Valtioneuvoston kanslian julkaisusarja 2024:xx

Suomen kyberturvallisuusstrategia

2024-2035

Rauli Paananen, Mikko Soikkeli, Mari Starck, Tiina Tuulensuu, Tuija Kuusisto, Tuomo Rusila, Mari Aro

Valtioneuvoston kanslia Helsinki 2024
LUONNOS

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Valtioneuvoston kanslia
Klikkaa ja valitse tekijänoikeustaso

ISBN pdf: VNK täyttää
ISSN pdf: VNK täyttää

ISBN painettu: VNK täyttää
ISSN painettu: VNK täyttää

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2024 Finland (kieliversioissa)

Paino: Grano Oy, 2024

Kuvailulehti
x.x.2024

Suomen kyberturvallisuusstrategia 2024-2035

VNK täyttää, sarja ja numero		**Teema**	Napsauta ja kirjoita
Julkaisija	Valtioneuvoston kanslia		
Tekijä/t	Napsauta ja kirjoita		
Toimittaja/t	Napsauta ja kirjoita		
Yhteisötekijä	Napsauta ja kirjoita		
Kieli	Napsauta ja kirjoita	**Sivumäärä**	VNK täyttää

Tiivistelmä

Suomen kyberturvallisuusstrategia on uudistettu Petteri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuusdirektiivin (NIS2) vaatimukset kansalliselle kyberturvallisuusstrategialle sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö. Hallitusohjelmaan kirjattu informaatiopuolustus on tarkoitus huomioida osana strategisen viestinnän toimintamallia ja puolustuspoliittista selontekoa.

Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035 ja strategia sisältää neljän pilarin alle muodostetut strategiset tavoitteet ja näille yhteiset kehittämistoimet.

Strategia on valmisteltu valtion kyberturvallisuusjohtajan johdolla valtioneuvoston kanslian 8.3.2024 asettaman Valtioneuvoston turvallisuusjohtamisen toimintamallin kehittäminen -hankkeen alatyöryhmässä. Työryhmään kuuluivat nimetyt jäsenet liikenne- ja viestintäministeriöstä, puolustusministeriöstä, valtioneuvoston kansliasta, sisäministeriöstä, ulkoministeriöstä, työ- ja elinkeinoministeriöstä, valtiovarainministeriöstä, oikeusministeriöstä, sosiaali- ja terveysministeriöstä, opetus- ja kulttuuriministeriöstä, maa- ja metsätalousministeriöstä ja Turvallisuuskomitean sihteeristöstä.

Strategian valmisteluun on osallistettu lähes 100 julkisen ja yksityisen sektorin, tiedeyhteisön sekä kansalaisjärjestöjen toimijaa.

Klausuuli	VNK täyttää		
Asiasanat	Napsauta ja kirjoita https://finto.fi/juho/fi/		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN nid.	VNK täyttää	**ISSN painettu**	VNK täyttää
Asianumero	VN/36693/2023	**Hankenumero**	VNK007:00/2024
Julkaisun osoite	VNK täyttää		

Presentationsblad
x.x.2024

Napsauta ja kirjoita otsikko ruotsiksi
Napsauta ja kirjoita alaotsikko ruotsiksi

VNK täyttää, sarjanimi ja numero		**Tema**	Napsauta ja kirjoita
Utgivare	Napsauta ja kirjoita ministeriö		
Författare	Napsauta ja kirjoita		
Redigerare	Napsauta ja kirjoita		
Utarbetad av	Napsauta ja kirjoita		
Språk	Napsauta ja kirjoita	**Sidantal**	VNK täyttää
Referat	Napsauta ja kirjoita tiivistelmä, enintään 1 400 merkkiä. Paina kappaleen lopussa Enter.		

Klausul	VNK täyttää		
Nyckelord	Napsauta ja kirjoita https://finto.fi/juho/fi/		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN tryckt	VNK täyttää	**ISSN tryckt**	VNK täyttää
Ärendenr.	Napsauta ja kirjoita	**Projektnr.**	Napsauta ja kirjoita
URN-adress	VNK täyttää		

Description sheet
x Month 2024

Napsauta ja kirjoita otsikko englanniksi
Napsauta ja kirjoita alaotsikko englanniksi

VNK täyttää, sarjanimi ja numero		**Subject**	Napsauta ja kirjoita
Publisher	Napsauta ja kirjoita		
Author(s)	Napsauta ja kirjoita		
Editor(s)	Napsauta ja kirjoita		
Group author	Napsauta ja kirjoita		
Language	Napsauta ja kirjoita	**Pages**	VNK täyttää
Abstract	Napsauta ja kirjoita tiivistelmä enintään 1 400 merkkiä. Paina kappaleen lopussa Enter.		

Provision	VNK täyttää		
Keywords	Napsauta ja kirjoita https://finto.fi/juho/fi/		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN printed	VNK täyttää	**ISSN printed**	VNK täyttää
Reference no.	Napsauta ja kirjoita	**Project no.**	Napsauta ja kirjoita
URN address	VNK täyttää		

Sisältö

ESIPUHE

Napsauta ja kirjoita teksti. Paina kappaleen lopussa Enter.

Napsauta ja kirjoita Allekirjoittajan nimi.
Napsauta ja kirjoita julkaisukuukausi ja -vuosi, esim. Huhtikuu 2018

Johdanto – kyberturvallisuus on osa kokonaisturvallisuutta

Kyberturvallisuus on osa Suomen kokonaisturvallisuutta ja digitalisoituvaa yhteiskuntaa. Kyberturvallisuudella varmistetaan osaltaan kansallisen turvallisuuden, maanpuolustuksen, huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytykset. Geopoliittisen tilanteen muutos on entisestään korostanut kansallisen ja kansainvälisen yhteistyön merkitystä kyberturvallisuuden varmistamisessa. Erityisesti on kasvanut tarve viranomaisten ja elinkeinoelämän väliselle yhteistyölle, yhteiskunnan kriisinkestävyyden tukemiselle sekä vihamieliseen toimintaan vastaamiselle. Toimintaympäristöä määrittävät voimakkaasti digitalisaatio, uusien teknologioiden kehitys ja niihin liittyvä globaali kilpailu, keskinäisriippuvuudet ja väestön ikääntyminen. Yhteiskunnan perusrakenteiden ja -palvelujen kuten tieto- ja viestintäverkkojen ja niihin kytkeytyvän infrastruktuurin on toimittava kaikissa olosuhteissa.

Pääministeri Petteri Orpon hallitusohjelman mukaisesti kansallinen kyberturvallisuusstrategia on uudistettu vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuudella tarkoitetaan yleisesti toimia, joilla suojataan viestintä- ja tietojärjestelmät sekä muut sähköiset järjestelmät, niissä tallennettavat, käsiteltävät tai siirrettävät tiedot sekä niiden käyttäjät, hyödyntäjät ja muut asianosaiset henkilöt kyberuhkilta. Perinteisesti kyberturvallisuutta on tarkasteltu teknisemmästä näkökulmasta eikä niinkään valtion turvallisuuden kysymyksenä. Tässä strategiassa käsitellään kansallista kyberturvallisuutta, jolla tarkoitetaan niitä toimia, joiden seurauksena digitaalinen yhteiskunta kykenee varautumaan, tunnistamaan, torjumaan ja kestämään sähköisten ja verkotettujen järjestelmien häiriöitä ja niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin, toipumaan niistä sekä varmistamaan kansallisen turvallisuuden, maanpuolustuksen ja huoltovarmuuden toimintaedellytykset.

Kyberturvallisuusstrategian uudistamista on edellyttänyt myös Euroopan unionin kyberturvallisuusdirektiivi (NIS 2) ja sen kansallinen täytäntöönpano, jotka

asettavat velvoitteita myös jäsenvaltioiden kyberturvallisuusstrategioille. Suomen uudistettu kyberturvallisuusstrategia on järjestyksessään kolmas ja jatkaa edellisen kyberturvallisuusstrategian pohjalta laaditussa kehittämisohjelmassa esitellyn kyberturvallisuuden ekosysteemiajattelun edistämistä. Strategian valmistelussa on otettu huomioon muu aiheeseen liittyvä kansallinen strategia- ja selontekotyö, joista keskeisimpiä ovat seuraavat valtioneuvoston periaatepäätökset: Suomen kyberturvallisuuden kehittämisohjelma, Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (TITUKRI) ja Julkisen hallinnon digitaalinen turvallisuus sekä Valtioneuvoston selonteko Suomen digitaalisesta kompassista ja sen toimeenpanosuunnitelma. Lisäksi valmistelussa on huomioitu vuonna 2023 tehty selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa ja tästä työstä saadut huomiot ja kehittämiskohteet. Lisäksi on tehty yhteistyötä muiden hallitusohjelmaan sisältyvien, samanaikaisesti valmisteilla olevien hankkeiden kanssa.

Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035, ja sen strategiset tavoitteet sisältyvät neljän osa-alueen eli pilarin alle: I **Osaaminen, teknologia ja tutkimus-, kehitys- ja innovaatiotoiminta (TKI); II Varautuminen; III Yhteistoiminta; sekä IV Reagointi ja vastatoimet.**

Kansallisessa tavoitetilassa kyberturvallisuus on erottamaton osa Suomen kokonaisturvallisuutta.

Digitalisoitunut yhteiskuntamme on toimintavarma ja luotettava. Hyödynnämme teknologiset mahdollisuudet ja ymmärrämme niihin liittyvät uhkat kybertoimintaympäristölle ja yhteiskunnalle. Kehitämme osaamista laaja-alaisesti.

Suomi havaitsee, tunnistaa, torjuu ja kestää kyberhäiriötilanteita, toipuu niistä sekä toimii päättäväisesti vastatessaan häiriöihin.

Suomi edistää kyberturvallisuutta aktiivisesti ja määrätietoisesti tiiviin kansallisen ja kansainvälisen yhteistoiminnan ja tiedonvaihdon kautta.

Tavoitetilan saavuttamiseksi varmistetaan riittävät resurssit, ja niitä käytetään tehokkaasti.

Suomi käyttää tällä hetkellä vuosittain lähes 300 miljoonaa euroa valtionhallinnon kyberturvallisuuden varmistamiseen. Julkisten investointien lisäksi myös elinkeinoelämä investoi kyberturvallisuuteen varovaisen arvion mukaan noin kymmenkertaisesti verrattuna julkisiin investointeihin.

Strategian tavoitetilasta johdetut kehittämisehdotukset toimeenpannaan strategian hyväksymisen jälkeen laadittavan toimeenpanosuunnitelman mukaisesti.

Strategian liitteenä on kuvaus kansallisen kyberturvallisuuden yhteistoimintamallista. Strategian lopussa on määritelty tässä asiakirjassa käytetyt keskeiset termit.

Toimintaympäristön muutos

Suomen ja Euroopan turvallisuusympäristö on muuttunut voimakkaasti vuoden 2019 jälkeen, jolloin edellinen kansallinen kyberturvallisuusstrategia julkaistiin. Kiihtyvä digitalisaatio ja sitä entisestään vauhdittanut COVID19-pandemia, Venäjän hyökkäyssota Ukrainassa, maailmanlaajuisesti kiristynyt geopoliittinen tilanne ja Suomen Nato-jäsenyys sekä voimakkaasti kehittynyt kyberturvallisuuteen vaikuttava EU-sääntely korostavat kyberturvallisuuden merkitystä osana yhteiskunnan suojaamista.

Toimintaympäristön muutos haastaa kansainvälistä sääntöpohjaista järjestelmää

Uhkat ovat moninaistuneet ja kyberympäristöä hyödynnetään laajalti hybridivaikuttamisessa, rikollisuudessa, terrorismissa ja sodankäynnissä. Valtioiden välillä kybervaikuttamista käytetään myös poliittisten päämäärien ajamiseen. Valtiollinen kybervakoilu ei uhkaa ainoastaan ulko- ja turvallisuuspolitiikan valmistelua. Myös suomalaisten yritysten aineettoman pääoman suojaaminen laittomalta tiedonhankinnalta kybertoimintaympäristössä on tunnistettava yhtenä keskeisenä kehityskohteena talouden kilpailukyvyn säilyttämiseksi.

Suomeen kohdistuva vihamielinen kybertoiminta lisääntyy

On todennäköistä, että monenlainen vihamielinen kybertoiminta Suomea vastaan tulevaisuudessa jatkuu ja lisääntyy. Yhteiskunnan digitalisoituminen luo valtiollisille toimijoille uudenlaisia mahdollisuuksia mm. toteuttaa tiedustelua ja hyödyntää haavoittuvuuksia ilman suurta riskiä paljastumisesta.

Teknisten häiriöiden lisäksi myös vihamielisen toiminnan vaikutukset voivat yltää Suomeen myös valtion rajojen ulkopuolelta ja levitä ennalta-arvaamattomasti, vaikka Suomi ei olisikaan niiden pääasiallisena kohteena. Kun vihamielinen kybertoiminta lisääntyy ja kohdistuu yhä laajemmin myös hallituksiin, demokraattisiin instituutioihin, yrityselämään ja kansalaisiin, kasvaa myös tarve rajat ylittävälle yhteistyölle. Tämän vuoksi oman toimintaympäristön, tietojärjestelmien ja etenkin näiden välisten keskinäisriippuvuuksien tuntemus on entistä tärkeämpää.

Teknologinen murros lisää kaikkien vastuuta kyberturvallisuudesta

Teknologinen murros ja yhteiskuntien digitalisaatio kasvattavat hyökkäyspinta-alaa eli internetiin julkisesti näkyvien tietojärjestelmien ja palveluiden määrää, ja siten lisäävät yhteiskunnan haavoittuvuutta ja alttiutta kyberhäiriöille. Tietoverkossa toimivien laitteiden määrän odotetaan globaalisti kasvavan miljardeilla vuoteen 2030 mennessä. Teknologisia häiriötilanteita aiheuttavat esimerkiksi inhimilliset virheet ohjelmistokehityksessä ja niiden toimitusketjuissa sekä tarkoituksella luodut haavoittuvuudet kuten takaportit teknologiaan. Ne luovat rikollisille ja valtiollisille toimijoille pääsyn tietojärjestelmiin. Organisaatioiden ja kansalaisten vastuu ohjelmistojen päivityksissä on jatkossakin tärkeää. Sääntelyllä voidaan edistää turvallisen teknologian kehittymistä, mutta samaan aikaan kun turvallisuustoimenpiteitä tehdään, myös hyökkääjät kehittävät uusia tapoja niiden kiertämiseksi.

Kansainvälinen yhteistyö vahvistaa Suomen kyberturvallisuutta

Nato-jäsenyys vahvistaa Suomen turvallisuutta ja puolustusta, mutta asettaa myös uusia haasteita ja velvollisuuksia. Nato-jäsenyyden pelotevaikutus saattaa johtaa vihamielisen toiminnan painopisteen siirtymiseen entistä enemmän kybertoimintaympäristöön, jossa tekijän on helpompi kiistää osallisuutensa. Samaan aikaan teknologian kehittyminen, datalähtöisyys, kansainvälinen yhteistyö sekä kybertoiminnan geopoliittisten yhteyksien analysointi luovat kuitenkin entistä paremmat mahdollisuudet erityisesti valtiollisten toimijoiden attribuoimiseksi eli syyksilukemiseksi.

Suomi on merkittävä liittokunnan teknologisten ratkaisujen tuottaja kyberturvallisuudessa ja -puolustuksessa. Sotilaallisesti liittoutuneena maana Suomi edistää jatkossa Naton kyberpuolustuksen kehittämistä ja hyödyntää liittokunnan suorituskykyjä. Tätä tukee kyberpuolustuksen suunnitelmallinen kehittäminen ja ylläpitäminen osana kansallista kyberturvallisuutta. Suomen infrastruktuuria kehitetään osana liittokunnan infrastruktuuria, mikä vahvistaa yhteistyötä ja kyberpuolustusta. Useimmat Naton määrittämistä seitsemästä resilienssin perusvaatimuksesta asettavat vaatimuksia myös kansallisen kyberturvallisuuden kehittämiselle. Samalla Suomelle tärkeä EU pysyy yhä keskeisenä viitekehyksenä yhteiskunnan kybersietokyvyn ja resilienssin vahventamisessa.

Kyberturvallisuuteen ja -puolustukseen liittyvät kansalliset EU- ja Nato-kannat on tärkeää sovittaa yhteen. Naton ja EU:n kybertoimien koherenssi täydentää ja vahvistaa sekä kansainvälistä kyberturvallisuutta että Suomen kansallista kyberturvallisuutta. Nato-jäsenyyden rinnalla myös kahden- ja monenvälinen kansainvälinen yhteistyö kyberturvallisuudessa ja -puolustuksessa on laajentunut ja syventynyt. Samanmielisten maiden aloitteilla ja yhteistyöllä pyritään vastaamaan keskeisiin kyberuhkakuviin ja parantamaan kollektiivista kyberturvallisuutta. Myös YK:ssa ja erilaisissa alueellisissa järjestöissä tunnistetaan kyberturvallisuuden merkitys kansainväliselle turvallisuudelle.

Viime vuosina merkittävästi kehittynyt kyberturvallisuuteen vaikuttava EU-sääntely vahvistaa Suomen ja muiden EU-maiden kyberturvallisuutta. Sääntelyn kansallinen täytäntöönpano ja organisaatioiden toiminnan mukauttaminen sen mukaisesti haastavat tulevina vuosina niin viranomaisia kuin elinkeinoelämääkin. Nämä kasvattavat osaamis- ja koulutustarpeita ja kustannuksia riittävän suojan rakentamiseksi ja edellyttävät lisätoimenpiteitä kyberriskien hallitsemiseksi. Sääntelyllä luodaan edellytykset parantaa yhteiskunnan kriittisten toimijoiden kyberturvaa ja laitteiden ja ohjelmistojen sisäänrakennettua turvallisuutta. Samalla kehitetään viranomaisten toimintaa varautumisessa, häiriötilanteissa sekä reagoinnissa ja vastatoimissa.

Kansallista toimintamallia kehitetään

Kansallinen toimintamalli kyberturvallisuudessa on perustunut kykyyn parantaa jatkuvasti tietojärjestelmien ja organisaatioiden toimintaa kyberhyökkäyksien ja teknisten häiriöiden sietämiseksi ja niistä palautumiseksi. Toimintaympäristön ja kyberuhkien muutos haastaa aikaisemmat toimintatavat ja tarve varautumistoimien ja reagoinnin kehittämiselle sekä aiempaa proaktiivisemmille koordinoiduille vastatoimille on kasvanut. Kokonaisturvallisuuden malli mahdollistaa myös kyberturvallisuusalan varautumisen ja yhteistyön kehittämisen yhteiskunnan turvallisuusstrategian mukaisesti.

Kyberrikollisuuden kasvu koskettaa koko yhteiskuntaa

Vakavalla kyberrikollisuudella voidaan vaarantaa yhteiskunnan elintärkeiden toimintojen häiriötön toiminta, uhata kansallista turvallisuutta tai aiheuttaa muuten yhteiskuntaan laajasti vaikuttavia häiriöitä. Kyberrikollisuuden määrän

kasvu ja uhkien nopea kehittyminen koskettavat koko yhteiskuntaa. Kyberrikollisuus voi vaarantaa kansalaisten perusoikeuksia, heikentää luottamusta palveluihin ja aiheuttaa merkittäviä taloudellisia menetyksiä. Kyberrikollisuus kytkeytyy yhä enemmän myös järjestäytyneeseen rikollisuuteen ja valtiollisiin toimijoihin. Vihamielisessä toiminnassa valtiot hyödyntävät usein myös muun muassa erilaisia sijaistoimijoita kuten rikollisryhmiä ostopalveluina. Ostamalla rikollisilta palveluja vihamieliset valtiot saattavat pyrkiä vaikeuttamaan syyksilukemista tai esimerkiksi vaihtelemaan kyberoperaatioidensa intensiteettiä.

On huomionarvoista, että suuri osa yhteiskunnan toiminnan kannalta kriittisestä infrastruktuurista on yksityisen sektorin omistuksessa. Viranomaisten ja yksityisen sektorin välinen yhteistyö perustuu Suomessa sääntelyn, sopimusten ja palveluiden lisäksi luottamukseen ja vapaaehtoisuuteen, mikä on omiaan helpottamaan tiedonvaihtoa esimerkiksi erilaisista uhkista ja häiriöistä. Toimintaympäristön muutoksen vuoksi tiedonvaihto ja siihen käytettävät välineet sekä tilanneymmärryksen muodostaminen eivät nykyisellään ole riittäviä. Lainsäädännön, viranomaisten toimivaltuuksien ja yhteistyörakenteiden ja -verkostojen kehittäminen onkin välttämätöntä.

Toimitusketjujen turvallisuus korostuu

Vahvasti globalisoituneiden toimitusketjujen alttius häiriöille on tullut osaksi uhkaympäristöämme. Yhä keskinäisriippuvaisemmassa geotaloudessa esimerkiksi energia, raaka-aineet, logistiikka ja infrastruktuuri voidaan välineellistää geopoliittisiin tarkoituksiin myös kyberympäristössä. Palvelu- ja toimitusketjut ovat pidentyneet ja monimutkaistuneet, ja niitä on yhä vaikeampi hallita. Toimitusketjuhyökkäyksessä organisaation tietojärjestelmiin murtaudutaan sen ostamien palveluiden tai palvelutuottajien laitteiden tai ohjelmistojen kautta. Varsinaisen palvelun tai järjestelmän vaarantaminen tai siihen luvatta tunkeutuminen voi olla haasteellista, mutta vaikuttaminen toimitusketjuihin voi yhtä lailla johtaa hyökkääjän tavoittelemaan lopputulokseen. Yhteiskunnan toimintakyvyn kannalta kriittisten toimijoiden täytyykin varmistaa, että myös niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia.

Kybertoimintaympäristöön voivat aiheuttaa häiriöitä myös erilaiset fyysiset uhkat kuten sähkönsaannin häiriöt, tulvat, maanjäristykset, auringon aktiivinen toiminta tai muut luonnonmullistukset sekä inhimillisten virheiden aiheuttamat

vahingot. Nämä saattavat häiritä tietoliikenneyhteyksiä tai tietojärjestelmien toimintaa ja siten uhata kyberturvallisuutta.

Kyberturvallisuus mahdollistaa liiketoiminnan kasvun

Yhteiskunnan digitalisaatio luo myös merkittäviä kasvua tukevia liiketoiminta-mahdollisuuksia prosessien virtaviivaistamisesta uusien oppimismenetelmien kehittämiseen tai muihin tutkimus- ja kehitystyön avaamiin mahdollisuuksiin. Murrosteknologiat kuten tekoäly ja kvanttilaskenta mahdollistavat uudenlaisten ratkaisujen kehittämisen tämän päivän ja tulevaisuuden haasteisiin myös kyberympäristössä. Murrokselliset teknologiat ovat kuitenkin myös vihamielisten toimijoiden käytettävissä ja hyödynnettävissä, mikä haastaa nykyiset suojautumistavat. Toimintaympäristön muutoksen myötä kasvaa tarve uudenlaisille ja tehokkaille kyberturvallisuutta vahvistaville innovaatioille.

Valtiontalouden tämänhetkiset haasteet ja tietoturva-alan työvoimapula yhdistettynä EU:n lisääntyvään sääntelyyn vaikuttavat kyberturvallisuuden kehittämisen mahdollisuuksiin tulevaisuudessa. Julkisen sektorin kilpailukyky työnantajana on jäämässä yksityisen sektorin varjoon. Nämä asettavat haasteita Suomen kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman toteuttamiselle sekä kyberalan kansalliselle kasvulle.

Nykytila

Suomi on pitkälle digitalisoitunut yhteiskunta. Yhä suurempi osa ihmisten jokapäiväisestä toiminnasta ja julkisten palveluiden käytöstä tapahtuu digitaalisessa ympäristössä Suomen julkinen hallinto ja julkiset palvelut sijoittuvatkin digitalisaatiota koskevissa kansainvälisissä vertailuissa usein kärkisijoille. Suomessa on myös jatkuvasti vahvistettu digitaalisen toimintaympäristön turvallisuutta. Kyberturvallisuus on Suomessa kansainvälisten arviointien ja kansallisen itsearvioinnin perusteella verrattain hyvällä tasolla. Suomalaisten tekninen osaaminen, ymmärrys kyberturvallisuudesta ja maailmanlaajuisestikin katsottuna hyvin toimiva julkisen ja yksityisen sektorin yhteistyö myös kyberturvallisuuden alalla voidaan nähdä kansainvälisenä käyntikorttina ja potentiaalisena vientituotteena.

Suomessakin on koettu laajoja ihmisten arkeen vaikuttavia tietomurtoja, mutta olemme kuitenkin säästyneet yhteiskunnan toimintoja pitkäaikaisesti lamauttavien kyberhyökkäyksien vaikutuksilta. Samalla vihamielinen valtiollinen toiminta, kyberrikollisuus, palvelunestohyökkäykset, tietovuodot ja erilaiset haittaohjelmat sekä muut häiriötilanteet ovat yleistyneet myös Suomessa. Uhka uusille vakaville ja laajemmillekin vaikutuksille on olemassa.

Elinkeinoelämällä on merkittävä rooli kansallisen kyberturvallisuuden varmistamisessa.

Elinkeinoelämä vastaa Suomessa pitkälti digitaalisen infrastruktuurin ja sen palveluiden ylläpidosta ja kehityksestä. Kansalliset toimialakohtaiset tiedonvaihtoverkostot ovat elinvoimaisia. Näissä verkostoissa samalla sektorilla kilpailevat yritykset vaihtavat aktiivisesti kyberturvallisuuteen liittyvää tietoa sekä keskenään että julkisen sektorin kanssa.

Suomessakin on havaittavissa globaali trendi, joka jakaa yrityksiä ja toimialoja: organisaatiot jakautuvat yhä selkeämmin niihin, jotka ovat huolehtineet omasta kyberturvallisuudestaan ja niihin, jotka eivät ole. Keskinäisriippuvaisessa maailmassa tämä aiheuttaa riskejä koko yhteiskunnalle.

Yhteistyön merkitys korostuu

Suomi on luottamusyhteiskunta, jossa julkinen, yksityinen ja kolmas sektori tekevät tiiviistä yhteistyötä. Viranomaiset torjuvat yhteiskunnan kyberuhkia, ja niiden kanssa toimivat yritysten ja yhteisöjen kyberammattilaiset sekä kansalaisyhteiskunta omissa organisaatioissaan. On tärkeää, että viranomaistoiminta on luotettavaa ja palvelut turvataan kaikille – kansalaisia on kohdeltava yhdenvertaisesti ja varmistettava, että digitaaliseen teknologiaan ja palveluihin voivat luottaa sekä käyttäjät että palvelujen tarjoajat.

Positiiviset kokemukset yhteisestä vuorovaikutuksesta kasvattavat luottamusta. Kybertoimintaympäristössä tarvitaan luottamuksen lisäksi toimintavarmat digitaaliset menettelyt, joilla tunnistetaan kenen tai minkä kanssa ollaan tekemisissä: käyttäjän on tiedettävä, kenen palvelusta on kyse tai kuka on tiedon lähde. Varmuus viestinnän osapuolista sekä viestinnän oikeellisuudesta ja turvallisuudesta on tärkeää. Tekoälyn ja laajojen kielimallien mahdollistamat uudet huijaustavat ovat jo nyt uhka niin kyber- kuin informaatioympäristöllekin.

Kvanttiteknologian tuloon on varauduttava

Salausteknologioiden kansallisissa kyvykkyyksissä yhdistyvät kansallisen turvallisuuden ja maanpuolustuksen toimintaedellytysten turvaaminen, huoltovarmuuden ja tietopääoman varmistaminen sekä kansainvälinen yhteistyö. Suomessa on joillakin osa-alueilla vahvaa osaamista salausteknologioiden tuottamisessa ja hyödyntämisessä. Syvällisestä osaamisesta huolimatta osaajien lukumäärä kokonaisuudessaan on kuitenkin suppea, mikä vaikuttaa teknologioiden kehittämiseen ja käyttöönottoon.

Kvanttiteknologian nopea kehittyminen haastaa entisestään tämänhetkistä kansallista salauskyvykkyyttä. Suomi on jäänyt verrokkimaiden suhteen jälkeen salaustekniikoiden kansallisten ratkaisuiden kehittämisessä, eikä Suomessa ole velvoittavaa lainsäädäntöä hyväksyttyjen salausteknologioiden käytölle. Salausteknologioiden viranomaisarviointien ja -hyväksyntöjen hitaus ja kansallisen salausteknologisen laboratorion puuttuminen voivat pahimmillaan estää kehitystyötä.

Kyberturvallisuus huomioitava yhteiskunnan digitalisaatiokehityksessä

Suomen digitaalinen kompassi (digikompassi) on vuoteen 2030 ulottuva kansallinen strateginen etenemissuunnitelma Suomen digitalisaatiokehitykselle. Kompassin mukaan Suomi tavoittelee yritysten ja kansalaisten asiointitarpeen merkittävää keventymistä julkisen hallinnon yhtenäisen ja määrätietoisen uudistamisen avulla. Kompassissa on kuvattu tähän tarvittavat kyber- ja digiturvallisuuden kehittämisen keskeiset tavoitteet ja avaintulokset.

Viimeisin merkittävä hallinnollinen uudistus oli vuoden 2023 alussa toimintansa aloittaneiden itsehallinnollisten hyvinvointialueiden muodostaminen. Muutos vaikutti merkittävästi myös hyvinvointialueiden krittiseen infrastruktuuriin ja julkisiin palveluihin. Hyvinvointialueet vastaavat palveluistaan ja palveluihin liittyvästä kyberturvallisuudesta. Kuntakentässä kyberturvallisuuden on arvioitu toteutuneen keskimäärin muuta julkista hallintoa heikommin. Hyvinvointialueet ja kunnat tarvitsevat kyberturvallisuuden varmistamisessa nykyistä enemmän tukea, kuten keskitettyjä kyberturvallisuuspalveluja. Kyberuhkiin vastaamisen on toimittava saumattomasti eri kokoisten toimijoiden välillä ja ajallisesti portaattomasti niin valtakunnallisesti kuin alue- ja paikallistasollakin.

Kyberhäiriöiden aiheuttamat vahingot voivat olla sellaisia, ettei niitä pystytä täysin korvaamaan esimerkiksi tietojen tuhouduttua tai vuodettua pysyvästi. Jotkin pienet yritykset ovat jopa joutuneet lopettamaan toimintansa kyberturvallisuusriskien toteuduttua. Tämä korostaa entisestään riittävien resurssien kohdentamista kyberturvallisuuteen sekä yhteistyön ja yhteisten menettelytapojen tärkeyttä.

Yhteisen tilanneymmärryksen merkitys korostuu

Kyberympäristössä valtiollisten toimijoiden tiedonhankinnan ja vaikuttamisen kohteena ovat poliittisen päätöksenteon ohella myös viranomaiset, yhteiskunnan elintärkeät toiminnot, palvelut ja niitä tukeva kriittinen infrastruktuuri, yritysten ja tutkimuslaitosten tietopääoma sekä innovaatiot. Lisäksi vihamieliset valtiolliset toimijat voivat koordinoida toimiaan keskenään tehostaakseen päämääriään. Hyökkäyksellisten kyberoperaatioiden keskeisenä tarkoituksena on häiritä tai pyrkiä lamauttamaan yhteiskunnan kriittisen infrastruktuurin kuten energia-, vesi- tai terveydenhuollon toimintakykyä. Samalla tavoitteena on

yleensä pyrkiä vaikuttamaan valtionhallintoon ja poliittiseen päätöksentekokykyyn. Esimerkiksi Venäjän Ukrainassa käynnistämän hyökkäyssodan eräinä merkittävimpinä oppeina voidaan nähdä viranomaisten ja kyberalan yritysten kykyjen hyödyntämisen ja tiiviin yhteistyön keskeinen merkitys kyberturvallisuuden ja yhteiskunnan kriittisen infrastruktuurin toiminnan varmistamisessa valtiollisia uhkia vastaan.

Nykytilassa viranomaisilla on arvioitu olevan riittämättömät toimintaedellytykset tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Viranomaisten keskenään koordinoimassa ja analysoimassa tilannekuvassa ja tilanneymmärryksessä on edelleen kehitettävää. Myöskään julkisten palveluiden kyberturvallisuustietoja ei nykytilassa riittävästi jaeta strategia-, normi-, resurssi- ja informaatio-ohjauksen näkökulmista kaikkien julkisen hallinnon ja elinkeinoelämän toimijoiden välillä.

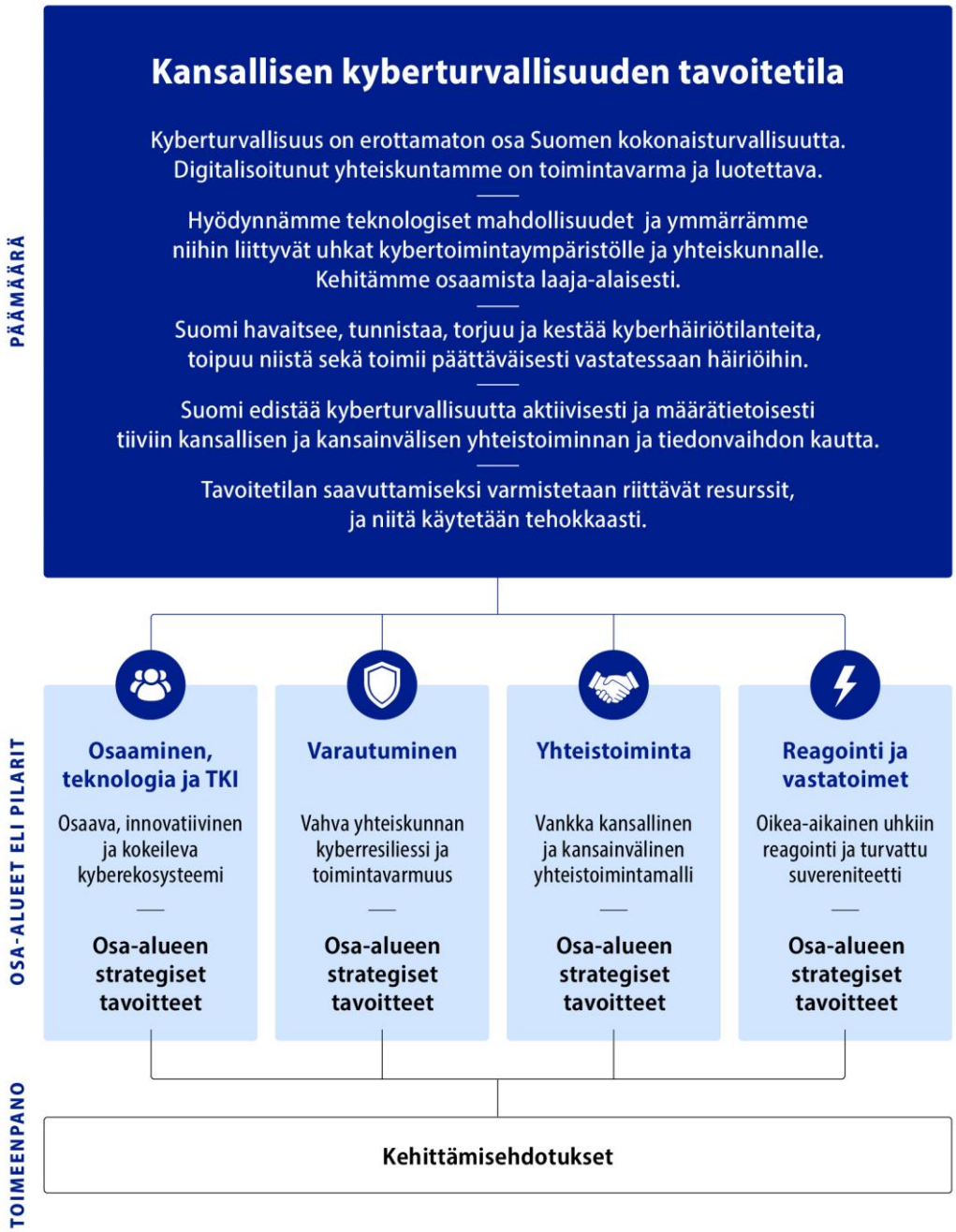
Kybertoimintaympäristön turvallisuutta vaarantava tapahtuma voi olla samanaikaisesti tietoturvauhka, rikos sekä kansallista turvallisuutta ja maanpuolustusta vaarantava uhka, jolla on ulko- ja turvallisuuspoliittisia vaikutuksia. Siksi tapahtuman selvitys on useimmiten samanaikaisesti usean viranomaisen vastuulla. Suomessa ei toistaiseksi ole kuitenkaan riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta kybertoimintaympäristössä, eikä säännöksissä ole otettu riittävästi huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa.

Viranomaiset, yritykset ja yhteisöt tuottavat nykytilassa tehtäviensä hoitamiseksi tilannekuvia eri tasoilla, eri käyttötarkoituksiin ja erilaisella sisällöllä. Hallinnonalat tuottavat omaa tilannekuvaansa myös valtionjohdon tarpeisiin. Kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja analysoinnista vastaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus yhteistyötahojen kanssa. Strategisella tasolla toimivan Kyberturvallisuuden koordinaatioryhmän tavoitteena on varmistaa, että ministeriöillä ja kyberturvallisuusviranomaisilla on yhdenmukainen yleistilannekuva yhteiskunnan kyberturvallisuuden tilasta. Valtion kyberturvallisuusjohtaja toimii valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa.

Kyberturvallisuuden ekosysteemin merkitys korostuu

Kestävän talouskasvun mahdollistamiseksi uhkien ja mahdollisuuksien tasapaino haetaan yhteistyössä kyberturvallisuuden ekosysteemin toimijoiden kanssa. Teknologian kehittämistä tuetaan erilaisia rahoitusmalleja hyödyntämällä. Tiivis vuoropuhelu ja yhteiskunnan eri toimijoiden välinen yhteistyö lisäävät luottamusta ja tukevat viranomaispäätösten lainmukaisuutta. Kansainvälisessä viitekehyksessä Suomi on turvallisuuden tuottaja, mikä parantaa EU:n ja Naton turvallisuutta kokonaisuutena.

Tavoitetila ja rakenne



Kuva 1: Kyberturvallisuusstrategian tavoitetila ja strategian rakenne

Pilarit ja niiden strategiset tavoitteet

Pilari I: Osaaminen, teknologia ja TKI

Osaava, innovatiivinen ja kokeileva kyberekosysteemi.

OSA-ALUEEN STRATEGISET TAVOITTEET:

- Kyberturvallisuusosaaminen kasvatuksen ja koulutuksen sekä yhteiskunnan ja työelämän kaikilla tasoilla on vahvaa.
- Kansalaiset tuntevat kyberturvallisuusvastuunsa.
- Suomi ottaa etulinjassa käyttöön murrosteknologioiden hyödyt ja edellyttää laitteisiin ja palveluihin sisäänrakennettua turvallisuutta.
- Kyberturvallisuuden tietopääoma on suojattu ja Suomi pyrkii kriittisen salausteknologian osalta omavaraisuuteen.
- Suomi varmistaa TKI-ympäristön houkuttelevuuden ja edistää kyberturvallisuusalan yritysten kilpailukykyä.
- EU:n ja Naton yhteistyö- ja rahoitusmahdollisuudet hyödynnetään.

Innovatiivinen ja kokeileva kyberekosysteemi

Kyberturvallisuuden ekosysteemi on kokonaisuus, joka käsittää laajasti yksityisen ja julkisen sektorin toimijat, yhteiskunnan eri tasojen osaamisen ja kyvykkyydet, toimijoiden välisen yhteistyön ja toimintatavat, vahvan kotimaisen kyberteollisuuden ja tutkimuslaitokset. Kyberekosysteemin päämääränä on tuottaa elinvoimaa ja kasvua, lisätä kyberturvallisuusalan työpaikkoja, luoda tarvittavaa osaamista ja vahvistaa digitaalisen yhteiskunnan kestävyyttä ja omavaraisuutta sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan. Toimiva ja kokeileva kyberekosysteemi lisää tuottavuutta ja tehokkuutta ja parantaa palveluiden laatua.

Kansalaiset tuntevat kyberturvallisuusvastuunsa

Kyberturvallisuusosaaminen kuuluu kansalaistaitoihin, ja jokainen voi omalla toiminnallaan myötävaikuttaa yhä turvallisemman kybertoimintaympäristön syntyyn. Kyberturvallista arkea voidaan tukea muun muassa vahvistamalla kansalaisten medialukutaitoa ja lisäämällä tietoisuutta hyvästä kyberhygieniasta. Kyberhygienia eli hyvien tietoturvakäytänteiden noudattaminen osana päivittäisiä rutiineja tuleekin nähdä luonnollisena osana jokaisen yksilön kansalaisvastuuta. Vastuullisesti kybertoimintaympäristössä toimivat kansalaiset lisäävät merkittävällä tavalla myös yhteisöjen ja organisaatioiden turvallisuutta.

Osaaminen on kaikilla tasoilla vahvaa

Yritysten vastuulliseen toimintaan kuuluu kehittää kyberturvallisia kyvykkyyksiä, tunnistaa uhkat, reagoida haitalliseen toimintaan ja ilmoittaa häiriöistä kybertoimintaympäristössä. Kouluissa opettajien valmiuksia kasvattaa oppilaita kriittiseen medialukutaitoon sekä tietoisuuteen kyberriskeistä on vahvistettava laajan yhteiskunnallisen resilienssin lujittamiseksi. Kokonaisuudessaan suomalainen kyberturvallisuusosaaminen varmistetaan vahvistamalla kyberturvallisuuden roolia laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla.

Innovatiivinen ja kokeileva kyberekosysteemi

Kyberuhkiin varautuminen, suojautumisen kehittäminen ja suomalaisten kyberturvallisuusalan yritysten kasvu ovat mahdollisia vain, jos osaavaa työvoimaa on saatavilla. Yhteiskunnallisesti vaikuttavalle ja innovatiiviselle tutkimus- ja kehitystoiminnalle luodaan perusta tukemalla alan perustutkimusta ja koulutusta. Julkisen hallinnon henkilöstön osaamista kyberturvallisuudesta ja siihen liittyvistä vastuista kehitetään riittävän osaamistason varmistamiseksi. Innovatiivista kybertoimintaympäristöä tukee aktiivinen tiedon, osaamisen ja tilanneymmärryksen jakaminen.

Kansalaiset, yritykset ja yhteisöt hyötyvät turvallisesta toimintaympäristöstä, jonka ennakoitavuus paranee osaamisen kehittymisen myötä. Samalla Suo-

men kiinnostavuus niin investointikohteena kuin osaamisen keskittymänä kasvaa. Suomi profiloituu myös kansainvälisesti kyberturvallisena maana, mikä parhaimmillaan voi olla Suomelle sekä kilpailuvaltti että vientituote.

Hyödynnämme murrokselliset teknologiat

Murrokselliset teknologiat kuten tekoäly ja kvanttiteknologia sekä uudet matkaviestinverkkosukupolvet tuovat mukanaan uudenlaisia ja vielä tuntematto-miakin kyberturvallisuusuhkia. Lisäksi näiden teknologioiden yhteisvaikutukset ovat erittäin vaikeasti ennakoitavissa. Näihin haasteisiin vastaaminen edellyttää syvää ja kattavaa teknologista osaamista ja yhteiskunnallisten muutosten jatkuvaa seurantaa ja arviointia.

Suomen tavoitteena on ottaa rohkeasti ensimmäisten joukossa käyttöön murrosteknologiat kyberturvallisuuden varmistamisen tukena. Käyttöön otettavien teknologioiden laajamittainen hyödyntäminen edellyttää, että teknologiat ja ohjelmistot suunnitellaan jo lähtökohtaisesti turvallisiksi ja niiden turvallisuudesta huolehditaan säännöllisesti koko niiden elinkaaren ajan. Tämä sisäänrakennetun turvallisuuden periaate on tärkeää huomioida kaikessa teknologioita koskevassa kansallisessa säädösvalmistelussa sekä EU-ennakkovaikuttamisessa. EU:ssa ja kansainvälisessä yhteistyössä tehtävä yhteentoimivuus- ja standardointityö on keskeisessä roolissa kyberturvallisuuden ja uusien teknologioiden turvallisuuden varmistamisessa. Suomi on aktiivinen toimija kyberturvallisuuden standardien kehittämisessä.

Yritysten kilpailukykyä edistetään

Vahva kotimainen kyberturvallisuusuusalan yritystoiminta on keskeistä toimivan kyberturvallisuuden ekosysteemin kehittämiseksi ja ylläpitämiseksi. Kyberturvallisuuden tutkimus-, kehitys- ja innovaatiotoiminnan (TKI) panostusten suunnittelussa hyödynnetään EU:n ja Naton tarjoamat kansainväliset yhteistyö- ja rahoitusmahdollisuudet ja panostetaan niissä tarvittaviin prosesseihin, resursseihin ja ennakoivaan yhteistyöhön. Osallistuminen kansainvälisiin rahoitusohjelmiin kuten Naton DIANA innovaatioaloitteeseen ja EU:n Horisontti Eurooppa ja Digitaalinen Eurooppa (DEP) -puiteohjelmiin lisäävät Suomen tunnettuutta korkean teknologian ja kyberturvallisuuden osaajana ja parantavat suomalaisten yritysten liiketoimintamahdollisuuksia kansallisesti ja kan-

sainvälisesti. Lisäksi voidaan hyödyntää Euroopan avaruusjärjestö ESA:n yhteistyö- ja rahoitusmahdollisuuksia kyberturvallisuuden huomioimiseksi avaruusteknologian nopeassa kehityksessä.

Tavoitteena on, että Suomi pystyy tuottamaan globaalisti kilpailukykyisiä kyberturvallisuusalan teknologisia ratkaisuja kasvun mahdollistamiseksi. Suomen TKI-ympäristön tulee kannustaa ja tukea kyberturvallisuutta tukevien ratkaisujen kehittämistä ja hyödyntämistä sekä niitä kaupallistavien yritysten kansainvälistä kilpailukykyä. Näin edistetään sekä Suomen kyberturvallisuusalan että laajemmin turvallisen TKI- ja liiketoimintaympäristön houkuttelevuutta suomalaisille ja ulkomaisille osaajille, yrityksille ja investoinneille.

Kyberturvallisuuden tietopääoma on suojattu

On tärkeää, että julkisen ja yksityisen sektorin kriittinen tietopääoma tunnistetaan ja suojataan. Kyberturvallisuuden tietopääomaan lukeutuvat esimerkiksi palvelut, tietojärjestelmät, osaaminen, prosessit, patentit, tavaramerkit ja kumppanuudet. Eri toimijoiden aktiivisella tiedonvaihdolla ja tietoon pohjautuvalla päätöksenteolla voidaan tehokkaasti päättää tarvittavista kyberturvallisuuden kehittämistoimenpiteistä, joilla tietopääomaa voidaan suojata yhteiskunnan toimivuuden varmistamiseksi.

Pyrimme salausteknologiseen omavaraisuuteen

Kansallisesti merkittävien tietovarantojen käytettävyys, saatavuus ja luotettavuus kaikissa tilanteissa on tärkeä osa kyberresilienssiä. Kvanttiteknologian kehittyminen uhkaa murtaa nykyaikaiset salausalgoritmit ja vaarantaa kansallisesti suojattavat tietoaineistot. Suomen yhtenä strategisena tavoitteena on olla kriittisten salausteknologioiden osalta omavarainen ja kvanttiuhkaan varautunut valtio 2030-luvun alkuun mennessä. Tämä edellyttää, että kansallisesti kriittisiä salausteknologioita kuten kvantinkestäviä salausratkaisuja kehitetään kotimaassa ja kokonaisvaltaista salausteknologista kyvykkyyttä vahvistetaan muun muassa tuotannon, tutkimuksen, laskennan, takaisinmallinnuksen sekä organisoitumisen osa-alueilla. Kvantinkestävän salauksen kansallisessa kehittämistyössä huomioidaan myös EU:n yhteiset politiikkatoimet ja sääntely sekä Naton asettamat vaatimukset.

Pilari II: Varautuminen

Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus

OSA-ALUEEN STRATEGISET TAVOITTEET:

- Kriittinen infrastruktuuri, yhteiskunnan elintärkeät toiminnot, julkiset palvelut sekä huoltovarmuuskriittiset toimijat ovat kybersietoisia.
- Kansalaiset, yritykset, yhteisöt ja viranomaiset ovat yhdessä varautuneet kyberhäiriöihin.
- Suomi edistää kyberturvallisuuden varautumismalliaan vientituotteena.
- Ennalta ehkäistään kyberrikollisuutta.
- Varautuminen perustuu kokonaisvaltaiseen yhteiseen tilanneymmärrykseen ja pitkäjänteiseen resursointiin.
- Kyberharjoitusten ympäristöjä ja käytäntöjä kehitetään ja eri toimialojen välistä harjoittelua lisätään.

Voimme luottaa yhteiskunnan toimivuuteen

Suomi varautuu kyberuhkiin ennakoivasti. On tärkeää, että yhteiskunnan toimivuuteen voidaan luottaa kaikissa oloissa. Riittävä ja oikea-aikainen varautuminen kyberhäiriöihin on digitaalisen yhteiskunnan toimintavarmuuden kivijalka. Ennakoinnilla ja pitkäjänteisellä varautumisella edistetään yhteiskunnan palveluiden saatavuutta ja häiriönsietokykyä kaikissa olosuhteissa. Keskeistä on varmistaa yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin, tietovarantojen, julkisten palvelujen sekä huoltovarmuuskriittisten toimijoiden toimivuus ja häiriönsietokyky. Varautumisen osana tehtävän huoltovarmuustyön tavoitteena on turvata kriittisen infrastruktuurin, tuotannon ja palveluiden toimivuus siten, että ne kykenevät täyttämään väestön, talouselämän ja maanpuolustuksen välttämättömimmät perustarpeet kaikissa olosuhteissa myös kybertoimintaympäristössä.

Yritykset ovat kiinnostuneita kehittämään varautumistaan liiketoiminnallisista lähtökohdista. Julkisen hallinnon on huomioitava toimintaympäristön muutokset asettaessaan yrityksille varautumisvaatimuksia turvallisuuden näkökulmasta ja tukiessaan yritysten varautumista. Toimivuuden varmistamisessa ja häiriönsietokyvyn kehittämisessä tärkeää on erityisesti kyberharjoittelun kehittäminen ja ulottaminen entistä laajemmalle huomioiden palvelu- ja toimitusketjujen kyberturvallisuus sekä erilaiset keskinäisriippuvuudet. Turvalliset tietojärjestelmät luovat perustaa kybersietoiselle yhteiskunnalle, ja niiden hankintaan, kehittämiseen ja ylläpitoon on kiinnitettävä huomiota niin julkisella kuin yksityisellä sektorilla.

Julkiset palvelut ovat turvallisia

On tärkeää, että julkiset palvelut ovat turvallisia käyttää ja kansalaiset ja yhteisöt luottavat niiden toimintavarmuuteen. Julkisten palveluiden kyberturvallisuutta johdetaan ennakoivasti tilannetietoon sekä uhka- ja riskiarvioon perustuen. Julkisten palveluiden kyberturvallisuuden tasosta ja puutteista tarvitaan kattavaa ja luotettavaa tilannekuvaa riskien hallitsemiseksi ja kyberturvallisuuden vahvistamiseksi. Kyberturvallisuuden vaikuttavuutta, hyötyjä ja kustannuksia seurataan ja painopisteitä priorisoidaan. Julkisten palveluiden teknologioilta ja palvelutuotannolta edellytetään kyberturvallisuuden vaatimustenmukaisuutta koko elinkaaren ajan. Julkisten palveluiden vaatimustenmukaisuuden arviointia ja hyväksyntää sekä arviointikriteeristöjä on kehitettävä ja selkeytettävä ja siihen velvoitettava entistä paremmin. Lisäksi automaattista teknistä seurantaa ja valvontaa on tärkeää kehittää ja siihen velvoittaa. On varmistettava, että palvelut priorisoidaan turvallisuustilanteen mukaisesti, potentiaalisiin häiriötilanteisiin varaudutaan ja häiriöiden vaikutukset viranomaisten ja yhteiskunnan toimintaan kyetään minimoimaan.

Varautumistyötä tehdään yhteistyössä

Kokonaisturvallisuuden mallin mukaisesti viranomaiset tekevät kyberturvallisuuden varautumistyötä tiiviissä yhteistyössä yritysten, järjestöjen ja kansalaisten kanssa. Kyberuhkien tunnistamisen ja niihin varautumisen on pohjauduttava systemaattiseen tiedolla johtamiseen ja yhteiseen tilanneymmärrykseen, jonka perustan muodostavat ennakointi, tiedustelu ja tutkimustiedon hyödyntäminen. Tiedustelu tukee varautumista ja ennakointia hankkimalla ja jakamalla tiedustelutietoa sekä vihamielisten kybertoimijoiden suorituskyvyistä

että kyberhyökkäysten tavoitteista ja kohteista kansallisen turvallisuuden suojaamiseksi.

Suomi edistää yhteistyötä ja vuoropuhelua korostavaa varautumisen toimintamallia myös EU- ja Nato-yhteistyössä ja edesauttaa kyberturvallisuuden varautumismallin ja parhaiden käytäntöjen soveltamista myös kumppanimaissa. Yhteiskunnan eri toimijoiden keskinäinen luottamus sekä luottamus julkisiin instituutioihin ja niiden palveluihin rakentavat vahvaa kansallista resilienssiä. Luottamus on myös onnistuneen kansallisen kyberturvallisuustyön, varautumisen, yhteisesti jaetun tilanneymmärryksen ja oikea-aikaisen reagoinnin edellytys.

Kyberrikollisuutta ehkäistään

Kyberrikollisuuden ennalta estäminen edellyttää koko yhteiskunnan kaikkien toimijoiden tavoitteellisia ja aktiivisia toimia. Kyberrikostorjunnan painopiste on mahdollisimman varhaisessa ennalta estämisessä ja uhkien tunnistamisessa. Tämän vuoksi kansalaisille tarjottavat palvelut on suunniteltava, toteutettava ja ylläpidettävä siten, että kyberrikollisten hyökkäyspinta-ala pienenee. On tärkeää, että käyttäjät voivat luottaa palvelujen turvallisuuteen ja heillä on riittävä osaaminen tunnistaa väärennetyt palvelut ja huijaukset. Kyberrikollisuuteen liittyvistä uhkista on viestittävä ymmärrettävästi ja ohjeistettava ja neuvottava oikeista tavoista toimia. Kansalaisiin ja yrityksiin kohdistuvien rikosten varhainen ilmoittaminen viranomaisille mahdollistaa samankaltaisten rikosten ennalta estämisen ja laajempien vahinkojen syntymisen. Kyberrikosten ennalta estämistä on tuettava lainsäädännöllä, joka mahdollistaa tiedon jakamisen viranomaisten ja yritysten kesken.

Varautuminen perustuu pitkäjänteiseen resursointiin

Kattavan uhka- ja riskiarvion ja lakisääteisten velvoitteiden pohjalta tunnistettujen tarpeiden edellyttämät kyberturvallisuusresurssit sisällytetään julkisen hallinnon, yritysten ja yhteisöjen toiminta- ja taloussuunnitelmiin. Kyberturvallisuuden resurssien tehokas käyttäminen edellyttää, että kyberturvallisuustehtävät suunnitellaan ja toteutetaan tehokkaasti laajassa kansallisessa ja kansainvälisessä yhteistyössä valtionhallinnon, yritysten ja yhteisöjen sekä alue- ja paikallishallinnon kanssa. Valtioneuvostossa yhteisiä strategisen tason kyber-

turvallisuuden johtamisen resursseja on keskitetty valtion kyberturvallisuusjohtajan toimistoon. Muita keskitettyjä kyberturvallisuustehtäviä hoitavia viranomaisia resursoidaan niille säädettyjen tehtävien mukaisesti. Lisäksi alue- ja paikallishallinnossa on edistettävä yhteisten kyberturvallisuustehtävien keskittämistä päällekkäisen työn välttämiseksi ja resurssien käytön tehostamiseksi.

Keskitettyä julkisen talouden suunnitelmaan sisällytettyä hankerahoitusta on mahdollista kohdentaa uusien kyberturvallisuustoimintojen, -tehtävien tai -palvelujen käynnistämiseksi. Viranomaisen mahdollisuus tarjota kyberturvallisuuspalvelu asiakkaille maksullisena palveluna on selvitettävä aina uutta palvelua käyttöönotettaessa.

Kyberturvallisuustoiminnan tuottavuutta ja vaikuttavuutta on tärkeää seurata ja kehittää aktiivisesti sekä yhteiskunnan tasolla että jokaisessa organisaatiossa. Rahoituksen käyttöä suunnitellaan, seurataan ja valvotaan yhteisen resurssitilannekuvan avulla osana julkisen talouden suunnittelua. Sen keräämisen ja ylläpitämisen tarvitsema tiedonvaihdon sääntely ja toimintamallit on toteutettava.

Harjoitustoimintaa lisätään

Kansallisten kyberharjoitusten avulla simuloidaan erilaisia kyberhäiriöitä eli luodaan olosuhteet, joissa kyberhäiriöiden vaikutuksia ja niistä toipumista voidaan testata ja harjoitella. Harjoitukset kehittävät osaamista ja ylläpitävät yksilöiden ja organisaatioiden valmiutta ja kykyä varautua erilaisiin kyberhäiriöihin ja uhkiin. Aktiivinen harjoittelu normaalioloissa vahvistaa osaamista kaikissa tilanteissa. Lisäksi organisaatioita kannustetaan kehittämään pitkäjänteisesti omaa harjoitustoimintaa, tarvittaessa viranomaisten tuella.

Kyberharjoitustoiminnalla rakennetaan koko yhteiskunnan vahvaa kyberresilienssiä. Kyberharjoitusten ympäristöjä ja käytäntöjä on tärkeää kehittää ja lisätä erityisesti eri toimialojen välistä harjoittelua. Kansainväliset kyberharjoitukset tukevat rajat ylittäviin kyberuhkiin ja häiriöihin varautumista, päätöksentekoa ja vastaamista. Suomelle on tärkeää osallistua kansainvälisiin kyberharjoituksiin, vaikuttaa niissä aktiivisesti sekä kehittää ja tarjota kyberharjoitusosaamista kansainvälisille kumppanimaille.

Avaruuspalveluiden avulla parannetaan maanpäällisten järjestelmien resilienssiä

Avaruuspalveluja voidaan hyödyntää kybertilannekuvan tuottamisessa. On tärkeää, että tarvittavat avaruuspalvelut kuten aika- ja paikkatiedot, tietoliikenne ja kaukokartoitus ovat yhteiskunnan toimijoiden käytettävissä. Avaruusjärjestelmien kyberturvallisuutta seurataan osana avaruustilannekuvaa. Avaruusjärjestelmien kyberturvallisuus huomioidaan avaruuslupaehdoissa ja järjestelmien elinkaarenhallinnassa. Potentiaalisiin häiriötilanteisiin sekä niistä toipumiseen varaudutaan ja häiriöiden vaikutukset viranomaisten ja yhteiskunnan toimintaan minimoidaan vaihtoehtoisten toimintamallien ja varajärjestelyjen avulla.

Pilari III: Yhteistoiminta

Vankka kansallinen ja kansainvälinen yhteistoimintamalli

OSA-ALUEEN STRATEGISET TAVOITTEET:

- Suomi vaikuttaa ja osallistuu aktiivisesti kybertoimintaympäristöä koskevaan normatiiviseen kansainväliseen yhteistyöhön kuten kyberdiplomatiaan ja sääntelyn kehittämiseen.
- Suomi osallistuu aktiivisesti ja vaikuttaa ennakoivasti kyberturvallisuuden, kyberrikostorjunnan ja kyberpuolustuksen yhteistoimintaan ja tukee kumppanimaita.
- EU:n ja Naton tuomat mahdollisuudet kyberturvallisuudelle varmistetaan.
- Julkinen ja yksityinen sektori kehittävät tiiviimpää ja luottamusta vahvistavaa yhteistoimintamallia.
- Viranomaisten yhteistoiminnassa tarvittava tieto liikkuu sujuvasti ja saumattomasti.
- Julkinen sektori yhdessä yksityisen sektorin kanssa kehittää ja tarjoaa keskitettyjä kyberturvallisuuspalveluja.

Ulko- ja turvallisuuspoliittinen selonteko, puolustusselonteko, sisäisen turvallisuuden selonteko sekä kyberturvallisuusstrategia asettavat kansalliset pitkän aikavälin tavoitteet kyberuhkiin vastaamiseksi. Niissä huomioidaan Naton sekä EU:n kyberturvallisuuden ja -puolustuksen päämäärät ja velvoitteet. Kansallisella kyberpolitiikalla on tarkennettu näitä tavoitteita. Kyberdiplomatialle, kyberturvallisuudelle ja kyberpuolustukselle asetettujen tavoitteiden toimeenpanoa ja tuloksellisuuden seurantaa yhteensovitetaan strategisella tasolla laajassa yhteistyössä.

Suomi vaikuttaa ja osallistuu aktiiviseen yhteistyöhön

Suomi jatkaa tiivistä osallistumista kybertoimintaympäristöä koskevaan normatiiviseen kansainväliseen yhteistyöhön ja näkemysten vaihtoon siitä, miten

kansainvälinen oikeus tietyissä kysymyksissä sääntelee valtioiden informaatio- ja kommunikaatioteknologioiden käyttöä. Suomi päivittää omaa kantaansa kansainvälisen lain soveltamisesta kybertoimintaympäristössä. Suomi vaikuttaa kyberturvallisuutta, kyberrikollisuutta ja kyberpuolustusta koskevaan päätöksentekoon niin YK:ssa, EU:ssa, Natossa kuin muissakin keskeisissä kansainvälisissä järjestöissä ja verkostoissa. Suomi on luotettava toimija euroatlanttisessa yhteistyössä ja turvallisuuden tuottaja ja vastuullinen valtiotoimija myös kyberympäristön osalta. Kyberyhteistyötä tehdään laajasti ja syvennetään erityisesti keskeisten samanmielisten EU-maiden, Pohjoismaiden sekä euroatlanttisten ja myös joidenkin indopasifisen alueen maiden kanssa yhteisten arvojen pohjalta.

Suomi edistää monenvälistä kyberdiplomatiaa tavoitteenaan avoimen, vapaan, turvallisen ja vakaan kyberympäristön luominen ja säilyttäminen. EU:n kyberdiplomatian työkalupakki antaa välineitä kyberuhkiin vastaamiseen sekä niiden ehkäisemiseen. Suomi suojautuu kolmansien maiden luomilta potentiaalisilta kyberuhkilta kyberpuolustuksen, kyberturvallisuuden ja kyberdiplomatian keinoin. Kyberdiplomatian keinoja ovat monenkeskisen järjestelmän vahvistaminen kansainvälisen oikeuden pohjalta, kumppanuudet, vuoropuhelu ja luottamusta lisäävät toimet. EU:n yhteinen kyberpolitiikka ja kyberturvallisuuteen vaikuttava sääntely luovat kehikon myös Suomen kyberturvallisuuden lainsäädännölle. Uuden sääntelyn toimeenpanoon, sen vaikutusten arviointiin ja viranomaisten riittävään resursointiin on kiinnitettävä huomiota.

Suomi tukee kumppanimaita

Suomi vaikuttaa aktiivisesti EU:n kyberturvallisuuspolitiikan- ja sääntelyn kehittämiseen ja vie omaa kansallista kokonaisturvallisuuteen ja ennakolliseen varautumiseen pohjautuvaa malliaan unioniin ja muihin jäsenmaihin. EU:ssa viime vuosina luotujen uusien kyberturvallisuustoimintojen ja -elimien vahvistaminen ja vakiinnuttaminen ovat tärkeä osa unionin kyberturvallisuuden vahvistamista ja kansallisen tilannekuvan rakentamista. Tavoitteena on edesauttaa EU:n yhteisen tahtotilan kehittämistä kuten häiriösietoisuutta kyberympäristössä. Keskeisenä tuloksena on strategisen autonomian saavuttaminen ja avoimen talouden säilyttäminen.

Naton jäsenenä Suomi on kybersuorituskykyjen kehitystyön ytimessä ja on merkittävä liittokunnan ratkaisujen tuottaja kyberturvallisuudessa ja kyberpuolustuksessa. Naton ja EU:n kybertoimet täydentävät toisiaan ja toimien yhteensovittaminen vahvistaa niiden ja Suomen kansallista kyberturvallisuutta. Kyberturvallisuuden ja -puolustuksen kahden ja monenvälinen yhteistyö on nyt ja tulevaisuudessa operatiivisen toiminnan keskeisin yhteistyömuoto.

Yhteinen tilanneymmärrys toiminnan perustana

Tiivis yhteistyö on keskeistä kyberturvallisuuden tavoitetilan saavuttamiseksi. Yhteinen tilanneymmärrys mahdollistaa viranomaisten, yritysten ja yhteisöjen välisen tehokkaan ja luotettavan yhteistoiminnan kybertoimintaympäristössä. Organisaatioiden eri tasojen sekä viranomaisten ja yksityisen sektorin välinen kehittynyt yhteistoiminta mahdollistuu vain matalan kynnyksen jatkuvan monenvälisen tiedonvaihdon sekä ratkaisuhakuisen yhteistoimintakulttuurin muodostumisen kautta. Tämä lisää luottamusta ja tukee sektorivastuiden toteuttamista.

Kyberturvallisuuden yhteistoiminnalle tuovat haasteita sääntelyn ja tehtävien hajautuminen usealle eri toimijalle sekä yhteistoiminnan erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute. Kybertoimintaympäristön havainnoinnin osalta on tarve systematisoida tietojen kokoamista siten, että saavutetaan laajempi tilanneymmärrys Suomeen kohdistuvista vakavista kyberuhkista. Tiedonvaihdon laajentaminen edellyttää lainsäädäntöön kirjattuja, selkeiden edellytyksien ja osallistuvien tahojen määrittelyä ja toisaalta nykyisten rajoitteiden perusteiden arviointia. Tiedonvaihtoa on kehitettävä myös nykyisiä laintulkintoja yhdenmukaistamalla ja tarkentamalla sekä yhteisiä toimintamalleja muokkaamalla.

Yhteistyön ja tiedonvaihdon kehittämisen painopiste on valtiollisten sekä yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvien vakavien kyberuhkien ennalta estämisessä ja torjunnassa sekä tähän liittyvien toimintaedellytysten luomisessa. Tiedonvaihdon tulee olla riittävää, luottamusta ylläpitävää, tasapainoista ja käyttötarkoitussidonnaista perustuen tiedon luovuttamisen ja saamisen oikeuteen sekä intressiin ja oikeuteen jakaa tietoa sitä tarvitsevien kesken. Tiedon tuottajan tai haltijan tulisi pystyä tunnistamaan ja jakamaan tietoa oma-aloitteisesti tilanneymmärryksen perusteella. Tilannetietoja vakavista kyberuhkista on voitava jakaa entistä tehokkaammin

huoltovarmuuskriittisille yrityksille, kunnille, kuntaomisteisille palveluntarjoajille sekä hyvinvointialueille tarkoituksenmukaisella tavalla jakelurajoitteet huomioiden. Korkeasti turvallisuusluokitellun tiedon jakaminen edellyttää siihen soveltuvien järjestelmien kehittämistä ja käyttöönottoa.

Selvityksessä viranomaisten toimintaedellytyksistä kyberturvallisuudessa on tunnistettu kehittämistoimenpiteitä, joiden tavoitteena on parantaa viranomaisten toimintaedellytyksiä, suojata kansallista kyberturvallisuutta, torjua vakavaa kyberrikollisuutta ja kehittää kyberpuolustusta ja tiedustelua vastaamaan kehittyvän kyberuhkaympäristön tuomiin vaatimuksiin. Yhteistoimintaa ja viranomaisprosesseja, tilannekuvan muodostamista, tiedonvaihtoa ja tiedonhankintaa sekä vakaviin kyberuhkiin reagoimista koskevat kehittämisehdotukset on toteutettava tunnistettua uhkaympäristöä vastaavaksi. Tiivis viranomaisyhteistyö, tilannekuvan ja -ymmärryksen muodostaminen sekä tiedonhankinnan edellytysten varmistaminen ovat keskeisiä tavoitetilan saavuttamiseksi. Esimerkiksi julkisten palvelujen osalta tarvitaan nykyistä parempia keinoja ja edellytyksiä kerätä, analysoida ja jakaa tietoa kyberturvallisuuden ja kyberresilienssin tasosta.

Viranomaisten yhteistoiminta on sujuvaa ja saumatonta

Operatiivisen yhteistyön toimeenpanoa, vastuita sekä vakaviin kyberuhkiin ja -häiriöihin varautumista ja niihin vastaamista koordinoidaan virastotason yhteistyörakenteessa, jonka muodostavat Liikenne- ja viestintävirasto Traficom, keskusrikospoliisi, Puolustusvoimat sekä suojelupoliisi. Koordinaatio perustuu yhteiseen jaettuun tilanneymmärrykseen. Tehtävien ja kyberuhkiin vastaamisen toimeenpano tapahtuu aikaisempaa tiiviimmässä ja osallistavammassa viranomaisten yhteistoiminnassa taktisella ja teknisellä tasolla.

Kyberturvallisuuden toimintakulttuuria tulee uudistaa kokonaisturvallisuuden mallin mukaisesti vahvistamalla kansainvälistä sekä kansallista valtionhallinnon, aluehallinnon, paikallishallinnon ja yhteisöjen kyberturvallisuuden yhteistoimintaa. Tämän saavuttamiseksi hyödynnetään yhä laajemmin kansainvälisten kumppanien toimintamalleja ja kyberturvallisuuden ratkaisuja tuottavia teknologioita. Uusina toimijoina hyvinvointialueiden on tärkeää edistää kyberturvallisuuskulttuuria ja -osaamista yhteistyössä muiden toimijoiden kanssa.

Keskitetyt kyberturvallisuuspalvelut

Kansainvälisten kyberturvallisuushankkeiden keskinäistä koordinaatiota on tärkeää parantaa. Keskitettyjen kyberturvallisuuspalvelujen kehittämisen ja käytön koordinaatiota edistetään. Palvelujen käyttöastetta nostamalla voidaan tehostaa toimintaa ja suorituskykyjen käyttöä sekä välttää päällekkäisyyksiä. Liikenne- ja viestintävirasto Traficom, Digi- ja väestötietovirasto, muut valtionhallinnon toimijat sekä hyvinvointialueiden ja kuntien omistamat yritykset yhdessä yksityisen sektorin kanssa tarjoavat keskitettyjä kyberturvallisuuspalveluja. Niitä käyttävät valtionhallinto, alue- ja paikallishallinto ja hyvinvointialueet sekä soveltuvin osin yritykset, yhteisöt, korkeakoulut ja tutkimuslaitokset. Keskitettyjen palvelujen on oltava toimintavarmoja, kustannustehokkaita, suorituskykyisiä ja käyttäjäystävällisiä. Yhteistyön tavoitteena on tuottaa yhteiseen käyttöön tarkoitettuja aineistoja, koulutuksia sekä tietoa ja palveluja.

Pilari IV: Reagointi ja vastatoimet

Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti

OSA-ALUEEN STRATEGISET TAVOITTEET:

- Julkisen ja yksityisen sektorin toimijoilla on selkeät roolit ja toimivaltuudet sekä kyky reagoida oikea-aikaisesti ja oikealla tavalla kyberhäiriöihin.
- Reagointi ja vastatoimet perustuvat kattavaan tilanneymmärrykseen.
- Torjutaan järjestäytynyttä ja vakavaa kyberrikollisuutta.
- Kyberpuolustusdoktriini antaa kansalliset toimintaperiaatteet valtiollisiin ja valtion turvallisuutta vaarantaviin uhkiin vastaamiseksi.

Valtion suvereniteetin loukkaus on kansainvälisen oikeuden vastainen teko. Tämä koskee myös kyberympäristöä. Suomen lähtökohta on, että kansainvälinen oikeus ja vastuullisen valtiokäyttäytymisen normit luovat olennaiset puitteet valtioiden toiminnalle kyberympäristössä.

Mahdollisuudet ja kyvyt vastata kyberuhkiin varmistetaan

Kyberuhkiin on tärkeää vastata kokonaisvaltaisesti, pitkäjänteisesti ja oikea-aikaisesti. Tämä edellyttää sitä, että kyberturvallisuutta vahvistavia ja kyberuhkia ennaltaehkäiseviä toimenpiteitä hyödynnetään kattavasti ja määrätietoisesti. Suomen on turvattava valtiollinen suvereniteettinsa myös kybertoimintaympäristössä. Suomi vastaa geopoliittisen tilanteen kyberympäristölle asettamiin haasteisiin aktiivisilla kyberdiplomatian, -puolustuksen ja -turvallisuuden toimilla itsenäisesti ja osana monenvälistä toimintaa.

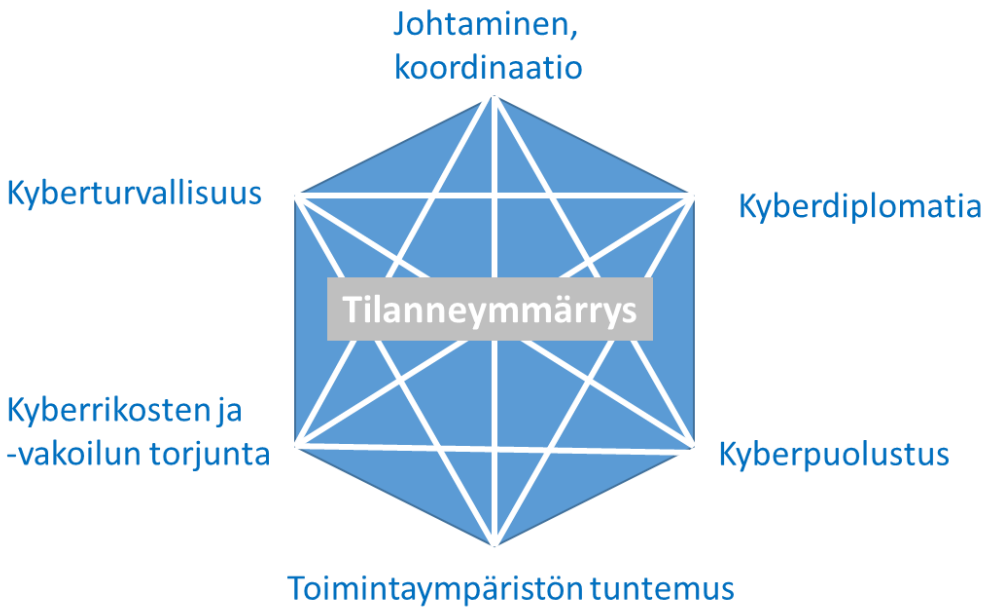
Yhteiskunnan toimijoiden mahdollisuudet ja kyvyt vastata kyberuhkiin on varmistettava kaikissa olosuhteissa. Yhteiskunnan häiriöttömän toimivuuden edellytyksenä on, että organisaatioilla on kyky palautua kyberhäiriöistä ja hyökkäyksistä nopeasti ja palauttaa järjestelmät ripeästi ja turvallisesti takaisin käyttöön.

Operatiivisesta toiminnasta vastaavien viranomaisten tehtävänä on ennaltaehkäistä, reagoida, selvittää sekä muodostaa tilannekuvaa kyberuhista. Kyberuhkien luonne asettaa vaatimuksia viranomaisten yhteistyön johtamiselle ja yhteistoiminnalle. Valtiollisiin kyberoperaatioihin reagoidaan ja vastataan eri tavoin kuin tavanomaisiin kyberuhkiin. Valtiolliseen vihamieliseen kybertoimintaan vastaaminen rikosvastuuseen saattamisen menetelmin ei välttämättä ole tehokkain tapa. Uhkiin vastataan yhdistelemällä eri keinoja ja toimia koko kybertoimintaympäristössä ja toiminnan eri tasoilla sekä arvioimalla myös kansainvälisen oikeuden näkökulmia. Jatkuvasti kehittyvän kybertoimintaympäristön uhkat edellyttävät eri toimijoiden roolien ja vastuiden määrittämistä kokonaisvaltaisesti kyberhyökkäyksiin vastaamiseksi.

Kokonaisvaltaisen ja laajan keinovalikoiman hyödyntämisen mahdollisuudet korostuvat etenkin valtiollisiin operaatioihin ja vakavaan kyberrikollisuuteen vastaamisessa. Uudessa toiminta ja -uhkaympäristössä roolien ja vastuiden määrittäminen pelkästään toimintojen ja infrastruktuurin teknisen tai toiminnallisen suojaamisen kautta ei riitä, vaan vihamieliseen toimintaan vastaamisen on oltava mahdollista koko toimintaympäristön laajuudessa. Kohdelähtöistä lähestymistä on täydennettävä siten, että tavanomaisen resilienssin ja tietoturvan varmistamisen lisäksi toteutetaan myös laajempia kokonaisvaltaisia toimenpiteitä. Esimerkiksi tietojärjestelmien suojaaminen pelkästään tietoturvan keinoin ei ole enää riittävää, vaan tarvitaan uusia keinoja, kuten tehostettua kansainvälistä tietojenvaihtoa, pakotteita tai aktiivista kyberpuolustusta.

Kyberhäiriöiden ja -uhkatilanteiden johtamismallia kehitetään.

Oikea-aikaisen reagoinnin ja vastatoimien tueksi muodostetaan operatiivisten viranomaisten yhteinen analysoitu tilannekuva. Sillä tuetaan yhteisen tilanneymmärryksen muodostamista, mikä mahdollistaa toimenpiteiden suunnittelun, valmistelun ja toimeenpanon. Johtamismalli muodostetaan edellä III pilarissa kuvatussa virastotason yhteistyörakenteessa. Yhteistyörakenteella ja siihen kuuluvilla viranomaisilla on oltava riittävät tiedon luovutus- ja saantioikeudet, jotta toiminnan koordinointi pystytään toteuttamaan. Kansallisen kyberturvallisuuden ja sen edellyttämän viranomaisten tiedonhankinnan, tiedonsaantioikeuden ja tiedonvaihdon painopiste on yhteiskunnan elintärkeisiin toimintoihin, kansalliseen turvallisuuteen, maanpuolustukseen ja huoltovarmuuteen kohdistuvien vakavien kyberuhkien ja -rikollisuuden ehkäisyssä ja torjunnassa kaikilla hallinnon tasoilla.



Kuva 2 Yhteinen tilanneymmärrys on koordinoitujen toimien perusedellytys.

Torjutaan järjestäytynyttä ja vakavaa kyberrikollisuutta

Kyberrikollisuutta torjutaan paljastamalla, ennalta estämällä ja selvittämällä epäillyt rikokset sekä hyödyntämällä tehokasta tiedolla johtamiseen perustuvaa rikostiedustelua. Viranomaisten tavoitteena on torjua erityisesti järjestäytynyttä ja vakavaa kyberrikollisuutta, heikentää rikollisten toimintaedellytyksiä sekä varmistaa, etteivät järjestäytyneet rikollisryhmät tai muut yhteiskunnalle vaaralliset toimijat laajenna toimintaansa yhteiskunnan rakenteisiin, talouteen tai päätöksentekojärjestelmiin.

Oikeus- ja lainvalvontaviranomaisten toimintaedellytyksiä sekä kansallista ja rajat ylittävää yhteistyötä ja sen vaatimaa tietojen vaihtoa kehitetään vastaamaan muuttunutta turvallisuusympäristöä. Rajat ylittävässä kyberrikollisuuden

torjunnassa hyödynnetään yhteisiä kansainvälisiä tutkintaryhmiä. Rikostorjunnan ja sen keinovalikoiman tuottamaa tietoa hyödynnetään nykyistä paremmin myös kyberpuolustuksen, attribuution ja vastatoimien tukena. Attribuutio on tosiseikkojen keräämistä ja analyysiä, teknistä ja oikeudellista arviointia, päätöksentekoa ja lopulta tehdyn päätöksen kommunikointia eri tahoille. Kokonaisvaltaisessa attribuutioprosessissa on kyettävä hyödyntämään kaikki attribuutioon liittyvä tieto, jota tuottavat muun muassa tiedustelu-, kyberturvallisuus- sekä esitutkintaviranomaiset osana lakisääteisiä tehtäviään. Varmistetaan, että Suomella on edellytykset torjua Suomeen tai Suomen etuja vastaan kohdistuvaa valtiollista kybertoimintaa huolehtimalla siitä, että tiedustelu- ja turvallisuusviranomaisilla on ajantasaiset toimivaltuudet ja toimintaedellytykset.

Kyberpuolustuksen tehtäviä ja roolia tarkennetaan

Kansallisen kyberpuolustuksen toteuttamisen tueksi laaditaan kyberpuolustusdoktriini, jossa tarkennetaan kyberpuolustuksen tavoitteita. Siinä kuvataan, miten kyberpuolustus toteutetaan hyödyntäen kansalliset ja Naton tuomat kyvykkyydet, muut kyvykkyydet ja toimintamahdollisuudet. Kyberpuolustusta kehitetään tasapainoisesti kansallisen kyberresilienssin, -turvallisuuden, ja -rikostorjunnan kehittämisen rinnalla. Kansallisen ja sotilaallisen kyberpuolustuksen rooli rauhan, kriisin ja konfliktin oloissa on tarkennettu turvallisuusympäristön edellyttämälle tasolle. Kansallisen kyberpuolustuksen kehittäminen on myös osa kokonaismaanpuolustuksen kehittämistä ja toimeenpanoa.

Suomi tarkastelee asemoitumistaan ja lähestymistään vihamieliseen kybertoimintaympäristössä tapahtuvaan toimintaan. Kansallisesti varaudutaan aktiiviseen kyberpuolustukseen sekä vastustajan attribuoinnin ja vastatoimien mahdollisuuteen. Kyberpuolustuksen toiminta yhteensovitetaan ulko- ja turvallisuuspolitiikan toiminnan ja toimijoiden kanssa.

Tavoitteena on, että Suomi vastaa kolmansien maiden aiheuttamiin kyberuhkiin niin ennaltaehkäisevin, reaktiivisin kuin pitkän aikajänteen toimenpitein ja hyödyntää kattavasti koko kansallista keino- ja suorituskykyvalikoimaa. Näitä ovat muun muassa diplomatian, tiedustelun, informaation hallinnan ja strategisen viestinnän, sotilaallisen suorituskyvyn, rikostorjunnan ja finanssialan keinot sekä taloudelliset, oikeudelliset ja muut kyberturvallisuuden keinot. Jos valtion elimiä tai valtion puolesta toimivia yksityisiä ryhmiä tai yksityishenkilöitä

voidaan tunnistaa valtion kansainvälisiä velvoitteita loukkaavan kyberoperaation tekijöiksi, kyseisellä valtiolla on niistä vastuu.

Suomen etu on tehdä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Tämä koskee teknistä, operatiivista ja strategista yhteistyötä, kansainvälisten normien ja standardien kehittämistä, poliittista vuoropuhelua sekä kykyä attribuointiin ja vastatoimien toteuttamiseen. Suomi osallistuu myös Naton kyberpuolustuksen toimintaan täysimääräisesti ja hyödyntää EU:n toimintamahdollisuudet suorituskyky-yhteistyön, tiedonvaihdon, koordinoitujen vastatoimien ja regulaation osalta kansallisen kyberpuolustuksen tukena. Kyberpuolustus on osa Suomen ja Naton puolustusta ja pelotetta.

Resursointi, toimeenpano ja seuranta

Resursointi

Suomessa kyberturvallisuuden toimijat torjuvat uhkia joka päivä. Toimintaympäristön muutos kasvattaa ja monimuotoistaa kyberuhkia ja -riskejä. Siten myös resursseja on lisättävä muuttuvaa uhkaympäristöä ja uudistuvaa sääntelyä vastaaviksi. Jo nykytilan ylläpitämiseen tarvitaan nykyistä enemmän resursseja ja niiden käytön tehostamista.

Tällä hetkellä Suomi käyttää vuosittain lähes 300 miljoonaa euroa valtionhallinnon kyberturvallisuuden varmistamiseen. Tämän lisäksi alue- ja paikallishallinto käyttää resursseja omaan kyberturvallisuuteensa, mutta niiden käytön seurantaa on vielä kehitettävä. Huomionarvoista on myös, että elinkeinoelämä omistaa merkittävän osan Suomen kriittisestä infrastruktuurista ja vastaa sen kyberturvallisuuden varmistamisesta. Varovaisen arvion mukaan elinkeinoelämän panostukset kyberturvallisuuteen ovat vähintään kymmenkertaisia verrattuna valtionhallinnon osoittamaan rahoitukseen. Myös huoltovarmuuden näkökulmasta yritysten käyttämät resurssit kyberturvallisuuteen on yhä tärkeämpää. Kyberturvallisuuteen investoidaan myös välillisesti. Esimerkiksi kyberosaamiseen panostetaan Suomessa kaikilla koulutusasteilla ja erilaisissa tutkimushankkeissa. Kyberkoulutukseen ja -tutkimukseen sijoitettu euro näkyy kyberturvallisuuden vahvistumisessa usein vasta myöhemmin.

Kaikkien strategisten tavoitteiden ja kehittämistoimien toteuttamiseen on suunnattava lisää resursseja. Suomen kyberprofiilin muuttaminen edellyttää paitsi resurssien kasvattamista myös niiden suunnittelun ja seurannan tarkentamista sekä käytön tehostamista.

Toimivan ja elinvoimaisen kyberturvallisuuden ekosysteemin rakentaminen tarkoittaa merkittäviä taloudellisia investointeja koko yhteiskunnan tasolla. Toimiva ekosysteemi tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa digitaalisen yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristön haitallisia ilmiöitä vastaan.

Kokonaisturvallisuuden mallin nykyistä laajempi ja syvempi hyödyntäminen kyberturvallisuuden varmistamisessa ja siihen pohjautuva varautuminen, reagointi ja vastatoimet ovat välttämättömiä toimia, jotta voidaan välttyä vakavien kyberhäiriötilanteiden aiheuttamilta kustannuksilta. Kokonaisturvallisuuden malli tehostaa olemassa olevien resurssien käyttöä ja kasvattaa yleistä resilienssiä, kun osaamista ja toimintamalleja sekä parhaita käytäntöjä saadaan jaettua eri tasoisesti varautuneiden organisaatioiden kesken.

Murrosteknologioihin kohdistuva korkeatasoinen tutkimus- ja kehitystoiminta sekä kansalliseen kyberturvallisuuteen tehtävät investoinnit ovat keskeisiä keinoja kyberturvallisen ja -kriisinkestävän yhteiskunnan säilyttämiseksi. TKI-toimintaa on tärkeää tukea myös Suomen kilpailukyvyn lisäämiseksi. Osaamista tarvitaan kaikilla tasoilla, ja esimerkiksi merkittävän osan kansalaisista tavoittava järjestöjen tekemä valistus- ja neuvontatyö tai eri toimijoiden järjestämät kyberharjoitukset edellyttävät resursointia.

Naton innovaatiorahoituksen ja EU:n kehittämisrahoituksen hyödyntäminen on oleellinen osa Suomen kyberekosysteemin kehittämistä. Tämä edellyttää Suomelta vastinrahaa ja hallinnonalojen välistä resurssien käytön koordinointia. Lisäksi Nato-jäsenyys edellyttää lisäpanostuksia kyberturvallisuuteen ja -puolustukseen sekä infrastruktuurin kyberresilienssin kehittämiseen. Nato-jäsenyys vaatii Suomelta myös uudenlaisia suorituskykyjä ja resursseja liittolaisten tukemiseksi. Samalla myös EU-sääntelyn myötä lisääntyneet viranomaistehtävät ja velvoitteet edellyttävät riittäviä resursseja.

Kansallisten resurssien määrittämisessä keskeistä on arvioida vaihtoehtoiskustannuksia eli kustannuksia, jotka syntyvät, jos strategian kehittämistoimia ei toteuteta tehokkaasti. Näitä ovat toteutuneista kyberhyökkäyksistä aiheutuneiden henkilö- ja ict-kustannusten lisäksi esimerkiksi tietovuodoista, kyberrikollisuudesta ja mainehaitoista aiheutuneet seuraukset.

Strategian toimeenpano ja seuranta

EU:n kyberturvallisuusdirektiivi (NIS2) ja sen kansallinen täytäntöönpano edellyttävät, että kansallisen kyberturvallisuusstrategian päivitystarvetta arvioidaan viiden vuoden välein. Tarvittaessa strategiaa kehitetään ja ajantasaistetaan useamminkin. Päivitykset tehdään yhteistyössä viranomaisten, elinkeinoelämän, tutkimuslaitosten, järjestöjen ja kansalaisten kanssa.

Strategian toimeenpanoa seurataan kansallisesti vuosittain. Seurannan koordinointivastuu on valtion kyberturvallisuusjohtajan toimistolla, jolle hallinnonalat tuottavat kyberturvallisuuden toimeenpanoraportin omasta vastuualueestaan julkisen talouden suunnitteluprosessin aikataulun mukaisesti. Näistä toimisto laatii koosteen viranomaisille ja poliittisille päättäjille. Strategian seurannasta raportoidaan yhteiskunnan uudistamisen ministerityöryhmälle ja etenemisestä informoidaan myös sisäisen turvallisuuden ja oikeudenhoidon ministerityöryhmää sekä Turvallisuuskomiteaa.

Kyberturvallisuusstrategian uudistamista varten asetetun työryhmän työtä jatketaan strategian valmistuttua, ja ryhmä muutetaan strategian toimeenpanon seurantaryhmäksi. Seurantaryhmä laatii strategian toimeenpanosuunnitelman kuuden kuukauden sisällä strategian valmistumisesta. Toimeenpanosuunnitelmassa määritetään toimeenpanovastuut ja aikataulu hallinnonaloittain ja kuvataan tarkemmin mittarit, joilla strategian toimeenpanoa vuosittain seurataan ja arvioidaan.

Kyberturvallisuuden suorituskykyindikaattorien määrittelytyössä hyödynnetään soveltuvin osin mm. EU:n kyberturvallisuusvirasto ENISAn, OECD:n ja Naton kyberkyselyitä, DVV:n vuosittain teettämää digiturvakyselyä (julkinen hallinto), Huoltovarmuuskeskuksen toimialojen kyberkypsyysmittareita (elinkeinoelämä) sekä DVV:n tuottamaa digiturvabarometriä (kansalaisten kyberkestävyys).

Tavoitteena on laajentaa kyberkestävyyden indikaattorit kattamaan myös ennakoiva kybervarautumistyö. Keskeisten indikaattoreiden määrittämisessä Suomi hakee tarvittaessa tukea EU:n ENISAlta NIS2-direktiivissä säädetyn mukaisesti. Suomen menestymistä kansainvälisesti seurataan myös kansainvälisiin indekseihin perustuen (ITU: Global Cybersecurity Index (GCI) ja e-Governance Academy: National Cyber Security Index (NCSI).

Strategian toimeenpanossa painotetaan parhaiden käytäntöjen tunnistamista ja ja poikkeamatilanteista opittujen toimintatapojen laajaa hyödyntämistä. Siten edistetään johdonmukaisten toimintatapojen muodostumista ja ylläpitämistä ja tuetaan koko yhteiskunnan resilienssiä. Toimeenpanon arvioinnin tarkoituksena on tukea poliittista päätöksentekoa, viranomaistoimintaa ja yhteiskunnallista keskustelua.

Strategiset kehittämisehdotukset

Alla olevat kehittämisehdotukset on muotoiltu strategisten tavoitteiden pohjalta. Kehittämisehdotusten perusteella laaditaan tarkempi, aikataulutettu ja vastuutettu toimeenpanosuunnitelma.

- Kirkastetaan Suomen asemoitumista kyberturvallisuudessa ja kyberpuolustuksessa, kehitetään osallistumista kansainväliseen kyberturvallisuuden yhteistoimintaan, luodaan tätä varten tarvittava kansallinen koordinaatio.

- Varaudutaan uusien murrosteknologioiden, erityisesti kvanttilaskennan, kehittymisen tuomiin uhkiin ja mahdollisuuksiin.

- Edistetään teknologisen suvereniteetin ja kyberturvallisuuden ekosysteemin kehittämistä ja varmistetaan Suomen teknologinen edelläkävijyys ja uudet innovaatiot. Kehitetään viranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset.

- Kehitetään viranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset.

- Muutetaan säädöspohjaa, normeja ja ohjeita strategian kehittämistoimien edellyttämällä tavalla.

- Vahvistetaan viranomaisten, alue- ja paikallishallinnon, yksityissektorin ja kansalaisyhteiskunnan yhteistoimintaa ja yhteistä varautumista.

- Ylläpidetään ja parannetaan luottamusta turvallisilla ja toimintavarmoilla julkisilla palveluilla.

- Suunnitellaan ja seurataan kyberturvallisuusresursseja pitkäjänteisesti.

- Kehitetään osaamista sekä kansalaisten ja kansalaisyhteiskunnan kybervalmiuksia ja varautumista.

- Kehitetään harjoitustoimintaa ja harjoitusympäristöjä varautumisen ja osaamisen lisäämiseksi.

- Kehitetään toimintaympäristötuntemusta muun muassa turvaamalla kansallinen havainnointikyky sekä turvallisuus- ja tiedusteluviranomaisten mahdollisuudet tietojen hankkimiseksi kybertoimintaympäristöstä.

- Edistetään kokonaisvaltaista kyberrikollisuuden torjuntaa.

- Kehitetään kyberpuolustusta osana kokonaismaanpuolustusta, Suomen suvereniteetin turvaamista ja integroitumista liittokunnan puolustukseen.

- Arvioidaan kyberturvallisuusnäkökulmia kaikissa lainsäädäntöhankkeissa.

Liitteet

Liite 1: Kyberturvallisuuden kansallinen yhteistoimintamalli

Tässä liitteessä kuvataan kyberturvallisuuden kansallisen yhteistoimintamallin nykytilaa ja toimijoita sekä vastataan kyberturvallisuusdirektiivin (NIS2) vaatimuksiin kansallisesta näkökulmasta.

Kyberturvallisuuden kansallinen yhteistoimintamalli (jatkossa kyberturvallisuuden yhteistoimintamalli) Suomessa on hajautettu ja vastaa periaatteiltaan kokonaisturvallisuuden yhteistoimintamallia (jatkossa kokonaisturvallisuuden malli). Yhteistyön perustana ovat lakisääteiset tehtävät, yhteistyösopimukset ja yhteiskunnan turvallisuusstrategia, jonka jokaisessa strategisessa tehtävässä otetaan huomioon kyberturvallisuus. Kyberturvallisuuden yhteistoimintamalli skaalautuu kaikille tasoille, eli on sovellettavissa kansalliselta tasolta alue- ja paikallistasolle, kansainväliset kumppanit huomioiden.

Kokonaisturvallisuuden tavoitteena on varmistaa kaikissa oloissa keskeisten toimijoiden tiivis yhteistyö varautumisessa. Laajemmat varautumistoimenpiteet koordinoidaan yhteistyössä tarvittavien julkisen ja yksityisen sektorin toimijoiden kanssa. Kyberturvallisuuden yhteistoimintamallia kehitetään edelleen kokonaisturvallisuuden mallin mukaiseksi huomioiden kyberturvallisuuden ominaispiirteet.

Kyberturvallisuuden yhteistoimintamallissa ja kyberturvallisuusdirektiivin tarkoittamassa kyberkriisitilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Toimivaltaiset viranomaiset, toiminnan yhteensovittaminen sekä tukeminen määritetään tarvittaessa yhteiskunnan kriisijohtamisen mallin mukaisesti. Jokainen toimija vastaa varautumisestaan ja on valmiuslain ja sektorilainsäädännön kautta velvoitettu huolehtimaan siitä, että kriittiset palvelut toimivat kaikissa olosuhteissa esimerkiksi asettamalla palveluntuottajille vaatimuksia ja valvomalla niiden toteuttamista. Kyberhäiriötilanteisiin varaudutaan ja niihin reagoidaan tiiviissä yhteistyössä julkisen sektorin, elinkeinoelämän ja kansalaisyhteiskunnan

kanssa. Julkisen sektorin yhdessä elinkeinoelämän kanssa tarjoamat keskitetyt kyberturvallisuuspalvelut tukevat organisaatioita ja kansalaisia varautumisessa ja häiriötilanteissa. Näin varmistetaan yhdenmukainen toiminta, vältytään päällekkäisiltä kustannuksilta ja yleisesti tarvittavat palvelut kuten verkkokoulutukset, kybertilannekuva ja ohjeistus ovat kaikkien saatavilla. Viranomaiset, kuten Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus (jatkossa Kyberturvallisuuskeskus) sekä julkisten palvelujen tuottajat viestivät aktiivisesti niin kansalaisille, yrityksille kuin julkisille toimijoille kyberturvallisuuden häiriötilanteista ja haavoittuvuuksista.

Kyberturvallisuusdirektiivin mukaisena kyberkriisinhallintaviranomaisten välisenä koordinaattorina toimii Kyberturvallisuuskeskus. Se vastaa myös kansallisen NIS2-direktiivin edellyttämän kyberkriisinhallintakehyksen laatimisesta laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallitsemiseksi yhteistyössä muiden viranomaisten kanssa.

Alla on kuvattu yhteiskunnan eri toimijat kansallisen kyberturvallisuuden varmistamisessa. Varautuminen, reagointi ja vastatoimet toteutetaan laajassa yhteistoiminnassa, johon sisältyy myös tiedonvaihtoa yhteisen tilanneymmärryksen muodostamiseksi ja yhteisten toimien koordinoimiseksi.

Kuva 3: Yhteiskunnan eri toimijat kansallisen kyberturvallisuuden varmistamisessa

Poliittinen päätöksenteko

Poliittisessa päätöksenteossa ratkaistaan merkittäviä kybervarautumiseen ja häiriönhallintaan liittyviä kysymyksiä kuten lainsäädännölliset linjaukset ja ulko- ja turvallisuuspoliittisen prosessin mukaiset päätökset. Viranomaiset raportoivat kyberturvallisuuden tilanteesta ja toimista tasavallan presidentille, eduskunnalle, valtioneuvostolle sekä ministerityöryhmille.

Strateginen taso

Valtioneuvosto ja sen ministeriöt vastaavat kansallisen kyberturvallisuuden lainsäädännön valmistelusta, yleisistä linjauksista, resurssien kohdentamisesta, toimintaperiaatteista, strategisesta ohjauksesta, varautumisesta sekä vastatoimista ja yhteistoiminnasta.

Valtion kyberturvallisuusjohtajan toimisto vastaa kansallisesti kyberturvallisuuden kehittämisen, suunnittelun, varautumisen ja kriittisen tieto- ja viestintäteknisen infrastruktuurin varautumisen koordinaatiosta ja yhteensovittamisesta. Valtion kyberturvallisuusjohtaja koordinoi ja sovittaa yhteen kansallista kyberturvallisuuden kehittämistä, suunnittelua ja varautumista sekä toimii valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa.

Strategisella tasolla toimii myös liikenne- ja viestintäministeriön asettama Kyberturvallisuuden koordinaatioryhmä, joka tavoitteena on varmistaa, että kansallisilla kyberturvallisuudesta, kyberpuolustuksesta ja kyberdiplomatiasta vastaavilla ministeriöillä ja kyberturvallisuusviranomaisilla on yhdenmukainen tilannekuva yhteiskunnan kyberturvallisuuden tilasta ja kyberturvallisuuteen vaikuttavista tapahtumista sekä kyberturvallisuusympäristön muutoksesta.

Valvovat viranomaiset (NIS2 ja muut)

Valvovilla viranomaisilla tarkoitetaan [*NIS2-lain*] mukaisia valvovia viranomaisia. Ne valvovat [*NIS2 -lain*] mukaisia yksityisten ja julkisten palveluntarjoajien varautumista, häiriönhallintaa sekä palautumista. Suomessa toimitaan hajautetun mallin mukaisesti, jolloin sektoriviranomaiset valvovat sektorillaan olevia toimijoita. Lisäksi Kyberturvallisuuskeskus toimii kansallisena koordinaatiopisteenä. Valvovia viranomaisia ovat Liikenne- ja viestintävirasto Traficom, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveydenalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus ja kehittämiskeskus ja Finanssivalvonta.

Kyberhyökkäysten kuten tietomurtojen seurauksena voi hyökkääjän haltuun päätyä esimerkiksi henkilötietoja, jolloin kyseessä on henkilötietojen tietoturvaloukkaus. Henkilötietojen tietoturvaloukkausten osalta kansallinen valvontaviranomainen on Tietosuojavaltuutetun toimisto, joka valvoo tietosuojalainsäädännön noudattamista.

Lisäksi on muita valvovia viranomaisia kuten Säteilyturvakeskus ja Suomen Pankki.

Operatiiviset viranomaiset

Kyberturvallisuuden operatiivisilla viranomaisilla on keskeinen kansallinen rooli niin kyberhäiriötilanteisiin varautumisessa kuin niihin reagoimisessa ja vastatoimissa. Suomessa toimii lisäksi useita vapaaehtoisuuteen perustuvia kansallisia tiedonvaihtoverkostoja.

Kyberturvallisuuskeskuksen keskeinen tehtävä on vastata kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja kansallisesta haavoittuvuuskoordinaatiosta. Se kerää ja analysoi tietoa Suomessa tapahtuvista tietoturvauhkista ja -loukkauksista sekä selvittää osaltaan Suomeen kohdistuvia teknisiä tietoturvapoikkeamia. Sen tehtäviin kuuluu myös yleisen kyberturvallisuustietoisuuden lisääminen. Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa.

Esitutkintaviranomaisten tehtävänä on ennalta estää rikosten tapahtuminen sekä selvittää tapahtuneen rikoksen osalta tapahtuman osapuolet sekä tosiseikat rikosprosessiin. Rikosprosessiin kuuluvat poliisi, syyttäjä sekä tuomioistuin. Poliisi tutkii tietoverkkorikoksia ja pyrkii saamansa tiedon avulla myös estämään ennalta mahdollisia tulevia rikoksia. Poliisi ylläpitää tietoverkkorikosten kansallista tilannekuvaa. Myös esimerkiksi keskusrikospoliisi osallistuu aktiivisesti tietoisuuden lisäämiseen erityisesti osana ennaltaehkäisevää toimintaa.

Tiedusteluviranomaisia ovat suojelupoliisi ja sotilastiedusteluviranomaiset (Puolustusvoimien pääesikunta ja Puolustusvoimien tiedustelulaitos). Tiedusteluviranomaisten tehtävänä on hankkia tietoa, analysoida ja raportoida sitä turvallisuusviranomaisten ja valtionjohdon tueksi. Tiedustelutiedot auttavat ennakoimaan Suomeen kohdistuvia kyberuhkia ja torjumaan niitä toimivaltaisten viranomaisten toimesta. Tiedusteluviranomaiset suorittavat tiedustelua muun muassa verkossa tapahtuvien kyberhyökkäysten tekijöiden sekä hyökkäysten taustojen ja motiivien selvittämiseksi kansallisen turvallisuuden suojaamiseksi, ylimmän valtionjohdon päätöksenteon tukemiseksi myös attribuutioprosessissa sekä muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

Puolustusvoimien tehtävien voidaan katsoa kattavan myös kybertoimintaympäristö (kyberpuolustus ja tiedustelu kybertoimintaympäristössä). Tähän liittyen Puolustusvoimien tehtäviin kuuluu muun muassa Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä kansainvälisen avun antaminen, yhteistoiminta ja muu kansainvälinen toiminta. Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen.

Keskus-, alue- ja paikallishallinto sekä itsenäiset laitokset

Virastoilla ja alue- ja paikallisviranomaisilla sekä itsenäisillä laitoksilla on keskeinen rooli huolehtia kyberturvallisuudesta viranomaisten päivittäisessä toiminnassa. Toimijoihin kuuluvat valtion virastot, liikelaitokset ja yhtiöt, aluehallinnon toimijat, hyvinvointialueet, kunnat ja kuntayhtymät, sekä julkiset palveluntuottajat ja itsenäiset laitokset. Näistä osan velvollisuutena on ohjata, valvoa, ohjeistaa, auttaa, koordinoida, tukea ja varoittaa, sekä kerätä, analysoida ja jakaa tietoa myös kyberturvallisuudesta päätöksenteon ja toiminnan kehittämisen tueksi. Ne myös tuottavat julkiset palvelut yhteistyössä elinkeinoelämän kanssa ja huolehtivat palveluiden turvallisuudesta, riskien- ja jatkuvuudenhallinnasta sekä varautumisesta.

Yritykset ja yhteisöt

Yksityisen sektorin toiminnot, osaaminen ja voimavarat muodostavat merkittävän osan Suomen kansallista kyberturvallisuutta. Valtaosa Suomen kriittisestä infrastruktuurista on elinkeinoelämän omistuksessa. Elintärkeiden toimintojen turvaaminen ja kriittinen infrastruktuuri ovat keskeisiä yhteiskunnan toimintakyvyn, jatkuvuudenhallinnan ja huoltovarmuuden näkökulmasta. Yrityksillä on teknologisen kyvyn lisäksi myös vahva osaamisperusta, tahtotila ja resurssit varautua kyberturvallisuuden uhkiin liiketoiminnassaan sekä kotimaassa että kansainvälisillä markkinoilla.

Elinkeinoelämän varautuminen perustuu osin lainsäädäntöön mutta myös vapaaehtoiseen varautumis- ja huoltovarmuustyöhön. Julkisen ja yksityisen sektorin välistä yhteistyötä tehdään päivittäin tilannekuvan keräämisessä ja aktiivisella tiedonvaihdolla sekä pitkäjänteisellä kehittämistyöllä. Elinkeinoelämän

toimijat osallistuvat tiiviisti erilaisiin yhteistyöryhmiin, mikä lisää luottamusta yksityisen ja julkisen sektorin välillä ja tarjoaa mahdollisuuden vaikuttavaan yhteistyöhön myös kansainvälisesti.

Elinkeinoelämä tuottaa valtaosan yhteiskunnan tieto- ja kyberturvallisuuspalveluista. Yksityiset ict-palveluntarjoajat ovat keskeisessä asemassa niin kansalaisten, yritysten kuin valtiollisten ja alueellisten toimijoiden kyberturvallisuudessa.

Huoltovarmuusorganisaatio

Huoltovarmuusorganisaatio (HVO) on verkosto, johon kuuluvat Huoltovarmuuskeskus (HVK) ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Huoltovarmuuskriittiset toimijat kuuluvat Huoltovarmuuskeskuksen seitsemään sektoriin tai kahdeksaan pooliin. HVK:n lakisääteisiin tehtäviin kuuluu yhteistyöverkostonsa avulla kehittää ja yhteensovittaa julkishallinnon ja elinkeinoelämän yhteistoimintaa huoltovarmuusasioissa. Toimijat pitävät yllä ja kehittävät huoltovarmuutta ja jatkuvuudenhallintaa myös kyberturvallisuuden näkökulmasta oman toimialansa yritysten ja organisaatioiden verkostossa yhteistyössä viranomaisten kanssa.

Valvottavat toimijat (NIS2)

[NIS2-lain] mukaisia riskienhallinta- ja poikkeamaraportointivelvoitteita eli kyberturvallisuuslakia sovelletaan valvottaviin toimijoihin eli [*täydennetään kun HE etenee*].

Palveluntuottajat ja niiden toimitusketjut

Palveluntuottajilla tarkoitetaan organisaatioita, jotka tuottavat palveluita tai tuotteita yhteiskunnalle. Palveluntuottaja vastaa palvelunsa ja tuotteensa elinkaaren aikaisesta kyberturvallisuudesta koko arvoketjun kattavasti. Toimitusketjun kyberturvallisuus varmistetaan riskienhallinnan keinoin [NIS2 -lain] mukaisesti tai sopimusperusteisesti.

Palveluntuottajia ovat myös tutkimuslaitokset ja korkeakoulut. Ne tuottavat kyberturvallisuuden osaamis- ja tietopääomaa ja innovaatioita.

Järjestöt ja neljännen sektorin toimijat

Suomi tunnetaan maailmalla lukuisista kansalaisjärjestöistään ja ihmistensuuresta halusta osallistua kansalaisyhteiskunnan toimintaan. Kansalaisjärjestöjen ja vapaaehtoisten merkitys myös kansallisen kyberturvallisuuden varmistamisessa on kasvussa. Järjestökentän integrointi kyberturvallisuuden verkostoihin edistää kansallista resilienssiä, minkä lisäksi järjestöt kaipaavat tukea kyberturvallisuuden kehittämisessä muilta toimijoilta. Järjestöt ovat helposti lähestyttäviä ja niihin luotetaan, minkä myötä järjestökentän rooli kansalaistaitojen kehittämisessä on merkittävää. Lisäksi erityisesti Maanpuolustuskoulutusyhdistys (MPK), tarjoaa tukea kyberpuolustuksen kehittämisessä järjestämällä kursseja ja kehittämällä ja kasvattamalla kyberreserviä. Järjestöjen rooli ei kuitenkaan ole vielä vakiintunut osa kyberturvallisuuden ekosysteemiä.

Järjestöillä ja neljännen sektorin eli järjestäytymättömän kansalaistoiminnan toimijoilla on paljon annettavaa häiriötilanteiden hallinnan tukemiseen, ja näiden tuesta viranomaistoiminnalle merkittävien häiriötilanteiden hallinnassa on jo kokemusta.

Kansalaiset

Yksilön osaaminen vahvistaa organisaatioiden ja yhteiskunnan kyberresilienssiä. Uudet teknologiaratkaisut ovat yhä kiinteämmin osa jokapäiväistä elämää, mikä nostaa esiin myös yksittäisen kansalaisen roolin kansallisessa kyberturvallisuudessa. Valppautta tarvitaan niin kotioloissa kuin työelämässäkin, ja jokainen voi omalla toiminnallaan vaikuttaa siihen, miten kybertoimintaympäristössä tapahtuvat häiriötilanteet elämään vaikuttavat. Kyberturvallisuus on luonnollinen osa jokaisen yksilön yhteiskuntavastuuta, joka vaatii jatkuvaa tietotaidon kehittämistä ja ylläpitämistä. Myös läheisille tarjottava tuki ja oikeaaikainen ilmoittaminen omista havainnoista edesauttavat kansallisen kyberresilienssin ylläpitämisessä ja kehittämisessä sekä kyberrikosten selvittämisessä.

Termit

Alla olevat termit määritelmineen kuvaavat tässä asiakirjassa käytettyjä käsitteitä. Termejä on käytetty tiivistämään strategian kerrontaa ja välttämään toistoa, ja niiden avaamisella on tarkoitus auttaa lukijaa ymmärtämään tarkoitettu asiayhteys. Strategiassa käytetyt termit poikkeavat osin tai kokonaan olemassa olevista sanastoista kuten TEPA-termipankki tai Kyberturvallisuuden sanasto, sillä kyberturvallisuuteen liittyvien kansallisten käsitteiden osalta on tunnistettu päivitystarve. Päivitystarve johtuu erityisesti pyrkimyksestä kansainvälisesti yhdenmukaiseen käsitteistöön sekä lainsäädännön, erityisesti EU- regulaation, sisältämien käsitteiden tuomisesta sanastoon.

Kansallinen kyberturvallisuus

Ne toimet, joiden seurauksena digitaalinen yhteiskunta kykenee varautumaan, tunnistamaan, torjumaan ja kestämään sähköisten ja verkotettujen järjestelmien häiriöitä ja niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin, toipumaan niistä sekä varmistamaan osaltaan kansallisen turvallisuuden, maanpuolustuksen ja huoltovarmuuden toimintaedellytykset.

Kyberturvallisuus

Ne toimet, joilla suojataan viestintä- ja tietojärjestelmät sekä muut sähköiset järjestelmät, niissä tallennettavat, käsiteltävät tai siirrettävät tiedot sekä niiden käyttäjät, hyödyntäjät ja muut asianosaiset henkilöt kyberuhilta.

Kansallinen kyberpuolustus

Ne kansalliset ja kansainväliset sotilaalliset ja siviilialojen toimet, joilla turvataan Suomen valtiollinen itsenäisyys sekä kansan elinmahdollisuudet ja turvallisuus ulkoisia, valtioiden aiheuttamia kyberuhkia ja -häiriöitä vastaan ja toimeenpannan tarvittavat vastatoimet kaikissa valmiustiloissa.

Sotilaallinen kyberpuolustus

Ne toimet, joilla turvataan Suomen puolustuskykyyn vaikuttavat järjestelmät ja eri sektorien toimijat erityisesti valtiollisilta uhkatoimijoilta ja niiden edustajilta

puolustuskyvyn varmistamiseksi sekä turvataan Suomen suvereniteettia ja toimeenpannaan sotilaalliset kyberoperaatiot.

Resilienssi; ~kriisinkestävyys; ~kriisinsietoisuus

Valtion, organisaatioiden, yhteisöjen ja yksilöiden kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä.

Kyberresilienssi; ~kybersietoisuus

Valtion, organisaation, yhteisön tai yksilöiden kyky ylläpitää toimintakykyä kybertoimintaympäristön muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja uhkia, palautua niistä ja tarvittaessa reagoida niihin.

Kyberhygienia

Turvallisuusorientoitunut ajattelutapa, kehittynyt organisaation turvallisuuskulttuuri, yhdistettynä arjen säännöllisiin rutiineihin, käytänteisiin ja prosesseihin, joiden avulla yhteisö ja yksilö tietojärjestelmiä, tietokonetta tai muita laitteita käyttäessään kehittää ja ylläpitää osaltaan ympäristön kyberturvallisuutta.

Kyberuhka

Potentiaalinen tilanne, tapahtuma tai toiminta, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.

Kyberympäristö, -avaruus

Kyberympäristö tarkoittaa ihmisen luomaa ja hallinnoimaa globaalia tilaa, joka perustuu informaatioteknologiaan ja sähkömagneettisen spektrin käyttämiseen informaation luomiseksi, muokkaamiseksi, vaihtamiseksi ja hyödyntämiseksi sekä toisiinsa liitettyjen että toisistaan erillisten informaatioteknologiaa käyttävien verkkojen kautta.

Kybertoimintaympäristö

Kybertoimintaympäristö muodostuu yhdestä tai useammasta digitaalisen datan tai informaation käsittelyyn tarkoitetusta tietojärjestelmästä, niiden fyysisestä ja loogisesta rakenteesta sekä toimintaympäristön toimijoista luonnollisine ja digitaalisine identiteetteineen. Kybertoimintaympäristö painottaa kyberympäristön hyödyntämistä tavoitteellisen toiminnan näkökulmasta.

Yhteiskunnan elintärkeä toiminto

Toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta.

Kriittinen infrastruktuuri, yhteiskunnan kriittinen infrastruktuuri

Hyödyke, tila, laitteisto, verkosto tai järjestelmä tai osa hyödykkeestä, tilasta, laitteistosta, verkostosta tai järjestelmästä, tai tärkeä palvelu, joka on välttämätön yhteiskunnan elintärkeän toiminnon ylläpitämiseksi tai muun keskeisen palvelun tarjoamiseksi.

Puolustuskyvylle kriittinen infrastruktuuri

Ne puolustusjärjestelmän ja kriittisen infrastruktuurin rakenteet, palvelut ja niihin liittyvät toiminnot sekä ne yhteiskunnan elintärkeät toiminnot, jotka ovat välttämättömiä maanpuolustuksen toimintaedellytyksille kaikissa valmiustiloissa.

Attribuutio, syyksilukeminen

Vihamielisen kyberoperaation toteuttajan tunnistaminen, paikantaminen ja yksilöiminen analyyttisen eri tietolähteitä hyödyntävän prosessin kautta. Kansallisella tasolla prosessiin kytkeytyy niin tekninen analyysi kuin viranomaisvastuut sekä ulko- ja turvallisuuspoliittinen harkinta. Attribuutio on analyysiprosessin lopputulos riippumatta siitä, onko tulos julkistettava vai ei-julkinen. Attribuutio on usein edellytys oikeudelliseen tai poliittiseen vastuuseen saattamiselle, kansainvälisten velvoitteiden mukaisille toimenpiteille (retorsio) ja sallituille vastatoimille. Attribuutio, esimerkiksi julkinen syyksilukeminen, voi olla myös itsessään retorsiokeino.

Kyberekoekosysteemi, ~kyberturvallisuuden ekosysteemi

Vuoden 2021 kyberturvallisuuden kehittämisohjelmassa kuvattu yritysten, tutkimuksen, julkishallinnon sekä kolmannen sektorin toimijoiden välille rakentuva ja ylläpidettävä keskinäisriippuvuuksien verkosto, jonka tavoitteena on tuottaa innovaatioita, elinvoimaa, kasvua, työpaikkoja ja osaamista sekä parantaa digitaalisen yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristön haitallisia ilmiöitä vastaan.