VALTIONEUVOSTON KANSLIAN JULKAISUJA 2024:11

Suomen kyberturvallisuus-strategia 2024–2035

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

Valtioneuvoston kanslian julkaisuja 2024:11

Suomen kyberturvallisuusstrategia 2024–2035

Valtioneuvoston kanslia Helsinki 2024

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Valtioneuvoston kanslia

ISBN pdf: 978-952-383-376-0
ISSN pdf: 2490-1164

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2024

Kuvailulehti
10.10.2024

Suomen kyberturvallisuusstrategia 2024–2035

Valtioneuvoston kanslian julkaisuja 2024:11

Julkaisija	Valtioneuvoston kanslia		
Tekijä/t	Puheenjohtaja Rauli Paananen, varapuheenjohtaja Mikko Soikkeli, sihteeristön puheenjohtaja Mari Starck, sihteeristön jäsenet Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu		
Yhteisötekijä	Liikenne- ja viestintäministeriö		
Kieli	suomi	**Sivumäärä**	58

Tiivistelmä

Suomen kyberturvallisuusstrategia on uudistettu pääministeri Petteri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuusdirektiivin (NIS2) vaatimukset 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. 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 valtioneuvoston kansliasta, ulkoministeriöstä, oikeusministeriöstä, sisäministeriöstä, puolustusministeriöstä, valtiovarainministeriöstä, opetus- ja kulttuuriministeriöstä, maa- ja metsätalousministeriöstä, liikenne- ja viestintäministeriöstä, työ- ja elinkeinoministeriöstä, sosiaali- ja terveysministeriöstä ja Turvallisuuskomitean sihteeristöstä.

Strategian valmistelutyöpajoihin on osallistunut lähes 100 julkisen ja yksityisen sektorin, tiedeyhteisön sekä kansalaisjärjestön organisaatiota.

Asiasanat	kyberturvallisuus, kokonaisturvallisuus, tietoturva, digitalisaatio, osaaminen, teknologia, tutkimus- ja kehittämistoiminta, innovaatiotoiminta, varautuminen, huoltovarmuus, kansainvälinen yhteistyö, kyberrikollisuus

ISBN PDF	978-952-383-376-0	**ISSN PDF**	2490-1164
Asianumero	VN/36693/2023	**Hankenumero**	VNK007:00/2024

Julkaisun osoite https://urn.fi/URN:ISBN:978-952-383-376-0

Presentationsblad

10.10.2024

Strategi för cybersäkerheten i Finland 2024–2035

Statsrådets kanslis publikationer 2024:11

Utgivare	Statsrådets kansli		
Författare	Ordförande Rauli Paananen, vice ordförande Mikko Soikkeli, sekretariatets ordförande Mari Starck, sekretariatets medlemmar Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu		
Utarbetad av	Kommunikationsministeriet		
Språk	finska	**Sidantal**	58

Referat

Strategin för cybersäkerheten i Finland har reviderats i enlighet med regeringsprogrammet för statsminister Petteri Orpos regering för att motsvara den förändrade verksamhetsmiljön. I revideringen av Strategin för cybersäkerheten i Finland har man beaktat kraven enligt cybersäkerhetsdirektivet (NIS 2) samt annat centralt strategi- och redogörelsearbete som anknyter till ämnet. Informationsförsvaret som skrivits in i regeringsprogrammet ska beaktas som en del av verksamhetsmodellen för strategisk kommunikation och den försvarspolitiska redogörelsen.

Målsättningen för strategin för cybersäkerheten i Finland sträcker sig till år 2035. Strategin innehåller strategiska mål som formulerats under fyra pelare och gemensamma utvecklingsåtgärder för dessa.

Strategin har beretts under ledning av statens cybersäkerhetsdirektör i underarbetsgruppen för projektet för utveckling av verksamhetsmodellen för statsrådets säkerhetsledning som statsrådets kansli tillsatte 8.3.2024. Arbetsgruppen har bestått av utsedda medlemmar från statsrådets kansli, utrikesministeriet, justitieministeriet, inrikesministeriet, försvarsministeriet, finansministeriet, undervisnings- och kulturministeriet, jord- och skogsbruksministeriet, kommunikationsministeriet, arbets- och näringsministeriet, social- och hälsovårdsministeriet och Säkerhetskommitténs sekretariat.

I de förberedande workshopparna för strategin deltog nästan 100 aktörer inom den offentliga och privata sektorn, vetenskapssamfundet samt det civila samhällets organisationer.

Nyckelord cybersäkerhet, övergripande säkerhet, informationssäkerhet, digitalisering, kompetens, teknologi, forsknings- och utvecklingsverksamhet, innovationsverksamhet, beredskap, försörjningsberedskap, internationellt samarbete, cyberbrottslighet

ISBN PDF	978-952-383-376-0	**ISSN PDF**	2490-1164
Ärendenummer	VN/36693/2023	**Projektnummer**	VNK007:00/2024

URN-adress https://urn.fi/URN:ISBN:978-952-383-376-0

Description sheet
10 October 2024

Finland's Cyber Security Strategy 2024–2035

Publications of the Prime Minister's Office 2024:11
Publisher Prime Minister's Office

Author(s) Chair Rauli Paananen, Vice-Chair Mikko Soikkeli, Secretariat Chair Mari Starck, Secre-tariat Members Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu.
Group author Ministry of Transport and Communications
Language Finnish **Pages** 58

Abstract

Finland's Cyber Security Strategy has been revised in accordance with the Programme of Petteri Orpo's Government to respond to the changed operating environment. In the revision work, account has been taken of the requirements set by the EU directive on cyber security (NIS2) and other related key strategies and reports. The concept of information defence included in the Government Programme is set to be covered in the upcoming model for strategic communication as well the Government's Defence Report.

The timeline for Finland's cyber security strategy extends to 2035. The strategy includes a set of strategic objectives divided under four pillars, followed by joint development proposals.

The strategy was prepared under the supervision of the National Cyber Security Director by a sub-working group in a project set up by the Prime Minister's Office on 8 March 2024 for developing an operating model for governmental level security management. The working group included appointed persons from the Prime Minister's Office, Ministry for Foreign Affairs, Ministry of Justice, Ministry of the Interior, Ministry of Defence, Ministry of Finance, Ministry of Education and Culture, Ministry of Agriculture and Forestry, Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of Social Affairs and Health, and the Security Committee's Secretariat.

Nearly 100 organisations from the public and private sector, the academia and the non-governmental sector participated in the preparatory workshops.

Keywords Cybersecurity, comprehensive security, data security, digitalisation, know-how, technol-ogy, research and development operations, innovation activity, preparedness, security of supply, international cooperation, cybercrime

ISBN PDF 978-952-383-376-0 **ISSN PDF** 2490-1164
Reference number VN/36693/2023 **Project number** VNK007:00/2024

URN address https://urn.fi/URN:ISBN:978-952-383-376-0

Sisältö

ESIPUHE

Uudistetulla kyberturvallisuusstrategialla vastaamme muuttuneeseen geopoliittiseen tilanteeseen ja teknologiseen kehitykseen. Se jatkaa yli 20-vuotista perinnettä tieto- ja kyberturvallisuudesta huolehtimiselle suomalaisessa yhteiskunnassa. Kyberturvallisuuden tilanne on Suomessa hyvä, mutta jatkuvassa muutoksessa mukana pysyminen edellyttää jatkuvaa parantamista.

Kyberturvallisuus on elintärkeä osa suomalaista kokonaisturvallisuuden mallia. Yhteiskuntamme on lähes täysin digitalisoitunut ja osana luottamusyhteiskuntaa haluamme jatkossakin huolehtia siitä, että suomalaiset voivat luottaa digitaalisten palveluiden kyberturvallisuuteen. Kyberturvallisuus vaatii kaikilta yhteiskunnan toimijoilta johdon vastuuta ja panostusta. Myös EU:n kyberturvallisuusdirektiivi edellyttää entistä voimakkaampaa osallistumista eri yhteiskunnan sektoreilta, jotta kaikki digitaaliset palvelut ovat luotettavia.

Euroopan unioni on Suomen tärkein poliittinen ja taloudellinen viitekehys sekä arvoyhteisö kyberturvallisuudessa. Suurin osa tämänhetkisestä kyberturvallisuussääntelystä ja muista politiikkatoimenpiteistä tulee Euroopan unionista. Suomi on näissä aktiivinen vaikuttaja. Nato-jäsenyytemme vahvistaa Suomen kyberturvallisuutta ja -puolustusta, mutta asettaa myös uusia velvollisuuksia. Haluamme olla vahva kyberturvallisuuskumppani Euroopan unionissa ja Natossa. Tuleva kyberpuolustusdoktriini tulee antamaan kansalliset toimintaperiaatteet valtiollisiin ja valtion turvallisuutta vaarantaviin uhkiin vastaamiseksi. Kansallisesti varaudumme aktiiviseen kyberpuolustukseen sekä attribuoinnin ja vastatoimien mahdollisuuteen.

Strategia on rohkea ja kunnianhimoinen – ja sitä sen on oltava. Suomalaisen kyberturvallisuuden toimintamallin ytimessä on yhteistyö eri toimijoiden välillä. Strategian täytäntöönpano vaatii viranomaisten toimivaltuuksien ja tiedonvaihdon edellytyksien tarkastelua. Viranomaisten ja yksityisen sektorin luottamuksellisesta yhteistyöstä on pidettävä kiinni. Yhteistyöllä ja riittävillä viranomaisresursseilla voimme torjua alati kasvavaa ja monimuotoistuvaa kyberrikollisuutta.

Murrosteknologiat ovat globaali haaste. Meillä on tarvittavaa osaamista nousta johtavaksi kvanttiturvallisuuden yhteiskunnaksi. Toimien aika on nyt. Tämä edellyttää yhä vahvempaa suomalaista kyberturvallisuuden ekosysteemiä ja hallinnon sekä yrityselämän yhteistyötä.

Strategia tähtää kymmenen vuotta eteenpäin, mikä helpottaa tulevia panostuksia strategian toteuttamiseksi. Erilaiset Euroopan unionin ja Naton rahoitusohjelmat muodostavat tärkeän välineen kansallisten kyvykkyyksien kehittämisessä, uudenlaisten vientituotteiden innovoinnissa sekä kansallisen varautumisen tukemisessa.

Eri toimijoiden osallistaminen ja kuuleminen on ollut strategiamme ytimessä. Strategian laatimiseen ovat osallistuneet sadat asiantuntijat, julkisen ja yksityisen sektorin, tiedeyhteisön sekä kansalaisjärjestöjen toimijat. Tämä kuvastaa erinomaisesti suomalaisen yhteiskunnan sitoutumista ja suomalaista kokonaisturvallisuuden mallia.

Pääministeri Petteri Orpo

Lokakuu 2024

1 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 digitalisaation kiihtyminen, uusien teknologioiden kehitys ja niihin liittyvä globaali kilpailu, keskinäisriippuvuuksien jatkuva kasvu ja muut tulevaisuuteen vaikuttavat megatrendit kuten ilmastonmuutos ja väestörakenteen muutos. 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 erityisesti 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. 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), 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. Strategian päivitystarvetta arvioidaan viiden vuoden välein, ja tarvittaessa strategiaa kehitetään tai ajantasaistetaan useamminkin.

Suomi käyttää valtionhallinnon kyberturvallisuuden varmistamiseen tällä hetkellä vuosittain lähes 300 miljoonaa euroa ja elinkeinoelämä tähän verrattuna vähintään kymmenkertaisesti. Tästä huolimatta rahoituksen perustaso ei nykyisellään ole riittävä vastaamaan toimintaympäristön muutokseen.

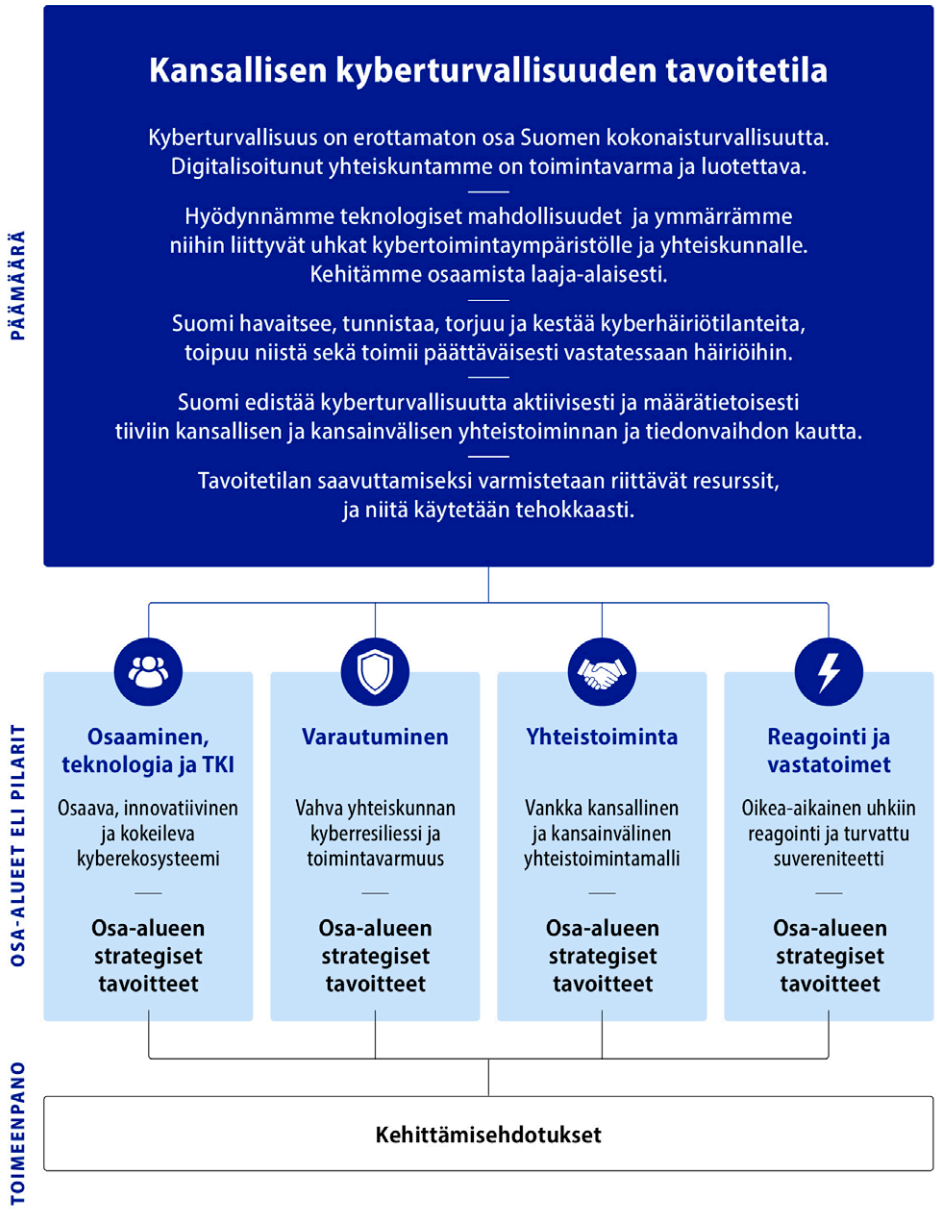
Strategian tavoitetilasta johdetut kehittämisehdotukset toimeenpannaan erillisen toimeenpanosuunnitelman mukaisesti.

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

2 Tavoitetila ja rakenne

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**.

Kuva 1. Kyberturvallisuusstrategian tavoitetila ja strategian rakenne



3 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.

3.1 Haasteena moninaiset uhkat

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 aineettomaan pääomaan voi kohdistua laitonta tiedonhankintaa, mikä uhkaa talouden säilymistä kilpailukykyisenä.

Kybertoimintaympäristöön voivat aiheuttaa häiriöitä myös erilaiset fyysiset uhkat kuten sähkönsaannin häiriöt, tulvat, maanjäristykset, auringon aktiivinen toiminta tai muut luonnonmullistukset sekä inhimillisten virheiden aiheuttamat vahingot. Nämäkin saattavat häiritä tietoliikenneyhteyksiä tai tietojärjestelmien toimintaa ja siten uhata kyberturvallisuutta.

3.2 Suomeen kohdistuva vihamielinen kybertoiminta todennäköisesti lisääntyy

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

Teknisten häiriöiden lisäksi 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 yksilöihin, kasvaa tarve rajat ylittävälle yhteistyölle. Tämän vuoksi oman toimintaympäristön, tietojärjestelmien ja etenkin näiden välisten keskinäisriippuvuuksien tuntemus on entistä tärkeämpää.

3.3 Teknologinen murros lisää kaikkien vastuuta kyberturvallisuudesta

Teknologinen murros ja yhteiskuntien digitalisaatio kasvattavat 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. Murroksellisten teknologioiden kuten tekoälyn, kvanttilaskennan, pilvipalvelujen, 6G-teknologian ja satelliittiteknologioiden nopea kehitys asettaa haasteita kyberturvallisuudelle. Sääntelyllä voidaan edistää turvallisen teknologian kehittymistä. Samaan aikaan, kun turvallisuustoimenpiteitä tehdään, myös hyökkääjät kehittävät uusia tapoja niiden kiertämiseksi.

3.4 Kansainvälinen yhteistyö vahvistaa Suomen kyberturvallisuutta

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

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 sekä viranomaisia että elinkeinoelämää. Osaamis- ja koulutustarpeet sekä kustannukset riittävän suojan rakentamiseksi kasvavat ja edellyttävät lisätoimenpiteitä kyberriskien hallitsemiseksi. Sääntelyllä luodaan edellytykset parantaa yhteiskunnan kriittisten toimijoiden kyberturvaa sekä laitteiden ja ohjelmistojen sisäänrakennettua turvallisuutta. Samalla kehitetään viranomaisten toimintaa varautumisessa ja häiriötilanteissa sekä reagoinnissa ja vastatoimissa.

EU- ja Nato-jäsenyyden rinnalla myös muu 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. YK:ssa ja erilaisissa alueellisissa järjestöissä tunnistetaan kyberturvallisuuden merkitys kansainväliselle turvallisuudelle.

3.5 Kansallista yhteistoimintamallia kehitetään

Kansallinen yhteistoimintamalli 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.

3.6 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 perusoikeuksia, heikentää luottamusta palveluihin ja aiheuttaa merkittäviä taloudellisia menetyksiä. Kyberrikollisuus kytkeytyy yhä enemmän järjestäytyneeseen rikollisuuteen ja valtiollisiin toimijoihin. Vihamielisessä toiminnassa valtiot

hyödyntävät usein 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. Yhteistyöllä ja riittävillä viranomaisresursseilla voidaan torjua myös alati kasvavaa ja monimuotoistuvaa kyberrikollisuutta.

3.7 Toimitusketjujen turvallisuus korostuu

Globaalien 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 niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia.

3.8 Kyberturvallisuus mahdollistaa liiketoiminnan kasvun

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

4 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 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 kyberturvallisuuden alalla voidaan nähdä kansainvälisenä käyntikorttina ja potentiaalisena vientituotteena.

4.1 Kyberturvallisuus ja yhteiskunnan digitalisaatiokehitys

Suomen digitaalinen kompassi (digikompassi) on vuoteen 2030 ulottuva kansallinen strateginen etenemissuunnitelma Suomen digitalisaatiokehitykselle. Digikompassin 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.

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. Tekoälyteknologian mahdollistamat uudet huijaustavat ovat jo nyt uhka niin kyber- kuin informaatioympäristöllekin. Uhka uusille vakaville ja laajemmillekin vaikutuksille on olemassa.

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. Henkilötietojen tietoturvaloukkausten vaikutukset ihmisten hyvinvointiin ja luottamukseen yhteiskunnan toimivuuteen voivat olla mittavia. Nämä korostavat entisestään riittävien resurssien kohdentamista kyberturvallisuuteen sekä yhteistyön ja yhteisten menettelytapojen tärkeyttä.

4.2 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.

4.3 Kyberturvallisuus huomioitava hyvinvointialueilla ja kunnissa

Viimeisin merkittävä hallinnollinen uudistus oli vuoden 2023 alussa toimintansa aloittaneiden itsehallinnollisten hyvinvointialueiden muodostaminen. Muutos vaikutti merkittävästi myös alueiden krittiseen infrastruktuuriin ja julkisiin palveluihin. Hyvinvointialueet vastaavat palveluistaan ja niihin liittyvästä kyberturvallisuudesta. Kuntakentällä taas kyberturvallisuuden taso on keskimäärin heikompi kuin valtion- ja aluehallinnossa, mutta kuntatoimijoiden koossa ja resursseissa on eroja. Sekä hyvinvointialueet että kunnat tarvitsevat kyberturvallisuuden varmistamiseksi nykyistä enemmän tukea, kuten keskitettyjä kyberturvallisuuspalveluja. Kyberuhkiin vastaamisen on toimittava saumattomasti eri kokoisten toimijoiden välillä ja oikea-aikaisesti kaikilla julkisen hallinnon tasoilla.

4.4 Yhteistyöllä rakennetaan luottamusta

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. Viranomaistoiminta on oltava luotettavaa ja palvelut on turvattava kaikille – kansalaisia on kohdeltava yhdenvertaisesti ja varmistettava, että digitaaliseen teknologiaan ja palveluihin voivat luottaa sekä käyttäjät että palvelujen tarjoajat. Esimerkiksi väestörakenteen muutos asettaa yhteiskunnalle haasteita. On varmistettava, että digitalisaatio on inhimillistä ja kuuluu jokaiselle.

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.

4.5 Kvanttiteknologian nopea kehittyminen haastaa kansallista salauskyvykkyyttä

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 kvanttiteknologian kehitystyötä ja sen hyödyntämistä.

4.6 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 kyberturvallisuusalan yritysten kykyjen hyödyntämisen ja tiiviin yhteistyön keskeinen merkitys kyberturvallisuuden ja yhteiskunnan kriittisen infrastruktuurin toiminnan varmistamisessa valtiollisia uhkia vastaan.

Kyberturvallisuutta vaarantavassa tilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Siitä huolimatta, että yhteistyö on jo nykyisellään toimivaa, viranomaisilla on kuitenkin arvioitu olevan nykytilassa riittämättömät toimintaedellytykset tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Kyberturvallisuuden yhteistoiminnalle tuovat haasteita sääntelyn ja tehtävien hajautuminen usealle eri toimijalle sekä yhteistoiminnan erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute. 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. Tästä syystä 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 tilannekuvaa 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 eri 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.

5 Pilarit ja niiden strategiset tavoitteet

KANSALLISEN KYBERTURVALLISUUDEN TAVOITETILA

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.

5.1 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.
- Jokainen tuntee kyberturvallisuusvastuunsa.
- Suomi ottaa käyttöön murrosteknologioiden hyödyt, ja edellyttää laitteisiin, ohjelmistoihin 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.

Kyberturvallisuuden ekosysteemi kehittyy

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. Kestävän talouskasvun mahdollistamiseksi uhkien ja mahdollisuuksien tasapaino haetaan yhteistyössä kyberturvallisuuden ekosysteemin toimijoiden kanssa.

Vahva kotimainen kyberturvallisuusalan tutkimus-, kehitys- ja innovaatiotoiminta (TKI) ja menestyvä yritystoiminta ovat keskeisiä toimivan kyberturvallisuuden ekosysteemin kehittämiseksi ja ylläpitämiseksi. Tämä on tarpeen myös yhteiskunnallisen toimintavarmuuden ja kilpailukyvyn vahvistamiseksi.

Osaaminen on kaikilla tasoilla vahvaa

Kokonaisuudessaan suomalainen kyberturvallisuusosaaminen varmistetaan vahvistamalla kyberturvallisuuden roolia laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla. Kouluissa opettajien valmiuksia kasvattaa oppilaita kriittiseen medialukutaitoon sekä tietoisuuteen kyberriskeistä on vahvistettava laajan yhteiskunnallisen resilienssin eli kriisinkestävyyden lujittamiseksi. Tavoitteisiin pääsemiseksi kyberturvallisuus on huomioitava digitaalisen osaamisen osana opetussuunnitelmia laadittaessa ja opettajien kyberturvallisuusosaamista on edistettävä. Kansalaisjärjestöillä on merkittävä rooli yksilöiden osaamisen kehittämisessä koulupolun jälkeen. Kyberosaajien koulutukseen tähtäävän tutkintokoulutuksen ohella kehitetään mahdollisuuksia osaamisen kehittämiseen jatkuvan oppimisen tarjontaa vahvistamalla. Organisaatioiden vastuulliseen toimintaan kuuluu kehittää henkilöstön osaamista, tunnistaa uhkat, reagoida haitalliseen toimintaan ja ilmoittaa häiriöistä kybertoimintaympäristössä.

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 ja osaamisen jakaminen.

Kaikki yksittäiset ihmiset, yritykset ja yhteisöt hyötyvät turvallisesta toimintaympäristöstä, jonka ennakoitavuus paranee osaamisen kehittymisen myötä. Samalla Suomen kiinnostavuus niin investointikohteena kuin osaamisen keskittymänä kasvaa.

Jokainen tuntee kyberturvallisuusvastuunsa

Kyberturvallisuusosaaminen kuuluu kansalaistaitoihin, ja jokainen voi omalla toiminnallaan myötävaikuttaa yhä turvallisemman kybertoimintaympäristön syntyyn. Kyberturvallista arkea voidaan tukea muun muassa vahvistamalla medialukutaitoa ja lisäämällä tietoisuutta hyvästä kyberhygieniasta. Kyberhygienia eli hyvien tietoturvakäytänteiden noudattaminen osana päivittäisiä rutiineja tuleekin nähdä

luonnollisena osana jokaisen yksilön yhteiskuntavastuuta. Vastuullisesti kybertoimintaympäristössä toimivat ihmiset lisäävät merkittävällä tavalla myös yhteisöjen ja organisaatioiden turvallisuutta.

Yhteiskunnan on varauduttava murroksellisten teknologioiden kehitykseen

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 tulee huomioida kaikessa teknologioita koskevassa kansallisessa säädösvalmistelussa sekä EU-ennakkovaikuttamisessa.

EU:n uuteen kyberlainsäädäntöön kytkeytyy standardointi- ja sertifiointityö. Suomen etu on olla aktiivinen toimija kyberturvallisuuden standardien ja sertifiointijärjestelmien kehittämisessä sekä käyttämisessä. Samalla on tärkeää hyödyntää aihealueen tarjoamia liiketoimintamahdollisuuksia.

Murrokselliset teknologiat kuten tekoäly ja kvanttiteknologia sekä uudet matkaviestinverkkosukupolvet tuovat mukanaan uudenlaisia ja vielä tuntemattomiakin kyberturvallisuusuhkia. Lisäksi näiden teknologioiden yhteisvaikutukset ovat erittäin vaikeasti ennakoitavissa. Näihin haasteisiin vastaaminen edellyttää syvää ja monipuolista teknologista osaamista ja yhteiskunnallisten muutosten jatkuvaa seurantaa ja arviointia. Esimerkiksi kvanttiteknologian kehittymisen vaikutuksiin on syytä valmistautua jo nyt.

Kyberturvallisuusalan yritysten kilpailukykyä edistetään

Kyberturvallisuuden 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, EU:n Horisontti Eurooppa ja Digitaalinen Eurooppa (DEP) -puiteohjelmiin tai Euroopan puolustusrahastojen ohjelmiin lisäävät Suomen tunnettuutta korkean teknologian ja kyberturvallisuuden osaajana ja parantavat suomalaisten yritysten liiketoimintamahdollisuuksia kansallisesti ja kansainvälisesti. Suomen on tärkeää vaikuttaa aktiivisesti jo suunnitteluvaiheessa näiden ohjelmien sisältöihin. 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 vahvistavien ratkaisujen kehittämistä ja hyödyntämistä sekä niitä kaupallistavien yritysten kansainvälistä kilpailukykyä. Samalla edistetään sekä Suomen kyberturvallisuusalan että laajemmin turvallisen TKI- ja liiketoimintaympäristön houkuttelevuutta suomalaisille ja ulkomaisille osaajille, yrityksille ja investoinneille.

Kyberturvallisuuden tietopääoma on suojattu

Julkisen ja yksityisen sektorin kriittinen tietopääoma on tunnistettava ja suojattava. 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 luottamuksellisuus, eheys ja saatavuus 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.

5.2 Pilari II: Varautuminen

Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus

OSA-ALUEEN STRATEGISET TAVOITTEET:

- Yhteiskunnan elintärkeät toiminnot, kriittinen infrastruktuuri, julkiset palvelut sekä huoltovarmuuskriittiset toimijat ovat kybersietoisia.
- Yksilöt, yritykset, yhteisöt ja viranomaiset ovat yhdessä varautuneet kyberhäiriöihin ja -uhkiin.
- 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. Yhteiskunnan toimivuuteen on voitava 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 toimivuus ja häiriönsietokyky. Elintärkeät toiminnot sisältävät muun muassa kybertoimintaympäristön kannalta kriittisen infrastruktuurin, tietovarannot, julkiset palvelut sekä huoltovarmuuden. 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.

Julkisen hallinnon on huomioitava toimintaympäristön muutokset asettaessaan yrityksille varautumisvaatimuksia turvallisuuden näkökulmasta ja tukiessaan yritysten varautumista. Toimivuuden varmistamisessa ja häiriönsietokyvyn kehittämisessä

tärkeää on erityisesti kyberharjoitustoiminnan kehittäminen ja ulottaminen entistä laajemmalle huomioiden palvelu- ja toimitusketjujen kyberturvallisuus sekä erilaiset keskinäisriippuvuudet. Turvalliset tietojärjestelmät luovat perustaa kybersietoiselle yhteiskunnalle. 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 voivat luottaa 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 on edellytettävä kyberturvallisuuden, tietoturvallisuuden ja tietosuojan vaatimustenmukaisuutta koko elinkaaren ajan. Julkisten palveluiden vaatimustenmukaisuuden arviointia ja hyväksyntää sekä arviointikriteeristöjä on kehitettävä ja selkeytettävä ja tarpeellisin osin velvoitettava. Lisäksi teknisen ympäristön automaattista seurantaa ja valvontaa on tärkeää kehittää ja siihen velvoittaa. On varmistettava, että palvelujen toimivuus priorisoidaan tilanteen mukaisesti, potentiaalisiin häiriötilanteisiin varaudutaan ja häiriöiden vaikutukset viranomaisten ja yhteiskunnan toimintaan kyetään minimoimaan.

Varautumista tehdään yhteistyössä

Kyberturvallisuuden varautumistyötä tehdään tiiviissä yhteistyössä kokonaisturvallisuuden mallin mukaisesti. Kyberuhkien tunnistamisen ja niihin varautumisen on pohjauduttava systemaattiseen tiedolla johtamiseen ja yhteiseen tilanneymmärrykseen, jonka perustan muodostavat ennakointi, havainnointi, 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 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.

Käyttäjien on voitava luottaa palvelujen turvallisuuteen ja heillä on oltava riittävä osaaminen tunnistaa väärennetyt palvelut ja huijaukset. Tekoälyn kehittyminen tekee kyberrikollisuudesta aiempaa kohdennetumpaa ja vaikuttavampaa. Jatkossa onkin yhä tärkeämpää tunnistaa niin tekoälyn kuin muidenkin murrosteknologioiden vaikutukset kyberturvallisuuteen ja kehittää keinoja vastata niihin.

Kyberrikollisuuteen liittyvistä uhkista on viestittävä ymmärrettävästi ja ohjeistettava ja neuvottava oikeista toimintatavoista. Yksilöihin 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, alue- ja paikallishallinnon, hyvinvointialueiden sekä 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, aluehallinnon, hyvinvointialueiden ja kuntien sekä yritysten ja yhteisöjen kanssa.

Valtioneuvostossa yhteisiä strategisen tason kyberturvallisuuden johtamisen resursseja on keskitetty valtion kyberturvallisuusjohtajan toimistoon. Muita keskitettyjä kyberturvallisuustehtäviä hoitavia viranomaisia resursoidaan niille säädettyjen tehtävien mukaisesti. Lisäksi aluehallinnossa, hyvinvointialueilla ja kunnissa on soveltuvin osin edistettävä kyberturvallisuustehtävien keskittämistä 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 tarvitsemat toimintamallit on toteutettava.

Harjoitustoimintaa kehitetään

Kyberharjoitustoiminnalla rakennetaan koko yhteiskunnan vahvaa kyberresilienssiä. Kyberharjoitusten ympäristöjä ja toimintamalleja on jatkuvasti kehitettävä vastaamaan toimintaympäristön muutosta. Organisaatioita kannustetaan kehittämään pitkäjänteisesti omaa harjoitustoimintaa, tarvittaessa viranomaisten tuella.

Kansallisesti tunnistetaan erityisesti eri toimialojen välisen harjoittelun merkityksen ja lisäämisen tärkeys. Kansallisten kyberharjoitusten avulla simuloidaan erilaisia kyberhäiriötilanteita eli luodaan olosuhteet, joissa kyberhäiriöiden vaikutuksia voidaan tunnistaa ja niistä toipumista testata ja harjoitella. Harjoitukset kehittävät osaamista sekä yksilöiden ja organisaatioiden valmiutta ja kykyä varautua erilaisiin kyberhäiriöihin ja uhkiin. Aktiivinen ja säännöllinen harjoittelu normaalioloissa vahvistaa osaamista kaikissa tilanteissa.

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

Yhteiskunnan toimivuuden kannalta on tärkeää, että avaruuspalvelut kuten aika- ja paikkatiedot, tietoliikenne ja kaukokartoitus ovat käytettävissä. Avaruusjärjestelmien kyberturvallisuutta seurataan osana avaruustilannekuvaa. Avaruusjärjestelmien kyberturvallisuus tulee huomioida myös avaruuslupaehdoissa ja järjestelmien elinkaarenhallinnassa. Potentiaalisiin häiriötilanteisiin sekä niistä

toipumiseen voidaan varautua ja häiriöiden vaikutukset viranomaisten ja yhteiskunnan toimintaan minimoida vaihtoehtoisten toimintamallien ja varajärjestelyjen avulla.

5.3 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 saumattomasti.
- Julkinen sektori yhdessä yksityisen sektorin kanssa kehittää ja tarjoaa keskitettyjä kyberturvallisuuspalveluja.

Suomi vaikuttaa ja osallistuu aktiivisesti yhteistyöhön

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

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 vaikutusten arviointiin ja toimeenpanoon, sekä viranomaisten riittävään resursointiin on kiinnitettävä huomiota.

Suomi EU:n ja Naton jäsenenä

Euroopan unioni on Suomen tärkein poliittinen ja taloudellinen viitekehys ja arvoyhteisö. Suomi osallistuu ja vaikuttaa aktiivisesti EU:n kyberturvallisuustyöhön, mukaan lukien EU:n kyberturvallisuusvirasto ENISAn ja Euroopan kyberturvallisuuden kompetenssikeskuksen ECCC:n toiminta. Vaikuttamalla EU:ssa Suomi edistää kokonaisturvallisuuden kannalta tärkeitä hankkeita ja päätöksiä, jotka kehittävät unionin ja sen jäsenmaiden varautumista. Tämä pätee myös kyberturvallisuuden osa-alueella.

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 ja vahvistaa siten häiriösietoisuutta kyberympäristössä. Keskeisenä tuloksena on EU:n strategisen autonomian saavuttaminen ja avoimen talouden säilyttäminen.

Suomi on rakentava, luotettava ja suorituskykyinen Nato-liittolainen. Suomi ylläpitää vahvaa kansallista puolustuskykyä osana Naton yhteistä pelotetta ja puolustusta ja osallistuu aktiivisesti Naton kyberpuolustuksen kehittämiseen. Naton jäsenenä Suomi pyrkii kybersuorituskykyjen kehitystyön ytimeen. Tavoitteena on olla merkittävä liittokunnan ratkaisujen tuottaja kyberturvallisuudessa ja kyberpuolustuksessa.

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.

Kyberturvallisuuteen ja -puolustukseen liittyvät kansalliset EU- ja Nato-kannat on tärkeää sovittaa yhteen. EU:n ja Naton kybertoimien keskinäinen yhteensopivuus täydentää ja vahvistaa sekä kansainvälistä kyberturvallisuutta että Suomen kansallista kyberturvallisuutta.

Tiedonvaihtoon perustuva yhteinen tilanneymmärrys toiminnan perustana

Tiivis yhteistyö, tilannekuvan ja -ymmärryksen muodostaminen sekä tiedonhankinnan edellytysten varmistaminen ovat keskeisiä tavoitetilan saavuttamiseksi. Tiedonvaihtoon perustuva yhteinen tilanneymmärrys mahdollistaa viranomaisten, yritysten ja yhteisöjen välisen tehokkaan ja luotettavan yhteistoiminnan kybertoimintaympäristössä. Tämä lisää luottamusta ja tukee sektorivastuiden toteuttamista.

Kybertoimintaympäristön havainnoinnin osalta on tarve systematisoida tietojen kokoamista siten, että tiedon pohjalta voidaan muodostaa 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.

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 jakelurajoitteet huomioiden. Julkisten palvelujen osalta tarvitaan nykyistä parempia keinoja ja edellytyksiä kerätä, analysoida ja jakaa tietoa kyberturvallisuuden ja kyberresilienssin tasosta.

Korkeasti turvallisuusluokitellun tiedon jakaminen edellyttää siihen soveltuvien järjestelmien kehittämistä ja käyttöönottoa. Viranomaisten välisen tiedonvaihdon kehittämisessä tulee huomioida vuonna 2022 tehty selvitys viranomaisten toiminta-edellytyksistä kyberturvallisuudesta.

Viranomaisten yhteistoiminta on sujuvaa ja saumatonta

Operatiivisen yhteistyön toimeenpanoa, vastuita sekä vakaviin kyberuhkiin ja -häiriöihin varautumista ja niihin vastaamista koordinoidaan nykyistä tiiviimmässä ja osallistavammassa virastotason yhteistyörakenteessa, jonka muodostavat Liikenne- ja viestintävirasto Traficom, keskusrikospoliisi, Puolustusvoimat sekä suojelupoliisi. Koordinaatio perustuu yhteiseen jaettuun tilanneymmärrykseen. Yhteistyörakenteella ja siihen kuuluvilla viranomaisilla on oltava riittävät tiedon luovutus- ja saantioikeudet. Yhteistoimintarakenne johtaa tarpeeseen myös tiivistää viranomaisten yhteistoimintaa taktisella ja teknisellä tasolla.

Kyberturvallisuuden toimintakulttuuria tulee uudistaa kokonaisturvallisuuden mallin mukaisesti vahvistamalla kansainvälistä sekä kansallista valtionhallinnon, aluehallinnon, hyvinvointialueiden, kuntien, 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

Tällä hetkellä keskitettyjä kyberturvallisuuspalveluja tarjoavat Liikenne- ja viestintävirasto Traficom, Digi- ja väestötietovirasto, muut valtionhallinnon toimijat sekä hyvinvointialueiden ja kuntien omistamat yritykset yhdessä yksityisen sektorin kanssa. Näitä palveluja ovat esimerkiksi Traficomin tuottamat vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO ja hyökkäyspinta-alan

kartoituspalvelu HYÖKY sekä DVV:n tarjoamat tieto- ja kyberturvallisuuden verkkokoulutukset. Keskitettyjä palveluja käyttävät valtionhallinto, alue- ja paikallishallinto, hyvinvointialueet ja kunnat sekä soveltuvin osin yritykset, yhteisöt, korkeakoulut ja tutkimuslaitokset.

Keskitettyjen kyberturvallisuuspalvelujen kehittämisen ja käytön koordinaatiota edistetään. Keskitettyjen palvelujen on oltava toimintavarmoja, kustannustehokkaita, suorituskykyisiä ja käyttäjäystävällisiä. Yhteistyön tavoitteena on välttää päällekkäisyyksiä ja tuottaa yhteiseen käyttöön tarkoitettuja aineistoja ja koulutuksia sekä tietoa ja palveluja.

5.4 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.

Mahdollisuudet ja kyvyt vastata kyberuhkiin varmistetaan

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.

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

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 kyberuhkista. Kyberuhkien luonne asettaa vaatimuksia viranomaisten 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.

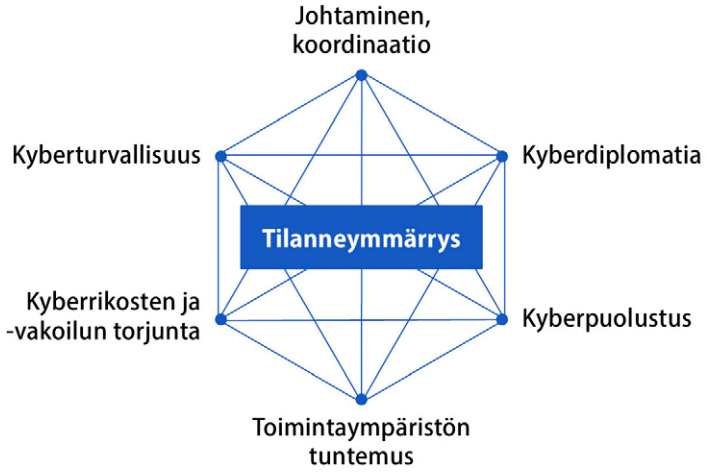
Kokonaisvaltaisen ja laajan keinovalikoiman hyödyntämisen mahdollisuudet korostuvat etenkin valtiollisiin operaatioihin ja vakavaan kyberrikollisuuteen vastaamisessa. Uudessa toiminta ja -uhkaympäristössä roolien ja vastuiden määrittäminen pelkästään toimintojen ja infrastruktuurin teknisen tai toiminnallisen 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 koordinaatiomallia 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. Reagoinnin ja vastatoimien koordinaatiomalli muodostetaan edellä III pilarissa kuvatussa virastotason yhteistyörakenteessa. Yhteinen tilanneymmärrys varmistaa koordinoidut toimet kunkin viranomaisen omalle toiminnalle. 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 eli syyksilukemisen ja vastatoimien tukena.

Kansallista attribuutiotoimintaa kehitetään

Suomi kehittää kansalliset suuntaviivat ja prosessin tavoitteelliselle ja johdonmukaiselle kyberattribuutiotoiminnalle, huomioiden keskeiset liittolaiset ja kumppanit. Attribuutio on tosiseikkojen keräämistä ja analyysiä, teknistä, oikeudellista ja poliittista 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, liittokunnan ja kumppanien kyvykkyydet. 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 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 koko kansallista keino- ja suorituskykyvalikoimaa tarkoituksenmukaisesti. 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.

6 Resursointi, toimeenpano ja seuranta

6.1 Resursointi

Suomessa kyberturvallisuuden toimijat torjuvat uhkia joka päivä. Toimintaympäristön muutos kasvattaa ja monimuotoistaa kyberuhkia ja -riskejä. Kyberturvallisuuden tämänhetkinen resursointi on ollut tarpeisiin nähden riittämätöntä jo nykytilankin ylläpitämiseksi. Kyberturvallisuuden varmistaminen ja vahvistaminen muuttuneessa toimintaympäristössä sekä uuden lainsäädännön toimeenpano ja valvontatehtävät eri toimialoilla vaativat tulevaisuudessa uutta resursointia.

Tällä hetkellä Suomi käyttää valtionhallinnon kyberturvallisuuden varmistamiseen vuosittain lähes 300 miljoonaa euroa. Tämän lisäksi aluehallinto, hyvinvointialueet ja kunnat sekä paikallishallinto käyttävät resursseja omaan kyberturvallisuuteensa, mutta niiden käytön seurantaa on vielä kehitettävä. Huomionarvoista on, 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 ovat yhä tärkeämpiä. Kyberturvallisuuteen investoidaan myös välillisesti. Esimerkiksi kyberosaamiseen panostetaan Suomessa kaikilla koulutusasteilla ja erilaisissa tutkimushankkeissa. Kyberkoulutukseen ja -tutkimukseen sijoitettu euro näkyy kyberturvallisuuden vahvistumisessa usein vasta myöhemmin.

Valtiontalouden tämänhetkiset haasteet, teknologinen korjausvelka ja kyberturvallisuusalan osaamisvajeesta johtuva 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 kyberturvallisuusalan kansalliselle kasvulle.

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.

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 tai mainehaitoista aiheutuneet seuraukset.

Resurssien käyttöä voi tehostaa osaamisen sekä resurssien ketterä jakaminen viranomaisten yhteistoiminnassa. Viranomaisen tulisi esimerkiksi voida sopia jonkin kyberturvallisuustehtävän hoitamisesta toisen viranomaisen lukuun, jos se katsotaan tarkoituksenmukaiseksi.

Resursseista ja niiden kohdentamisesta ja yhteensovittamisesta päätetään valtion talousarvioita koskevin päätöksentekoprosessein, ja ne määräytyvät julkisen talouden suunnitelmien ja valtion talousarvioiden mukaisten määrärahojen ja henkilötyövuosimäärien puitteissa.

6.2 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.

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. Toimeenpanosuunnitelma hyväksytään valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämishankkeen valtiosihteereistä koostuvassa ohjausryhmässä. Strategian seurannasta raportoidaan valtiosihteerien ohjausryhmän lisäksi yhteiskunnan uudistamisen ministerityöryhmälle ja etenemisestä informoidaan myös sisäisen turvallisuuden ja oikeudenhoidon ministerityöryhmää sekä Turvallisuuskomiteaa.

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 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.

7 Strategiset kehittämisehdotukset

Strategian perusteella laaditaan aikataulutettu ja vastuutettu toimeenpanosuunnitelma. Sen toimeenpanolla on tarkoitus viedä käytäntöön pilarien strategiset tavoitteet. Alla on listattu keskeiset strategiatyössä tunnistetut kehittämisehdotukset, joita tarkennetaan ja tarvittaessa täydennetään toimeenpanosuunnitelmassa. Jokaiseen kehittämistoimeen liittyy olennaisesti säädösten ja normien arviointi, mikä voi johtaa säädösten purkamiseen tai täsmentämiseen. Alla oleva jako pilareihin on viitteellinen, sillä useat kehittämistoimet jakautuvat useamman kuin yhden pilarin alle.

7.1 PILARI I: Osaaminen, teknologia ja TKI

- Kehitetään julkisen ja yksityisen sektorin huippuosaamista ja työelämätaitoja sekä kansalaisten ja kansalaisyhteiskunnan kybervalmiuksia ja varautumista.
- Varaudutaan uusien murrosteknologioiden kehittymisen tuomiin uhkiin ja mahdollisuuksiin, ja huomioidaan ne ennakointityössä ja teknologioiden käyttöönotossa ja hyödyntämisessä.
- Edistetään kyberturvallisuuden ekosysteemin ja teknologisen suvereniteetin kehittämistä vahvistamalla kotimaisen kyberturvallisuusalan TKI- ja yritystoimintaa. Hyödynnetään kansalliset ja kansainväliset yhteistyö- ja rahoitusmahdollisuudet.
- Huomioidaan järjestöjen mahdollisuudet viestiä ja ohjeistaa kansalaisia kyberturvallisuudesta.

7.2 PILARI II: Varautuminen

- Syvennetään kyberturvallisuuden toimijoiden yhteistä varautumista osana kokonaisturvallisuuden mallia.
- Arvioidaan kyberturvallisuusnäkökulmia kaikissa lainsäädäntöhankkeissa.

- Suunnitellaan ja seurataan julkisen hallinnon kyberturvallisuusresursseja pitkäjänteisesti.
- Hyödynnetään kyberturvallisuuden ja tietoturvallisuuden standardeja yhteisten toimintatapojen ja kriisinkestävyyden kehittämiseksi kybertoimintaympäristössä ja vaikutetaan aktiivisesti kansainväliseen standardointiin.
- Kehitetään organisaatioiden toimintaan sekä tietojärjestelmiin liittyviä arviointi- ja hyväksymismenetelmiä sekä niihin liittyviä vaatimuksia.
- Kehitetään harjoitustoimintaa ja harjoitusympäristöjä varautumisen ja osaamisen lisäämiseksi.

7.3 PILARI III: Yhteistoiminta

- Kirkastetaan Suomen kansainvälistä asemoitumista kyberturvallisuudessa ja kyberpuolustuksessa, kehitetään osallistumista kansainväliseen kyberturvallisuuden yhteistoimintaan, vakiinnutetaan tätä varten tarvittava kansallinen koordinaatio.
- Vahvistetaan turvallisuusviranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset. Tähän liittyen toteutetaan vuonna 2022 tehdyssä selvityksessä viranomaisten toimintaedellytyksistä kyberturvallisuudessa esitetyt kehittämistoimet.
- Vahvistetaan julkisen hallinnon, yksityissektorin ja kansalaisyhteiskunnan yhteistoimintaa, tiedonvaihtoa ja yhteistä tilanneymmärrystä kyberturvallisuudessa kokonaisturvallisuuden toimintamallin mukaisesti.
- Ylläpidetään ja parannetaan luottamusta turvallisilla ja toimintavarmoilla julkisilla palveluilla.

7.4 PILARI IV: Reagointi ja vastatoimet

- Kehitetään hyvinvointialueiden ja kuntien sekä yksityisen sektorin valmiuksia ja kykyä varautua ja reagoida oikea-aikaisesti kyberhäiriöihin.
- Kehitetään toimintaympäristötuntemusta muun muassa turvaamalla kansallinen havainnointikyky sekä turvallisuus- ja

tiedusteluviranomaisten mahdollisuudet tietojen hankkimiseksi kybertoimintaympäristöstä.
- Edistetään kokonaisvaltaista kyberrikollisuuden torjuntaa.
- Kehitetään kyberpuolustusta osana kokonaismaanpuolustusta, Suomen valtiollisen suvereniteetin turvaamista kybertoimintaympäristössä ja integroitumista liittokunnan puolustukseen.

8 Käsitteet ja määritelmät

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.

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.

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.

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.

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.

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.

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.

Kyberresilienssi; ~kybersietoisuus

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

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.

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.

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.

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.

Resilienssi; ~kriisinkestävyys; ~kriisinsietoisuus

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

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.

Yhteiskunnan elintärkeä toiminto

Toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta.

Yhteiskunnan elintärkeä toiminto

Toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta.

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 eli hyvinvointialueille ja kuntiin, kansainväliset kumppanit huomioiden.

Kokonaisturvallisuuden toimintamallissa yhteiskunnan elintärkeät toiminnot turvataan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistoiminnalla kaikissa olosuhteissa ja kaikilla tasoilla. 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 palvelun-tuottajille 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. Ulko- ja turvallisuuspoliittisesti merkittävien asioiden kannalta keskeinen toimielin on tasavallan presidentin ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta (TP-UTVA).

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-direktiivin täytäntöönpanevan kansallisen lainsäädännön määrittämiä valvovia viranomaisia NIS2-direktiivi pannaan Suomessa täytäntöön kyberturvallisuuslailla sekä julkisen hallinnon tiedonhallinnasta annetulla lailla. Valvovat viranomaiset valvovat laissa säädettyjen tehtävien noudattamista yksityisellä ja julkisella sektorilla. 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 terveysalan 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.

Onnettomuustutkintakeskus on viranomainen, joka voi tutkia tapahtumaa turvallisuustutkinnan keinoin, mikäli kyberturvallisuuteen liittyvä häiriötilanne aiheuttaa ihmishengen menetyksiä tai huomattavia taloudellisia tai materiaalisia vahinkoja. Turvallisuustutkinnan tarkoituksena on mahdollistaa vastaanvankaltaisten tapahtumien välttäminen, tapahtumista oppiminen sekä ennakoivan turvallisuuskulttuurin kehittäminen.

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. Lisäksi Kyberturvallisuuskeskus tekee laajaa luottamukseen perustuvaa operatiivista yhteistyötä ja tiedonvaihtoa keskeisten kansallisten ja kansainvälisten verkostojen kanssa. Kyberturvallisuuskeskuksessa toimii Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen Suomen kansallinen koordinointikeskus (NCC-FI).

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 estämään ennalta mahdollisia

tulevia rikoksia. Poliisi ylläpitää tietoverkkorikosten kansallista tilannekuvaa. 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

Keskus-, alue- ja paikallishallinnolla, hyvinvointialueilla, kunnissa sekä itsenäisillä laitoksilla on keskeinen rooli huolehtia kyberturvallisuudesta viranomaisten päivittäisessä toiminnassa. Toimijoihin kuuluvat valtion virastot, liikelaitokset ja yhtiöt, aluehallinnon toimijat, hyvinvointialueet, kunnat ja kuntayhtymät, hyvinvointialueiden ja kuntien omistamat yhtiöt 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. Kriittisen infrastruktuurin ja huoltovarmuuden turvaaminen osana yhteiskunnan elintärkeitä toimintoja on keskeistä yhteiskunnan toimintakyvyn ja jatkuvuudenhallinnan 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. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä useiden alueellisten toimikuntien kanssa.

Huoltovarmuusorganisaatio ylläpitää ja kehittää Suomen huoltovarmuutta yhteistyössä julkisen sektorin, useiden satojen yritysten, järjestöjen ja kolmannen sektorin toimijoiden kanssa. Tavoitteena on turvata huoltovarmuuden kannalta kriittisten organisaatioiden ja sitä kautta koko yhteiskunnan toimintaedellytykset kaikissa olosuhteissa.

Valvottavat toimijat (NIS2)

NIS2-direktiivin mukaisia riskienhallinta- ja poikkeamaraportointivelvoitteita sovelletaan yhteiskunnan toiminnan kannalta kriittisillä toimialoilla toimiviin, direktiivissä määriteltyihin keskeisiin ja tärkeisiin toimijoihin, joiden koon on yleensä ylitettävä tietyt kynnysarvot. Näihin tahoihin viitataan tässä valvottavina toimijoina.

NIS2-direktiivin liitteissä I ja II on lueteltu toimijatyypit, jotka kuuluvat direktiivin soveltamisalaan. Direktiivin soveltamisala kattaa seuraavat toimialat: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, TVT- eli tieto- ja viestintätekniikan palveluiden hallinta, julkishallinto ja avaruus (liite I) sekä posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden teollinen tuotanto, jalostus ja tukkukauppa, valmistus, digitaalisen palvelun tarjoajat ja tutkimustoiminta (liite II).

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 kyberturvallisuuslain mukaisesti tai sopimusperusteisesti.

Palveluntuottajia ovat myös tutkimuslaitokset ja korkeakoulut sekä osa kansalaisjärjestöistä. Ne tuottavat kyberturvallisuuden osaamis- ja tietopääomaa ja innovaatioita sekä tukea varautumiseen ja kriiseistä palautumiseen.

Järjestöt ja neljännen sektorin toimijat

Suomi tunnetaan maailmalla lukuisista kansalaisjärjestöistään ja ihmisten suuresta halusta osallistua kansalaisyhteiskunnan toimintaan. Kansalaisjärjestöjen ja vapaaehtoisten merkitys 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. Läheisille tarjottava tuki ja oikea-aikainen ilmoittaminen omista havainnoista edesauttavat kansallisen kyberresilienssin ylläpitämisessä ja kehittämisessä sekä kyberrikosten selvittämisessä.

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

SNELLMANINKATU 1, HELSINKI
PL 23, 00023 VALTIONEUVOSTO
p. 0295 16001
info.vnk@gov.fi
vnk.fi/julkaisut

ISBN pdf: 978-952-383-376-0
ISSN pdf: 2490-1164