Hallitusohjelma toimenpide-esitys: TKI-alue

Kyberturvallisuus

Vahvistetaan kansallista kyberresilienssiä tehostamalla kyberpolitiikkatoimia, vahvistamalla strategista johtamista, PPP-yhteistyötä, huoltovarmuutta ja alan osaamista.

Kyberturvallisuuden kehittäminen tulevalla hallituskaudella

- **Kehityskohteita**
    - Kansallisen kyberturvallisuuden johtamisen terävöittäminen
    - Kansallisen kyberturvallisuusosaamisen lisääminen
    - Kansallisen julkisen ja yksityisen yhteistyön vahvistaminen
    - Kansallisen kyberhuoltovarmuuden tehostaminen

- **Tilannekuva:** Suomalainen yhteiskunta digitalisoituu vauhdilla ja Suomi on yksi maailman kärkimaista julkisissa sähköisissä palveluissa. Tavoitteena on tehdä palveluista toimivampia ja joustavampia sekä kustannustehokkaita. Digitalisaatiossa tulisi aikaan saada entistä paremmat ja luotettavammat palveluketjut ja järjestelmät kansalaisten, julkisen sektorin ja yritysten tarpeisiin.

  Digitalisaatiosta on tullut yhä tärkeämpi osa yritysten ja ihmisten toimintaa. Digitaalisuus on tänä päivänä myös yhä syvemmällä ihmisten ja yritysten arjessa; digitaaliset palvelut helpottavat yritysten ja ihmisten arkea ja elämää. Digitaalisuuteen pohjautuvia innovaatiomahdollisuuksia syntyy yhä enemmän.

  Venäjän hyökkäys Ukrainaan on osoittanut kansallisen kriittisen infrastruktuurin merkityksen. Suomessa on liikkeellä jatkuvasti haittaohjelmia kohteinaan kansalaiset, yritykset ja julkinen sektori. Lisäksi kybervakoilu ja kyberhyökkäykset yritysten tuotanto- ja automaatiojärjestelmiin ovat lisääntyneet.

  Suomalaisilla on myös tutkitusti EU-maiden paras digiosaaminen. Tehtyjen selvitysten mukaan kyberturvallisuusalan osaajapula on suuri. Suomi on maailman johtava digitalisaation hyödyntäjä ja siksi tarvitsemme nykyistä enemmän kyberturvallisuuden erityisosaajia, korkealaatuista korkeakoulutusta sekä tutkimus- ja innovaatiotoimintaa, ja myös vahvaa kytkeytymistä muualla tuotettuun uuteen tietoon.

- **Kehittämisen tavoitteet:**
    - Luodaan Suomen kyberpolitiikkaohjelma kansallisten tavoitteiden vahvistamiseksi.
    - Vahvistetaan kansallista kyberturvallisuusrelienssiä luomalla laaja-alainen kehittämisohjelma, jossa mukana eri ministeriöt omine kyberturvallisuusohjelmineen, alan yritykset ja korkeakoulusektori
    - Vahvistetaan Suomen yliopistojen ja ammattikorkeakoulujen keskinäistä opetusyhteistyötä sekä vahvistetaan vuorovaikutusta yritysten ja julkisen sektorin kanssa, jotta alan tutkinto-opetusta ja jo työelämässä olevien kyberturvallisuusosaamista voidaan kehittää.

- **Uudistamistarpeet:**
    - Tarvitaan kansallinen kyberturvallisuusresilienssin investointiohjelma.
    - Tarvittava osaamisen kasvattaminen vaatii koulutusjärjestelmältä nopeaa reagointia ja kykyä luoda joustavia ja kyberturvallisuuden eri osa-alueita laajasti kattavia opintokokonaisuuksia perinteisten tutkintojen rinnalle.
    - Tutkimusten mukaan tarvitsemme jopa 10 000 ammattilaista kyberturvallisuuden eri tehtäviin, kuten turvallisen tuotannon, suojaamisen, valvonnan ja analyysin sekä johtamisen työtehtäviin seuraavien vuosien aikana.
    - Kyberturvallisuuden osaajien määrää yhteiskunnassa voidaan lisätä vaikuttamalla useaan eri tekijään kuten aloituspaikkoja, muunto- ja täydennyskoulutusta sekä jatkuvaa oppimista lisäämällä. Opetusyhteistyön syventäminen yliopistojen ja ammattikorkeakoulujen välillä mahdollistaa opetuksen tehostamisen.

- **Toimenpiteet:**
    - Hankkeella tuotetaan kyberturvallisuuden perusosaamista suurelle määrälle opiskelijoita ja lisätään valmistuvien kyberturvallisuuden erityisosaajien määrää. Tähän päästään lisäämällä kyberturvallisuuden koulutustarjontaa sekä määrällisesti että laadullisesti.
    - Perusosaamista parannetaan luomalla opetusta, joka skaalautuu suurelle määrälle opiskelijoita ja jota on mahdollista jakaa verkossa korkeakoulujen ja elinikäisten oppijoiden käyttöön.
    - Kyberturvallisuuden erityisosaajien määrää lisätään tarjoamalla opiskelijoille opintokokonaisuuksia, jotka koostuvat usean korkeakoulun kursseista yhdistäen näiden opetuksen ja tutkimuksen vahvuusalueita.
    - Opetusresursseja käytetään tehokkaasti selvittämällä todelliset koulutustarpeet ja koordinoimalla opetustarjontaa korkeakoulujen välillä.
    - Lisäresurssit kehittäisivät opetusta, ja se näkyisi kyberturvallisuuden käytännön taitoja kehittävien harjoitusten määrän lisäämisen opetuksessa.
    - Vuotuinen lisärahoitustarve on 10 miljoonaan euroa, jolla voidaan sekä laajentaa kyberturvallisuuden opetusta että lisätä valmistuvien opiskelijoiden määriä.

Laaja tilannekuva- ja tavoiteanalyysi

1. Poliittinen ulottuvuus

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne (engl. Cyber Politics). Kybertoimintaympäristö on jatkuvassa muutoksen tilassa, ja tätä kehitystä pyritään poliittisin keinoin ohjaamaan. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä kuten EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa.

Kyberdiplomatiassa käsitellään alan kansainvälistä oikeutta ja normeja, kyberturvallisuutta ja muita luottamusta lisääviä toimia. Keskinäisen yhteisymmärryksen ja yhteisten pelisääntöjen avulla voidaan vähentää erilaisten konfliktien uhkaa. EU on jo muutamien vuosien ajan kiinnittänyt huomiota kyberdiplomatiaan. EU:n neuvosto päätti 2017 kehittää

kyberdiplomatiaan välineistön, joka on EU:n yhteinen diplomaattinen vastaus haitallisiin kybertoimiin. Vuonna 2018 EU julkaisi päätelmät haitallisista kybertoimista. Päätelmissä korostui kybertoimintaympäristön vapaus, vakaus, turvallisuus, avoimuus ja globaalius. EU:n neuvosto vahvisti kehyksen vuonna 2019, jonka avulla EU voi määrätä kohdennettuja rajoittavia toimenpiteitä, joilla estetään ja vastataan kyberhyökkäyksiin, jotka muodostavat uhkan EU:lle tai sen jäsenvaltiolle. Myös kyberhyökkäykseen osallistuneet kolmannet maat tai kansainväliset järjestöt voivat olla toimenpiteiden kohteena, jos se katsotaan tarpeelliseksi ulko- ja turvallisuuspolitiikan tavoitteiden saavuttamiseksi. EU käytti tätä välineistöä ensimmäistä kertaa heinäkuussa 2020, kun neuvosto päätti määrätä rajoittavia toimenpiteitä useista kyberhyökkäyksistä vastuussa olevia tai niihin osallistuneita kuutta henkilöä (Kiina, Venäjä) ja kolmea yhteisöä (Kiina, Pohjois-Korea, Venäjä) vastaan.

Kyberturvallisuudessa valtioiden välisen luottamuksen lisääminen on keskeinen kysymys. Valtioiden välistä keskustelua tulee tiivistää kybertoimintaympäristöön liittyvissä kysymyksissä niin monenvälisesti, alueellisesti kuin kahdenvälisestikin. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita.

2. Kybervoima

Kybervoima/valta (engl. Cyber Power) kuvaa valtion kybersuorituskykyä vallankäytön välineinä. Kybervoimaa voidaan käyttää haluttujen tulosten tuottamiseen kyberympäristössä tai sen ulkopuolella. Kybervoima jakaantuu maailmassa niin eri valtiollisten kuin ei-valtiollisten toimijoiden kesken. Suurvalloille on mahdollista investoida laaja-alaisiin puolustuksellisiin ja hyökkäyksellisiin kyvykkyyksiin, kun taas pienet valtiot keskittyvät erikoisosaamiskykyihin.

Kybertoimintaympäristö on yhä merkittävämpi tila, jossa vaikutetaan Suomen kansalliseen turvallisuuteen. 2020-luvun sodankäyntiin sekoittuu uusia kyberoperaatioelementtejä, joiden tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpitoa voidaan toteuttaa kyberoperaatioiden avulla.

Useat valtiot ja NATO ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin. Kesäkuussa 2021 NATO teki linjauksen, jonka mukaan merkittävät haitalliset kybertoimet voidaan jatkossa tietyissä tapauksissa rinnastaa aseelliseen hyökkäykseen. Lokakuussa 2021 NATO-maiden puolustusministerit sopivat yleissuunnitelmasta, jossa varaudutaan Venäjän mahdolliseen aggressioon, jossa kyberoperaatiot olisivat yksi toimintamuoto.

Ukrainan sota on lisännyt uhkia kyber- ja informaatioympäristössä. Suomen kansallista kybervoimaa/valtaa tulee kehittää edelleen, jota tarvetta mahdollinen NATO-jäsenyys edelleen vahvistaa. Kyberhyökkäykset ovat osa Venäjän hyökkäystä Ukrainaan ja että Venäjä todennäköisesti laajentaa kyber- ja informaatio-operaatioitaan Ukrainasta länteen, on erittäin todennäköinen.

3. Kyberresilientti yhteiskunta

Yhteiskuntaan kohdistuvan kyberuhan kohteista keskeisiä ovat kansallisen turvallisuuden kohteet sekä yhteiskunnan elintärkeät toiminnot, joilla turvataan kansalaisten elinmahdollisuudet. Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat

välttämättömiä yhteiskunnan jatkuvalle toiminnalle. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. Nämä verkostot eivät ole erillisiä entiteettejä vaan muodostava kansallisen kriittisen infrastruktuuriverkoston, jossa on paljon keskinäisriippuvuuksia. Yhden systeemin lamaantuminen tai romahtaminen vaikuttaa verkoston muihin osiin.

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja korkean käyttövarmuuden omaavista sähköjärjestelmistä ja tiedonsiirtoverkostoista sekä muista luotettavista ja tietosisällöltään eheistä hallinnon ja kansalaisten palveluista. Teknologinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan digitalisoitumiseen, verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Kyse on myös kansalaisten luottamuksen ylläpitämisestä yhteiskunnan toimintaan.

Kyberhyökkäykset eri muodoissaan ja erilaiset informaatiovaikuttamisen muodot lisääntyvät jatkuvasti. Tämän kehityksen vuoksi on lisättävä edelleen varautumista kyberuhkiin ja -häiriötilanteisiin, jotka vaarantavat yhteiskunnalle välttämättömien järjestelmien ja rakenteiden toimivuutta jo normaalioloissa. Suomalaisen yhteiskunnan ja yritysten riippuvuus kybertoimintaympäristöstä kasvaa entisestään tulevina vuosina.

Toimenpiteitä yritysten kasvun tukemiseksi on lisättävä erityisesti korkeaa arvonlisää tuottavilla toimialoilla kuten kyberturvallisuusalalla. Tarvitaan tehokkaita toimenpiteitä julkisen talouden tasapainottamiseksi ja yritysten kasvuedellytysten parantamiseksi myös kyberturvallisuuden näkökulmasta.

Kybertoimintaympäristön turvaamisen kannalta oikea, laaja-alainen ja jaettu tilannekuva ja kehittämissuunnitelma ovat välttämättömiä. Siksi Suomeen kehitettävän vahvan kyberturvallisuuden ekosysteemin kehittämistä tulee vahvistaa. Tässä ekosysteemissä kansainvälinen tutkimus- ja kehitysyhteistyö on erittäin tärkeää ja välttämätöntä.

Kyberturvallisuuden kannalta huoltovarmuuskriittiset yritykset ovat keskiössä. Tämän lisäksi tulee ottaa huomioon Suomen elinkeinorakenteen mikro- ja pk-yritysten suuri osuus, jotta kyberturvallisuusresilienssi saadaan laajasti toimimaan koko yrityskentässä. Tämä sektori erityisesti tarvitsee laajasti sekä hallinnollista, että kyberteollisuuden tukea, palveluita ja ratkaisuja turvallisuutensa parantamiseksi.

Kriittisen infrastruktuurin suojaamiseksi tarvitaan sekä välittömiä että pitkän ajan toimenpiteitä. Erityisen huomion kohteena tulee olla infrastruktuurin IT-, OT-, SCADA- ja ICS-osat, sillä niiden avulla ohjataan järjestelmiä ja niihin hyökkääjä kohdistaa lamauttavia ja tuhoavia kyberhyökkäyksiä. Meillä voidaan käyttää kotimaista kyberturvallisuusosaamista nopeaan järjestelmien suojauksen tehostamiseen. Tätä osaamista on saatavissa alan yrityksistä ja oppilaitoksista. Pidemmän aikavälin osalta tarvitaan resurssointeja julkisten järjestelmien kyberturvallisuuden resilienssin parantamiseen ja vahvistamiseen

4. Kyberturvallisuuden strateginen johtaminen

Tällä hetkellä kyberturvallisuuden (digitaalisen) turvallisuuden vastuut ovat valtionhallinnossa liian hajallaan. Kyberturvallisuus on kaikkea toimintaa läpileikkaava teema, jota tulisi johtaa keskitetysti. Hajallaan olevat vastuut ja resurssit haittaavat kansallisen

kyberturvallisuusresilienssin kehittämistä. Tarvitaan ymmärrystä kyberturvallisuuden arvoketjuista ja on tunnistettava eri toimintojen ja toimialojen rajapinnat ja mahdolliset epäjatkuvuuskohdat. Tässä tarvitaan vahvaa julkisen ja yksityisen sektorin yhteistoimintaa. Kyberalan yritysten rooli kyberturvallisuuden ratkaisujen kehittäjänä ja tuottajana, yhteistyössä julkisen sektorin kanssa, on aivan olennaista.

Kansallinen kyberturvallisuuden strategisen tason johtaminen muodostuu seuraavista kolmesta osakokonaisuuksista:

1. normaaliaikojen kyberturvallisuuden toteuttaminen (kybersuojaus),
2. laajamittaisten häiriötilanteiden hallinnan johtaminen normaali- ja poikkeusoloissa
3. kybervarautumisen ja -huoltovarmuuden johtaminen

Kohdan 1 toimenpiteistä huolehtii kukin hallinnonalan ja organisaatio osana jokapäiväistä toimintaansa. Arjessa yksilöt ja organisaatiot kohtaavat säännöllisesti kyberhyökkäyksiä, joilta suojaudumme oikean toimintatavan ja teknologian avulla.

Vakavia häiriötilanteita voi esiintyä sekä normaaliaikana että poikkeusoloissa. Normaaliajan häiriötilanteet hallitaan viranomaisten tavanomaisin toimivaltuuksin ja organisaatioiden voimavaroin. Normaalioloissa rakennettavat järjestelmät ja varautumistoimenpiteet luovat perustan toiminnalle poikkeusoloissa. Vastaavasti poikkeusolojen varalle luotuja järjestelyitä voidaan hyödyntää normaaliolojen häiriötilanteiden hallinnassa.

Kohdan 3 mukaiseen varautumiseen yhdistyy huoltovarmuus ja kyberomavaraisuudesta huolehtiminen. Tämä tarkoittaa väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen ja niihin liittyvien teknisten järjestelmien turvaamista poikkeusolojen ja niihin verrattavissa olevien vakavien kyberhäiriöiden varalta. Varautumista ohjaa eri elintärkeille toiminnoille asetetut velvoitteet ja organisaatioiden omat tavoitteet erityisesti toiminnan jatkuvuuden hallinnan kannalta. Yhteiskunnan digitalisaatio lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien laaja-alaisten kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti.

Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta. Tarvitaan kyky reagoida riittävän nopeasti laajamittaiseen kyberhyökkäykseen tai häiriötilanteeseen sekä tuottaa alati muuttuviin kyberuhkiin varautumisen kannalta välttämätöntä ennakoivaa strategista analyysitietoa. Laajamittaisessa kyberhyökkäystilanteessa vastatoimenpiteet tulee aloittaa välittömästi, aikaa ei ole määritellä vastuutahoja tai -toimijoita. Tehokas kyberhäiriötilanteiden torjunta edellyttää hyvää ja kattavaa kybertilannekuvaa.

Nykyistä johtamisrakennetta ei voi pitää varautumisen yhteensovittamisen, strategisten tavoitteiden tunnistamisen tai kansallisen kyberturvallisuusidentiteetin vahvistamisen kannalta optimaalisena. Nykymalli ei ohjaa riittävästi hallinnonalojen, elinkeinoelämän ja kolmannen sektorin kyberturvallisuusvarautumista eikä muodosta riittävän keskitettyä strategista analysointikykyä tilannetietoisuuden tuottamisen tueksi. Kyberturvallisuuden kansallisen omavaraisuuden tunnistaminen ja kehittäminen jäävät nykymallissa

puutteelliseksi. Kansainvälisissä vertailuissa korostunut kyberturvallisuuden strategisen johtamisen läheisen yhteyden tarpeellisuus poliittiseen päätöksentekoon ei näyttäydy selkeänä.

Säädökset

- Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen.
- Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa. Suomen alueellisen koskemattomuuden valvonta määriteltyyn toimintaympäristöön. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä aluloukkauksen estämiseksi tai torjumiseksi, jotka ovat sidottu lain määrittämään toimintaympäristöön.
- Kybertoimintaympäristön vahvistuminen osaksi kansallista toimintaympäristöä tulee aluevalvontalakia ja siihen liittyviä säädöksiä on tarkistettava vastaamaan Suomen kybertoimintaympäristön suojaamisen tarpeita. Uudistus tarvitaan, koska meiltä puuttuu selkeä ja tarkkarajainen juridinen määrittely kansallisesta kybertoimintaympäristöstä. NATO-jäsenyys vahvistaa tätä tarvetta.
- Kansallisen kybertilan määrittely tarvitaan, jotta Suomen kybertilan koskemattomuuden valvonta ja torjunta voidaan tehokkaasti toteuttaa. Tämä tila ei ole vain teknologinen toimintaympäristö vaan merkittävällä tavalla ulko- ja turvallisuuspoliittinen toimintaympäristö.

Kasvun ja investointien rahoittaminen

- Toteutetaan *Kansallinen kyberturvallisuusresilienssi* -kehittämisohjelma, jossa kehitettäviä kasvuun ja investointeihin liittyviä osakokonaisuuksia ovat:
    - Kyberturvallisuuden kansallisen tason johtamisen terävöittäminen,
    - Kyberturvallisuuden tilannekuvan kehittäminen,
    - Kyberturvallisuuden erityisosaamisen vahvistaminen,
    - Kansallisen kyberhuoltovarmuuden varmistaminen,
    - Kyberturvallisuuden PPP-toiminnan tehostaminen,
    - Kyberrikollisuuden torjunnan ja sotilaallisen kyberpuolustuksen vahvistaminen.

Käynnissä olevat hankkeet ja kehitystoimenpiteet

- Kyberturvallisuuden kansalaistaitojen koulutuspaketti Euroopan unionin alueelle (LVM), 2022–2025
- Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen (OKM/60/522/2022), 2022–2025.