Digitaalinen turvallisuus 2030 -ohjelma

Väliraportti 2021–2023

Huoltovarmuuskeskus

Huoltovarmuuskeskus

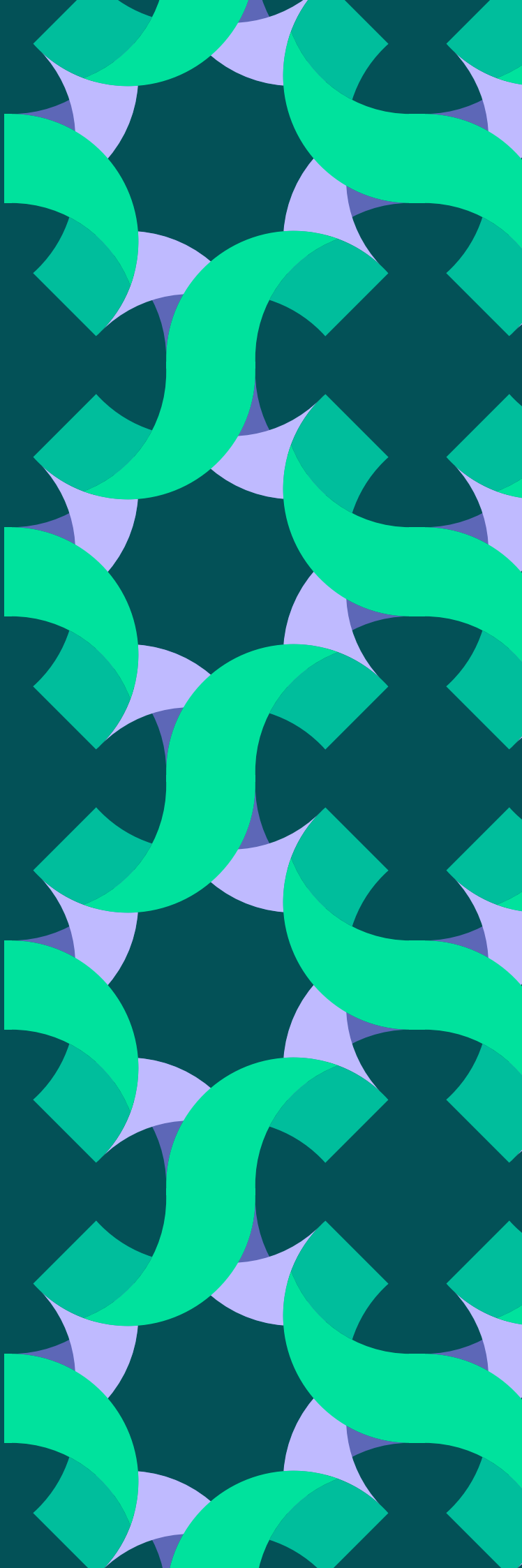
www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuusorganisaatio (HVO) on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä alueellisten toimikuntien kanssa.

Julkaisija: Huoltovarmuuskeskus
Laatinut: Juha Ilkka
Kansikuva: Getty Images
Taitto: LM Someco Oy
Julkaisuvuosi: 2025
ISBN: 978-952-7470-43-5



Sisältö

Yhteenveto

Huoltovarmuuskeskuksen tehtävä on rakentaa yhdessä julkisen sektorin, elinkeinoelämän sekä kolmannen sektorin kanssa kriisinkestävää yhteiskuntaa, jotta myös kriisitilanteissa yhteiskunta toimii ja elämä jatkuu mahdollisimman häiriöttä. HVK:n ohjelmakokonaisuus on työväline strategisten tavoitteiden saavuttamiseksi organisaation tavanomaisen toiminnan rinnalla. Ohjelmatyön avulla kehitetään huoltovarmuustyötä vastaamaan yhteiskunnan ja talouden suurten murrosten vaikutuksiin. Strategiakaudella 2021–2023 HVK:n ohjelmakokonaisuuteen kuuluivat Alue 2030, Digitaalinen turvallisuus 2030, Energia 2030 ja Logistiikka 2030 -ohjelmat. Sisäistä toimintaa kehitettiin mallintamalla ohjelmien johtaminen. Tämä raportti käsittelee erityisesti Digitaalinen turvallisuus 2030 -ohjelmaa.

Digitaalinen turvallisuus 2030 -ohjelma (DT2030) on jatkoa vuosina 2017–2020 toteutetulle KYBER2020-ohjelmalle. DT2030 tarkoituksena on vastata digitaalisen murroksen aiheuttamiin huoltovarmuusriskeihin ja koota yhteen mahdollisimman laajasti kaikki Huoltovarmuuskeskuksen (HVK) tavoittelemat digitaalisen yhteiskunnan turvallisuuden edistämiseen liittyvät projektit ja merkittävimmät toimenpiteet. Kyberturvallisuus, laajasti ymmärrettynä, on ohjelman keskeinen teema.

DT2030 -ohjelma on sisältää yhteisten palvelujen kehittämistä, valikoitujen toimialojen kyberturvallisuuden kehittämisen käynnistämistä, digitaalisen infrastruktuurin vahvistamista sekä elintärkeiden toimintojen häiriönhallinnan toimintamallien kehittämistä ja harjoittelua.

Ohjelman visiona oli vuosina 2021–2023, että yhteiskunnan kriittiset toiminnot kestävät kyberhäiriöt. Tämä edellyttää, että yritykset tietävät mihin varautua ja miten, sietävät kyberiskuja ja palautuvat niistä toimintakuntoon nopeasti. Lisäksi yrityksillä ja viranomaisilla pitää olla tahto, yhteistyöverkostot ja yhteiset toimintamallit kriittisten toimintojen suojaamiseksi. Kansainvälinen yhteistyö täydentää kansallista osaamista ja kykyä havainnoida ja torjua huoltovarmuuden kannalta kriittisiä uhkia.

Ohjelman projektit tiivistyvät toteuttamaan neljää keskeistä tavoitetta, joiden avulla tavoitellaan vision toteutumista:

1. Varautuminen
2. Toimintakyky
3. Yhteistyö
4. Tulevaisuus

Ohjelman tavoitteet saavutettiin ohjelmakaudella 2021–2023 varsin hyvin. Digitaalisen infrastruktuurin varautumista parannettiin uusille keinolla ja infrastruktuurin toiminnasta tehtiin useita selvityksiä. Kyberturvallisuuden kansallista havainnointikykyä kehitettiin mm. parantamalla kansallisen kyberturvallisuuden tilannekuvaan käytettävää Havaro-palvelua. Toimialojen kyberturvallisuutta parannettiin useilla harjoituksilla ja toimialakohtaisilla hankkeilla. Tulevaisuustyössä tuotetiin uutta tietoa nousevista teknologioista erilaisilla tutkimuksilla, järjestettiin hackaton-tilaisuuksia ja luotiin skenaarioita varautumisen tueksi.

1. Ohjelman tausta ja tavoite

1.1. Ohjelman tavoite

Digitaalinen turvallisuus 2030 -ohjelma käynnistyi vuonna 2021. Digitaalinen turvallisuus 2030 -ohjelman visioksi vuosille 2021–2023 määriteltiin ”yhteiskunnan kriittiset toiminnot kestävät kyberhäiriöt”. Visio perustui kulmakiville, jotka olivat ohjelman alkaessa seuraavat:

- Yritykset tietävät mihin varautua ja miten, sietävät kyberiskuja ja palautuvat niistä toimintakuntoon nopeasti
- Yrityksillä ja viranomaisilla on tahto, yhteistyöverkostot ja yhteiset toimintamallit kriittisten toimintojen suojaamiseksi
- Kansainvälinen yhteistyö täydentää kansallista osaamista ja kykyä havainnoida ja torjua huoltovarmuuden kannalta kriittisiä uhkia

Kokonaisuuden taustalla oli ajatus kasvavista digitaalisen toimintaympäristön riippuvuuksista, jossa digitaalisista ekosysteemeistä riippuvainen kriittisten toimijoiden yhteiskunta tukeutuu jatkossa yhteydenpitoon, automatisaatioon ja koneoppimiseen. Samalla kun yhteiskunnan digitaalinen infrastruktuuri on kompleksinen, häiriöt laajenevat siinä nopeasti ja ennakoimattomasti. Keskinäisriippuvaisuuksien takia yksittäiseen organisaatioon kohdistuvat häiriöt voivat vaikuttaa toimitusketjun kautta laajasti muihin toimijoihin.

Kriittisen infrastruktuurin digitaalinen ekosysteemi on globaali. Kriittisen organisaation omasta järjestelmäkeskeisyydestä on siirryttävä prosessien suojaamiseen koko kumppaniverkostossa. Yleistyvät kyberhyökkäykset heikentävät yhteiskunnan luottamusta kriittisiin digitaalisiin palveluihin. Kompleksisessa toimintaympäristössä ilman toimenpiteitä riskit kasvavat samalla kun riskinäkyvyys heikkenee.

Tähän kehitykseen vastatakseen ohjelman alkaessa projektit tiivistyivät toteuttamaan neljää keskeistä tavoitetta vision toteutumiseksi:

Varautumisessa tärkeintä on kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuuksien ymmärtäminen ja turvaaminen sekä yhteistoimintamallien harjoittelu. Keskeistä on myös yritysten varautuminen sekä kyber- ja digiosaamisen kasvattaminen. Varautumisen keskeiset tavoitteet olivat:

- Ymmärretään ja turvataan kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet
- Hallitaan kyberriskejä verkostoissa elinkaaren läpi
- Edistetään kyberymmärrystä ja –osaamista yhteiskunnassa
- Säännölliset harjoitukset ovat osa suunniteltua varautumiskehitystä

Toimintakyvyn osalta keskeistä on havainnointi- ja analysointikyvykkyyden parantaminen sekä tiedonvaihto ja jaetun tilannekuvan ylläpitäminen. Lisäksi kiinnitetään huomiota häiriöitilanteiden hallintaan ja informaatiovaikuttamisen tunnistamiseen teknisin keinoin. Toimintakyvyn keskeiset tavoitteet olivat:

- Parannetaan havainnointi- ja analysointikyvykkyyttä
- Toimialat reagoivat havaintoihin asianmukaisesti
- Työvälineet tehostavat tiedonvaihtoa ja jaettua tilannekuvaa
- Otetaan käyttöön laaja-alaisen kyberhäiriötilanteen toimintamalli

Yhteistyö sekä kansallisesti että kansainvälisesti on edellytys ohjelman tavoitteiden toteutumiselle. Yhteistyöverkostojen keskeiset tavoitteet olivat:

- Aktiiviset tiedonvaihtoverkostot käyttävät yhteisiä toimintamalleja tiedonjakoon
- Toimijat tuntevat verkostolliset vastuunsa ja roolinsa
- Kansainvälinen yhteistyö edistää kansallista huoltovarmuutta
- Hyödynnetään kansainvälisiä tietovarantoja aktiivisesti

Tulevaisuus tarkoittaa digitaalisen maailman nousevien ilmiöiden tutkimusta. Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimusorganisaatioiden ja oppilaitosten kanssa. Tulevaisuuden keskeiset tavoitteet olivat:

- Tunnistetaan nousevien ilmiöiden vaikutus huoltovarmuuteen
- Tutkimus- ja koulutusyhteistyö yritysten, tutkimus- ja oppilaitosten kesken tuottaa tietoa ja osaajia kriittisen infrastruktuurin tarpeisiin
- Tutkimustuloksista valikoituu kehityskohteita digitaalisen turvallisuuden edistämiseen

Kuva 1. Ohjelman tavoitteet jakautuivat neljään osaan

VARAUTUMINEN

- Organisaatioiden, palveluiden, verkkojen ja kriittisen digitaalisen infran riippuvuudet ja kriittiset pisteet on tunnistettu ja suojattu asianmukaisesti
- Kriittiset digitaaliset palvelut kyetään pitämään käytettävissä, palauttamaan tai ne kyetään korvaamaan vastaavilla palveluilla nopeasti
- Huoltovarmuudelle kriittisten toimintojen kyberturvallisuus perustuu riskienhallintaan. Riskienhallinnassa havaitut tarpeet otetaan huomioon toimintavarmuudessa koko elinkaaren läpi
- Yhdessä kehitetyt toimintamallit toimivat arjessa ja harjoittelun perustana
- Yritykset voivat hyödyntää toimialoille määriteltyjä suosituksia kybervarautumisen perustasolle
- Turvallisuustietoisuus ja -osaaminen on kiinteä ja läpileikkaava osa yritysten johdon, asiantuntijaryhmien ja muun henkilöstön osaamista

YHTEISTYÖVERKOSTOT

- Yhteisiä toimintamalleja ja pelisääntöjä ylläpidetään ja kehitetään yritysten ja viranomaisten aktiivisella yhteistyöllä
- Kyberyhteistyö on kansallisesti koordinoitua ja toimialarajat ylittävää
- Tiedonvaihtoverkostot, toimintatavat ja periaatteet tiedon jakamiseen on määritelty ja vastuutettu
- Kansainvälinen kumppaniverkosto mahdollistaa kansainvälisen yhteistyön varautumistoimenpiteissä
- Viimeisimpään kansainväliseen tutkimus- ja tilannetietoon on pääsy
- Kansainvälisissä kehityssykleissä vaikutetaan hyvissä ajoin
- Kansainvälisten ICT-yritysten kanssa toimimiseen on tavoitteet ja toimintatavat

TOIMINTAKYKY

- Huoltovarmuuskriittisillä yrityksillä ja toimialaviranomaisilla on käytössään aina ajantasainen ja olennainen tieto
- Havainnointi- ja analyysikyky perustuu laaja-alaiseen dataan useista eri lähteistä ja koneoppimisella tuettuun kohdennettuun analyysiin
- Toimialoilla on ymmärrys ja vaatimukset havainnointi- ja reagointi kyvylleen
- Lainsäädäntö, tekniset keinot ja menettelytavat mahdollistavat kokonaisvaltaisen keskitetyn kybertilannekuvan muodostamisen ja arvion tulevasta
- Tietoturvapoikkeamista toivutaan nopeasti ja toipumisprosessia hyödynnetään kriittisten palveluiden ja verkkojen turvallisuuden parantamiseen
- Laaja-alaisen häiriötilanteen kyberjohtamisen malli, vastuut ja yhteiset toimintamallit on määritelty

TULEVAISUUS

- Uusien ilmiöiden tuottamiin kyberriskeihin osataan varautua
- Tutkimusyhteisö tuottaa huoltovarmuuden/kyberturvallisuuden kannalta merkittävää tietoa ja osaamista nousevien ilmiöiden kyberriskeistä
- Digitaalisen turvallisuuden kyvykkyyksien kehittämisessä tehdään tutkimusyhteistyötä kansainvälisesti
- Kansalliselle huoltovarmuudelle kriittisten toimintojen tuottajat ovat tietoisia teknologiavalintoihin tarjolla olevista suositelluista laatukriteeristöistä ja soveltavat niitä hankinnoissaan ja toiminnassaan

1.2. Ohjelman hyödyt ja mittarit

Ohjelmalle määriteltiin hyötytavoitteiksi:

1. Kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet ymmärretään niiden toiminnan turvaamiseksi (Varautuminen)
2. Tiedonvaihtoa tukee kattava havainnointi- ja analysointikyky, johon riittävät työkalut (Toimintakyky)
3. Tiedonvaihtoverkostot toimivat aktiivisesti määritetyin tiedonjakomallein ja vastuin (Yhteistyöverkostot)
4. Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimus- ja oppilaitosten kesken (Tulevaisuus)

Ohjelma jakautui aluksi kahdeksaan konkreettisempaan kehitysalueeseen, joiden alla projekteja toteutettiin vastaamaan tavoiteltuja hyötytavoitteita. Ohjelman kehittämisalueet olivat:

1. Yhteiskunnan valmiudet
2. Toimialojen osaaminen
3. Digitaalinen infrastruktuuri
4. Kansainvälinen yhteistyö
5. Nousevien ilmiöiden tutkimus
6. Kuntasektorin huoltovarmuus
7. Informaatiovaikuttamiseen varautuminen
8. Ohjelman johtaminen

Myöhemmin ohjelman johtamisen tehtävät siirtyivät osaksi HVK:n perustetun ohjelmatoimiston tehtäviä. Kuntasektorin huoltovarmuus kytkettiin osaksi toimialojen osaamista (toimialojen ja kuntien osaaminen).

Jokainen projekti toteutti osaltaan yhtä tai useampaa tavoitetta. Hyötytavoitteiden toteutumista arvioitiin laadullisesta näkökulmasta osana ohjelman raportointia.

Taulukko 1. Projektien jakautuminen hyötytavoitteittain

	2021	2022	2023	Yhteensä
Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimus- ja oppilaitosten kesken (Tulevaisuus)	3	6	6	**15**
Kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet ymmärretään niiden toiminnan turvaamiseksi (Varautuminen)	2	17	19	**38**
Tiedonvaihtoa tukee kattava havainnointi- ja analysointikyky, johon riittävät työkalut (Toimintakyky)	1	12	9	**22**
Tiedonvaihtoverkostot toimivat aktiivisesti määritetyin tiedonjakomallein ja vastuin (Yhteistyöverkostot)	2	6	8	**16**
Yhteensä	**8**	**41**	**42**	**91**

2. Ohjelman toteutus

2.1. Toteutuksen organisointi

Ohjelman johtaminen, toteutus ja seuranta jakaantui kolmeen alueeseen: Ohjelman johtaminen, ohjelman toteutus ja ohjelman ohjausryhmä. Ohjelman johtamisessa päätettiin ohjelman käytössä olevista resursseista, hyväksyttiin ohjelman tavoitteet ja ohjattiin toteutusta HVK:n tavoitteiden mukaisesti. Ohjelman toteutuksessa käynnistettiin ja toteutettiin projekteja ohjauksen mukaisesti. Lisäksi neuvonantajaryhmät tarjosivat toimialojen asiantuntemusta määritettäessä ohjelman tavoitteita sekä ohjelmaan valittavia projekteja.

Ohjelmaa on johtanut Jarna Hartikainen ja myöhemmin Juha Ilkka.
Ohjelman ohjausryhmään on kuulunut 2021–2023:

- Tuomo Haukkovaara, Digipoolin puheenjohtaja
- Jaakko Wallenius, Elisa
- Rauli Paananen, LVM
- Tuija Kuusisto, VM
- Sauli Pahlman, Traficom Kyberturvallisuuskeskus
- Kari Luoto, Päivittäistavarakauppa PTY ry
- Aaro Toivonen, HUS
- Timo Aaltonen, Helen
- Jaakko Pekki, HVK
- Sauli Savisalo, HVK
- Jarna Hartikainen, HVK

Ohjelman sisäisessä valmisteluryhmässä on toiminut Marja Marttinen, Tuomas Seppälä, Katja Ahola ja Antti Sillanpää.

DT2030 noudatti HVK:n ohjelma- ja projektijohtamisen malleja sekä vuosikelloa ja osallistui myös merkittävästä ohjelmatoiminnan kehittämiseen.

HVK:N JOHTORYHMÄ

- Ohjelmien rahoituskehyksenvalmistelu ja esittäminen hallitukselle, osana HVK:n budjettimenettelyä
- Ohjelmien projektisuunnitelmien hyväksyntä toteutukseen & projektien rahoituspäätökset
- Hallinnoi ohjelmaportfoliota

DT2030-OHJELMAN OHJAUSRYHMÄ

- Ohjelman toimeenpanon ohjaaminen HVK:n strategian ja linjausten mukaan
- Ohjelman sisäisen vision, tavoitteiden, tehtävien ja toimintatavan kehittäminen ja ylläpito HVK:n linjausten mukaan
- Ohjelman sisäiset rahoituspäätökset
- Hallinnoi ohjelmaan kuuluvaa projektiportfoliota
- Vuosikellosta minimi kokoontumistiheydelle (substanssin/työsuunnitelman edellyttäessä useammin)
- Osastojohtaja vetää, ohjelmavastaava, DT2030-ohjelman ohjelmakoordinaattori, DT2030-ohjelman viestinnästä vastaava koordinaattori, rahoittajien edustajat, hankintaorganisaation edustajat (PROXYT, esim. KTK tai ERVE)
- Digipoolintoimikunta, NIS-viranomaiset, Väestörekisterikeskus, MSB voivat toimia sekä ohjelman, että projektien ohjausryhmissä

Valmistelee ohjausryhmän kokoukset

DT2030-OHJELMAN VALMISTELURYHMÄ

- Valmistelee ohjausryhmän kokoukset
- Ryhmään kuuluvat: Osa-alueiden vetäjät (HVK:n sisäisiä henkilöitä) ja ohjelmakoordinaattori
- Projekti-ideat tulevat “ideasta hankkeeksi” -mallin mukaisesti
- Strategisten kumppaneiden toiminnan ohjaaminen sekä yhteistoiminnan toteuttaminen
- Projekti-ideoiden keruu ja työstäminen projektiesityksiksi ja edelleen projektisuunnitelmiksi sivulla esiteltyjen projektikriteerien perusteella
- Projektiesitysten arviointi ja priorisointi
- Muut ohjelman toimeenpanon käytännön tehtävät
- Toiminta vuosikellon mukainen (periaatteessa!)

Projektikohtainen johtaminen käsitelty eri dokumentissa

Ohjelman suunnitteluun ja toteuttamiseen on lisäksi kytkettiin ohjelman aikana mukaan useita HVK:n ulkopuolisia organisaatioita erilaisissa rooleissa. Keskeisimmät toteutuksen kannalta ovat olleet Huolto-varmuusorganisaation Digipooli ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Lisäksi mukana on projektitoteutuksissa toimialoittain yhteistoimintaryhmiä, virastoja, ohjaavia ministeriöitä, etujärjestöjä, keskeisiä yrityksiä ja oppilaitoksia.

2.2. Seuranta ja arviointi

Ohjelmaa on seurattu ohjausryhmän toimesta neljä kertaa vuodessa, sekä vuositasolla budjetin ja toteutuneiden projektien näkökulmasta. Neljännesvuosiraportin käsittelee Huoltovarmuuskeskuksen johtoryhmä sekä HVK:n operatiivisen osaston johtoryhmä, jonka jälkeen raportti toimitetaan HVK:n hallitukselle, sekä tarvittaville sidosryhmille.

Ohjelmaa on seurattu vuosittain 'ohjelman tila ja tulevaisuus' -raportoinnilla hallitukselle. Raportointi toteutettu vuosina 2021 ja 2022.

Ohjelmien neljännesvuosiraportointi on toteutettu koordinoidusti 2021 vuoden toisesta kvartaalista alkaen. Neljännesvuosiraportin käsittelevät Huoltovarmuuskeskuksen johtoryhmä ja operatiivisen osaston johtoryhmä, minkä jälkeen se toimitetaan tiedoksi HVK:n hallitukselle.

2.3. Resurssit ja rahoitus

Digitaalinen turvallisuus 2030 -ohjelman varainkäytön toteuma vuosina 2021–2023 oli yhteensä reilu 35 miljoona €, josta HVK:n rahoitus oli lähes 30 miljoona €. Ulkopuolista rahoitusta oli yhteensä yli 5 miljoona €.

2.4. Ohjelman viestintä

Ohjelmalle on laadittu oma viestintäsuunnitelma, ja ohjelmakauden aikana on toteutettu vuosittain suunnitelmallista viestintää eri kohderyhmille. Viestintää on kohdennettu kaikille kriittisille toimijoille, jotka käyttävät toiminnassaan digitaalisia yhteyksiä tai järjestelmiä.

HVK on viestinyt ohjelman toteutuksen edistymisestä ja valmistuneista projekteista mm.

- Varmuuden vuoksi -sivuilla (varmuudenvuoksi.fi)
- HVK:n sivuilla (huoltovarmuuskeskus.fi)
- HVO extranet -sivuilla.
- HVO verkoston sidosryhmätilaisuuksissa
- Digitaalinen turvallisuus 2030 -ohjelman omalla verkkosivulla

Ohjelman projekteista viestittiin sosiaalisen median kanavilla, joista erityisesti Twitter ja LinkedIn oli aktiivisessa käytössä. Lisäksi ohjelma on järjestänyt vuosiseminaarin webinaarina ohjelman etenemisestä. Webinaareihin osallistui keskimäärin noin 300 henkilöä vuosittain. Ohjelman tekijät osallistuivat aktiivisesti muihin alan webinaareihin viestien HVK:n toiminnasta digitaalisen turvallisuuden kentällä.

Ohjelmaviestinnän ja HVK:n viestinnän lisäksi ohjelman alla projekteja toteuttavat sidosryhmät ovat viestineet projektien toteutuksesta ja tuloksista omissa viestintäkanavissaan. Näin ollen digitaalisen turvallisuuden viestintä ja ohjelman toimenpiteet ovat tavoittaneet laajan vastanottajajoukon eri kanavien kautta.

3. Tulokset

3.1. Ohjelman tavoitteiden saavuttaminen

Digitaalinen turvallisuus 2030 -ohjelmalle asetetut hyötytavoitteet ohjelman alkaessa edistyi tai saavutettiin varsin hyvin vuosien 2021–2023 aikana. Projekteja käynnistyi vuosina 2021–2023 yhteensä 91 kappaletta, joilla parannettiin kansallista kyberturvallisuutta ja ICT-varautumista useasta eri näkökulmasta.

1. Kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet ymmärretään niiden toiminnan turvaamiseksi (Varautuminen): digitaalisen infrastruktuurin varautumista parannettiin uusille keinolla ja infrastruktuurin toiminnasta tehtiin useita selvityksiä, joilla lisättiin kansallisen tason ymmärrystä infrastruktuurin ja sen palveluiden toiminnasta. Kyberturvallisuuden kypsyyskartoitus tuotti tietoa kriittisen infrastruktuurin toimijoiden kybertilasta, kehityskohteista ja keskinäisriippuvaisuuksista. Projekteja toteutettiin hyötytavoitteelle yhteensä 15 kpl.

2. Tiedonvaihtoa tukee kattava havainnointi- ja analysointikyky, johon riittävät työkalut (Toimintakyky): Suurimpina kokonaisuuksina Traficomin kyberturvallisuuskeskukseen toteutettiin kaksi monivuotista projektia (Havaro ja Kyberilmasto), joilla parannettiin kansallisen tason havainnointi- ja analysointikykyä. Kyberilmasto-projekti jatkoi toimintaansa vielä vuodelle 2024. Projekteja toteutettiin hyötytavoitteelle yhteensä 38 kpl.

3. Tiedonvaihtoverkostot toimivat aktiivisesti määritetyin tiedonjakomallein ja vastuin (Yhteistyöverkostot): huoltovarmuuskriittisten yritysten yhteistoimintaa parannettiin lisäämällä osaamista ja tietoisuutta mm. aktiivisen harjoitustoiminnan, erilaisten selvitysten ja seminaarien avulla. Toimintaan osallistui tuhansia ihmisiä eri toimialoilta. Projekteja toteutettiin hyötytavoitteelle yhteensä 22 kpl.

4. Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimus- ja oppilaitosten kesken (Tulevaisuus): ohjelmassa kehitettiin useita selvityksiä nousevista ilmiöistä. Tekoälyn kyberturvallisuudesta laadittiin kolme selvitystä, kvanttilaskennan vaikutuksista tehtiin oma selvitys, joiden lisäksi tehtiin useita kokeiluja ja tutkimuksia muista alaan liittyvistä aiheista ja tekniikoista. Projekteja toteutettiin hyötytavoitteelle yhteensä 16 kpl.

3.2. Keskeiset tuotokset

Ohjelma käynnistyi keskellä koronaepidemiaa, joka näkyi vuoden 2021 käynnistyneiden projektien määrässä. Useat toteutusten kannalta keskeiset sidosryhmät keskittivät resursseja akuutin tilanteen hoitamiseen, kun ihmisten fyysisen etäisyyden mahdollistamiseksi hyödynnettiin vahvasti digitaalista yhteydenpitoa, mikä työllisti alan työntekijöitä. Tekeminen pääsi kunnolla käyntiin vuonna 2022, jolloin projekteja oli käynnissä 41 kpl.

Hyötytavoite	2021	2022	2023	Yhteensä
Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimus- ja oppilaitosten kesken (Tulevaisuus)	3	6	6	**15**
Kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet ymmärretään niiden toiminnan turvaamiseksi (Varautuminen)	2	17	19	**38**
Tiedonvaihtoa tukee kattava havainnointi- ja analysointikyky, johon riittävät työkalut (Toimintakyky)	1	12	9	**22**
Tiedonvaihtoverkostot toimivat aktiivisesti määritetyin tiedonjakomallein ja vastuin (Yhteistyöverkostot)	2	6	8	**16**
Yhteensä	**8**	**41**	**42**	**91**

Taulukko 2. Digitaalinen turvallisuus 2030 -ohjelman projektien määrät hyötytavoitteittain. Samalla projektilla voi olla useampi tavoite (ensisijainen ja muu hyötytavoite).

Digitaalisen infrastruktuurin toimintaa kehitettiin usealla eri projektilla, joita ei turvallisuussyistä tarkemmin avata julkisessa raportissa.

Ohjelman rahoituksella edistettiin kyberturvallisuuspalveluja huoltovarmuuskriittisille yrityksille. Näihin toimiin kuuluu esimerkiksi uusi versio kansallisesta kyberturvallisuuden havainnointijärjestelmä Havarosta. Havaro on Traficomin kyberturvallisuuskeskuksen tarjoama keskeinen palvelu kriittisille yrityksille, kun ne pyrkivät tunnistamaan vakavia tietoturvahyökkäyksiä yhteiskunnan elintärkeissä toiminnoissa. Uuden version avulla Havaron toimintaideaa muutettiin siten, että palvelu hyödyntää vahvasti myös kaupallisten toimijoiden osaamista avulla kriittisten, jotka toimivat kyberhyökkäyshavaintojen palvelupisteenä kriittisille toimijoille. Näin hyödynnetään kattavasti koko kyberekosysteemin osaamista ja tehostetaan kansallista tiedonvaihtoa.

Kyberilmasto-projektissa Traficomin kyberturvallisuuskeskuksen tilannekuvatoimintoa kehitettiin siten, että keskus kykenee tuottamaan tarkempaa ja ajankohtaisempaa tilannekuvaa huoltovarmuuskriittisille yrityksille. Keskuksen tietoon tulevat tietoturvapoikkeamat pystytään nopeammin kohdistamaan yrityksille, jolloin tietoturvahyökkäysten leviämiseen kyetään nopeammin reagoimaan ja estämään.

Useita projekteja käynnistettiin ohjelman avulla toimialakohtaisen digitaalisen turvallisuuden ja varautumisen parantamiseksi. Ohjelman avulla kiinteistö- ja rakennusalalle perustettiin oma tiedonvaihtoverkosto (ISAC) ja alalle tuotettiin uutta opetusmateriaalia. Kuntaomisteisen kriittisen infrastruktuurin kyberturvallisuuden tilasta tehtiin selvitys ja Traficomin kyberturvallisuuskeskukseen rahoitettiin kunta-alan toimialavastaavan tehtävä. Näiden toimenpiteiden avulla kuntien kyberturvallisuutta on kyetty viemään eteenpäin Huoltovarmuuskeskuksen, Traficomin ja Kuntaliiton yhteistyössä. KYBER-ELY -projektissa arvioitiin kunnallisten vesihuoltolaitosten kapasiteettia vastata ja reagoida alati muuttuviin tieto- ja kyberturvallisuusuhkiin ja kehittää seudullista ymmärrystä ja yhteistyötä kyberuhkien tunnistamisessa ja niihin varautumisessa. Useat näistä toteutuksista jatkuvat yhä kotiorganisaatioissa.

Finanssialan huoltovarmuuskriittisten organisaatioiden TIBER-FI -testejä tuotiin Suomeen ja laajennettiin Digitaalinen turvallisuus -ohjelman avulla. Projektin tuloksena kasvatettiin testien vuotuisia lukumääriä ja testauskohteita. Testien avulla finanssialan huoltovarmuuskriittiset organisaatiot pystyivät selvittämään kyberhäiriönsietokykyään ja parantamaan suojautumistaan korjaamalla testeissä havaittuja heikkouksia.

Digitaalinen turvallisuus ohjelma käynnisti vuonna 2022 informaatioturvallisuuden osaamiskeskus -pilotin, jonka tavoitteena oli rakentaa Suomeen tekninen kyvykkyys tunnistaa automatisoituja informaatiovaikuttamiskampanjoita sosiaalisessa mediassa. Projekti jatkoi toimintaa edelleen myös raportointikauden jälkeen.

JAMKin kyberharjoitusympäristöä kehitettiin siten, että sen avulla voidaan toteuttaa toimialakohtaisia harjoituksia huoltovarmuuskriittisille yrityksille. Strategiakaudella ympäristöä kehitettiin mm. logistiikan ja rahoitusalan osalta rakentamalla toimialoja simuloiva verkko ja järjestämällä alan toimijoille verkkoa hyödyntävä harjoitus. Harjoitustoiminta oli raportointikaudella aktiivista: vuonna 2022 järjestettiin kansallinen TIETO-harjoitus ja Traficomin kyberturvallisuuskeskus järjesti n. 3 toimialakohtaista harjoitusta vuosittain.

Tekoälyn kyberturvallisuudesta laadittiin kolmiosainen julkaisusarja, joiden avulla kuvatiin miten tekoälyn hyödyntämisessä on huomioitava kyberturvallisuus, miten tekoälyä käytetään kyberturvallisuusratkaisuissa ja miten tekoälypohjaiset hyökkäysmenetelmät toimivat.

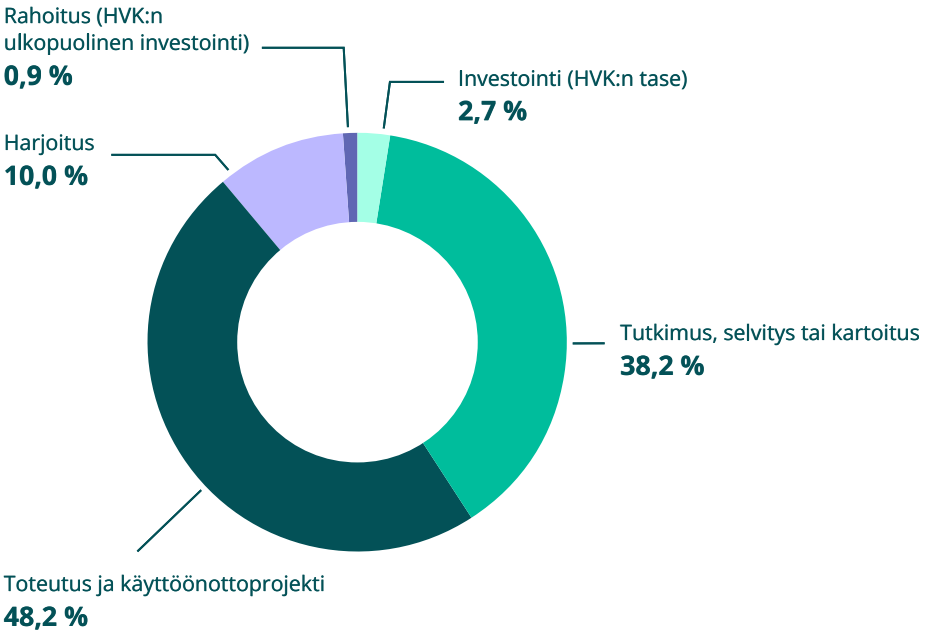
3.3. Aikaansaadut muutokset ja vaikuttavuus

Digitaalinen turvallisuus 2030 -ohjelman avulla vuoisna 2021–2023 parannettiin merkittävästi kyberturvallisuuden kansallista havainnointikykyä, tilannekuvaa ja osaamista. Toimintaa kuvasi hyvin se, että samalla kun pyrittiin ratkomaan olemassa olevia ongelmia, teknologinen murros toi paljon uusia asioita ratkottavaksi kuten mm. tekoälyn ja kvanttilaskennan riskit.

Projektien sisällölliset toteutukset jakautuivat ICT-alan lisäksi eri toimialoille. Merkittävä aikaansaatu muutos ohjelmakaudella oli, että digitaalista turvallisuutta alettiin huomioida osana liiketoimintaa usealla eri toimialalla sen sijaan, että IT- ja kyberturvallisuuden ammattilaiset olisivat olleet asiassa aloitteellisia. Tämä oli iso henkinen muutos, jonka tulokset ovat nähtävissä vasta tulevaisuudessa.

Ohjelman vaikuttavuuden laajuutta kuvaa se, että toimintaan osallistui tuhansia ihmisiä usealta eri toimialalta, sadoista yrityksistä ja projekteja käynnistettiin yhteensä 113 kpl. Ohjelman tuotoksia hyödynnettiin lainsäädäntötyössä ja kansallisessa kyberturvallisuusstrategiassa.

Ohjelmakaudella toteutus ja käyttöönottoprojekteja oli 48,2 %. Tutkimus, selvitys tai kartoitus -projekteja kokonaisuudesta oli 38,2 %.

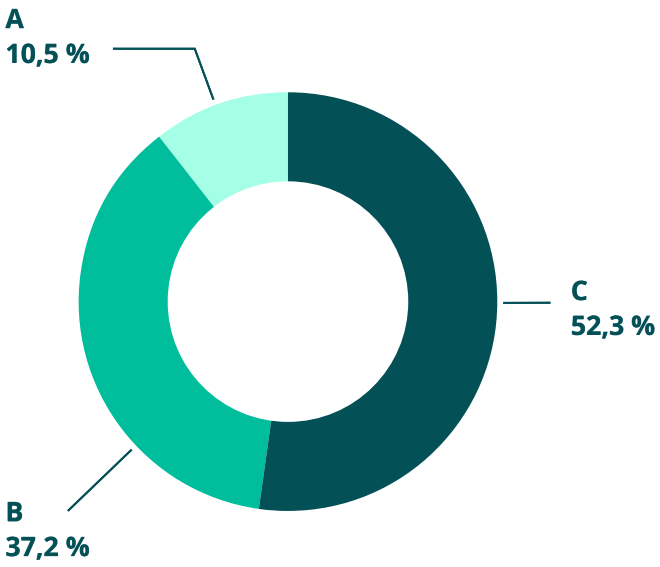


Kuva 2. Ohjelman projektit jaoteltuna sisällön mukaan

Huoltovarmuuskeskuksen rahoittamia projekteja arvioidaan ABC-luokittelun avulla. ABC-projektiluokka ilmaisee projektin kompleksisuuden ja haastavuuden projektinjohtamisen näkökulmasta. Projektiluokittelun tuloksena projekti sijoittuu johonkin seuraavista luokista:

A: Hyvin monimutkainen ja paljon riskejä sisältävä projekti
B: Tyypillinen, ns. normaali projekti
C: Yksinkertainen ja suoraviivainen projekti

Digitaalinen turvallisuus 2030 -ohjelmassa A-luokan projekteja oli ohjelmakaudella 10,5%, B-luokan projekteja 37,2 % ja C-luokan projekteja 52,3%.



Kuva 3. Ohjelman projektit ABC-luokittelun mukaan

4. Johtopäätökset

4.1. Ohjelman toteutuksen arviointi

Ohjelman toteutus on vuosien 2021–2023 aikana onnistunut hyvin, vaikka koronapandemia ja Venäjän hyökkäyssodan alkaminen Ukrainassa haastoi resurssien käyttöä niin HVK:ssa kuin sidosryhmissä. Projekteja käynnistyi ja päättyi merkittävä määrä ja projektien onnistuminen tavoiteltuun hyötyihin nähden on hyvä. Usea pitkäkestoinen projekti jatkuvat yhä. Lisäksi 2021–2023 toteutetut projektien tuotokset ovat lisänneet ymmärrystä digitaalisen turvallisuuden riskeistä, minkä pohjalta on käynnistetty uusia kehitysprojekteja varautumisen edistämiseksi. Hyötyjä toteutuu vielä jatkossa.

Yleisesti voidaan todeta, että ohjelman aikana projektit ovat rakentaneet kansallisen tason kyvykkyyksiä, joilla on ollut merkittävä vaikutus kansalliseen varautumiseen. Ohjelma on oman toiminnan ohella kyennyt lisäämään muiden rahoituslähteinen ja yritysten omia investointeja kyberturvallisuuteen. Osa projekteista on jatkanut omaa elämää ilman HVK:n rahoitusta, joka on selkeä merkki onnistumisesta.

4.2. Keskeiset opit ja onnistumiset

Digitaalinen turvallisuus 2030 -ohjelmassa on tehty useita selvityksiä, joista on myös päästy konkreettisempaan toteutusprojektiin. Esimerkiksi toimialojen kyberturvallisuuskartoituksesta on noussut käytännönläheisiä projekteja kuten ohjelmistoturvallisuuden kehittämisprojekti. Osa selvityksistä ei ole vienyt eteenpäin tai niiden jalkautus on jäänyt selkeästi yritysten omalle vastuulle. Näissä projekteissa viestintä on keskiössä.

Digitaalinen turvallisuus 2030 -ohjelman myötä Huoltovarmuuskeskus, Traficom ja Kyberala ry on alkanut järjestämään pienimuotoisia webinaareja 3–4 kertaa vuodessa. Näihin webinaareihin on osallistunut n. 300–600 henkilöä per tilaisuus. Webinaarit ovat olleet hyvä kanava lisätä tietoisuutta selvitysten tuloksista. Vielä tarvitaan kuitenkin työtä sen eteen, että projekteista syntyvät selvitykset ovat helposti saatavilla ja tavoittaa asiantuntijat kattavasti.

Ohjelmassa on pyritty muodostamaan projekteista isompia kokonaisuuksia, jotta vaikuttavuus olisi suurempi. Tämä on ollut toimiva ratkaisu, kun esim. kuntaomisteisen kriittisen infrastruktuurin kyberturvallisuutta on kehitetty eteenpäin. Harjoitustoiminnasta muodostui lopulta suurempi kokonaisuus kuin ohjelmaa suunniteltaessa pohdittiin. Harjoituksiin on osallistunut iso joukko yrityksiä käytännössä kaikilta toimialoilta. Tämä on selkeä onnistuminen ja vienyt kyberturvallisuutta aimo harppauksen eteenpäin.

Toimialakohtaiset projektit ovat olleet lainsäädännön takia haastavia rahoittaa. Useat projektit ovat kuuluneet de minimis -tuen piiriin, joka on asettanut raamit projektien kokoluokalle. Näihin projekteihin toteutustapojen arviointi tavoiteltujen hyötyjen saavuttamiseksi on syytä arvioida kansallisten huoltovarmuustavoitteiden saavuttamiseksi.

4.3. Jatkokehitys ja kohdealueen tulevaisuus

Digitaalinen turvallisuus on jatkuvassa muutostilassa. Kaikki alat ovat kohdanneet digitaalisten riippuvuuksien kasvun. Uudet murrokselliset teknologiat kuten kvanttilaskenta ja tekoäly muuttaa myös digitaalista turvallisuutta ja siten uusien digitaalisten riskien kautta huoltovarmuuden riskejä. Samanaikaisen turvallisuustilanne edellyttää yhä kasvavaa fokusta turvallisuuteen, mikä digitaalisessa toimintaympäristössä tarkoittaa kyberturvallisuutta. Näiden yhteisvaikutuksesta digitaalisen turvallisuuden kehitystoimenpiteitä pitää pystyä jatkuvasti tunnistamaan, jotta jo saavutettu riskitaso säilyy, eikä laske. Huoltovarmuuden turvaamiseksi kyberturvallisuuden tarve kasvaa jatkossa.

Myönteistä huoltovarmuuden kehityksen kannalta on, että eri toimialat ovat alkaneet vahvemmin toteuttaa oman alansa kyberturvallisuutta parantavia toimenpiteitä liiketoiminnan jatkuvuuden hallinnan näkökulmasta. Tämä luo erinomaiset edellytykset ohjelman toteutukselle HVK:n strategiakaudella 2024–2027, joka painottuu entistä vahvemmin turvallisuustilanteen aiheuttamiin huoltovarmuustarpeisiin,

Digitaalinen turvallisuus on jatkossa yhä keskeisempi osa huoltovarmuutta, kansallista turvallisuutta ja varautumista. Tätä työtä Huoltovarmuuskeskus jatkaa strategiakaudella 2024–2027 Digitaalinen turvallisuus 2030 -ohjelmalla.

LIITTEET

Liite 1: Ohjelmassa muodostunut julkinen aineisto

Julkinen aineisto on mittava. Listaus ei ole täydellinen, koska aineistoa jaetaan usean eri organisaatio sivuilla.

Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/sosiaali-ja

Materiaaleja kriittisen infran turvaamiseen
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/materiaaleja

Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-paikallisten-matkaviestinverkkojen-kyberturvallisuudesta-ja-riskienhallinnasta

Toimialojen kyberkypsyyden selvitys 2022
https://www.huoltovarmuuskeskus.fi/files/bbdecbcd7921768bd3ac5496af7992a0460a9f2b/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

Digi-HTA
https://oys.fi/fincchta/digi-hta/

Elintarvikeketjun kyberturvallisuus
https://www.jamk.fi/fi/tutkimus-ja-kehitys/tki-projektit/elintarvikeketjun-kyberturvallisuus

5G Cyber Security Hack 2021
https://hackthenetworks.fi/en/previous-hacks/5g-cyber-security-hack-2021

Hack the networks
https://hackthenetworks.fi/fi

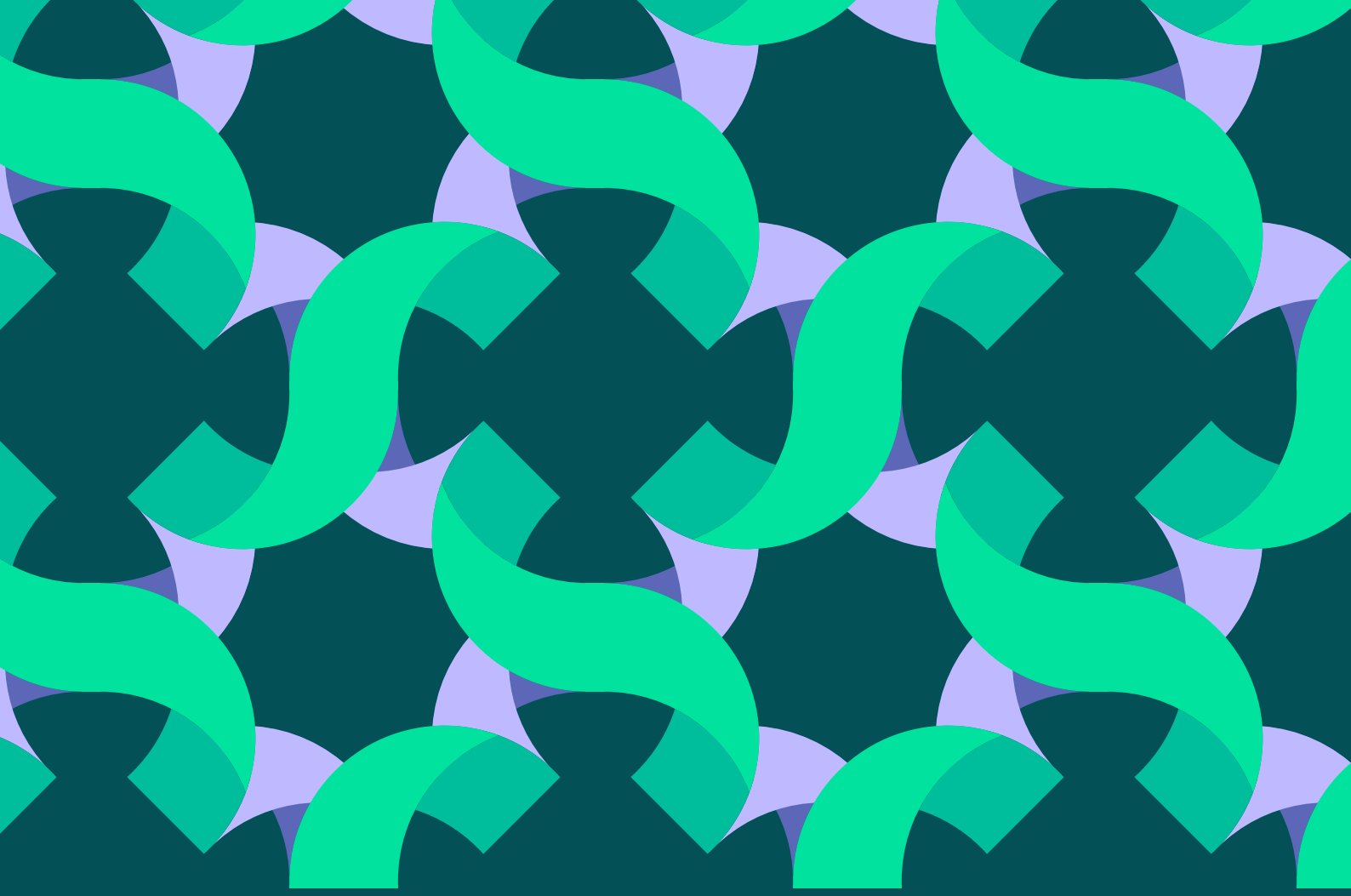
Havaro
https://havaro.fi/fi

Toteutettavuustestaukset
https://www.kyberturvallisuuskeskus.fi/fi/tonttu

Informaatioturvallisuuden osaamiskeskus
https://www.huoltovarmuuskeskus.fi/informaatioturvallisuuden-osaamiskeskus

Kvanttilaskennan tietoturvavaikutukset
https://www.huoltovarmuuskeskus.fi/files/15e58655d01a83d82639ecd5255c0562d66bf433/hvk-kvanttilaskennan-tietoturvavaikutukset-raportti-2024-saavutettava-20241007.pdf

Huoltovarmuutta pilvipalveluilla
https://teknologiateollisuus.fi/digipooli/wp-content/uploads/sites/12/2024/09/Huoltovarmuutta-Pilvipalveluilla_0.pdf



Huoltovarmuuskeskus