Statsrådets kanslis publikationsserie 2024:xx

Strategi för cybersäkerheten i Finland

2024–2035

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

UTKAST

Statsrådets kansli, Helsingfors 2024.

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Statsrådets kansli
Klicka och välj upphovsrättsnivå

ISBN pdf: SRK fyller i
ISSN pdf: SRK fyller i

ISBN tryckt: SRK fyller i
ISSN tryckt: SRK fyller i

Layout: Statsrådets förvaltningsenhet, Publikationsproduktion

Helsingfors 2024 Finland (i språkversioner)

Tryck: Grano Oy, 2024

Presentationsblad
x.x.2024

Strategi för cybersäkerheten i Finland 2024–2035

SRK fyller i, publikationsserie och nummer		**Teema**	Napsauta ja kirjoita
Utgivare	Statsrådets kansli		
Författare	Napsauta ja kirjoita		
Toimittaja/t	Napsauta ja kirjoita		
Utarbetad av	Klicka och skriv in		
Språk	Klicka och skriv in	**Sidantal**	VNK täyttää

Sammanfattning

Strategin för cybersäkerheten i Finland har reviderats i enlighet med regeringsprogrammet för Petteri Orpos regering för att motsvara den förändrade verksamhetsmiljön. I revideringen av Strategin för cybersäkerheten i Finland har man beaktat kraven enligt cybersäkerhetsdirektivet (NIS2) på nationella cybersäkerhetsstrategier 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.

Måltillståndet för strategin för cybersäkerheten i Finland sträcker sig till år 2035 och 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 kommunikationsministeriet, försvarsministeriet, statsrådets kansli, inrikesministeriet, utrikesministeriet, arbets- och näringsministeriet, finansministeriet, justitieministeriet, social- och hälsovårdsministeriet, undervisnings- och kulturministeriet, jord- och skogsbruksministeriet och Säkerhetskommitténs sekretariat.

I beredningen av strategin har nästan 100 aktörer inom den offentliga och privata sektorn, vetenskapssamfundet samt medborgarorganisationer fått vara delaktiga.

Klausul	VNK täyttää
Nyckelord	Klicka och skriv inhttps://finto.fi/juho/fi/

ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN nid.	VNK täyttää	**ISSN painettu**	VNK täyttää
Ärendenummer	VN/36693/2023	**Projektnummer**	Napsauta ja kirjoita
Julkaisun osoite	VNK täyttää		

Presentationsblad
x.x.2024

Klicka och skriv rubriken på svenska
Klicka och skriv underrubriken på svenska

SRK fyller i, serienamn och nummer		**Tema**	Klicka och skriv in
Utgivare	Klicka och ange ministerium		
Författare	Klicka och skriv in		
Redigerare	Klicka och skriv in		
Utarbetad av	Klicka och skriv in		
Språk	Klicka och skriv in	**Sidantal**	VNK täyttää
Referat	Klicka och skriv in ett referat, högst 1 400 tecken. Tryck på Enter i slutet av stycket.		

Klausul	VNK täyttää		
Nyckelord	Klicka och skriv inhttps://finto.fi/juho/fi/		
ISBN PDF	VNK täyttää	**ISSN PDF**	SRK fyller i
ISBN tryckt	SRK fyller i	**ISSN tryckt**	SRK fyller i
Ärendenr	Klicka och skriv in	**Projektnr**	Klicka och skriv in
URN-adress	SRK fyller i		

Description sheet
x Month 2024

Klicka och skriv rubrik på engelska
Napsauta ja kirjoita alaotsikko englanniksi

VNK täyttää, sarjanimi ja numero		**Subject**	Napsauta ja kirjoita
Publisher	Napsauta ja kirjoita		
Author(s)	Napsauta ja kirjoita		
Editor(s)	Napsauta ja kirjoita		
Group author	Napsauta ja kirjoita		
Language	Napsauta ja kirjoita	**Pages**	VNK täyttää

Abstract Napsauta ja kirjoita tiivistelmä enintään 1 400 merkkiä. Paina kappaleen lopussa Enter.

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

Innehåll

FÖRORD

Klicka och skriv in text. Tryck på Enter i slutet av stycket.

Klicka och skriv in Undertecknarens namn.
Klicka och skriv publikationsmånad och -år, t.ex. april 2018

Inledning – cybersäkerhet är en del av den övergripande säkerheten

Cybersäkerheten är en del av Finlands övergripande säkerhet och det digitaliserade samhället. Genom cybersäkerhet säkerställs verksamhetsförutsättningarna för den nationella säkerheten, landets försvar, försörjningsberedskapen, näringslivet och civilsamhället. Förändringen i det geopolitiska läget har ytterligare framhävt betydelsen av nationellt och internationellt samarbete i säkerställandet av cybersäkerhet. I synnerhet har det uppkommit behov av samarbete mellan myndigheter och näringslivet, stöd för samhällets kristålighet och bemötande av fientlig verksamhet. Verksamhetsmiljön definieras kraftigt av digitaliseringen, utvecklingen av nya tekniker och global konkurrens i fråga om dessa, ömsesidigt beroende och befolkningens åldrande. Samhällets grundstrukturer och -tjänster, såsom informations- och kommunikationsnäten och infrastrukturen i fråga om dessa, måste fungera under alla omständigheter.

Den nationella cybersäkerhetsstrategin har reviderats för att motsvara den förändrade verksamhetsmiljön i enlighet med regeringsprogrammet för statsminister Petteri Orpos regering. Med cybersäkerhet avses allmänt åtgärder för att skydda kommunikations- och informationssystem samt andra elektroniska system, de uppgifter som lagras, behandlas eller överförs i dem samt deras användare, utnyttjare och andra berörda personer från cyberhot. Traditionellt har cybersäkerheten granskats ur ett mer tekniskt perspektiv och inte så mycket som en fråga om statens säkerhet. I denna strategi behandlas nationell cybersäkerhet, med vilket man avser de åtgärder som medför att det digitala samhället kan bereda sig på, identifiera, bekämpa och klara av störningar i elektroniska och nätverksanslutna system och deras konsekvenser för vitala samhällsfunktioner och -tjänster, återhämta sig från dem samt säkerställa verksamhetsförutsättningarna för den nationella säkerheten, landets försvar och försörjningsberedskapen.

Revideringen av cybersäkerhetsstrategin har även föregåtts av Europeiska unionen cybersäkerhetsdirektiv (NIS 2) och dess nationella genomförande,

som fastställer skyldigheter även för medlemsstaternas cybersäkerhetsstrategier. Den reviderade strategin för cybersäkerheten i Finland är den tredje i ordningen och fortsätter att främja det ekosystemtänkande i fråga om cybersäkerheten som framfördes i utvecklingsprogrammet som utarbetades på basis av den föregående cybersäkerhetsstrategin. I beredningen av strategin har hänsyn tagits till annat nationellt strategi- och redogörelsearbete som anknyter till ämnet, varav de viktigaste är statsrådets följande principbeslut: Utvecklingsprogram för cybersäkerheten, Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället (TITUKRI) och Digital säkerhet inom den offentliga förvaltningen samt statsrådets redogörelse om Finlands digitala kompass och dess genomförandeplan. I beredningen har man dessutom beaktat den utredning som gjordes 2023 om myndigheternas verksamhetsförutsättningar inom cybersäkerhet och anmärkningarna och utvecklingsobjekten i fråga om detta arbete. Dessutom har man samarbetat med andra projekt som ingår i regeringsprogrammet och bereds samtidigt.

Måltillståndet för strategin för cybersäkerheten i Finland sträcker sig till år 2035, och dess strategiska mål omfattar fyra delområden, dvs. pelare: I **Kompetens, teknologi och forsknings-, utvecklings- och innovationsverksamhet (FUI); II Beredskap; III Samarbete samt IV Reagerande och svarsåtgärder.**

I det nationella måltillståndet är cybersäkerheten en oskiljaktig del av Finlands övergripande säkerhet.

Vårt digitaliserade samhälle är driftsäkert och pålitligt. Vi utnyttjar tekniska möjligheter och förstår hoten relaterade till dem mot cybermiljön och samhället. Vi utvecklar kompetensen i stor utsträckning.

Finland observerar, identifierar, bekämpar och klarar av situationer med cyberstörningar, återhämtar sig från dem och reagerar beslutsamt på störningarna.

Finland främjar cybersäkerhet aktivt och målmedvetet genom tätt nationellt och internationellt samarbete och informationsutbyte.

Tillräckliga resurser säkerställs för att uppnå måltillståndet, och de används effektivt.

I nuläget använder Finland nästan 300 miljoner euro årligen på att säkerställa cybersäkerheten inom statsförvaltningen. Utöver de offentliga investeringarna investerar även näringslivet cirka tiofalt i cybersäkerhet jämfört med de offentliga investeringarna enligt en försiktig uppskattning.

Utvecklingsförslagen som härletts ur strategins måltillstånd genomförs i enlighet med den genomförandeplan som utarbetas efter att strategin godkänts.

Som bilaga till strategin finns en beskrivning av samarbetsmodellen för den nationella cybersäkerheten. I slutet av strategin definieras de centrala termerna som använts i detta dokument.

Förändring i verksamhetsmiljön

Säkerhetsmiljön har förändrats kraftigt i Finland och Europa efter 2019, då den föregående nationella cybersäkerhetsstrategin publicerades. Den accelererande digitaliseringen och covid-19-pandemin som ytterligare påskyndade den, Rysslands anfallskrig i Ukraina, det globalt åtstramade geopolitiska läget och Finlands Natomedlemskap samt EU-regleringen som påverkar cybersäkerheten och som utvecklats kraftigt framhäver betydelsen av cybersäkerhet som en del av skyddet av samhället.

Den förändrade verksamhetsmiljön utmanar det internationella regelbaserade systemet

Hoten har blivit mer varierande och cybermiljön utnyttjas i hög grad för hybridpåverkan, brottslighet, terrorism och krigföring. Cyberpåverkan används även för att driva politiska mål mellan staterna. Statlig cyberspionerі hotar inte enbart beredningen av utrikes- och säkerhetspolitiken. Skyddet av finländska företags immateriella kapital mot olaglig informationsanskaffning i cybermiljön ska också identifieras som ett viktigt utvecklingsobjekt för att bibehålla ekonomins konkurrenskraft.

Den fientliga cyberverksamheten mot Finland ökar

Det är sannolikt att den varierande fientliga cyberverksamheten mot Finland fortsätter och ökar i framtiden. Digitaliseringen av samhället skapar nya möjligheter för de statliga aktörerna att bland annat genomföra underrättelseinhämtning och utnyttja sårbarheter utan någon stor risk för avslöjande.

Utöver tekniska störningar kan effekterna av fientlig verksamhet även nå Finland från andra länder och sprida sig oförutsett, även om Finland inte är deras huvudsakliga mål. När den fientliga cyberverksamheten ökar och allt mer omfattande även riktar sig mot regeringar, demokratiska institutioner, företagslivet och medborgarna ökar även behovet av ett gränsöverskridande samarbete. Av denna anledning är det viktigare än tidigare att känna till den egna verksamhetsmiljön, informationssystemen och framför allt deras inbördes beroendeförhållande.

Den teknologiska omvälvningen ökar allas ansvar för cybersäkerheten

Den teknologiska omvälvningen och samhällenas digitalisering ökar attackytan, dvs. mängden informationssystem och tjänster som syns offentligt på internet, och ökar därmed samhällets sårbarhet och utsatthet för cyberstörningar. Antalet enheter som verkar i datanätet förväntas öka med miljarder globalt sett fram till 2030. Tekniska störningssituationer orsakas exempelvis av mänskliga misstag i programutvecklingen och i deras leveranskedjor samt av avsiktligt skapade sårbarheter, såsom kryphål till tekniken. De ger kriminella och statliga aktörer tillgång till informationssystemen. Organisationernas och medborgarnas ansvar vid programuppdatering är viktig även i fortsättningen. Genom reglering kan utvecklingen av säker teknologi främjas, men samtidigt som säkerhetsåtgärder vidtas utvecklar även inkräktarna nya sätt att kringgå dem.

Internationellt samarbete stärker Finlands cybersäkerhet

Natomedlemskapet stärker Finlands säkerhet och försvar, men innebär även nya utmaningar och skyldigheter. Natomedlemskapets avskräckande effekt kan leda till att den fientliga verksamhetens tyngdpunkt allt mer övergår till cybermiljön, där utövaren lättare kan bestrida sin delaktighet. Samtidigt skapar den teknologiska utvecklingen, dataorienteringen, det internationella samarbetet samt analyseringen av geopolitiska förbindelser inom cyberverksamheten ändå allt bättre möjligheter i synnerhet för att attribuera, dvs. tillräkna, statliga aktörer.

Finland är en betydande producent av tekniska lösningar inom cybersäkerhet och -försvar inom alliansen. I egenskap av ett militärt allierat land främjar Finland i fortsättningen utvecklingen av Natos cyberförsvar och utnyttjar alliansens kapacitet. Detta stöds av planmässig utveckling och planmässigt upprätthållande av cyberförsvaret som en del av den nationella cybersäkerheten. Finlands infrastruktur utvecklas som en del av alliansens infrastruktur, vilket stärker samarbetet och cyberförsvaret. De flesta av de sju grundläggande resilienskraven som Nato fastställt ställer även krav på utveckling av den nationella cybersäkerheten. Samtidigt förblir den för Finland viktiga EU alltjämt en viktig referensram i stärkandet av samhällets cybertolerans och resiliens.

Det är viktigt att samordna de nationella EU- och Natoståndpunkterna vad gäller cybersäkerhet och -försvar. Koherensen av Natos och EU:s cyberåtgärder kompletterar och stärker både den internationella cybersäkerheten och Finlands nationella cybersäkerhet. Parallellt med Natomedlemskapet har även det bilaterala och multilaterala internationella samarbetet inom cybersäkerhet och -försvar utvidgats och fördjupats. Genom initiativ av och samarbete med likasinnade länder strävar man efter att svara mot centrala cyberhotbilder och förbättra den kollektiva cybersäkerheten. Även inom FN och olika regionala organisationer identifieras cybersäkerhetens betydelse för den internationella säkerheten.

Under de senaste åren har EU-regleringen som påverkar cybersäkerheten utvecklats i hög grad, vilket stärker cybersäkerheten för Finland och andra EU-länder. Det nationella genomförandet av regleringen och anpassningen av organisationernas verksamhet i enlighet med den innebär utmaningar såväl för myndigheterna som näringslivet under de kommande åren. Dessa ökar kompetens- och utbildningsbehoven och kostnaderna för att bygga upp ett tillräckligt skydd och kräver ytterligare åtgärder för att hantera cyberriskerna. Genom regleringen skapas förutsättningar för att förbättra cybersäkerheten för samhällets kritiska aktörer och den inbyggda säkerheten i apparater och program. Samtidigt utvecklas myndigheternas verksamhet i fråga om beredskap, störningssituationer samt insatser och svarsåtgärder.

Den nationella verksamhetsmodellen utvecklas

Den nationella verksamhetsmodellen inom cybersäkerhet har baserat sig på förmågan att fortlöpande förbättra informationssystemens och organisationernas verksamhet för att tåla cyberattacker och tekniska störningar samt återhämta sig från dem. Förändringen i verksamhetsmiljön och cyberhoten utmanar de tidigare verksamhetssätten och ökar behovet av att utveckla beredskapsåtgärderna och insatserna samt av samordnade svarsåtgärder som är mer proaktiva än tidigare. Modellen med en övergripande säkerhet möjliggör även beredskap inom cybersäkerhetsbranschen och utveckling av samarbetet i enlighet med samhällets säkerhetsstrategi.

Den ökade cyberbrottsligheten berör hela samhället

Allvarlig cyberbrottslighet kan äventyra vitala samhällsfunktioners ostörda verksamhet, hota den nationella säkerheten eller annars orsaka omfattande störningar i samhället. Den ökade mängden cyberbrottslighet och hoten som utvecklas snabbt berör hela samhället. Cyberbrottslighet kan äventyra medborgarnas grundläggande rättigheter, försämrar tilltron till tjänster och kan orsaka betydande ekonomiska förluster. Cyberbrottslighet är allt mer kopplad även till den organiserade brottsligheten och statliga aktörer. Vid fientlig verksamhet utnyttjar staterna ofta också bland annat olika ersättande aktörer, såsom kriminella grupper, som köptjänster. Genom att köpa tjänster av kriminella kan de fientliga staterna försöka försvåra tillräknande eller till exempel variera intensiteten i sina cyberoperationer.

Det är beaktansvärt att en stor del av infrastrukturen som är kritisk med avseende på samhällets funktioner ägs av den privata sektorn. Samarbetet mellan myndigheterna och privata sektorn baserar sig i Finland på reglering, avtal och tjänster, men även på förtroende och frivillighet, vilket bidrar till att underlätta informationsutbytet om exempelvis olika hot och störningar. På grund av den förändrade verksamhetsmiljön räcker det i nuläget inte med det befintliga informationsutbytet och de redskap som används för det samt bildandet av en lägesuppfattning. Det är nödvändigt att utveckla lagstiftningen, myndigheternas befogenheter samt samarbetsstrukturerna och -nätverken.

Säkerheten i leveranskedjorna framhävs

De starkt globaliserade leveranskedjornas utsatthet för störningar har blivit en del av vår hotmiljö. I en geoekonomi med ett allt större ömsesidigt beroende kan till exempel energi, råmaterial, logistik och infrastruktur göras till medel för geopolitiska syften även i cybermiljön. Service- och leveranskedjorna har blivit längre och mer komplicerade och det är allt svårare att hantera dem. Vid en attack på en leveranskedja bryter man sig in i organisationens informationssystem via de tjänster som den köpt eller via serviceproducenternas apparater eller program. Det kan vara svårt att äventyra den egentliga tjänsten eller systemet eller att olovligt göra intrång i det, men att påverka leveranskedjor kan på samma sätt leda till det slutresultat som inkräktaren eftersträvar. De kritiska aktörerna med avseende på samhällets funktionsförmåga måste således säkerställa att även deras serviceproducenter och leveranskedjor är cybersäkra.

Störningar i cybermiljön kan även orsakas av olika fysiska hot, såsom störningar i eltillgången, översvämningar, jordbävningar, solaktivitet eller andra naturfenomen samt skador orsakade av mänskliga misstag. Dessa kan störa dataförbindelserna eller informationssystemens verksamhet och därmed hota cybersäkerheten.

Cybersäkerhet möjliggör affärsverksamhetens tillväxt

Samhällets digitalisering skapar även betydande affärsverksamhetsmöjligheter som stöder tillväxt, allt från förenklade processer till utveckling av nya inlärningsmetoder eller andra möjligheter som forsknings- och utvecklingsarbetet öppnar upp. Omvälvande teknologier, såsom artificiell intelligens och kvantberäkning möjliggör utveckling av nya lösningar för dagens och framtidens utmaningar även i cybermiljön. Omvälvande teknologier kan dock även användas och utnyttjas av fientliga aktörer, vilket ställer krav på de nuvarande sätten att skydda sig. I och med förändringarna i verksamhetsmiljön ökar behovet av nya och effektiva innovationer som stärker cybersäkerheten.

Statsrådets nuvarande utmaningar och arbetskraftsbristen inom datasäkerhetsbranschen tillsammans med EU:s ökade reglering påverkar möjligheterna att utveckla cybersäkerheten i framtiden. Offentliga sektorns konkurrenskraft som arbetsgivare håller på att komma i skuggan av privata sektorn. Dessa medför utmaningar för genomförandet av strategin för cybersäkerheten i Finland och dess genomförandeplan samt cyberbranschens nationella tillväxt.

Nuläge

Finland är ett långt digitaliserat samhälle. En allt större del av människornas dagliga aktiviteter och användning av offentliga tjänster sker i den digitala miljön. Finlands offentliga förvaltning och offentliga tjänster placerar sig ofta på de högsta platserna i internationella jämförelser som gäller digitalisering. I Finland har man även ständigt förbättrat säkerheten för den digitala verksamhetsmiljön. Cybersäkerheten i Finland är på en jämförelsevis god nivå på basis av internationella bedömningar och en nationell självutvärdering. Finländarnas tekniska kunnande och förståelse för cybersäkerheten samt det välfungerande samarbetet inom cybersäkerhetsbranschen mellan den offentliga och privata sektorn även ur global synvinkel kan ses som ett internationellt visitkort och en potentiell exportprodukt.

Även i Finland har man upplevt omfattande dataintrång som påverkar människors vardag, men vi har ändå besparats från effekter av cyberattacker som lamslår samhällets funktioner under en lång tid. Samtidigt har fientlig statlig verksamhet, cyberbrottslighet, överbelastningsangrepp, informationsläckor och olika skadeprogram samt andra störningssituationer blivit vanligare även i Finland. Det finns ett hot om nya allvarliga och mer omfattande effekter.

Näringslivet spelar en betydande roll i säkerställandet av den nationella cybersäkerheten.

I Finland svarar näringslivet långt för upprätthållandet och utvecklingen av den digitala infrastrukturen och dess tjänster. De nationella branschspecifika nätverken för informationsutbyte är livskraftiga. Inom dessa nätverk utbyter företag som konkurrerar inom samma sektor aktivt information om cybersäkerhet både mellan varandra och med den offentliga sektorn.

Även i Finland kan man observera en global trend som delar företagen och branscherna: organisationerna indelas allt tydligare i dem som har sörjt för sin egen cybersäkerhet och dem som inte har gjort det. I en värld där man är ömsesidigt beroende av varandra orsakar detta risker för hela samhället.

Betydelsen av samarbetet framhävs

Finland är ett förtroendesamhälle där den offentliga, privata och tredje sektorn samarbetar intensivt. Myndigheterna bekämpar cyberhot mot samhället, och cyberproffsen i de företag och organisationer som arbetar med dem samt civilsamhället i sina egna organisationer. Det är viktigt att myndighetsverksamheten är pålitlig och att tjänsterna säkerställs för alla – medborgarna ska behandlas jämlikt och det ska säkerställas att både användarna och de som tillhandahåller tjänster kan lita på den digitala tekniken och servicen.

Positiva erfarenheter av gemensam interaktion ökar förtroendet. I cybermiljön behövs det förutom förtroende även driftsäkra digitala förfaranden för att identifiera med vem eller vad man agerar: användaren måste veta vems tjänst det är fråga om eller vem som är informationskällan. Det är viktigt att man är säker på parterna i kommunikationen samt kommunikationens korrekthet och säkerhet. De nya bedrägerisätten som möjliggörs av artificiell intelligens och omfattande språkmodeller utgör redan nu ett hot såväl för cybermiljön som informationsmiljön.

Beredskap inför kvantteknologins ankomst

I krypteringsteknikernas nationella förmågor förenas säkerställande av verksamhetsförutsättningarna för den nationella säkerheten och försvaret, försörjningsberedskapen och kunskapskapitalet och internationellt samarbete. Inom vissa delområden i Finland finns det starkt kunnande i fråga om framtagande och utnyttjande av krypteringstekniker. Trots det djupa kunnandet är det totala antalet sakkunniga ändå litet, vilket påverkar utvecklingen och införandet av tekniker.

Den snabba utvecklingen av kvantteknologin ger ytterligare utmaningar för den nuvarande nationella krypteringsförmågan. Finland har sackat efter referensländerna vad gäller utvecklingen av nationella lösningar för krypteringstekniker, och i Finland saknas det förpliktande lagstiftning för användning av godkända krypteringstekniker. Långsamheten i myndigheternas bedömning och godkännande av krypteringstekniker och avsaknaden av ett nationellt krypteringsteknologiskt laboratorium kan i värsta fall hindra utvecklingsarbetet.

Cybersäkerheten ska beaktas i samhällets digitaliseringsutveckling

Finlands digitala kompass är en nationell strategisk färdplan för Finlands digitaliseringsutveckling som sträcker sig till 2030. Enligt kompassen strävar Finland efter en betydande lättnad i företagens och medborgarnas behov av ärendehantering med hjälp av en enhetlig och målmedveten revidering av den offentliga förvaltningen. I kompassen beskrivs de väsentliga målen och nyckelresultaten för utveckling av cybersäkerhet och digital säkerhet som behövs för detta.

Den senaste betydande administrativa reformen var bildandet av välfärdsområdena med självstyre som inledde sin verksamhet i början av 2023. Ändringen påverkade i hög grad även välfärdsområdenas kritiska infrastruktur och offentliga tjänster. Välfärdsområdena svarar för sina tjänster och cybersäkerheten i anslutning till tjänsterna. Inom kommunfältet bedöms cybersäkerheten i genomsnitt ha genomförts sämre än inom den övriga offentliga förvaltningen. Välfärdsområdena och kommunerna behöver mer stöd än hittills i säkerställandet av cybersäkerheten, till exempel centraliserade cybersäkerhetstjänster. Bekämpningen av cyberhot måste fungera smidigt mellan olika stora aktörer och tidsmässigt steglöst såväl nationellt som på regional och lokal nivå.

De skador som orsakas av cyberstörningar kan vara sådana att de inte helt kan ersättas till exempel om information förstörs eller läcker ut permanent. En del små företag har till och med varit tvungna att avsluta sin verksamhet på grund av cybersäkerhetsrisker som förverkligats. Detta framhäver ytterligare vikten av att tillräckliga resurser allokeras för cybersäkerheten samt vikten av samarbete och gemensamma förfaringssätt.

Betydelsen av en gemensam lägesuppfattning framhävs

Föremål för statliga aktörers informationsanskaffning och påverkan i cybermiljön är förutom det politiska beslutsfattandet även myndigheter, vitala samhällsfunktioner, tjänster och den kritiska infrastrukturen som stöder dem, företags och forskninginstituts kunskapskapital samt innovationer. Dessutom kan fientliga statliga aktörer koordinera sina åtgärder sinsemellan för att effektivisera sina mål. Det centrala syftet med angripande cyberoperationer är att störa eller försöka lamslå samhällets kritiska infrastruktur, såsom energi- och vattenförsörjningens eller hälso- och sjukvårdens funktionsförmåga. Samtidigt

är målet vanligtvis att försöka påverka den statliga förvaltningen och den politiska beslutsförmågan. Några av de viktigaste lärdomarna av till exempel anfallskriget som Ryssland inledde mot Ukraina kan anses vara den centrala betydelsen av myndigheternas och cyberbranschens företags utnyttjande av färdigheterna och täta samarbete i tryggandet av cybersäkerheten och den kritiska infrastrukturens funktion gentemot statliga hot.

I nuläget har myndigheterna bedömts ha otillräckliga verksamhetsförutsättningar för att effektivt förbereda sig för och bekämpa allvarligare cyberhot som äventyrar den nationella cybersäkerheten och landets försvar. Lägesbilden och -uppfattningen som myndigheterna samordnar och analyserar sinsemellan behöver vidareutvecklas. Offentliga tjänsters cybersäkerhetsinformation delas i nuläget inte heller i tillräcklig grad mellan alla aktörer inom offentliga förvaltningen och näringslivet med avseende på strategi-, norm-, resurs- och informationsstyrning.

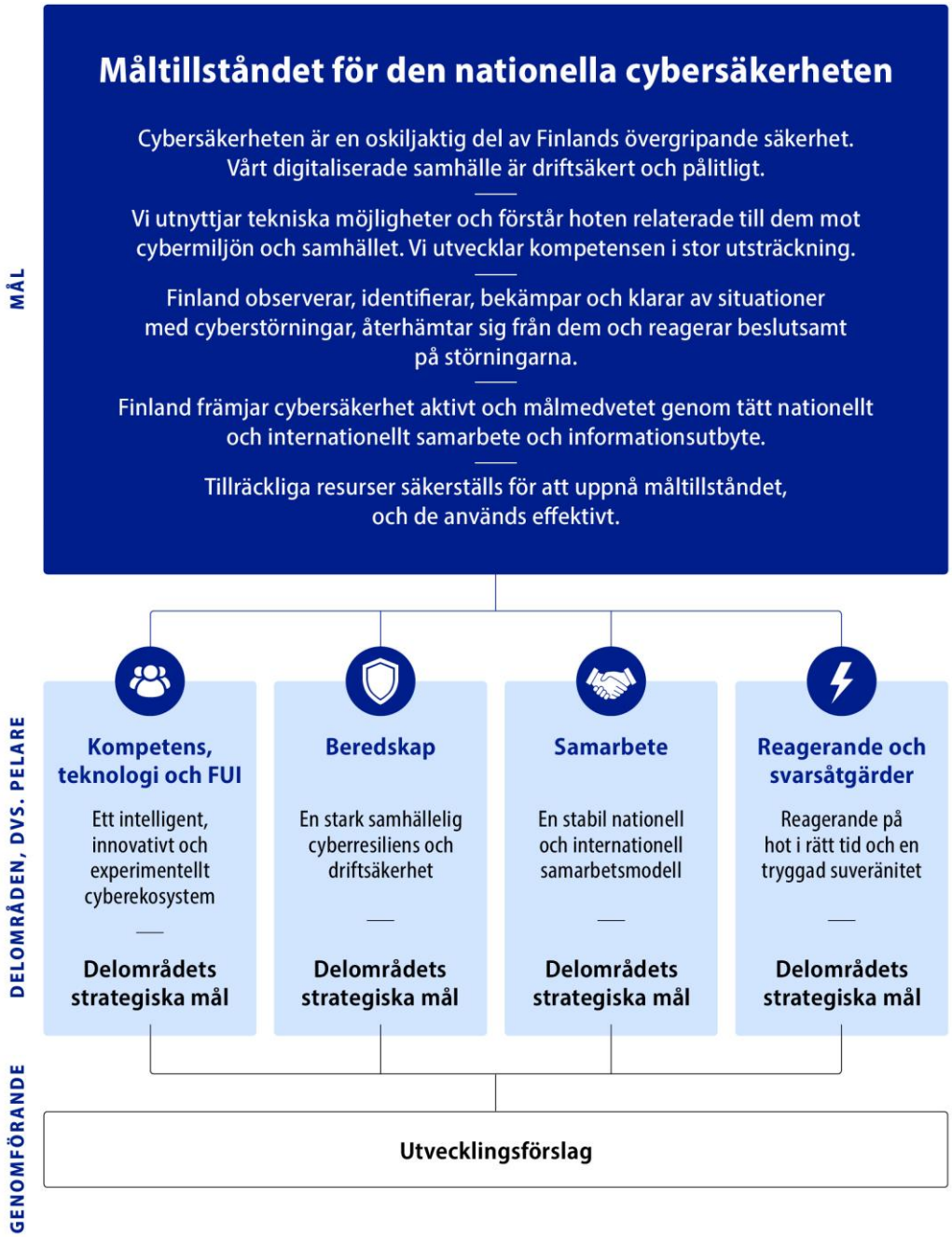
En händelse som äventyrar cybermiljöns säkerhet kan samtidigt vara ett informationssäkerhetshot, ett brott och ett hot som äventyrar den nationella säkerheten och försvaret och som har utrikes- och säkerhetspolitiska konsekvenser. Därför ligger ansvaret för att reda ut händelsen oftast samtidigt på flera myndigheter. I Finland har det hittills inte i tillräcklig omfattning reglerats om samordningen och samarbetet mellan myndigheter i fråga om cybermiljön, och i bestämmelserna har särdragen i cybermiljön vad gäller bekämpningen av cyberhot och informationsutbytet inte beaktats i tillräcklig grad.

Myndigheter, företag och organisationer tar i nuläget fram lägesbilder på olika nivåer, för olika användningsändamål och med olika innehåll för utförandet av sina uppgifter. Förvaltningsområdena tar fram sin egen lägesbild även för statsledningens behov. Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter svarar tillsammans med sina samarbetspartner för upprätthållandet och analyseringen av en lägesbild över den nationella cybersäkerheten. Samordningsgruppen för cybersäkerhet som fungerar på en strategisk nivå har som mål att säkerställa att de nationella ministerierna och cybersäkerhetsmyndigheterna har en enhetlig lägesbild av samhällets cybersäkerhetsläge. Statens cybersäkerhetsdirektör fungerar som statsledningens rådgivare i frågor som gäller cybersäkerhet.

Betydelsen av cybersäkerhetens ekosystem framhävs

För att möjliggöra en hållbar ekonomisk tillväxt söker man en balans mellan hot och möjligheter i samarbete med aktörerna inom ekosystemet för cybersäkerhet. Den tekniska utvecklingen stöds genom användning av olika finansieringsmodeller. En aktiv dialog och samarbete mellan olika aktörer i samhället ökar förtroendet och stöder myndighetsbeslutens lagenlighet. Inom en internationell referensram är Finland en säkerhetsproducent, vilket förbättrar säkerheten i EU och Nato som helhet.

Måltillstånd och struktur



Figur 1: Cybersäkerhetsstrategins måltillstånd och strategins struktur

Pelarna och deras strategiska mål

Pelare I: Kompetens, teknologi och FUI

Ett intelligent, innovativt och experimentellt cyberekosystem.

DELOMRÅDETS STRATEGISKA MÅL:

- Cybersäkerhetskunnandet är starkt på alla nivåer inom fostran och utbildning samt samhället och arbetslivet.
- Medborgarna är medvetna om sitt cybersäkerhetsansvar.
- Finland är i främsta linjen och tar i bruk fördelarna med omvälvande teknologier och kräver inbyggd säkerhet i apparater och tjänster.
- Cybersäkerhetens kunskapskapital är skyddat och Finland strävar efter att vara självförsörjande i fråga om kritisk krypteringsteknik.
- Finland säkerställer FUI-miljöns attraktionskraft och främjar konkurrenskraften för företag inom cybersäkerhetsbranschen.
- Möjligheterna till samarbete med och finansiering av EU och Nato utnyttjas.

Ett innovativt och experimentellt cyberekosystem

Ekosystemet för cybersäkerhet är en helhet som i stor utsträckning omfattar aktörer inom privata och offentliga sektorn, kompetens och skicklighet på olika samhällsnivåer, samarbete och förfaringssätt mellan aktörer, en stark inhemsk cyberindustri och forskningsinstitut. Målet med cyberekosystemet är att producera livskraft och tillväxt, öka arbetsplatserna inom cybersäkerhetsbranschen, ta fram behövlig kompetens och stärka det digitala samhällets hållbarhet och självförsörjning samt toleransen mot olika fenomen i cybermiljön. Ett fungerande och experimentellt cyberekosystem ökar produktiviteten och effektiviteten samt förbättrar kvaliteten på tjänsterna.

Medborgarna är medvetna om sitt cybersäkerhetsansvar

Cybersäkerhetskompetens hör till medborgarfärdigheterna och var och en kan genom sitt eget handlande medverka till uppkomsten av en allt säkrare cybermiljö. En cybersäker vardag kan stödjas bland annat genom att stärka medborgarnas medieläskunnighet och öka kunskapen om en god cyberhygien. Cyberhygien, dvs. iakttagande av god datasäkerhetspraxis som en del av de dagliga rutinerna, ska ses som en naturlig del av varje individs medborgaransvar. Medborgare som agerar ansvarsfullt i cybermiljön ökar på ett betydande sätt även sammanslutningarnas och organisationernas säkerhet.

Kompetensen är stark på alla nivåer

Det hör till företagens ansvarsfulla verksamhet att utveckla cybersäkra förmågor, identifiera hot, reagera på skadlig verksamhet och anmäla störningar i cybermiljön. I skolorna ska lärarnas färdigheter att fostra eleverna till en kritisk medieläskunnighet samt en medvetenhet om cyberrisker stärkas för att göra samhällets resiliens starkare. Finländsk cybersäkerhetskompetens säkerställs i sin helhet genom att i stor utsträckning stärka cybersäkerhetens roll inom fostran, utbildning och undervisning samt på alla nivåer i samhället och arbetslivet.

Ett innovativt och experimentellt cyberekosystem

Beredskap inför cyberhot, utveckling av skydd och tillväxt för finländska företag inom cybersäkerhetsbranschen är möjliga endast om det finns kompetent arbetskraft att tillgå. En grund skapas för den innovativa forsknings- och utvecklingsverksamheten som har en samhällelig påverkan genom att stödja grundläggande forskning och utbildning inom branschen. För att säkerställa en tillräcklig kompetensnivå utvecklas kompetensen angående cybersäkerhet och det relaterade ansvaret hos anställda inom den offentliga förvaltningen. Aktiv delning av information, kunnande och lägesuppfattning stöder en innovativ cybermiljö.

Medborgarna, företagen och organisationerna gynnas av en säker verksamhetsmiljö som blir mer förutsägbar i och med att kompetensen utvecklas.

Samtidigt ökar intresset för Finland såväl som investeringsobjekt som kompetenscentrum. Finland profilerar sig även internationellt som ett cybersäkert land, vilket i bästa fall kan vara både en konkurrensfördel och en exportprodukt för Finland.

Vi utnyttjar omvälvande tekniker

Omvälvande tekniker såsom artificiell intelligens och kvantteknologi samt nya generationer av mobilnät för med sig nya och ännu okända cybersäkerhetshot. Dessutom är de sammantagna effekterna av dessa tekniker mycket svåra att förutse. Bemötandet av dessa utmaningar kräver en djup och omfattande teknisk kompetens och en fortlöpande uppföljning och utvärdering av de samhälleliga förändringarna.

Finland har som mål att modigt vara bland de första som tar i bruk omvälvande tekniker som stöd för säkerställandet av cybersäkerheten. Storskalig användning av de tekniker som tas i bruk förutsätter att man utgår från att teknikerna och programmen planeras så att de är säkra och att man regelbundet sörjer för deras säkerhet under hela deras livscykel. Det är viktigt att beakta denna princip om inbyggd säkerhet i all nationell lagberedning som gäller teknologi samt i föregripande EU-inflytande. Interoperabilitets- och standardiseringsarbetet som utförs i samarbete med EU och internationellt är i en central roll när cybersäkerheten och säkerheten i nya tekniker säkerställs. Finland är en aktiv aktör vad gäller utveckling av standarder för cybersäkerhet.

Företagens konkurrenskraft främjas

En stark inhemsk företagsverksamhet inom cybersäkerhetsbranschen är väsentlig för att utveckla och upprätthålla ett fungerande ekosystem för cybersäkerheten. I planeringen av satsningarna på forsknings-, utvecklings- och innovationsverksamhet (FUI) som rör cybersäkerhet utnyttjas de internationella samarbets- och finansieringsmöjligheter som EU och Nato tillhandahåller och via dem satsas det på behövliga processer, resurser och proaktivt samarbete. Deltagande i internationella finansieringsprogram, såsom Natos innovationsinitiativ DIANA och EU:s ramprogram Horisont Europa och Digitalt Europa

(DEP), ökar Finlands ryktbarhet som ett land med kompetens inom högteknologi och cybersäkerhet och förbättrar finländska företags affärsverksamhetsmöjligheter nationellt och internationellt. Dessutom kan samarbets- och finansieringsmöjligheterna inom Europeiska rymdorganisationen ESA utnyttjas för att beakta cybersäkerheten i rymdteknologins snabba utveckling.

Målet är att Finland ska kunna ta fram globalt konkurrenskraftiga tekniska lösningar inom cybersäkerhetsbranschen för att möjliggöra tillväxt. Finlands FUI-miljö ska uppmuntra och stödja utvecklingen och användningen av lösningar som stöder cybersäkerheten samt den internationella konkurrenskraften för de företag som kommersialiserar dem. På så sätt främjas attraktionskraften hos både den finländska cybersäkerhetsbranschen och vidare hos en säker FUI- och affärsverksamhetsmiljö för finländska och utländska experter, företag och investeringar.

Cybersäkerhetens kunskapskapital är skyddat

Det är viktigt att den offentliga och privata sektorns kritiska kunskapskapital identifieras och skyddas. Kunskapskapitalet i fråga om cybersäkerheten omfattar till exempel tjänster, informationssystem, kunnande, processer, patent, varumärken och partnerskap. Genom olika aktörers aktiva informationsutbyte och kunskapsbaserat beslutsfattande kan beslut tas effektivt om de utvecklingsåtgärder som behövs för cybersäkerheten, genom vilka kunskapskapitalet kan skyddas för att säkerställa samhällets funktionsduglighet.

Vi strävar efter självförsörjning inom krypteringsteknik

En viktig del av cyberresiliensen är att nationellt betydande informationsresurser är användbara, tillgängliga och pålitliga i alla situationer. Kvantteknologins utveckling hotar att knäcka moderna krypteringsalgoritmer och äventyra nationellt skyddade informationsmaterial. Ett strategiskt mål för Finland är att vara självförsörjande i fråga om kritiska krypteringstekniker och en stat med beredskap inför kvanthot senast i början av 2030-talet. Detta förutsätter att nationellt kritiska krypteringstekniker, såsom kvantsäkra krypteringslösningar, utvecklas i hemlandet och att den övergripande krypteringstekniska förmågan stärks bland annat inom delområdena produktion, forskning, kalkylering, de-

kompilering och organisering. I det nationella utvecklingsarbetet med kvantsäker kryptering beaktas även EU:s gemensamma politiska åtgärder och reglering samt de krav som Nato ställer.

Pelare II: Beredskap

En stark samhällelig cyberresiliens och driftsäkerhet

DELOMRÅDETS STRATEGISKA MÅL:

- Den kritiska infrastrukturen, de vitala samhällsfunktionerna, de offentliga tjänsterna och de kritiska aktörerna med avseende på försörjningsberedskapen är cybertåliga.
- Medborgarna, företagen, organisationerna och myndigheterna har tillsammans förberett sig för cyberstörningar.
- Finland främjar sin modell för cybersäkerhetsberedskap som exportprodukt.
- Cyberbrottslighet förebyggs.
- Beredskapen baserar sig på en övergripande gemensam lägesuppfattning och långsiktig resursering.
- Miljön och praxis för cyberövningar utvecklas och övningar mellan olika sektorer ökas.

Vi kan lita på samhällets funktionsduglighet

Finland förbereder sig på cyberhot med framförhållning. Det är viktigt att man kan lita på samhällets funktionsduglighet i alla förhållanden. En tillräcklig beredskap för cyberstörningar i rätt tid utgör grundvalen för det digitala samhällets funktionsduglighet. Genom prognostisering och långsiktig beredskap främjas tillgången på samhällets tjänster och förmågan att klara av störningar i alla förhållanden. Det är viktigt att säkerställa att de vitala samhällsfunktionerna, den kritiska infrastrukturen, informationsresurserna, de offentliga tjänsterna och aktörerna som är kritiska med avseende på försörjningsberedskapen fungerar och är störningståliga. Målet med försörjningsberedskapsarbetet som utförs som en del av beredskapen är att säkerställa att den kritiska infrastrukturen, produktionen och tjänsterna fungerar så att de kan tillgodose befolkningens, näringslivets och försvarets mest nödvändiga grundläggande behov i alla förhållanden även i cybermiljön.

Företagen är intresserade av att utveckla sin beredskap utgående från affärsverksamheten. Den offentliga förvaltningen ska beakta förändringarna i verksamhetsmiljön när de ställer beredskapskrav på företag ur säkerhetsperspektiv och när de stöder företagens beredskap. I säkerställandet av funktionsdugligheten och utvecklingen av störningstoleransen är det i synnerhet viktigt att utveckla cyberövningarna och göra dem mer omfattande med hänsyn till cybersäkerheten inom service- och leveranskedjorna samt olika ömsesidiga beroendeförhållanden. Säkra informationssystem utgör en grund för ett cybertåligt samhälle och uppmärksamhet bör fästas vid deras anskaffning, utveckling och upprätthållande såväl inom den offentliga som den privata sektorn.

Offentliga tjänster är säkra

Det är viktigt att de offentliga tjänsterna är säkra att använda och medborgarna och organisationerna litar på deras funktionsduglighet. Cybersäkerheten i de offentliga tjänsterna styrs proaktivt på basis av lägesinformation samt hot- och riskbedömning. För att hantera riskerna och stärka cybersäkerheten behövs det en omfattande och pålitlig lägesbild av nivån på och bristerna i cybersäkerheten i de offentliga tjänsterna. Effektiviteten, nyttan och kostnaderna med cybersäkerheten följs upp och tyngdpunkter prioriteras. Av offentliga tjänsters tekniker och serviceproduktionen krävs det kravenlighet för cybersäkerheten under hela livscykeln. Bedömningen och godkännandet av offentliga tjänsters kravenlighet samt bedömningskriterierna ska utvecklas och förtydligas och åläggandet i fråga om dessa ska förbättras. Dessutom är det viktigt att utveckla den automatiska tekniska uppföljningen och tillsynen och förplikta till detta. Det bör säkerställas att tjänsterna prioriteras i enlighet med säkerhetsläget, att det finns beredskap för potentiella störningssituationer och att effekterna av störningarna på myndigheternas och samhällets verksamhet kan minimeras.

Beredningen sker i samarbete

I enlighet med modellen för övergripande säkerhet bereder sig myndigheterna i fråga om cybersäkerheten i samarbete med företagen, organisationerna och medborgarna. Identifieringen av cyberhot och beredskapen inför dessa ska basera sig på systematisk kunskapsledning och en gemensam lägesuppfattning som baserar sig på prognostisering, underrättelseinhämtning och utnyttjande av forskningsdata. Underrättelseinhämtningen stöder beredskapen och

prognostiseringen genom anskaffning och delning av underrättelseinformation både om fientliga cyberaktörers kapacitet och om målen och föremålen för cyberattacker för att skydda den nationella säkerheten.

Finland främjar en verksamhetsmodell för beredskap som betonar samarbete och dialog även i samarbetet med EU och Nato, och främjar tillämpningen av beredskapsmodellen för cybersäkerhet och bästa praxis även i partnerländerna. Det inbördes förtroendet mellan olika aktörer i samhället och tilltron till offentliga institutioner och deras tjänster bygger en stark nationell resiliens. Förtroende är också en förutsättning för framgångsrikt nationellt cybersäkerhetsarbete, beredskap, en gemensam lägesuppfattning och insatser i rätt tid.

Cyberbrottslighet förebyggs

Förebyggande av cyberbrottslighet kräver målinriktade och aktiva åtgärder av alla aktörer i hela samhället. Tyngdpunkten för bekämpningen av cyberbrottslighet ligger på förebyggande i ett så tidigt skede som möjligt och identifiering av hot. Av denna anledning ska de tjänster som tillhandahålls medborgarna planeras, genomföras och upprätthållas så att ytan som kan attackeras av cyberbrottslingar minskar. Det är viktigt att användarna kan lita på säkerheten i tjänsterna och att de har tillräckligt kunnande för att identifiera förfalskade tjänster och bedrägeri. Hoten förknippade med cyberbrottslighet ska kommuniceras på ett förståeligt sätt och anvisningar och råd ska ges om korrekta förfaringssätt. En tidig anmälan till myndigheterna av brott som riktar sig mot medborgare och företag möjliggör förebyggande av liknande brott och uppkomsten av mer omfattande skador. Förebyggandet av cyberbrott ska stödas genom lagstiftning, som gör det möjligt att dela information mellan myndigheter och företag.

Beredskap baserar sig på långsiktig resursering

På grundval av en omfattande hot- och riskbedömning och lagstadgade skyldigheter inkluderas de cybersäkerhetsresurser som de identifierade behoven kräver i offentliga förvaltningens, företagens och organisationernas verksamhets- och ekonomiplaner. En effektiv användning av resurser för cybersäkerhet förutsätter att cybersäkerhetsuppgifterna planeras och genomförs effektivt i ett omfattande nationellt och internationellt samarbete med statsförvaltningen, företag och organisationer samt region- och lokalförvaltningen. Vid

statsrådet har de gemensamma resurserna för ledning av cybersäkerheten på strategisk nivå koncentrerats till statens cybersäkerhetsdirektörs byrå. Andra myndigheter som utför centraliserade cybersäkerhetsuppgifter tilldelas resurser i enlighet med de uppgifter som föreskrivs för dem. Dessutom ska centralisering av gemensamma cybersäkerhetsuppgifter främjas inom region- och lokalförvaltningen för att undvika överlappande arbete och för att effektivisera resursanvändningen.

Den centraliserade projektfinansieringen som ingår i planen för de offentliga finanserna kan allokeras för införande av nya cybersäkerhetsfunktioner, -uppgifter eller -tjänster. Myndighetens möjlighet att erbjuda cybersäkerhetstjänster åt kunderna som en avgiftsbelagd tjänst ska alltid utredas när en ny tjänst införs.

Det är viktigt att följa upp och aktivt utveckla cybersäkerhetsverksamhetens produktivitet och effektivitet både på samhällsnivå och i varje organisation. Användningen av finansieringen planeras, följs upp och övervakas med hjälp av en gemensam lägesbild över resurserna som en del av planeringen av den offentliga ekonomin. Den reglering och de verksamhetsmodeller för informationsutbytet som behövs för inhämtandet och upprätthållandet av den ska genomföras.

Övningsverksamheten ökas

Genom nationella cyberövningar simuleras olika cyberstörningar, dvs. man skapar förhållanden där man kan testa och öva effekterna av cyberstörningar och återhämtning från dem. Övningarna utvecklar kunnandet och upprätthåller individers och organisationers beredskap och förmåga att förbereda sig för olika cyberstörningar och hot. Aktiva övningar i normalförhållanden stärker kunnandet i alla situationer. Dessutom uppmuntras organisationerna att långsiktigt utveckla sin övningsverksamhet, vid behov med stöd av myndigheterna.

Genom cyberövningsverksamheten bygger man en stark cyberresiliens för hela samhället. Det är viktigt att utveckla miljön och praxis för cyberövningar och särskilt att utöka övningarna mellan olika sektorer. Internationella cyberövningar stöder beredskapen inför, beslutsfattandet om och bekämpningen av gränsöverskridande cyberhot och störningar. För Finland är det viktigt att delta

i internationella cyberövningar, påverka aktivt under dessa samt utveckla och erbjuda kunnande om cyberövningar åt internationella partnerländer.

Genom rymdtjänsterna förbättras resiliensen för markbundna system.

Rymdtjänsterna kan utnyttjas för framtagande av en cyberlägesbild. Det är viktigt att behövliga rymdtjänster, såsom tid- och platsinformation, datatrafik och distanskartläggning är tillgängliga för aktörerna i samhället. Rymdsystemens cybersäkerhet övervakas som en del av rymdlägesbilden. Rymdsystemens cybersäkerhet beaktas i villkoren för rymdtillstånd och i hanteringen av systemens livscykel. Man förbereder sig för potentiella störningssituationer och återhämtning från dem och effekterna av störningarna på myndigheternas och samhällets verksamhet minimeras med hjälp av alternativa verksamhetsmodeller och reservarrangemang.

Pelare III: Samarbete

En stabil nationell och internationell samarbetsmodell

DELOMRÅDETS STRATEGISKA MÅL:

- Finland påverkar och deltar aktivt i det normativa internationella samarbetet rörande cybermiljön, såsom cyberdiplomati och utveckling av lagstiftningen.
- Finland deltar aktivt i och påverkar förebyggande samarbetet kring cybersäkerhet, bekämpning av cyberbrott och cyberförsvar och stöder partnerländerna.
- Möjligheterna i fråga om cybersäkerhet som erbjuds genom EU och Nato säkerställs.
- Den offentliga och privata sektorn utvecklar en samarbetsmodell som är aktivare och stärker förtroendet.
- Den information som behövs i myndigheternas samarbete utbyts smidigt och friktionsfritt.
- Den offentliga sektorn utvecklar och tillhandahåller centraliserade cybersäkerhetstjänster tillsammans med den privata sektorn.

Den utrikes- och säkerhetspolitiska redogörelsen, försvarsredogörelsen, redogörelsen för den inre säkerheten och cybersäkerhetsstrategin fastställer långsiktiga nationella mål för bekämpning av cyberhot. I dem beaktas Natos och EU:s mål och skyldigheter i fråga om cybersäkerhet och cyberförsvar. Dessa mål har preciserats genom nationell cyberpolitik. Genomförandet av de mål som fastställts för cyberdiplomatin, cybersäkerheten och cyberförsvaret och uppföljningen av resultaten samordnas på strategisk nivå i ett omfattande samarbete.

Finland påverkar och deltar i det aktiva samarbetet

Finland fortsätter det aktiva deltagandet i det normativa internationella samarbetet som gäller cybermiljön och i utbytet av åsikter om hur den internationella

rätten i vissa frågor reglerar användningen av staternas informations- och kommunikationstekniker. Finland uppdaterar sin ställning i fråga om tillämpning av internationell lag i cybermiljön. Finland påverkar beslutsfattandet rörande cybersäkerhet, cyberbrottslighet och cyberförsvar såväl inom FN, EU, Nato som även i andra viktiga internationella organisationer och nätverk. Finland är en pålitlig aktör i det euroatlantiska samarbetet och en säkerhetsproducent och ansvarsfull statlig aktör även vad gäller cybermiljön. Cybersamarbetet är omfattande och det fördjupas på grundval av gemensamma värden i synnerhet med viktiga likasinnade EU-länder, de nordiska länderna samt euroatlantiska länder och även vissa länder i indo-pacifiska regionen.

Finland främjar multilateral cyberdiplomati med mål att skapa och bibehålla en öppen, fri, säker och stabil cybermiljö. EU:s verktygslåda för cyberdiplomati ger verktyg för bekämpning och förebyggande av cyberhot. Finland skyddar sig mot potentiella cyberhot från tredjeländer genom cyberförsvar, cybersäkerhet och cyberdiplomati. Metoderna inom cyberdiplomatin innebär stärkande av det multilaterala systemet på grundval av internationell rätt, partnerskap, dialog och åtgärder som ökar förtroendet. EU:s gemensamma cyberpolitik och regleringen som påverkar cybersäkerheten utgör ett ramverk även för Finlands cybersäkerhetslagstiftning. Uppmärksamhet ska fästas vid genomförandet av den nya regleringen, bedömningen av dess konsekvenser och tillräckliga resurser för myndigheterna.

Finland stöder partnerskapsländer

Finland påverkar aktivt utvecklingen av EU:s cybersäkerhetspolitik och -reglering och för ut sin nationella modell som baserar sig på övergripande säkerhet och föregripande beredskap till unionen och de andra medlemsländerna. Stärkandet och etableringen av de nya cybersäkerhetsfunktioner och -organ som inrättats inom EU under de senaste åren är en viktig del i stärkandet av cybersäkerheten inom unionen och i byggandet av en nationell lägesbild. Målet är att främja utvecklingen av EU:s gemensamma vilja, såsom störningstolerans i cybermiljön. Ett viktigt mål är uppnående av en strategisk autonomi och bibehållande av en öppen ekonomi.

Som Natomedlem är Finland i kärnan av utvecklingen av cyberprestanda och en betydande producent av lösningar inom cybersäkerhet och -försvar inom

alliansen. Natos och EU:s cyberåtgärder kompletterar varandra och samordningen av åtgärderna stärker deras och Finlands nationella cybersäkerhet. Det bilaterala och multilaterala samarbetet inom cybersäkerhet och -försvar är den viktigaste samarbetsformen inom den operativa verksamheten nu och i framtiden.

En gemensam lägesuppfattning som grund för verksamheten

Det är viktigt med ett aktivt samarbete för att uppnå måltillståndet med cybersäkerheten. En gemensam lägesuppfattning möjliggör ett effektivt och tillförlitligt samarbete i cybermiljön mellan myndigheterna, företagen och organisationerna. Ett utvecklat samarbete mellan olika organisationsnivåer samt myndigheterna och den privata sektorn är endast möjligt genom kontinuerligt multilateralt informationsutbyte med låg tröskel och genom att skapa en lösningsorienterad samarbetskultur. Detta ökar förtroendet och stöder fullföljandet av sektoransvaren.

Utmaningar för samarbetet kring cybersäkerheten utgör distribueringen av regleringen och uppgifterna på flera olika aktörer samt de olika verksamhetsmodellerna för samarbetet och bristen på lämpliga gemensamma informationssystem. När det gäller observationsverksamheten i cybermiljön behöver informationsinsamlingen systematiseras så att det är möjligt att nå en mer omfattande lägesuppfattning om allvarliga hot som riktas mot Finland. En utvidgning av informationsutbytet förutsätter fastställande av tydliga förutsättningar och deltagande aktörer som skrivs in i lagstiftningen och även bedömning av grunderna för de nuvarande begränsningarna. Informationsutbytet ska även utvecklas genom harmonisering och precisering av de nuvarande lagtolkningarna samt genom revidering av de gemensamma verksamhetsmodellerna.

Tyngdpunkten för utvecklingen av samarbetet och informationsutbytet ligger på förebyggande och bekämpning av statliga cyberhot och cyberhot som riktar sig mot vitala samhällsfunktioner och kritisk infrastruktur samt skapande av verksamhetsförutsättningar i anknytning till detta. Informationsutbytet ska vara tillräckligt, stabilt, upprätthålla förtroendet och ändamålsbundet samt basera sig på rätten att lämna ut och få information samt intresset och rätten att dela information med dem som behöver den. Den som producerar eller innehar informationen ska kunna identifiera och dela informationen på eget initiativ i enlighet med lägesuppfattningen. Lägesinformation om allvarliga cyberhot måste

kunna delas effektivare än tidigare, och på ett ändamålsenligt sätt med hänsyn till begränsningarna i fråga om distribution, med företag som är kritiska för försörjningsberedskapen, kommuner, kommunalt ägda tjänsteleverantörer och välfärdsområdena. Delning av information med en hög säkerhetsklassificering förutsätter utveckling och införande av system som lämpar sig för detta.

I en utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerheten har man identifierat utvecklingsåtgärder, vars mål är att förbättra myndigheternas verksamhetsförutsättningar, skydda den nationella cybersäkerheten, bekämpa allvarlig cyberbrottslighet och utveckla cyberförsvaret och underrättelseinhämtningen för att motsvara de krav som cybermiljön i utveckling för med sig. Utvecklingsförslagen som gäller samarbetet och myndighetsprocesserna, upprättande av en lägesbild, informationsutbyte och -anskaffning samt reagerande på allvarliga cyberhot ska genomföras så att de överensstämmer med den identifierade hotmiljön. Ett aktivt myndighetssamarbete, upprättande av en lägesbild och -uppfattning samt säkerställande av förutsättningarna för informationsanskaffning är viktiga för att uppnå måltillståndet. Till exempel i fråga om de offentliga tjänsterna behövs det bättre metoder och förutsättningar än nu att samla in, analysera och dela information om nivån på cybersäkerheten och cyberresiliensen.

Myndigheternas samarbete är smidigt och friktionsfritt

Genomförandet av det operativa samarbetet, ansvaret samt beredskapen inför allvarliga cyberhot och -störningar och bekämpning av dessa samordnas i en samarbetsstruktur på ämbetsverksnivå, som består av Transport- och kommunikationsverket Traficom, centralkriminalpolisen, Försvarsmakten och skyddspolisen. Samordningen baserar sig på en gemensam delad lägesuppfattning. Utförandet av uppgifterna och bekämpningen av cyberhot sker på taktisk och teknisk nivå i ett aktivare och mer delaktigt myndighetssamarbete än tidigare.

Verksamhetskulturen i fråga om cybersäkerhet ska förnyas enligt modellen för övergripande säkerhet genom att stärka det nationella och internationella samarbetet gällande cybersäkerhet mellan statsförvaltningen, regionförvaltningen, lokalförvaltningen och organisationer. För att uppnå detta utnyttjas i allt större utsträckning internationella partners verksamhetsmodeller och tekniker som producerar cybersäkerhetslösningar. Som nya aktörer är det viktigt

att välfärdsområdena främjar cybersäkerhetskulturen och -kunnandet i samarbete med andra aktörer.

Centraliserade cybersäkerhetstjänster

Det är viktigt att förbättra den inbördes samordningen mellan internationella cybersäkerhetsprojekt. Utvecklingen av centraliserade cybersäkerhetstjänster och samordningen av användningen av dessa främjas. Genom att öka användningsgraden för tjänsterna kan verksamheten och utnyttjandet av kapaciteten effektiviseras och överlappningar undvikas. Transport- och kommunikationsverket Traficom, Myndigheten för digitalisering och befolkningsdata, övriga aktörer inom statsförvaltningen samt företag som ägs av välfärdsområden och kommuner tillhandahåller centraliserade cybersäkerhetstjänster tillsammans med den privata sektorn. Dessa används av stats-, region- och lokalförvaltningen samt av välfärdsområdena och till tillämpliga delar av företag, organisationer, högskolor och forskningsinstitut. De centraliserade tjänsterna ska vara driftsäkra, kostnadseffektiva, prestationsdugliga och användarvänliga. Målet med samarbetet är att ta fram material, utbildningar samt information och tjänster som är avsedda för gemensamt bruk.

Pelare IV: Insatser och svarsåtgärder

Insatser mot hot i rätt tid och en tryggad suveränitet

DELOMRÅDETS STRATEGISKA MÅL:

- Aktörerna inom den offentliga och privata sektorn har tydliga roller och behörigheter samt förmåga att reagera på cyberstörningar i rätt tid och på rätt sätt.
- Insatserna och svarsåtgärderna baserar sig på en heltäckande lägesuppfattning.
- Organiserad och allvarlig cyberbrottslighet bekämpas.
- Cyberförsvarsdoktrinen ger nationella verksamhetsprinciper för bekämpning av statliga hot och hot som äventyrar statens säkerhet.

En kränkning av statens suveränitet är en gärning som strider mot internationell rätt. Detta gäller även cybermiljön. Finlands utgångspunkt är att den internationella rätten och normerna för ansvarsfullt statsbeteende skapar väsentliga ramar för staternas verksamhet i cybermiljön.

Möjligheterna och förmågan att bekämpa cyberhot säkerställs

Det är viktigt att bekämpa cyberhot övergripande, långsiktigt och i rätt tid. Detta förutsätter att åtgärder som stärker cybersäkerheten och förebygger cyberhot utnyttjas i stor utsträckning och målmedvetet. Finland måste trygga sin statliga suveränitet även i cybermiljön. Finland bemöter utmaningarna som det geopolitiska läget ställer på cybermiljön genom aktiva åtgärder inom cyberdiplomatin, -försvaret och -säkerheten både självständigt och som en del av multilateral verksamhet.

Möjligheterna och förmågan hos aktörerna i samhället att bekämpa cyberhot ska säkerställas i alla förhållanden. För att samhället ska fungera störningsfritt krävs det att organisationerna har förmåga att snabbt återhämta sig från cyberstörningar och attacker samt snabbt och säkert återställa systemen i bruk.

De myndigheter som svarar för den operativa verksamheten ska förebygga, reagera, utreda och bilda en lägesbild om cyberhot. Cyberhotens karaktär ställer krav på ledningen av myndigheternas samarbete och deras samverkan. Reaktionen och bemötandet i fråga om statliga cyberoperationer är annorlunda än i fråga om vanliga cyberhot. Att svara på statlig fientlig cyberverksamhet med straffrättsliga ansvarsåtgärder är inte nödvändigtvis det effektivaste sättet. Hoten bekämpas genom att kombinera olika metoder och åtgärder i hela cybermiljön och på olika nivåer av verksamheten samt även genom att bedöma perspektiven med avseende på internationell rätt. Hoten i cybermiljön som ständigt utvecklas kräver att olika aktörers roller och ansvar fastställs uttömmande för att bekämpa cyberattacker.

Möjligheterna att utnyttja ett övergripande och omfattande utbud av metoder framhävs framför allt i fråga om bekämpning av statliga operationer och allvarlig cyberbrottslighet. I den nya verksamhets- och hotmiljön räcker det inte enbart att fastställa rollerna och ansvaret genom tekniskt eller funktionellt skydd av funktionerna och infrastrukturen, utan den fientliga verksamheten ska kunna bekämpas i hela verksamhetsmiljön. Det målinriktade angreppssättet ska kompletteras så att man utöver det vanliga säkerställandet av resiliensen och datasäkerheten även vidtar mer omfattande övergripande åtgärder. Det räcker alltså inte längre att man till exempel enbart skyddar informationssystemen genom datasäkerhetsmetoder, utan det behövs nya metoder, såsom effektiviserat internationellt informationsutbyte, sanktioner eller aktivt cyberförsvar.

Ledningsmodellen för situationer med cyberstörningar och hot utvecklas.

För att stödja insatser och svarsåtgärder i rätt tid upprättas en gemensam analyserad lägesbild av de operativa myndigheterna. Den bidrar till att skapa en gemensam lägesuppfattning, vilket möjliggör planering, beredning och genomförande av åtgärder. Ledningsmodellen skapas i den samarbetsstruktur på ämbetsverksnivå som beskrivs ovan i pelare III. Samarbetsstrukturen och de myndigheter som ingår i denna ska ha tillräckliga rättigheter att lämna ut och få information för att verksamheten ska kunna samordnas. Tyngdpunkten för den nationella cybersäkerheten och informationsanskaffningen, rätten att få information och informationsutbytet som denna medför för myndigheter lig-

ger på alla förvaltningsnivåer i fråga om förebyggande och bekämpning av allvarliga cyberhot och -brottslighet som riktar sig mot vitala samhällsfunktioner, den nationella säkerheten, landets försvar och försörjningsberedskapen.

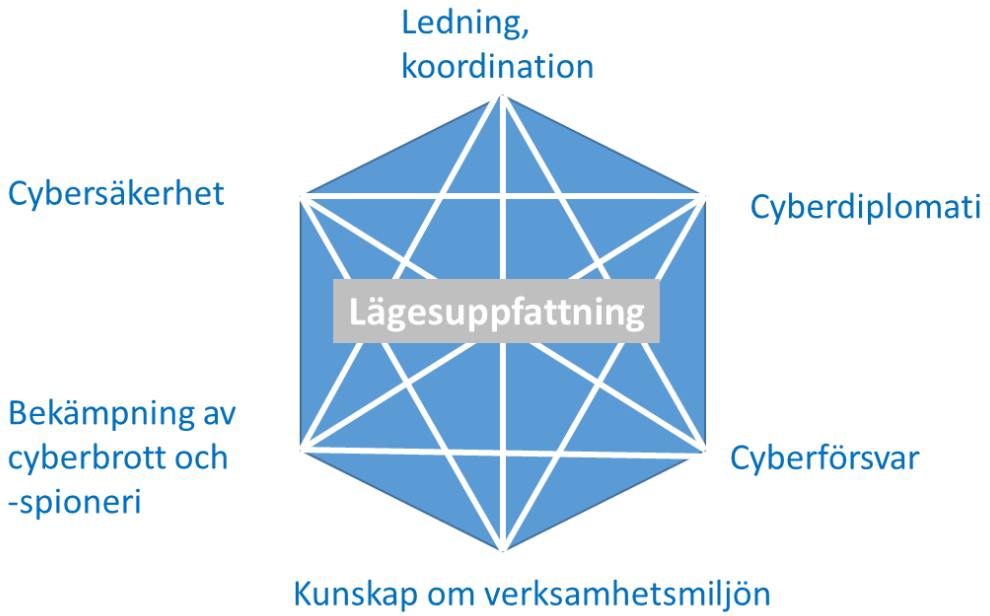


Bild 2 En gemensam lägesuppfattning är en grundläggande förutsättning för samordnade åtgärder.

Organiserad och allvarlig cyberbrottslighet bekämpas.

Cyberbrottslighet bekämpas genom att avslöja, förebygga och utreda misstänkta brott samt genom att utnyttja kriminalunderrättelseverksamhet som baserar sig på effektiv kunskapsledning. Myndigheterna har som mål att särskilt bekämpa organiserad och allvarlig cyberbrottslighet, försvaga brottslingars verksamhetsförutsättningar och säkerställa att organiserade kriminella grupper eller andra aktörer som är farliga för samhället inte utvidgar sin verksamhet till samhällsstrukturerna, ekonomin eller beslutssystemen.

Verksamhetsförutsättningarna för de rättsliga och brottsbekämpande myndigheterna samt det nationella gränsöverskridande samarbetet och det informationsutbyte som det kräver utvecklas för att svara mot den förändrade säkerhetsmiljön. I bekämpningen av den gränsöverskridande cyberbrottsligheten utnyttjas gemensamma internationella utredningsgrupper. Den information som tas fram genom brottsbekämpning och dess urval av metoder utnyttjas bättre än hittills som stöd för cyberförsvaret, attribuering och svarsåtgärder. Attribuering innebär insamling och analys av fakta, teknisk och juridisk bedömning, beslutsfattande och slutligen kommunicering av beslutet till olika aktörer. I den övergripande attribueringsprocessen måste man kunna utnyttja all information som anknyter till attribueringen, och som tas fram bland annat av underrättelse-, cybersäkerhets- och förundersökningsmyndigheterna inom deras lagstadgade uppgifter. Man säkerställer att Finland har förutsättningar att bekämpa statlig cyberverksamhet som riktar sig mot Finland eller Finlands intressen genom att se till att underrättelse- och säkerhetsmyndigheterna har aktuella befogenheter och verksamhetsförutsättningar.

Cyberförsvarets uppgifter och roll preciseras

För att stödja genomförandet av det nationella cyberförsvaret utarbetas en cyberförsvarsdoktrin, där målen med cyberförsvaret preciseras. I den beskrivs hur cyberförsvaret genomförs genom användning av kapacitet som finns nationellt eller kommer med Nato, övriga kapaciteter och verksamhetsmöjligheter. Cyberförsvaret utvecklas stabilt vid sidan om utvecklingen av den nationella cyberresiliensen, -säkerheten och -brottsbekämpningen. Det nationella och militära cyberförsvarets roll i freds-, kris- och konfliktförhållanden har justerats till den nivå som säkerhetsmiljön kräver. Utvecklingen av det nationella cyberförsvaret är också en del av utvecklingen och genomförandet av landets försvar som helhet.

Finland granskar sin ställning och förhållningssätt till den fientliga verksamhet som sker i cybermiljön. Nationellt har man beredskap för ett aktivt cyberförsvar samt möjligheter till attribuering av motståndaren och svarsåtgärder. Cyberförsvarsverksamheten samordnas med den utrikes- och säkerhetspolitiska verksamheten och aktörerna inom denna.

Målet är att Finland bekämpar cyberhot orsakade av tredjeländer genom såväl förebyggande, reaktiva som långsiktiga åtgärder och i stor utsträckning utnyttjar hela det nationella utbudet av metoder och kapacitet. Dessa är bland annat metoder inom diplomati, underrättelseinhämtning, informationshantering och strategisk kommunikation, militär kapacitet, brottsbekämpning och finansbranschen samt ekonomiska och rättsliga metoder samt andra cybersäkerhetsmetoder. Om statliga organ eller privata grupper eller privatpersoner som agerar för en stats räkning kan identifieras som genomförare av cyberoperationer som strider mot statens internationella förpliktelser, är staten i fråga ansvarig för dem.

Det ligger i Finlands intresse att ha ett nära samarbete med internationella aktörer på multilateral, regional och bilateral nivå. Detta gäller tekniskt, operativt och strategiskt samarbete, utveckling av internationella normer och standarder, den politiska dialogen samt förmågan att genomföra attribuering och svarsåtgärder. Finland deltar även fullt ut i Natos cyberförsvar och utnyttjar EU:s verksamhetsmöjligheter i fråga om resultatsamarbetet, informationsutbyte, samordnade svarsåtgärder och reglering som stöd för det nationella cyberförsvaret. Cyberförsvaret är en del av Finlands och Natos försvar och avskräckning.

Resursering, genomförande och uppföljning

Resurser

I Finland bekämpar cybersäkerhetsaktörerna hot varje dag. Förändringen i verksamhetsmiljön ökar och diversifierar cyberhoten och -riskerna. Således måste även resurserna ökas så att de motsvarar hotmiljön i förändring och regleringen som förnyas. Redan för att upprätthålla det nuvarande läget behövs det mer resurser än nu och en effektiviserad användning av dem.

I nuläget använder Finland nästan 300 miljoner euro årligen på att säkerställa cybersäkerheten inom statsförvaltningen. Utöver detta använder region- och lokalförvaltningen resurser för sin egen cybersäkerhet, men uppföljningen av deras användning ska ännu utvecklas. Det bör också beaktas att näringslivet äger en betydande del av Finlands kritiska infrastruktur och svarar för säkerställandet av dess cybersäkerhet. Enligt en försiktig uppskattning är näringslivets satsningar i cybersäkerhet minst tiofalt större än den finansiering som statsförvaltningen anvisar. Även med avseende på försörjningsberedskapen är de resurser som företagen använder på cybersäkerheten allt viktigare. Investeringar i cybersäkerhet sker även indirekt. Till exempel satsas det på cyberkompetens i Finland på alla utbildningsstadier och i olika forskningsprojekt. De pengar som investeras i cyberutbildning och -forskning märks ofta först senare i form av en stärkt cybersäkerhet.

Mer resurser måste allokeras för genomförandet av alla strategiska mål och utvecklingsåtgärder. En ändring av Finlands cyberprofil kräver förutom ökade resurser även precisering av planeringen och uppföljningen av dem samt en effektiviserad användning.

Uppbyggande av ett fungerande och livskraftigt ekosystem för cybersäkerhet innebär betydande ekonomiska investeringar för hela samhället. Ett fungerande ekosystem producerar livskraft och tillväxt, ökar arbetsplatserna inom branschen, tar fram behövlig kompetens och förbättrar det digitala samhällets hållbarhet och tolerans mot skadliga fenomen i cybermiljön.

Ett mer omfattande och djupare utnyttjande än hittills av modellen för övergripande säkerhet i säkerställandet av cybersäkerheten samt beredskapen, insatserna och svarsåtgärderna som baserar sig på denna är nödvändiga åtgärder för att kunna undvika kostnader som orsakas av allvarliga cyberstörningar. Modellen med övergripande säkerhet effektiviserar användningen av de befintliga resurserna och ökar den allmänna resiliensen då kompetensen och verksamhetsmodellerna samt bästa praxis kan delas mellan organisationer som förberett sig på olika nivåer.

En högklassig forsknings- och utvecklingsverksamhet angående omvälvande tekniker samt investeringar i den nationella cybersäkerheten är väsentliga metoder för att bibehålla ett cybersäkert och cyberkriståligt samhälle. Det är viktigt att stödja FUI-verksamheten även för att öka Finlands konkurrenskraft. Kunnande behövs på alla nivåer, och resursering krävs till exempel för det upplysnings- och rådgivningsarbete som utförs av organisationer som når ut till en betydande del av medborgarna eller för cyberövningar som ordnas av olika aktörer.

Utnyttjande av Natos innovationsfinansiering och EU:s utvecklingsfinansiering är en väsenligt del av utvecklingen av Finlands cyberekosystem. Detta kräver medfinansiering av Finland och samordning av resursanvändningen mellan förvaltningsområdena. Dessutom förutsätter Natomedlemskapet ytterligare satsningar i cybersäkerhet och -försvar samt i utveckling av infrastrukturens cyberresiliens. Natomedlemskapet kräver även ny prestanda och nya resurser av Finland som stöd för de allierade. Samtidigt krävs det även tillräckliga resurser av myndighetsuppgifterna och skyldigheterna, som ökat i och med EU-regleringen.

När de nationella resurserna fastställs är det viktigt att bedöma de alternativa kostnaderna, dvs. kostnaderna som uppkommer om utvecklingsåtgärderna enligt strategin inte genomförs effektivt. Dessa är förutom de personal- och IKT-kostnader som orsakats av genomförda cyberattacker även till exempel följderna av informationsläckor, cyberbrottslighet och ryktesskador.

Genomförande och uppföljning av strategin

Enligt EU:s cybersäkerhetsdirektiv (NIS2) och dess nationella genomförande ska behovet av uppdatering av den nationella cybersäkerhetsstrategin bedömas vart femte år. Vid behov utvecklas och uppdateras strategin oftare. Uppdateringarna görs i samarbete med myndigheter, näringslivet, forskningsinstitut, organisationer och medborgare.

Genomförandet av strategin följs upp årligen på nationell nivå. Statens cybersäkerhetsdirektörs byrå har ansvaret för att samordna uppföljningen, och förvaltningsområdena utarbetar en rapport åt byrån om genomförandet av cybersäkerheten inom sitt ansvarsområde i enlighet med tidsplanen för den offentliga ekonomins planeringsprocess. Av dessa rapporter gör byrån en sammanställning åt myndigheterna och de politiska beslutsfattarna. Uppföljningen av strategin rapporteras till ministerarbetsgruppen för samhällsförnyelse och framskridandet informeras även till ministerarbetsgruppen för inre säkerhet och rättsvård samt till Säkerhetskommittén.

Arbetet i arbetsgruppen som tillsatts för revidering av strategin för cybersäkerhet fortsätter efter att strategin blivit färdig, och gruppen ändras till en uppföljningsgrupp för genomförandet av strategin. Uppföljningsgruppen utarbetar en genomförandeplan för strategin inom sex månader efter att strategin blivit färdig. I genomförandeplanen anges genomförandeansvaret och tidsplanen per förvaltningsområde och de mätare med vilka genomförandet av strategin följs upp och utvärderas årligen beskrivs närmare.

I arbetet med att definiera resultatindikatorerna för cybersäkerheten utnyttjas till tillämpliga delar bland annat EU:s cybersäkerhetsbyrå ENISA, OECD:s och Natos cyberenkäter, enkäten för organisationens digitala säkerhet (offentliga förvaltningen) som MDB låter göra varje år, cybermognadsindikatorerna för Försörjningsberedskapscentralens sektorer (näringslivet) samt barometern för digital säkerhet (medborgarnas cybertålighet) som MDB tar fram.

Målet är att utvidga indikatorerna för cybertålighet så att de även omfattar förebyggande cyberberedskapsarbete. I definieringen av de väsentliga indikatorerna söker Finland vid behov stöd av EU:s Enisa i enlighet med bestämmelserna i NIS2-direktivet. Finlands internationella framgång följs även upp på basis av internationella index (ITU: Global Cybersecurity Index (GCI) och e-Governance Academy: National Cyber Security Index (NCSI).

I det strategiska genomförandet betonas identifiering av bästa praxis och omfattande användning av tillvägagångssätt som man lärt sig genom incidenter. På så sätt främjas uppkomsten och upprätthållandet av konsekventa tillvägagångssätt och hela samhällets resiliens stöds. Syftet med utvärderingen av genomförandet är att stödja politiskt beslutsfattande, myndighetsverksamhetn och den samhälleliga debatten.

Strategiska utvecklingsförslag

Utvecklingsförslagen nedan har utformats på grundval av de strategiska målen. Utifrån utvecklingsförslagen utarbetas en noggrannare genomförandeplan med en tidsplan och ansvarsfördelning.

- Finlands ställning i fråga om cybersäkerhet och cyberförsvar klargörs, deltagandet i internationellt samarbete kring cybersäkerhet utvecklas och för detta upprättas en behövlig nationell samordning.

- Förberedelser görs för de hot och möjligheter som kommer av att nya omvälvande tekniker, särskilt kvantberäkning, utvecklas.

- Utvecklingen av en teknisk suveränitet och ett ekosystem för cybersäkerhet främjas och Finlands tekniska pionjärskap och nya innovationer säkerställs.

- Myndigheternas samarbete och gemensamma lägesuppfattning utvecklas genom att skapa behövliga samarbetsstrukturer och samordningsmodeller, förtydliga rollerna och ansvarsfördelningen samt säkerställa förutsättningarna för informationsutbyte och tillgång till information.

- Den rättsliga grunden, normerna och anvisningarna ändras på det sätt som strategins utvecklingsåtgärder kräver.

- Samarbetet mellan myndigheterna, region- och lokalförvaltningen, privata sektorn och civilsamhället och den gemensamma beredskapen stärks.

- Förtroende upprätthålls och stärks genom säkra och driftsäkra offentliga tjänster.

- Cybersäkerhetsresurserna planeras och följs upp långsiktigt.

- Kunnandet samt medborgarnas och civilsamhällets cyberfärdigheter och beredskap utvecklas.

- Övningsverksamheten och -miljöerna utvecklas för att öka beredskapen och kompetensen.

- Verksamhetsmiljökunskaperna utvecklas bland annat genom att säkerställa den nationella observationsförmågan samt säkerhets- och underrättelsemyndigheternas möjligheter att skaffa information om cybermiljön.

- Övergripande bekämpning av cyberbrottslighet främjas.

- Cyberförsvaret utvecklas som en del av landets försvar som helhet, säkerställandet av Finlands suveränitet och integration i alliansens försvar.

- Cybersäkerhetssynvinklar bedöms i alla lagstiftningsprojekt.

Bilagor

Bilaga 1: En nationell samarbetsmodell för cybersäkerhet

I denna bilaga beskrivs nuläget för den nationella samarbetsmodellen för cybersäkerhet och dess aktörer och kraven enligt cybersäkerhetsdirektivet (NIS2) bemöts ur nationell synvinkel.

Den nationella samarbetsmodellen för cybersäkerhet (nedan samarbetsmodellen för cybersäkerhet) i Finland är distribuerad och motsvarar till sina principer samarbetsmodellen för övergripande säkerhet (nedan modellen för övergripande säkerhet). Samarbetet baserar sig på lagstadgade uppgifter, samarbetsavtal och säkerhetsstrategin för samhället, där cybersäkerheten beaktas i varje strategiska uppgift. Samarbetsmodellen för cybersäkerhet är skalbar på alla nivåer, dvs. den kan tillämpas på allt från nationell nivå till regional och lokal nivå, med beaktande av internationella partner.

Målet med den övergripande säkerheten är att säkerställa ett aktivt beredskapssamarbete mellan de väsentliga aktörerna i alla förhållanden. Mer omfattande beredskapsåtgärder samordnas i samarbete med de behövliga aktörerna inom den offentliga och privata sektorn. Samarbetsmodellen för cybersäkerhet vidareutvecklas i enlighet med modellen för övergripande säkerhet med beaktande av särdragen för cybersäkerhet.

I en sådan cyberkrissituation som avses i samarbetsmodellen för cybersäkerhet och i cybersäkerhetsdirektivet leder de behöriga myndigheterna hanteringen av störningssituationen inom ramen för vars och ens uppgifter och behörighet. De behöriga myndigheterna, samordningen av verksamheten samt stödet fastställs vid behov enligt modellen för krisledning i samhället. Varje aktör svarar för sin beredskap och är genom beredskapslagen och sektorlagstiftningen skyldig att se till att de kritiska tjänsterna fungerar i alla förhållanden, till exempel genom att ställa krav på serviceproducenterna och övervaka uppfyllandet av dem. Beredskapen inför situationer med cyberstörningar och reagerandet på dem genomförs i aktivt samarbete med den offentliga sektorn, näringslivet och civilsamhället. De centraliserade cybersäkerhetstjänster som

den offentliga sektorn tillhandahåller tillsammans med näringslivet stöder organisationerna och medborgarna i beredskapsarbetet och i störningssituationer. På så sätt säkerställs en enhetlig verksamhet, överlappande kostnader undviks och tjänster som behövs allmänt, såsom webbutbildningar, cyberlägesbilder och anvisningar, är tillgängliga för alla. Myndigheterna, såsom Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter (nedan Cybersäkerhetscentret), samt de som producerar offentliga tjänster kommunicerar aktivt såväl till medborgarna, företag som offentliga aktörer om störningssituationer och sårbarheter som gäller cybersäkerheten.

Cybersäkerhetscentret fungerar som koordinator mellan myndigheterna som hanterar cyberkriser i enlighet med cybersäkerhetsdirektivet. Det svarar även för utarbetandet av de ramar för hantering av cybersäkerhetskriser som krävs enligt det nationella NIS2-direktivet för hantering av storskaliga cybersäkerhetsincidenter och -kriser i samarbete med andra myndigheter.

Nedan beskrivs olika aktörer i samhället i säkerställande av den nationella cybersäkerheten. Beredskap, insatser och svarsåtgärder genomförs i ett omfattande samarbete, där det även ingår informationsutbyte för att åstadkomma en gemensam lägesuppfattning och samordna de gemensamma åtgärderna.

Figur 3: Olika aktörer i samhället i säkerställande av den nationella cybersäkerheten

Politiskt beslutsfattande

I det politiska beslutsfattandet avgörs betydande frågor som gäller cyberberedskap och hantering av störningar, såsom lagstiftningsriktlinjer och beslut enligt den utrikes- och säkerhetspolitiska processen. Myndigheterna rapporterar om cybersäkerhetsläget och åtgärderna till republikens president, riksdagen, statsrådet och ministerarbetsgrupperna.

Strategisk nivå

Statsrådet och dess ministerier svarar för beredningen av den nationella cybersäkerhetslagstiftningen, allmänna riktlinjer, resursallokering, verksamhetsprinciper, strategisk styrning, beredskapsarbetet samt svarsåtgärder och samarbete.

Statens cybersäkerhetsdirektörs byrå svarar för koordinationen och samordningen av utvecklingen och planeringen av den nationella cybersäkerheten, beredskapen rörande denna samt beredskapen som gäller den kritiska informations- och kommunikationstekniska infrastrukturen. Statens cybersäkerhetsdirektör koordinerar och samordnar utvecklingen och planeringen av den nationella cybersäkerheten, beredskapen rörande denna samt fungerar som statsledningens rådgivare i frågor som gäller cybersäkerhet.

Samordningsgruppen för cybersäkerhet, som är tillsatt av kommunikationsministeriet, fungerar också på en strategisk nivå och dess mål är att säkerställa att de nationella ministerierna som svarar för cybersäkerhet, cyberförsvar och cyberdiplomati och cybersäkerhetsmyndigheterna har en enhetlig lägesbild av samhällets cybersäkerhetsläge och de händelser som påverkar cybersäkerheten samt förändringarna i cybersäkerhetsmiljön.

Tillsynsmyndigheter (NIS2 och andra)

Med tillsynsmyndigheter avses tillsynsmyndigheter enligt [*NIS2-lagen*]. De övervakar privata och offentliga tjänsteleverantörers beredskap, störningshantering och återhämtning enligt [*NIS2-lagen*]. I Finland följer man en distribuerad modell, varvid sektormyndigheterna övervakar aktörerna inom sin sektor. Dessutom fungerar Cybersäkerhetscentret som nationell samordningspunkt. Tillsynsmyndigheter är Transport- och kommunikationsverket Traficom, Energimyndigheten, Säkerhets- och kemikalieverket, Tillstånds- och tillsynsverket för social- och hälsovården, NTM-centralen i Södra Savolax, Livsmedelsverket, Säkerhets- och utvecklingscentret för läkemedelsområdet samt Finansinspektionen.

Till följd av cyberattacker, såsom dataintrång, kan inkräktaren få tillgång till exempelvis personuppgifter, varvid det är fråga om en personuppgiftsincident. I

fråga om personuppgiftsincidenter är Dataombudsmannens byrå den nationella tillsynsmyndigheten och övervakar iakttagandet av dataskyddslagstiftningen.

Dessutom finns det andra tillsynsmyndigheter, såsom Strålsäkerhetscentralen och Finlands Bank.

Operativa myndigheter

De operativa myndigheterna inom cybersäkerhet har en viktig nationell roll såväl när det gäller beredskapen inför cyberstörningar som insatser och svarsåtgärder mot dessa. I Finland finns det dessutom flera nationella nätverk för informationsutbyte på frivilligbasis.

Cybersäkerhetscentrets centrala uppgift är att svara för upprätthållandet av en lägesbild över den nationella cybersäkerheten och för den nationella sårbarhetskoordinationen. Det samlar in och analyserar information om informationssäkerhetshot och säkerhetsöverträdelser samt utreder för sin del tekniska incidenter som riktas mot Finland. Till dess uppgifter hör även att öka den allmänna cybersäkerhetsmedvetenheten. Cybersäkerhetscentrets kunder kan använda information om lägesbilden när de ordnar och prioriterar sin beredskap.

Förundersökningsmyndigheterna har som uppgift att förebygga brott samt utreda parterna i händelsen och fakta för straffprocessen i fråga om brott som begåtts. Straffprocessen omfattar polis, åklagare och domstol. Polisen utreder brott i informationsnät och försöker även förebygga eventuella framtida brott utifrån den information som polisen har fått. Polisen uppdaterar den nationella lägesbilden av brott i informationsnät. Även till exempel centralkriminalpolisen är aktivt delaktiga i att öka medvetenheten särskilt inom den förebyggande verksamheten.

Underrättelsemyndigheter är skyddspolisen och de militära underrättelsemyndigheterna (Försvarsmaktens huvudstab och Försvarsmaktens underrättelsetjänst). Underrättelsemyndigheterna har som uppgift att skaffa information samt analysera och rapportera den som stöd för säkerhetsmyndigheterna och

den statliga ledningen. Underrättelseinformationen bidrar till att förutse cyberhot mot Finland och för de behöriga myndigheterna att bekämpa dem. Underrättelsemyndigheterna utför underrättelseinhämtning bland annat för att utreda gärningsmännen vid cyberattacker som sker på nätet samt bakgrunden och motiven till attackerna i syfte att skydda den nationella säkerheten, som stöd för den högsta statliga ledningens beslutsfattande även i attribueringsprocessen samt för andra myndigheters lagstadgade uppgifter med anknytning till den nationella säkerheten.

Försvarsmaktens uppgifter kan även anses omfatta cybermiljön (cyberförsvar och underrättelseinhämtning i cybermiljön). I anslutning till detta omfattar Försvarsmaktens uppgifter bland annat det militära försvaret av Finland, stödjande av andra myndigheter samt internationellt bistånd, samarbete och annan internationell verksamhet. Försvarsmakten tryggar Finlands territorium, befolkningens livsbetingelser och statsledningens handlingsfrihet samt försvarar den lagliga samhällsordningen vid behov med militära maktmedel när ett väpnat angrepp eller ett motsvarande yttre hot riktas mot Finland.

Central-, region- och lokalförvaltningen samt självständiga inrättningar

Ämbetsverken och de regionala och lokala myndigheterna samt självständiga inrättningar har en central roll i att sörja för cybersäkerheten i myndigheternas dagliga verksamhet. Aktörerna omfattar statens ämbetsverk, affärsverk och bolag, aktörer inom regionförvaltningen, välfärdsområdena, kommunerna och samkommunerna samt offentliga serviceproducenter och självständiga inrättningar. En del av dessa har skyldighet att styra, övervaka, anvisa, hjälpa, samordna, stödja och varna samt samla in, analysera och dela information även som stöd för beslutsfattande om cybersäkerheten och utveckling av verksamheten. De producerar även offentliga tjänster i samarbete med näringslivet och sörjer för tjänsternas säkerhet, risk- och kontinuitetshanteringen samt beredskapen.

Företag och sammanslutningar

Funktionerna, kompetensen och resurserna inom den privata sektorn utgör en betydande del av Finlands nationella cybersäkerhet. Merparten av Finlands kritiska infrastruktur ägs av näringslivet. Säkerställandet av vitala funktioner

och den kritiska infrastrukturen är viktiga med avseende på samhällets funktionsförmåga, kontinuitetshanteringen och försörjningsberedskapen. Utöver den tekniska förmågan har företagen även en stark kompetensgrund, vilja och resurser att förbereda sig på cybersäkerhetshot i sin affärsverksamhet både i hemlandet och på den internationella marknaden.

Näringslivets beredskap baserar sig delvis på lagstiftning, men även på frivilligt beredskaps- och försörjningsberedskapsarbete. Den offentliga och privata sektorn samarbetar dagligen kring inhämtandet av en lägesbild och genom aktivt informationsutbyte samt långsiktigt utvecklingsarbete. Aktörerna inom näringslivet deltar aktivt i olika samarbetsgrupper, vilket ökar förtroendet mellan den privata och offentliga sektorn och erbjuder en möjlighet till ett effektivt samarbete även internationellt.

Näringslivet tillhandahåller merparten av samhällets informations- och cybersäkerhetstjänster. De privata IKT-tjänsteleverantörerna är i en central ställning i fråga om cybersäkerheten för medborgare, företag samt statliga och regionala aktörer.

Försörjningsberedskapsorganisationen

Försörjningsberedskapsorganisationen är ett nätverk som omfattar Försörjningsberedskapscentralen och dess styrelse, försörjningsberedskapsrådet samt sektorerna och poolerna inom olika branscher. De försörjningsberedskapskritiska aktörerna hör till Försörjningsberedskapscentralens sju sektorer eller åtta pooler. Till Försörjningsberedskapscentralens lagstadgade uppgifter hör att med hjälp av sitt samarbetsnätverk utveckla och samordna den offentliga förvaltningens och näringslivets samarbete i försörjningsberedskapsfrågor. Aktörerna upprätthåller och utvecklar försörjningsberedskapen och kontinuitetshanteringen även ur perspektivet cybersäkerhet i nätverket för företagen och organisationerna inom den egna branschen i samarbete med myndigheterna.

Aktörer som ska övervakas (NIS2)

Skyldigheterna som gäller riskhantering och incidentrapportering enligt [NIS2-lagen], dvs. cybersäkerhetslagen, tillämpas på de övervakande aktörerna, dvs. [*kompletteras då RP framskrider].*

Serviceproducenter och deras leveranskedjor

Med serviceproducenter avses organisationer som producerar tjänster eller produkter åt samhället. En serviceproducent svarar för cybersäkerheten under sin tjänsts eller produkts livscykel så att det täcker hela värdekedjan. Cybersäkerheten för leveranskedjan säkerställs genom riskhanteringsmetoder i enlighet med [NIS2-lagen] eller på avtalsbasis.

Forskningsinstitut och högskolor är också serviceproducenter. De producerar kompetens- och kunskapskapital och innovationer för cybersäkerhet.

Organisationer och aktörer inom fjärde sektorn

Finland är känt i världen för sina talrika medborgarorganisationer och människornas starka vilja att delta i civilsamhällets verksamhet. Betydelsen av medborgarorganisationer och frivilliga ökar också inom säkerställandet av den nationella cybersäkerheten. Integrering av organisationsfältet i cybersäkerhetsnätverk främjar den nationella resiliensen, och dessutom behöver organisationerna stöd för utveckling av cybersäkerheten av andra aktörer. Det är enkelt att närma sig organisationerna och man litar på dem, varför organisationsfältets roll är betydande i utvecklingen av medborgarfärdigheterna. Dessutom erbjuder i synnerhet Försvarsutbildningsföreningen (MPK) stöd för utveckling av cybersäkerheten genom att ordna kurser och utveckla och öka cyberreserven. Organisationernas roll är inte ännu en etablerad del av ekosystemet för cybersäkerhet.

Organisationerna och fjärde sektorn, dvs. aktörerna inom den oorganiserade medborgarverksamheten, har mycket att bidra med i form av stöd för hanteringen av störningssituationer, och det finns redan erfarenheter av deras stöd till myndighetsverksamheten i hanteringen av betydande störningssituationer.

Medborgare

Individens kompetens stärker organisationernas och samhällets cyberresiliens. Nya tekniska lösningar utgör en allt mer bestående del av det dagliga li-

vet, vilket lyfter fram även den enskilda medborgarens roll i den nationella cybersäkerheten. Vaksamhet behövs såväl i hemförhållanden som i arbetslivet, och var och en kan genom sina egna handlingar påverka hur störningarna i cybermiljön påverkar livet. Cybersäkerhet är en naturlig del av varje individs samhällsansvar, som kräver kontinuerlig utveckling och upprätthållande av know-how. Även stödet till närstående och anmälan i rätt tid om egna observationer främjar upprätthållandet och utvecklingen av den nationella cyberresiliensen, samt utredningen av cyberbrott.

Termer

Termerna nedan jämte sina definitioner beskriver de begrepp som används i detta dokument. Termerna har använts för att koncentrera framställningen av strategin och undvika upprepning, och genom att förklara termerna avser man underlätta läsarens förståelse av det avsedda sammanhanget. Termerna som används i strategin avviker delvis eller helt från befintliga ordlistor, såsom Termbanken Tepa eller ordlistan om cybersäkerhet, eftersom ett behov av uppdatering i fråga om de nationella begreppen som gäller cybersäkerhet har konstaterats. Uppdateringsbehovet beror särskilt på strävan efter internationellt enhetliga begrepp samt på införandet av de begrepp som ingår i lagstiftningen, särskilt i EU-reglering, i vokabulären.

Nationell cybersäkerhet

Åtgärder som medför att det digitala samhället kan bereda sig på, identifiera, bekämpa och klara av störningar i elektroniska och nätverksanslutna system och deras konsekvenser för vitala samhällsfunktioner och -tjänster, återhämta sig från dessa samt för sin del säkerställa verksamhetsförutsättningarna för den nationella säkerheten, landets försvar och försörjningsberedskapen.

Cybersäkerhet

Åtgärder för att skydda kommunikations- och informationssystem samt andra elektroniska system, de uppgifter som lagras, behandlas eller överförs i dem samt deras användare, utnyttjare och andra berörda personer från cyberhot.

Nationellt cyberförsvar

Nationella och internationella militära och civila branschers åtgärder för att säkerställa Finlands självständighet som stat samt folkets livsbetingelser och säkerhet gentemot yttre cyberhot och -störningar orsakade av stater och de svarsåtgärder som behövs för genomförandet i alla beredskapslägen.

Militärt cyberförsvar

Åtgärder för att säkerställa system och aktörer inom olika sektorer som påverkar Finlands försvarsförmåga i synnerhet mot statliga hotfulla aktörer och deras företrädare för att säkerställa försvarsförmågan samt säkerställa Finlands suveränitet och genomföra militära cyberoperationer.

Resiliens; ~kristålighet; ~kristolerans

Statens, organisationernas, sammanslutningarnas och individernas förmåga att upprätthålla funktionsförmågan i föränderliga förhållanden samt beredskap att bekämpa störningar och kriser och återhämta sig från dem.

Cyberresiliens; ~cybertolerans

Statens, organisationernas, sammanslutningarnas och individernas förmåga att upprätthålla funktionsförmågan i cybermiljöns föränderliga förhållanden samt beredskap att bekämpa störningar och hot, återhämta sig från dem och vid behov reagera på dem.

Cyberhygien

Ett säkerhetsorienterat tankesätt, en utvecklad organisatorisk säkerhetskultur, i kombination med vardagens regelbundna rutiner, praxis och processer, genom vilka organisationen och individen för sin del utvecklar och upprätthåller cybersäkerheten i miljön vid användning av informationssystem, datorer eller andra enheter.

Cyberhot

En potentiell situation, händelse eller aktivitet som kan skada eller störa kommunikationsnät och informationssystem, användarna av sådana system och andra personer eller på något annat sätt påverka dessa skadligt.

Cybermiljö, -rymd

Med cybermiljö avses ett globalt utrymme skapat och förvaltat av människan, som baserar sig på informationsteknologi och användning av det elektromagnetiska spektrumet för att skapa, redigera, utbyta och utnyttja information

både genom sammankopplade och från varandra fristående nätverk som är använder informationsteknologi.

Cybermiljö

Cybermiljön består av ett eller flera informationssystem som är avsedda för behandling av data eller information i digital form, deras fysiska och logiska struktur samt aktörerna i verksamhetsmiljön med sina naturliga och digitala identiteter. Cybermiljön betonar användningen av cybermiljön ur synvinkeln målinriktad verksamhet.

Vital samhällsfunktion

En funktion som är nödvändig för att samhället ska fungera.

Kritisk infrastruktur, kritisk infrastruktur för samhället

Nyttighet, utrymme, apparatur, nätverk eller system eller del av nyttighet, utrymme, apparatur, nätverk eller system, eller viktig tjänst som är nödvändig för att upprätthålla de vitala samhällsfunktionerna eller för att tillhandahålla någon annan viktig tjänst.

Kritisk infrastruktur för försvarsförmågan

Strukturer och tjänster i fråga om försvarssystemet och kritisk infrastruktur och funktioner i anknytning till dessa samt de vitala samhällsfunktioner som är nödvändiga för försvarets verksamhetsförutsättningar i alla beredskapslägen.

Attribuering, tillräknande

Identifiering, lokalisering och individualisering av den som genomför en fientlig cyberoperation genom en analytisk process som utnyttjar olika informationskällor. På nationell nivå omfattar processen såväl teknisk analys som myndighetsansvar samt utrikes- och säkerhetspolitisk prövning. Attribuering är analysprocessens slutresultat oberoende av om resultatet ska publiceras eller inte är offentligt. Attribuering är ofta en förutsättning för att ställa någon till svars

juridiskt eller politiskt, för åtgärder enligt internationella skyldigheter (retorsion) och tillåtna svarsåtgärder. Attribuering, till exempel offentligt tillräknande, kan även vara en retorsionsmetod i sig själv.

Cyberekosystem, ~ekosystem för cybersäkerhet

Ett nätverk med ömsesidigt beroende, enligt utvecklingsprogrammet för cybersäkerheten 2021, som byggs och upprätthålls mellan företag, offentlig förvaltning samt aktörer inom forskning och tredje sektorn, vars mål är att ta fram innovationer, livskraft, tillväxt, arbetsplatser, kompetens och förbättra det digitala samhällets hållbarhet samt toleransen mot skadliga fenomen i cybermiljön.