Turvallisuus- ja puolustusasiain komitea
Säkerhets- och försvarskommittén
The Security and Defence Committee

SAATE

1 (1)

24.1.2013

FI.PLM.2013-451
429/80.01.99/2011

UTP – 2/2013 vp

Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta

Ohessa lähetetään Valtioneuvoston yleisistunnossaan 24.1.2013 hyväksymä periaatepäätös Suomen kyberturvallisuusstrategiasta.

Puheenjohtaja
Kansliapäällikkö
Arto Räty

Liitteet — Valtioneuvoston periaatepäätös 24.1.2013: Suomen kyberturvallisuusstrategia
Statsrådets principbeslut 24.1.2013: Strategi för cybersäkerheten i Finland

Jakelu — Eduskunnan puolustusvaliokunta
Eduskunnan ulkoasiainvaliokunta

Tiedoksi — -

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

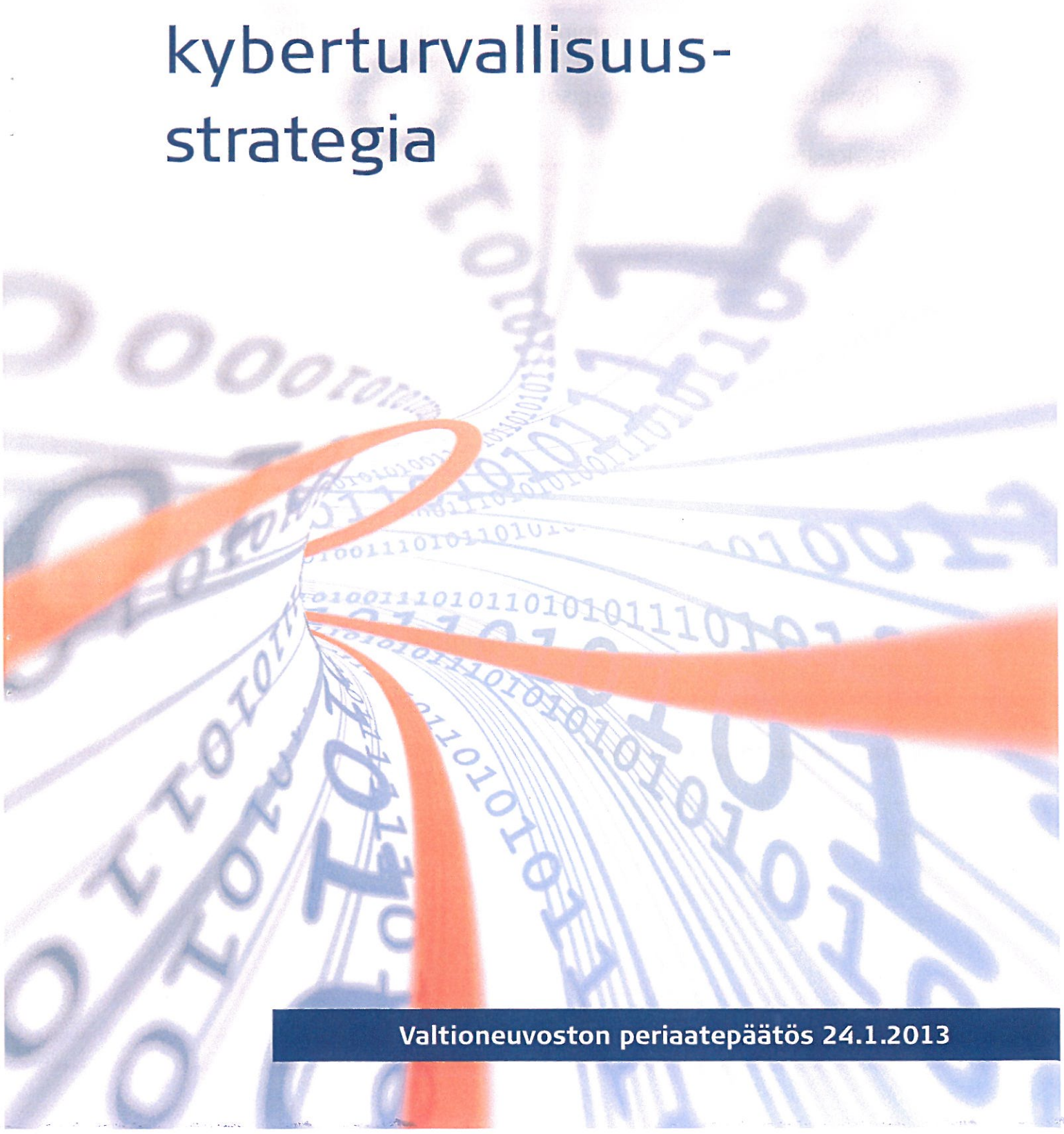
Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tpak@defmin.fi
www.defmin.fi

Suomen kyberturvallisuus-strategia



Valtioneuvoston periaatepäätös 24.1.2013

Sisällys

Turvallisuus- ja puolustusasiain komitean sihteeristö
Eteläinen Makasiinikatu 8
PL 31, 00131 HELSINKI

www.yhteiskunnanturvallisuus.fi

Taitto: Tiina Takala/puolustusministeriö
Paino: Forssa print, 2013

ISBN: 978-951-25-2433-4 nid.
ISBN: 978-951-25-2434-1 pdf

1. JOHDANTO

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoiminta-ympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä, ja yhteiskuntamme elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö.

Yhteiskunnan lisääntynyt tietointensiivisyys, ulkomaisen omistuksen kasvu ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi normaalioloissa, normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa.

Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi yksittäisten ihmisten, yritysten sekä koko yhteiskunnan kannalta. Uhkia muodostavat toimijat ovat ammattimaisempia kuin ennen ja nykyään niihin voidaan laskea kuuluviksi myös valtiolliset toimijat. Kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.

Kybertoimintaympäristö tulee nähdä myös mahdollisuutena ja voimavarana. Turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä lisää taloudellista aktiviteettia. Hyvä toimintaympäristö parantaa myös Suomen kansainvälistä houkuttelevuutta investointikohteena. Näiden lisäksi kyberturvallisuus on itsessään uusi ja vahvistuva liiketoiminnan alue. Kansallinen kyberturvallisuus ja suomalaisten yritysten menestys ovat yhteydessä keskenään.

Tässä strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. Kyberturvallisuusstrategian linjausten ja niiden toteuttamiseksi tarvittavien toimenpiteiden avulla Suomi kykenee kansallisesti hallitsemaan kybertoimintaympäristön tahallisia tai tahattomia haittavaikutuksia sekä vastaamaan ja toipumaan niistä.

Kokonaisturvallisuuden järjestelyt on kuvattu valtioneuvoston 5.12.2012 antamassa periaatepäätöksessä kokonaisturvallisuudesta. Yhteiskunnan elintärkeiden toimintojen turvaamisen periaatteet on kuvattu Yhteiskunnan turvallisuusstrategiassa (2010). Elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys. Kyberturvallisuusstrategiaprosessi on osa Yhteiskunnan turvallisuusstrategian toimeenpanoa. Kyberturvallisuusstrategia noudattaa yhteiskunnan turvallisuusstrategiassa olevia periaatteita ja määritelmiä sekä valtioneuvoston päätöstä huoltovarmuuden tavoitteista. Huoltovarmuuden turvaamisen painopisteet ja tavoitteet määritellään valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (2013). Strategiassa on otettu huomioon periaatepäätös kokonaisturvallisuuden järjestelyistä.

Kyberturvallisuus ei ole tarkoitettu oikeudelliseksi käsitteeksi, joka perustaisi uusia toimivaltuuksia viranomaisille tai muille toimielimille. Tältä osin ei ehdoteta muutoksia varautumisjärjestelyjen perusteisiin, eikä eri viranomaisten toimivaltamäärittelyihin.

Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Valmisteltava toimeenpano-ohjelma tulee sisältämään hallinnonalojen ja toimijoiden valmisteluvastuulle tulevat käytännön toimenpiteet, joilla luodaan edellytykset strategisten linjausten toteutumiseksi sekä vision kuvaamaan tavoitetilaan pääsemiseksi mukaan lukien yhdessä sovitut poikkiyhteiskunnalliset toimenpiteet.

2. KYBERTURVALLISUUDEN VISIO

Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Meillä on vahva osaamisperusta sekä pitkät perinteet tiivistä ja luottamuksellisesta yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojen välisestä yhteistyöstä.

Suomen kyberturvallisuuden visiona on, että:

- Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.
- Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.
- Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

KUVIO 1 Kyberturvallisuuden visio

3. KYBERTURVALLISUUDEN JOHTAMINEN JA KANSALLINEN KOORDINAATIO

Toimintamalli

Kybertoimintaympäristössä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan vaikeasti ennakoitavia. Informaatioteknologian kehityssykli on lyhyt ja sama trendi koskee eri kyberhyökkäysmuotoja ja haittaohjelmia. Tämä asettaa kasvavan haasteen yhteiskunnan kyvylle varautua erilaisiin kyberuhkiin. Kyberuhkiin varautuminen ja niiden torjuminen edellyttää yhteiskunnan kaikilta osapuolilta entistä nopeampaa, läpinäkyvämpää ja paremmin koordinoitua toimintaa, sekä erikseen että yhdessä.

Kyberturvallisuuden johtamisen ylimmän tason muodostaa Valtioneuvosto. Valtioneuvoston tehtävänä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen.

Kyberturvallisuuden johtaminen ja häiriötilanteiden hallinta edellyttävät, että valtioneuvostolla ja eri toimijoilla on käytettävissään luotettava ja ajantasainen kyberturvallisuuden tilannekuva yhteiskunnan elintärkeiden toimintojen tilasta ja niihin kohdistuvista häiriöistä. Kukin ministeriö ja hallinnonala vastaavat kyberturvallisuudesta ja siihen liittyvien häiriötilanteiden hallinnasta. Kybertoimintaympäristö ja uhkien luonne korostavat yhteistyötä ja varautumisen yhteensovittamistoimenpiteiden tehokkuutta ja joustavuutta. Ministeriöiden kyberturvallisuuden strategiset tehtävät ja niihin liittyvät kehittämistarpeet perustuvat tunnistettujen kyberuhkien analysointiin ja niistä muodostettujen häiriötilanteiden hallinnan asettamiin vaatimuksiin. Kunkin ministeriön tulee toimivaltansa mukaisesti huolehtia siitä, että tavoitetilojen perusteella määritetyt strategiset tehtävät toteutetaan.

Kansallinen kyberuhkien sietokyky (kyberresilienssi) mitoitetaan siten, että sillä kyetään luomaan kokonaisturvallisuuden päämäärien mukainen varautumis- ja ennakointikyky, toimintakyky kyberhäiriötilanteissa sekä kyberhäiriöiden jälkeinen toipumis- ja palautumiskyky.

Suomen kyberturvallisuuden toimintamalli rakentuu seuraavien periaatteiden varaan:

1. Kyberturvallisuuden asiat kuuluvat pääsääntöisesti valtioneuvoston toimivaltaan siten, että tehtävät on säädetty eri ministeriöiden toimialalle. Kukin ministeriö vastaa toimialallaan valtioneuvostolle kuuluvien, kyberturvallisuuteen liittyvien asioiden valmistelusta ja hallinnon asianmukaisesta järjestämisestä.

2. Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS) määritettyjä periaatteita ja toimintatapoja.

3. Kyberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin. Kyberturvallisuuden edellytys on jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut. Näiden toteuttamista edesautetaan ja tuetaan erilaisten yhteistoimintaan perustuvien rakenteiden ja harjoitusten avulla.

4. Kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa. Tämä edellyttää kansallisen Kyberturvallisuuskeskuksen perustamista sekä koko yhteiskunnan ympärivuorokautisen tietoturvatoiminnan kehittämistä.

5. Kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Tarve sopeutua nopeisiin muutoksiin, kyky hyödyntää uusia mahdollisuuksia ja reagoida yllättäviin tilanteisiin vaatii toimijoilta strategisen ketteryyden periaatteiden ymmärtämistä ja noudattamista kyberturvallisuuteen tähtäävien toimien kehittämisessä ja johtamisessa.

6. Kyberturvallisuutta rakennetaan toiminnallisten ja teknisten vaatimusten perusteella. Kansallisten toimenpiteiden lisäksi panostetaan kansainväliseen yhteistoimintaan ja osallistutaan kansainväliseen tutkimus- ja kehittämistoimintaan sekä harjoitustoimintaan. Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana.

7. Kyberturvallisuuden kehittämisessä panostetaan voimakkaasti kybertoimintaympäristön tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista.

8. Kyberturvallisuuskehityksen varmistamiseksi huolehditaan siitä, että Suomessa on voimassa sellainen lainsäädäntö ja kannustimet, jotka tukevat tämän alueen yritystoimintaa ja sen kehittymistä. Alan osaaminen kehittyy keskeiseltä osaltaan yritystoiminnan kautta.

4. KYBERTURVALLISUUDEN STRATEGISET LINJAUKSET

Kansallista kyberturvallisuutta kehitetään strategisten linjausten mukaisesti. Niillä luodaan edellytykset kyberturvallisuuden kansallisen vision toteutumiselle. Erikseen laadittavassa toimeenpano-ohjelmassa määritetään ne toimenpiteet, joilla varmistetaan kansallisten kyberturvallisuustavoitteiden toteutuminen. Toimeenpano-ohjelma koostuu eri toimijoiden ja hallinnonalojen laatimista suunnitelmista sekä niiden pohjalta laadittavista poikkihallinnollisista toimenpiteistä.

Strategisten linjausten toimeenpanolla vahvistetaan suomalaisen turvallisuusyhteistyön vahvuudeksi koettua julkisen ja yksityisen sektorin välistä yhteistoimintaa. Tämän yhteistyön avulla voidaan parhaiten palvella koko yhteiskuntaa ja tukea sen elintärkeitä toimintoja tuottavia toimijoita. Päämääränä on huolehtia eri toimintojen häiriöttömästä ja turvallisesta jatkumisesta arjessa ja häiriötilanteissa.

Kyberturvallisuus perustuu pitkäjänteiseen ja riittävään suorituskykyjen kehittämiseen, niiden oikea-aikaiseen ja joustavaan käyttöön sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden häiriötilanteita. Viranomaisten kyberturvallisuuden suorituskykyä kehitetään toimivaltaisten ministeriöiden johdolla ja esimerkiksi määrittämällä ministeriöiden strategiset kyberturvallisuuden tehtävät. Useimpien strategisten kyberturvallisuustehtävien ja niihin liittyvien suorituskykyjen kehittämiseen liittyy myös muiden ministeriöiden, alue- ja paikallishallinnon, elinkeinoelämän sekä järjestöjen toimenpiteitä ja resursointia. Suorituskykyjen kehittämisessä ja käytössä ministeriöiden on aina otettava huomioon hallinnon eri tasot sekä elinkeinoelämän ja järjestöjen rooli. Kokonaisturvallisuuden alalla toimivaksi, varautumisen pysyväksi yhteistoimintaelimeksi perustetaan Turvallisuuskomitea, jonka tehtävistä säädetään erikseen.

STRATEGISET LINJAUKSET:

1	**Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.** Kyberturvallisuusstrategian strategisia linjauksia edistetään lisäämällä toimijoiden välistä aktiivista yhteistoimintaa, jonka tavoitteena on jaettu tilannetietoisuus ja tehokas uhkien torjunta. Eri toimialojen valmiutta toimia elintärkeiden toimintojen häiriötilanteissa harjoitellaan säännöllisesti. Jokainen toimija kehittää kansallista ja kansainvälistä osallistumista harjoitustoimintaan. Toimijat parantavat kansainvälisissä harjoituksissa parhaiden käytänteiden ja saatujen oppien hyödyntämistä tehostamalla tiedonvaihtoa ja koordinaatiota. Harjoitustoiminnan tavoitteena on parantaa osallistujien mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kehittää suorituskykyjään ja kouluttaa henkilöstöään. Kyberuhkien torjumiseksi tiedonvaihtoa viranomaisten ja elinkeinoelämän kesken edistetään kehittämällä sääntelyä ja yhteistyötä.
2	**Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.** Tavoitteena on parantaa eri toimijoiden tilannetietoisuutta tarjoamalla niille ajantasaista, koottua ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Tilannekuvaan sisältyy kybertoimintaympäristöstä aiheutuvien uhkien arviot ja ennusteet. Kyberuhkien ennakointi edellyttää poliittisen, sotilaallisen, sosiaalisen, kulttuurisen, teknisen ja teknologisen sekä taloudellisen tilanteen arviointia. Yhdistetyn kyberturvallisuuden tilannekuvan tuottamiseksi ja ylläpitämiseksi perustetaan Kyberturvallisuuskeskus, joka toimii osana Viestintävirastoa. Kyberturvallisuuskeskus kerää tietoa kybertapahtumista ja välittää sitä eri toimijoille. Toimijat arvioivat häiriön vaikutuksia vastuullaan olevaan toimintaan. Nämä analyysit välitetään takaisin keskukselle ja sisällytetään muodostettavaan kyberturvallisuuden yhdistettyyn tilannekuvaan. Tämä koonnos jaetaan päätöksenteon pohjaksi eri toimijoille. Valtioneuvoston tilannekeskuksella tulee olla käytettävissään luotettava, kattava ja ajantasainen kokonaistilannearvio kyberturvallisuudesta. Arvio koostuu Kyberturvallisuuskeskuksen yhdistetystä tilannekuvasta sekä hallinnonalojen arvioista kybertapahtumien vaikutuksista yhteiskunnan elintärkeille toiminnoille. Valtionjohdolla on käytettävissään kokonaistilannearvio sekä arvio muun toimintaympäristön kehityksestä.

3	**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.** Yhteiskunnan elintärkeiden toimintojen kannalta keskeiset yritykset ja organisaatiot ottavat turvallisuus- ja valmiussuunnittelussaan sekä niihin liittyvissä palvelurakenteissa kattavasti huomioon yhteiskunnan elintärkeisiin toimintoihin liittyvät kyberuhkatekijät ja pitävät yllä tarvittavaa suojautumiskykyä. Tavoitteena on, että riskiarvioissa esiin tulleet elintärkeiden toimintojen mahdolliset häiriöt tunnistetaan ja havaitaan, ja niihin reagoidaan tavalla, joka minimoi häiriöiden haitalliset vaikutukset. Keskeiset toimijat kehittävät sietokykyään, mukaan lukien varamenetelmien suunnittelu ja harjoittelu niin, että ne voivat toimia kyberhyökkäysten alaisena. Huoltovarmuusorganisaatio tukee toimintaa selvityksin, ohjeistuksin ja koulutuksella.
4	**Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.** Kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten esitutkintaviranomaisena toimii poliisi. Poliisi kokoaa analysoidun ja korkealaatuisen tilannekuvan kyberrikollisuudesta ja jakaa sen osaksi strategisessa linjauksessa 2 kuvattua yhdistettyä tilannekuvaa. Poliisi toimii tiiviissä yhteistyössä Kyberturvallisuuskeskuksen kanssa. Huolehditaan, että poliisilla on riittävät toimivaltuudet, resurssit sekä osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin. Jatketaan ja syvennetään kansainvälistä operatiivista yhteistyötä ja tiedonvaihtoa EU:n ja muiden maiden lainvalvontaviranomaisten ja vastaavien toimijoiden kuten Europolin kanssa.
5	**Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.** Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Puolustusvoimat suojaa omat järjestelmänsä siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään huolimatta kybertoimintaympäristön uhkista. Suorituskyvyn varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä. Edellä mainittujen tehtävien täyttämiseksi laaditaan puolustusministeriön johdolla puolustusvoimille tarvittava toimivaltuussäännöstö. Tunnistetut puutteet toimivaltuussäädöksissä korjataan lainsäädäntötoimenpitein. Kyberpuolustusta harjoitellaan ja kehitetään yhdessä keskeisten viranomaisten, järjestöjen ja elinkeinoelämän toimijoiden kanssa kansallisesti ja kansainvälisesti. Puolustusvoimat antaa virka-apua lainsäädännön salliessa.

6	**Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.** Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa. Varautumisen ja muun kyberturvallisuuden toteuttaminen jää vaillinaiseksi ilman tehokasta ja järjestelmällisesti koordinoitua kansainvälistä yhteistyötä. Jokainen viranomainen omalla toimialallaan harjoittaa yhteistyötä erityisesti niiden valtioiden ja organisaatioiden kanssa, jotka ovat maailmanlaajuisesti edelläkävijöitä kyberturvallisuuteen liittyvissä asiakokonaisuuksissa. Aktiivista yhteistyötä tehdään tutkimus- ja kehittämistyön, erilaisten sopimusten valmistelutyön, organisaatioiden työryhmätyöskentelyn, sekä kansainväliseen harjoitustoimintaan osallistumisen kautta. Euroopan unioni sekä monet kansainväliset järjestöt, kuten YK, ETYJ,-Nato-ja OECD, ovat Suomelle tärkeitä foorumeita kyberturvallisuutta kehitettäessä. EU toimii yhä aktiivisemmin kyberturvallisuuden alalla ja sillä on myös yhteistyötä kolmansien maiden kanssa. Suomi osallistuu aktiivisesti tähän kehittämistyöhön.
7	**Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.** Yhteiskunnan toimijoiden jatkuvan osaamisen ja tietämyksen kehittämisen tukena panostetaan yhteisten kyberturvallisuuden ja tietoturvallisuuden ohjeistojen kehittämiseen, hyödyntämiseen ja kouluttamiseen. Yhteiskunnan kokonaisvaltaisen valmiuden kehittämiseksi harjoitustoimintaan otetaan mukaan myös yhteiskunnan elintärkeiden toimintojen kannalta tärkeät yritykset ja kansalaisjärjestöt. Perustetaan olemassa olevan ICT-SHOKin (TIVIT) yhteyteen kyberturvallisuuden strateginen huippuosaamisen keskittymä, joka tarjoaa tutkimusyksiköille ja tutkimustuloksia hyödyntäville yrityksille tehokkaan tavan tehdä tiivistä ja pitkäjänteistä yhteistyötä keskenään. Keskittymä luo edellytyksiä vahvan kansallisen kyberosaamisklusterin rakentumiselle. Lisätään panostuksia tutkimukseen, tuotekehitykseen ja koulutukseen sekä toimenpiteitä kyberturvallisuuden osaamisen kehittämiseksi koko yhteiskunnan osalta.

8 Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.

Kartoitetaan kybertoimintaympäristöön ja -turvallisuuteen vaikuttava ja liittyvä lainsäädäntö sekä sen kehittämistarpeet hallinnonalojen ja elinkeinoelämän yhteistyönä. Lainsäädäntökartoituksen tuloksena ovat lainsäädännön kehittämisehdotukset, joilla edistetään kyberturvallisuusstrategian mukaisten tavoitteiden toteutumista.

Kartoituksen yhtenä tarkoituksena on se, että lainsäädäntö antaisi mahdollisuuden sekä riittävät keinot ja toimivaltuudet eri alojen toimivaltaisille viranomaisille sekä muille toimijoille toteuttaa yhteiskunnan elintärkeiden toimintojen ja erityisesti valtion turvallisuuden suojaamista kyberuhkia vastaan. Tarkasteltavaksi otetaan myös 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 arvioitaisiin 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.

Yhteiskunnan kriittisestä infrastruktuurista on valtaosa yksityisessä omistuksessa ja liiketoiminnallisesti operoitua. Yritykset toteuttavat suurelta osin kyberkyvykkyyden, osaamisen sekä palveluiden luomisen ja suojaamisen. Kybertoimintaympäristöä säätelevän kansallisen lainsäädännön tulee olla sellaista, että liiketoiminnan kehittämiselle on olemassa suotuisat edellytykset. Tämä mahdollistaa osaltaan kansainvälisesti tunnustetun, kilpailukykyisen ja vientimahdollisuudet omaavan kyberosaamisklusterin syntymisen. Samalla Suomesta kehittyy houkutteleva kyberturvallinen toimintaympäristö, johon kannattaa tehdä investointeja ja yritysten toimintojen sijoituspäätöksiä.

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

Kyberturvallisuuden kehittäminen vaatii selkeää vastuiden määrittelyä ja tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää, että kukin hallinnonala tekee riskiarvioinnin ja kypsyysanalyysin, joiden avulla tunnistetaan kyberturvallisuuden kannalta merkittävät haavoittuvuudet ja riskit sekä niiden hallinnan taso. Saatujen tulosten perusteella laaditaan kunkin hallinnonalan toimeenpano-ohjelmat sekä tuetaan elinkeinoelämän toimeenpano-ohjelmien tekemistä yhteistoiminnassa huoltovarmuusorganisaation kanssa.

10 Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Ministeriöt ja virastot vastaavat toimialalleen kuuluvasta strategian toimeenpanosta, kyberturvallisuuteen liittyvien tehtävien ja huoltovarmuusjärjestelyiden toteuttamisesta sekä niiden kehittämisestä. Perustettava Turvallisuuskomitea seuraa ja yhteen sovittaa strategian toimeenpanoa. Kyberturvallisuuden yhteensovittamisen päämääriä ovat päällekkäisen toiminnan välttäminen, mahdollisten puutteiden tunnistaminen ja varmistuminen vastuutahoista. Varsinaiset päätökset tekee toimivaltainen viranomainen sen mukaisesti, mitä asiasta on säädetty. VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset. Ministeriöt, virastot ja laitokset sisällyttävät kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa.

LIITE

Käsite	Määritelmät
Informaatio-infrastruktuuri	Informaatioinfrastruktuurilla tarkoitetaan tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely.
Kriittinen informaatio-infrastruktuuri	Kriittisellä informaatioinfrastruktuurilla tarkoitetaan yhteiskunnan elintärkeiden toimintojen tietojärjestelmien perustana olevia rakenteita ja toimintoja, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely.
Kriittinen infrastruktuuri	Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja.
Kyber-	Kyber-sanaa käytetään lähes poikkeuksetta yhdyssanan määriteosana eikä yksinään. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin. Vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan katsoa olevan oma merkityksensä. Sanan kyber voidaan katsoa tulevan alun perin kreikankielen sanasta "kybereo" - ohjata, opastaa, hallita.
Kyberriski	Kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta, joka toteutuessaan tai jota hyväksi käyttäen kybertoimintaympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä.
Kybertoiminta-ympäristö	Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Tarkennus 1 Ympäristölle 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. Tarkennus 2 Informaation (tietojen) käsittely tarkoittaa informaation (tietojen) keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita informaatioon (tietoihin) kohdistuvia toimenpiteitä.

Käsite	Määritelmät
Kyberturvallisuus	Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Tarkennus 1 Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Tarkennus 2 Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä ("yhteisöllinen tietoturva"). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia. Tarkennus 3 Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.
Kyberuhka	Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Tarkennus Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan.
Tietojärjestelmä	Tietojärjestelmällä tarkoitetaan ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi.
Tietosuoja	Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista oikeudettomalta tai henkilöä vahingoittavalta käytöltä. Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.
UTVA	Ulko- ja turvallisuuspoliittinen ministerivaliokunta
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
YTS	Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010

www.yhteiskunnan turvallisuus.fi