KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO-OHJELMA

Sisältö

KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO-OHJELMA 1
1 JOHDANTO 2
1.1 Oikeudellinen viitekehys 3
1.2 Viranomaisten kansainvälinen yhteistyö 5
2 TEHOKAS JA TURVALLINEN JULKISHALLINTO 9
2.1 Kriittiset toiminnot ja järjestelmät 9
2.2 Viranomaisten osaamisen ja kyvykkyyksien kehittäminen 10
2.3 Tilannekuva 11
2.4 Tiedonhankinta ja tutkinta kyberympäristössä 12
3 KANSALAISTEN HYVINVOINTI JA YRITYSTEN MENESTYS 14
3.1 Osaamisen kehittäminen 14
3.2 Hyvinvointipalveluiden turvaaminen 15
3.3 Yritysten toimintaedellytykset ja jatkuvuuden hallinta 16
4 Kyberturvallisuusstrategian ja toimeenpano-ohjelman seuranta ja kehittäminen 17
5 YHTEENVETOTAULUKKO ESITYKSISTÄ 18
LIITE 1: KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO-OHJELMAN ESITYKSET 24
TEHOKAS JA TURVALLINEN JULKISHALLINTO 24
Kriittiset toiminnot ja järjestelmät 24
Viranomaisten osaamisen ja kyvykkyyksien kehittäminen 27
Tilannekuva 34
Tiedonhankinta ja tutkinta kyberympäristössä 39
KANSALAISTEN HYVINVOINTI JA YRITYSTEN MENESTYS 45
Osaamisen kehittäminen 45
Hyvinvointipalveluiden turvaaminen 49
Yritysten toimintaedellytykset ja jatkuvuuden hallinta 52
LIITE 2: LYHENNELUETTELO 56

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelman keskeiset kehittämiskohteet ovat:

- **kyberturvallisuuskeskus,**
- **valtion ympärivuorokautinen tietoturvatoiminta,**
- **salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (SATU),**
- **poliisin toimintakyky kyberrikollisuuden torjunnassa,**
- **kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen sekä**
- **tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen.**

Toimeenpano-ohjelmassa on yhteensä 74 toimenpidettä.

1 JOHDANTO

Kyberturvallisuusstrategiasta 24.1.2013 annetun valtioneuvoston periaatepäätöksen mukaan Suomen tulisi olla maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa vuoteen 2016 mennessä. Strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Strategiassa edellytetään, että laaditaan kansallinen kyberturvallisuuden toimeenpano-ohjelma. Tämä ohjelma esittää keskeisimmät toimenpiteet kyberturvallisuusstrategian asettamien tavoitteiden saavuttamiseksi.

Kyberturvallisuus ei rajaudu kansallisesti eikä kunnioita valtiorajoja. Toimijoiden joukossa on intressiltään ja voimavaroiltaan erilaisia valtiollisia toimijoita sekä monenlaisia ei-valtiollisia toimijoita. Suomen kannanotot ja toiminta kyberturvallisuuteen liittyvissä kysymyksissä omalta osaltaan vaikuttavat Suomen kansainväliseen asemaan sekä Suomen kahdenvälisiin suhteisiin muiden valtioiden kanssa. Kansainvälisillä foorumeilla Suomen viiteryhmä poliittisissa kysymyksissä ovat muut demokratiaa, ihmisoikeuksia ja oikeusvaltioperiaatetta korostavat maat, erityisesti Euroopan unionin jäsenmaat sekä Pohjoismaat. Suomi toimii kyberturvallisuuteen liittyvissä kysymyksissä YK:n, Etyjin, Naton ja muiden kansainvälisten organisaatioiden ja prosessien puitteissa. Suomelle on tärkeää tukea EU:n yhteisten toimintalinjojen vahvistamista kyberturvallisuudessa, mukaan lukien EU:n kyberstrategiatyö. Suomen kyberturvallisuusstrategia tukee EU:n digitaaliagendaan (2010) ja Suomen digitaaliagendaan (Tuottava ja uudistuva Suomi – Digitaalinen agenda vuosille 2011–2020) sisältyviä kyber- ja tietoturvallisuustavoitteita.

Suomi korostaa, että kaikkien tulee noudattaa kansainvälisen oikeuden velvoitteita, mihin perustuu kansainvälinen luottamus ja yhteistyö. Suomen omassa varautumisessa huomioidaan, että pyrki-

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

myksistä huolimatta tämän kansainvälisen tavoitetilan täydellinen toteutuminen on tulevaisuudessakin epätodennäköistä.

Kyberturvallisuuden poliittinen ohjaus kuuluu valtioneuvostolle, joka päättää myös strategisista linjauksista, kyberturvallisuuden voimavaroista ja toimintaedellytyksistä. Ministeriöt ja virastot vastaavat toimialalleen kuuluvasta strategian toimeenpanosta, kyberturvallisuustehtävien toteuttamisesta ja niiden kehittämisestä sekä kyberhäiriötilanteiden hallinnasta. Kyberturvallisuustehtävät ovat ”Yhteiskunnan turvallisuusstrategiassa” määritettyihin strategisiin tehtäviin liittyviä ministeriöiden tehtäviä. Toiminnassaan ministeriöiden on aina otettava huomioon kansallinen ja kansainvälinen yhteistyö, hallinnon eri tasot sekä elinkeinoelämän ja järjestöjen rooli. Ministeriöt, virastot ja laitokset sisällyttävät kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa. Kunnalliset viranomaiset vastaavat niiden tehtävävastuulle kuuluvalta osalta kyberturvallisuudesta.

Turvallisuuskomitea seuraa ja yhteensovittaa strategian toimeenpanoa. Yhteensovittamisen päämääriä ovat päällekkäisen toiminnan välttäminen, mahdollisten puutteiden tunnistaminen ja varmistuminen vastuutahoista. Varsinaiset päätökset tekee toimivaltainen viranomainen sen mukaisesti, mitä asiasta on säädetty.

Ensimmäisen kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma on viranomaiskeskeinen, vaikka suurin osa tuotannosta ja palveluista tuotetaan yksityisellä sektorilla. Muiden toimijoiden osuus vahvistuu ja näkyy paremmin strategian toimeenpanon edetessä. Turvallista kybertoimintaympäristöä pyritään kehittämään tavalla, joka vahvistaa tietoyhteiskunnan mahdollisuuksia lisääviä vaikutuksia kansalaisille, yrityksille ja viranomaisille sekä edistää kaikille kuuluvien perusoikeuksien toteutumista. Kullakin toimijalla, yksilöistä yrityksiin ja hallintoon asti, on silti vastuu omasta varautumisestaan kyberuhkien varalle.

Koulutuksella, tutkimuksella ja elinkeinoelämällä on tärkeä rooli kyberturvallisuuden ylläpitäjänä ja kehittäjänä. Useat toimeenpano-ohjelmassa esitettävät toimenpiteet tähtäävät ratkaisuihin, joilla edistetään suomalaisten yritysten kyberturvallisuutta, liiketoimintamahdollisuuksia sekä viranomaisten ja yritysten välistä yhteistyötä. Valtionhallintoa koskevissa toimenpiteissä yritykset osallistuvat toimintaan lähtökohtaisesti markkinaehtoisesti sopimusosapuolina ja kumppaneina. Yhteiskunnan elintärkeiden toimintojen kannalta välttämättömät yritykset kehittävät kyberturvallisuuttaan myös osana riskin- ja jatkuvuudenhallintatoimenpiteitään sekä yhteistyössä huoltovarmuusorganisaatiossa. Tutkimus ja koulutus ovat keskeisiä kyberturvallisuuden jatkuvassa kehittämisessä ja tiedon välittämisessä laajasti yhteiskunnassa. Osaamisen vahvistaminen tukee hallitusohjelman ja kyberturvallisuusstrategian tavoitteiden saavuttamista.

Toimeenpano-ohjelmassa on yhteensä 74 toimenpidettä kyberturvallisuuden parantamiseksi. Ne on koottu hallinnonalojen ja huoltovarmuusorganisaation esityksistä. Muutama toimenpide on lähetetty sihteeristöön suoraan toimijoilta. Toimenpiteet tehdään valtionhallinnon osalta pääosin valtiontalouden kehyksen ja vuotuisten talousarvioiden sisällä uudelleenkohdennuksin.

Toimeenpano-ohjelman luonnos lähetettiin lausunnoille 121 organisaatiolle, joista osa välitti pyynnön eteenpäin. Lausunto saatiin 54 toimijalta, jotka olivat 12 ministeriötä, 14 muuta julkishallinnon edustajaa, 8 yliopistoa, korkeakoulua tai tutkimuslaitosta, 3 yritystä ja 17 järjestöä.

1.1 Oikeudellinen viitekehys

Kybertoimintaympäristöön liittyvä sääntely on osa yhteiskunnan oikeudellista viitekehystä. Kybertoimintaympäristön häiriöitä sekä niistä reaalimaailman elintärkeisiin toimintoihin heijastuvia tilan-

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

teita säännellään eri kohdissa lainsäädäntöä. Tämä on havaittavissa niin Suomessa kuin ulkomaalaisessa lainsäädännössä.

Kansainvälisestä oikeudesta on johdettavissa kybertoimintaympäristöön liittyviä oikeuksia ja velvollisuuksia, jotka on otettava huomioon toimeenpano-ohjelmassa. Kansainvälisen oikeuden perusteella valtion suvereenisuuteen kuuluu toimivalta sen alueella olevaan infrastruktuuriin. Myös valtioiden voimankäyttöä koskevat kansainvälisen oikeuden säännöt sekä kansainvälinen humanitaarinen oikeus sisältävät toimeenpano-ohjelman kannalta merkityksellisiä sääntöjä rajankäynnissä verkko-operaatioiden ja verkkosodankäynnin välillä. Keskeistä on tunnistaa kansainvälisen oikeuden määräysten vaikutukset eri hallinnonaloilla. EU-oikeus sisältää normeja, jotka sääntelevät kybertoimintaympäristöä ja sen heijastevaikutuksia reaalimaailmassa.

Kansallista ja EU-tason lainsäädäntöä on kehitettävä siten, että kyberuhkat voidaan ajoissa tunnistaa ja niihin on mahdollista reagoida tai niitä voidaan ennalta estää. Esitutkintaa suorittavilla viranomaisilla tulee olla selkeät toimivaltuudet kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten tutkintaan. Tulee harkita tiedonhankintakyvyn kehittämistä kybertoimintaympäristössä huomioimalla samalla kansalaisten perusoikeudet. Samoin on turvattava oikeus sananvapauteen eli vapauteen hankkia, vastaanottaa ja levittää tietoja ja ajatuksia.

Oikeusministeriö on asettanut työryhmän, jonka tehtävänä on panna toimeen kansallisesti tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva EU:n direktiivi. Direktiivillä pyritään torjumaan tietojärjestelmiin kohdistuvia rikoksia varmistamalla, että kaikissa unionin jäsenvaltioissa on säädetty teoista riittävät rangaistukset. Direktiivillä pyritään myös parantamaan tällaisten rikosten tutkintaan liittyvää jäsenvaltioiden välistä yhteistyötä ja rikosten tilastointia. Direktiivissä on uusia säännöksiä, joiden tarkoituksena on muun muassa puuttua uusiin uhkakuviin kuten laajamittaisiin tietoverkkohyökkäyksiin ja tietoverkkorikoksen yhteydessä tapahtuvaan henkilöllisyyden väärinkäyttöön.

Euroopan neuvoston tietoverkkorikosyleissopimus (ns. Budapestin sopimus, CETS 185) on saatettu Suomessa voimaan 2007. Suomi pyrkii siihen, että Budapestin sopimus toimisi tietoverkkorikollisuuden vastaisen toiminnan globaalina viitekehyksenä.

Kansainvälisen esitutkinta- ja syyttäjäviranomaisten yhteistyön tulee perustua oikeusapuinstrumentteihin, ja Suomen tulee edistää myös niihin perustuvan yhteistyön tehostamista. Suomi edistää kansainvälisiä hankkeita, joilla voidaan edesauttaa sitä, että rajat ylittävä rikostutkinta tulee globaalisti säännellyksi. Euroopan unioni ei ole tietoverkkorikossääntelyssä riittävän kattava toimija ja Suomen tuleekin osaltaan edesauttaa Euroopan neuvoston tietoverkkorikosyleissopimuksen mahdollisimman laajaa ratifiointia myös Euroopan neuvoston ulkopuolisissa valtioissa. Myös neuvoteltavana olevan tietoverkkorikosyleissopimuksen (ns. transborder access –pöytäkirja) lisäpöytäkirjan tulisi olla sellainen, johon mahdollisimman moni valtio voisi liittyä.

Perus- ja ihmisoikeuksiin liittyvät valtion velvoitteet perustuvat kansainvälisten ja alueellisten ihmisoikeussopimusten sitoviin määräyksiin. Osa keskeisistä ihmisoikeuksia ja kansalaisvapauksia koskevista sopimuksista, kuten YK:n yleissopimus kansalaisoikeuksista ja poliittisista oikeuksista sekä Euroopan ihmisoikeussopimus, ovat jo vuosikymmenten takaa, mutta niiden tulkinnan kehittymisen myötä ne kattavat entistä laajemmin myös nykyaikaiset viestintämuodot turvaten yksilön oikeuksia. Voimassa olevien sopimusten tulkinnan kehittäminen ja erityisesti tehokkaammat täytäntöönpanotoimet ovat ensisijaisia kehittämiskohteita. Perus- ja ihmisoikeuskysymyksissä tulee ottaa huomioon ihmisoikeusmyönteinen tulkinta niin kansallisella kuin kansainväliselläkin tasolla. Vastuu ihmisoikeuksien toteuttamisesta internetissä ja muita viestintäteknologioita käytettäessä on valtiolla, mutta tämän rinnalla muiden kybertoimijoiden tulee noudattaa huolellisuusvelvoitetta (due diligence) omassa toiminnassaan.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Suomi on sitoutunut noudattamaan kansainvälisistä tietoturvavelvoitteista annetun lain (588/2004) mukaisesti EU:n neuvoston turvallisuussääntöjä (2013/488/EU) sekä valtiosopimuksina tehtyjä tietoturvallisuussopimuksia. Nämä kansainvälisiä tietoturvallisuusvelvoitteita koskevat säännöt luovat perustan kansainvälisille hankkeille ja yhteistyölle, joiden toteuttaminen edellyttää pääsyä salassa pidettävään turvallisuusluokiteltuun tietoon. Kansainvälisillä tietoturvallisuusvelvoitteilla on kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta.

Tieto- ja kyberturvallisuus sekä tietosuoja on huomioitava kaikessa perustietovarantoihin liittyvässä toiminnassa olemassa olevien linjausten mukaisesti. Suomessa vuonna 2011 voimaan tullut laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011 nk. tietohallintolaki) pyrkii yleisesti julkisen hallinnon tietojärjestelmien yhteentoimivuuteen. Julkisen hallinnon kokonaisarkkitehtuuriperiaatteita tulee noudattaa koko julkisen hallinnon toiminnan ja tietojärjestelmien kehittämisessä, mukaan luettuna perustietovarannot. Kyberturvallisuuteen liittyviä vaatimusmäärittelyitä tarkennetaan osana julkishallinnon kokonaisarkkitehtuurityötä.

Tietoturvallisuusasetuksen (681/2010) mukaisen tietoturvallisuuden perustason (5 §) toteuttaminen tukee kyberuhkiin varautumista edellyttämällä muun muassa riittävää osaamista, kouluttamista ja valvontaa. Tietoturvallisuuden perustason täyttäminen parantaa tieto- ja kyberturvallisuuskulttuuria. Kunnilla ei ole vielä vastaavaa velvoitetta tai yhteistä tietoturvallisuuden perustasoa. Julkisen hallinnon ICT-strategian laatimisen yhteydessä on todettu olevan tarve säätää kuntien tietoturvallisuuden perustasosta vastaavalla tavalla kuin valtionhallinnossa.

Tietoturvallisuuden arvioinnista annettu laki (1406/2011) parantaa viranomaisten tietoturvallisuuden kehittämistä ja tietojärjestelmiensä arviointia. Viranomaiset voivat käyttää Viestintäviraston sekä sen hyväksymien arviointilaitosten palveluja. Lisäksi valtiovarainministeriö voi pyytää Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta tietoturvallisuuden edistämiseksi ja varmistamiseksi.

Tietoverkkoihin ja viestintään liittyvät ohjeistukset ovat tällä hetkellä hajanaisia, mikä on haitannut muun muassa erilaisten kansalaisille ja yrityksille tarjottavien palvelujen kehittämistä. Liikenne- ja viestintäministeriö on valmistellut eduskunnalle annettavaksi hallituksen esityksen sähköisen viestinnän lainsäädännön kokonaisuudistukseksi (ns. tietoyhteiskuntakaari). Lain tarkoituksena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä. Lain tavoitteena on muun muassa varmistaa, että viestintäverkot ja palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja ja turvallisia sekä hinnaltaan edullisia. Uudistuksella sähköisen viestinnän yksityisyyden suojan sääntelyä ja tietoturvallisuuden varmistamista kohennettaisiin siten, että perusoikeuksien suojaa turvaavat vaatimukset ulotettaisiin koskemaan kaikkia viestinnän välittäjiä. Lisäksi uudistuksella edistetään mahdollisuutta ehkäistä ja hallita häiriötilanteita yhteistoiminnassa siten, että kriittisten tuotantoalojen yrityksillä ja viranomaisilla säilyy mahdollisimman korkea toimintakyky eikä kenenkään mahdollisuus käyttää sähköisiä viestintäpalveluja estyisi. Esityksen mukaan teleyritysten tulisi tarkemmin suunnitella, miten niiden toiminnan jatkuvuus voidaan turvata häiriötilanteissa ja käytettäessä valmiuslain 9 luvun mukaisia toimivaltuuksia. Keskeisimmät verkonvalvomot ja muut kriittiset järjestelmät olisi jatkossa ylläpidettävä siten, että niiden toiminnot voidaan valmiuslain mukaisissa poikkeusoloissa tarvittaessa viipymättä palauttaa Suomeen.

1.2 Viranomaisten kansainvälinen yhteistyö

Kansainvälisellä yhteistyöllä pyritään nostamaan kansallisen kyberturvallisuuden tasoa. Yhteistyömahdollisuuksia hyödynnetään eri foorumeilla silloin kun se ylläpitää tai vahvistaa Suomen kansainvälistä asemaa ja kehittää suomalaista osaamista. Työskentelytapoina on vaihtaa tietoja ja koke-

muksia sekä oppia parhaista käytännöistä. Yhteistyötä tehdään monella tasolla kahdenvälisesti ja monenkeskisesti, joita tämän luvun esimerkit kuvaavat.

Suomen diplomaattiset edustustot ulkomailla tukevat kotimaisten viranomaisten toimintaa tarvittaessa hankkimalla tietoja, välittämällä Suomen kantoja sekä neuvottelemalla muiden valtioiden ja kansainvälisten toimijoiden kanssa.

Suomen kannalta Euroopan unionilla on keskeinen rooli myös kyberturvallisuuskysymyksissä. Suomi osallistuu EU:n jäsenmaana päätöksentekoon ja vaikuttamiseen kyberturvallisuuden kehittämisessä. Tiedonanto EU:n kyberturvallisuusstrategiaksi annettiin helmikuussa 2013. Strategiassa on viisi painopistealuetta: kyberuhkien sietokyky, kyberrikollisuuden vähentäminen, kyberpuolustuksen ja yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) valmiuksien kehittäminen, kyberturvallisuuteen liittyvien teollisten voimavarojen vahvistaminen ja johdonmukainen kansainvälinen yhteistyö kyberturvallisuudessa. Suomi edistää EU:n kyberturvallisuusyhteistyön vahvistamista sekä EU:n kyberturvallisuusstrategian aktiivista ja tehokasta toimeenpanoa.

Valtioiden välisen luottamuksen lisääminen kybertoimintaympäristössä on keskeistä. Etyjissä on sovittu ensimmäisistä luottamusta lisäävistä toimista kybertoimintaympäristössä. Kyse on vapaaehtoisuuteen perustuvasta tiedonvaihtojärjestelystä Etyj-maiden kesken. Suomi toimeenpanee osaltaan Etyjissä sovitut luottamusta lisäävät toimet.

Suomi tekee yhteistyötä Naton kanssa rauhankumppanuusohjelmassa (Partnership for Peace, PfP) sekä osallistuu Naton monikansallisiin, kyberpuolustukseen liittyviin tutkimus- ja kehittämisohjelmiin sekä harjoituksiin. Suomi tukee kansallisten harjoitteluympäristöjen verkottumista kansainvälisesti. Yhteistyöllä tavoitellaan osaamisen kehittämistä ja resurssisäästöjä.

Pohjoismaat ovat tiivistäneet yhteistyötä kyberturvallisuuden alalla. Pohjoismaiden kansallisten tietoturvaviranomaisten (CERT) yhteistyöverkosto on toiminnassa. Työryhmätasolla pohditaan parhaillaan uusia mahdollisia yhteistyöaloja kyberturvallisuuteen liittyvissä ulko- ja turvallisuuspoliittisissa aiheissa. Pohjoismaat ja Baltian maat (NB8-maat) tapaavat säännöllisesti kyberturvallisuuteen liittyen.

Kansainvälisessä yhteistyössä Suomi korostaa johdonmukaisesti ihmisoikeuksien toteutumisen tärkeyttä viestintäteknologioita käytettäessä. Erityistä huomiota kiinnitetään sananvapauden ja yksityisyydensuojan toteutumiseen. Kyberturvallisuuteen liittyvät ihmisoikeuskysymykset ovat kasvavassa määrin esillä YK:ssa erityisesti yleiskokouksen I-komiteassa, III-komiteassa ja ihmisoikeusneuvostossa. Yhdessä EU:n jäsenmaiden ja muiden samanmielisten maiden kanssa Suomi vaikuttaa näihin liittyviin aloitteisiin korostamalla erityisesti kansalaisoikeuksia ja poliittisia oikeuksia koskevia valtion velvoitteita ja sitoumuksia sekä edistäen näiden ihmisoikeusmyönteistä tulkintaa. Kysymykset ovat esillä myös Euroopan neuvostossa.

Suomi on liittynyt keväällä 2012 Freedom Online -koalitioon (Freedom Online Coalition, FOC), joka tukee ihmisoikeuksien toteutumista internetissä ja muissa viestintäteknologioissa. Suomi on myös tehnyt linjaukset liittymisestä FOC:n alaiseen Digital Defenders Partnership:iin (DDP). Suomi tukee monitoimijamalliin perustuvan, kaikki sidosryhmät osallistavan, internetin hallintomallin kehittämistä. Suomi tukee taloudellisesti WSIS-prosessin (tietoyhteiskuntaa käsittelevä huippukokous, World Summit on the Information Society) seurantavaiheen kannalta keskeisiä toimijoita korostaen tarvetta pitää kehityskysymykset ja ihmisoikeudet läpileikkaavina teemoina internetin hallinnasta käytävässä keskustelussa.

EU:n verkko- ja tietoturvavirastossa (ENISA) tapahtuvan yhteistyön tärkeänä tavoitteena on kehittää edelleen jäsenvaltioiden välistä tietoturvayhteistyötä ja pyrkiä edistämään hyvien ja toimivien

tietoturvaa koskevien käytäntöjen leviämistä jäsenvaltiosta toiseen. Suomi osallistuu toimintaan ja sen kehittämiseen siten, että virasto voi mahdollisimman hyvin tukea jäsenvaltioidensa tietoturvan riittävän korkeasta tasosta.

Suomi jatkaa aktiivista osallistumista OECD:n (Taloudellisen yhteistyön ja kehityksen järjestö, Organisation for Economic Co-operation and Development) kyberturvallisuutta koskevien kansainvälisten linjausten valmisteluun. Meneillään on OECD:n turvallisuuden perusperiaatteiden (OECD Security Guidelines) päivittäminen. Valtiovarainministeriö vastaa OECD:ssä Suomen tieto- ja kyberturvallisuuden yhteistyöstä.

Suomi tekee moninaista kansainvälistä yhteistyötä kyberrikostorjunnan eri sektoreilla kuten Europolin (European Cyber Crime Center, EC3) ja jatkossa myös Interpolin (Digital Crime Center, syyskuusta 2014 alkaen) kanssa.

Kansainvälisten tietoturvallisuusvelvoitteiden kokonaisvastuu on Suomessa ulkoasiainministeriöllä. Se toimii kansallisena turvallisuusviranomaisena (NSA, National Security Authority), joka huolehtii kansainvälisten tietoturvavelvoitteiden toteuttamisesta. Kansallisen turvallisuusviranomaisen tehtävänä on erityisesti ohjata ja valvoa, että kansainväliset turvallisuusluokitellut tietoaineistot suojataan ja niitä käsitellään asianmukaisesti. Se koordinoi määrättyjen turvallisuusviranomaisten toimintaa ja edustaa Suomea kansainvälisissä turvallisuuskomiteoissa ja -työryhmissä sekä osallistuu kansainvälisten turvallisuussääntöjen valmisteluun. Lisäksi se neuvottelee kahden- ja monenvälisiä tietoturvallisuussopimuksia ja myöntää henkilö- ja yhteisöturvallisuustodistuksia kansainvälistä yhteistyötä varten. Toiminnan ansiosta suomalaiset yritykset voivat osallistua sellaisiin kansainvälisiin hankkeisiin, joissa käsitellään turvallisuusluokiteltua tietoa.

Suojaus- ja käsittelyohjeet perustuvat niihin velvoitteisiin, joita Suomella on sekä EU:n turvallisuussääntöjen että kahden- ja monenvälisten tietoturvallisuussopimusten johdosta. Määrätyt kansalliset turvallisuusviranomaiset Suomessa (Designated Security Authority, DSA) ovat puolustusministeriö, pääesikunta ja suojelupoliisi, joille kullekin on jaettu omat vastuualueensa kansallisen turvallisuusviranomaisen kokonaisvastuukentässä.

Viestintävirasto toimii määrättynä tietoliikenneturvallisuusviranomaisena (National Communication Security Authority, NCSA) tapauksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. Tähän liittyen Viestintäviraston viranomaistehtäviin kuuluvat salausteknisen aineiston jakeluverkon hallinnointi, kirjanpito sekä ohjeistus aineiston turvalliselle käsittelystä (Crypto Distribution Authority, CDA), salaustuotteiden hyväksyntä kansainvälisen turvaluokitellun tiedon suojaamiseksi Suomessa (Crypto Approval Authority, CAA), kansainvälistä turvaluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä (Security Accreditation Authority, SAA) sekä sähkömagneettisen hajasäteilyn haittoja minimoivan TEMPEST-toiminnan kansallinen koordinointi ja ohjeistus (National Tempest Authority, NTA).

Suomi toteuttaa kyberturvallisuuteen liittyvää kansainvälistä yhteistoimintaa ICT-järjestelmien sietokykyä EP3R-foorumilla (European Public-Private Partnership for Resilience, EP3R). Se toimii Euroopan laajuisen joustavan tieto- ja viestintäteknologiainfrastruktuurin varmatoimisen ohjausjärjestelmän kehittämiseksi ja edistää julkisen ja yksityisen sektorin yhteistyötä tietoturva- ja varmatoimisuustavoitteisiin, perusvaatimuksiin sekä hyviin käytänteisiin ja toimintatapoihin liittyvissä kysymyksissä. Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin (Body of European Regulators for Electronic Communications, BEREC) edistää erityisesti sähköisten viestintäverkkojen ja -palvelujen sisämarkkinoiden kehittämistä ja parempaa toimintaa. Sitä tehdään pyrkimällä varmistamaan, että sähköistä viestintää koskevaa EU:n sääntelyjärjestelmää sovelletaan yhdenmukaisesti. Euroopan jäsenvaltiofoorumi (European Forum for Member States, EFMS) edistää keskustelua ja tiedonvaihtoa viranomaisten hyvistä käytännöistä, jotka liittyvät ICT-infrastruktuurin turvallisuu-

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

teen ja vaurioiden sietokykyyn. EFMS keskittyy yhteistyöhön kansallisten/valtiollisten tietotekniikan kriisiryhmien eli CERT-ryhmien välillä. Se pyrkii määrittelemään taloudellisia kannustimia ja sääntelymekanismeja kyberturvallisuuden ja sietokyvyn parantamiseen, arvioimaan verkkoturvallisuustilannetta Euroopassa, edistämään yleiseurooppalaisia harjoituksia sekä keskustelemaan painopisteistä kansainvälisessä tietoinfrastruktuurien suojaamiseen ja sietokykyyn liittyvässä yhteistyössä.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

2 TEHOKAS JA TURVALLINEN JULKISHALLINTO

Toimeenpano-ohjelman kehitysehdotuksista suurin osa on viranomaisten toimintatapojen kehittämistä. Tieto- ja kyberturvallisuuden kehittäminen julkishallinnossa parantaa myös väestölle ja yrityksille tarjottavia palveluja.

Kyberturvallisuuteen liittyviä uhkia on hallinnossa käsitelty usein yksinomaan tietotekniikkaan liittyvänä ongelmana, minkä vuoksi kokonaisturvallisuuden ja toiminnan turvaamisen merkitys on jäänyt osin vähäiselle huomiolle. Pelkästä tietoturvallisuudesta ei välttämättä enää seuraa kyberturvallisuutta. Toimintatapoja ja prosesseja tulee kehittää hallinnon turvallisen, verkostomaisen toiminnan tarpeita vastaavaksi. Toimeenpano-ohjelma pyrkii tukemaan tietoteknisten ja toiminnallisten tarpeiden tunnistamista, valtionhallinnon toimijoiden roolien selkeyttämistä sekä kyvykkyyksien kehittämistä.

Turvallisen kybertoimintaympäristön eräänä perustana toimii turvallinen julkisen hallinnon yhteinen tieto- ja viestintätekniikka (ICT). Sen kehittämistyössä keskeistä on kokonaisarkkitehtuuri, joka tarkoittaa kokonaissuunnitelmaa organisaation toimintaprosesseista, tiedosta ja järjestelmistä. Päällekkäisten arkkitehtuuriselvitysten välttämiseksi tarvitaan koordinointia. Vuonna 2013 asetettiin valtionhallinnon Tietohallinnon kehittämis- ja koordinaatioryhmä (TIETOKEKO), jonka eräänä tehtävänä on kehittää malli hallinnonalojen tietohallinnon ohjaamiseen kokonaisarkkitehtuurin avulla. Kyberturvallisuuteen voidaan vaikuttaa merkittävästi, kun valtionhallinnon tieto- ja viestintäteknisten palvelujen keskittyvät palvelukeskuksiin, kuten VALTORI.

Hallinnonalat varmistavat kyberturvallisuuden riittävän tason, kun ne hankkivat yrityksiltä järjestelmiä ja palveluja käyttäen arvioinnissa apuna esimerkiksi kansallista turvallisuusauditointikriteeristöä (KATAKRI). Hallinnon, elinkeinoelämän ja kansalaisten on voitava luottaa hallinnon ylläpitämiin perusrekistereihin myös häiriötilanteissa ja poikkeusoloissa. Eheys ja kiistämättömyys edellyttävät sääntöjen ja ohjeiden noudattamisen lisäksi auditointia, raportointia ja korjaavien toimenpiteiden tekemistä tarvittaessa. Luottamuksellisuus edellyttää omaan toimintaan liittyvien riskien tunnistamista ja sen pohjalta tapahtuvaa tietoturvallisuuden kehittämistä ja toimivia tietoturvakäytänteitä.

Kyberhäiriötilanteiden hallinnassa noudatetaan voimassa olevaa lainsäädäntöä sekä yhteiskunnan turvallisuusstrategiassa ja kokonaisturvallisuuden periaatepäätöksessä esitettyjä johtamisen periaatteita. Lähtökohtana on toimiminen viranomaisten normaaliorganisaatiolla ja normaalien toimintamallien mukaisesti.

Toimenpiteet kuvataan tarkemmin liitteessä, mutta seuraavissa alaluvuissa esitellään taustaa ja toimenpiteiden keskeinen sisältö.

2.1 Kriittiset toiminnot ja järjestelmät

Kriittisten toimintojen ja järjestelmien turvaamisessa on parannettava työn organisointia. Painopisteisiin kuuluvat turvallisuusverkon (TUVE) ja valtionhallinnon toimialariippumattomien tieto- ja viestintäteknisten tehtävien kokoamishankkeen (TORI) kehittäminen sekä salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatio (SATU). Valtion ympärivuorokautinen tietoturvatoiminta on kuvattu luvussa 2.3.

Hallinnon sisäisessä toiminnassa ICT-toimintojen ja niiden avulla hoidettavien palvelujen keskittämisellä on tavoiteltu tehokkuutta ja säästöjä. Palveluiden järjestämisen hajautettu malli ei mahdollista riittävää teknistä tieto- ja kyberturvallisuutta, osaamista eikä kustannustehokkuutta. Kyberuhat eivät kuitenkaan kohdennu samanlaisina kaikkiin hallinnon toimijoihin. Erilaisten turvallisuustarpeiden huomioimiseksi keskitetyt palvelut tulee suunnitella huolella.

Hallinnon turvallisuusverkko (TUVE) on valtion ylimmän johdon korkean varautumisen tietoliikenneratkaisu. Verkon käyttäjiksi tulevat valtion ylimmän johdon ja ministeriöiden lisäksi yleisen järjestyksen ja turvallisuuden, pelastustoiminnan, meripelastustoiminnan, rajaturvallisuuden, hätäkeskustoiminnan, maahanmuuton, ensihoitopalvelun sekä maanpuolustuksen kannalta keskeiset viranomaiset. Turvallisuusverkko varmistaa valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden yhteistoiminnan ja viestinnän sekä mahdollistaa johtamiskyvyn kaikissa turvallisuustilanteissa. Turvallisuusverkkohankkeessa on parannettu merkittävästi tietoliikenneverkon suojaustasoa ja käytettävyyttä sekä luotu yhteisiä turvallisia palveluja. Turvallisuusverkolla tulee olemaan noin 35 000 viranomaiskäyttäjää. Tulevassa toimialariippumattomien ICT-tehtävien palvelukeskuksessa (VALTORI) tuotetaan myös korkean varautumis- ja tietoturvatason turvallisuusverkkopalveluja. TUVE-lakiesitys edellyttää, että TUVE-palvelut tuotetaan toiminnallisesti, taloudellisesti ja hallinnollisesti omana kokonaisuutenaan toiminnan turvallisuus-, varautumis- ja läpinäkyvyysvaatimusten takia. TUVE:n vaatimuksenmukaisuus tullaan arvioimaan kuten viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011) ja kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004) säädetään.

Toimenpiteissä on kahdeksan ehdotusta TUVE- ja TORI-ratkaisujen parantamiseksi. Näihin kuuluvat muun muassa järjestelmien riippuvuuksia ja priorisointia kartoittavat hankkeet ja kyberturvallisuuden hallinnan periaatteiden ja ICT-hankintaprosessien selkeyttäminen.

Salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatio (SATU) on hanke, jossa korotetaan ICT-infrastruktuurin ja –palvelujen tasoa turvallisuuskriteeristön mukaiselle korkeammalle turvallisuustasolle sekä luodaan viranomaisten välille turvaluokitellun tiedon käsittelypalvelut. Ulkoasiainministeriön hallinnoimassa SALVE-hankkeessa on kehitetty kansallisen ja kansainvälisen turvaluokitellun tiedon käsittely- ja välitysjärjestelmää, jota SATU-hankkeessa hyödynnetään. SATUa koskevissa toimenpiteissä on kuvattu myös siihen mahdollisesti liitettävä mobiilipäätelaitteiden toimintaa parantava kehitysehdotus.

2.2 Viranomaisten osaamisen ja kyvykkyyksien kehittäminen

Viranomaisten tieto- ja kyberturvallisuusosaamisessa on puutteita. Tärkeimpinä parannusehdotuksina ovat yhteisten toimintamallien kehittäminen, kryptolaboratorion perustaminen, koulutuksen lisääminen sekä osaamistason arviointi.

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tieto- ja kyberturvallisuuden kehittämistä sekä asettaa ja ylläpitää toimialallaan yhteistyön ohjaamisen, kehittämisen ja koordinaation toimielimet. Valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuuden linjaukset. VAHTI myös seuraa valtionhallinnon tieto- ja kyberturvallisuuden tilannetta tätä varten kehitettyjä mittareita käyttäen. Toimeenpano-ohjelman esitykset parantavat vakiintuneita yhteisiä työskentelymuotoja ja niistä saatavia tuloksia.

Kyberturvallisuuden tutkimus ja opetus, alan teknologioiden kehittäminen sekä innovaatiot ovat talouskasvun lähteitä ja kansallisia erottautumistekijöitä. Viranomaisten välistä tutkimusyhteistyötä vahvistetaan osana turvallisuustutkimuksen toimeenpano-ohjelmaa. Poikkihallinnollisia tutkimustarpeita ja -prioriteetteja johdetaan yhteisiksi tutkimusteemoiksi ja vuositason tutkimushankkeiksi. Suomessa havaittujen krypto-osaamisen vakavien puutteiden korjaamiseksi Puolustusvoimat perustaa kansallisen kryptolaboratorion. Laboratorio on kryptologian osaamiskeskus, jonne luodaan tekninen ympäristö osaamisen kehittämiseksi sekä salausteknisten ratkaisuiden ja tuotteiden testaamiseksi ja niiden vahvuuden verifioimiseksi. Kryptolaboratorio tukee muita viranomaisia, kuten Viestintäviraston tietoliikenneturvallisuustoimintoa (NCSA), salausratkaisujen evaluoinnissa tarjoamalla

käytännön tason testaus- ja verifiointipalveluita. Kryptolaboratorio tekee lisäksi yhteistyötä tiedeyhteisön kanssa tukemalla kryptologian tutkimustyötä sekä tarjoamalla teknisen laboratorioympäristön resursseja tutkimuskäyttöön. Yhteistyöverkostossa on myös alan palveluja tuottavia yrityksiä.

Toimeenpano-ohjelmassa on nostettu esille muutamia esimerkkejä viranomaisten koulutus- ja harjoitustoiminnasta. Näitä ovat mm. kyberturvallisuuskoulutuksen lisääminen poliisin peruskoulutukseen, Puolustusvoimien kyberharjoittelun ja siinä muille viranomaisille tarjottava yhteistyö sekä kansallisen turvallisuusviranomaisen (NSA) tarjoama koulutus.

Kehityskohteena ovat myös vakiintuneet toimintamallit. Esimerkkinä kuvataan toimenpide, jossa sosiaali- ja terveysministeriö kehittää kyberuhkiin varautumista muun muassa uusimalla hallinnonalan ohjeistusta yhteistyössä Huoltovarmuuskeskuksen ja muiden toimijoiden kanssa. Toimintatapoja muuttaa myös esitys kuriiritoiminnan uudelleen järjestämisestä aiempaa toimivammaksi niin Suomessa kuin kansainvälisesti. Lisäksi esitykset kyberturvallisuuden termien määrittelystä ja oikeustarkastelusta tukevat menettelytapojen päivittämistä.

Tietoteknisen osaamisen ja järjestelmien yleisen tason nostamiseksi ja puutteiden korjaamiseksi viranomaiset hyödyntävät aiempaa laajemmin kyberturvallisuutta parantavia standardeja ja arviointimenettelyjä. Tähän kuuluvat Puolustusvoimien kyberturvallisuuteen liittyvä tarkastusprosessi, VIRVE-verkon riskianalyysi sekä Ilmatieteen laitoksen ja Liikenteen turvallisuusviraston sertifiointi.

Toimenpiteet eivät edellytä lakimuutoksia.

2.3 Tilannekuva

Kyberturvallisuuskeskus ja valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke (SecICT) ovat kansallisella tasolla merkittäviä hankkeita, joiden toteutuksessa tukeudutaan verkostoituneeseen yhteistoimintaan. Tilannekuvahankkeissa on varmistuttava työnjaon selkeydestä sekä analyysi- ja reagointikyvystä.

Perustettavan valtiovarainministeriön alaisen valtionhallinnon ympärivuorokautisen tietoturvatoiminnon tehtävänä tulee olemaan vakavien ja laajavaikutteisten valtionhallinnon tieto- ja kybertapahtumien hallinta. Tilannekuvaa hyödynnetään ongelmien ennaltaehkäisyyn, tilanteiden johtamiseen, päätöksentekoon ja organisaatioiden toiminnan kehittämiseen. Nämä edellyttävät erilaisia, mukaan luettuna teknisiä tietoja. Luotettavalla ja ajantasaisella tilannekuvalla varmistetaan, että valtion johdolla on riittävä tilannetietoisuus. Valtion ympärivuorokautinen tietoturvatoiminto tekee tiivistä yhteistyötä muiden viranomaisten, valtionhallinnon organisaatioiden ja keskeisten ICT-toimijoiden kanssa.

Valtionhallinnon ympärivuorokautinen tietoturvatoiminta kattaa Valtiovarainministeriön rahoittamat ja ohjaamat GovSOC-palvelut ja sitä tukevat GovCERT-, GovHAVARO-, GovHUOVI-palvelut. GovSOC on valtionhallinnon ympärivuorokautinen tietoturvallisuuden operointipalvelu joka sisältää havainnointiin, reagointiin ja tilannekuvaan tarvittavat toiminnot.

Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeessa (SecICT) kehitetään, hankitaan ja laajennetaan eri palveluntuottajien kuten Viestintäviraston ja Huoltovarmuuskeskuksen palveluita. Huoltovarmuuskeskuksen Huovi-portaalin käyttöönotto aloitetaan valtionhallinnossa (GovHUOVI) vuonna 2014. Tämän lisäksi hankkeessa kehitetään täydentäviä tilannekuvajärjestelmäkokonaisuuden osia, joilla kerätään teknistä ja hallinnollista tilannetietoa toiminnoista ja kriittisistä ICT-järjestelmistä. Toimenpiteissä kuvataan hanketta ja muutamia kehittämishuomioita.

Viestintävirastoon perustettu Kyberturvallisuuskeskus vahventaa kansallisen tietoturvaviranomaisen tehtävien hoitamista. Keskus kerää tietoa kyberturvallisuustilanteesta, tukeutuu laajasti eri hallinnonalojen ja elinkeinoelämän asiantuntemukseen arvioidessaan ilmiöiden yhteiskunnallisia vaikutuksia sekä jakaa yhdessä toimijoiden kanssa analysoitua kyberturvallisuuden tilannekuvaa. Keskus tukee toimijoita laajojen kyberhäiriötilanteiden hallinnassa. Kyberturvallisuuskeskuksen tueksi kootaan laaja ja kaksisuuntaiseen tiedonvaihtoon perustuva yhteistyöverkosto. Kyberturvallisuuden tilannekuvan hyödyntämistä kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen tilannekuvan arviointiin kehitetään osana valtioneuvoston kanslian tilannekuvatoiminnan sekä valtion ympärivuorokautisen tietoturvatoiminnan kehittämistä (SecICT). Kyberturvallisuuskeskus vaihtaa tietoja valtioneuvoston tilannekeskuksen, valtion ympärivuorokautisen tietoturvatoiminnon, muiden viranomaisten ja elinkeinoelämän kanssa. Kyberturvallisuuskeskuksen kykyä saada tietoa sekä julkisen hallinnon että elinkeinoelämän toimijoilta sekä osallistua kansainväliseen tietoturvaloukkauksia koskevaan tiedonvaihtoon tulee hyödyntää koko yhteiskunnan hyväksi.

Kyberuhkiin liittyy myös muita viranomaisten tilannekuvatoimintoja. Valtioneuvoston kanslian tehtävänä on jatkuva kokonaisturvallisuuteen liittyvän tilannekuvan ylläpitäminen, poikkihallinnollisen tilannekuvan kokoaminen, yhteensovittaminen ja välittäminen häiriötilanteissa, ennakoivan tilannekuvan muodostaminen sekä ministeriöiden ja toimivaltaisten viranomaisten tilannekuvatoimintojen kehittämisen tukeminen. Puolustusvoimien oman kybertilannekuvan merkittävinä kehittämiskohteina ovat tilannekuvan visualisointi, ympärivuorokautinen valvonta sekä tiedonvaihtoa muiden viranomaisten ja kumppaneiden kanssa niin kansallisesti kuin kansainvälisesti muun muassa MILCERT–verkoston toimijana. Lisäksi Puolustusvoimat tuottaa kybertilannekuvaan analyyseja kybertoimintaympäristössä havaituista ilmiöistä. Tilannekuvatoimintojen ja valvomoiden toimintaan liittyvät myös toimenpide-ehdotukset ”Selvitys kyberturvallisuuspoikkeamista ilmoittamisen käytännöistä ja viranomaisyhteistyöstä” ja ”Kyberturvallisuuden yhtenäisen johtamismallin ja häiriötilanteiden hallinnan periaatteiden, tehtävien ja niihin liittyvien toimintamallien selkiyttäminen”.

Toimenpiteet eivät edellytä tässä vaiheessa lakimuutoksia.

2.4 Tiedonhankinta ja tutkinta kyberympäristössä

Kyberturvallisuusstrategiassa on todettu tarve vahvistaa yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden toimijoiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet. Kyberturvallisuusstrategiassa on todettu tarve huolehtia siitä, että poliisilla on tehokkaat edellytykset ennaltaehkäistä, paljastaa ja selvittää kybertoimintaympäristöön ~~ja~~ kohdistuvia ja sitä hyödyntäviä rikoksia. Strategian mukaan sotilaallisen kyberpuolustuskyvyn varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä osana muun sotilaallisen voimankäytön kehittämistä.

Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta käsittelivät kokouksessaan 7.11.2013 valtionhallinnon tietoturvallisuutta sekä laajemmin kyberturvallisuuteen liittyviä kysymyksiä sekä kansallisen kyberturvallisuuden kehittämistarpeita. Kokouksessa linjattiin, että on aloitettava välittömästi työ Suomen lainsäädännön kehittämiseksi.

Puolustusministeriö on kyberstrategian mukaisessa lainsäädännön riittävyyden tarkastelussaan arvioinut kyberpuolustuskykyyn liittyvää lainsäädäntöä eri maissa. Useissa muissa maissa tietoteknisen toimintaympäristön nopea kehittyminen ja muuttuminen on luonut tarpeen vastata uhkiin luomalla kansallista lainsäädäntöä valtion turvallisuusviranomaisten tiedonhankinnasta.

Puolustusministeriö on 13.12.2013 asettanut työryhmän, jonka tavoitteena on selvittää turvallisuusviranomaisten tiedonhankintaa koskevat toimintaedellytykset, erityisesti kybertoimintaympäristön kautta Suomeen kohdistuvat uhkat ottaen huomioon sekä tiedonhankintaa koskevat nykyiset toimi-

valtuudet että niiden kehittämistarpeet. Keskeisessä asemassa on Suomea velvoittavien ihmisoikeus- ja perusoikeusmääräyksien, kuten perustuslain, YK:n kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen sekä Euroopan ihmisoikeussopimuksen huomioon ottaminen. Tärkeää on ottaa huomioon myös yksilön oikeusturva sekä tehokkaat perustuslailliset valvontamekanismit. Hanke voi johtaa hallituksen esitysmuodossa olevaan lainsäädännön kehittämisehdotukseen tai siihen voi sisältyä ehdotukset erillisten lainsäädäntöhankkeiden käynnistämiseksi.

Jatkovalmistelu arvioidaan työryhmän saatua työnsä päätökseen. Jatkovalmistelussa on aiheen suuren yhteiskunnallisen merkityksen vuoksi erityisiä syitä noudattaa hyvän lainvalmistelun periaatteita kuten laajaa kuulemista.

Puolustusvoimat on alustavasti selvittänyt, kuinka toiminto voitaisiin järjestää. Poliisin kykyä vastata kyberrikollisuuden kasvuun tehostetaan useilla toimenpiteillä. Kykyä tutkia ja torjua kyberympäristössä tapahtuvia rikoksia kehitetään muun muassa rikostutkintaan ja kyberrikostilannekuvaan liittyvillä toimenpide-ehdotuksilla. Tullin rikostorjunnan kykyä torjua kyberrikollisuutta kehitetään vastaavalla tavalla Tullin tehtäväalueella.

Alaluvussa esitetyillä toimenpiteillä on vaikutuksia edellä mainittujen toimijoiden lisäksi muun muassa SecICT:hen, kyberturvallisuuskeskukseen, kansalaisiin ja yrityskenttään.

Toimenpiteet edellyttävät lainsäädäntötarkastelua.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

3 KANSALAISTEN HYVINVOINTI JA YRITYSTEN MENESTYS

Yritysten jatkuvuudenhallintaa ja varautumista tukevien toimenpiteiden avulla kehitetään koko yhteiskunnan kyberturvallisuutta. Varautumista tuetaan myös kehittämällä kansalaisten valmiuksia toimia yhä teknistyvämmässä toimintaympäristössä. Toimenpideesitykset keskittyvät osaamisen laaja-alaiseen kehittämiseen, kyberturvallisuudesta viestimiseen ja palvelujen varmentamiseen.

Toimenpiteet kuvataan tarkemmin liitteessä, mutta seuraavissa alaluvuissa esitellään taustaa ja toimenpiteiden keskeinen sisältö.

3.1 Osaamisen kehittäminen

Suomen Akatemian ja TEKESin ICT 2023 tutkimus-, kehitys- ja innovaatio-ohjelma ovat luomassa maailman parhaimmistoon kuuluvia kyberturvallisuuden menestystuotteita ja asiantuntijuutta. Tutkimus- ja opetusalalla on useita alan kansallisia ja kansainvälisiä yhteistyöprojekteja. Osaamista pyritään myös levittämään koulutushankkeilla.

Toimeenpano-ohjelman esimerkit kattavat vain osan laajasta tutkimuksen ja koulutuksen kirjosta. Opetus- ja kulttuuriministeriö on perustanut OKMICT-2015-hankkeen, jonka tehtävänä on muun muassa käsitellä korkeakoulujen ICT-alan osaamista ja profiloitumista. Yliopistot vahvistavat kansallisesti ja kansainvälisesti kyberturvallisuuden perustutkimuksen, soveltavan tutkimuksen ja innovaatiotoiminnan edellytyksiä. Ammattikorkeakouluissa vahvistetaan tuotekehitystyön, soveltavan tutkimuksen sekä innovaatiotoiminnan edellytyksiä.

Kyberturvallisuuteen liittyvän tutkimuksen ja yritystoiminnan kehittämisessä hyödynnetään laajoja kansallisia tutkimusohjelmia. Suomen Akatemia ja TEKES ovat ICT2015-raportin perusteella käynnistäneet yhteisen ICT 2023 tutkimus-, kehitys- ja innovaatio-ohjelman. Sen tavoitteena on ns. syvän tietojenkäsittely-osaamisen kehittäminen. Innovatiiviset kaupungit (INKA) –hankkeeseen liittyen Jyväskylään rakennetaan kyberturvallisuuden osaamis- ja innovaatiokeskittymä. Kyberturvallisuuden osaamis- ja innovaatiokeskittymä rakentuu eri kaupunkiseutujen toimijoiden ympärille ja yhteistyölle. Kyberturvallisuusteeman eri hankkeissa tuotetaan kansainvälisen tason huippututkimuksella ja koulutuksella osaamista ja liiketoimintamahdollisuuksia sekä tuetaan kansallisia kyberstrategian tavoitteita.

Suomalaiset korkeakoulut, kuten Aalto-yliopisto, Jyväskylän yliopisto, Oulun yliopisto ja Tampereen teknillinen yliopisto sekä tutkimuslaitokset, kuten VTT, ovat verkottuneet laajasti eurooppalaiseen kyberturvallisuusosaamiseen. Ne ovat mukana laajoissa kyberturvallisuuden yhteishankkeissa, jotka pyrkivät hyödyntämään suomalaista ja Euroopan Unionin rahoitusta. Näistä esimerkkeinä ovat vuoden 2016 alkuun jatkuva SASER CelticPlus -hanke ja keväällä 2014 käynnistyvä ECOSSIAN EU –projekti sekä hankkeet automaatiojärjestelmiin kohdistuvista kyberuhkista.

Suomalaisissa yrityksissä ja tutkimusyksiköissä on kyber- ja tietoturvallisuuden huippukyvykkyyttä, mutta osaaminen on pirstaleista. Kattavuuden parantamiseksi yksiköiden, laitosten ja muun yhteiskunnan yhteistyöhön on panostettava. Eräänä esimerkkinä yhteistyöstä on Tampereen alueella vuonna 2014 muodostettava kriittisen infrastruktuurin tietoturvatutkimuksen ja opetuksen ympäristön kokonaisuus (TUTCyberLabs). Ympäristö laajentaa olemassa olevan automaation tietoturvaopetuksen, -tutkimuksen ja yritysyhteistyön mahdollisuuksia. Työssä on mukana Tampereen teknillisen yliopiston lisäksi mm. Pirkanmaan turvallisuusklusteri. Ammattikorkeakouluyhteistyöstä esimerkkinä on ammattikorkeakoulujen tietohallintojohtajien verkosto (AAPA). Opetus- ja kulttuuriministeriön

tekemän kyselyn perusteella kansalliseen toimeenpano-ohjelmaan nousi useita yksittäisiä koulutusohjelmia.

Kyberturvallisuusosaamisen levittämiseksi yhteiskunnan eri sektoreille tarvitaan eri ryhmiin ulottuvaa opetusta ja viestintää. Opetus- ja kulttuuriministeriön toimenpide kuvaa, kuinka se on edistämässä yhteiskunnan kyberosaamista ja kybertoimintaympäristössä toimimista hankkeilla ja kampanjoilla. Niissä huomioidaan väestön erilaiset roolit niin kansalaisena, kuluttajana, työntekijänä kuin opiskelijana.

Huoltovarmuusorganisaatio on esittänyt useita koulutukseen liittyviä ohjelmiaan, jotka tukevat erityisesti huoltovarmuuskriittisten yritysten jatkuvuudenhallintaa.

Toimenpiteet eivät edellytä lakimuutoksia.

3.2 Hyvinvointipalveluiden turvaaminen

Digitalisoitunut ympäristö edellyttää lainsäädännön ja menettelytapojen kehittämistä. Luvun esitykset liittyvät identiteetin varmistamiseen sekä sosiaali- ja terveysministeriön hankkeisiin, joilla varmistetaan palveluiden saatavuutta.

Turvallisten sähköisten palvelujen luomisessa keskeistä on suunnittelun perusteita yhtenäistävä palveluarkkitehtuuri tai palveluväylä, jonka avulla päästään myös kustannussäästöihin. Siinä eri toimintojen järjestelmät ovat saatavilla avoimien rajapintojen avulla kaikille samaa tietoa tarvitseville järjestelmille. Tavoitteena on palveluväylän asteittainen käyttöönotto vuodesta 2015 alkaen.

Toimeenpano-ohjelmaan tuotu kehittämisehdotus sähköisen identiteetin hallintaratkaisusta liittyy palveluväyläkokonaisuuteen. Luotettava tunnistaminen edellyttää hyvää sähköisen identiteetin hallintaratkaisua, joka toimenpideohjelman esityksen mukaan kattaisi myös valtuutusten tunnistamisen sekä henkilön eri roolien tunnistamisen. Hallintaratkaisua tarvitaan kansallisen palveluarkkitehtuurin ja palveluväylän tehokkaaseen hyödyntämiseen. Tarkoituksena on taata kansalaisille turvallinen sähköinen tunnistaminen ja kehittää markkinoiden toimintaa. Tietoturvallisuuteen tulee kiinnittää erityistä huomiota. Kansalaisten tietosuojan varmistamiseksi kehitetään palvelu, jossa kansalainen voi nähdä ja hallinnoida itseään koskevien tietojen välittymistä eri organisaatioiden välillä.

Kuntasektori vastaa suurelta osin kansalaisten kannalta tärkeiden peruspalveluiden järjestämisestä. Kuntasektorin toimijoiden kyberturvallisuus edellyttää parantamista muun muuassa yleisessä valmiudessa ja osaamisessa. Sosiaali- ja terveydenhuollossa palvelutuotannon riskit ovat muuttuneet digitalisoitumisen seurauksena. Esimerkiksi potilaiden hoitoon liittyvät laitteet ja järjestelmät sekä sosiaaliturvan päätöksentekoon ja maksamiseen liittyvät järjestelmät ovat riippuvaisia tietoverkkojen ja tietojärjestelmien häiriöttömästä toiminnasta. Tilanteen parantamiseksi sosiaali- ja terveysministeriö esittää toimeenpano-ohjelmassaan varautumisen näkökulmien huomioimista valmistelussa olevaan sosiaali- ja terveydenhuollon järjestämislakiin, uuteen sosiaalihuoltolakiin sekä terveydenhuoltolakiin. Esityksinä ovat myös laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä hanke potilastietojen kevyistä käyttöliittymistä.

Toimenpide-ehdotuksissa on kuvattu sosiaali- ja terveydenhuollon järjestämislaki, sosiaalihuoltolaki, terveydenhuoltolain muutokset sekä sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevan lain muutokset.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

3.3 Yritysten toimintaedellytykset ja jatkuvuuden hallinta

Merkittävä osa yhteiskunnan toiminnan kannalta kriittisestä tuotannosta, infrastruktuurista ja palveluista on yksityisen sektorin omistamaa tai ylläpitämää. Yritysten toimintaedellytyksistä ja toiminnan jatkuvuudesta huolehtiminen on edellytys paitsi kilpailukykyiselle kansantaloudelle myös sen turvallisuudelle. Kehittämällä yritysten kykyä toimia kyberympäristössä turvallisesti kehitetään koko yhteiskunnan toimintakykyä häiriö- ja poikkeusoloissa. Esitetyt toimenpiteet liittyvät huoltovarmuuteen sekä yritysten kilpailukykyyn.

Kyberturvallisuus on huomioitu aikaisempaa laajemmin uudessa valtioneuvoston päätöksessä huoltovarmuuden tavoitteista. Yksi keskeisimmistä muutoksista on kriittisten tieto- ja viestintäjärjestelmien ja niiden keskinäisten riippuvuussuhteiden korostuminen. Toimeenpano-ohjelmassa esitetään joitakin elinkeinoelämälle suunnattuja tai elinkeinoelämän esittämiä toimenpiteitä. Elinkeinoelämän osallistumista kyberturvallisuusstrategian toimenpanoon tullaan kehittämään jatkuvan kehittämisen periaatteiden mukaisesti.

Yrityksiä palvelevat Viestintäviraston CERT-toiminto ja HAVARO-palvelut kuvataan tarkemmin viranomaistoimintoja käsittelevissä luvuissa ja toimenpiteissä. Tähän liittyvinä toimenpiteinä ovat Huovitilannekuvatoiminnon kehittäminen sekä eri toimenpiteitä häiriötilanteiden vaikutusten minimoimiseksi.

Toimijoiden tieto omasta tietoturvasta on usein puutteellinen. Ongelmaa korjaavat toimenpiteet painottuvat erilaisiin tieto- ja kyberturvallisuuden toteutus- ja arviointipalveluihin. Elinkeinoelämällä on itse tuotettuja, yhteisiä ja Huoltovarmuuskeskuksen kanssa toteutettavia palveluita. Toimeenpano-ohjelmassa esitetään esimerkkinä, kuinka suomalaiset yritykset tuottavat markkinoille omia turvallisuuspalvelujaan. Liitteessä kuvattu kyberlaboratorio pyrkii olemaan merkittävä palveluiden tarjoaja, joka yhdistää jäseninä toimivien yritysten ja tutkimuslaitosten resursseja. Palveluiden lisäksi korostuu yritysten omaehtoisen varautumisen ja harjoittelun merkitys toimintaedellytysten ja jatkuvuuden hallinnan takaamisessa häiriötilanteissa.

Osa kansantalouden kannalta tärkeistä yrityksistä jää strategiassa vähäisemmälle huomiolle. Strategian jatkokehittämisessä tulee huomioida elinkeinoelämän moninaisuus mukaan luettuna edellä mainittujen palveluiden ja viestinnän tavoitettavuus pk-yrityskentässä.

Liitteissä kuvataan myös kilpailukyvyn parantamiseen kohdistuvia toimenpiteitä. Tutkimus, koulutus, ja viestintä ovat merkittävässä roolissa koko elinkeinoelämän ja muun yhteiskunnan kyberturvallisuuden parantamisessa, ja niitä koskevat toimenpiteet on kuvattu aiemmissa luvuissa.

Toimenpiteet eivät aiheuta lakimuutoksia.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

4 Kyberturvallisuusstrategian ja toimeenpano-ohjelman seuranta ja kehittäminen

Valtioneuvoston periaatepäätös 24.1.2013 ensimmäisestä kansallisesta kyberturvallisuusstrategiasta ja sen toimintaohjelma ovat viranomaiskeskeisiä. Tämän painotuksen vuoksi yksityisen ja kolmannen sektorin merkittävä rooli kyberturvallisuudessa ei näy tässä toimeenpano-ohjelmassa. Tätä voidaan perustella sillä, että keskushallinnolla on parhaat edellytykset aloittaa koordinoidusti toimenpiteitä kansallisesti merkittävissä asioissa.

Hallinnonalat toteuttavat kansallista toimeenpano-ohjelmaa ja sitä tarkentavia omia toimeenpano-ohjelmiaan sekä varautumis- ja kehittämissuunnitelmiaan. Kehittämiseen liittyy usein poikkihallinnollisuutta, alue- ja paikallishallinnon, elinkeinoelämän sekä järjestöjen toimenpiteitä ja resursointia. Tiedon saatavuus sekä eri toimijoiden tietoisuuden lisääminen ovat merkittävä osa kyberturvallisuuden johtamista. Hallinnonalat ovat tehneet omia kyberturvallisuuden toimeenpano-ohjelmiaan, ja kaikkien hallinnonalakohtaisten toimeenpano-ohjelmien tulisi olla käynnissä vuonna 2014.

Turvallisuuskomitea seuraa strategian ja sen toimeenpano-ohjelman toteutumista. Osana tätä tehtävää Turvallisuuskomitea arvioi toteutettujen toimenpiteiden vaikuttavuutta sekä luo edellytykset tarvittavien toimenpiteiden ja tarpeiden yhteensovittamiseksi eri toimijoiden kesken. Turvallisuuskomitea laatii Valtioneuvostolle vuosittain arvion kyberturvallisuuden varautumisen tilasta. Arviossa voidaan käyttää kyberturvallisuuden kypsyystason arviointimallia.

Elinkeinoelämän ja järjestöjen osuus vahvistuu, kun kyberturvallisuusstrategiaa kehitetään jatkuvan parantamisen periaatteen mukaisesti. Tavoitteena on luoda jatkuva strategiaprosessi, jossa prosessin osia toistetaan säännöllisesti ja luodaan jatkuvaa toiminnan kehittymistä. Prosessin päivittämisessä on huomioitava syötteet laajasti yhteiskunnan eri sektoreilta. Erityisesti viranomaiset, elinkeinoelämä ja järjestöt sekä tutkimus ja strategian seurantatehtävä tuottavat näitä syötteitä.

Turvallisuuskomitea vastaa strategiaprosessista osana varautumisen yhteensovittamistehtäväänsä. Kyberturvallisuus huomioidaan myös Yhteiskunnan turvallisuusstrategian mahdollisessa päivityksessä.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

5 YHTEENVETOTAULUKKO ESITYKSISTÄ

	Nimi	*Vastuutaho*	*Edellyttää lainsäädäntö-muutoksia*	*Liittyy strategiseen linjaukseen nro:*
Tehokas ja turvallinen julkishallinto – Kriittiset toiminnot ja järjestelmät				
1	**Hallinnon turvallisuusverkkohankkeen (TUVE) ja toimialariippumattomien ICT -tehtävien (TORI) kehittäminen**	VM	Ei	3
	Yllä olevaan liittyviä toimenpiteitä:			
2	*Toimintojen priorisointiin perustuvan järjestelmäluokituksen ja kokonaispriorisoinnin tuottaminen ja näille päätöksenteko- ja toteutusprosessin toteuttaminen*	VM	Ei	3
3	*Järjestelmäriippuvuuksien selvittäminen laatimalla ylläpidettävä monitasoinen riippuvuuskuvaus*	VM	Ei	3
4	*Tieto- ja viestintäjärjestelmien energian saatavuuden riskikartoitus*	VM	Ei	3
5	*Valtion konesali- ja kapasiteettipalvelustrategia*	VM	Ei	3
6	*ICT -palveluiden ja palvelutoimittajien hallinta*	VM	Ei	3
7	*Tietojärjestelmien ja niiden alustojen sekä tietoliikennelaitteistojen ja –ohjelmistojen haavoittuvuuksien hallinnan kehittäminen*	VM	Ei	3
8	*Kyberyhteystietojen vastuunjako- ja virkaluettelo sekä toimintaprosessin kuvaus*	VM	Ei	1,3
9	*Turvallisten mobiilien viestintäratkaisujen nopea käyttöönotto*	VM	Ei	3
10	**Salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraation kehittäminen (SATU -palveluintegraatio)**	VM, JulkICT, UM	Ei	1,2, 9
Tehokas ja turvallinen julkishallinto – Viranomaisten osaamisen ja kyvykkyyksien kehittäminen				
11	**Valtioneuvoston tietoturvaverkosto virallistetaan ministeriöiden tieto- ja kyberturvallisuuden viralliseksi**	VNK	Ei	1, 2

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

	yhteistyöryhmäksi			
12	**Ehdotuksia valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) toimintasuunnitelmaan**	VM	Ei	1, 3, 9
	Yllä olevaan liittyviä toimenpiteitä:			
13	*ICT -varautumisen ja kybervaatimusten toteuttaminen yhteishankkeilla koko valtionhallinnolle*	VM	Ei	1, 3, 9
14	*Tietoturvahenkilöstön osaamisen parantaminen ja verkostoituminen hallinnossa*	VM	Ei	1, 3, 9
15	**Kansallisen kryptolaboratorion perustaminen**	PV	Ei	1, 2, 3, 4, 5, 6, 9
	Esimerkkejä hallinnonalakohtaisesta koulutuksesta:			
16	*Kansallisen turvallisuusviranomaisen antama koulutus viranomaisille (kansainvälistä luokiteltua aineistoa käsittelevät viranomaiset)*	NSA	Ei	3, 7
17	*Yhteistoimintamallin harjoittelu liikenne- ja viestintäministeriössä*	LVM	Ei	1,3,7
18	*Rikostorjunnan kyberosaamisen kehittäminen Poliisiammattikorkeakoulussa*	POLAMK	Ei	4,7
19	*Kyberpuolustuksen harjoitus-, koulutus- ja tutkimustoiminnan kehittäminen*	PV	Ei	5,7
20	**Henkilöturvallisuustodistus (personal security clearance, PSC) – tehtävämäärittely**	NSA	Ei	7, 9
21	**Yhteistoimintamallin kehittäminen LVM:ssä**	LVM	Ei	1
22	**Kyberuhkiin varautumisen sisällyttäminen sosiaali- ja terveydenhuollon uusittavaan valmiussuunnitteluohjeistukseen ja ohjeistuksen jalkauttaminen**	STM	Ei	1, 3, 9
23	**STM:n hallinnonalan kyberuhkiin varautumisen kehittäminen, kriittisten toimintojen tunnistaminen ja toimintamallin laatiminen**	STM	Ei	1, 3, 9
24	**Kansallinen kuriiritoiminta**	UM, VNK	Ei	1
25	**Tiiviin ja käytännönläheisen selvityksen tuottaminen kyberympäristöä koskevasta kansainvälisoikeudellisesta sääntelystä**	UM	Ei	7
26	**Kyberturvallisuuden termien määrittely**	SPEK	Ei	2, 7
	Esimerkkejä hallinnonalakohtaisesta standardisoimistyöstä ja arvioinneist:			
27	*Puolustusvoimien kyberturvalli-*	PV	Ei	5

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

	suuteen liittyvä tarkastusprosessi			
28	*VIRVE – verkon tietoturvallisuustilanteen arviointi ja riskianalyysi*	SM	Ei	3
29	*Ilmatieteen laitoksen ISO 27001-sertifikaatti*	FMI	Ei	3
30	*Liikenneviraston tietoturvatasohanke*	LiVi	Ei	3
31	*ISO 27001 tietoturvallisuussertifiointi liikenteen turvallisuusvirastossa (TRAFI)*	Trafi	Ei	3
Tehokas ja turvallinen julkishallinto – Tilannekuva				
32	**Valtion ympärivuorokautisen tietoturva-toiminnan kehittämishanke (SECICT)**	VM, JulkICT	Ei	1, 2, 3
	Yllä olevaan liittyviä toimenpiteitä:			
33	*Kyberturvallisuuden yhtenäisen johtamismallin ja häiriötilanteiden hallinnan periaatteiden, tehtävien ja niihin liittyvien toimintamallien selkiyttäminen*	VM	Ei	1, 2, 3
34	*Kohdistettujen haittaohjelmien havainnointikyvyn parantaminen*	Haltik, SecICT	Ei	3
35	*HAVARO -verkoston laajentaminen ja toiminnan kehittäminen*	VM	Ei	3
36	*HUOVI –portaalin käytön pilotointi kyberturvallisuuden kehittämistyökaluna*	VM	Ei	3, 7
37	**Kyberturvallisuuskeskus**	ViVi	Ei	2, 10
	Yllä olevaan liittyviä toimenpiteitä:			
38	*Tilannetietoisuuden ja tilanneymmärryksen parantaminen LVM:ssä*	LVM	Ei	2
39	*CERT-toiminnon kehittäminen*	ViVI	Ei	1, 2, 3, 7
40	Selvitys tietoturvallisuuspoikkeamista ilmoittamisen käytännöistä ja yhteistyöstä	LVM	Ei	1, 4, 5, 8
41	**Puolustusvoimien kyberturvallisuustilannekuvan luominen**	PLM, PV	Ei	1,2, 3, 4, 5, 6, 9
Tehokas ja turvallinen julkishallinto – Tiedonhankinta ja tutkinta kyberympäristössä				
42	**Kansallisen lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista**	PLM	Kyllä	4, 5, 8
43	**Kansallinen kybervalvonta ja kybertiedustelu**	PLM, PV	Kyllä	1, 2, 3, 4, 5, 6, 9

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

44	**Kyberrikosten tutkinta**			
	Yllä olevaan liittyviä toimenpiteitä:			
45	*Selvitys esitutkintaviranomaisen toimivaltuuksista kyberrikostorjunnassa*	Poha	Ei	4
46	*Tietoverkkorikososaamisen liittäminen poliisin 24/7 yhteyspisteeseen ja kansainvälisten palveluiden turvaaminen*	KRP	Ei	4
47	*Kyberrikostilannekuva ja -tiedonhankinta*	KRP, Tulli	Ei	4
48	Kyberrikostutkinnan järjestäminen ja resursointi	KRP, Tulli	Ei	4
Kansalaisten hyvinvointi ja yritysten menestys – Osaamisen kehittäminen				
49	**Kokonaiskuva kyberosaamisen nykytilasta ja toimenpiteet alan tutkimus- ja kehitystyön sekä innovaatiotoiminnan kapasiteetin kehittämiseen**	OKM	Ei	7
	Kansalliset laajat tutkimusohjelmat:			
50	*ICT 2023 tutkimus-, kehitys- ja innovaatio-ohjelma*	Suomen Akatemia, Tekes	Ei	7
51	*INKA, Tekesin strategiset tutkimusavaukset ja TKI -rahoitus*	Tekes	Ei	7
52	**Tietoyhteiskuntaosallisuus ja medialukutaidot**	OKM	Ei	7
	Esimerkkejä koulutus- ja tutkimushankkeista:			
53	*JYVSECTEC – Jyväskylä security technology – turvallisuusteknologian kehittämishanke*	JAMK	Ei	7
54	*Informaatioturvallisuuden yliopistotasoinen koulutus (Jyväskylän yliopisto)*	JYO	Ei	7
55	*Kyberturvallisuuden ylempi korkeakoulututkinto (JAMK)*	JAMK	Ei	7
56	*Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK-tutkinto (Laurea)*	Laurea	Ei	7
57	*Turvallisuusosaamisen koulutus, ylempi AMK-tutkinto (Laurea)*			7
58	*Kyberturvallisuuskurssi (Maanpuolustuskoulutusyhdistys, MPK))*	MPK	Ei	7
	Esimerkkejä HVK:n yrityksille suunnatusta koulutuksesta ja suunnittelusta:			
59	*ICT-poolin tuki muille pooleille*	HVK	Ei	2, 3, 7

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

	toimialojen kyberturvallisuuden kehittämisessä			
60	*Kyberturvallisuus tutuksi – kampanja*	HVK	Ei	3, 7
Kansalaisten hyvinvointi ja yritysten menestys – Hyvinvointipalvelujen turvaaminen				
61	**Sähköisen identiteetin hallintaratkaisu**	VM	Ei	1, 3
62	**Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin kansalliset täytäntöönpanotoimet**	OM	Kyllä	8
63	**Kevyet käyttöliittymät Kanta – järjestelmään ja Kansa-järjestelmän kehittäminen**	STM	Ei	7, 9
64	**Sosiaali- ja terveydenhuollon järjestämislaki, sosiaalihuoltolaki ja muutokset terveydenhuoltolakiin**	STM	Kyllä	8
65	**Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)**	STM	Kyllä	8
Kansalaisten hyvinvointi ja yritysten menestys – Yritysten toimintaedellytykset ja jatkuvuuden hallinta				
66	**FISC -kyberlaboratorio**	FISC	Ei	1, 2, 3, 7
67	**RGCE-kybertoimintaympäristö (Realistic Global Cyber Environment)**	JAMK	EI	2, 3, 5, 7
68	**HUOVI -tilannekuvatoiminnon jatkaminen, laajentaminen ja kehittäminen sisäisen turvallisuuden ohjelman mukaisesti**	HVK		2, 3, 6
69	**Kriittisten valvomoiden yhteistoiminnan kehittäminen**	HVK	Ei	1, 2, 3
70	**Selvitys tietoliikenneyhteyksien varmistamisesta**	ViVi	Ei	2, 3, 7
71	**Selvitys suomalaisen ICT -sektorin sääntelyn vaikutuksista Suomen kilpailukykyyn**	LVM	Ei	8
	Huoltovarmuuskeskuksen palveluihin liittyviä toimenpiteitä:			
72	*Teollisuusautomaation kybersuojauksen käytännöt ja kartoitukset (2014-2015)*	HVK	Ei	1, 2, 3
73	*Teollisuuden kyberturvallisuuden vaatimusten jalkauttaminen tuotantoon (2014-2016)*	HVK	Ei	1, 2, 3
74	*Tuotantoautomaatioverkon monitorointipalvelu (2014-2016)*	HVK	Ei	1, 2, 3

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

LIITE 1: KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO-OHJELMAN ESITYKSET

TEHOKAS JA TURVALLINEN JULKISHALLINTO

Kriittiset toiminnot ja järjestelmät

1. HALLINNON TURVALLISUUSVERKKOHANKKEEN (TUVE) JA TOIMIALARIIPPUMATTOMIEN ICT-TEHTÄVIEN (TORI) KEHITTÄMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 3
EHDOTUKSEN VASTUUTAHO: VM	EHDOTUKSEN YHTEISTYÖTAHOT: Kaikki Valtioneuvoston organisaatiot
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Keskeiset viranomaistahot ovat mukana turvallisuusverkon ja palveluiden kehittämisessä, ja hankkeiden resursointiin kiinnitetään vakavaa huomiota. **2. TOIMINTOJEN PRIORISOINTIIN PERUSTUVAN JÄRJESTELMÄLUOKITUKSEN JA KOKONAISPRIORISOINNIN TUOTTAMINEN JA NÄILLE PÄÄTÖKSENTEKO- JA TOTEUTUSPROSESSIN TOTEUTTAMINEN** ICT-palveluja ja niiden kautta hallinnon palveluja kansalaisille, yrityksille ja virkamiehille on pystyttävä priorisoimaan, jos vakavissa häiriötilanteissa resurssit ovat rajallisia. Priorisointi on vaikea tehtävä ja sen on tapahduttava tiukoilla ja hyvin määritellyillä yhdenmukaisilla kriteereillä. Palvelun omistajan, palveluntarjoajan tai palvelujen käyttäjän mielipide tai tahdonilmaisu yksin ei riitä. Koska priorisointi merkitsee samalla palvelujen priorisointia, tulisi selvittää ennakoivasti tehtävän suunnitelman/ luokittelun hyväksymismenettely ja luokittelun soveltamisesta häiriötilanteessa tapahtuva hyväksymismenettely. Priorisoinnissa on syytä ottaa huomioon useita periaatteita: miten järjestelmä vaikuttaa valtion toimintakykyyn (esim. VN verkko, järjestelmänhallinnan työkalut) miten järjestelmä vaikuttaa kansalaisten palveluihin ja yhteiskunnan elintärkeisiin toimintoihin (esim. pelastuspalvelu) luokittelua ei voida soveltaa mekaanisesti vaan kussakin häiriötilanteessa siihen parhaiten soveltuvalla tavalla, kattavuus toimialariippumattomien (mm.TORI, TUVE) sekä toimialariippuvien palveluiden näkökulmasta. Järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön.	
EHDOTUKSEN AIKATAULU:	
3. JÄRJESTELMÄRIIPPUVUUKSIEN SELVITTÄMINEN LAATIMALLA YLLÄPIDETTÄVÄ MONITASOINEN RIIPPUVUUSKUVAUS	
Vakavien häiriöiden selvitystilanteissa on tiedettävä nopeasti mihin yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta keskeisiin järjestelmiin ja toimintaprosesseihin häiriötilanne vaikuttaa. Tämän toteutus vaatii tietojärjestelmäkokonaisuutta, jossa osana ovat SecICT-hankkeessa koottavat laite-, ympäristö-, konfiguraatio- ja riippuvuustiedot sekä TORI:n ja TUVE:n tuotannonohjauskokonaisuudet. Näitä tietoja tuotetaan, päivitetään SecICT-hankkeen ohjauksessa etenkin TORI- ja TUVE-tuotannon toimesta. TORI:n ja TUVE:n tuotannonohjausjärjestelmät on erotettava fyysisesti toisistaan, jotta eliminoidaan mahdollisuuksien mukaan tätä kautta turvallisuusviranomaisiin kohdistuvien kyberhyökkäysten mahdollinen eskaloituminen TUVE-sisäverkkoon. Tietoja päivitetään mahdollisimman automaattisesti, kun järjestelmään tallennetaan tarvittavat tiedot ja kuvaukset. Tietojen määrittäminen palvelua varten on	

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

pakollista. Osa näistä tiedoista kerätään valtionhallinnon organisaatioista GovHUOVI-portaalin kautta. Järjestelmän takaisinmaksuaika tapahtuisi osittain jo säästyneinä kustannuksina nopeutuvasta häiriötilanteen vaikutuksen nopeammasta rajaamisesta ja häiriön- tai ongelmanratkaisuprosessin nopeutumisena, kun se voidaan kohdistaa oikeaan kohteeseen. Tällöin myös palvelukeskuksen asiakkaille voidaan tuottaa tarkempaa häiriöviestintää, kun häiriö ja sen vaikutus saadaan rajattua suoraan järjestelmässä olevien määritysten perusteella automaattisesti.

EHDOTUKSEN AIKATAULU: Toteutus tapahtuu vaiheittain vuosina 2014-2017.

4. TIETO- JA VIESTINTÄJÄRJESTELMIEN ENERGIAN SAATAVUUDEN RISKIKARTOITUS

Selvitetään tärkeimpien tieto- ja viestintäjärjestelmien osalta niihin kohdistuvat energian saantiin liittyvät riskit ja niiden pienentämismahdollisuudet. Selvityksen tulee kohdistua erityisesti tietoliikenneyhteyksien ja päätelaitteiden käyttöpaikkojen sähkönsaantiin.

EHDOTUKSEN AIKATAULU: Tehdään vuoden 2014 aikana. Tulokset raportoidaan asiakkaille 31.5.2015 mennessä.

5. VALTION KONESALI- JA KAPASITEETTIPALVELUSTRATEGIA

TORI-palvelut sekä Työ- ja elinkeinoministeriö luovat yhteisen valtion konesali- ja kapasiteettistrategian valtiovarainministeriön johdolla. Työssä arvioidaan myös uusia mahdollisia asiakastarpeita. Konesali- ja kapasiteettistrategian tavoitteena on huomioida kyberturvallisuus koko konesali- ja kapasiteettipalvelukokonaisuuden osalta. Synergiahyötyjen täysitehoiseksi hyödyntämiseksi tulee kokonaisuuden osana työssä tarkastella myös Suomen Erillisverkot Oy:n (Leijonaverkot Oy) hallussa olevia kriittisiä konesali- ja laitesuojatiloja.

EHDOTUKSEN AIKATAULU:

6. ICT-PALVELUIDEN JA PALVELUTOIMITTAJIEN HALLINTA

Noin kolmannes julkisen hallinnon ICT -kuluista on ICT -palveluiden ostoa, pääosin yksityisiltä yrityksiltä. Palvelutoimitus on usein sirpaloitunutta ja ketjuuntunutta. Lähes poikkeuksetta yhden ICT -palvelun toimittamiseen osallistuu useita palvelutoimittajia, joilla saattaa olla jopa 160 nimettyä alihankkijaa.

Ostajan puolella julkisessa hallinnossa ostaminen ja ostamisen osaaminen on hajaantunut suurelle määrälle toimijoita. Palveluiden tilaaminen ja toimittaminen vakavissa häiriötilanteissa ja poikkeusoloissa on ollut harjoittelun kohteena vuosien 2009 - 2013 TIETO-harjoituksissa. Niiden tuloksena ei kuitenkaan ole syntynyt yhteistä ymmärrystä tai dokumentoitua toimintatapaa.

Palvelutoimittajien kanssa sovittavaan toimintatapaan tulee arvioida vaatimukset palvelusopimukseen kuuluvien kyberturvallisuuskontrollien toteuttamisesta ja kyberturvallisuuden näkökulmasta riittävän tietoturvatason, varautumisen ja kapasiteettitason takaamisesta. Järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. TUVE-palveluiden pitää toimia kaikissa olosuhteissa, mikä on jo lähtökohtavaatimus TUVE-palveluille. TUVE-palveluiden vastuullinen integraattori on tällä hetkellä HALTIK. TORI:n toiminnan käynnistyessä on huomioitava, että TUVE:n liittyvät toiminnot on erotettava muusta toiminnasta toiminnallisesti, taloudellisesti ja hallinnollisesti. Toimenpiteessä on huomioitava myös yritysturvallisuusselvitysten rooli hankintasopimuksissa.

EHDOTUKSEN AIKATAULU:

Vuoden 2014 loppuun mennessä suunnitellaan toimittajahallinnan kokonaisprosessi. Sen päävastuullinen toteuttaja palveluintegraattorina on TORI. Prosessi otetaan käyttöön 2015 alusta alkaen sitä mukaa kun palvelut siirtyvät TORI:n vastuulle. Vuoden 2013 ja 2015 TIETO harjoitusten välissä suunnitellaan ja dokumentoidaan toimintatapa, jonka mukaan toimittajien kanssa toimitaan tilanteissa, joissa resursseja on vähemmän kuin palvelupyynnöt tarvitsisivat. Tämä toimintatapa testataan vuoden 2015 TIETO harjoituksessa. Kokonaisprosessien määrittelyssä on huomioitava HALTIK:n rooli TUVE:n palveluintegraattorina.
7. TIETOJÄRJESTELMIEN JA NIIDEN ALUSTOJEN SEKÄ TIETOLIIKENNELAITTEISTOJEN JA –OHJELMISTOJEN HAAVOITTUVUUKSIEN HALLINNAN KEHITTÄMINEN
Otetaan käyttöön kaikki valtionhallinnon yhteiset ja virastojen omat tietojärjestelmät kattava suunnitelmallinen ja koordinoitu haavoittuvuuksien hallintaprosessi ja hankitaan sitä tukeva tekninen järjestelmä. Prosessin käyttöönotto edellyttää myös neuvotteluja ja muutoksia järjestelmätoimittajien kanssa tehtäviin palvelusopimuksiin. Suunnitellun haavoittuvuuksien hallinnan kehittämisen lisäksi on tarpeen arvioida laitteiden, järjestelmien ja palvelujen haavoittuvuuksia ja palveluiden suojauksia. Toimenpide käynnistyy kuvausten, priorisoinnin, tavoitteiden ja aikataulun tarkentamisella.
EHDOTUKSEN AIKATAULU:
8. KYBERYHTEYSTIETOJEN VASTUUNJAKO- JA VIRKALUETTELO SEKÄ TOIMINTAPROSESSIN KUVAUS
Luodaan valtionhallinnon toimijoiden ja kumppaneiden tarvitsema yhteystietoluettelo kyberilmoituksia ja prosesseja varten. Vastuunjakotaulukon perusteella kehitetään toimiva tilanteenmukaiseen johtamiseen soveltuva johtamisjärjestelmä, joka kykenee hyödyntämään reaaliaikaisesti tilannekuvaa ja pystyy johtamaan tarvittavat toimenpiteet sekä johtamaan viestintää tilanteessa. Kartoituksella saadaan aikaan organisaatioiden sisäistä toimintaa palveleva yhteysluettelo, laajemmin koko valtionhallintoa sekä siihen liittyviä toimijoita (yrityksiä) koskeva luettelo ja perusteet yhteistyöprosessien kehittämiselle. Työssä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön.
EHDOTUKSEN AIKATAULU:
9. TURVALLISTEN MOBIILIEN VIESTINTÄRATKAISUJEN NOPEA KÄYTTÖÖNOTTO
Parannetaan nopealla aikataululla ministeriöissä sekä joillakin hallinnonaloilla aikaisempaa turvallisempia yhteisiä mobiileja viestintäratkaisuja ja selvitetään ratkaisun liittymistä TUVE-kokonaisuuteen.
EHDOTUKSEN AIKATAULU: Tavoiteaikataulu on 2014.

10. SALATUN TIEDONSIIRRON JA HALLINNON TURVALLISUUSVERKON PALVELUINTEGRAATION (SATU-PALVELUINTEGRAATIO)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1,2 ja 9
EHDOTUKSEN VASTUUTAHO: VM, JulkICT, UM	EHDOTUKSEN YHTEISTYÖTAHOT: Käyttäjätahot ovat valtion johto, turvallisuusviranomai-

	set ja TUVE-lain perusteella määräytyvät toimijat
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Salatun tiedon sähköisen käsittelyn ratkaisut on koottu yhteen hankkeeseen (SATU), joka mahdollistaa nykyistä helpommat menetelmät salatun tiedon käsittelyyn viranomaisten välillä. Perustettavassa hankkeessa korotetaan valtion johdon, ministeriöiden ja virastojen ICT-infrastruktuuri ja -palvelut tarvittavilta osin kansallisen lainsäädännön ja EU-vaatimusten edellyttämälle korkealle tietoturvatasolle. Päätavoite on parantaa valtionjohdon ja viranomaisten vuorovaikutusta tehostamalla työn tuottavuutta salassa pidettävän sekä kansallisen ja kansainvälisen turvaluokitellun tiedon käsittelyn ja välittämisen toimintaprosesseja kehittämällä. Tulevat SATU-palvelut ovat Salve-arkkitehtuurin mukaisesti toteutettavia avoimeen lähdekoodiin perustuvia korkean tietoturvatason ja varautumisen vaatimusten mukaisesti toteutettuja palveluita kuten: viestintäratkaisu, työryhmäympäristö, tilannekuvaportaali sekä liikkuvan käyttäjän tarvitsemat palvelut. Hankkeeseen on ehdotettu lisättäväksi mobiilipäätelaitteita tukeva yhteinen korkean turvallisuuden mahdollistava liikkuvan työskentelyn ympäristö sekä salattu globaalisti toimiva mobiili viestiyhteys. Globaalin ratkaisun tavoitteena on, että ulkomaan virkamatkalla olevalla virkamiehellä olisi mahdollisuus käsitellä suojaustasolle 3 kuuluvia tietoja (puhe, tekstiviestit, data). Hankkeessa arvioidaan salatun tiedonsiirron mahdollisuutta yksityisten toimijoiden esimerkiksi ydinvoimalaitosten kanssa.	
EHDOTUKSEN AIKATAULU: 2014 – 2018.	

Viranomaisten osaamisen ja kyvykkyyksien kehittäminen

11. VALTIONEUVOSTON TIETOTURVAVERKOSTO VIRALLISTETAAN MINISTERIÖIDEN TIETO- JA KYBERTURVALLISUUDEN VIRALLISEKSI YHTEISTYÖRYHMÄKSI.	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1 ja 2
EHDOTUKSEN VASTUUTAHO: VNK	EHDOTUKSEN YHTEISTYÖTAHOT: Kaikki hallinnonalat
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Tavoitteena on turvata oikea-aikainen päätöksenteko kaikissa oloissa kaikilla valtionhallinnon päätöksentekotasoilla. Hyödyllisiksi koettuja yhteistyöfoorumeita ehdotetaan samalla laajennettavaksi siten, että hallinnollinen ”koordinaatioryhmä” keskittyen kyberturvallisuuden hallintaan ja luokitteluun ja ”tekninen ryhmä” keskittyisi tietojärjestelmien hyödyntämiseen. Edellä mainittujen ja muiden ryhmien toiminnassa on vältettävä päällekkäisyyttä.	

12. EHDOTUKSIA VALTIONHALLINNON TIETO- JA KYBERTURVALLISUUDEN JOHTORYHMÄN (VAHTI) TOIMINTASUUNNITELMAAN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN:1, 3 ja 9

EHDOTUKSEN VASTUUTAHO: VM	EHDOTUKSEN YHTEISTYÖTAHOT: Hankkeiden vetovastuu tulee nimetä jollekin organisaatiolle, työmääräarviot saa pääpiirteittäin Valtiokonttorin tietoturvatasoyhteishankkeista.

EHDOTUKSEN KUVAUS JA PERUSTELUT

Valtiovarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. Sen kehittämiseksi ovat seuraavat esitykset:

13. ICT-VARAUTUMISEN JA KYBERVAATIMUSTEN TOTEUTTAMINEN YHTEISHANKKEILLA KOKO VALTIONHALLINNOLLE

Tavoitteena hallinnon kyberturvallisuuden hallinnassa on, että ICT-varautuminen on jatkuvaa toimintaa, jolla pyritään etukäteisvarautumiseen ja nykyisen hallinnan tason reaaliaikaiseen tietoon. Ehdotuksen mukaan tulisi käyttää enemmän hallinnon yhteisiä välineitä. Välineenä kyberturvallisuuden toteuttamiselle voisivat toimia tietoturvatasojen ja ICT-varautumisen vaatimukset, minkä vuoksi ei luoda uusia vaatimuskehikkoja, vaan hyödynnetään olemassa olevia vaatimuksia. Työssä yhtenäistetään hallinnonalojen kyberturvallisuuden käytäntöjä, hyödynnetään yhteisiä malleja ja välineitä. Työssä on varmistuttava siitä, että päällekkäisyyksiä muiden tietoturvan kehityshankkeiden kanssa ei tule, tietoturvatyön kehittämisen kokonaisuus etenee hallitusti ja taloudellisesti ja organisaatioiden erilaiset turvallisuusvaatimukset tulevat huomioiduksi.

14. TIETOTURVAHENKILÖSTÖN OSAAMISEN PARANTAMINEN JA VERKOSTOITUMINEN HALLINNOSSA

Parannetaan tietoturvallisuushenkilöstön osaamista järjestämällä vuosittain valtionhallinnon yhteisiä seminaareja ja koulutustilaisuuksia, joissa alustajina on kyberturvallisuuden parhaita asiantuntijoita niin hallinnosta kuin yritysmaailmastakin. Tilaisuuksien ohjelman tulisi olla sellainen, että niihin osallistujat voivat saada niitten kautta parhaan mahdollisen tiedon, josta olisi organisaatioiden toiminnassa myös selkeää (mitattavaa) hyötyä. Parempaa osaamista voidaan hyödyntää mm. riskienarvioinneissa ja mahdollisissa kyberpoikkeamatilanteiden arvioinneissa. Tietoturvallisuushenkilöstön tulee verkostoitua ja oppia tuntemaan toisiaan yhä paremmin, jolloin myös ns. epävirallinenkin tiedonkulku paranee.

EHDOTUKSEN AIKATAULU:

15. KANSALLISEN KRYPTOLABORATORION PERUSTAMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1,2,3,4,5,6 ja 9
EHDOTUKSEN VASTUUTAHO: PV	EHDOTUKSEN YHTEISTYÖTAHOT: Viestintävirasto, turvallisuusviranomaiset, yksityinen sektori ja tiedeyhteisö

EHDOTUKSEN KUVAUS JA PERUSTELUT

Hankkeessa kehitetään kansallista salausteknistä osaamista. Tavoitteena on, että Suomi on kryptologian osaamisessa samalla tasolla kuin muut eurooppalaiset valtiot.

Kehittämisen kulmakiveksi perustetaan kansallinen kryptolaboratorio, joka toimii kryptologian osaamiskeskuksena verkottamalla kansalliset toimijat viranomaiskentässä, yksityisellä sektorilla sekä tiedeyhteisössä. Kryptolaboratorioon luodaan tekninen ympäristö, jossa kehitetään

osaamista osaamista ja suorituskykyä salausteknisten ratkaisuiden ja tuotteiden testaamiseksi ja niiden vahvuuden verifioimiseksi. Kryptolaboratorio tukee muita viranomaisia, esimerkiksi Viestintäviraston NCSA-FI -toimintoa, salausratkaisuiden evaluoinnissa tarjoamalla käytännön tason testaus- ja verifiointipalveluita. Kryptolaboratorio tekee lisäksi yhteistyötä tiedeyhteisön kanssa tukemalla kryptologian tutkimustyötä sekä tarjoamalla teknisen laboratorioympäristön resursseja tutkimuskäyttöön.

EHDOTUKSEN AIKATAULU: Rakentaminen 2014 – 2018.

ESIMERKKEJÄ HALLINNONALAKOHTAISESTA KOULUTUKSESTA:

16. KANSALLISEN TURVALLISUUSVIRANOMAISEN ANTAMA KOULUTUS VIRANOMAISILLE (kansainvälistä luokiteltua aineistoa käsittelevät viranomaiset)

Kansallinen turvallisuusviranomainen (NSA) antaa koulutusta kansainvälisiin tietoturvavelvoitteisiin liittyvistä toimenpiteistä kuten asiakirjojen käsittelystä ja yhteistyössä henkilöturvallisuusselvityksiä laativien toimivaltaisten viranomaisten kanssa henkilöturvallisuusselvityksen ja -todistuksen (PSC) hakumenettelystä. Ensisijaisesti koulutusta annetaan ministeriöille ja näiden alaisille virastoille, jotka säännönmukaisesti käsittelevät kansainvälisiä turvallisuusluokiteltuja tietoja.

EHDOTUKSEN AIKATAULU: Koulutusta jatketaan vuonna 2014.

17. YHTEISTOIMINTAMALLIN HARJOITTELU LIIKENNE- JA VIESTINTÄMINISTERIÖSSÄ

Liikenne- ja viestintäministeriön hallinnonala järjestää, koordinoi ja harjoittaa sellaista harjoitustoimintaa, joka parantaa mm. eri toimijoiden kykyä ylläpitää toimintojaan ja harjoittaa kriisiviestintää sähköisten tieto- ja viestintäjärjestelmien häiriötilanteissa.

EHDOTUKSEN AIKATAULU: Jatkuvaa

18. RIKOSTORJUNNAN KYBEROSAAMISEN KEHITTÄMINEN POLIISIAMMATTIKORKEAKOULUSSA

Osaamisen kehittäminen on strategisesti eräs tärkeimmistä poliisihallinnon tehtävistä kyberturvallisuusstrategian tavoitteiden saavuttamisessa. Tämä vaatii laaja osaamisen kehittämistä mm. kyberasioiden lisäämisellä poliisin peruskoulutukseen. Alaan erikoistuville poliiseille tulee tarjota laadukas ja tehokkaasti järjestetty erityiskoulutus (tekninen ja taktinen tutkinta). Poliisiammattikorkeakoulun roolia tulee kehittää kyberrikostorjuntaosaamisen nostamisessa. Poliisihallinnon alan asiantuntijat (erityisesti KRP, Supo) osallistuvat työhön mm. koulutusten sisällön määrittelyin ja itse koulutuksen antamiseen. Poliisiyksiköt tulee velvoittaa kouluttaa riittävä määrä henkilöstöä (tutkinnanjohtaja ja tutkija) ammattitaitoisen esitutkinnan turvaamiseksi. Osaamisen kehittämisessä työssä oppiminen on yksi tehokkaimmista tavoista. Tämän vuoksi työkierron kehittäminen ja lisääminen poliisihallinnossa on tärkeää. Poliisiammattikorkeakoulun tulee lisätä kyberalan tutkimusta sekä yhteistyötä yliopistojen tutkimusryhmien kanssa. Poliisin asiantuntijoiden tulee varmistaa oma osaaminen sekä kansallisesti tarjottavan koulutuksen laatu kansainvälisen yhteistyön avulla (kurssit, tieteelliset konferenssit ja kokoukset). Tavoitteena osaamisen kehittämisessä on ajantasainen, korkealaatuinen ja kustannustehokas tietoverkkorikostutkinnan koulutus. Tulli kehittää Tullin rikostorjunnan kyberosaamista itse ja tiiviissä yhteistyössä Poliisiammattikorkeakoulun kanssa.

EHDOTUKSEN AIKATAULU: Tavoiteaikataulu on 2014-2016

19. KYBERPUOLUSTUKSEN HARJOITUS-, KOULUTUS- JA TUTKIMUSTOIMINNAN KEHITTÄMINEN
Puolustusvoimat luo tiedustelun, vaikuttamisen ja suojautumisen suorituskykyjä kehittämällä osaamista kyberpuolustuksen osa-alueella harjoitus-, koulutus- ja tutkimustoiminnan kautta kyberturvallisuusstrategian linjausten mukaisesti. Kansallista kyberpuolustusharjoitus- ja koulutustoimintaa kehitetään sekä mahdollistetaan muiden viranomaisten, huoltovarmuuskriittisten toimijoiden, alan yritysten, tiedeyhteisön ja alan yhdistysten osallistuminen yhteistoiminnassa Puolustusvoimien kanssa. Harjoitustoimintaa kehitetään järjestämällä ja osallistumalla kansallisiin ja kansainvälisiin kyberturvallisuusharjoituksiin yhdessä yhteistyötahojen kanssa sekä käyttämällä ja kehittämällä aktiivisesti saatavilla olevia harjoitusympäristöjä. Koulutustarjonnan hyödyntämistä tehostetaan järjestämällä ja hankkimalla koulutustilaisuuksia yhdessä yhteistahojen kanssa. Kyberpuolustuksen tutkimukseen panostetaan kansallisesti ja kansainvälisesti. Tutkimusta tehdään kansallisten ja kansainvälisten tutkimusprojektien ja -toimeksiantojen muodossa. Tutkimusten tulokset saatetaan yhteistyötahojen hyödynnettäväksi. Puolustusvoimille annetaan oikeus erillisessä, suojatussa ympäristössä ja tietoverkossa suunnitella ja testata kaikkia kyberhyökkäysmenetelmiä.
EHDOTUKSEN AIKATAULU: Rakentaminen 2014 – 2018.

20. HENKILÖTURVALLISUUSTODISTUS (PERSONAL SECURITY CLEARANCE, PSC) – TEHTÄVÄMÄÄRITTELY	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN:7, 9
EHDOTUKSEN VASTUUTAHO: NSA	EHDOTUKSEN YHTEISTYÖTAHOT: Kansainvälistä luokiteltua aineistoa käsittelevät viranomaiset
EHDOTUKSEN KUVAUS JA PERUSTELUT	
EU:n neuvoston turvallisuussääntöjen (2013/488/EU) mukaan jäsenvaltioiden on määriteltävä hallintorakenteissaan ne tehtävät, jotka edellyttävät pääsyä EU CONFIDENTIAL tai sitä korkeampaan turvallisuusluokan tietoihin ja sitä vastaavaa henkilöturvallisuustodistusta. Tehtävien määrittely tulee tehdä siten, että PRC-todistusta edellytetään vain sellaisissa tehtävissä, joissa on todellinen tiedonsaantitarve (need-to-know). Kansallinen turvallisuusviranomainen (NSA) tiedottaa ja kouluttaa viranomaisia, jotta PSC-todistusta edellyttävät valtionhallinnon ja muiden viranomaisten tehtävät voidaan määritellä yhdenmukaisella tavalla ja EU-velvoitteita vastaavasti.	
EHDOTUKSEN AIKATAULU: 2014	

21. YHTEISTOIMINTAMALLIN KEHITTÄMINEN LVM:SSÄ	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1
EHDOTUKSEN VASTUUTAHO:	EHDOTUKSEN YHTEISTYÖTAHOT: Hallinnonalat ja elinkeinoelämä

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

EHDOTUKSEN KUVAUS JA PERUSTELUT
Liikenne- ja viestintäministeriö huolehtii kybertoimintaympäristön olemassaolon, saatavuuden, toimivuuden ja luotettavuuden kannalta keskeisestä sähköisen viestinnän ja viestinnän luottamuksellisuuden yleisestä ohjauksesta. Liikenne- ja viestintäministeriö valmistelee sähköisen viestinnän toimintavarmuuden sekä viestinnän luottamuksellisuuden laatuvaatimukset sekä toimialaansa koskevat häiriötilanteiden hallinnan edellyttämät valtioneuvoston toimenpiteet, järjestää hallintonsa asianmukaisen toiminnan ja osallistuu häiriötilanteiden hallinnan edellyttämään yhteistyöhön valtioneuvostossa. Liikenne- ja viestintäministeriö on asettanut pysyvän virkamiestoimikunnan viestintämarkkinoiden sääntelyyn, sähköisten viranomaisverkkojen tarjontaan ja viestintäyritysten omistajapolitiikkaan kuuluvien viranomaistehtävien tukemiseksi ja niiden sovittamiseksi yhteen. Liikenne- ja viestintäministeriö osallistuu huoltovarmuusorganisaation tietoyhteiskuntasektorin sekä logistiikkasektorin työhön valtakunnallisella ja alueellisella tasolla ylläpitääkseen ja kehittääkseen maamme kuljetuslogistisen järjestelmän ja sähköisen tieto- ja viestintäinfrastruktuurin toimintaedellytyksiä huoltovarmuuden tavoitteista annetun valtioneuvoston päätöksen mukaisesti. Liikenne- ja viestintäministeriön hallinnonala osallistuu kyberturvallisuuden yhteistyöverkoston toimintaan ja toimii yhteistyössä mm. tietoa vaihtamalla perustettavan kyberturvallisuuskeskuksen kanssa. LVM kehittää kyberturvallisuuskeskuksen toimintaa ja tulosohjausta kyberturvallisuustyöryhmän avustamana. Liikenne- ja viestintäministeriö koordinoi viestinnän yhteistyötä hallinnonalan virastojen ja yhtiöiden viestinnän yhteistyöryhmän kautta ja osallistuu valtioneuvoston viestintäjohtaja- ja muihin yhteistyöryhmiin. Pidetään yllä hyviä yhteistyösuhteita liikenne- ja viestintätoimialan yritysten viestintävastaavien kanssa.
EHDOTUKSEN AIKATAULU: Jatkuvaa

22. KYBERUHKIIN VARAUTUMISEN SISÄLLYTTÄMINEN SOSIAALI- JA TERVEYDENHUOLLON UUSITTAVAAN VALMIUSSUUNNITTELUOHJEISTUKSEEN JA OHJEISTUKSEN JALKAUTTAMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1,3 ja 9
EHDOTUKSEN VASTUUTAHO: STM	EHDOTUKSEN YHTEISTYÖTAHOT: SM, HVK, sosiaali- ja terveydenhuollon alueet, AVIt, Pelastusopisto
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Sosiaali- ja terveydenhuollon valmiussuunnitteluohjeistus uusitaan ja kyberuhkiin varautuminen sisällytetään ohjeistukseen. Ohjeistuksen uusiminen toteutetaan pilottina yhdellä sosiaali- ja terveydenhuollon alueella yhteistyössä kyseisen alueen, HVK:n, elinkeinoelämän ja järjestöjen kanssa. Pilotin ensivaiheen jälkeen järjestetään seminaarisarja varautumisesta ja erityisesti kyberuhkiin varautumisesta sosiaali- ja terveydenhuollon paikalliselle ja alueelliselle tasolle. Jatkossa kyberuhkiin varautuminen sisällytetään STM:n yhteistyössä Pelastusopiston kanssa toteuttamiin varautumisen koulutuksiin sekä Aluehallintovirastojen yhdessä Puolustusvoimien kanssa järjestämiin alueellisiin maanpuolustuskurssien sisältöihin.	

EHDOTUKSEN AIKATAULU: Hanke aloitetaan vuonna 2014. Hankkeen lopullinen etenemisaikataulu riippuu päätöksistä sosiaali- ja terveydenhuollon palvelujärjestelmän rakenteesta ja aikataulusta. Hanke valmistuu osakokonaisuuksina. Kokonaisuuden todennäköinen valmistumisaikataulu on 2017.

23. STM:N HALLINNONALAN KYBERUHKIIN VARAUTUMISEN KEHITTÄMINEN, KRIITTISTEN TOIMINTOJEN TUNNISTAMINEN JA TOIMINTAMALLIN LAATIMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1, 3 ja 9
EHDOTUKSEN VASTUUTAHO: STM	EHDOTUKSEN YHTEISTYÖTAHOT: Asiantuntijalaitokset
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Kriittisyysluokitusta ja niihin liittyvien tietojärjestelmien ja tietojen tunnistamista jatketaan. Näiden pohjalta täydennetään varautumissuunnitelmat. Käynnistetään projekti kyberuhkien hallintaprosessin laatimiseksi ja uhkien tunnistamiseksi yhdessä asiantuntijalaitosten, elinkeinoelämän ja järjestöjen kanssa. Näin menetellen saadaan suurta synergiaetua virastojen ja ministeriön asiantuntemuksesta sekä mahdolliset yhteishankinnat tulevat kustannustehokkaaksi. Sosiaali- ja terveysministeriö välittää muille ministeriöille toimenpiteessä kerrytetyn uuden osaamisensa.	
EHDOTUKSEN AIKATAULU: Toteutus 2014	

24. KANSALLINEN KURIIRITOIMINTA	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN:1
EHDOTUKSEN VASTUUTAHO: Ulkomaan kuriiritoiminnan osalta UM ja pääkaupunkiseudulla VNK	EHDOTUKSEN YHTEISTYÖTAHOT:
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Valtionhallinnon kuriiritoiminta sekä pääkaupunkiseudulla että Helsingin ja ulkomailla sijaitsevien edustustojen välillä järjestetään uudelleen. Tarve valtion kuriiritoiminnan uudelleenjärjestämisestä johtuu ensisijaisesti kansainvälisistä tietoturvallisuusvelvoitteista ja teknologian kehittymisestä. Salatun elektronisen tiedonvälityksen enenevästä käytöstä seuraa henkilökuriirin lisääntyvä käyttötarve kansainvälisten salattua aineistoa koskevien käsittelyohjeiden johdosta. Valtion kuriiritoiminta järjestetään siten, että salassa pidettävä aineisto voidaan kuljettaa kansainvälisten ja kansallisten sääntöjen mukaisesti, turvallisesti ja oikea-aikaisesti. Tällä hetkellä eri hallinnonalojen toimintatavoissa turvallisuusluokitellun materiaalin ja salausavainten kuljettamisessa on eroja ja ohjeistuksessa päivittämisen tarvetta. Ulkomaille suuntautuvan henkilökuriiritarpeen kattamiseksi perustetaan kansallinen henkilökuriiripooli, johon osallistuu valmiuspohjalta ja oman toimen ohella yhteensä noin 35-40 valtionhallinnon virkamiestä, jotka koulutetaan kuriiritehtävään. He tulevat etupäässä ulkoasiainministeriöstä, puolustushallinnosta, sisäasiainhallinnosta ja Viestintävirastosta.	
EHDOTUKSEN AIKATAULU: 2014	

25. TIIVIIN JA KÄYTÄNNÖNLÄHEISEN SELVITYKSEN TUOTTAMINEN KYBERYMPÄRISTÖÄ KOSKEVASTA KANSAINVÄLISOIKEUDELLISESTA SÄÄNTELYSTÄ	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 7
EHDOTUKSEN VASTUUTAHO: UM	EHDOTUKSEN YHTEISTYÖTAHOT: PLM, Erik Castrén –instituutti ja Suomen Punainen Risti
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Selvitys kuvaisi kansainvälisoikeudellista normistoa, jolla on merkitystä kyber-asioiden ja niihin liittyvien ongelmatilanteiden käsittelyssä. Asiakokonaisuuden ulottuvuuksia ovat mm. hyökkäyskäsite ja kansainvälisen humanitaarisen oikeuden soveltuvuus. Tavoitteena on konkreettinen työkalu kansainvälisoikeudellisten kysymysten jäsentämiseen.	
EHDOTUKSEN AIKATAULU: Selvitys laaditaan tilaustutkimuksena vuoden 2014 aikana.	

26. KYBERTURVALLISUUDEN TERMIEN MÄÄRITTELY	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2 ja 7
EHDOTUKSEN VASTUUTAHO: Suomen Pelastusalan keskusjärjestö (SPEK)	EHDOTUKSEN YHTEISTYÖTAHOT: Turvallisuuskomitea ohjausryhmänä
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Suomen kyberturvallisuusstrategian liitteenä olevat käsitemääritelmät tarkastetaan terminologiaopillisesti osana meneillään olevaa varautumisen ja kokonaisturvallisuuden sanastotyöprojektia. Sanastotyöryhmä toimii yhteistyössä esimerkiksi VAHTI-ryhmän kanssa.	
EHDOTUKSEN AIKATAULU: 2014	

ESIMERKKEJÄ HALLINNONALAKOHTAISESTA STANDARDISOIMISTYÖSTÄ JA ARVIOINNEISTA

27. PUOLUSTUSVOIMIEN KYBERTURVALLISUUTEEN LIITTYVÄ TARKASTUSPROSESSI

Puolustusvoimat varmistaa omat toimintamahdollisuutensa kaikissa olosuhteissa suojaamalla ja valvomalla omat järjestelmänsä ja ympäristönsä. Ennaltaehkäisemisen kokonaisuuteen liittyy, että Puolustusvoimien tarkastus- ja akkreditointiprosessia kehitetään siten, että järjestelmät saavuttavat riittävän suojaus- ja kypsyystason ennen käyttöönottoa ja säilyttävät tämän tason elinkaarensa aikana. Tarkastuksissa nojaudutaan muun muassa tietoturvallisuusasetukseen (TTA 681/2010), kansalliseen turvallisuusauditointikriteeristöön sekä soveltuvin osin muuhun kansalliseen ja/tai kansainväliseen ohjeistukseen.

EHDOTUKSEN AIKATAULU:

28. VIRVE – VERKON TIETOTURVALLISUUSTILANTEEN ARVIOINTI JA RISKIANALYYSI

Selvitetään VIRVE – verkon tietoturvallisuuden taso ja sen käyttöön liittyvät riskit - huomioiden nykyinen toimintaympäristö sekä uhat. Mikäli puutteita havaitaan, niin laaditaan tarvittava kehittämissuunnitelma. Pyritään hyödyntämään riskianalyysissa GocHUOVI:n (SecICT) mahdollisuuksia.

EHDOTUKSEN AIKATAULU: 2014-2015
29. ILMATIETEEN LAITOKSEN ISO 27001-SERTIFIKAATTI
Ilmatieteen laitos on käynnistämässä tietoturvahanketta, jonka tavoitteena on saada laitoksen tietoturvan hallintajärjestelmä vastaamaan ISO 27001 standardin vaatimuksia sekä saada laitokselle ISO 27001 –sertifikaatti.
EHDOTUKSEN AIKATAULU: Hankkeen toteutus tapahtuu 2014-2015 aikana
30. LIIKENNEVIRASTON TIETOTURVATASOHANKE
Hankkeessa viraston tietojärjestelmien tietoturva- ja ICT-varautumisen tasot määritellään ja saatetaan luokitellut tietojärjestelmät vaaditulle tietoturva- ja varautumisen tasolle vuoteen 2016 mennessä. Hankkeelle on jo tiedossa jatko korotetun- ja korkean tietoturvan tason saavuttamiseksi. Korotettu ja korkea tietoturvan taso saavutetaan v. 2015 – 2016 vain niissä toiminnoissa, joissa se on ehdottoman tarkoituksenmukaista ottaen huomioon kyseessä olevaa toimintoa ohjaavat säädökset, tietoturvatyöhön käytettävissä olevat resurssit sekä toiminnon kriittisyys Liikenneviraston tehtävien hoidossa.
EHDOTUKSEN AIKATAULU: 2016 mennessä
31. ISO 27001 TIETOTURVALLISUUSSERTIFIOINTI LIIKENTEEN TURVALLISUUSVIRASTOSSA (TRAFI)
Trafin tietoturvallisuuden hallintamalli perustuu ISO 27001 –standardin mukaisesti riskienhallintaan ja on luonteeltaan riskilähtöinen. Tietoturvallisuuden hallintamalliin liittyvässä riskienhallinnassa käsitellään nimenomaan tietoriskejä. Riskienhallinta on aina osa tietoturvallisuuden hallintamallin vuosikelloa. Asetetut vähimmäisvaatimukset täyttävän riskienhallintamenetelmän olemassaolo on ISO 27001 –standardin perusvaatimus. Trafin tietoriskien hallinnan periaatteet ja menetelmä on kuvattu erillisessä säännöllisesti päivitettävässä menetelmäkuvauksessa, joka on osa tietoturvallisuuden hallintamallia. Menetelmäkuvaus kattaa myös riskien käsittelysuunnitelman ja jäännösriskien käsittelyn. Kyber-uhkat kohdistuvat joko suoraan tietojärjestelmiin tai tietojärjestelmien kautta muuhun toimintaan. Tietoturvallisuuden korkealla tasolla voidaan vastata osaltaan myös kyberuhkiin.
EHDOTUKSEN AIKATAULU:Trafin ISO27001 -sertifikaatin hankinta toteutettu loppuvuonna 2013, tietoturvan hallintomallia päivitetään jatkuvasti.

Tilannekuva

32. VALTION YMPÄRIVUOROKAUTISEN TIETOTURVATOIMINNAN KEHITTÄMISHANKE (SECICT)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1, 2 ja 3
EHDOTUKSEN VASTUUTAHO: VM – JulkICTtoiminto	EHDOTUKSEN YHTEISTYÖTAHOT: Viestintävirasto, TUVE- ja TORI –hanke, keskushallinnon uudistushanke (KEHU), KRP, Puolustusvoimat.

EHDOTUKSEN KUVAUS JA PERUSTELUT

Valtion vakavissa, laajavaikutteisissa ja usean hallinnonalan toimijan yhteistyötä vaativissa tietoturvatapahtumissa tarvitaan koordinointia. Joskus tilanteet vaativat selvitystyötä ja sellaisia korjaavia toimenpiteitä, joihin ei ole etukäteen varauduttu. Valtion sähköistä tietojenkäsittelyympäristöä ja siihen liittyviä ICT -palveluita ylläpidetään usein monen toimijan yhteistyöllä. Tällaisesta keskinäisriippuvaisesta ympäristöstä tulee pyrkiä muodostamaan valtion keskeisten toimintojen osalta ajantasaista tilannekuvaa. Kriittisten riippuvuuksien tunnistaminen, ongelmien vaikutusten laajuuden arviointi sekä valmiudet tilanteiden hallintaan tulee järjestää etukäteen.

Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeessa (SecICT) kehitetään ympärivuorokautista valtion keskeisiin toimintoihin kohdistuvien vakavien sekä laajavaikutteisten tietoturvapoikkeamien ennaltaehkäisyä ja hallintaa, valtion toiminnan kannalta keskeisen valtiohallinnon tieto- ja kyberturvallisuuden tilannekuvan hallintaa valtionhallinnolle tuotettavien ICT -palveluiden tietoturvallisuuden valvontaa ja tietoturvallisuuden ohjausta. Näihin tehtäviin perustetaan valtiovarainministeriön alaisuuteen uusi viranomaistoiminto, valtion ympärivuorokautinen tietoturvatoiminto.

Valtion ympärivuorokautinen tietoturvatoiminto kerää, analysoi ja jakaa järjestelmistä, sisäverkosta sekä muista lähteistä saatavaa tilannetietoa ja tilannekuvaa käytettäväksi eri tarpeisiin. Valtionhallinnon ympärivuorokautinen tietoturvatoiminnon tuottamaa valtionhallinnon tieto- ja kyberturvallisuuden tilannekuvaa koostetaan, analysoidaan ja jaetaan hallitusti yhteistyötahoille.

Valtiovarainministeriö ohjaa tällä hetkellä valtion keskeistä palvelutuotantoa mm. TORI-palvelukeskuksen ja TUVE-toiminnan kautta. Palvelutuotannossa kerättävää tietoa analysoidaan ensisijaisesti palvelutuottajien toimesta yhteistyönä valtiovarainministeriön asiantuntijoiden kanssa (myöhemmin ympärivuorokautisen tietoturvatoiminnon kanssa). Valtion ympärivuorokautinen tietoturvatoiminto kerää tilannetiedon lisäksi tarpeellista kriittisyys-, riippuvuus- ja turvallisuustietoa. Toiminto tukee ja huolehtii siitä, että valtion kriittisten järjestelmien haltuunotto on mahdollista poikkeusoloissa ja muissa vakavissa häiriötilanteissa. Tämä tapahtuu varmistamalla mm. riittävät laite-, ympäristö-, konfiguraatio- ja riippuvuustiedot.

Valtionhallinnon sisäverkkojen ja keskeisten tietojärjestelmien tiedot kootaan ja analysoidaan SecICT-hankkeessa suunniteltavilla erillisillä järjestelyillä ja järjestelmillä. Julkisen verkon ja sisäverkon rajapinnan suojaamiseksi käytetään useita järjestelyjä, joista Kyberturvallisuuskeskus tuottaa GovCERT- ja GovHAVARO-palveluja tukipalveluiksi valtion ympärivuorokautiselle tietoturvatoiminnolle. GovCERT- ja GovHAVARO-palveluiden havaitsemien tietoturvaloukkausepäilyjen koordinoinnista vastaa valtion ympärivuorokautinen tietoturvatoiminto.

EHDOTUKSEN AIKATAULU: Valtion ympärivuorokautinen tietoturvatoiminto on suunniteltu perustettavaksi 2015-2016.

Lisäksi SecICT:tä kehittävinä toimenpide-ehdotuksina on esitetty seuraavia:

33. KYBERTURVALLISUUDEN YHTENÄISEN JOHTAMISMALLIN JA HÄIRIÖTILANTEIDEN HALLINNAN PERIAATTEIDEN, TEHTÄVIEN JA NIIHIN LIITTYVIEN TOIMINTAMALLIEN SELKIYTTÄMINEN

Toimenpiteen tavoitteena on selvittää ja tarvittaessa yhtenäistää kyberturvallisuuden yhteistoiminta, yhteen sovittaminen ja toimintamallit. Työ perustuu olemassa olevaan lainsäädäntöön, ohjeisiin ja käytäntöihin. Kehittämisessä otetaan huomioon nykyisten ja valmisteilla olevien varautumiseen ja kyberturvallisuuden hallintaan liittyvien julkisen sektorin toimijoiden

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

tehtävät, roolit ja yhteistyö.
EHDOTUKSEN AIKATAULU: Aloitetaan vuonna 2014.

34. KOHDISTETTUJEN HAITTAOHJELMIEN HAVAINNOINTIKYVYN PARANTAMINEN

HALTIK kehittää SecICT-hankkeen kanssa HALTIKin hallinnoimien sisäverkkojen valvontakykyä siten, että siellä tapahtuneet muutokset ja poikkeava liikenne voidaan huomata ja reagoida mahdollisiin poikkeamiin. Tehtäviä toimenpiteitä ovat ainakin henkilöresurssien varaaminen, niiden kouluttaminen ja tarvittavien valvontajärjestelmien hankkiminen. Parannetaan tietoverkon tilannekuvaa siellä mahdollisesti olevien kohdennettujen haittaohjelmien tunnistamisen osalta luomalla kohdistettujen hyökkäysten havainnointiin tarkoitettu prosessi ja hankkimalla sen tueksi asianmukainen valvontaohjelmisto.

EHDOTUKSEN AIKATAULU:

35. HAVARO-VERKOSTON LAAJENTAMINEN JA TOIMINNAN KEHITTÄMINEN

HAVARO on Viestintäviraston tuottama ja Huoltovarmuuskeskuksen rahoittama järjestelmä, jonka tarkoitus on kehittää huoltovarmuuskriittisten organisaatioiden kykyä varautua tietoturvauhkiin. Järjestelmä tuottaa havaintoja ja varoituksia tietoturvauhkista. Järjestelmää laajennetaan kattamaan keskeisimpiä kriittisen infrastruktuurin osa-alueita tarvemukaisella otannalla vuoden 2014 aikana.

Valtionhallinnon julkisen verkon ja sisäverkon rajapinnan suojaamiseksi käytetään useita järjestelyjä, joista Kyberturvallisuuskeskus tuottaa GovCERT- ja GovHAVARO-palveluja tukipalveluiksi valtion ympärivuorokautiselle tietoturvatoiminnolle. Gov-CERT- ja GovHAVARO-palveluiden havaitsemien tietoturvaloukkausepäilyjen koordinoinnista vastaa valtion ympärivuorokautinen tietoturvatoiminto.

EHDOTUKSEN AIKATAULU:

36. HUOVI-PORTAALIN KÄYTÖN PILOTOINTI KYBERTURVALLISUUDEN KEHITTÄMISTYÖKALUNA.

Pilotoidaan HUOVI -portaalin kypsyysanalyysisovellusta eri hallinnonalojen ja organisaatioiden kyberturvallisuuden ja siihen liittyvien toimenpiteiden arvioinnissa. Toiminta on aloitettu syksyllä 2013.

Valtiovarainministeriö ja Huoltovarmuuskeskus kehittävät HUOVI-portaalista versiota valtionhallintoon (GovHUOVI-portaali). GovHUOVI-portaalin hankinnasta vastaa valtiovarainministeriö. GovHUOVI-portaalin kautta kerätään ja jaetaan tilannekuvatietoja sekä turvallisuustietoa.

EHDOTUKSEN AIKATAULU:

37. KYBERTURVALLISUUSKESKUS	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2 ja 10
EHDOTUKSEN VASTUUTAHO: Viestintävirasto	EHDOTUKSEN YHTEISTYÖTAHOT: VNK, VM, SecICT, Liikenne- ja viestintäministeriön asettama laajapohjainen kyberturvallisuustyöryhmä, Poliisihallitus, Puolustusvoimat ja muut turvallisuusviranomaiset

EHDOTUKSEN KUVAUS JA PERUSTELUT

Viestintävirastoon on perustettu kyberturvallisuuskeskus vahventamaan kansallisen tietoturvaviranomaisen tehtävien hoitamista. Keskus kerää tietoa kyberturvallisuustilanteesta, tukee eri hallinnonaloja ja toimijoita arvioimaan ilmiöiden yhteiskunnallisia vaikutuksia sekä jakaa analysoitua kyberturvallisuuden tilannekuvaa. Kukin hallinnonala vastaa kyberturvallisuuden ilmiöiden toimialallaan aiheuttamien häiriötilanteiden edellyttämistä toimenpiteistä ja toimialaansa koskevien häiriöiden raportoinnista. Keskus tukee toimijoita laajojen kyberhäiriötilanteiden hallinnassa. Kyberturvallisuuskeskuksen tueksi kootaan laaja ja kaksisuuntaiseen tiedonvaihtoon perustuva yhteistyöverkosto. Kyberturvallisuuskeskuksen muuta yhteiskuntaa tukevien toimintojen tehokkuus on täysin riippuvainen siitä, että eri toimialojen julkishallinnollisiin ja yksityisiin organisaatioihin syntyy riittävä kyky hyödyntää kyberturvallisuuden tilannekuvaa arvioitaessa vaikutuksia kokonaisturvallisuuteen ja yhteiskunnan elintärkeille toiminnoille sekä reagoitaessa havaittuihin tietoturvaloukkauksiin tai tietoturvauhkiin.

Kyberturvallisuuden tilannekuvan hyödyntämistä eri hallinnonaloilla kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen tilannekuvan arviointiin tulee kehittää osana hallinnonalojen tilannekuvajärjestelyjen, valtioneuvoston kanslian tilannekuvatoiminnan sekä valtion ympärivuorokautisen tietoturvatoiminnan kehittämistä (SecICT). Kokonaisturvallisuuden kannalta on olennaista, että eri hallinnonaloilta pystytään koostamaan valtioneuvoston käyttöön sellaista tilannekuvaa yhteiskunnan elintärkeiden toimintojen häiriöistä, jota voidaan hyödyntää ja jakaa häiriötilanteiden hallinnan edellyttämällä tavalla kaikilla toimialoilla viranomaisissa ja yrityksissä. Kyberturvallisuuskeskus vaihtaa tietoja valtioneuvoston tilannekeskuksen, valtion ympärivuorokautisen tietoturvatoiminnon, viranomaisten ja elinkeinoelämän kanssa. Kyberturvallisuuskeskuksen kykyä saada tietoa sekä julkisen hallinnon että elinkeinoelämän toimijoilta sekä osallistua kansainväliseen tietoturvaloukkauksia koskevaan tiedonvaihtoon tulee hyödyntää koko yhteiskunnan hyväksi. Toiminnassaan kyberturvallisuuskeskus osallistuu yhteistyössä muiden toimijoiden kanssa harjoitus- ja testaustoimintaan omien kyvykkyyksien kehittämiseksi.

Liikenne- ja viestintäministeriön asettama laajapohjainen kyberturvallisuustyöryhmä tukee liikenne- ja viestintäministeriötä Viestintävirastoon perustetun kyberturvallisuuskeskuksen toiminnan ja tulosohjauksen kehittämisessä sekä harjoittaa asiantuntijoiden yhteistoimintaa kyberturvallisuuden alalla. Kyberturvallisuustyöryhmä muun muassa arvioi kyberturvallisuuskeskuksen kykyä tukea tieto- ja viestintäjärjestelmäalan palvelun tuottajien toimintaedellytyksiä sekä lainsäädännön tehokkuutta sähköisten tieto- ja viestintäjärjestelmien häiriötilanteissa.

Valtioneuvoston tilannekeskus koordinoi luotettavan ja eheän tiedonvälityksen kyberturvallisuuskeskuksen kanssa valtion johdon päätöksenteon tueksi.

EHDOTUKSEN AIKATAULU: Viestintäviraston toimintasuunnitelma viimeistellään saatujen lausuntojen pohjalta keväällä 2014. Päivityksessä huomioidaan kyberturvallisuusstrategian toimeenpano-ohjelma. Kyberturvallisuuskeskuksen perustamisvaihe kestää vuoden 2015 loppuun asti. LVM:n kyberturvallisuustyöryhmän toimikausi jatkuu vuoden 2017 loppuun.

Lisäksi Kyberturvallisuuskeskusta ja kyberturvallisuutta tukemaan on esitetty seuraavia toimenpiteitä:

38. TILANNETIETOISUUDEN JA TILANNEYMMÄRRYKSEN PARANTAMINEN LVM:SSÄ

Liikenne- ja viestintäministeriö muodostaa koko hallinnonalansa kattavan analysoidun tilannekuvan häiriötilanteista toimialallaan ja ylläpitää ympärivuorokautista varallaolopäivystystä tätä tarkoitusta varten. Liikenne- ja viestintäministeriö osallistuu valtioneuvoston tilannekuvatoiminnan kehittämiseen ja pyrkii edistämään hallinnonalan virastojen mahdollisuuksia saada ja

jakaa edelleen toimialojen elinkeinotoimijoille ja kansalaisille sellaista tietoa valtioneuvoston tilannekuvasta, joka tukisi niitä ylläpitämään häiriöttömästi omia järjestelmiään ja omaa toimintaansa.

Liikenne- ja viestintäministeriön hallinnonalan virastot ilmoittavat ministeriölle ja valtioneuvoston tilannekeskukselle häiriöistä toimialoillaan. Viestintävirasto tuottaa ajantasaista tilannekuvaa viestintäverkoista sekä niiden vika- ja häiriötilanteista. Viestintävirasto kerää tietoa verkko- ja viestintäpalvelujen sekä lisäarvopalveluiden vioista ja häiriöistä sekä niihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista. Viestintävirasto tiedottaa tietoturva-asioista. Viestintävirasto perustaa kyberturvallisuuskeskuksen vahventamaan tietoturvatehtäviensä hoitamista, mikä on toimeenpano-ohjelmassa erillisenä toimenpiteenä.

Liikenne- ja viestintäministeriö ylläpitää, seuraa ja kehittää vapaaehtoisia sopimuksia ja lainsäädäntöä, jonka nojalla kannustetaan eri huoltovarmuuskriittisten alojen toimijoita ilmoittamaan ja saamaan sellaista tietoa tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista, mikä mahdollistaa järjestelmien ylläpitäjiä ryhtymään tarvittaviin toimenpiteisiin tietojärjestelmiensä ja toimintojensa suojaamiseksi.

Liikenne- ja viestintäministeriö koordinoi hallinnonalan viestinnällistä varautumista laajamittaisiin tietoliikennehäiriöihin valmistelemalla kriisiviestintäsuunnitelman. Suunnitelma laaditaan yhteistyössä LVM:n hallinnonalan ja toimialan yritysten kanssa osana VALHA- ja TIETO-harjoituksia.

39. CERT -TOIMINNON KEHITTÄMINEN

Kyberturvallisuuskeskus kehittää CERT-toiminnon analyysi- ja raportointikyvykkyyksiä prosessuaalisesti ja teknisesti siten, että tietoturvauhkien analyysiä ja raportointia kyetään paremmin kohdentamaan eri toimijoiden tarpeisiin (eri toimialat). Tavoitteena on kehittää kriittisen infrastruktuurin toimijoiden kyberturvallisuuden tilannetietoisuutta ja –ymmärrystä. CERT-toiminnon kehittämisessä tarkastellaan tarve ICS-CERT (The Industrial Control Systems CERT) toiminnon kehittämiselle.

EHDOTUKSEN AIKATAULU: Toimeenpannaan vuoden 2014 aikana.

40. SELVITYS TIETOTURVALLISUUSPOIKKEAMIEN ILMOITTAMISEN KÄYTÄNNÖISTÄ JA YHTEISTYÖSTÄ

Viranomaisten keskinäinen sekä viranomaisten ja elinkeinoelämän välinen yhteistyö on kyberloukkausten ja -hyökkäysten ennaltaehkäisyssä ja torjumisessa välttämätöntä. Kansainvälisen ja kansallisen yritysten ja viranomaisten välisen sekä viranomaisten keskinäisen tiedonvaihdon ja yhteistyön avulla voidaan tunnistaa uhkia sekä riskejä. EU:n komissio on 7.2.2013 antanut esityksen EU:n verkko- ja tietoturvadirektiiviksi. Liikenne- ja viestintäministeriö selvittää direktiivin kansallisen valmistelun yhteistyössä toimivaltaisten viranomaisten, elinkeinoelämän edustajien sekä järjestöjen kanssa tiedonvaihtotarpeita, -oikeuksia ja -velvollisuuksia tietoturvapoikkeamien paljastamiseksi ja selvittämiseksi. Tavoitteena on selvittää, miten kyberturvallisuuskeskus, kansalaiset, yritykset ja viranomaiset saavat kaikissa tilanteissa tiedon merkittävistä tietoturvaloukkauksista, jotta ne voivat ryhtyä asianmukaisiin toimenpiteisiin. Selvitystyössä voidaan hyödyntää kokemuksia rahanpesunselvittelykeskuksen kokemuksista, joissa keskeistä on, että kaikista rikosepäilyistä ei aloiteta esitutkintaa.

EHDOTUKSEN AIKATAULU: Direktiivin valmistelu on käynnissä.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

41. PUOLUSTUSVOIMIEN KYBERTURVALLISUUSTILANNEKUVAN LUOMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1,2,3,4,5,6 ja 9
EHDOTUKSEN VASTUUTAHO: PLM, PV	EHDOTUKSEN YHTEISTYÖTAHOT: Viestintävirasto, valtion ympärivuorokautinen tietoturvatoiminta, turvallisuusviranomaiset, elinkeinoelämä
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Hankkeessa kehitetään Puolustusvoimien kykyä luoda kybertilannekuvaa sekä jakaa sitä muiden viranomaisten ja toimijoiden kanssa. Puolustusvoimien kybertilannekuva muodostuu oman suojautumisen ja valvonnan avulla luodusta tilanneymmärryksestä yhdistettynä muista lähteistä saatuihin tilannetietoihin (esimerkiksi CERT-yhteistyö). Puolustusvoimat kehittää tilannekuvan visualisointia, ympärivuorokautista valvontaa sekä tiedonvaihtoa muiden viranomaisten ja kumppaneiden kanssa niin kansallisesti kuin kansainvälisesti. Puolustusvoimien kybertilannekuva tukee erityisesti kyberturvallisuuskeskusta kansallisen kyberturvallisuustilannekuvan muodostamisessa. Lisäksi Puolustusvoimat tuottaa kybertilannekuvaan analyyseja kybertilanneympäristössä havaituista ilmiöistä ja niiden mahdollisista merkityksistä.	
EHDOTUKSEN AIKATAULU: Rakentaminen 2014 – 2018.	

Tiedonhankinta ja tutkinta kyberympäristössä

42. KANSALLISEN LAINSÄÄDÄNNÖN KEHITTÄMINEN TURVALLISUUSVIRANOMAISTEN TIEDONHANKINTAKYVYN PARANTAMISEKSI KYBERTOIMINTAYMPÄRISTÖN UHKISTA	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 4, 5 ja 8
EHDOTUKSEN VASTUUTAHO: PLM	EHDOTUKSEN YHTEISTYÖTAHOT: TPK, UM, OM, VM, SM, LVM, TEM, Poliisihallitus, Supo, Pääesikunta sekä kutsutut asiantuntijat
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Tasavallan Presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta (UTVA) keskustelivat kokouksessaan 7.11.2013 valtionhallinnon tietoturvallisuudesta sekä laajemmin kyberturvallisuuteen liittyvistä kysymyksistä sekä kansallisen kyberturvallisuuden kehittämistarpeista. Osana kyberturvallisuusstrategian toimeenpanoa UTVA linjasi, että välittömästi aloitetaan työ Suomen lainsäädännön kehittämiseksi. Edelliseen liittyen asetti puolustusministeriö 13.12.2014 työryhmän, jonka tehtävänä on Suomen lainsäädännön kehittäminen erityisesti turvallisuusviranomaisten tiedonhankintaa koskevan sääntelyn osalta sekä arvioida lainsäädännön kehittämistarvetta siten, että Suomessa kyetään huolehtimaan kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi. Työryhmän asettamispäätöksen mukaan tavoitteena on selvittää turvallisuusviranomaisten tiedonhankintaa koskevat toimintaedellytykset ottaen huomioon erityisesti kybertoimintaympäristön kautta Suomeen kohdistuvat uhkat sekä selvittää tiedonhankintaa koskevat nykyiset toimivaltuudet ja niiden kehittämistarpeet.	

Lisäksi tavoitteena on, että Suomen kansallinen lainsäädäntö muodostaa valtion turvallisuudesta vastaavien viranomaisten kesken riittävän vahvan kokonaisuuden kyberuhkatilanteiden kokonaisvaltaiseksi ennakoimiseksi ja torjumiseksi sekä mahdollisiin uhkatilanteisiin reagoimiseksi. Kansallisella lainsäädännöllä voidaan osaltaan varmistaa tehokkaan kyberturvallisuuden toteuttamisen edellytykset. Keskeisessä asemassa on Suomea velvoittavien ihmisoikeus- ja perusoikeusmääräyksien, kuten perustuslain, YK:n kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen sekä Euroopan ihmisoikeussopimuksen huomioon ottaminen. Tärkeää on huomioida myös yksilön oikeusturva sekä tehokkaat perustuslailliset valvontamekanismit.

Kansainvälisesti tarkasteltuna voidaan todeta että kyberturvallisuuden merkitys osana perinteistä ulko-, turvallisuus-, ja puolustuspolitiikkaa on kasvanut. Useissa muissa maissa tietoteknisen ympäristön nopea kehittyminen ja muuttuminen on luonut tarpeen valtioille luoda uhkiin varautumisen osalta kansallista lainsäädäntöä valtion turvallisuusviranomaisten tiedonhankinnasta.

Kyberturvallisuusstrategian mukaisesti Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Niihin liittyen tulee varmistua siitä, että Puolustusvoimia koskeva kansallinen sääntely mahdollistaa Puolustusvoimien riittävän hyvän havainnointikyvyn myös kyberympäristön uhista.

Suomessa poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, selvittäminen ja syyteharkintaan saattaminen (poliisilaki 493/1995, 1 §). Suojelupoliisin tehtävänä on torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa (poliisin hallinnosta annettu laki 110/1992, 10 §). Puolustusvoimien tehtäviin kuuluu Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä osallistuminen kansainväliseen kriisinhallintaan (laki puolustusvoimista 551/2007, 2 §). Suomen sotilaalliseen puolustamiseen kuuluu maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen sekä kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen (551/2007, 2 § 1 kohta a ja b -alakohdat).

Sisäisten ja ulkoisten kyberuhkien torjumiselle on yhteistä, että niiden syntyminen on kyettävä havaitsemaan tarpeeksi varhaisessa vaiheessa, jotta maan sisäistä ja ulkoista turvallisuutta ylläpitävät mekanismit kykenevät toimimaan oikea-aikaisesti. Näin ollen on tärkeää, että myös Suomessa kansallinen lainsäädäntö muodostaa elinkeinoelämän toimijoiden sekä valtion turvallisuudesta vastaavien viranomaisten kesken riittävän vahvan kokonaisuuden kyberuhkatilanteiden kokonaisvaltaiseksi ennakoimiseksi ja torjumiseksi sekä mahdollisiin uhkatilanteisiin reagoimiseksi.

Jatkovalmistelu arvioidaan työryhmän saatua työnsä päätökseen. Jatkovalmistelussa on aiheen suuren yhteiskunnallisen merkityksen vuoksi erityisiä syitä noudattaa hyvän lainvalmistelun periaatteita kuten laajaa kuulemista.

EHDOTUKSEN AIKATAULU: Puolustusministeriön asettaman työryhmän määräaika on 30.6.2014.

43. KANSALLINEN KYBERVALVONTA JA KYBERTIEDUSTELU	
	EHDOTUS LIITTYY STRATEGIAN LINJAUK-

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

	SEEN: 1,2,5,6,8 ja 9
EHDOTUKSEN VASTUUTAHO: PLM, PV	EHDOTUKSEN YHTEISTYÖTAHOT: Liikenne- ja viestintäministeriö, Viestintävirasto, valtion ympärivuorokautinen tietoturvatoiminta, Supo, muut turvallisuusviranomaiset ja TUVE-lain perusteella määräytyvät toimijat sekä roolinsa mukaisesti elinkeinoelämän edustajat.

EHDOTUKSEN KUVAUS JA PERUSTELUT

Kybervalvonnan ja kybertiedustelun jatkovalmistelu arvioidaan Puolustusministeriön asettaman työryhmän (Kansallisen lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista, asettamispäätös 13.12.2013; toimenpide 42) saatua työnsä päätökseen. Jatkovalmistelussa on aiheen suuren yhteiskunnallisen merkityksen vuoksi erityisiä syitä noudattaa hyvän lainvalmistelun periaatteita kuten laajaa kuulemista.

Kansallisessa kyberturvallisuusstrategiassa on linjattu, että Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään ja että sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Tunnistettuja puutteita toimivaltuussäännöksissä tarkastellaan työryhmässä (toimenpide 42). **Esitettävän hankkeen toteutuminen on ehdollinen puolustusministeriön lainsäädäntöhankkeen** (toimenpide 42) **mahdollisesti aiheuttamille lakimuutoksille ja päätöksille.**

Turvallisuuskomiteassa 10.2.2014 hyväksyttyjen ministeriöiden kyberturvallisuustehtävien mukaan puolustushallinto vastaa Suomen sotilaallisesta puolustamisesta myös kybertoimintaympäristön kautta maan turvallisuuteen kohdistuvia, sotilaallisiin uhkiin rinnastettavia kyberuhkia vastaan. Aiemmin mainitun lakihankkeen mahdollistamissa rajoissa olisi tämä hanke luomassa osaltaan pohjan ja perusteet maamme kyberturvallisuuden kehittämiselle ja ylläpidolle. Puolustusvoimat arvioi, kuinka tulisi kehittää valtakunnallinen ympärivuorokautinen kyky maamme ulkorajan valvontaan kybertoimintaympäristössä ja siihen liittyvään kybertiedusteluun.

EHDOTUKSEN AIKATAULU: Päätösten mukaisesti

44. KYBERRIKOSTEN TUTKINTA

Tietoverkkorikollisuus ja tietoverkon avulla tehdyt rikokset on muuttanut esitutkintaviranomaisten toiminnan painopisteitä. Muutoksen hallinnan varmistamiseksi on useita yksittäisiä toimia, jotka yhdessä parantavat kyberrikosten tutkintaa.

45. SELVITYS ESITUTKINTAVIRANOMAISEN TOIMIVALTUUKSISTA KYBERRIKOSTORJUNNASSA

	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 4
EHDOTUKSEN VASTUUTAHO: Poliisihallitus	EHDOTUKSEN YHTEISTYÖTAHOT: KRP, Supo, RVL ja Tulli

EHDOTUKSEN KUVAUS JA PERUSTELUT

Perustetaan selvityshanke käymään läpi esitutkintaviranomaisten toimivaltasääntelyä muuttuvassa kyberympäristössä esitutkintaviranomaisten näkökulmasta ja tekemään esitys mahdollisista muutostarpeista vastuuministeriöille. Esitutkintaviranomaisella on oltava uhan vakavuus huomioiden riittävät toimivaltuudet selvittää kyberympäristössä toteutettuja vakavia rikoksia.

EHDOTUKSEN AIKATAULU:	
46. TIETOVERKKORIKOSOSAAMISEN LIITTÄMINEN POLIISIN 24/7 YHTEYSPISTEESEEN JA KANSAINVÄLISTEN PALVELUJEN TURVAAMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN:4
EHDOTUKSEN VASTUUTAHO: KRP	EHDOTUKSEN YHTEISTYÖTAHOT: Kansainväliset poliisi- ja viranomaisyhteisöt kuten Europol ja Interpol, muut valtiot, Viestintävirasto, valtion ympärivuorokautinen tietoturvatoiminta, muut turvallisuus- ja tilannekuvatoimijat, Huoltovarmuuskeskus sekä kansalliset, kriittisiä palveluja tarjoavat yritykset.
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Poliisin on luotava kattava kansainväliseen ja kansalliseen viranomaisyhteistyöhön sekä kansalliselle kriittiselle infrastruktuurille tarjottava 24/7 palvelu, jolla vastataan kansainvälisten sopimusten vaatimuksiin sekä turvataan nopea toimintakyky vaativiin tilanteisin. Siihen velvoittaa Suomen ratifioima Euroopan neuvoston tietoverkkorikossopimus. Palvelun kautta tulevat kiireelliset, muiden maiden pyytämät tietoverkkorikoksiin liittyvät virka-apu toimeksiannot poliisille. Samoin Suomen poliisi pyytää tämän verkoston kautta virka-apuna todisteiden (datan) jäädyttämistä vastaavasti muista maista kiireellisissä tapauksissa. Uuden 12.8.2013 vahvistetun direktiivin 2013/40/EU tietojenvaihtoa koskevan 13 artiklan mukaan jäsenvaltioiden on varmistettava, että niillä on toimiva kansallinen yhteyspiste ja että ne hyödyntävät nykyistä (vrt. ed. kohta) ympärivuorokautisesti ja kaikkina viikonpäivinä toimivien yhteyspisteiden verkostoa 3-8 artiklassa tarkoitettuja rikoksia varten. Jäsenvaltioiden on huolehdittava menettelyt, jotta toimivaltainen viranomainen voi kiireellisten toimeksiantojen osalta ilmoittaa 8 tunnin kuluessa pyytäjälle ainakin sen vastataanko pyyntöön ja milloin ja missä muodossa vastaus tulee. Poliisin 24/7–toiminto ei ole päällekkäinen muiden tilannekuvatoimintojen kanssa, koska se on tarkoitettu rikostorjuntatoimenpiteiden käynnistämiseen. Poliisin 24/7-toiminnon keskeisin tehtävä on käynnistää esitutkintaviranomaiset toimenpiteet viipymättä, jotta näyttö saadaan talteen. Poliisin 24/7 on kyberturvallisuuskeskuksen vastinkappale poliisissa. Menetelmät ovat lähtökohtaisesti erilaiset, vaikka kummankin yhteinen tavoite on jatkovahingon estäminen.	
EHDOTUKSEN AIKATAULU: Tavoite aikataulu on 2014 -2016.	
47. KYBERRIKOSTILANNEKUVA JA -TIEDONHANKINTA	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 4
EHDOTUKSEN VASTUUTAHO: KRP, Tulli	EHDOTUKSEN YHTEISTYÖTAHOT: Viestintävirasto ja muut viranomaiset. Muihin poliisiyksiköihin sijoitettavien henkilöresurssien osalta vastuutahona olisi kyseinen yksikkö. Kaikki KRP:tä koskevat esitykset on suunniteltu toteutettavaksi KRP:n kyberkeskusprojektin yhteydessä, jos projektin toteuttamiseksi osoitetaan riittävät varat.
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Tiedonhankinta tietoverkoista pitää sisällään: avointen lähteiden tiedonhankinnan, kohdistetun tiedonhankinnan viranomaisen toimivaltuuksin ja tiedonhankinnan yhteistyökumppaneilta. Nykytilan kehittäminen edellyttää valtakunnallisten yksikköjen resursoinnin lisäämistä (myös po-	

liisilaitokset osassa asioita) sekä vastuiden ja velvollisuuksien määrittämistä poliisilaitosten kanssa. Työprosessit on määriteltävä sekä normaaliolosuhteisiin että vaativiin poliisitoiminnallisiin tilanteisiin. Eräs keskeinen tehtävä on luoda tietojärjestelmät joilla turvataan tiedonhankinta, datan oikeusvarma käsittely sekä tiedon analyysi. Tiedonhankinta tietoverkoista on ns. rikoslajineutraalia, jolloin sitä voidaan hyödyntää vaativien kyberrikosten lisäksi myös muissa poliisin toimialaan kuuluvissa tehtävissä. Näin ollen yhteydet PTR:ään (poliisin, tullin ja rajavartiolaitoksen yhteistoiminta), johtokeskuksiin, yms. poliisin johtamisjärjestelyihin on luotava. Vastaavat kehittämistoimet tulee tehdä myös Tullissa tullirikostorjuntaa koskien. Hankkeessa huomioidaan esitutkintaa harjoittavien viranomaisten tarpeet. Poliisihallinnon kyberrikosilmiön tilannekuvan laatiminen on aloitettava KRP:ssä. Tilannekuva edellyttää tiedonkeruun lisäksi myös strategista analyysiä. Operatiivisen, tutkittaviin asioihin liittyvän, analyysitoiminnan sijoitus tähän yhteyteen on selvitettävä. Tilannekuvaa on tehtävä yhteistyössä muiden valtionhallinnon toimijoiden, yksityissektorin, kansainvälisten organisaatioiden kanssa. Tilannekuvatoiminto on myös liitettävä osaksi muuta rikollisuuden tilannekuvakäytäntöjä (PTR-toiminta). Tilannekuvaa on hyödynnettävä aktiivisella ulospäin suuntautuvalla tiedottamisella ja yhteistyön kehittämisellä sidosryhmien kanssa (alan yhteistyöryhmät). Tällä on tavoitteena rikosten ennalta ehkäisy ja toteutuneiden rikosten vahinkojen rajaaminen.

EHDOTUKSEN AIKATAULU: Tavoite aikataulu on 2014-2016

48. KYBERRIKOSTUTKINNAN JÄRJESTÄMINEN JA RESURSOINTI	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 4
EHDOTUKSEN VASTUUTAHO: KRP, Tulli	EHDOTUKSEN YHTEISTYÖTAHOT: Viestintävirasto ja muut viranomaiset. Muihin poliisiyksiköihin sijoitettavien henkilöresurssien osalta vastuutahona olisi kyseinen yksikkö. Kaikki KRP:tä koskevat esitykset on suunniteltu toteutettavaksi KRP:n kyberkeskusprojektin yhteydessä, jos projektin toteuttamiseksi osoitetaan riittävät varat.

EHDOTUKSEN KUVAUS JA PERUSTELUT

Rikoslajin luonteen vuoksi tehokas ja laadukas kansallinen tutkinta edellyttää kansallista koordinointia. Tämä rooli sopii KRP:n vastuulle. Koordinaation edellyttämät prosessit ja toimintatavat on luotava kaikkiin poliisiyksiköihin. Vaativa kyberrikostutkinta edellyttää erityistä osaamista ja tutkintarauhaa. Rikostyypin luonteen vuoksi tiedonhallinta ja -analyysi edellyttävät erityistä huomiota. Tämän vuoksi valtakunnallisiin yksiköihin ja poliisilaitoksille on nimettävä riittävä määrä tutkija ja tutkinnanjohtaja resurssia. Poliisin on myös luotava Poliisihallituksen johdolla tutkintavastuut. Esitetään, että KRP olisi vastuussa vaativista ja eniten resursseja sitovista jutuista sekä jutuista, joissa on vahva kansainvälinen ulottuvuus tai kytkentä järjestyneeseen rikollisuuteen. Suojelupoliisi toimisi omalla toimialallaan joko itsenäisesti tai yhteistyössä KRP:n kanssa. Poliisilaitokset myös osallistuisivat vaativien kyberrikosten tutkintaan, vaikka määrällisesti suurin poliisilaitosten jutuista onkin perusmuotoisista tietoverkoissa tapahtuneita juttuja. Erityisesti Helsingin poliisilaitoksella on muista poliisilaitoksia suurempi rooli, sillä sen alueella on suuri määrä yritysten pääkonttoreita. Juttujen luonteen ja erityisosaamisen tarpeen vuoksi poliisin alan tutkijoiden on verkostoiduttava ja tutkintaryhmien joustava käyttö mahdollistettava.

Koska Tullin rikostorjunta on valtakunnallinen toiminto, niin varsinaiseen Tullin sisäiseen koordinaatioon ei ole tarvetta, mutta Tullin oman tietoverkkotiedustelun tulee huolehtia erittäin tii-

viistä yhteistyöstä Keskusrikospoliisin vastaavan yksikön kanssa. Sen sijaan Tullin on sisäisesti ensiarvoisen tärkeää kouluttaa ja nimetä Tullin rikostorjunnan operatiivisiin yksikköihin riittävä määrä rikostutkijoita ja tutkinnanjohtajia vastaamaan vaativien, pitkäkestoisten kyberrikosten esitutkinnasta Tullin tehtäväalueella.
EHDOTUKSEN AIKATAULU: Tavoite aikataulu on 2014-2016

KANSALAISTEN HYVINVOINTI JA YRITYSTEN MENESTYS

Osaamisen kehittäminen

49. KOKONAISKUVA KYBEROSAAMISEN NYKYTILASTA JA TOIMENPITEET ALAN TUTKIMUS- JA KEHITYSTYÖN SEKÄ INNOVAATIOTOIMINNAN KAPASITEETIN KEHITTÄMISEEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 7
EHDOTUKSEN VASTUUTAHO: OKM	EHDOTUKSEN YHTEISTYÖTAHOT: TEM, LVM, VM, PLM, VNK ja muut hallinnonalat
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. Tästä huolimatta Suomessa ei ole kokonaiskuvaa kyberosaamisen nykytilasta eikä siten riittävää pohjaa TK&I-kapasiteetin (osaaminen, infrastruktuuri ja resurssit hallinnonaloilla, elinkeinoelämässä ja tiedeyhteisössä) kehittämiseen. Selvityksessä tunnistetaan myös kansallisen ja kansainvälisen tutkimuksen työnjakoa (esim. suhteessa EU Horizon 2020 -tutkimusohjelmiin). Kyseisen tutkimustoiminnan kehittäminen liittyy turvallisuustutkimuksen toimeenpano-ohjelmaan ja VN:n TULA-periaatepäätökseen (5.9.2013) valtioneuvoston tutkimuslaitosten ja tutkimusrahoituksen kokonaisuudistamiseksi. Kokonaiskuvan tuottamiseksi selvitetään kyberturvallisuuteen liittyvän osaamisen ja tutkimustoiminnan kannalta keskeisten osa-alueiden tilanne ja arvioidaan kypsyystaso, erityisenä kohteena korkeakoulutasoisen tieto- ja kyberturvallisuuden koulutuksen sekä tutkimus- ja kehitystyön edistäminen. Samalla varmistetaan kansallisen tutkimustoimintaan liittyvän infrastruktuurin toimintavarmuus ja käytettävyys sekä tietojen luottamuksellisuus, eheys ja saatavuus, mukaan lukien kulttuurin ja tutkimuksen digitaalisten tietovarantojen hallinta ja pitkäaikaissäilytys. Selvityksessä edistetään kybertoimintaympäristön kansallista ja kansainvälistä koulutus- ja tutkimusyhteistyötä. Selvityksessä tehdään laajapohjaista yhteistyötä poikki ministeriöiden toimialojen.	
EHDOTUKSEN AIKATAULU: Selvityshanke-ehdotus on mukana valtioneuvoston päätöksentekoa tukevan tutkimussuunnitelman työstämisessä, päätöksiä asiasta ei ole tehty	

KANSALLISET LAAJAT TUTKIMUSOHJELMAT	
50. ICT 2023 TUTKIMUS-, KEHITYS- JA INNOVAATIO-OHJELMA	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN:7
EHDOTUKSEN VASTUUTAHO: Suomen Akatemia, Tekes	EHDOTUKSEN YHTEISTYÖTAHOT:
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Suomen Akatemia ja Tekes toteuttavat yhteistyössä ICT 2023 tutkimus-, kehitys- ja innovaatio-ohjelmaa. Ohjelman tavoitteena on ICT 2015 -raportin mukaisesti syvän tietojenkäsittelyosaamisen kehittäminen. Akatemia on varannut ICT 2023 -ohjelman ensimmäiselle temaattiselle haulle viisi miljoonaa euroa. Ensimmäisen ICT-haun keskeiseksi teemaksi on valittu tietoturvaan liittyvä tutkimus. Kymmenen vuotta kestävässä tutkimus-, kehitys- ja innovaatio-ohjelmassa (ICT 2023) tavoitteena on koota Suomessa yhteen alan keskeiset osapuolet, kuten yliopistot, tutkimuslaitokset ja yritykset. Suomen Akatemia ja Tekes koordinoivat ICT 2023 –ohjelmaa yhdessä. Tekes on	

varautunut rahoittamaan hankkeita avaamalla yrityksille suunnatun rinnakkaisen haun.

EHDOTUKSEN AIKATAULU:
Hankkeiden rahoituskausi on kaksi vuotta. Hankkeiden rahoitus alkaa pääsääntöisesti 1.6.2014. Akatemiassa valmistellaan ICT 2023 tutkimus-, kehitys- ja innovaatio-ohjelman toista suunnattua temaattista hakua. Haku on suunniteltu avattavaksi huhtikuussa 2014.

51. INKA, TEKESIN STRATEGISET TUTKIMUSAVAUKSET JA TKI-RAHOITUS

Kyberturvallisuus on osa Tekesin Inka (Innovatiiviset kaupungit)-ohjelmaa ja kyberturvallisuuden osalta kansallinen vetovastuu on Jyväskylällä. Kyberturvallisuuden hankkeet kilpailevat rahoituksesta samoilla ehdoilla kun muutkin Tekesin innovaatiorahoituksella toteutettavat kehittämiskohteet.

INKA 2014–2020 -kyberturvallisuusteeman visiona on luoda Suomesta kansainvälisesti tunnustettu kyberturvallisuuden liiketoiminnan ja osaamisen sekä kyberuhkiin varautumisen maailmanlaajuinen edelläkävijä. Tavoitteen mukaan Suomesta on vuonna 2020 muodostunut kyberturvallisuusalan liiketoiminnan yksi johtavista maista. Suomeen on luotu kyberturvallisuusalan tutkimusta, koulutusta, tuotekehitystä ja testausta mahdollistavia avoimia innovaatio- ja kehitysympäristöjä. Nämä ympäristöt muodostavat monialaisia kokonaisuuksia ja niillä on vahva yhteys käyttäjiin. Kehitysympäristöjen avulla on vahvistettu yritysten kasvuedellytyksiä ja aikaansaatu kansainvälinen verkostoituminen globaaleille markkinoille. Kehitysympäristöt ovat luoneet yrityksille yhteisen toimintaympäristön, jossa ne voivat kehittää kyberturvallisuuteen pohjautuvaa liiketoimintaa ja yrittäjyyttä.

Kyberaiheeseen kohdistuvat Tekesin rahoittamat strategiset tutkimusavaukset ovat myös mahdollisia ja ne kilpailevat rahoituksesta samoilla ehdoilla muiden strategisten tutkimusavausten kanssa.

EHDOTUKSEN AIKATAULU:

52. TIETOYHTEISKUNTAOSALLISUUS JA MEDIALUKUTAIDOT

	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 7
EHDOTUKSEN VASTUUTAHO: OKM	EHDOTUKSEN YHTEISTYÖTAHOT: Opetushallitus, Kansallinen audiovisuaalinen instituutti, kirjastot, museot, nuorisopalvelut, järjestöt

EHDOTUKSEN KUVAUS JA PERUSTELUT

Kohdennettujen tieto- ja kyberturvallisuutta edistävien hankkeiden ja kampanjoiden avulla tuetaan yhteiskunnan kyberosaamista ja kybertoimintaympäristössä toimimista.

Hallitusohjelmassa jokaiselle lapselle ja nuorelle taataan edellytykset ja pääsy osallisuuteen tietoyhteiskunnassa. Opetus- ja kulttuuriministeriön laatimassa Lapsi- ja nuorisopolitiikan kehittämisohjelmassa 2012 - 2015 kiinnitetään huomiota medialukutaitoon ja teknologiseen osaamiseen osana yleissivistystä.

Opetus- ja kulttuuriministeriö on laatinut kulttuuripoliittiset suuntaviivat hyvän medialukutaidon edistämiseksi vuosille 2013–2016. Hyvää medialukutaitoa (esim. internetin turvallinen käyttö, lähdekriittisyys, sähköinen asiointi) tarvitaan informaatioyhteiskunnassa erilaisissa roo-

leissa: kansalaisena, kuluttajana, työntekijänä ja opiskelijana.

Mediakasvatuksen toteuttajia – mediakasvattajia – toimii kunnissa lasten ja nuorten kanssa kasvatus- ja koulutussektorilla päivähoidossa, esi- ja perusopetuksen sekä lukio-opetuksen piirissä. Mediakasvatusta tuetaan ja toteutetaan myös kuntien kulttuuripalvelujen piirissä, esimerkiksi kirjastoissa, museoissa ja nuorisopalveluissa. Valtakunnalliset järjestöt voivat edistää medialukutaitoa asiantuntijoina, vaikuttajina, kehittäjinä, tiedottajina ja hankkeiden toteuttajina. Opetushallituksen keskeisiä tehtäviä medialukutaidon edistämisessä ovat koulutuksen kehittäminen, opetussuunnitelmien ja tutkintojen perusteiden laadinta ja täydennyskoulutuksen järjestäminen sekä opetustoimen henkilöstökoulutuksen rahoittaminen.

Ministeriö on suunnannut Opetushallituksen kautta rahoitusta koulutuksen järjestäjille käytettäväksi oppimisympäristöjen kehittämiseen ja monipuolistamiseen. Tieto- ja viestintätekniikan roolina kehittämistyössä on toimia erilaisten oppimisympäristöjen yhdistäjänä mahdollistaen tiedon hankinnan, tuottamisen ja käsittelyn hyödynnettäessä erilaisia laaja-alaisia oppimisympäristöjä. Hankkeiden tulee tukea koulutuksen järjestäjän pedagogisten käyttötapojen kokonaisvaltaista kehittämistä. Rahoitusta suunnataan myös oppiainerajat ylittävään ja mediakriittisyyttä lisäävään toimintaan.

On tarpeellista tarkastella määräajoin toisaalta kyberturvallisuuden osaamistarvetta yhteiskunnassa ja toisaalta siihen liittyvän tutkimuksen ja koulutuksen laajuutta ja syvyyttä. Tilanne tässä suhteessa saattaa muuttua ennakoitua nopeammin.

EHDOTUKSEN AIKATAULU:
Tavoiteaikataulu 2014 – 2017; osittain toteutus on aloitettu, osittain suunnitteilla.

ESIMERKKEJÄ KOULUTUS- JA TUTKIMUSHANKKEISTA

53. JYVSECTEC – JYVÄSKYLÄ SECURITY TECHNOLOGY – TURVALLISUUSTEKNOLOGIAN KEHITTÄMISHANKE

Kehitystyön tavoitteena on parantaa kyberuhkien ehkäisyä ja ennakointia sekä toimintavalmiuksien kehittämistä. Jyväskylän ammattikorkeakoulun (JAMK) JYVSECTEC kyberturvallisuusteknologian hankkeessa kehitetään ja ylläpidetään kyberturvallisuuden harjoitusympäristöä, jossa tuotetaan tutkimus-, kehitys- ja koulutuspalvelua osana kansallista ja kansainvälistä yhteistyöverkostoa. JYVSECTEC toteuttaa kyberharjoituksia, joissa eri toimijat voivat harjoitella todenmukaisessa ympäristössä toimintaa erilaisia kyberuhkia ja hyökkäysmenetelmiä vastaan. JYVSECTEC:n tilannekeskuksessa on mahdollista demonstroida teknistä valvontakuvaa, koostettua tilannekuvaa sekä hyödyntää useita eri lähteitä tilannekuvan muodostamiseksi. Erillisessä tilannehuoneessa voidaan harjoittaa ja kehittää analyysi-, valvonta- ja johtamistoimintaa. Jyväskylän ammattikorkeakoulu (JAMK) ja JYVSECTEC voivat tukea Kyberturvallisuuskeskuksen toimintaa.

EHDOTUKSEN AIKATAULU: Jatkokehityshanke toteutetaan 9/2014 – 12/2016 välisenä aikana.

54. INFORMAATIOTURVALLISUUDEN YLIOPISTOTASOINEN KOULUTUS (JYVÄSKYLÄN YLIOPISTO)

Informaatioturvallisuuden maisteri- ja jatkokoulusta on kehitetty vuosille 2014–2017. Informaatioturvallisuuden maisterikoulutus (INTU) perustuu vahvaan Informaatioteknologian tiedekunnassa toteutettavaan kyberturvallisuuden tutkimukseen. INTU:n tavoitteena on luoda opiskelijalle vankka osaaminen työskentelyyn informaatio- ja kyberturvallisuuden kokonaishallinnan vaativissa johtamis- ja kehittämistehtävissä. Informaatioturvallisuuden suuntautumisvaihtoehto sisältää laitoskohtaiset opintopolut, joiden avulla opiskelija suuntautuu tutkintotavoitteiden mukaisiin osaamisprofiileihin. Informaatioturvallisuuden maisterikoulutus on Informaa-

tioteknologian tiedekunnan ainelaitosten yhteinen FM-tutkintoon johtava suuntautumisvaihtoehto kandidaattitutkinnon suorittaneille opiskelijoille. Lisäksi INTU on tarkoitettu aihepiiristä kiinnostuneille sivuaineopiskelijoille tai erillisellä opinto-oikeudella opiskeleville ei-tutkinto-opiskelijoille sekä jo työelämässä oleville tutkintonsa täydentäjille. Informaatioturvallisuuden maisterikoulutuksen yleisenä tavoitteena on antaa opiskelijalle johdatus informaatioturvallisuuden kokonaisuuteen sekä syventäviä opintoja informaatioturvallisuuden eri osa-alueilta. Informaatioturvallisuuden opetus muodostuu opintokokonaisuudessa, jossa tarkastellaan kybermaailmaa ja sen turvallisuutta yhteiskunnallisesta, toiminnallisesta, teknologisesta ja systeemisestä näkökulmasta. Kurssien ja tutkimustyön erilaisilla valinnoilla opiskelija voi suuntautua erilaisiin työtehtäviin kuten oman organisaation turvaaminen, kyberturvallisuusjärjestelmien tai kyberturvallisuusteknologian kehittäminen.

55. KYBERTURVALLISUUDEN YLEMPI KORKEAKOULUTUTKINTO (JAMK)

Jyväskylän ammattikorkeakoulussa (JAMK) on informaatioteknologian koulutusohjelma, jonka sisältönä on kyberturvallisuus. Koulutuksen pääsyvaatimuksena on ICT-alan insinöörin AMK-tutkinto tai muu soveltuva koulutus sekä vähintään kolmen vuoden työkokemus. Koulutusohjelma valmistaa tietotekniikan ylempään ammattikorkeakoulututkintoon kyberturvallisuuden erikoisasiantuntijoita. Koulutuksen tavoitteena on vastata kyberturvallisuuden kasvaviin haasteisiin. Kyberturvallisuuden koulutuksen keskeisiä sisältöjä ovat tietoverkkoturvallisuus ja sen seuranta, uhkien havaitseminen ja torjunta sekä toipuminen. Lisäksi koulutuksessa paneudutaan ICT-alan yleiseen turvallisuustoimintaan, alaan kuuluvaan lainsäädäntöön ja kansallisiin turvallisuuskriteereihin. Kyberturvallisuuden koulutusta tukee ICT-koulutuksen käytössä oleva moderni harjoitusympäristö. Erityispiirteenä ohjelmassa on opintojen lopussa suoritettava laaja kyberturvallisuusharjoitus ns. loppusota, jossa opiskelijat harjoittelevat käytännössä kybertoimintaympäristön suojaamista, hyökkäysten havainnointia ja torjumista sekä toipumista hyökkäyksistä.

56. TIETOJÄRJESTELMÄOSAAMISEN KOULUTUSOHJELMA, YLEMPI AMK-TUTKINTO (LAUREA)

Laurea-ammattikorkeakoulun tietojärjestelmäosaamisen koulutusohjelman tavoitteena on kouluttaa yritysten tietojärjestelmien kehittäjiä parantamaan yritysten kilpailukykyä sekä kotimaisilla että kansainvälisillä markkinoilla. Koulutusohjelmasta valmistunut osaa soveltaa tieto- ja viestintäteknologiaa uusien palvelutuotteiden kehittämiseen, vahvistaa yrityksen liiketoimintaa ja johtaa verkostoja. Koulutusohjelmassa menetelmällinen osaaminen kohdistuu työelämän kehittämiseen ja innovaatiotoimintaan. Koulutusohjelmasta valmistunut voi toimia tietojärjestelmien, niiden tietoturvallisuuden ja tietoverkkojen vaativissa kehittämistehtävissä, tietojärjestelmiin liittyvän liiketoiminnan suunnittelu- ja johtotehtävissä tai itsenäisenä liiketoimintavalmiudet omaavana ICT-alan yrittäjänä.

57. TURVALLISUUSOSAAMISEN KOULUTUS, YLEMPI AMK-TUTKINTO (LAUREA)

Laurea-ammattikorkeakoulu tarjoaa turvallisuusosaamisen koulutusohjelman, joka käsittelee turvallisuuden ja riskienhallintaa niin kansallisissa kuin kansainvälisissäkin ympäristöissä. Ohjelmassa koulutetaan turvallisuusosaajia organisaatioiden vaativiin kehitys- ja johtotehtäviin. Opetus perustuu suurelta osin opiskelijoiden itsensä valitsemien käytännön kehittämiskohteiden ratkaisemiseen. Näin opiskelija ymmärtää turvallisuusasioihin liittyvän, niin työelämän kuin laajemman yhteiskunnallisenkin merkityksen sekä alueellisella että kansainvälisellä tasolla.Koulutusohjelma antaa opiskelijalle valmiuksia ja työkaluja oman turvallisuustietämyksensä ja -ammattitaitonsa jatkuvaan kehittämiseen.

Turvallisuusalan koulutusohjelmassa (AMK-tutkinto) Laureassa voi opiskella turvallisuuden asiantuntijaksi. Turvallisuusalan tradenomin ydinosaamisalueita ovat riskienhallinta, turvallisuusjohtaminen, liiketoimintaosaaminen, henkilöturvallisuus, tietoturvallisuus ja turvallisuusjohta-

minen sekä toiminnan, toimitilojen ja ympäristön turvallisuus. Opiskelujen aikana opitaan myös ennakoimaan erilaisten turvallisuusuhkien ja -toimenpiteiden taloudellisia vaikutuksia. Turvallisuusalan tradenomi voi toimia esimerkiksi turvallisuusasiantuntijana, turvallisuussuunnittelijana, riskienhallintapäällikkönä, turvallisuuspäällikkönä, palotarkastajana tai turvallisuusalan opettajana.

58. KYBERTURVALLISUUSKURSSI (MAANPUOLUSTUSKOULUTUSYHDISTYS, MPK)

Maanpuolustuskoulutusyhdistys (MPK) kehittää kyberturvallisuuskurssia kansalaisille sekä teknistä osaamista hallitseville henkilöille.

ESIMERKKEJÄ HVK:N YRITYKSILLE SUUNNATUSTA KOULUTUKSESTA JA SUUNNITTELUSTA:

59. ICT-POOLIN TUKI MUILLE POOLEILLE TOIMIALOJEN KYBERTURVALLISUUDEN KEHITTÄMISESSÄ

	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2, 3 ja 7
EHDOTUKSEN VASTUUTAHO: HVK	EHDOTUKSEN YHTEISTYÖTAHOT: ICT-pooli, Huoltovarmuuskeskus, huoltovarmuusorganisaation poolit

ICT-pooli organisoi koulutus- ja seminaarisarjan, jonka tarkoitus on kouluttaa eri alojen toimijoita kyberturvallisuudesta sekä auttaa tunnistamaan eri toimialoilla olevia kyberturvallisuuteen liittyviä tarpeita.

EHDOTUKSEN AIKATAULU:

60. KYBERTURVALLISUUS TUTUKSI –KAMPANJA

Huoltovarmuusorganisaation kampanjan tavoitteena on luoda edellytyksiä strategian toimeenpanon kannalta tarpeellisille ja tarkoituksenmukaisille toimenpiteille. Kampanja kohdistetaan ensisijaisesti huoltovarmuuden kannalta kriittisiin yrityksiin. Kampanjan toteutuksessa tukeudutaan ensisijaisesti huoltovarmuusorganisaation eri toimielimiin: sektoreihin ja pooleihin.

Kansallinen kyberturvallisuusstrategia antaa kyberturvallisuudelle selkeän tulkinnan ja sisällön. Nykykäsitykset kyberturvallisuudesta kuitenkin vaihtelevat erilaisista viitekehyksistä johtuen merkittävästi. Ilman kuvattua kampanjaa ei eri toimijoilta voi odottaa yhteisiä, laajoja ja yhteensopivia tulkintoja ja toimenpiteitä strategian käytännön toteuttamiseksi.

Kampanja vaiheistetaan vähintään kahteen vaiheeseen. Ensimmäisen vaiheen tarkoituksena on avata strategian keskeinen sisältö ja keskeiset perusteet. Toisessa vaiheessa strategian toteuttamista syvennetään sektorikohtaisilla seminaareilla ja työpajoilla.

EHDOTUKSEN AIKATAULU: Hanke käynnistetään 1. vuosineljännes/2014. Tavoitteena on, että ensimmäinen vaihe tavoittaa kaikki huoltovarmuuden kannalta kriittiset yritykset vuoden loppuun mennessä. Vaiheen kaksi toteutus käynnistyy 2. vuosineljännes/2014 ja se etenee rinnan vaiheen 1 toimenpiteiden kanssa.

Hyvinvointipalveluiden turvaaminen

61. SÄHKÖISEN IDENTITEETIN HALLINTARATKAISU	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1 ja 3
EHDOTUKSEN VASTUUTAHO: VM	EHDOTUKSEN YHTEISTYÖTAHOT:

EHDOTUKSEN KUVAUS JA PERUSTELUT

Kansallisen palveluarkkitehtuurin ja palveluväylän tehokkaan toiminnan edellytys on toimiva ja edullinen kansallinen sähköisen identiteetin hallintaratkaisu, joka kattaa henkilötunnistamisen, valtuutusten tunnistamisen sekä yritysten edustajien ja terveydenhuollon ammattihenkilöiden ja muiden mahdollisten roolien tunnistamisen. Periaatteena on se, että aina ensin tunnistetaan henkilö ja sen jälkeen tarkistetaan hänen roolinsa käytetyssä palvelussa. Kansallista sähköisen identiteetin ratkaisua on suunniteltu v. 2013 alusta valtiovarainministeriön, liikenne- ja viestintäministeriön ja Sitran yhteistyöllä. Kaikki osapuolet pitävät toimivaa ja helppokäyttöistä sähköistä tunnistamista kansallisesti ehdottoman tärkeänä sähköisten palvelujen käytölle ja kehittämiselle.

Toimenpiteessä huomioidaan SM:n näkemykset siitä, että väestörekisterikeskuksen asiointikorttiympäristö ei mahdollista kaikissa tilanteissa korkean käytettävyyden vaatimuksia. Arvion mukaan tilanteen parantamiseksi tulisi rakentaa korkean turvallisuustason ja –käytettävyyden mahdollistama ympäristö, joka sisältää luotettavat tunnistautumis- ja salausratkaisut.

EHDOTUKSEN AIKATAULU:

62. TIETOJÄRJESTELMIIN KOHDISTUVIA HYÖKKÄYKSIÄ KOSKEVAN EU:N DIREKTIIVIN KANSALLISET TÄYTÄNTÖÖNPANOTOIMET	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 8
EHDOTUKSEN VASTUUTAHO: OM	EHDOTUKSEN YHTEISTYÖTAHOT: OM, SM, LVM, Tietosuojavaltuutetun toimisto, Suomen asianajajaliitto, Valtakunnansyyttäjänvirasto. Hankkeella on liityntä myös hallitusohjelmassa olevaan kirjaukseen: "Tietoverkkorikollisuuden torjuntaan panostetaan osana järjestäytyneen rikollisuuden torjuntaa. Turvataan keinot torjua identiteettivarkaudet kaikissa tapauksissa."

EHDOTUKSEN KUVAUS JA PERUSTELUT

Oikeusministeriö on asettanut työryhmän jonka tehtävänä on valmistella ehdotus tietojärjestelmiin kohdistuvia hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamista koskevan direktiivin 2013/40/EU kansallista täytäntöönpanoa koskevaksi lainsäädännöksi. Direktiivi sisältää nykyisen puitepäätöksen vastaavat säännökset pääosin sellaisenaan. Direktiiviin lisättäisiin myös eräitä kriminalisointivelvoitteita, joita vastaavat ovat Euroopan neuvoston tietoverkkorikollisuutta koskevassa yleissopimuksessa (SopS 60/2007). Lisäksi direktiivissä on uusia säännöksiä, joiden tarkoituksena on muun muassa puuttua uusiin uhkakuviin kuten laajamittaisiin tietoverkkohyökkäyksiin niin sanottuja bot-verkkoja käyttämällä ja tietoverkkorikoksen yhteydessä tapahtuvaan henkilöllisyyden väärinkäyttöön.

Direktiivillä pyritään torjumaan tietojärjestelmiin kohdistuvia rikoksia varmistamalla, että kaikissa unionin jäsenvaltioissa on säädetty teoista riittävät rangaistukset. Direktiivillä pyritään myös parantamaan tällaisten rikosten tutkintaan liittyvää jäsenvaltioiden välistä yhteistyötä ja

rikosten tilastointia. EU:n tietoverkkorikosdirektiivin kansallisten täytäntöönpanotoimien yhteydessä arvioidaan myös toisen henkilön identiteettitietojen väärinkäyttöä saattaen osaksi Suomen kansallista lainsäädäntöä direktiiviin liittyvät asiaa koskevat määräykset. Kyseisissä määräyksissä huomioidaan myös sille henkilölle aiheutuva vahinko, jota identiteettitieto koskee.
EHDOTUKSEN AIKATAULU: Direktiivin edellyttämät kansalliset täytäntöönpanotoimet on tehtävä viimeistään 4.9.2015.

63. KEVYET KÄYTTÖLIITTYMÄT KANTA–JÄRJESTELMÄÄN JA KANSA-JÄRJESTELMÄN KEHITTÄMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 7 ja 9
EHDOTUKSEN VASTUUTAHO: STM	EHDOTUKSEN YHTEISTYÖTAHOT: STM, Kela
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Rakennetaan kevyt käyttöliittymä, jonka avulla potilastietojen käsittely onnistuu käyttämättä paikallisia järjestelmiä, sekä potilaiden yksityisyyden suojaa tai muita perusoikeuksia vaarantamatta. Järjestelmää voidaan käyttää poikkeusoloissa varajärjestelmänä. (jos paikalliset potilastietojärjestelmät eivät toimi, tai jos tietoja tarvitaan kohteissa, joissa ei ole kiinteää tietojärjestelmää). Tämä edellyttää kuitenkin toimivaa tietoliikenneyhteyttä. Kantaa vastaavan Kansan valmistelu on käynnissä. Kansallinen arkisto sosiaalihuollon asiakirjoille on tulossa vuosikymmenen lopussa. Tämä tulee olemaan turvallisuustasoltaan parempi kuin nykyinen järjestelmä. Vastaava suorakäyttöliittymä on mahdollista, mikäli näin halutaan.	
EHDOTUKSEN AIKATAULU: Tavoitteena on, että käyttöliittymä olisi valmis vuonna 2015. Kansa-järjestelmän toteutus on vuodesta 2015 alkaen, ja sen arvioidaan olevan täysin operatiivinen 2017.	

64. SOSIAALI- JA TERVEYDENHUOLLON JÄRJESTÄMISLAKI, SOSIAALIHUOLTOLAKI JA MUUTOKSET TERVEYDENHUOLTOLAKIIN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 8
EHDOTUKSEN VASTUUTAHO: STM	EHDOTUKSEN YHTEISTYÖTAHOT:
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Varautumisvelvoitteen sisällyttäminen sosiaali- ja terveydenhuollon järjestämislakiin ja sosiaalihuoltolakiin. Varautumisvelvoitteen tarkistukset terveydenhuoltolaissa. Varautumisvelvoite, joka sisältää kyberuhkiin varautumisen, sisällytetään entistä selkeämmin toimialan lainsäädäntöön.	
EHDOTUKSEN AIKATAULU: Sosiaali- ja terveydenhuollon järjestämislaki ja uusi sosiaalihuoltolaki sekä muutokset terveydenhuoltolakiin Suunnitelma tässä vaiheessa: HE 2014 keväällä, lait voimaan 1.1.2015, siirtymäaikaa rakenteiden osalta vuoteen 2017	

65. LAKI SOSIAALI- JA TERVEYDENHUOLLON ASIAKASTIETOJEN SÄHKÖISESTÄ KÄSITTELYSTÄ (159/2007)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 8
EHDOTUKSEN VASTUUTAHO: STM	EHDOTUKSEN YHTEISTYÖTAHOT:
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007). Lakiin on tulossa muutos, joka edellyttää tietojärjestelmien sertifiointia. Sertifioinnin toteuttaisi Viestintävirasto osana julkisen hallinnon sertifiointia käyttäen VAHTI luokittelua. Koska VAHTI-luokittelu ei välttämättä huomioi kaikkia sosiaali- ja terveydenhuollon ominaispiirteitä, on sitä paikallaan verrata organisaatioissa nyt käytössä oleviin menettelytapoihin.	
EHDOTUKSEN AIKATAULU: 2014	

Yritysten toimintaedellytykset ja jatkuvuuden hallinta

66. FISC-KYBERLABORATORIO	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1,2,3 ja 7
EHDOTUKSEN VASTUUTAHO: Finnish Information Security Cluster (FISC)	EHDOTUKSEN YHTEISTYÖTAHOT: Suomalaisten tietoturva-alan yritysten yhteenliittymä (Finnish Information Security Cluster, FISC) sekä tutkimuslaitokset
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Suomalaisten tietoturva-alan yritysten yhteenliittymä (Finnish Information Security Cluster, FISC) pyrkii synnyttämään kansallisesti merkittävän kyberlaboratorion. Sen tavoitteena on tuottaa uusia yhteistyömalleja ja vahvistaa klusteriyritysten ja tutkimuslaitosten osaamista osana kansallista kyberturvaklusteria. Kyberlaboratorio tulee tarjoamaan mm. merkittävien tietojärjestelmien haavoittuvuuksien sekä tuotteiden ja palveluiden kyberturvallisuuden tutkimista. Lisäksi kyberlaboratorio toimii suomalaisen yksityissektorin yhteistyöfoorumina. FISC-yhteistyö pyrkii olemaan toimiva esimerkki public-private –toimintamallista. Laboratorio olisi myös kanava rakentaa uusia innovaatioita jo alalla toimiville yrityksille tai mahdollisesti pohjana kokonaan uusille yrityksille. Yhteenliittymä on huomioinut kilpailulain vaatimukset, jotta kiellettyjä toimintamalleja ei syntyisi. Kyberlaboratorio on voittoa tavoittelematon yhtiö.	
EHDOTUKSEN AIKATAULU:	

67. RGCE-KYBERTOIMINTAYMPARISTÖ (REALISTIC GLOBAL CYBER ENVIRONMENT)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2,3,5 ja 7

EHDOTUKSEN VASTUUTAHO: Jyväskylän ammattikorkeakoulu (JAMK)	EHDOTUKSEN YHTEISTYÖTAHOT:
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Jyväskylän ammattikorkeakoulu (JAMK) on toteuttanut JYVSECTEC:n RGCE-kybertoimintaympäristön (Realistic Global Cyber Environment). Ympäristössä tapahtuvan tutkimus-, kehitys- ja koulutustoiminnan tavoitteena on parantaa yritysten ja muiden toimijoiden häiriönsietokykyä, mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kykyä havaita ja torjua kyberuhkia sekä kehittää henkilöstön osaamista. Vahvistamalla kyberturvallisuuden osaamispohjaa edistetään innovaatioiden syntymistä, teknologista kehitystä, tuottavuuden kasvua ja tätä kautta kansallista kilpailukykyä ja hyvinvointia.	
EHDOTUKSEN AIKATAULU: Käynnissä ja palvelun jatkokehittäminen vuodesta 2014 eteenpäin	

68. HUOVI-TILANNEKUVATOIMINNON JATKAMINEN, LAAJENTAMINEN JA KEHITTÄMINEN SISÄISEN TURVALLISUUDEN OHJELMAN MUKAISESTI	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2, 3 ja 6
EHDOTUKSEN VASTUUTAHO: HVK	EHDOTUKSEN YHTEISTYÖTAHOT: HVK, yritysturvallisuuden kansallinen yhteistyöryhmä; VNp sisäisen turvallisuuden III ohjelmasta
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Sisäisen turvallisuuden III ohjelmassa esitettiin elinkeinoelämän ja viranomaisten yhteisen tilannekuvatoiminnan perustamista Huoltovarmuuskeskuksen HUOVI-portaalin yhteyteen. VNp:ssä linjattiin seuraavaa: Laaditaan HUOVI-portaalin tekniselle alustalle ensi vaiheessa huoltovarmuuden piiriin kuuluville yrityksille ja myöhemmässä vaiheessa pilottivaiheen tulosten perusteella mahdollisesti kaikille yrityksille avoin vahvalla tunnistamisella kirjautumissuojattu tilannekuvaportaali, jonne viranomaiset ja vertaisyritykset voivat tuottaa operatiivista turvallisuustilannetietoa mm. tietoturvan tilannekuvasta. Tilannekuvan käynnistämisvaiheen aikainen käyttäjäpalaute on ollut hyvää ja tilannekuvaa pidetään yritysten puolelta yhtenä HVK:n kärkihankkeista. Ajantasainen, koottu ja jaettu tilannekuva on välttämätön edellytys kyberuhkien torjuntaan koko taloudellisessa verkostossa.	
EHDOTUKSEN AIKATAULU: Palvelu on jo käytössä.	

69. KRIITTISTEN VALVOMOIDEN YHTEISTOIMINNAN KEHITTÄMINEN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1, 2 ja 3
EHDOTUKSEN VASTUUTAHO: HVK	EHDOTUKSEN YHTEISTYÖTAHOT: HVK, Erillisverkot, yhteiskunnalle kriittisiä palveluja tarjoavat yritykset, joilla on 24/7 valvomo. Arviolta n. 100 organisaatiota.
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Krivat on toimintakonsepti, joka parantaa yhteiskunnan kriittisen infrastruktuurin kannalta	

keskeisten yritysten ja niiden välittömien, kriittisten sidosryhmien yhteistyötä 24/7 valvomotoiminnassa mm. kyberturvallisuuteen liittyvissä häiriötilanteissa: • sähkön, lämmön ja kaasun tuotanto/jakelu • tele- ja tietoliikenne • IT-palvelut • logistiikka
EHDOTUKSEN AIKATAULU: Hanke on toimeenpanovaiheessa.

70. SELVITYS TIETOLIIKENNEYHTEYKSIEN VARMISTAMISESTA	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 2, 3 ja 7
EHDOTUKSEN VASTUUTAHO: Viestintävirasto	EHDOTUKSEN YHTEISTYÖTAHOT: Ministeriöt, muut tarvittavat viranomaiset sekä tietoliikenneoperaattorit
Alan toimijat pyrkivät varmistamaan häiriötilanteiden tietoliikenneyhteydet solmimalla sopimuksia useamman operaattorin kanssa. Käytännössä yhteyksien luotettava varmistaminen on kuitenkin joissain tilanteissa vaikeaa. Toimenpiteen tarkoituksena on luoda konkreettinen toimintamalli sellaista tilannetta varten, jossa kansainvälisen tietoliikenteen kapasiteetti supistuu voimakkaasti ja eri käyttäjien tai käyttäjäryhmien tarpeita joudutaan priorisoimaan, mutta valmiuslain soveltamisen edellytykset eivät vielä täyty.	
EHDOTUKSEN AIKATAULU:	

71. SELVITYS SUOMALAISEN ICT-SEKTORIN SÄÄNTELYN VAIKUTUKSISTA SUOMEN KILPAILUKYKYYN	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 8
EHDOTUKSEN VASTUUTAHO: LVM	EHDOTUKSEN YHTEISTYÖTAHOT: TEM, VM, elinkeinoelämä
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Selvitetään Suomen ICT-sektoria koskeva lainsäädäntö suhteessa keskeisiin kilpailijamaihin ja sen vaikutukset elinkeinoelämän kilpailukykyyn. Selvityksen perusteella arvioidaan, mahdollistaako Suomen sääntely-ympäristö kilpailukykyisen ja vientiä harjoittavan kyberosaamisklusterin syntymisen ja miten sääntely vaikuttaa yleisesti ICT:hen nojaavien suomalaisyritysten kilpailukykyyn. Selvityksessä huomioidaan ICT-palveluiden läpileikkaavuus ja vaikutukset ICT:tä käyttävien muiden sektoreiden kilpailukykyyn.	
EHDOTUKSEN AIKATAULU: Aikataulu 2014	

HUOLTOVARMUUSKESKUKSEN PALVELUIHIN LIITTYVIÄ TOIMENPITEITÄ:	
72. TEOLLISUUSAUTOMAATION KYBERSUOJAUKSEN KÄYTÄNNÖT JA KARTOITUKSET (2014-2015)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUK-

	SEEN: 1,2 ja 3
EHDOTUKSEN VASTUUTAHO:	EHDOTUKSEN YHTEISTYÖTAHOT: HVK, VTT, Teollisuusautomaatiota hyödyntävät ja kehittävät yritykset
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Kehitetään ja testataan yhdessä teollisuuden kanssa tarvittavat palvelut, käytännöt ja vertailupohjat tuotannon kybersuojauksen tason parantamiseksi. Työ kattaa automaatiota hyödyntävän teollisuuden tuotantoon liittyvät toiminnot ja järjestelmät sekä antaa suositukset toimenpiteille kyberturvallisuuden ja tuotannon jatkuvuuden parantamiseksi. Tavoitteena on jatkaa kybersuojauksen ja jatkuvuuden varmistamisen käytäntöjen kehittämistä.	
EHDOTUKSEN AIKATAULU:2014-2015	
73. TEOLLISUUDEN KYBERTURVALLISUUDEN VAATIMUSTEN JALKAUTTAMINEN TUOTANTOON (2014-2016)	
Sovelletaan ja jatkojalostetaan tietoturvavaatimuksia ja jalkautetaan niitä kohdeyritysten automatisoidun tuotannon prosesseihin. Sulautetaan kyberturvallisuuden ja jatkuvuudenhallinnan tarpeet ja suojauskäytännöt saumattomasti teollisuusyrityksen muihin olemassa oleviin tuotantokäytäntöihin.	
EHDOTUKSEN AIKATAULU: 2014-2016.	
74. TUOTANTOAUTOMAATIOVERKON MONITOROINTIPALVELU (2014-2016)	
	EHDOTUS LIITTYY STRATEGIAN LINJAUKSEEN: 1, 2 ja 3
EHDOTUKSEN VASTUUTAHO:	EHDOTUKSEN YHTEISTYÖTAHOT: HVK, VTT, teollisuusautomaatiota hyödyntävät ja kehittävät yritykset
EHDOTUKSEN KUVAUS JA PERUSTELUT	
Kehitetään ja testataan yhdessä teollisuuden kanssa tekniset monitorointipalvelut, joilla voidaan seurata tuotannon tietoverkon kyberturvallisuuden tilaa reaaliaikaisesti. Palvelu kattaa normaalista tuotannosta poikkeavien tapahtumien tunnistamisen ja raportoinnin perustuen teknologia- ja palveluyritysten, tuotantoyritysten sekä tutkimuslaitosten yhteistyöhön	
EHDOTUKSEN AIKATAULU: 2014-2016.	

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

LIITE 2: LYHENNELUETTELO

Lyhenne:	**Selvennys:**
AVI	Aluehallintovirasto
AMK	ammattikorkeakoulu
CAA	salaustuotteiden hyväksynnästä ja kansainvälisen turvaluokitellun tiedon suojaamisesta vastaava viranomainen, Crypto Approval Authority
CDA	aineiston jakeluverkon hallinnoinnista, kirjanpidosta sekä aineiston turvallisen käsittelyn ohjeistuksesta vastaava viranomainen, Crypto Distribution Authority
CERT	tietoturvaviranomainen
CMDB	Configuration Management Data Base
DDP	Digital Defenders Partnership
DSA	määrätty kansallinen turvallisuusviranomainen, Designated Security Authority
EC3	Europolin kyperrikollisuus keskus, European Cyber Crime Center
EK	Elinkeinoelämän keskusliitto
ENISA	EU:n verkko- ja tietoturvavirasto
FISC	Suomen tietoturvaklusteri, Finnish Information Security Cluster
FMI	Ilmatieteenlaitos
FOC	Freedom Online Coalition
FSC	yhteisöturvallisuusmenettely, facility security clearance
GovHUOVI	valtionhallinnon HUOVI-portaali
HALTIK	Hallinnon tietotekniikkakeskus

HAVARO	huoltovarmuuskriittisille yrityksille suunnattu tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä
HE	hallituksen esitys
HUOVI	verkossa toimiva huoltovarmuuskriittisten yritysten, poolien ja Huoltovarmuuskeskuksen varautumisen suojattu tietokanava
HVK	Huoltovarmuuskeskus
Inka	Innovatiiviset kaupungit (ohjelma)
ICT	tieto- ja viestintätekniikka
ISO 27001	(eräs) tietoturvallisuussertifiointi
JAMK	Jyväskylän ammattikorkeakoulu
JulkICT	julkisen hallinnon ICT
JYVSECTEC	Jyväskylä security technology -turvallisuusteknologian kehittämishanke
JYO	Jyväskylän yliopisto
Kanta	Kansallinen sosiaalihuollon asiakastietovaranto
Kansa	Kansallisen Terveysarkisto
KEHU	keskushallinnon uudistushanke
KELA	Kansaneläkelaitos
KRIVAT	toimintakonsepti kriittisten valvomojen turvallisuuden parantamiseksi
KRP	Keskusrikospoliisi
LiVi	Liikennevirasto
LTL	luottamusta ja turvallisuutta lisäävät (toimet)
LVM	liikenne- ja viestintäministeriö

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

MPK	Maanpuolustuskoulutusyhdistys
MILCERT	Military Computer Emergency Response Team
NB8-maat	Pohjoismaat ja Baltian maat
NCSA	tietoliikenneturvallisuusviranomainen, National Communication Security Authority
NSA	(Suomen oma) kansallinen turvallisuusviranomainen, National Security Authority
NTA	sähkömagneettisen hajasäteilyn haittojen minimoinnin kansallisesta koordinoinnista ja ohjeistuksesta vastaava viranomainen, National Temptest Authority
OECD	Taloudellisen yhteistyön ja kehityksen järjestö, Organization for Economic Cooperation and Development
OKM	opetus- ja kulttuuriministeriö
OM	oikeusministeriö
PEJOJÄPÄÄL	pääesikunnan johtamisjärjestelmäpäällikkö
PVOPPÄÄLL	Puolustusvoimien operaatiopäällikkö
PfP	Naton rauhankumppanuusohjelma, Partnership for Peace
POLAMK	Poliisiammattikorkeakoulu
PLM	puolustusministeriö
PSC	henkilöturvatodistus, personal security clearance
PTR	poliisin, tullin ja rajavartioston yhteistoiminta
PV	Puolustusvoimat
RGCE	Kyberturvallisuuden kehitysympäristö, Realistic Global Cyber Environment

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

SAA	kansainvälistä turvaluokiteltua tietoa käsittelevien tietojärjestelmien hyväksynnästä vastaava viranomainen, Security Accreditation Authority
Salve	Ulkoasiainhallinnon ja sen sidosryhmien turvaluokitellun tiedon käsittely-ympäristö
SATU	salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (Salve-Tuve-integraatio)
SecICT	valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke
SM	sisäministeriö
STM	sosiaali- ja terveysministeriö
SPEK	Suomen Pelastusalan Keskusjärjestö
Supo	Suojelupoliisi
Tekes	Teknologian ja innovaatioiden kehittämiskeskus
TEMPEST	sähkömagneettisen hajasäteilyn haittojen minimointiin tähtäävä ohjelma
TK&I	tutkimus, kehitys ja innovaatio
TORI	toimialariippumattomat ICT-tehtävät
TRAFI	Liikennevirasto
TUVE	hallinnon turvallisuusverkko
UM	ulkoasiainministeriö
VAHTI	valtionhallinnon tietoturvallisuuden johtoryhmä
VIRVE	viranomaisverkko
ViVi	Viestintävirasto
VM	valtiovarainministeriö
VN	valtioneuvosto

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

VNK	valtioneuvoston kanslia
VNp	valtioneuvoston periaatepäätös
VP	valtiopäivät
VTT	Valtion teknillinen tutkimuskeskus
WSIS	tietoyhteiskuntaa käsittelevän huippukokous, World Summit on the Information Society
YTPP	(EU:n) yhteinen turvallisuus- ja puolustuspolitiikka

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
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
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi