STATSRÅDETS KANSLIS PUBLIKATIONER 2024:12

Strategi för cybersäkerheten i Finland 2024–2035

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

Statsrådets kanslis publikationer 2024:12

Strategi för cybersäkerheten i Finland 2024–2035

Statsrådets kansli Helsingfors 2024

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Statsrådets kansli

ISBN pdf: 978-952-383-411-8
ISSN pdf: 2490-1164

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2024

Presentationsblad

10.10.2024

Strategi för cybersäkerheten i Finland 2024–2035

Statsrådets kanslis publikationer 2024:12

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

Referat

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

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

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

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

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

ISBN PDF	978-952-383-411-8	**ISSN PDF**	2490-1164
Ärendenummer	VN/36693/2023	**Projektnummer**	VNK007:00/2024
URN-adress	https://urn.fi/URN:ISBN:978-952-383-411-8		

Kuvailulehti
10.10.2024

Suomen kyberturvallisuusstrategia 2024–2035

Valtioneuvoston kanslian julkaisuja 2024:12

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

Tiivistelmä

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

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

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

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

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

ISBN PDF	978-952-383-411-8	**ISSN PDF**	2490-1164
Asianumero	VN/36693/2023	**Hankenumero**	VNK007:00/2024

Julkaisun osoite https://urn.fi/URN:ISBN:978-952-383-411-8

Description sheet
10 October 2024

Finland's Cyber Security Strategy 2024–2035

Publications of the Prime Minister's Office 2024:12
Publisher Prime Minister's Office

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

Abstract

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

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

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

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

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

ISBN PDF 978-952-383-411-8 **ISSN PDF** 2490-1164
Reference number VN/36693/2023 **Project number** VNK007:00/2024

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

Innehåll

FÖRORD

Den reviderade strategin för cybersäkerheten är avsedd att bemöta det förändrade geopolitiska läget och den tekniska utvecklingen. Den utgör fortsättningen på en över 20-årig tradition av att sörja för det finländska samhällets informations- och cybersäkerhet. Cybersäkerhetsläget i Finland är bra, men det krävs kontinuerlig förbättring för att hålla jämna steg med den kontinuerliga förändringen.

Cybersäkerheten är en vital del av den finländska modellen med övergripande säkerhet. Vårt samhälle är nästan helt digitaliserat och som en del av förtroendesamhället vill vi även i fortsättningen se till att finländarna kan lita på cybersäkerheten när det gäller de digitala tjänsterna. Cybersäkerheten kräver att ledningen hos alla aktörer i samhället tar ansvar för den och satsar på den. EU:s cybersäkerhetsdirektiv förutsätter också ett starkare deltagande än tidigare av de olika sektorerna i samhället, så att alla digitala tjänster är pålitliga.

Europeiska unionen är Finlands viktigaste politiska och ekonomiska referensram samt värdegemenskap inom cybersäkerheten. Merparten av den nuvarande cybersäkerhetsregleringen och övriga politiska åtgärder härstammar från Europeiska unionen. Finland är påverkar aktivt dessa. Vårt Natomedlemskap stärker Finlands cybersäkerhet och -försvar, men medför även nya skyldigheter. Vi vill vara en stark cybersäkerhetspartner i Europeiska unionen och Nato. Den kommande cyberförsvarsdoktrinen introducerar nationella verksamhetsprinciper för bekämpning av statliga hot och hot som äventyrar statens säkerhet. Nationellt bereder vi oss för ett aktivt cyberförsvar samt för möjligheten till attribution och motåtgärder.

Strategin är modig och ambitiös – och det ska den vara. Kärnan i den finländska verksamhetsmodellen för cybersäkerhet utgörs av samarbete mellan olika aktörer. Genomförandet av strategin kräver granskning av myndigheternas befogenheter och förutsättningar för informationsutbyte. Vi måste hålla fast vid myndigheternas och den privata sektorns förtroendefulla samarbete. Genom samarbete och tillräckliga myndighetsresurser kan vi bekämpa cyberbrottsligheten som ständigt ökar och blir mångformigare.

De omvälvande teknikerna är en global utmaning. Vi har den kompetens som behövs för att bli ett ledande samhälle inom kvantsäkerhet. Nu är det dags att agera. Detta kräver ett allt starkare finländskt ekosystem för cybersäkerhet och samarbete mellan förvaltningen och företagslivet.

Strategin sträcker sig tio år framåt, vilket underlättar kommande satsningar för att genomföra strategin. Europeiska unionens och Natos olika finansieringsprogram utgör ett viktigt instrument för utveckling av nationella kompetenser, innovation av nya typer av exportprodukter samt stödjande av den nationella beredskapen.

Att delaktiggöra och höra olika aktörer har ingått i kärnan i vår strategi. Hundratals sakkunniga samt aktörer inom den offentliga och privata sektorn, vetenskapssamfundet och det civila samhällets organisationer har deltagit i beredningen av strategin. Detta återspeglar utmärkt det finländska samhällets engagemang och den finländska modellen med övergripande säkerhet.

Statsminister Petteri Orpo

Oktober 2024

1 Inledning – cybersäkerheten 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 den tilltagande digitaliseringen, utvecklingen av nya tekniker och den globala konkurrensen i fråga om dessa, det ständigt ökande ömsesidiga beroendet och övriga megatrender som påverkar framtiden, såsom klimatförändringen och förändringen i befolkningsstrukturen. Samhällets grundstrukturer och -tjänster, såsom informations- och kommunikationsnäten och infrastrukturen i fråga om dessa, måste fungera i alla förhållanden.

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 särskilt den nationella cybersäkerheten, 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. 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), 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.

Målsättningen för strategin för cybersäkerheten i Finland sträcker sig till år 2035. Behovet av att revidera strategin bedöms vart femte år, och vid behov utvecklas eller uppdateras strategin också oftare.

I nuläget använder Finland nästan 300 miljoner euro årligen på att säkerställa cybersäkerheten inom statsförvaltningen och näringslivet minst tiofalt i jämförelse med detta. Trots detta är basnivån för finansieringen i dagens läge inte tillräcklig för att motsvara den förändrade verksamhetsmiljön.

Utvecklingsförslagen som härletts ur strategins målsättning genomförs i enlighet med en separat genomförandeplan.

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

2 Målsättning och struktur

De strategiska målen omfattar fyra delområden, dvs. pelare: **I Kompetens, teknologi och forsknings-, utvecklings- och innovationsverksamhet (FUI); II Beredskap; III Samarbete samt IV Reaktion och motåtgärder.**

Bild 1. Cybersäkerhetsstrategins målsättning och strategins struktur

3 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.

3.1 Många slags hot utgör en utmaning

Den förändrade verksamhetsmiljön utmanar den internationella regelbaserade ordningen. 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. Statligt cyberspionage hotar inte enbart beredningen av utrikes- och säkerhetspolitiken. Finländska företags intellektuella kapital kan också utsättas för olaglig informationsanskaffning, vilket utgör ett hot mot en bibehållen konkurrenskraftig ekonomi.

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

3.2 Den fientliga cyberverksamheten mot Finland ökar sannolikt

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 större risk för avslöjande.

Utöver tekniska störningar kan effekterna av fientlig verksamhet nå Finland från andra länder och sprida sig oförutsett, även om Finland inte är det huvudsakliga målet. När den fientliga cyberverksamheten ökar och alltmer omfattande även riktar sig mot regeringar, demokratiska institutioner, företagslivet och individer ökar 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.

3.3 Den tekniska omvälvningen ökar allas ansvar för cybersäkerheten

Den tekniska omvälvningen och samhällenas digitalisering ökar mängden informationssystem och tjänster som syns offentligt på internet, och ökar därmed samhällets sårbarhet och utsatthet för cyberstörningar. Antalet anslutna enheter 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 i tekniken. De ger kriminella och statliga aktörer tillgång till informationssystemen. Den snabba utvecklingen av omvälvande tekniker, såsom artificiell intelligens, kvantberäkning, molntjänster, 6G-teknologi och satellitteknologi, medför utmaningar för cybersäkerheten. Genom reglering kan utvecklingen av säker teknologi främjas. Samtidigt som säkerhetsåtgärder vidtas utvecklar dock även inkräktarna nya sätt att kringgå dem.

3.4 Internationellt samarbete stärker Finlands cybersäkerhet

Natomedlemskapet stärker Finlands säkerhet och försvar, men medför samtidigt nya utmaningar och skyldigheter. Natomedlemskapets avskräckande effekt kan leda till att den fientliga verksamhetens tyngdpunkt alltmer övergår från traditionella hot till cyberdomänen, där utövaren lättare kan bestrida sin delaktighet. Den tekniska utvecklingen, datadrivenheten, det internationella samarbetet samt analyseringen av geopolitiska förbindelser inom cyberverksamheten skapar ändå allt bättre möjligheter i synnerhet för att attribuera, dvs. tillskriva, statliga aktörer.

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. Kompetens- och utbildningsbehoven och kostnaderna för att bygga upp ett tillräckligt skydd ökar 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 och störningssituationer samt reaktioner och motåtgärder.

Parallellt med EU- och Natomedlemskapet har även det övriga bilaterala och multilaterala internationella samarbetet inom cybersäkerhet och -försvar utvidgats och fördjupats. På initiativ av och i samarbete med likasinnade länder strävar man efter att svara på centrala cyberhotbilder och förbättra den kollektiva cybersäkerheten. Inom FN och olika regionala organisationer identifieras cybersäkerhetens betydelse för den internationella säkerheten.

3.5 Den nationella samarbetsmodellen utvecklas

Den nationella samarbetsmodellen inom cybersäkerhet har baserat sig på förmågan att fortlöpande förbättra informationssystemen 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 reagerandet samt av samordnade motåtgärder 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.

3.6 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 grundläggande rättigheter, försämra tilltron till tjänster och orsaka betydande ekonomiska förluster. Cyberbrottslighet är alltmer kopplad till den organiserade brottsligheten och statliga

aktörer. Vid fientlig verksamhet utnyttjar staterna ofta olika ersättande ombud, såsom kriminella grupper, som köptjänster. Genom att köpa tjänster av kriminella kan de fientliga staterna försöka försvåra tillskrivande eller till exempel variera intensiteten i sina cyberoperationer.

Det är värt att beakta att en stor del av infrastrukturen som är kritisk med avseende på samhällets funktioner ägs av den privata sektorn. Samarbetet mellan myndigheterna och den 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. Genom samarbete och tillräckliga myndighetsresurser kan vi även bekämpa cyberbrottsligheten som ständigt ökar och blir mångformigare.

3.7 Säkerheten i leveranskedjorna framhävs

De globala 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 deras serviceproducenter och leveranskedjor är cybersäkra.

3.8 Cybersäkerhet möjliggör affärsverksamhetens tillväxt

Samhällets digitalisering skapar betydande affärsverksamhetsmöjligheter som stöder tillväxten, genom allt från förenklade processer till utveckling av nya inlärningsmetoder eller andra möjligheter som forsknings- och utvecklingsarbetet öppnar upp. Omvälvande tekniker, såsom artificiell intelligens och kvantberäkning möjliggör utveckling av nya lösningar för framtidens utmaningar i cybermiljön. Omvälvande tekniker 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 har det uppstått ett behov av nya och effektiva innovationer som stärker cybersäkerheten.

4 Nuläge

Digitaliseringen av det finländska samhället har kommit långt. 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 i täten i internationella jämförelser som gäller digitalisering.

I Finland förbättras ständigt 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 ur global synvinkel kan ses som ett internationellt visitkort och en potentiell exportprodukt.

4.1 Cybersäkerheten och samhällets digitaliseringsutveckling

Finlands digitala kompass är en nationell strategisk färdplan för Finlands digitaliseringsutveckling som sträcker sig till 2030. Enligt den digitala kompassen strävar Finland efter att avsevärt minska 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.

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. De nya bedrägerisätten som möjliggörs av AI-teknik och omfattande språkmodeller utgör redan nu ett hot såväl för cybermiljön som informationsmiljön. Det finns ett hot om nya allvarliga och mer omfattande effekter.

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. Dataintrång i personuppgifter kan leda till betydande konsekvenser för människors välbefinnande och tillit till samhällets funktionsduglighet. Detta framhäver ytterligare vikten av att tillräckliga resurser allokeras för cybersäkerheten samt vikten av samarbete och gemensamma förfaringssätt.

4.2 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 sinsemellan och med den offentliga sektorn.

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

4.3 Cybersäkerheten ska beaktas i välfärdsområdena och kommunerna

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 områdenas kritiska infrastruktur och offentliga tjänster. Välfärdsområdena svarar för sina tjänster och cybersäkerheten i anslutning till dem. Inom kommunfältet är nivån på cybersäkerheten i genomsnitt sämre än inom stats- och regionalförvaltningen, men det finns skillnader i de kommunala aktörernas storlek och resurser. Både välfärdsområdena och kommunerna behöver mer stöd än hittills för att säkerställa cybersäkerheten, till exempel centraliserade cybersäkerhetstjänster. Bekämpningen av cyberhot måste fungera smidigt mellan olika stora aktörer och i rätt tid på alla nivåer av den offentliga förvaltningen.

4.4 Förtroende byggs upp genom samarbete

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 bekämpar cyberhot i sina egna organisationer. Myndighetsverksamheten ska vara pålitlig och tjänsterna ska säkerställas 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. Till exempel medför förändringen i befolkningsstrukturen utmaningar för samhället. Det måste säkerställas att digitaliseringen är human och tillkommer var och en.

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.

4.5 Den snabba utvecklingen av kvantteknologin utmanar den nationella krypteringsförmågan

I krypteringsteknikernas nationella förmågor förenas säkerställande av verksamhetsförutsättningarna för den nationella säkerheten och försvaret, säkerställande av försörjningsberedskapen och kunskapskapitalet samt 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 medför 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 krypteringstekniskt laboratorium kan i värsta fall hindra utvecklingen och utnyttjandet av kvantteknologin.

4.6 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 forskningsinstituts kunskapskapital samt innovationer. Dessutom kan fientliga statliga aktörer koordinera sina åtgärder sinsemellan för att effektivisera sina mål. Det centrala syftet med offensiva 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 utnyttjandet av myndigheters och cybersäkerhetsföretags färdigheter och deras täta samarbete i tryggandet av cybersäkerheten och den kritiska infrastrukturens funktionsduglighet gentemot statliga hot.

I en situation som äventyrar cybersäkerheten leder de behöriga myndigheterna hanteringen av störningssituationen inom ramen för vars och ens uppgifter och behörighet. Trots att samarbetet redan nu är välfungerande har myndigheterna ändå i nuläget bedömts ha otillräckliga verksamhetsförutsättningar för att effektivt förbereda sig för och bekämpa allvarligare cyberhot som äventyrar den nationella cybersäkerheten och landets försvar. Utmaningar för samarbetet kring cybersäkerheten utgörs av en splittrad reglering och ansvar som delas av flera aktörer samt de olika verksamhetsmodellerna för samarbetet och bristen på lämpliga gemensamma informationssystem. Offentliga tjänsters cybersäkerhetsinformation delas i nuläget inte heller i tillräcklig grad mellan alla aktörer inom den offentliga förvaltningen och näringslivet med avseende på strategi-, norm-, resurs- och informationsstyrning.

En händelse som äventyrar cyberdomänens säkerhet kan samtidigt vara ett informationssäkerhetshot, ett brott och ett hot som äventyrar den nationella säkerheten och försvaret och ha utrikes- och säkerhetspolitiska konsekvenser. Av denna anledning 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 egna lägesbilder även för statsledningens

behov. Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter svarar tillsammans med olika 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.

5 Pelarna och deras strategiska mål

MÅLSÄTTNINGEN FÖR DEN NATIONELLA CYBERSÄKERHETEN

Cybersäkerheten är 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 vår kompetens 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 målsättningen, och de används effektivt.

5.1 Pelare I: Kompetens, teknologi och FUI

Ett kunnigt, innovativt och experimentellt cyberekosystem.

DELOMRÅDETS STRATEGISKA MÅL:

- Cybersäkerhetskunnandet är starkt på alla nivåer inom fostran och utbildning samt samhället och arbetslivet.
- Var och en känner till sitt cybersäkerhetsansvar.
- Finland tar i bruk fördelarna med omvälvande tekniker och kräver inbyggd säkerhet i apparater, program 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.

Ekosystemet för cybersäkerhet utvecklas

Ekosystemet för cybersäkerhet är en helhet som i stor utsträckning omfattar aktörer inom den 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 uthållighet och självförsörjning samt toleransen mot olika fenomen i cybermiljön. Ett fungerande och experimentellt cyberekosystem ökar produktiviteten och effektiviteten samt förbättrar kvaliteten på tjänsterna. För att möjliggöra en hållbar ekonomisk tillväxt söker man en balans mellan hot och möjligheter i samarbete med aktörerna inom ekosystemet för cybersäkerhet.

Det är viktigt med en stark inhemsk forsknings-, utvecklings- och innovationsverksamhet (FUI) och framgångsrik företagsverksamhet inom cybersäkerhetsbranschen för att utveckla och upprätthålla ett fungerande ekosystem för cybersäkerheten. Detta behövs även för att stärka den samhälleliga driftsäkerheten och konkurrenskraften.

Kompetensen är stark på alla nivåer

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. I skolorna ska lärarnas färdigheter att fostra eleverna till en kritisk medieläskunnighet samt en medvetenhet om cyberrisker stärkas för att göra samhällets resiliens, dvs. kristålighet, starkare. För att uppnå målen måste cybersäkerheten beaktas som en del av det digitala kunnandet när läroplanerna utarbetas och lärarnas cybersäkerhetskompetens ska främjas. Det civila samhällets organisationer har en betydande roll i att utveckla individers kunnande efter skolgången. Vid sidan om examensutbildning med inriktning på utbildning för cyberexperter utvecklas möjligheterna till kompetensutveckling genom att stärka utbudet inom kontinuerligt lärande. Det hör till organisationernas ansvarsfulla verksamhet att utveckla personalens kompetens, identifiera hot, reagera på skadlig verksamhet och anmäla störningar i cybermiljön.

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

Alla enskilda människor, företag och organisationer 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.

Var och en känner till sitt cybersäkerhetsansvar

Cybersäkerhetskompetens hör till medborgarfärdigheterna och var och en kan genom sina handlingar medverka till uppkomsten av en allt säkrare cybermiljö. En cybersäker vardag kan stödjas bland annat genom att stärka 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 samhällsansvar. Människor som agerar ansvarsfullt i cybermiljön ökar på ett betydande sätt även sammanslutningarnas och organisationernas säkerhet.

Samhället måste förbereda sig på utvecklingen av omvälvande tekniker

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. Denna princip om inbyggd säkerhet ska beaktas i all nationell lagberedning som gäller teknologi samt i föregripande EU-inflytande.

EU:s nya cyberlagstiftning är förknippad med standardiserings- och certifieringsarbete. Det ligger i Finlands intresse att vara en aktiv aktör i utvecklingen och användningen av standarder och certifieringssystem inom cybersäkerheten. Samtidigt är det viktigt att utnyttja de affärsverksamhetsmöjligheter som ämnesområdet erbjuder.

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 mångsidig teknisk kompetens och en fortlöpande uppföljning och utvärdering av de samhälleliga förändringarna. Det finns skäl att redan nu förbereda sig för till exempel effekterna av kvantteknologins utveckling.

Konkurrenskraften främjas för företagen inom cybersäkerhetsbranschen

I planeringen av FUI-satsningarna 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, EU:s ramprogram Horisont Europa och Digitalt Europa (DEP) eller de europeiska försvarsfondernas program ökar Finlands ryktbarhet som ett land med kompetens inom högteknologi och cybersäkerhet och förbättrar finländska företags affärsverksamhetsmöjligheter nationellt och internationellt. Det är viktigt att Finland aktivt påverkar innehållet i dessa program redan i planeringsskedet. 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 stärker cybersäkerheten samt den internationella konkurrenskraften för de företag som kommersialiserar dem. Samtidigt främjas både den finländska cybersäkerhetsbranschens och även den säkra FUI- och affärsverksamhetsmiljöns attraktionskraft för finländska och utländska experter, företag och investeringar.

Cybersäkerhetens kunskapskapital är skyddat

Den offentliga och privata sektorns kritiska kunskapskapital ska identifieras och skyddas. Kunskapskapitalet i fråga om cybersäkerhet 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 konfidentialiteten, integriteten och tillgängligheten i alla situationer för de nationellt betydande informationsresurserna. Kvantteknologins utveckling hotar att knäcka moderna krypteringsalgoritmer och äventyra nationellt skyddat 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, dekompilering och organisering. I det nationella utvecklingsarbetet med kvantsäker kryptering beaktas även EU:s gemensamma politiska åtgärder och reglering samt de krav som Nato ställer.

5.2 Pelare II: Beredskap

Stark cyberresiliens och driftsäkerhet i samhället

DELOMRÅDETS STRATEGISKA MÅL:

- De vitala samhällsfunktionerna, den kritiska infrastrukturen, de offentliga tjänsterna och de kritiska aktörerna med avseende på försörjningsberedskapen är cybertåliga.
- Individerna, företagen, organisationerna och myndigheterna har tillsammans förberett sig för cyberstörningar och -hot.
- 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. Vi ska kunna 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 till samhällets tjänster och förmågan att klara av störningar i alla förhållanden. Det är viktigt att säkerställa att de vitala samhällsfunktionerna fungerar och är störningståliga. De vitala funktionerna omfattar bland annat infrastruktur som är kritisk med avseende på cybermiljön, informationsresurser, offentliga tjänster och försörjningsberedskap. 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 cyberdomänen.

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 cyberövningsverksamheten och göra den 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 anskaffning, utveckling och upprätthållande av dem 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 kan lita 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 av cybersäkerheten följs upp och tyngdpunkter prioriteras. Av offentliga tjänsters tekniker och serviceproduktion ska det krävas kravenlighet i fråga om cybersäkerheten, informationssäkerheten och dataskyddet under hela livscykeln. Bedömningen och godkännandet av offentliga tjänsters kravenlighet samt bedömningskriterierna ska utvecklas och förtydligas och förpliktas till behövliga delar. Dessutom är det viktigt att utveckla den automatiska uppföljningen och tillsynen av den tekniska miljön och förplikta till detta. Det bör säkerställas att tjänsternas funktionalitet prioriteras i enlighet med situationen, att det finns beredskap för potentiella störningssituationer och att effekterna av störningarna på myndigheternas och samhällets verksamhet kan minimeras.

Beredskapsarbetet sker i samarbete

Beredskapsarbetet som gäller cybersäkerheten utförs i tätt samarbete i enlighet med modellen för övergripande säkerhet. Identifieringen av cyberhot och beredskapen inför dessa ska basera sig på systematisk kunskapsledning och en gemensam lägesuppfattning som baserar sig på prognostisering, observation, 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 en förutsättning för framgångsrikt nationellt cybersäkerhetsarbete, beredskap, en gemensam lägesuppfattning och reagerande 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 attackytan för cyberbrottslingar minskar.

Användarna ska kunna lita på säkerheten i tjänsterna och de ska ha tillräckligt kunnande för att identifiera förfalskade tjänster och bedrägeri. Utvecklingen av artificiell intelligens gör cyberbrottsligheten mer målinriktad och verkningsfull än tidigare. I fortsättningen är det därför allt viktigare att identifiera konsekvenserna på cybersäkerheten av såväl artificiell intelligens som andra omvälvande tekniker samt utveckla metoder att bekämpa dem.

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 individer 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, region- och lokalförvaltningen, välfärdsområdena och företag.

Beredskap baserar sig på långsiktig resursering

På basis 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, regionförvaltningen, välfärdsområdena och kommunerna samt företag och organisationer.

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 en centralisering av cybersäkerhetsuppgifterna främjas i lämplig utsträckning i regionförvaltningen, välfärdsområdena och kommunerna i syfte att effektivisera resursanvändningen.

Den centraliserade projektfinansieringen som ingår i planen för de offentliga finanserna kan allokeras för införande av nya cybersäkerhetsfunktioner, -uppgifter eller -tjänster. Myndigheternas möjligheter att erbjuda cybersäkerhetstjänster åt kunder 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 de offentliga finanserna. De verksamhetsmodeller som behövs för inhämtandet och upprätthållandet av den ska genomföras.

Övningsverksamheten utvecklas

Genom cyberövningsverksamheten bygger man en stark cyberresiliens för hela samhället. Miljöerna och verksamhetsmodellerna för cyberövningarna ska kontinuerligt utvecklas för att motsvara förändringen i verksamhetsmiljön. Organisationer uppmuntras att långsiktigt utveckla sin övningsverksamhet, vid behov med stöd av myndigheterna.

Nationellt identifieras särskilt betydelsen av övningar mellan olika sektorer samt vikten av att öka antalet övningar. Genom nationella cyberövningar simuleras olika cyberstörningssituationer, dvs. man skapar förhållanden där man kan identifiera effekterna av cyberstörningar samt testa och öva återhämtning från dem. Övningarna utvecklar kunnandet samt individers och organisationers beredskap och förmåga att förbereda sig för olika cyberstörningar och hot. Aktiva och regelbundna övningar i normalförhållanden stärker kunnandet i alla situationer.

Internationella cyberövningar stöder beredskapen inför, beslutsfattandet om och bekämpningen av gränsöverskridande cyberhot och störningar. För Finland är det viktigt att delta i internationella cyberövningar, agera aktivt under dessa samt utveckla och erbjuda kunnande om cyberövningar åt internationella partnerländer.

Genom rymdtjänsterna förbättras resiliensen för markbundna system

Med avseende på samhällets funktionsduglighet är det viktigt att rymdtjänster, såsom tid- och platsinformation, datatrafik och distanskartläggning är tillgängliga. Rymdsystemens cybersäkerhet övervakas som en del av rymdlägesbilden. Rymdsystemens cybersäkerhet ska även beaktas i villkoren för rymdtillstånd och i hanteringen av systemens livscykel. Man kan förbereda sig för potentiella störningssituationer och återhämtning från dem, och minimera effekterna av störningarna på myndigheternas och samhällets verksamhet med hjälp av alternativa verksamhetsmodeller och reservarrangemang.

5.3 Pelare III: Samarbete

En stabil nationell och internationell samarbetsmodell

DELOMRÅDETS STRATEGISKA MÅL:

- Finland påverkar och deltar aktivt i det normativa internationella samarbetet rörande cyberdomänen, 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.
- Den offentliga sektorn utvecklar och tillhandahåller centraliserade cybersäkerhetstjänster tillsammans med den privata sektorn.

Finland påverkar och deltar aktivt i samarbete

Den utrikes- och säkerhetspolitiska redogörelsen, försvarsredogörelsen, redogörelsen för den inre säkerheten och cybersäkerhetsstrategin fastställer långsiktiga nationella mål för bekämpning av cyberhot. I dessa beaktas EU:s och Natos mål och skyldigheter i fråga om cybersäkerhet och cyberförsvar. Målen preciseras 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 fortsätter det aktiva deltagandet i det normativa internationella samarbetet som gäller cyberdomänen och i utbytet av åsikter om hur den internationella rätten i vissa frågor reglerar användningen av staters informations- och kommunikationstekniker. Finland uppdaterar sin ställning i fråga om tillämpningen av internationell lag i cyberdomänen. Finland påverkar beslutsfattandet rörande cybersäkerhet, cyberbrottslighet och cyberförsvar såväl inom FN, EU, Nato som 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 utifrån gemensamma värden i synnerhet med viktiga likasinnade EU-länder, de nordiska länderna samt euroatlantiska länder och även vissa länder i den 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 bedömningen av konsekvenserna och genomförandet av den nya regleringen, samt tillräckliga resurser för myndigheterna.

Finland som medlem i EU och Nato

Europeiska unionen är Finlands viktigaste politiska och ekonomiska referensram och värdegemenskap. Finland deltar i och påverkar aktivt EU:s cybersäkerhetsarbete, inklusive EU:s cybersäkerhetsbyrå ENISA:s och Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ECCC:s verksamhet.

Genom påverkan inom EU främjar Finland projekt och beslut som är viktiga med avseende på den övergripande säkerheten och utvecklar beredskapen i unionen och dess medlemsländer. Detta gäller även inom cybersäkerhetens delområde.

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 i 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 och därmed stärka störnings-toleransen i cybermiljön. Ett viktigt mål är att uppnå EU:s strategiska autonomi och bibehålla en öppen ekonomi.

Finland är en konstruktiv, pålitlig och prestationsduglig Natoallierad. Finland upprätthåller en stark nationell försvarsförmåga som en del av Natos gemensamma avskräckning och försvar, och deltar aktivt i utvecklingen av Natos cyberförsvar. Som medlem i Nato vill Finland vara i kärnan av utvecklingen av cyberprestanda. Målet är att vara en betydande producent av lösningar inom cybersäkerhet och cyberförsvar 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.

Det är viktigt att samordna de nationella EU- och Natoståndpunkterna vad gäller cybersäkerhet och -försvar. Den ömsesidiga förenligheten mellan EU:s och Natos cyberåtgärder kompletterar och stärker både den internationella cybersäkerheten och Finlands nationella cybersäkerhet.

En gemensam lägesuppfattning baserad på informationsutbyte som grund för verksamheten

Ett aktivt samarbete, upprättande av en lägesbild och -uppfattning samt säkerställande av förutsättningarna för informationsanskaffning är viktiga för att uppnå målsättningen. En gemensam lägesuppfattning baserad på informationsutbyte

möjliggör ett effektivt och tillförlitligt samarbete i cyberdomänen mellan myndigheterna, företagen och organisationerna. Detta ökar förtroendet och stöder fullföljandet av sektorsansvaren.

När det gäller observationsverksamheten i cyberdomänen behöver informationsinsamlingen systematiseras så att det är möjligt att utifrån informationen skapa 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.

Informationsutbytet ska vara tillräckligt, stabilt, ändamålsbundet och upprätthålla förtroendet 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 information ska kunna identifiera och dela informationen på eget initiativ i enlighet med lägesuppfattningen. Med hänsyn till begränsningarna i fråga om distribution måste lägesinformation om allvarliga cyberhot kunna delas effektivare än tidigare med företag som är kritiska för försörjningsberedskapen, kommuner, kommunalt ägda tjänsteleverantörer och välfärdsområdena. 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.

Delning av information med en hög säkerhetsklassificering förutsätter utveckling och införande av system som lämpar sig för detta. När informationsutbytet mellan myndigheterna utvecklas ska hänsyn tas till den utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet som gjordes 2022.

Myndigheternas samarbete är smidigt och obehindrat

Genomförandet av det operativa samarbetet, ansvaret samt beredskapen inför allvarliga cyberhot och -störningar och bekämpning av dessa samordnas i en samarbetsstruktur på ämbetsverksnivå med större intensitet och delaktighet än nu, som består av Transport- och kommunikationsverket Traficom, centralkriminalpolisen, Försvarsmakten och skyddspolisen. Samordningen baserar sig på en gemensam delad lägesuppfattning. Samarbetsstrukturen och de myndigheter som ingår i denna ska ha tillräckliga rättigheter att lämna ut och få information. Samarbetsstrukturen leder till ett behov av att även intensifiera myndigheternas samarbete på en taktisk och teknisk nivå.

Verksamhetskulturen i fråga om cybersäkerhet ska förnyas enligt modellen för övergripande säkerhet genom att stärka det nationella och internationella cybersäkerhetssamarbetet mellan statsförvaltningen, regionförvaltningen, välfärdsområdena, kommunerna, 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

Centraliserade cybersäkerhetstjänster tillhandahålls i nuläget av Transport- och kommunikationsverket Traficom, Myndigheten för digitalisering och befolkningsdata, övriga aktörer inom statsförvaltningen samt av företag som ägs av välfärdsområden och kommuner tillsammans med den privata sektorn. Till dessa tjänster hör exempelvis HAVARO-systemet som upptäcker och varnar för allvarliga kränkningar av informationssäkerheten och HYÖKY-tjänsten för kartläggning av angreppsytan, som båda upprätthålls av Traficom, samt de webbutbildningar om informations- och cybersäkerhet som MDB tillhandahåller. De centraliserade tjänsterna används av stats-, region- och lokalförvaltningen, välfärdsområdena och kommunerna samt till lämpliga delar av företag, organisationer, högskolor och forskningsinstitut.

Utvecklingen av centraliserade cybersäkerhetstjänster och samordningen av användningen av dessa främjas. De centraliserade tjänsterna ska vara driftsäkra, kostnadseffektiva, prestationsdugliga och användarvänliga. Målet med samarbetet är att undvika överlappningar och ta fram material och utbildningar samt information och tjänster som är avsedda för gemensamt bruk.

5.4 Pelare IV: Reaktion och motåtgärder

Reagerande på hot i rätt tid och 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.
- Reaktionerna och motåtgärderna 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.

Möjligheterna och förmågan att bekämpa cyberhot säkerställs

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.

Cyberhot måste bekämpas övergripande, långsiktigt och i rätt tid. Detta förutsätter att åtgärder som stärker cybersäkerheten och förebygger cyberhot utnyttjas i stor utsträckning och målmedvetet. 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. Finland måste trygga sin statliga suveränitet även i cyberdomänen.

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.

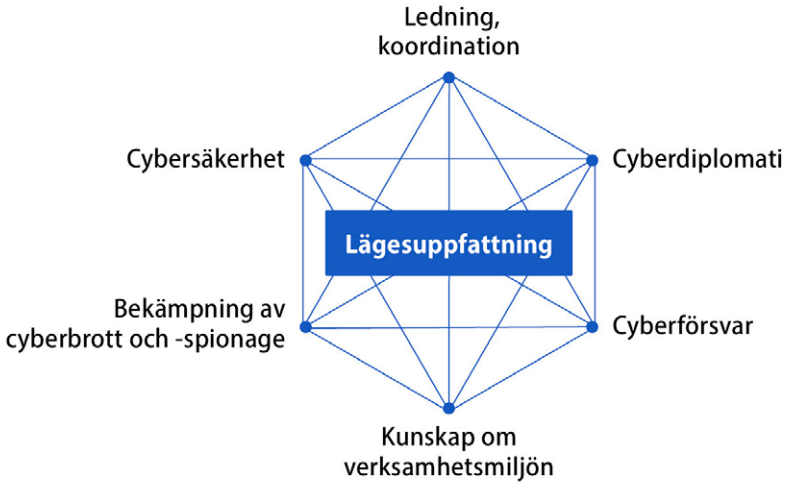
De myndigheter som svarar för den operativa verksamheten ska förebygga, reagera, utreda och bilda en lägesbild om cyberhot. Cyberhotens karaktär ställer krav på myndigheternas samarbete. Reaktionerna och motåtgärderna i fråga om statliga cyberoperationer är annorlunda än i fråga om vanliga cyberhot. 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 cyberdomänen 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.

Samordningsmodellen för situationer med cyberstörningar och hot utvecklas

För att stödja reagerande och motåtgärder 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. Samordningsmodellen för reaktion och motåtgärder skapas i den samarbetsstruktur på ämbetsverksnivå som beskrivs ovan i pelare III. En gemensam lägesuppfattning säkerställer de samordnade åtgärderna för varje myndighets egen verksamhet. Tyngdpunkten för den nationella cybersäkerheten och informationsanskaffningen, rätten att få information och informationsutbytet som denna medför för myndigheter ligger 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, attribution, dvs. tillskrivande, och motåtgärder.

Den nationella attributionsverksamheten utvecklas

Finland utvecklar de nationella riktlinjerna och processen för en målinriktad och konsekvent cyberattributionsverksamhet med beaktande av centrala allierade och partner. Attribution innebär insamling och analys av fakta, teknisk, juridisk och politisk bedömning, beslutsfattande och slutligen kommunicering av beslutet till olika aktörer. I den övergripande attributionsprocessen måste man kunna utnyttja all information som anknyter till attributionen, 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, inom alliansen och hos partner. 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 en del av utvecklingen och genomförandet av landets försvar som helhet.

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

Målet är att Finland ska bekämpa cyberhot orsakade av tredjeländer genom såväl förebyggande, reaktiva som långsiktiga åtgärder och utnyttja hela det nationella utbudet av metoder och kapacitet på ett ändamålsenligt sätt. Dessa är bland annat metoder inom diplomati, underrättelseinhämtning, informationshantering och strategisk kommunikation, militär förmåga, 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 attribution och mot-åtgärder. Finland deltar även fullt ut i Natos cyberförsvar och utnyttjar EU:s verksamhetsmöjligheter i fråga om resultatsamarbetet, informationsutbyte, samordnade motåtgärder och reglering som stöd för det nationella cyberförsvaret. Cyberförsvaret är en del av Finlands och Natos försvar och avskräckning.

6 Resursering, genomförande och uppföljning

6.1 Resurser

I Finland bekämpar cybersäkerhetsaktörerna hot varje dag. Förändringen i verksamhetsmiljön ökar och diversifierar cyberhoten och -riskerna. Den nuvarande resurseringen för cybersäkerheten har varit otillräcklig i förhållande till behoven till och med för att upprätthålla nuläget. För att säkerställa och stärka cybersäkerheten i den förändrade verksamhetsmiljön samt genomföra den nya lagstiftningen och tillsynsuppgifterna inom de olika sektorerna krävs det nya resurser i framtiden.

I nuläget använder Finland nästan 300 miljoner euro årligen på att säkerställa cybersäkerheten inom statsförvaltningen. Utöver detta använder regionförvaltningen, välfärdsområdena och kommunerna samt lokalförvaltningen resurser för sin egen cybersäkerhet, men uppföljningen av deras användning ska ännu utvecklas. Det bör 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.

De nuvarande utmaningarna för statsfinanserna, den tekniska reparationsskulden och arbetskraftsbristen som beror på kompetensbrist inom cybersäkerhetsbranschen tillsammans med EU:s ökade reglering påverkar möjligheterna att utveckla cybersäkerheten i framtiden. Den offentliga sektorns konkurrenskraft som arbetsgivare håller på att överskuggas av den privata sektorn. Dessa medför utmaningar för genomförandet av strategin för cybersäkerheten i Finland och dess genomförandeplan samt cybersäkerhetsbranschens nationella tillväxt.

Mer resurser måste allokeras för genomförandet av alla strategiska mål och utvecklingsåtgärder. En ändring av Finlands cyberprofil kräver förutom ökade resurser även preciserad planering och uppföljning av dessa 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 uthållighet 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 för beredskapen, reagerandet och motåtgärderna 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 väsentlig 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.

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 eller ryktesskador.

Användningen av resurserna kan effektiviseras genom en smidig resursdelning inom myndigheternas samarbete. En myndighet ska till exempel kunna avtala om att utföra någon cybersäkerhetsuppgift för en annan myndighet om det anses vara ändamålsenligt.

Beslut om resurser och deras allokering och samordning tas i de beslutsprocesser som gäller statsbudgeten, och de bestäms inom ramen för de anslag och antal årsverken som anges i planerna för de offentliga finanserna och statsbudgeterna.

6.2 Genomförande och uppföljning av strategin

Enligt EU:s cybersäkerhetsdirektiv (NIS 2) 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 planeringsprocessen för de offentliga finanserna. Av dessa rapporter gör byrån en sammanställning åt myndigheterna och de politiska beslutsfattarna.

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. Genomförandeplanen godkänns i en styrgrupp bestående av statssekreterare inom projektet för utveckling av verksamhetsmodellen för statsrådets säkerhetsledning. Uppföljningen av strategin rapporteras till statssekreterarnas styrgrupp och till ministerarbetsgruppen för samhällsförnyelse, och framskridandet informeras även till ministerarbetsgruppen för inre säkerhet och rättsvård samt till Säkerhetskommittén.

I arbetet med att definiera resultatindikatorerna för cybersäkerheten utnyttjas till tillämpliga delar bland annat EU:s cybersäkerhetsbyrå Enisas, 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 NIS 2-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, myndighetsverksamheten och den samhälleliga debatten.

7 Strategiska utvecklingsförslag

Utifrån strategin utarbetas en genomförandeplan med en tidsplan och ansvarsfördelning. Genomförandet av planen ska implementera de strategiska målen enligt pelarna. Nedan finns en förteckning över de viktigaste utvecklingsförslagen som identifierats i strategiarbetet, och dessa preciseras samt kompletteras vid behov i genomförandeplanen. Varje utvecklingsåtgärd är i hög grad förknippad med bedömning av bestämmelser och normer, vilket kan leda till att bestämmelser upphävs eller preciseras. Indelningen i pelare nedan är riktgivande, eftersom flera utvecklingsåtgärder fördelas på fler än en pelare.

7.1 PELARE I: Kompetens, teknologi och FUI

- Utveckling av spetskompetenser och arbetslivsfärdigheter inom den offentliga och privata sektorn samt medborgarnas och civilsamhällets cyberfärdigheter och beredskap.
- Förberedelse inför de hot och möjligheter som uppstår av att nya omvälvande tekniker utvecklas, och beaktande av dem i prognostiseringen samt i införandet och utnyttjandet av tekniker.
- Främjande av utvecklingen av ekosystemet för cybersäkerhet och den tekniska suveräniteten genom att stärka FUI- och företagsverksamheten inom den inhemska cybersäkerhetsbranschen. Nationella och internationella samarbets- och finansieringsmöjligheter utnyttjas.
- Beaktande av organisationers möjligheter att kommunicera och instruera medborgarna om cybersäkerheten.

7.2 PELARE II: Beredskap

- Den gemensamma beredskapen fördjupas för aktörer inom cybersäkerhet inom modellen för övergripande säkerhet.
- Cybersäkerhetssynvinklar bedöms i alla lagstiftningsprojekt.
- Den offentliga förvaltningens cybersäkerhetsresurser planeras och följs upp långsiktigt.
- Standarder för cybersäkerhet och informationssäkerhet utnyttjas för att utveckla gemensamma tillvägagångssätt och kristålighet i

cyberdomänen och den internationella standardiseringen påverkas aktivt.
- Utveckling av metoder för bedömning och godkännande i anknytning till organisationers verksamhet och informationssystem samt kraven som gäller dem.
- Övningsverksamheten och -miljöerna utvecklas för att öka beredskapen och kompetensen.

7.3 PELARE III: Samarbete

- Finlands internationella ställning i fråga om cybersäkerhet och cyberförsvar klargörs, deltagandet i internationellt samarbete kring cybersäkerhet utvecklas och för detta etableras en behövlig nationell samordning.
- Säkerhetsmyndigheternas samarbete och gemensamma lägesuppfattning stärks genom att behövliga samarbetsstrukturer och samordningsmodeller skapas, rollerna och ansvarsfördelningen förtydligas samt förutsättningarna för informationsutbyte och tillgång till information säkerställs. I anslutning till detta genomförs de utvecklingsåtgärder som ingår i utredningen om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet som gjordes 2022.
- Förbättring av samarbetet, informationsutbytet och den gemensamma lägesuppfattningen rörande cybersäkerheten mellan den offentliga förvaltningen, den privata sektorn och civilsamhället i enlighet med modellen för övergripande säkerhet.
- Förtroende upprätthålls och stärks genom säkra och driftsäkra offentliga tjänster.

7.4 PELARE IV: Reaktion och motåtgärder

- Utveckling av välfärdsområdenas och kommunernas samt den privata sektorns färdigheter och förmåga till beredskap och reaktioner på cyberstörningar i rätt tid.
- Verksamhetsmiljökunskaperna utvecklas bland annat genom att säkerställa den nationella observationsförmågan samt säkerhets- och underrättelsemyndigheternas möjligheter att skaffa information om cyberdomänen.

- Övergripande bekämpning av cyberbrottslighet främjas.
- Utveckling av cyberförsvaret som en del av landets försvar som helhet, säkerställande av Finlands statliga suveränitet i cyberdomänen och integration i alliansens försvar.

8 Begrepp och definitioner

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.

Attribution, tillskrivande

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. Attribution är analysprocessens slutresultat oberoende av om resultatet ska publiceras eller inte är offentligt. Attribution är ofta en förutsättning för att ställa någon till svars juridiskt eller politiskt, för åtgärder enligt internationella skyldigheter (retorsion) och tillåtna motåtgärder. Attribution, till exempel offentligt tillskrivande, kan även vara en retorsionsmetod i sig själv.

Cyberdomän

Cyberdomänen 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. Cyberdomänen betonar användningen av cybermiljön ur synvinkeln målinriktad verksamhet.

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 uthållighet samt toleransen mot skadliga fenomen i cybermiljön.

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.

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.

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 använder informationsteknologi.

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.

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.

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.

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.

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 mot-åtgärder som behövs för genomförandet i alla beredskapslägen.

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.

Resiliens; ~kristålighet

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

Vital samhällsfunktion

En funktion som är nödvändig för att samhället ska fungera.

Bilagor

Bilaga 1: En nationell samarbetsmodell för cybersäkerhet

I denna bilaga beskrivs nuläget för den nationella samarbetsmodellen för cybersäkerhet och dess aktörer och hur kraven enligt cybersäkerhetsdirektivet (NIS 2) 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 strategisk uppgift. Samarbetsmodellen för cybersäkerhet är skalbar på alla nivåer, den kan med andra ord tillämpas på allt från nationell nivå till regional och lokal nivå, dvs. på välfärdsområdena och kommunerna, med beaktande av internationella partner.

Enligt verksamhetsmodellen för övergripande säkerhet säkerställs de vitala samhällsfunktionerna i alla förhållanden och på alla nivåer genom samarbete mellan myndigheterna, näringslivet, organisationerna och medborgarna. 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 sektorslagstiftningen 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 NIS 2-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, reaktion och motåtgärder genomförs i ett omfattande samarbete, där det även ingår informationsutbyte för att åstadkomma en gemensam lägesuppfattning och samordna de gemensamma åtgärderna.

Bild 3. Olika aktörer i samhället i säkerställandet 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. Republikens president och statsrådets utrikes- och säkerhetspolitiska ministerutskott är ett centralt organ med avseende på utrikes- och säkerhetspolitiskt viktiga frågor.

Strategisk nivå

Statsrådet och dess ministerier svarar för beredningen av den nationella cybersäkerhetslagstiftningen, allmänna riktlinjer, resursallokering, verksamhetsprinciper, strategisk styrning, beredskapsarbetet samt motåtgärder 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 (NIS 2 och andra)

Med tillsynsmyndigheter avses övervakande myndigheter enligt den nationella lagstiftningen som implementerar NIS 2-direktivet. NIS 2-direktivet verkställs i Finland genom cybersäkerhetslagen och lagen om informationshantering inom den offentliga förvaltningen. Tillsynsmyndigheterna övervakar fullföljandet av de lagstadgade uppgifterna inom den privata och offentliga sektorn. I Finland följer man en distribuerad modell, varvid sektorsmyndigheterna 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.

Olycksutredningscentralen är en myndighet som kan utreda en händelse med hjälp av säkerhetsutredning, om en störningssituation som rör cybersäkerheten orsakar förlust av människoliv eller avsevärda ekonomiska eller materiella skador. Syftet med säkerhetsutredningar är att man ska kunna undvika att liknande händelser inträffar, lära sig av det som inträffat samt utveckla en proaktiv säkerhetskultur.

Operativa myndigheter

De operativa myndigheterna inom cybersäkerhet har en viktig nationell roll såväl när det gäller beredskapen inför cyberstörningar som reaktioner och motåtgärder 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. Dessutom har Cybersäkerhetscentret ett omfattande förtroendebaserat operativt samarbete och informationsutbyte med centrala nationella och internationella nätverk. Vid Cybersäkerhetscentret verkar Finlands nationella samordningscentrum (NCC-FI) inom ramen för Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning.

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 förebygga eventuella framtida brott utifrån den information som polisen har. Polisen uppdaterar den nationella lägesbilden av brott i informationsnät. Centralkriminalpolisen är aktivt delaktig 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 attributionsprocessen samt för andra myndigheters lagstadgade uppgifter med anknytning till den nationella säkerheten.

Försvarsmaktens uppgifter kan även anses omfatta cyberdomänen (cyberförsvar och underrättelseinhämtning i cyberdomänen). 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

Central-, region- och lokalförvaltningen, välfärdsområdena, kommunerna 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, bolag som ägs av välfärdsområden och kommuner 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. Med tanke på samhällets funktionsförmåga och kontinuitetshanteringen är det viktigt att säkerställa den kritiska infrastrukturen och

försörjningsberedskapen som en del av de vitala samhällsfunktionerna. 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. Dessutom samarbetar man med regionala aktörer, såsom regionförvaltningsverken, kommunerna och städerna samt många regionala kommittéer.

Försörjningsberedskapsorganisationen upprätthåller och utvecklar Finlands försörjningsberedskap i samarbete med den offentliga sektorn, flera hundra företag, organisationer och aktörer inom tredje sektorn. Målet är att skydda organisationer som är kritiska med avseende på försörjningsberedskapen och därmed hela samhällets verksamhetsförutsättningar i alla förhållanden.

Aktörer som ska övervakas (NIS 2)

Skyldigheterna enligt NIS 2-direktivet i fråga om riskhantering och rapportering av incidenter tillämpas på sådana väsentliga och viktiga aktörer enligt direktivet som verkar inom sektorer som är kritiska med avseende på samhällets funktion och vars storlek i allmänhet ska överstiga vissa tröskelvärden. Dessa aktörer anges här som aktörer som ska övervakas.

I bilagorna I och II till NIS 2-direktivet anges de typer av aktörer som omfattas av direktivets tillämpningsområde. Direktivets tillämpningsområde omfattar följande sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster, offentlig förvaltning och rymden (bilaga I) samt post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning, digitala leverantörer och forskning (bilaga II).

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 cybersäkerhetslagen eller på avtalsbasis.

Forskningsinstitut och högskolor samt en del av det civila samhällets organisationer är också serviceproducenter. De genererar kompetens- och kunskapskapital och innovationer för cybersäkerhet samt stöd för beredskap och återhämtning från kriser.

Organisationer och aktörer inom fjärde sektorn

Finland är känt i världen för sina talrika organisationer inom det civila samhället och människornas starka vilja att delta i civilsamhällets verksamhet. Betydelsen av det civila samhällets organisationer och frivilliga ökar 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 alltmer bestående del av det dagliga livet, 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. Cybersäkerheten är en naturlig del av varje individs samhällsansvar, som kräver kontinuerlig utveckling och upprätthållande av know-how. Stödet till närstående och anmälan i rätt tid om egna observationer främjar upprätthållandet och utvecklingen av den nationella cyberresiliensen, samt utredningen av cyberbrott.

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

SNELLMANSGATAN 1, HELSINGFORS
PB 23, 00023 STATSRÅDET
tfn 0295 16001
info.vnk@gov.fi
vnk.fi/sv

ISBN pdf: 978-952-383-411-8
ISSN pdf: 2490-1164