamaan luottamusta ja turvallisuutta ICT:n käyttöä kohtaan. Suomi osallistuu YK-elimissä käytävään kyberturvallisuuskeskusteluun ja tukee WSIS-sitoumusten mukaisesti kaikkien toimijoiden välisen yhteistyön vahvistamista turvallisuu-

teen liittyvissä kysymyksissä. Kansainvälinen televiestintäliitto ITU edistää myös tätä tavoitetta Global Cybersecurity Agenda -aloitteellaan.

Taloudellisen yhteistyön ja kehityksen järjestö OECD:n piirissä tehtävä työ pyrkii kehittämään tai harmonisoimaan jäsenmaiden politiikkaa eri talous- ja yhteiskuntaelämän sektoreilla. Suomi osallistuu OECD:n yhteistyöhön tietoturvallisuutta ja yksityisyydensuojaa koskevissa ryhmissä. OECD toimii asiantuntija-organisaationa, joka tukee jäsenmaissa tehtävää talous- ja yhteiskuntapoliittista päätöksentekoa. OECD on laatinut suosituksia tietojärjestelmien ja -verkkojen turvallisuusperiaatteista sekä tehnyt vertailututkimusta jäsenmaiden kansallisista kyberturvallisuusstrategioista.

4.6 Tutkimuksen ja osaamisen kehittäminen sekä harjoitustoiminta

Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.

Tavoitteena on parantaa viranomaisten, elinkeinoelämän ja kansalaisten ymmärrystä, osaamista ja taitoja kyberturvallisuuden merkityksestä yhteiskunnan toiminnalle ja luoda vahva kansallinen kyberosaamisklusteri. Kyberturvallisuustutkimusta kehitetään osaksi kansallista huippututkimusta ja luodaan kyberturvallisuuden strateginen huippuosaamisen keskittymä osaksi jo olemassa olevia rakenteita. Harjoitustoiminnan tavoitteena on parantaa osallistujien mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kehittää suorituskykyjään ja kouluttaa henkilöstöään. Eri toimialojen valmiutta toimia elintärkeiden toimintojen häiriötilanteissa harjoitellaan säännöllisesti.

Kustannustehokkain tapa lisätä kansallista kyberturvallisuutta on osaamisen parantaminen. Viranomaisten, elinkeinoelämän ja kansalaisten tietoisuuden lisääminen kybertoimintaympäristön uhkista ja riskeistä parantaa kaikkien osaamista kyberturvallisuustoimenpiteiden toteuttamisessa. Alan huippututkimuksella luodaan perusta sekä osaamisen että kyberturvallisuusjärjestelmien kehittämiselle.

Suomen koulutusjärjestelmässä huolehditaan sellaisen korkean osaamisen tason säilymisestä ja kehittymisestä, jota hyödyntämällä voidaan turvata ja kehittää yhteiskunnan elintärkeiden toimintojen turvallisuutta kybertoimintaympäristössä. Kyberturvallisuuden perustietojen ja taitojen opiskelun tulee sisältyä kaikille opetustasoille. Kyberturvallisuuden oppisisältövaatimukset tulee sisällyttää yleissivistävään perusopetukseen (peruskoulu), ammatilliseen koulutukseen ja lukiokoulutukseen sekä korkea-asteen koulutukseen.

Kyberturvallisuuden perustutkimuksen, soveltavan tutkimuksen ja innovaatiotoiminnan edellytyksiä vahvistetaan yliopistoissa ja tuotekehitystyön edellytyksiä vahvistetaan ammattikorkeakouluissa. Kyberturvallisuuden tutkimuksen tasoa nostetaan ja tutkimusedellytykset turvataan, jotta kyetään jatkuvasti tuottamaan sekä perustutkimuksella että soveltavalla tutkimuksella korkeatasoisia uusia innovaatioita ja tieteellisiä läpimurtoja. Esimerkiksi krypto-osaamisen kehittymistä tuetaan, jotta Suomesta saadaan tuotteita ja palveluita niin kotimaiseen kuin kansainväliseenkin käyttöön.

Perustetaan olemassa olevan ICT-SHOKin (TIVIT) yhteyteen kyberturvallisuuden poikkitieteellinen strateginen huippuosaamisen keskittymä, joka tarjoaa huipputason tutkimusyksiköille ja tutkimustuloksia hyödyntäville yrityksille tehokkaan tavan tehdä tiivistä ja pitkäjänteistä yhteistyötä keskenään. Keskittymässä toteutetaan yritysten, yliopistojen ja tutkimuslaitosten yhdessä määrittelemää sovelluslähtöistä ja monitieteellistä tutkimusstrategiaa, jonka tulokset palvelevat kansallisen kyberturvallisuusstrategian toteuttamista ja kansainvälisen huippuosaamisen kehittymistä. Näillä toimilla tuetaan uuden kannattavan kansainvälisen kyberturvallisuusliiketoiminnan muodostumista.

Liiketoimintojen jatkuvan kehittämisen kannalta on välttämätöntä huolehtia korkean tason osaamisen säilymisestä maassamme. Osaamisen varmistamisella mahdollistetaan kansallinen kykymme hyödyntää kybertoimintaympäristöä. Elinkeinoelämän tarpeiden perusteella tulisi uudelleen kouluttaa vuoden 2013 aikana vähintään 100 henkilöä toimialalle yhdessä 1-2 eri oppilaitoksen kanssa. Siirtymäkoulutusta jatketaan samantasoisena useita vuosia. Lisätään mahdollisimman nopeasti kyber/tietoturvakursseja korkeakouluihin ja ammattikorkeakouluihin. Lisätään tietoturva-alan aloituspaikkoja alan koulutusta antavissa oppilaitoksissa sekä lisätään sivuainekursseja kyberturvallisuudesta. Perustetaan välittömästi kyberturvallisuuteen keskittyvä professuuri ja lisätään pidemmällä aikataululla kyberturvallisuuteen liittyvien professuurien määrää.

Kyberharjoituksista saadut havainnot ja kokemukset antavat konkreettista tietoa yhteiskunnan elintärkeiden toimintojen turvaamisesta ja tarvittavasta yhteistoiminnasta. Lisäksi saadaan tietoa hallinnonalojen ja organisaatioiden strategisten tehtävien edellyttämistä kehittämistarpeista sekä yhteiskunnan varautumisen ja kriisijohtamisvalmiuksien kokonaistilanteesta. Harjoitustoiminnalla testataan kyberturvallisuusstrategian periaatteita ja toimintamalleja sekä mitataan strategian toimeenpanoa.

Poikkeusoloihin ja normaaliolojen vakaviin häiriötilanteisiin varautumista tulee harjoitella säännöllisesti. Tämä antaa mahdollisuuden tehdä arvioita saavutetusta kyberturvallisuuden kehittymisestä Suomessa ja luoda jatkuvasti toimintaa parantavia toimenpiteitä. Kyberturvallisuusuhkat muuttuvat hyvin nopealla syklillä, minkä vuoksi kaiken kansallisen ja kansainvälisen harjoitustoiminnan tulee olla jatkuvaa ja hyvin organisoitua niin, että toiminta tukee tehokkaasti kansallista kyberturvallisuutta.

Tuloksellinen kyberharjoitustoiminta edellyttää suunnitelmallisuutta ja selkeitä johtamisvastuita. Laaja-alaisten valtakunnallisten kyberharjoitusten valmistelua ja toteuttamista koordinoidaan Yhteiskunnan turvallisuusstrategiassa määritettyjen periaatteiden mukaisesti. Kansallisen kyberturvallisuuden toteuttaminen edellyttää julkishallinnon ja yksityisen sektorin kiinteää yhteistoimintaa. Yhteiskunnan kokonaisvaltaisen valmiuden kehittämiseksi harjoitustoimintaan otetaan mukaan myös yhteiskunnan elintärkeiden toimintojen kannalta tärkeät yritykset ja kansalaisjärjestöt.

Julkisen hallinnon ja yksityisen sektorin kykyä kyberhäiriötilanteiden hallintaan harjoitellaan valtakunnallisissa kyberharjoituksissa, joissa testataan kyberturvallisuusstrategian uhkamalliin liittyvien häiriötilanteiden vaatimaa valmiutta sekä johtamisjärjestelyjen toimivuutta ja yhteistoimintajärjestelyjä. Harjoitusten aiheet sidotaan ajankohtaisiin kyberturvallisuusympäristön muutosten aiheuttamiin haasteisiin.

Osallistuminen kansainvälisiin, toiminnan monilla eri tasoilla toteutettaviin harjoituksiin tukee merkittävällä tavalla kansallista kyberturvallisuuden kehittämistä, alan osaamista ja toimintatapojen kehittämistä sekä kansainvälisen viranomaisyhteistyön ja asiantuntijayhteysverkoston luomista. Suomen tulee pyrkiä aktiivisesti vaikuttamaan jo harjoitusten suunnitteluvaiheessa harjoituksen rakenteeseen ja läpivientiin siten, että pääsemme harjoituksissa kehittämään kansallista osaamista ja testaamaan kansallisen kybertoimintaympäristömme vahvuuksia ja haavoittuvuuksia.

5. KYBERTURVALLISUUTTA KOSKEVA SÄÄNTELY

Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.
Kyberturvallisuudessa kysymys on oikeudellisesti uudesta ilmiöstä. Kyberuhkille on tyypillistä, että ne ovat valtioiden rajat ylittäviä. Toimijat kyberhyökkäysten takana voivat vaihdella ja niitä on haastava tunnistaa. Kyberhyökkäysten tekniikat ovat moninaisia ja nopeasti muuntuvia sekä kehittyviä. Kyberturvallisuus koskee kaikkia elämänaloja, hallinnonaloja ja yhteiskunnan perustoimintoja. Perus- ja ihmisoikeudet takaavat oikeuden yksityisyyden ja luottamuksellisen viestin suojaan. Kyberuhkatilanteeseen sovellettavan oikeudellisen normiston määrittää kyberuhan alkuperä ja toiminnan laatu.

5.1 Kyberturvallisuuteen liittyvä sääntely kansainvälisellä ja kansallisella tasolla

Yhdistyneet kansakunnat (YK) tunnisti 1990-luvulla tietotekniikan väärinkäytön valtioiden rajat ylittäväksi rikokseksi. YK on julkaissut päätöslauselmia taistelussa informaatioteknologian väärinkäyttöä vastaan ja suojattaessa kriittistä informaatioinfrastruktuuria.

Euroopan unionin piirissä on laadittu yleissopimuksia, puitepäätöksiä, direktiivejä, ehdotuksia ja tiedonantoja, jotka käsittelevät tietoverkkorikollisuutta ja sen torjuntaa, tietojärjestelmiin kohdistuvien hyökkäyksien torjuntayhteistyötä sekä kriittisen infrastruktuurin ja informaatioinfrastruktuurin suojaamista.

Yhtenäistä, kaikki kyberuhkatilanteet kattavaa valtioita sitovaa valtiosopimusta ei ole. Kansainvälisessä oikeudessa kyberuhan muodostavia tilanteita on käsitelty sirpaleisesti ja eri näkökulmista. Yksimielisyyttä ei ole myöskään saavutettu esimerkiksi siitä, mitä tarkoitetaan kyberhyökkäyksellä, kyberpuolustuksella tai kyberkonfliktilla/-selkkauksella. Asiakokonaisuutta koskeva oikeudellinen keskustelu kansainvälisellä tasolla on viime vuosina vilkastunut. Tämä tullee

johtamaan kyberuhkatilanteiden arviointia koskevien oikeudellisten tulkintojen luomiseen eri tahoilla valtioiden välillä tai kansainvälisissä yhteisöissä. Oletettavaa on, että nämä tulkinnat eivät ole valtioita oikeudellisesti sitovia, mutta osoittavat tavoitteita, joihin järjestelyissä mukana olevat valtiot ovat valmiita yhtymään.

Voimankäyttöä valtioiden välisissä suhteissa sääntelee YK:n peruskirja. Voimankäyttö on kielletty lukuun ottamatta itsepuolustusta aseellisen hyökkäyksen tilanteissa sekä osallistumista turvallisuusneuvoston valtuutuksella toimeenpantaviin aseellisiin pakotteisiin. Kansainvälisessä yhteisössä on parhaillaan käynnissä keskustelu ja tulkintojen muodostaminen siitä, voivatko kyberhyökkäykset joissakin tilanteissa ylittää YK:n peruskirjassa tarkoitetun aseellisen hyökkäyksen kynnyksen siten, että valtiolla olisi oikeus aseellisiin vastatoimiin. Suvereenisuudesta seuraa myös vastuu. Valtion on huolehdittava siitä, ettei sen aluetta käytetä hyökkäyksiin toista valtiota vastaan. Sen on siis omalla alueellaan pyrittävä estämään myös yksityisten tahojen tekemät hyökkäykset rajojensa ulkopuolelle. Kyberoperaatioita varten ei ole olemassa omaa voimankäyttönormistoa.

Kansallisessa lainsäädännössä ei ole kyberuhkia koskevaa yhtenäistä sääntelyä. Toimintaa tietoverkoissa sääntelevä normisto on hajanaista ja lähestyy kyberuhkatilanteita eri näkökulmista. Kansallisesti eri hallinnonalat määrittävät kyberuhkat omasta näkökulmastaan ja toimivaltuudet ovat hallinnonalakohtaisia, vaikka kybertoiminta sen luonteen takia yleensä ylittää hallinnonalat. Kyberuhan alkuperästä ja toiminnan laadusta riippuen sama toiminta voi tulla arvioitavaksi yksittäisenä rikosoikeudellisena tekona, laajempana terrorismirikoksena taikka valtion välisten suhteiden ja sotilaallisen puolustuksen näkökulmasta. Tämä vaikeuttaa kyberuhkatilanteen oikeudellista arviointia ja yhtenäisen kansallisen oikeudellisen tulkinnan luomista tilanteesta.

Kansallisella tasolla perustuslakimme määrää, että julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen maassamme. Perusoikeuksia on suojeltava myös tietoverkoissa. Kyberturvallisuuden lisääminen voi tehostaa esimerkiksi verkon käyttäjien yksityisyyden ja omaisuuden suojaa. Toimivien tietoverkkoyhteyksien voidaan katsoa edistävän myös kansalaisten sananvapauden toteutumista. Kyberturvallisuuteen liittyvää tarkempaa sääntelyä on rikoslain 34 luvussa, aluevalvontalaissa, valmiuslaissa, puolustustilalaissa ja puolustusvoimista annetussa laissa sekä viestintämarkkinalaissa ja sähköisen viestinnän tietosuojalaissa.

Valmiuslain tarkoittama viranomaisten varautumisvelvollisuus kyetä huolehtimaan tehtävistään hyvin kaikissa tilanteissa käsittää myös kybersuorituskykyjen kehittämisen. Valmiuslain mukaisten toimivaltuuksien käyttöönoton ja käytön keskeisenä soveltamisedellytyksenä on laissa säädettyjen poikkeusolojen olemassaolo. Lain perustelujen mukaan poikkeusolomääritelmään sisältyvässä vakavuudeltaan aseelliseen hyökkäykseen rinnastettavassa hyökkäyksessä voi kyse olla muustakin kuin perinteisin asein toteutetusta hyökkäyksestä. Esimerkiksi hyökkäys voi olla tietojärjestelmiin kohdistunut isku. Hyökkäys voi tarkoittaa myös ei-valtiollisen toimijan hyökkäystä silloin, kun hyökkäys on niin järjestäytynyt ja laaja, että se on verrattavissa valtion toteuttamaan hyökkäykseen.

5.2 Lainsäädännön kehittäminen

Suomi kansainvälisessä toiminnassaan tukee ja osallistuu kansainvälisen oikeuden piirissä tapahtuvaan tulkintojen muodostamiseen, joiden tarkoituksena on linjata eri valtioissa noudatettavat oikeusperiaatteet mahdollisimman yhdenmukaisiksi. Samalla tämä merkitsee sitä, että yksinomaan Suomen kansallisen lainsäädännön kehittäminen kyberuhkatilanteet kattavaksi ei ole riittävää. Suomi osallistuu aktiivisesti eri toimijoiden väliseen yhteistoimintaan, jossa keskeisiä tavoitteita ovat avoin tietojenvaihto, yhteisen oikeudellisen normiston luominen sekä eri toimijoiden vastuunjaosta sopiminen. Näin voidaan esimerkiksi rajoittaa tilanteita, joissa kansallisten lakien eroavaisuudet antavat rikollisille kybertoimijoille mahdollisuuden sijoittaa toimintansa itselleen sopiviin valtioihin.

Kansallista lainsäädäntöä tulee tarkastella niin, että siinä otetaan huomioon kyberturvallisuuteen liittyvä kansainvälinen oikeus ja EU-lainsäädäntö. Tässä työssä tulee selvittää eri hallinnonalojen kyberturvallisuuteen liittyvä sääntely, sen ajantasaisuus ja riittävyys, sekä kartoittaa mahdolliset lainsäädännön muutostarpeet. Lähtökohtana on, että yhteiskuntaa vaarantavan ja vahingoittavan kyberhäiriötilanteiden hallinnan edellyttämät toimivaltuudet sisältyvät viranomaisten normaaleihin toimivaltuuksiin. Perustuslaki säätää, että julkisen vallan perusteista ja toimivaltuuksista on säädettävä lailla.

Lainsäädäntöä tulee kehittää siten, että se ottaa huomioon nopeasti muuttuvat kybertoimintaympäristön ilmiöt ja antaa mahdollisuuden eri alojen toimivaltaisille viranomaisille toteuttaa niille määrättyjä tehtäviä, joilla turvataan valtion itsenäisyys, väestön elinmahdollisuudet ja turvallisuus yhteiskunnan elintärkeisiin toimintoihin kohdistuvia kyberuhkia vastaan. Kyberturvallisuutta on tarkasteltava erottamatta sitä muista turvallisuuteen liittyvistä elementeistä. Yhteiskunnan toiminnan kannalta keskeistä on lainsäädännössä löytää tasapaino viranomaisten ja elinkeinoelämän tilannetietoisuuden, vastuiden ja toimintatapojen välillä. Tässä tarkastelussa on otettava huomioon myös Suomen kansainvälisen kilpailukyvyn turvaaminen. Maassa vallitseva vakaa kyberturvallisuustilanne osaltaan mahdollistaa elinkeinotoiminnalle houkuttelevat toimintaedellytykset.

Valtion turvallisuutta vaarantavien kyberuhkien torjumiseksi otetaan tarkasteltavaksi mahdolliset lainsäädännölliset ja kansainvälisistä sopimuksista johtuvien velvoitteiden aiheuttamat esteet ja rajoitteet sekä tiedon käsittelyä koskevat velvoitteet, jotka haittaavat kyberuhkien tehokkaaksi torjumiseksi tarvittavan tiedon saamista, luovuttamista ja vaihtamista eri viranomaisten ja muiden toimijoiden välillä. Tietojen keräämistä ja muuta käsittelyä koskevassa tarkastelussa arvioidaan lisäksi sitä onko syytä vastuuviranomaisille luoda nykyistä paremmat mahdollisuudet ennalta kerätä, koota ja saada tietoa kyberuhista ja niiden aiheuttajista kiinnittämällä samalla huomiota perusoikeuksina olemassa oleviin yksityisyyden suojaan ja luottamuksellisen viestin suojaan.

Poliisitoiminnan osalta kysymys on erityisesti toimivaltuuksien saamisesta tiedusteluun ja tutkintaan kyberrikollisuuden ennaltaehkäisemiseksi, havaitsemiseksi ja torjumiseksi. Puolustusvoimien osalta lainsäädäntöä uudistettaessa tulee kybervaikutuskeinoja ja -tiedustelua koske-

via toimivaltasäännöksiä selkeyttää ja parantaa. Toimivaltuuksia mahdollisesti laajennettaessa tulee ottaa huomioon erityisesti ihmis- ja perusoikeudet ja niiden vaikutukset toimivaltuuskysymyksiin esimerkiksi tiedusteluoikeuksia lisättäessä.

6. KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO

6.1 Strategian toimeenpanon periaatteet

Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.

Yhteiskunnan kyberturvallisuus ja elintärkeiden toimintojen turvaaminen perustuvat ministeriöiden strategisiin tehtäviin ja huoltovarmuusjärjestelmän toimivuuteen kaikissa turvallisuustilanteissa. Kukin hallinnonala vastaa oman kyberriskianalyysinsa tekemisestä. Analyysiprosessin avulla tiedostetaan haavoittuvuudet ja tehdään kypsyysanalyysi. Prosessin tuloksena muodostuvat kunkin hallinnonalan toimeenpano-ohjelmat, joilla vastataan osoitettuihin tarpeisiin. Tarkemmassa suunnittelussa määritellään ne mittarit ja muut toimenpiteet, joita tarvitaan kyberturvallisuuden parantamiseksi. Toimijoiden varautumissuunnitelmat ja -järjestelyt on tarkistettava säännöllisesti ja aina kun yhteiskunnassa tai turvallisuusympäristössä tapahtuu olennaisia muutoksia. Perustettava Turvallisuuskomitea seuraa ja yhteen sovittaa strategian toimeenpanoa ja sen kehittämistä.

Jokaisella toimijalla tai yhteiskunnan sektorilla on myös omia erillisiä kyberturvallisuustehtäviä. Erityistehtävät syventävät Yhteiskunnan turvallisuusstrategian määrittelemiä strategisia tehtäviä, huoltovarmuustehtäviä ja toimialakohtaisia tehtäviä kyberturvallisuuden näkökulmasta.

Yhteiskunnan kyberturvallisuuden ylläpitäminen edellyttää oikeaa tietoa hallinnonalojen ja elinkeinoelämän valmiudesta ja toimintakyvystä sekä koko yhteiskunnan kriisinkestävyydestä ja -valmiudesta. Strategian toimeenpanon seurannan tulee mahdollistaa oikea-aikaiset ja -suuntaiset ylläpito- ja kehittämistoimenpiteet. Seurannalla tuotetaan valtionjohdolle ajantasaista tietoa siitä, onko voimavarat kohdennettu oikein kyberturvallisuusstrategian tavoitteiden mukaisesti.

Kyberturvallisuuden toteuttaminen edellyttää strategian periaatteiden johdonmukaista toimeenpanoa myös alueellisella ja paikallisella tasolla. Tämä edellyttää riittävää yhteistyötä eri toimijoiden välillä ja parhaiden käytänteiden hyödyntämistä.

Strategian toimeenpanon yhteistä seurantaa ja kehittämistä yhteensovitetaan perustettavassa Turvallisuuskomiteassa. Valtioneuvostolle laaditaan vuosittain raportti strategian toimeenpanon tilanteesta.

6.2 Toimeenpanon edellyttämiä toimenpiteitä

Ministeriöt seuraavat toimialalleen kuuluvien kyberturvallisuuteen liittyvien tehtävien sekä huoltovarmuusjärjestelyiden toteuttamista ja niiden kehittämistä. Seuranta toteutetaan osana hallinnonalojen vakiintuneita käytäntöjä.

Kyberturvallisuuskeskus tuottaa yhteistyössä verkostonsa kanssa eri viranomaisille säännöllisesti raportin kyberturvallisuusympäristön tapahtumista. Keskus laatii vuosittain yhteistyössä verkoston kanssa raportin, jossa käsitellään ainakin seuraavia kokonaisuuksia:

- tapahtuneiden häiriötilanteiden hallinta ja niistä saadut kokemukset, analyysit ja taloudelliset vaikutukset yhteiskunnan elintärkeille toiminnoille,
- arviot varautumisjärjestelyiden toimivuudesta ja kehittämistarpeista,
- kokemuksia hallinnonalojen, valtioneuvoston ja valtakunnallisista kybervalmiusharjoituksista,
- toiminnan ja osaamisen kehittäminen sekä resursointi.

Kyberhäiriötilanteiden hallinnassa on tärkeää, että häiriötilanteen hallitsemiseksi käynnistetyt toimenpiteet kirjataan ja analysoidaan mahdollisimman kattavasti. Myös niin sanottujen ”läheltä piti” -tilanteiden analysointi on liitettävä osaksi tätä seurantaa, erityisesti uhkien ja riskien ennaltaehkäisemiseksi. Tilanteista saadut opit ja niistä aiheutuneet toimenpiteet käsitellään eri yhteistyöelimissä parhaiden käytänteiden hyödyntämisen varmistamiseksi.

Kyberharjoituksista saadut havainnot ja kokemukset antavat konkreettista tietoa yhteiskunnan elintärkeiden toimintojen turvaamisesta ja tarvittavasta yhteistoiminnasta. Lisäksi saadaan tietoa hallinnonalojen ja organisaatioiden strategisten tehtävien edellyttämistä kehittämistarpeista sekä yhteiskunnan varautumisen ja kriisijohtamisvalmiuksien kokonaistilanteesta. Harjoitustoiminnalla testataan kyberturvallisuusstrategian periaatteita ja toimintamalleja sekä arvioidaan strategian toimeenpanoa.

Strategian toimeenpanon seuranta tuottaa myös perusteita ja vaatimuksia kyberturvallisuustutkimukselle ja sen kansalliselle yhteistyölle. Kansallista ja kansainvälistä turvallisuustutkimusta toteutetaan ja yhteistyömuotoja kehitetään Kansallisen turvallisuustutkimuksen strategian (2009) periaatteiden mukaisesti. Kyberturvallisuusstrategiaa tukevaa tutkimusta tuotetaan eri tutkimusyksiköissä ja -laitoksissa sekä yliopistojen ja korkeakoulujen tutkimusohjelmissa.

Kyberstrategian ylläpito ja kehittäminen perustuvat jatkuvan kehittämisen prosessiin. Kyberturvallisuusstrategia käsitellään perustettavassa Turvallisuuskomiteassa vuosittain. Tällä varmistetaan strategian ajantasaisuus ja toimenpiteiden eteneminen. Prosessissa tehdyn arvion ja analyysin perusteella tehdään mahdolliset strategian ja toimeenpano-ohjelman päivitykset. Kyberturvallisuusstrategian keskeiset osat sisällytetään yhteiskunnan turvallisuusstrategiaan kun se seuraavan kerran päivitetään.

6.3 Toimenpiteiden resursointi

Ministeriöt, virastot ja laitokset sisällyttävät kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa. Eduskunta antaa eri ministeriöille määrärahakehykset, joihin sisällytetään kyberturvallisuustoimenpiteiden edellyttämät resurssit. Ministeriöt suunnittelevat resurssitarpeensa osana omia toimeenpano-ohjelmiaan. Yritykset ottavat kyberturvallisuuden edellyttämät toimenpiteet huomioon tehdessään päätöksiään omista budjeteistaan ja resursoinneistaan.

Edellä mainitut toimijat ovat yhteistyössä perustettavan Kyberturvallisuuskeskuksen kanssa muodostaen tiiviin verkoston. Perustettava keskus hyödyntää verkostossa olevaa osaamista, mikä vaikuttaa myös sen omaan resursointiin. Kyberturvallisuuskeskuksen rakentamiseen ja toimintaan osoitetaan erillinen lisämääräraha, jonka suuruus suunnitellaan osana yhteistä toimeenpanosuunnitelmaa. Kyberturvallisuuskeskukselle luodaan 24/7 toimintakyky, mikä alustavan arvion mukaan edellyttää noin kymmenen henkilötyövuoden ja ainakin miljoonan euron lisäresursseja.

6.4 Toimeenpano-ohjelma ja tuloksellisuuden mittaaminen

Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Kyberturvallisuusstrategian 1. vaiheen toimeenpano toteutetaan vuosina 2013–2015, jona aikana laaditaan yksityiskohtaiset kyberturvallisuuden varautumis- ja kehittämissuunnitelmat, jotta saavutetaan 2016 mennessä hallitusohjelman tavoite, että Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä. Vuodesta 2016 kyberturvallisuusstrategiaa toteutetaan jatkuvan parantamisen periaatteen mukaisesti. Kyberturvallisuuden edellyttämä budjetointi toteutetaan hallinnonaloittain voimassa olevan toimintamallin mukaisesti.

Toimeenpano-ohjelman pääkohtia ovat Kyberturvallisuuskeskuksen perustaminen, toimenpiteet ministeriöiden strategisten tavoitteiden saavuttamiseksi ja tarvittavat säädösmuutokset. Osana toimeenpano-ohjelmaa kehitetään kyberturvallisuuden kypsyysmalli, jolla voidaan mitata toiminnan tasoa ja kehittymistä.

LIITE
KYBERTURVALLISUUSSTRATEGIAN JATKUVAN KEHITTÄMISEN PROSESSI

Kansallisen kyberstrategiaprosessin tavoitteena on aikaansaada jatkuvan parantamisen toimintatapamalli, jolloin kyberturvallisuustoimenpiteitä toteutetaan tulevaisuudessa tehokkaammin ja vaikuttavammin. Strategiaprosessi ilmentyy monella tasolla ja se sisältää eri vaiheita. Tavoitteena on luoda jatkuva strategiaprosessi, jossa prosessin osia toistetaan säännöllisesti ja luodaan jatkuvaa toiminnan kehittymistä.

Kyberturvallisuusprosessi (liitteen kuvio 1) sisältää viisi vaihetta:

Analyysivaihe

Strategian analyysivaiheessa määritellään oma asemamme, toisin sanoen missä tilassa olemme suhteessa toimintaympäristöön ja sen eri elementteihin. Kyberstrategiassa tämä tarkoittaa kyberuhkaympäristön analyysiä ja yhteiskunnan elintärkeiden toimintojen haavoittuvuuksien tunnistamista sekä tästä kokonaisuudesta aiheutuvien riskien arvioimista. Lisäksi arvioidaan omat suorituskyvyt ja niiden puutteet.

Toimintaympäristön analyysissä tunnistetaan kybertoimintaympäristön ilmiöt ja tehdään strategiaa varten tarvittavat määrittelyt sekä tunnistetaan olemassa olevat kansalliset kyberturvallisuushankkeet ja niitä sivuavat hankkeet ja projektit.

Benchmarking -menetelmällä hankitaan tietoja muiden maiden kyberturvallisuusstrategioista ja tunnistetaan niistä itselle sopivia parhaita käytäntöjä.

Analyysivaiheen lopputuloksena syntyy näkemys, joka asemoi meidät kansalliseen ja kansainväliseen kybertoimintaympäristöön ja antaa jatkotyöskentelylle perusteet määrittelyjen ja selvitystehtävien muodossa.

Suunnitteluvaihe

Suunnitteluvaiheessa määritellään kyberturvallisuuden visio, kansalliset periaatteet ja kyberturvallisuuskonsepti. Suunnitteluprosessissa otetaan huomioon suorituskykyvaatimukset, käytettävissä olevat taloudelliset resurssit ja osaaminen. Tavoitetilaan pääsemisestä laaditaan vaihtoehtoisia suunnitelmia.

Päätösvaihe

Päätösvaiheessa vertaillaan eri vaihtoehtoja ja valitaan eri vaihtoehdoista haluttu tavoitetila sekä kansallinen toimintakonsepti ja toimenpiteet sen saavuttamiseksi. Lisäksi määritellään halutut kybersuorituskyvyt ja toimenpiteet niiden luomiseksi.

Tuottamisvaihe

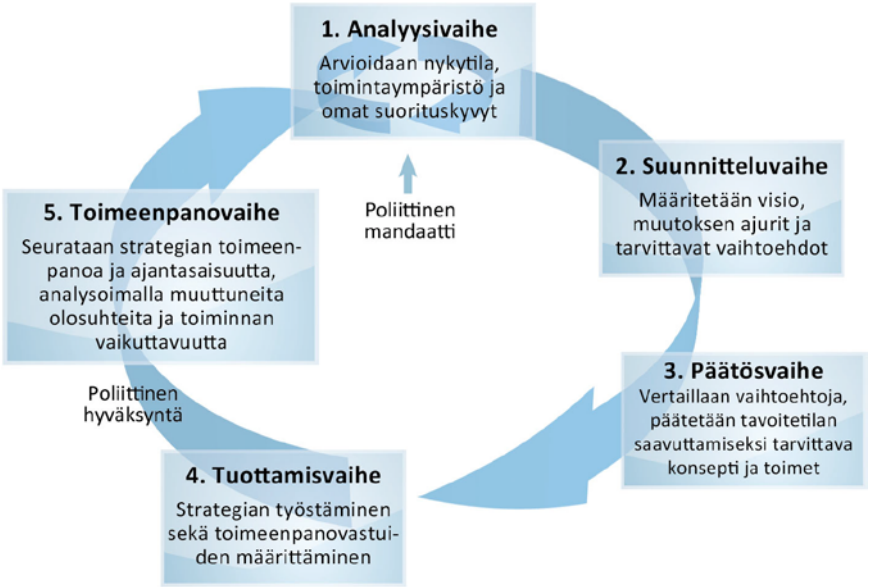
Tuottamisvaiheessa määritellään kyberturvallisuusstrategian rakenne, asioiden esittämistapa ja kyberturvallisuuden konkreettiset tavoitteet ja vastuut. Tuottamisvaiheessa on useita iteraatiokierroksia ja väliesittelyin varmistetaan strategisen päätöksen ilmentyminen laaditussa tekstissä. Strategian laadinta päättyy strategian esittelyyn toimeksiantajalle ja sen hyväksymiseen.

Toimeenpanovaihe

Strategiaprosessin aikaisemmat vaiheet ovat tuottaneet hyväksytyn strategia-asiakirjan, johon sisältyy myös sen toimeenpanosuunnitelma ja suunnitelma siitä, kuinka strategiaprosessi pidetään jatkuvasti kehittyvänä. Toimeenpanovaiheessa strategia viedään käytäntöön siten, että strategiassa esitetyt toimenpide-esitykset jalkautetaan käytännön toimiksi hallinnon ja organisaatioiden eri tasoille. Muutoksen johtamista varten luodaan kyberturvallisuuden kypsyyden mittaus- ja seurantajärjestelmä, jolla toimeenpanon onnistumista voidaan seurata. Toimeenpanon toteuttamisesta seuraa perustettava Turvallisuuskomitea ja laaditaan vuosiraportti valtioneuvostolle.

Toimeenpanovaiheessa seurataan kybertoimintaympäristön kehitystä ja tarvittaessa tuetaan hallinnonaloja niiden toteuttaessa strategian periaatteita. Tavoitteena on ylläpitää kybertoimintaympäristöstä ja sen muutoksista kokonaisvaltaista tilannekuvaa sekä seurata vastatoimenpiteiden edellyttämien suorituskykyjen kehittymistä. Voimavarojen allokointi on tärkeä osa strategian toimeenpanoa. Toiminnan tuloksellisuus ja vaikuttavuus ovat suoraan riippuvaisia käytettävistä taloudellisista ja henkisistä voimavaroista. Hallituksen budjettiohjauksella luodaan kehykset kyberturvallisuuden resursoinnille. Vastuulliset hallintoyksiköt oman budjettivaltansa mukaisesti allokoivat voimavaroja kyberturvallisuuden käytännön toteuttamiseen kuten esimerkiksi tilannekuvan luomiseen, varautumiseen, tutkimukseen ja kehittämiseen sekä koulutukseen.

Kyberturvallisuusprosessi edustaa jatkuvan kehittämisen mallia, jossa seurataan muuttuvia olosuhteita ja toiminnan vaikuttavuutta ja niiden perusteella tehdään analyysejä ja tarvittaessa päivitetään strategiaa.



LIITTEEN KUVIO 1 Kyberturvallisuuden jatkuvan kehittämisen prosessi