Strategi för cybersäkerheten i Finland

Statsrådets principbeslut 24.1.2013

INNEHÅLL

Säkerhetskommitténs sekretariat
Södra Magasinsgatan 8
PB 31, 00131 HELSINGFORS

www.yhteiskunnanturvallisuus.fi/sve

Layout: Tiina Takala/försvarsministeriet
Svensk översättning: Ursula Vuorenlinna/försvarsministeriet
Tryckeri: Forssa print, 2013

ISBN: 978-951-25-2435-8 häft
ISBN: 978-951-25-2436-5 pdf

1. INLEDNING

Med cybersäkerhet avses ett måltillstånd där man kan lita på cyberomgivningen och där dess funktion tryggas.

En av statsmaktens centrala uppgifter är att sörja för säkerheten i samhället, och de vitala funktionerna i samhället måste kunna garanteras i alla situationer. I egenskap av ett informationssamhälle är Finland beroende av att datanäten och datasystemen fungerar och således också mycket sårbart för störningar som riktas mot dem. För denna mångsidiga omgivning, som är avsedd för hantering av information i elektronisk form och som har ett ömsesidigt beroendeförhållande, har man internationellt börjat använda termen cyberomgivning.

Den tilltagande informationsintensiteten i samhället, det ökande utländska ägandet och utläggandet av funktioner på entreprenad, informations- och kommunikationssystemens ömsesidiga integration, användningen av datanät som är öppna för alla samt det ökande beroendet av el har ställt krav av nya slag när det gäller att trygga samhällets vitala funktioner i normala förhållanden, i allvarliga störningssituationer under normala förhållanden och i undantagsförhållanden.

De hot som riktar sig mot cyberomgivningen har förändrats så att konsekvenserna av dem har blivit farligare för enskilda människor, företag och hela samhället. De aktörer som åstadkommer dessa hot är mera professionella än tidigare och numera kan till dem också räknas statliga aktörer. Attacker som genomförs i cyberomgivningen kan användas som verktyg för politisk och ekonomisk påtryckning och i en allvarlig kris som en påverkningsmetod utöver mera traditionella militära maktmedel.

Cyberomgivningen bör också ses som en möjlighet och en resurs. En säker cyberomgivning gör det lättare för individerna och företagen att planera sin verksamhet, vilket ökar den ekonomiska aktiviteten. En bra omgivning gör också Finland mera attraktivt som investeringsobjekt internationellt. Utöver dessa är cybersäkerheten i sig ett nytt och allt starkare affärsverksamhetsområde. Den nationella cybersäkerheten och de finska företagens framgång hänger ihop.

I denna strategi fastslås centrala mål och verksamhetslinjer med hjälp av vilka de utmaningar som riktar sig mot cyberomgivningen kan bemötas och dess funktion säkerställas. Med hjälp av riktlinjerna i cybersäkerhetsstrategin och de åtgärder som behövs för att realisera dessa riktlinjer kan Finland nationellt hantera avsiktliga eller oavsiktliga skadliga verkningar för cyberomgivningen samt besvara dem och återhämta sig från dem.

Arrangemangen i fråga om den övergripande säkerheten har beskrivits i det av statsrådet den 5 december 2012 utfärdade principbeslutet om den övergripande säkerheten. Principerna för tryggandet av samhällets vitala funktioner beskrivs i Säkerhetsstrategi för samhället (2010). Vitala funktioner är ledningen av staten, internationell verksamhet, Finlands försvarsförmåga, den inre säkerheten, ekonomins och infrastrukturens funktion, befolkningen utkomstskydd och handlingsförmåga samt mental kristålighet. Processen med cybersäkerhetsstrategin är en del av verkställandet av Säkerhetsstrategi för samhället. Cybersäkerhetsstrategin följer de principer och definitioner som ingår i Säkerhetsstrategi för samhället samt statsrådets beslut om målen med försörjningsberedskapen. Tyngdpunkterna och målen för tryggandet av försörjningsberedskapen fastställs i statsrådets beslut om målen för försörjningsberedskapen (2013). I strategin har principbeslutet om den övergripande säkerheten beaktats.

Cybersäkerheten är inte avsedd att vara ett juridiskt begrepp som skulle ge myndigheter eller andra organ nya befogenheter. Till denna del föreslås inga ändringar i grunderna för beredskapssystemet och inte heller i bestämmelserna om olika myndigheters befogenheter.

I denna strategi skildras en vision, en handlingsmodell och strategiska riktlinjer för cybersäkerheten. Det verkställighetsprogram som ska beredas kommer att innehålla de praktiska åtgärder som förvaltningsområdena och aktörerna får beredningsansvar för. Med dessa åtgärder skapas förutsättningar för att genomföra de strategiska riktlinjerna samt för att man ska kunna nå det måltillstånd som beskrivs i visionen inklusive de tvärsektoriella åtgärder som man kommit överens om tillsammans.

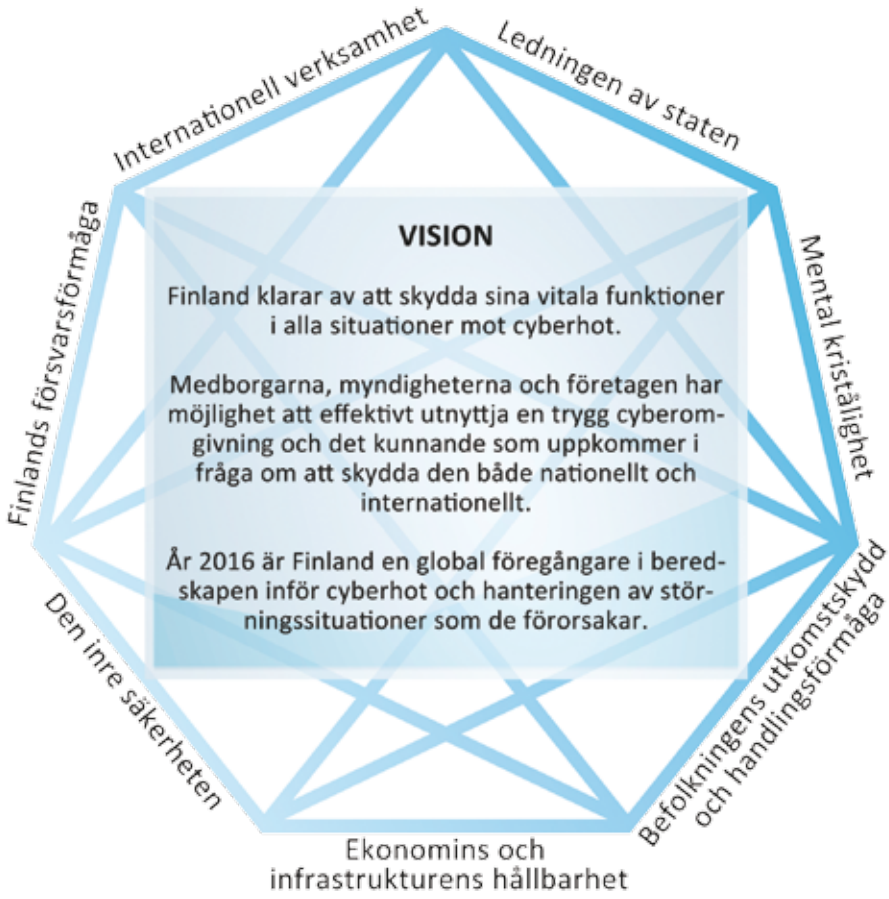
2. VISION OM CYBERSÄKERHETEN

I egenskap av ett litet och kunnigt land med samarbetsförmåga har Finland utmärkta förutsättningar att bli ett toppland inom cybersäkerheten. Vi har en stark kunskapsbas samt långa traditioner av ett intensivt och förtroligt samarbete mellan den privata och den offentliga sektorn samt mellan förvaltningens områden.

Den finska cybersäkerhetens vision är:

- Finland kan skydda sina vitala funktioner i alla situationer mot cyberhot.
- Medborgarna, myndigheterna och företagen har möjlighet att både nationellt och internationellt effektivt utnyttja en säker cyberomgivning och det kunnande som uppkommer i och med att omgivningen skyddas.
- År 2016 är Finland en global föregångare inom beredskapen inför cyberhot och hanteringen av de störningssituationer som de förorsakar.

FIGUR 1 Vision om cybersäkerheten



3. LEDNINGEN AV CYBERSÄKERHETEN OCH EN NATIONELL HANDLINGSMODELL

Handligsmodell

De ändringar som sker i cyberomgivningen är snabba och deras konsekvenser svåra att förutse. Informationsteknologins utvecklingscykel är kort och samma trend gäller olika cyberattackformer och skadeprogram. Detta ställer en allt större utmaning på samhällets förmåga att förbereda sig på olika slag av cyberhot. Beredskapen inför cyberhot och bekämpningen av dem förutsätter snabbare, mera transparent och bättra samordnad verksamhet av alla parter i samhället både separat och tillsammans.

Vid ledningen av cybersäkerheten står Statsrådet överst. Statsrådet har till uppgift att politiskt styra cybersäkerheten och dra upp strategiska riktlinjer för den samt att besluta om cybersäkerhetens resurser och verksamhetsbetingelser.

Ledningen av cybersäkerheten och hanteringen av störningssituationer förutsätter att statsrådet och de olika aktörerna till sitt förfogande har en tillförlitlig och aktuell lägesbild över cybersäkerheten om tillståndet hos samhällets vitala funktioner och om de störningar som riktar sig mot dem. Varje ministerium och förvaltningsområde svarar för cybersäkerheten och för hanteringen av de störningssituationer som anknyter till den. Cyberomgivningen och hotens art framhäver samarbetet och effektiviteten och flexibiliteten i de åtgärder som vidtas för att sammanjämka samarbetet och beredskapen. Ministeriernas strategiska uppgifter inom cybersäkerheten och de utvecklingsbehov som anknyter till dem grundar sig på en analys av identifierade cyberhot och på de krav som ställs för hanteringen av de störningssituationer som dessa orsakar. Varje ministerium bör i enlighet med sina befogenheter sörja för att de strategiska uppgifter som fastställs utgående från måltillstånden blir genomförda.

Den nationella förmågan att tåla cyberhot (cyberresilience) dimensioneras så att man med den klarar av att skapa en förmåga till beredskap och förutseende som stämmer överens med målen för den övergripande säkerheten, handlingsförmåga i cyberstörningssituationer samt förmåga att återhämta sig efter cyberstörningar.

Handlingsmodellen för den finska cybersäkerheten bygger på följande principer:

1. De ärenden som gäller cybersäkerheten hör i regel till statsrådets befogenheter på så sätt att det har föreskrivits att uppgifterna ingår i ministeriernas ansvarsområden. Varje ministerium svarar inom sitt område för beredning av och korrekt organisering av förvaltningen i fråga om de ärenden som hör till statsrådet och anknyter till cybersäkerheten.

2. Cybersäkerheten utgör en fast del av samhällets övergripande säkerhet och dess handlingsmodell följer de principer och handlingssätt som fastställts i Säkerhetsstrategi för samhället (SSS).

3. Cybersäkerheten baserar sig på arrangemang som gäller datasäkerheten i hela samhället. En förutsättning för cybersäkerheten är att var och en som agerar i cyberomgivningen genomför ändamålsenliga och tillräckliga säkerhetslösningar för datasystemen och datanäten. Genomförandet av dessa främjas och stöds med hjälp av olika slag av strukturer och övningar som grundar sig på samverkan.

4. Handlingsmodellen för cybersäkerheten grundar sig på ett effektivt och vidsträckt system för att skaffa, samla in och analysera information, på gemensam och delad lägesuppfattning samt på beredskap att samverka nationellt och internationellt. För detta förutsätts att ett nationellt cybersäkerhetscenter grundas samt att dataskyddsverksamhet dygnet runt för hela samhället utvecklas.

5. I de arrangemang som gäller cybersäkerheten följs en ansvarsfördelning mellan myndigheter, företag och organisationer som baserar sig på författningar och överenskommet samarbete. Behovet att anpassa sig till snabba ändringar, förmåga att utnyttja nya möjligheter och reagera på överraskande situationer kräver att aktörerna förstår sig på och följer principerna om strategisk lättrörlighet vid utvecklandet och ledningen av de åtgärder som siktar till att åstadkomma cybersäkerhet.

6. Cybersäkerheten skapas utgående från funktionella och tekniska krav. Utöver nationella åtgärder satsas det på internationell samverkan och deltas det i internationell forskning och utveckling samt i övningar. Genomförandet av sådan forskning, utveckling och utbildning som siktar till cybersäkerhet på olika nivåer förstärker det nationella kunnandet och Finland som informationssamhälle.

7. Vid utvecklandet av cybersäkerheten satsas det kraftigt på forskning, utbildning, sysselsättning och produktutveckling inom cyberomgivningen för att Finland ska kunna utvecklas till ett ledande land på cybersäkerhet.

8. För säkerställande av cybersäkerhetsutvecklingen sörjer man för att det i Finland finns en sådan gällande lagstiftning och incitament som stöder företagsverksamheten på detta område och utvecklandet av den. Till en central del utvecklar sig kunnandet i branschen via företagsverksamhet.

4. STRATEGISKA RIKTLINJER FÖR CYBERSÄKERHETEN

Den nationella cybersäkerheten utvecklas i enlighet med strategiska riktlinjer. Med dem skapas förutsättningar för att realisera en nationell vision om cybersäkerheten. I ett verkställighetsprogram, som ska utarbetas separat, fastställs de åtgärder med vilka det säkerställs att de nationella cybersäkerhetsmålen uppnås. Verkställighetsprogrammet består av planer som de olika aktörerna och förvaltningsområdena har utarbetat samt av tvärsektoriella åtgärder som ska vidtas utgående från dem.

Genom verkställandet av de strategiska riktlinjerna förstärker man samarbetet mellan den offentliga och den privata sektorn, vilket upplevs som en styrka för det finska säkerhetssamarbetet. Med hjälp av detta samarbete kan man bäst betjäna hela samhället och stöda de aktörer som producerar dess vitala funktioner. Målet är att sörja för att de olika funktionerna kan fortgå störningsfritt och säkert i vardagen och i störningssituationer.

Cybersäkerheten baserar sig på ett långsiktigt och tillräckligt utvecklande av kapaciteterna, på en flexibel användning av dem i rätt tid samt på de vitala funktionernas förmåga att tåla störningssituationer i cybersäkerheten. Myndigheternas kapacitet i cybersäkerheten utvecklas under ledning av behöriga myndigheter och t.ex. genom att ministeriernas strategiska uppgifter i cybersäkerheten fastställs. Med utvecklandet av de flesta strategiska cybersäkerhetsuppgifterna och de kapaciteter som är förknippade med dem sammanhänger också åtgärder och resurser från andra ministerier, region- och lokalförvaltning, näringsliv och organisationer. Vid utvecklandet och användningen av kapaciteterna ska ministerierna alltid beakta förvaltningens olika nivåer samt näringslivets och organisationernas roll. En Säkerhetskommitté grundas inom den övergripande säkerhetens område för att vara ett permanent samarbetsorgan för beredskapen. Om Säkerhetskommitténs uppgifter föreskrivs särskilt.

DE STRATEGISKA RIKTLINJERNA:

1	**För att främja den nationella cybersäkerheten och avvärja cyberhoten skapas en modell för effektiv samverkan mellan myndigheter och andra aktörer.** De strategiska riktlinjerna för cybersäkerhetsstrategin främjas genom att den aktiva samverkan mellan aktörerna, där målet är en delad lägesuppfattning och effektiv avvärjning av hot, utökas. Sektorernas beredskap att agera vid störningar i de vitala funktionerna övas regelbundet. Varje aktör utvecklar sitt nationella och internationella deltagande i övningarna. I de internationella övningarna förbättrar aktörerna utnyttjandet av bästa praxis och erhållna lärdomar genom att effektivera informationsutbytet och samordningen. Målet med övningsverksamheten är att ge deltagarna bättre möjligheter att upptäcka sårbarheter i verksamheten och systemen, utveckla kapaciteterna och utbilda personalen. För avvärjande av cyberhoten främjas informationsutbytet mellan myndigheter och näringsliv genom att reglering och samarbete utvecklas.
2	**De centrala aktörer som är med och tryggar samhällets vitala funktioner ges en bättre övergripande lägesuppfattning och lägesförståelse i fråga om cybersäkerheten.** Målet är att förbättra de olika aktörernas lägesuppfattning genom att erbjuda dem aktuell, samlad och analyserad information om sårbarheter, störningar och konsekvenserna av dem. I lägesbilden ingår uppskattningar av och prognoser över de hot som cyberomgivningen medför. För att cyberhoten ska kunna förutsägas förutsätts bedömning av den politiska, militära, sociala, kulturella, tekniska och teknologiska samt ekonomiska situationen. För att en sammanställd lägesbild över cybersäkerheten ska kunna produceras och upprätthållas, grundas ett cybersäkerhetscenter som en del av Kommunikationsverket. Cybersäkerhetscentret samlar information om cyberhändelser och förmedlar den till de olika aktörerna. Aktörerna analyserar hur störningen inverkar på den verksamhet som de ansvarar för. Dessa analyser sänds i retur till centret och inbegrips i den sammanställda lägesbild över cybersäkerheten som ska utformas. Denna sammanställning delas ut till de olika aktörerna som grund för beslutsfattandet. Statsrådets lägescentral bör till sitt förfogande ha en tillförlitlig, täckande och aktuell övergripande lägesbedömning av cybersäkerheten. Bedömningen utgörs av cybersäkerhetscentrets sammanställda lägesbild samt förvaltningsområdenas bedömningar av cyberhändelsernas verkningar på samhällets vitala funktioner. Statsledningen har till sitt förfogande en övergripande lägesbedömning samt en bedömning av utvecklingen i den övriga omgivningen.

3	**Förmåga att upptäcka och avvärja cyberhot och cyberstörningssituationer som äventyrar en vital funktion samt att återhämta sig från dem som en del av kontinuitetshanteringen i näringslivet upprätthålls och utvecklas hos de företag och organisationer som är viktiga med tanke på tryggandet av samhällets vitala funktioner.** De företag och organisationer som är viktiga med tanke på samhällets vitala funktioner tar i sin säkerhets- och beredskapsplanering samt i de servicestrukturer som anknyter till dem i täckande grad i beaktande cyberhotmodellerna och upprätthåller den skyddsförmåga som behövs. Målet är att de eventuella störningar av de vitala funktionerna som kommer fram vid riskbedömningar ska upptäckas och identifieras och på dem ska reageras på ett sätt som minimerar deras skadliga verkningar. Centrala aktörer utvecklar sin tolerans, inklusive planering och inövning av reservmetoder, så att de kan agera under cyberattacker. Försörjningsberedskapsorganisationen stöder verksamheten med utredningar, anvisningar och utbildning.
4	**Det sörjs för att polisen har effektiva förutsättningar att förebygga, avslöja och reda ut brott som riktar sig mot och utnyttjar cyberomgivningen.** Förundersökningsmyndighet vid brott som riktar sig mot och utnyttjar cyberomgivningen är polisen. Polisen sammanställer en analyserad och högklassig lägesbild av cyberkriminaliteten och distribuerar den som en del av den sammanställda lägesbild som beskrivs i den andra strategiska riktlinjen. Det sörjs för att polisen har tillräckliga befogenheter och resurser samt en kunnig och motiverad personal som sköter förebyggandet, den taktiska förundersökningen och behandlingen och analyseringen av digitalt bevismaterial om brott som riktar sig mot och utnyttjar cyberomgivningen. Det internationella operativa samarbetet och informationsutbytet med EU:s och andra länders lagövervakningsmyndigheter och motsvarande aktörer, såsom Europol, fortgår och fördjupas.

5	**Försvarsmakten skapar en övergripande cyberförsvarsförmåga i sina lagstadgade uppgifter.** För att de uppgifter som nämns ovan ska kunna uppfyllas, utarbetas under försvarsministeriets ledning det befogenhetsregelverk som försvarsmakten behöver. Identifierade brister i de författningar som gäller befogenheterna korrigeras med lagstiftningsåtgärder. Den militära cyberförsvarsförmågan bildas av kapaciteterna underrättelse, påverkan och skyddande. Försvarsmakten skyddar sina egna system så att den klarar av sina lagstadgade uppgifter trots hoten från cyberomgivningen. För att säkerställa kapaciteten utvecklas underrättelse- och påverkansförmågan i cyberomgivningen som en del av utvecklandet av den övriga användningen av militära maktmedel. För att de uppgifter som nämns ovan ska kunna uppfyllas utarbetas under försvarsministeriets ledning ett regelverk över de befogenheter som försvarsmakten behöver. Brister som upptäcks i befogenhetsbestämmelserna korrigeras med lagstiftningsåtgärder. Cyberförsvar övas och utvecklas tillsammans med centrala myndigheter, organisationer och näringslivets aktörer både nationellt och internationellt. Försvarsmakten ger handräckning när lagstiftningen tillåter det.
6	**Den nationella cybersäkerheten förstärks genom ett aktivt och effektivt deltagande i verksamheten vid de internationella organisationer och samarbetsforum som är viktiga med tanke på cybersäkerheten.** Målet med den internationella samverkan är att utbyta information och erfarenheter samt att lära sig bästa praxis för att nivån på den nationella cybersäkerheten ska kunna höjas. Genomförandet av beredskapen och annan cybersäkerhet är ofullständigt utan effektiv och systematisk samordning av det internationella samarbetet. Varje myndighet bedriver inom sitt område samarbete särskilt med de stater och organisationer som är globala föregångare i sakhelheter som anknyter till cybersäkerheten. Aktivt samarbete bedrivs genom att det deltas i forsknings- och utvecklingsarbete, beredningen av olika avtal, organisationers arbetsgruppsarbete, och internationella övningar. Europeiska unionen och många internationella organisationer, såsom FN, OSSE, NATO och OECD är viktiga forum för Finland när cybersäkerheten utvecklas. EU är allt aktivare verksam inom cybersäkerhetens område och unionen har också samarbete med tredje länder. Finland deltar aktivt i detta utvecklingsarbete.

7	**Cyberkunnandet och cyberförståelsen förbättras hos alla aktörer i samhället.** För att ett kontinuerligt utvecklande av kunskap och vetande hos samhällets aktörer ska kunna stödjas satsas det på utveckling, utnyttjande och utbildning i gemensamma anvisningar för cybersäkerheten och informationssäkerheten. För att en övergripande beredskap ska utvecklas i samhället tas i övningsverksamheten med också de företag och medborgarorganisationer som är viktiga med tanke på samhällets vitala funktioner. I samband med den redan existerande ICT-SHOK (TIVIT) grundas en strategisk koncentration av spetskompetens inom cybersäkerheten, som erbjuder forskningsenheter och företag som utnyttjar forskningsresultaten ett effektivt sätt att bedriva intensivt och långsiktigt samarbete. Koncentrationen skapar förutsättningar för att bygga upp ett starkt nationellt cyberkunskapskluster. Satsningarna på forskning, produktutveckling och utbildning utökas liksom också åtgärderna för att utveckla kunnandet i cybersäkerhet i hela samhället.
8	**Genom nationell lagstiftning säkerställs förutsättningarna för att effektivt realisera cybersäkerheten.** Den lagstiftning som påverkar och anknyter till cyberomgivningen och cybersäkerheten samt behoven att utveckla den kartläggs i samarbete mellan förvaltningsområdena och näringslivet. Som ett resultat av lagstiftningskartläggningen erhålls förslag till hur lagstiftningen kan utvecklas, och med dessa förslag främjas att målen enligt cybersäkerhetsstrategin nås. Ett syfte med kartläggningen är att lagstiftningen ska ge möjlighet och tillräckliga metoder och befogenheter för behöriga myndigheter och andra aktörer inom olika områden att realisera skyddandet av samhällets vitala funktioner och i synnerhet statens säkerhet mot cyberhot. Också de hinder och begränsningar som lagstiftningen och förpliktelser som härrör från internationella fördrag eventuellt ställer, tas upp till granskning samt de förpliktelser som gäller informationsbehandling och som utgör en olägenhet när det gäller att få, överlåta och mellan olika myndigheter och andra aktörer utbyta den information som behövs för att cyberhot ska kunna avvärjas effektivt. I en granskning som gäller insamling och annan hantering av uppgifter ska dessutom bedömas om det finns skäl att för de ansvariga myndigheterna skapa bättre möjligheter än dagens att på förhand samla in, sammanställa och få information om cyberhot och om dem som orsakar sådana. Detta görs så att man samtidigt ägnar uppmärksamhet åt integritetsskyddet och skyddet för förtroliga meddelanden som är grundläggande fri- och rättigheter. Största delen av samhällets kritiska infrastruktur är i privat ägo och opereras som affärsverksamhet. En stor del av skapandet och skyddandet av cyberförmåga, kunnande och tjänster som gäller detta genomförs av företag. Den nationella lagstiftning som reglerar cyberomgivningen bör vara sådan att förutsättningarna för att utveckla affärsverksamhet är gynnsamma. Detta igen möjliggör uppkomsten av ett cyberkunskapskluster som är internationellt erkänt, konkurrenskraftigt och har exportmöjligheter. Samtidigt utvecklas Finland till en attraktiv cybersäker miljö, som det lönar sig att göra investeringar och fatta beslut om att etablera företag i.

9	**Uppgifter och tjänstemodeller som gäller cybersäkerheten samt gemensamma grunder för hanteringen av de krav som cybersäkerheten ställer fastställs för myndigheterna och näringslivets aktörer.** För att cybersäkerheten ska kunna utvecklas krävs en klar definiering av ansvaret och fördelning av uppgifterna i enlighet med de strategiska riktlinjerna. I praktiken förutsätter detta att varje förvaltningsområde gör en riskbedömning och mogenhetsanalys med hjälp av vilka det identifieras vilka sårbarheter och risker som är av betydelse med tanke på cybersäkerheten samt på vilken nivå de ska hanteras. På basis av de resultat som erhålls utarbetas verkställighetsprogram för varje förvaltningsområde samt understöds utarbetandet av verkställighetsprogram för näringslivet i samverkan med försörjningsberedskapsorganisationen.
10	**Verkställandet av strategin övervakas och utfallet följs upp.** Ministerierna och ämbetsverken svarar inom sitt verksamhetsområde för verkställandet av strategin, genomförandet av de uppgifter och försörjningsberedskapsarrangemang som anknyter till cybersäkerheten samt för utvecklandet av dem. Den kommande Säkerhetskommittén följer och samordnar verkställandet av strategin. Målen med samordningen av cybersäkerheten är att undvika överlappande verksamhet, identifiera eventuella brister och försäkra sig om ansvariga parter. De egentliga besluten fattas av behörig myndighet i enlighet med vad som föreskrivs om saken. VAHTI behandlar och samordnar statsförvaltningens centrala riktlinjer som gäller informations- och cybersäkerheten. Ministerierna, ämbetsverken och inrättningarna tar i sina verksamhets- och ekonomiplaner in de resurser som förutsätts för att cybersäkerhetsstrategin ska kunna verkställas.

Begrepp	Definition
Cyber-	Ordet cyber används nästan utan undantag som den bestämmande delen av ett sammansatt ord, inte ensamt. Ordets betydelse anknyter i allmänhet till behandlingen av information (data) i elektronisk form: till informationsteknik, elektronisk kommunikation (dataöverföring), informations- och datorsystem. Endast hela det sammansatta ordet (en kombination av förled och grundled) kan anses ha en egen betydelse. Ordet cyber anses ha sitt ursprung i det grekiska ordet ”kybereo” – styra, handleda, behärska.
Cyberhot	Cyberhot avser möjligheten till en sådan gärning eller händelse som påverkar cyberomgivningen och vilken om den realiseras äventyrar någon funktion som är beroende av cyberomgivningen. Anmärkning Hot som riktar sig mot cyberomgivningen är datasäkerhetshot som, om de realiseras, äventyrar korrekt eller avsedd funktion i informationssystemet.
Cyberomgivning	Cyberomgivningen är en omgivning som är avsedd för hantering av information (data) i elektronisk form och som består av ett eller flera informationssystem. Anmärkning 1 Symtomatiskt för omgivningen är att det elektroniska och elektromagnetiska spektret används för att lagra, bearbeta och överföra data och information med hjälp av kommunikationsnät. Till omgivningen hör också fysiska strukturer som anknyter till hanteringen av data och information. Anmärkning 2 Hantering av information (data) innebär insamling, sparande, organisering, användning, överföring, överlåtelse, förvaring, ändring, kombinering, skyddande, avlägsnande, förstöring av information (data) samt andra åtgärder som vidtas i fråga om information (data).
Cyberrisk	Med cyberrisk avses risk för skada eller sårbarhet som riktar sig mot cyberomgivningen och som, om den realiseras eller om man utnyttjar den, kan orsaka skada, olägenhet eller störning för en funktion som är beroende av en fungerande cyberomgivning.
Cybersäkerhet	Med cybersäkerhet avses ett måltillstånd där man kan lita på cyberomgivningen och där dess funktion tryggas. Anmärkning 1 I måltillståndet orsakar cyberomgivningen ingen fara, olägenhet eller störning för den verksamhet som är beroende av att elektronisk data (information) hanteras och inte heller för dess funktion. Anmärkning 2 Förtroendet för cyberomgivningen grundar sig på att dess aktörer vidtar ändamålsenliga och tillräckliga åtgärder gällande informationssäkerheten (”kollektiv datasäkerhet”). Med hjälp av åtgärderna kan man förhindra att hoten mot dataskyddet realiseras och, om de eventuellt realiseras, förhindra, lindra eller klara av verkningarna av dem. Anmärkning 3 Cybersäkerheten omfattar de åtgärder som inriktas på samhällets vitala funktioner och kritiska infrastruktur, vilkas mål är att uppnå förmåga att förutseende hantera och vid behov tåla cyberhot och verkningarna av dem, vilka kan orsaka betydande skada eller risk för Finland eller dess befolkning.

Begrepp	Definition
Dataskydd eller datasekretess	Med dataskydd avses skyddet av en persons integritet mot orättmätig eller för personen skadlig användning. I dataskyddet ingår skyddet av människors privatliv och andra rättigheter som tryggar detta när personuppgifter hanteras. Med personuppgift avses alla slags anteckningar som beskriver en fysisk person eller hans eller hennes egenskaper eller levnadsförhållanden, vilka kan identifieras som gällande personen eller hans eller hennes familj eller dem som lever i samma hushåll.
Datasäkerhet eller informationssäkerhet	Med datasäkerhet avses de arrangemang genom vilka man försöker säkerställa att data är användbar, sammanhängande och konfidentiell.
Informationsstruktur	Med informationsstruktur avses strukturer och funktioner som utgör informationssystemens grund och vilkas uppgift är att sända, överföra, ta emot, lagra eller annars hantera information i elektronisk form.
Informationssystem	Med informationssystem avses ett system som består av människor, databehandlingsapparatur, dataöverföringsapparatur och programvaror och vars syfte är att genom att behandla information effektivera eller underlätta en verksamhet eller göra en verksamhet möjlig.
Kritisk informationsstruktur	Med kritisk informationsstruktur avses strukturer och funktioner som utgör informationssystemens grund för samhällets vitala funktioner och vilkas uppgift är att sända, överföra, ta emot, lagra eller annars hantera information i elektronisk form.
Kritisk infrastruktur	Den kritiska infrastrukturen omfattar de strukturer och funktioner som är nödvändiga för samhällets vitala funktioner. Till dem räknas både fysiska inrättningar och strukturer och elektroniska funktioner och tjänster.
VAHTI	Ledningsgruppen för datasäkerheten inom statsförvaltningen
SSS	Säkerhetsstrategi för samhället, Statsrådets principbeslut av den 16 december 2010

www.yhteiskunnanturvallisuus.fi/sve

BAKGRUNDSPROMEMORIA TILL STRATEGI FÖR CYBERSÄKERHETEN I FINLAND

Säkerhetskommitténs bakgrundspromemoria

1. INLEDNING

Denna bakgrundspromemoria har upprättats som en del av Strategin för cybersäkerheten i Finland. Det centrala syftet med bakgrundspromemorian är att öka förståelsen bland cybersäkerhetens aktörer för cyberomgivningen och genom detta hjälpa dem att utveckla sin egen cybersäkerhet. Bakgrundspromemorian fördjupar den egentliga strategin och beskriver mera i detalj vår nationella handlingsmodell för cybersäkerheten samt den hotmodell som beskrivits som grund för cyberomgivningen och beredskapen. I bakgrundspromemorian förklaras de åtgärder som de strategiska riktlinjerna kräver samt det nationella och internationella regelverk som hänför sig till cybersäkerheten. I slutet av promemorian presenteras grunder för utarbetandet av verkställighetsprogram för de olika förvaltningsområdena och andra aktörer.

2. CYBEROMGIVNINGEN OCH CYBERHOT

Den globala cyberomgivningen består av ett världsomfattande informationsnätverk som är komplicerat och har flera nivåer. Till detta nätverk hör säkerhetsmyndigheternas, den övriga offentliga förvaltningens och företagsvärldens nationella kommunikationsnät samt övervaknings- och styrsystem för industrin och kritisk infrastruktur. Den globala cyberomgivningen gör att stater, företag och medborgare kommer varandra närmare mera i realtid än tidigare. Denna utveckling har i betydande grad ökat välfärden, men också medfört risker av helt nya slag. Det att datatekniska apparater och system inte fungerar, informationsinfrastrukturen kollapsar eller allvarliga cyberattacker utförs kan medföra ytterst negativa konsekvenser för de offentliga tjänsterna, företagslivet och förvaltningen och därmed för hela samhällets funktion.

Genom cyberattacker kan man orsaka stora störningar och t.o.m. lamslå delar av den kritiska infrastrukturen och samhällets vitala funktioner. En stat eller en organisation kan utsättas för påtryckning till att ge politiska, militära eller ekonomiska eftergifter. Stormakterna har jämställt cyberattacker med militära åtgärder som kan besvaras med alla till buds stående medel.

Tills vidare har cyberoperationer tolkats som s.k. mjuka åtgärder, vilket gör att tröskeln för att använda dem kan bedömas vara lägre än vid traditionella militära operationer. Ökande cyberaktivism, cyberkriminalitet och cyberspionage visar att både statliga och icke-statliga aktörer utökar sina aktioner. Cyberomgivningen har följaktligen förändrat de traditionella internationella maktkonstellationerna. Den ger också små stater och icke-statliga aktörer möjlighet att agera effektivt. I cybervärlden är storleken och massan inte längre rådande, utan kunskapen.

Den ovan beskrivna utvecklingen av cyberomgivningen påverkar också Finland. Finland är ett av de mest utvecklade informationssamhällena, vars funktioner är beroende av olika elektroniska nät och de tjänster de erbjuder. Finland har redan blivit föremål för

cyberoperationer, där tyngdpunkten har varit cyberaktivism, cyberkriminalitet och cyberspionage. Den internationella utveckling som sker i cyberomgivningen ökar risken för att nya hot kommer att riktas mot oss. Den offentliga förvaltningen och näringslivet är hela tiden utsatta för försök att utnyttja sårbarheter i systemen eller bryta sig in i dem. Attackernas professionella natur kan ses i det att föremålet för attackerna har valts ut och ett noggrant underrättelsearbete har gjorts om det. I allt högre grad används avancerade skadeprogram och tekniker vid attackerna.

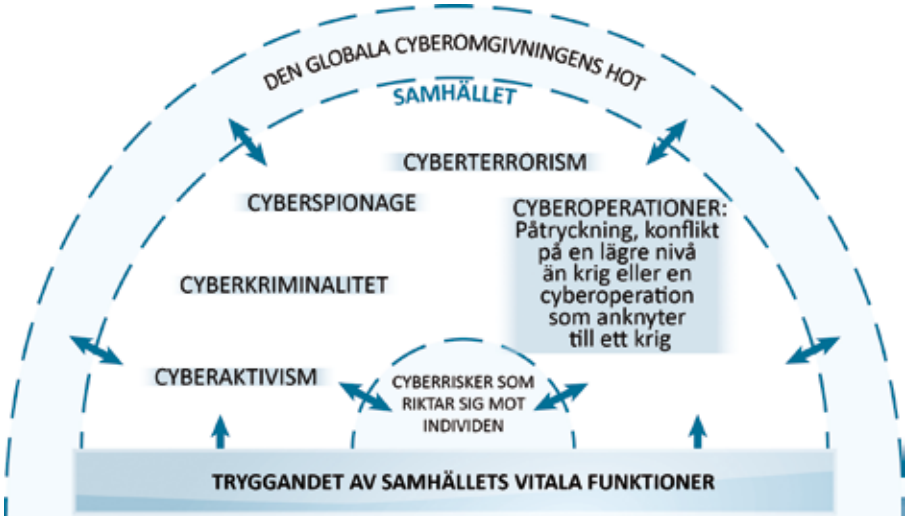
Det att cybervärlden är öppen gör attacker från olika håll av världen möjliga genom att sårbarheter i systemen utnyttjas. Dessa sårbarheter finns såväl i människornas handlande och organisationernas verksamhetsprocesser som också i den informationsteknologi som används. Det är svårt att skydda sig mot komplicerade och avancerade skadeprogram. Det är också svårt att identifiera eller hitta dem som utför attackerna. Det faktum att datatekniken har spritt sig allt mera vidsträckt till industriproduktions- och styrsystemen har skapat nya sårbarheter och möjliga föremål för attacker i cyberomgivningen.

Vad gäller cybersäkerheten var år 2010 början på en ny era, när nätmasken Stuxnet hittades. Med hjälp av den genomfördes en attack mot iranska kärnanläggningar, där Stuxnet skadade centrifuger som var avsedda för anrikning av uran och därmed fördröjde det iranska anrikningsprojektet med upp till flera år. Utvecklandet av Stuxnetkoden har krävt stor skicklighet och betydande resurser. Detta skadeprogram visade att man med cyberverktyg kan orsaka också fysisk förstörelse i elektriska anläggningar och system. I denna nya fas är industriautomation och programmerbar logik oftare än tidigare det första föremålet för cyberangrepp medan det slutliga målet är att påverka samhällets vitala funktioner.

Med en cyberhotmodell avses en beskrivning av de störningar som cyberhot orsakar, hotets verkningsmekanismer, källa, föremål och inverkan på föremålet. Hoten kan riktas direkt eller indirekt mot samhällets vitala funktioner, nationell kritisk infrastruktur och/eller medborgare och hotet kan vara inhemskt eller utländskt.

I cyberhotmodellen är cyberhoten

- cyberaktivism (cybervandalism, hacktivism)
- cyberkriminalitet
- cyberspionage
- cyberterrorism
- cyberoperationer; påtryckning, en konflikt på lägre nivå än krig eller en cyberoperation i anknytning till ett krig



FIGUR 1 Finsk cyberhotmodell.

De hot som riktas mot samhällets vitala funktioner och kritiska infrastruktur kan förekomma självständigt, samtidigt eller som förlängning av varandra. Hur snabbt hoten eskalerar och hur länge de räcker varierar, men mycket ofta realiseras effekterna på kort tid. Till följd av cyberomgivningens natur är det svårt att förutse skälen till hoten, vilka aktörer som ligger bakom dem, exakta objekt och mål, vilken omfattning de kommer att ha eller vilka konsekvenserna av dem blir. Med cyberhoten kan också sammanhänga andra hot. Till exempel i terrorism kan olika slags operationer i cyberomgivningen fogas till angrepp som orsakar fysisk förstörelse.

3. PRINCIPERNA FÖR LEDNINGEN AV CYBERSÄKERHETEN OCH HANTERINGEN AV STÖRNINGSSITUATIONER

3.1 De allmänna principerna för ledningen av cybersäkerheten

Statsrådet utgör högsta nivån på ledningen av cybersäkerheten. Statsministern leder statsrådets verksamhet och sörjer för samordningen av beredningen och behandlingen av de ärenden som hör till statsrådet. Ärendena behandlas och sammanpassas i förberedande syfte vid statsrådets ministerutskott, som leds av statsministern, samt vid behov vid regeringens aftonskola och överläggning. Statsrådet har till uppgift att politiskt styra cybersäkerheten och dra upp de strategiska riktlinjerna för den samt att besluta om resurser och verksamhetsbetingelser för cybersäkerheten.

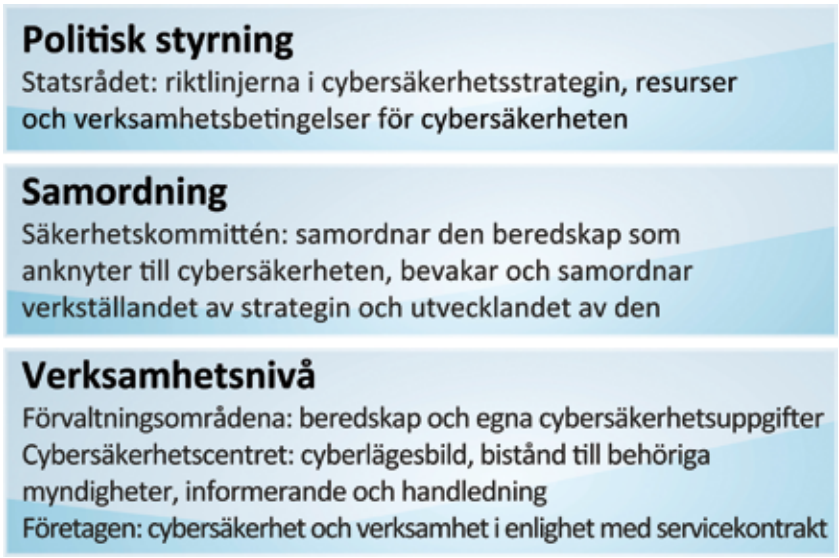
I enlighet med grundprinciperna i Säkerhetsstrategi för samhället svarar behöriga myndigheter för hanteringen av störningssituationer och för den beredskap som sammanhänger med detta. Varje ministerium svarar för beredningen av lagstiftningen inom sitt verksam-

hetsområde och leder ansvarsområdets verksamhet samt deltar enligt behov i samverkan ministerierna emellan. Cybersäkerhetsstrategin ändrar inte på de uppgifter som fastställs i Säkerhetsstrategi för samhället. I enlighet med dem svarar kommunikationsministeriet för säkerställandet av att de elektroniska informations- och kommunikationssystemen fungerar och finansministeriet för tryggandet av statsförvaltningens IT-funktioner och datasäkerhet samt de servicesystem som är gemensamma för statsförvaltningen.

Den nya Säkerhetskommitté som ska tillsättas kommer att samordna beredskapen inom cybersäkerheten och följa verkställandet av cybersäkerhetsstrategin samt komma med förslag till hur den ska utvecklas i fortsättningen. Säkerhetskommittén verkar i nära samarbete med övriga samarbetsorgan, som samordnar de frågor som sammanhänger med cybersäkerheten i anknytning till sina egna uppgifter.

Ett nytt cybersäkerhetscenter, som ska grundas, kommer att stöda och bistå cybersäkerhetens aktörer i enlighet med de uppgifter som centret självt ansvarar för. Ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) stöder statsrådet och finansministeriet i det beslutsfattande som gäller förvaltningens datasäkerhet. VAHTI behandlar alla betydande ärenden som gäller statsförvaltningens data- och cybersäkerhet.

Hur effektiv ledningen i störningssituationer är beror på hur väl de föregripande åtgärderna lyckas. Arrangemangen för cybersäkerheten under normala förhållanden inverkar i avgörande grad på hur man i undantagsförhållanden kan klara sig ur cyberhotsituationer. Varje område av förvaltningen och varje företag och organisation som är kritisk med tanke på försörjningsberedskapen har en skyldighet att förbereda sig på cyberhot. Företagen planerar beredskapen på cyberhot som en del av övrig kontinuitetshantering.



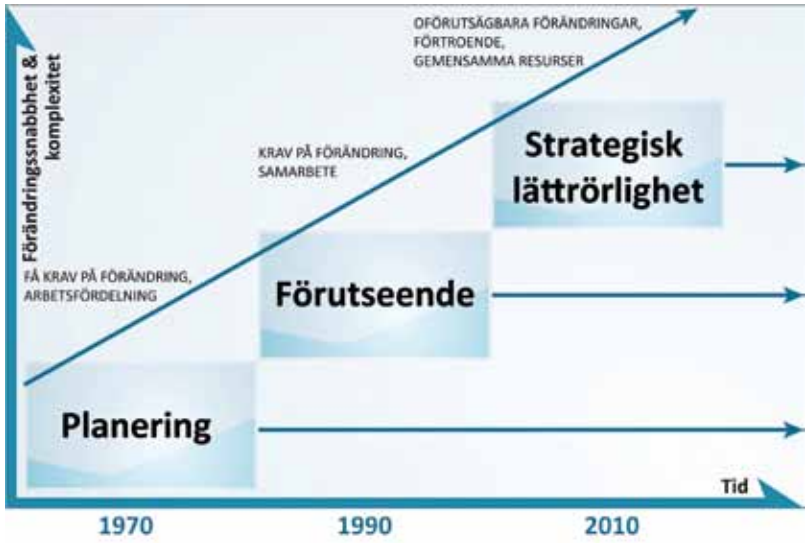
FIGUR 2 Principerna för ledningen av cybersäkerheten

För att cyberhot ska kunna avvärjas krävs god planering och framförhållning. Vår nya omgivning förutsätter följaktligen att alla parter har ett starkt kunnande samt att de snabbt och enhetligt reagerar i rätt riktning, dvs. det som kallas strategisk lättrörlighet. I ledningen av cybersäkerheten visar sig alla tre faktorer som ingår i strategisk lättrörlighet. De är strategisk känslighet, en enhetlig ledning samt en flexibel användning av resurserna.

Strategisk känslighet förutsätter förmåga att snabbt forma en lägesbild och bilda sig en lägesuppfattning. En enhetlig ledning förutsätter delad lägesuppfattning, samordnat och nätverkande ledarskap samt optimering av den fördel som helheten ger. En flexibel användning av resurserna kräver tillräckligt cyberkunnande samt förmåga att snabbt allokera motåtgärder och ekonomiska resurser. I cyberomgivningen bör man kunna lösgöra sig från att endast optimera delarna samt från den stelhet som silotänkandet i fråga om strukturerna medför.

Förändringshastigheten i cyberomgivningen och dess komplexa natur förutsätter således en nätverksbaserad verksamhetsmodell av ett nytt slag, som grundar sig på en stark samordning och gemensamma spelregler (figur 3). I verksamheten måste man kunna förena fördelarna av både koncentrering och splittring. Dessa fördelar är en stark samordning samt reaktionssnabbhet som uppkommer i och med att man är delaktig i saken.

I princip har Finland i förhållande till många andra länder utmärkta möjligheter att stiga fram som en föregångare i världen vad gäller cybersäkerhet och den nya verksamhetsmodell som den kräver. Våra obestridda styrkeområden är ett starkt kunnande, en tradition av samarbete både inom den offentliga förvaltningen och mellan den offentliga och den privata sektorn samt väl definierade verksamhetsmodeller och säkerhetsansvar mellan de olika aktörerna (SSS).



FIGUR 3 Strategisk lättrörlighet

3.2 Hanteringen av de störningssituationer som hotar samhället

I takt med att samhällets sårbarhet ökar är det nödvändigt att man snabbt kan inleda de åtgärder som förutsätts för att överraskande och snabbt uppkomna cyberstörningssituationer ska kunna fås under kontroll. För cyberstörningssituationer är det symtomatiskt att deras inverkan är flerdimensionell, vilket gör att det är nödvändigt att den behöriga myndigheten när det behövs till sitt förfogande får ett så vidsträckt tvärsektoriellt stöd som möjligt. Samtidigt måste man kunna säkerställa att samhället fungerar på ändamålsenlig nivå trots störningssituationerna.

Vid hanteringen av cyberstörningssituationerna följs laglighetsprincipen och gällande sektorindelning. Samma principer gällande hanteringen av en störningssituation följs både i normala förhållanden och i undantagsförhållanden. Myndigheternas ansvarfördelning och samarbetsorganens handlingsmodeller är de samma som under normala förhållanden. Situationerna leds med framförhållning och tillräckliga resurser tas genast i bruk. Den behöriga myndigheten leder den operativa verksamheten och de tvärsektoriella samarbetsorganen stöder den ansvariga myndigheten. Den part som leder verksamheten svarar också för kommunikationen. Övriga myndigheter, företag och organisationer deltar i verksamheten i den omfattning som förutsätts för att situationen ska kunna fås under kontroll. Utöver operativa åtgärder framhävs i samband med hanteringen av störningssituationerna att informationsutbytet mellan aktörerna måste säkerställas samt statsledningen informeras tillräckligt.

Hanteringen av störningssituationer organiseras och genomförs på det sätt som presenteras i Säkerhetsstrategi för samhället. I enlighet med den inleder den ansvariga myndigheten de åtgärder som hänför sig till hanteringen av en störningssituation, informerar övriga myndigheter och aktörer om situationen i den omfattning som behövs samt kopplar in i verksamheten andra aktörer som behövs för att störningssituationen ska kunna hanteras. Hanteringen av störningssituationer i cybersäkerheten kan delas in i fyra helheter. De är beredskap, formande av en lägesbild, avvärjning och återställande.

4. TRYGGANDET AV SAMHÄLLETS VITALA FUNKTIONER MOT CYBERHOT

4.1 Cyberlägesuppfattning och grundandet av ett cybersäkerhetscenter

De centrala aktörer som är med och tryggar samhällets vitala funktioner ges en bättre övergripande lägesuppfattning och lägesförståelse i fråga om cybersäkerheten. Ett cybersäkerhetscenter grundas och som stöd för det upprättas ett nätverk som samarbetar intensivt.

Statsledningens och myndigheternas beslutsfattande kräver tillräcklig lägesuppfattning och att de olika aktörerna till sitt förfogande har en tillförlitlig och tidsenlig lägesbild över cybersäkerheten gällande tillståndet för samhällets vitala funktioner och kritiska infrastruktur samt de störningar som riktas mot dem. En skalbar lägesbild i realtid över cybersäkerheten utformas genom teknisk övervakning och bevakning samt även genom en analys av iakttagelser, underrättelse och annan informationsinförskaffning och av erfarenheter som gjorts tidigare.

Ett nationellt cybersäkerhetscenter grundas för att betjäna myndigheter, näringsliv och andra aktörer när det gäller att upprätthålla och utveckla cybersäkerheten. De arrangemang som gäller tjänsterna och det kommande cybersäkerhetscentrets verksamhetssätt kommer man överens om som en del av den sammanställda verkställighetsplanen för cybersäkerhetsstrategin. Den viktigaste tjänsten är att utforma, upprätthålla och distribuera en cyberlägesbild i nära samarbete med det nätverk som stöder centret. Cybersäkerhetscentret bildas genom att den nuvarande funktionen CERT-FI samt funktionen GOV-CERT, som är under utveckling, slås samman och genom att de tilläggsresurser som behövs för centrets uppgifter reserveras. Cybersäkerhetscentret stöds av ett funktionellt nätverk, i vilket alla nödvändiga myndigheter, företag samt andra aktörer, med vilka man kommer överens separat, deltar. Deltagarna har till uppgift att bereda sig inför och reagera på kränkningar av cybersäkerheten.

När cybersäkerhetscentret grundas beaktas också andra projekt som går i samma riktning för att lägesbildsarrangemangen ska kunna strömlinjeformas och effektiveras. Statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen stakar ut en riktlinje för att upptäckts- och handlingsförmåga i fråga om informationssäkerheten ska kunna realiseras dygnet runt inom statsförvaltningen. Planeringen och genomförandet av denna funktion samordnas med verksamheten vid cybersäkerhetscentret. Dessutom beaktas vid utformandet av lägesbilden de gemensamma projekt som gäller utvecklandet av informationssäkerheten inom statsförvaltningen, såsom säkerhetsnätsprojektet (TUVE).

Cybersäkerhetscentrets uppgifter:

1. utforma och distribuera en lägesbild över cybersäkerheten
2. sammanställa och upprätthålla en riskanalys över cyberhot tillsammans med olika förvaltningsområden och aktörer
3. stöda behöriga myndigheter och aktörer inom den privata sektorn vid hanteringen av omfattande cyberstörningssituationer
4. effektivera samarbetet och stöda utvecklandet av kompetensen

Cybersäkerhetscentrets centralaste tjänster är att skapa, sammanställa, upprätthålla och till dem som behöver den distribuera en lägesbild över cybersäkerheten i samhället. Skapandet av en lägesbild förutsätter förmåga att samla in och analysera de uppgifter som behövs samt att åtgärda olika parters begäran om uppgifter. Den övergripande lägesbild som cybersäkerhetscentret producerar i samarbete med nätverket innehåller både en teknisk lägesbild och en bedömning av vilken total verkan cyberkränkningarna har på samhällets vitala funktioner. Cybersäkerhetscentret kommer med olika aktörer överens om de behov av uppgifter som hänför sig till deras verksamhet. Den information om sårbarheter som är riktad till underhållspersonalen utvecklas så att den blir allt mera automatisk. Däremot utvecklas den lägesbild som ska ges till myndigheter och beslutsfattare mera i riktning mot en bedömning av konsekvenserna för samhällets vitala funktioner.

Begränsningen av skadorna i en cyberstörningssituation ankommer på de myndigheter och företag som drabbas av störningen. Cybersäkerhetscentret kan i omfattande cyberstörningssituationer, som samtidigt drabbar flera myndigheter eller företag, stöda den myndighet som har ansvaret för ledningen. Cybersäkerhetscentret producerar en bedömning av cybersäkerhetens allmänna läge, som grundar sig på den övergripande lägesbild över cybersäkerheten som centret har utformat. Med hjälp av denna lägesöversikt är syftet att stöda förvaltningsområdena i deras egen cyberberedskap och planeringen av den.

Cybersäkerhetscentret bevakar cybersäkerhetshoten och analyserar samt gör prognoser om deras konsekvenser för Finland i samarbete med sina internationella samarbetspartner. Utgående från den bevakning som cybersäkerhetscentret har realiserat, hotmodellerna i Säkerhetsstrategin för samhället, cyberhotmodellen och nationell övervakningsinformation i realtid, varnar centret de företag och myndigheter som är viktiga med tanke på samhällets vitala funktioner om nya former av cyberhot som hotar Finland och om förhöjda nivåer på cyberhotet samt bistår på begäran när det gäller att bereda sig på dessa hot.

Statsledningens lägesbild produceras av statsrådets lägescentral. Ett intensivt samarbete mellan lägescentralen och cybersäkerhetscentret ökar den tvärsektoriella iakttagelse- och analysförmågan på basis av vilken man kan sammanställa en gemensam övergripande lägesbild. Med hjälp av gemensam lägesuppfattning och lägesförståelse kan man reagera på hot på ett ändamålsenligt sätt på politisk och operativ nivå.

För den resultatorienterade styrningen av cybersäkerhetscentret svarar kommunikationsministeriet. För att säkerställa den resultatorienterade styrningen av centret

grundas en separat cybersäkerhetsarbetsgrupp, där alla producenter och användare av cybersäkerhetscentrets tjänster samt de som ger centret resurser är representerade. I denna arbetsgrupp bör de personer som representerar parterna vara sakkunniga, som har en vidsträckt förståelse för beredskapen hos de parter de representerar, för cybersäkerhetens tillstånd och behov.

4.2 Tryggandet av näringslivets verksamhetsbetingelser och försörjningsberedskapen

Förmågan att upptäcka och avvärja cyberhot och cyberstörningssituationer som äventyrar en vital funktion samt att återhämta sig från dem som en del av kontinuitetshanteringen i näringslivet upprätthålls och utvecklas hos de företag och organisationer som är viktiga med tanke på tryggandet av samhällets vitala funktioner.

Syftet är att trygga att verksamheten hos de företag som är viktigast för samhället kan fortgå också medan cyberstörningar pågår. Planeringen av näringslivets kontinuitetshantering stöds, när den kan ha effekter på de vitala funktionerna och på skapandet av en säker cyberomgivning. Vid säkerställandet av näringslivets verksamhetsbetingelser har Försörjningsberedskapsorganisationen en viktig roll. Med beredskapsåtgärder säkerställs den infrastruktur som är nödvändig och fortgången av den produktion som är kritisk för ett fungerande samhälle i alla situationer.

Samhällets kritiska produktionsprocesser är mera beroende än tidigare av automationssystem. Automationssystemens utvecklingscykel är långsam och de sammanhänger med datatekniska lösningar som utvecklas snabbt. Vid kontinuitetshanteringen av kritisk infrastruktur måste man sörja för dataskyddet också i fråga om automationssystemen. Kontakterna mellan de apparater som fungerar i den fysiska världen och datanäten ska planeras så att en enkel cyberattack inte kan få en inrättning eller enhet att sluta fungera. Med tanke på samhällets kritiska funktioner är det centralt att man kan begränsa sårbarheten till ett minimum vid fjärranvändning och fjärravläsning av automationssystem, som t.ex. fastighetsautomationen.

För närvarande ägs och produceras största delen av den kritiska infrastrukturen och dess tjänster av den privata sektorn. Företagens förutsättningar att sörja för kontinuiteten i affärsverksamheten i situationer där det förekommer cyberhot förbättras och därmed utökas förtroendet för att de nyttigheter som de producerar kan fås också i fortsättningen.

Försörjningsberedskapsorganisationen är ett nätverk som upprätthåller och utvecklar den finska försörjningsberedskapen utgående från principen om partnerskap mellan den offentliga och den privata sektorn. Försörjningsberedskapen bygger på en fungerande marknad och en konkurrenskraftig ekonomi. Samhällets ekonomiska och tekniska basfunktioner bereder man sig på att upprätthålla med försörjningsberedskapsåtgärder, som

kompletterar verksamheten på marknadsvillkor, också under olika störningssituationer och undantagsförhållanden.

De åtgärder som tryggar fortgången av affärsverksamheten hos företagen och som är viktiga med tanke på den finska försörjningsberedskapen kartläggs och vidtas som en del av försörjningsberedskapsbeslutet och verkställandet av det. I en enskild organisation realiseras beredskapen inför cyberhot i praktiken oftast med den traditionella informationssäkerhetens metoder, medel och strukturer. Företagen bör utveckla sin förmåga att bedöma riskerna för cyberattacker, deras konsekvenser samt de åtgärder som behövs. Utvärderingsmetoder för och bedömningar av funktionssäkerheten i olika funktionskedjor och nätverk effektiveras samt vetskapen om nätverkens funktion och funktionssäkerhet utökas. För att det ska gå att trygga sig mot cyberhot förutsätts att aktörerna har samma slag av eller till varandra anpassad skyddspraxis. Försörjningsberedskapsorganisationen producerar verktyg för de företag som är kritiska med tanke på försörjningsberedskapen. Dessa verktyg gör det lättare för företagen att kartlägga risker med anknytning till verksamheten och utveckla kontinuitetshanteringen av verksamheten.

Tack vare sin goda cybersäkerhet kan Finland också vara ett attraktivt land att investera i. Den offentliga sektorns uppgift är att skapa en trygg och effektiv verksamhetsmiljö, men företagen själva ansvarar för utvecklandet av nya affärsverksamhetsmodeller, produkter och tjänster. Målet är att åstadkomma ett cybersäkerhetskluster på internationell nivå. Starka internationella förbindelser säkerställer en tillräcklig kunskapsbas och möjliggör en internationellt nätverkande affärsverksamhet.

I olika slag av nationella utvecklingsprojekt, som sköts tillsammans med bl.a. Tekes (Utvecklingscentralen för teknologi och innovationer) och TIVIT (informations- och kommunikationsindustrins forskning) bör tyngdpunkten förskjutas i riktning mot ny affärsverksamhet och forskning som klart stöder skyddandet av cyberomgivningen. Till exempel ett utvecklingslaboratorium för molntjänster, som inleder sin verksamhet år 2013, har som ett prioritetsområde att utveckla nya skyddstjänster för cyberomgivningen.

För säkerheten i företagsverksamheten sörjs det genom att olaglig ekonomisk underrättelse och cyberspionage bekämpas samt genom att kunskapskapitalriskerna minskas. För att förstärka den inhemska informationssäkerhetssektorn ökar statsförvaltningen sin satsning på forskning, produktutveckling och utbildning samt sina åtgärder för att internt utveckla förvaltningens ämbetsverk. Den nationella informationssäkerhetsmyndigheten uppnår ställning som en internationellt erkänd myndighet som beviljar internationella dataskyddscertifieringar.

4.3 Bekämpningen av cyberkriminalitet

Det sörjs för att polisen har effektiva förutsättningar att förebygga, avslöja och reda ut brott som riktar sig mot och utnyttjar cyberomgivningen.

Polisen måste kunna identifiera och bekämpa förberedelser för, finansiering och ledning av terroristiska brott och andra brott som pågår i datanätet och äventyrar samhällsordningen samt klara av att reda ut misstänkta brott.

Datanätskriminaliteten har blivit ett mycket täckande delområde av kriminaliteten och verkningarna av den inriktar sig såväl på stater och enskilda medborgare som också på affärsverksamhet. Datanätet är för de kriminella både ett förmånligare och i relationen mellan risk och nytta samt risk och skada en attraktivare miljö än tidigare att begå brott i, då målet är ekonomiskt eller terroristiskt. Sårbarheter i datanäten och datasystemen utnyttjas också av den traditionella organiserade kriminaliteten. Genom attacker i nätet kan man äventyra samhällets kritiska infrastruktur och genomföra terrordåd. Utöver terrorgärningar begås också traditionella brott, såsom bedrägerier, sexuellt utnyttjande av barn och industrispionage, allt oftare i cyberomgivningen.

Vid förebyggandet, utredningen och lämnandet till åtalsprövning av brott är i regel polisen behörig myndighet i samarbete med övriga lagövervakande myndigheter. Den kriminalitet som riktar sig mot datasystem är ofta gränsöverskridande och undersökningen av den förutsätter mången gång internationellt polisiärt och juridiskt samarbete. Juridiskt samarbete behövs bl.a. för att skaffa fram bevis eller överlåta den som är misstänkt för ett brott.

Det sörjs för att polisen har tillräcklig behörighet samt kunnande och tillräckliga rättigheter att få information för att kunna identifiera kriminella fenomen som anknyter till cyberomgivningen, förebygga datanätsbrott, avslöja de kriminella som är verksamma i cyberomgivningen och reda ut dessa brott. Likaså säkerställs det att polisen har tillräcklig behörighet samt kunnande och tillräckliga rättigheter att få information för att kunna identifiera och bekämpa förberedelser inför, finansiering och ledning av terroristiska och andra brott som äventyrar samhällsordningen samt den propagandainformering och åsiktsbildning som anknyter till dem samt förmåga att reda ut misstänkta brott.

För polisen skapas skicklighet, förmåga och tillräckliga juridiska möjligheter att utbyta information och samarbeta med olika lagövervakande myndigheter för att förebygga, avslöja och reda ut brott. Polisen satsar på bekämpningen av datanätskriminalitet som en del av bekämpningen av den organiserade kriminaliteten. Polisen utvecklar och förstärker de nationella metoderna för att bekämpa datanätskriminaliteten, bl.a. genom att utöka samarbetet mellan olika polisinrättningar och snabb beredskap hos dem.

Centralkriminalpolisen upprätthåller i enlighet med Polisstyrelsens föreskrifter en lägesbild över internationell och organiserad kriminalitet. Utöver detta upprätthåller centralkriminalpolisen en lägesbild över den totala kriminaliteten i samarbete

med den lokala polisen. Vid utformandet av lägesbilden utnyttjas PTG –brottsunderrättelse- och brottsanalyscentret. Skyddspolisen upprätthåller en lägesbild över sitt verksamhetsområde.

Polisen bör ha en kunnig och motiverad personal som sköter den taktiska förundersökningen av krävande datanätsbrott samt behandlingen och analyseringen av digitalt bevismaterial på ett rättssäkert sätt. Det kunnande hos myndigheter, åklagare och domare som behövs vid bekämpningen och undersökningen av cyberkriminalitet förbättras genom att den utbildning som behövs på området utvecklas.

4.4 Cyberförsvarsförmågan

Försvarsmakten skapar en övergripande cyberförsvarsförmåga i sina lagstadgade uppgifter.

Cyberförsvarsförmågan består av kapaciteterna underrättelse, påverkan och skyddande. Målet är att kapaciteten ska dimensioneras så att den så effektivt som möjligt stöder försvarsmaktens verksamhet för att trygga den territoriella integriteten och försvara landet. Cyberförsvaret genomförs som en helhet, som innehåller försvarsmaktens, övriga myndigheters och samhällets övriga kapaciteter.

En trovärdig kapacitet byggs upp i samarbete med andra myndigheter, företag och universitet. Under normala tider utvecklas kapaciteten genom nätverkande, utbyte av information, gemensamma projekt samt genom att man deltar i nationella och internationella arbetsgrupper och övningar. Verksamhetens baslösningar ändras inte i undantagsförhållanden eller olika störningssituationer. På cyberhot bereder man sig och hoten hanterar man genom att olika slags skydds- och påverkansmetoder utvecklas och upprätthålls och dessutom skapas den förmåga som behövs för att man ska kunna återhämta sig från cyberattacker.

Cyberpåverkan kan användas som medel för politisk och ekonomisk påtryckning samt i en allvarlig kris som en påverkansmetod jämsides med andra traditionella militära maktmedel. Försvarsmakten skyddar sina system och nät samt skapar och upprätthåller förmåga till underrättelse och påverkan i cyberomgivningen. Utvecklandet av kapaciteterna baserar sig på utarbetade kapacitetskrav och till buds stående resurser.

Uppkomsten av cyberhot måste man kunna upptäcka i tid, och fenomen och händelser i cybervärlden måste man kunna följa i realtid. Detta förutsätter att en cyberlägesbild utformas för att en tidig förvarning och tid att förbereda sig ska kunna åstadkommas samt påverkan kunna genomföras. När försvarsmaktens cyberlägesbild utformas verkar man i samarbete med det kommande nationella cybersäkerhetscentret.

Med underrättelsekapaciteterna produceras information om sammansättningen av och sårbarheter i systemen och näten hos aktörerna i cyberomgivningen samt en bedömning av aktörernas förmåga att genomföra cyberoperationer. Målet med cyberunderrät-

telsen är att skapa den lägesuppfattning och underrättelseinformation som skyddande och påverkan förutsätter.

Cyberförsvarets kapacitet utvecklas på nationell nivå i samarbete med övriga myndigheter, näringslivet, vetenskapssamfundet och övriga aktörer. Samordningen av den nationella verksamheten, bildandet av en gemensam riksomfattande lägesbild samt upprätthållandet av förutsättningarna för samverkan kräver regelbundet informationsutbyte mellan de olika aktörerna.

Det internationella samarbete som sammanhänger med cyberförsvaret intensifieras fortsättningsvis med centrala aktörer. Samverkan baserar sig på bilaterala fördrag samt multinationellt samarbete. Målet med den internationella samverkan är att göra det möjligt att regelbundet utbyta information mellan olika aktörer i synnerhet för att utveckla den egna kapaciteten och förenhetliga verksamhetsmodellerna.

Försvarsmakten ger övriga myndigheter handräckning i störningssituationer som orsakas av cyberhot. Vid behov får försvarsmakten stöd av övriga myndigheter för realiseringen av sina cyberförsvarsuppgifter. Försvarsmaktens förmåga att stöda övriga myndigheter i cyberstörningssituationer utvecklas.

De verksamhetsmöjligheter och befogenheter som sammanhänger med cyberkapaciteten förutsätter en grundlig fortsatt granskning. I detta arbete bör det granskas hur lämplig och tillräcklig gällande internationell rätt och nationell reglering är samt vilka behov av eventuella författningsändringar cyberförsvarsförmågan förutsätter.

Försvarsmakten ges befogenheter, kunnande och tillräckliga rättigheter att få information som behövs för att försvars-, handräcknings-, territorieövervaknings- och krishanteringsuppdragen ska kunna fullgöras.

4.5 Internationellt samarbete

Den nationella cybersäkerheten förstärks genom aktivt och effektivt deltagande i verksamheten vid de internationella organisationer och samarbetsforum som är viktiga med tanke på cybersäkerheten.

I cybersäkerhetsverksamheten bedrivs på nationell nivå aktiv samverkan mellan olika aktörer med målet att åstadkomma en delad lägesuppfattning, effektiv hantering av störningar och avvärjning av hot. Till följd av att cybersäkerheten är så vidsträckt framhävs betydelsen av internationellt samarbete mera än tidigare. Målet med den internationella samverkan är att utbyta information och erfarenheter samt att lära sig av bästa praxis för att nivån på den nationella cybersäkerheten ska kunna höjas.

Internationellt samarbete i fråga om cybersäkerhet bedrivs på många nivåer och i många forum, i Norden, Europarådet, Europeiska unionen och mellan internationella organisationer, såsom NATO, OSSE och FN. Cyberhoten överskrider de nationella gränserna och därför är det nödvändigt att bedriva internationellt samarbete i olika interna-

tionella forum. Samarbetet ger möjlighet att utbyta information och erfarenheter samt att lära sig av bästa praxis. Dessutom ger verksamheten grunder för att utveckla den nationella cybersäkerheten som en del av den globala cybersäkerheten samt att öka cyberförsvarets kompatibilitet och interoperabilitet.

Samarbetet fördelar sig dels på verksamhet med olika organisationer och dels på bilateralt samarbete. I fråga om organisationerna är EU och NATO de centralaste aktörerna inom cybersäkerheten i Europa. Det samarbete som ska utvecklas tillsammans med dem är till sin art i första hand utbyte av information om läget, samarbete vid utvecklandet av gemensamma kapaciteter samt utbildning och övningar.

Det traditionella nordiska samarbetet ger också en möjlighet att främja cybersäkerheten. Vid ett utrikesministermöte år 2009 kom man överens om att intensifiera cybersäkerhetssamarbetet mellan de nordiska länderna. I enlighet med rekommendationerna från den sakkunnigarbetsgrupp som tillsattes, bereds just nu ett nordiskt samarbetsnätverk mellan myndigheterna och ett säkert datanät som stöder detta.

Europarådets konvention om it-relaterad brottslighet (den s.k. Budapestkonventionen) från år 2001 utgör grunden för utvecklandet av bekämpningen av all cyberkriminalitet. Också Europeiska unionen är ett mycket viktigt forum för Finland när cybersäkerheten utvecklas. EU bereder just nu en egen strategi över cybersäkerheten. För närvarande har EU i sina anvisningar och direktiv koncentrerat sig på bekämpningen av datanätskriminalitet, skydd av kritisk informationsinfrastruktur samt på arbetet på lagstiftning som gäller elektronisk kommunikation, dataskydd och datasekretess.

Finland fortgår med sitt nära samarbete med europeiska samarbetsorganisationer, såsom Europeiska byrån för nät- och informationssäkerhet (European Network and Information Security Agency, ENISA), Europeiska unionens polisbyrå (Europol), Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Body of European Regulators for Electronic Communications, BEREC), EU-forumet för medlemsstaterna för skydd av kritisk infrastruktur (European Forum for Member States, EFMS) samt Det offentligt-privata EU-partnerskapet för motståndskraft (European Public-Private Partnership for resilience, EP3R).

När cyberförsvaret utvecklas fortgår samarbetet med EU:s militära stab (EUMS), Europeiska försvarsbyrån (EDA) och NATO. NATO kommer att samarbeta med partnerskapsländerna för att bemöta nya säkerhetsutmaningar, stödja NATO-ledda operationer och förbättra lägesuppfattningen.

Inom ramen för Organisationen för säkerhet och samarbete i Europa OSSE försöker man utveckla åtgärder som ökar förtroendet för att förhindra cyberkonflikter på ett sådant sätt att öppenheten, samarbetet och stabiliteten utökas. Målet är att detta arbete ska komplettera arbetet i andra internationella organisationer och det grundar sig på OSSEs uppfattning om en övergripande säkerhet.

I slutdokumenten från FN:s toppmöte om informationssamhället (WSIS, World Summit on the Information Society) förbinder sig medlemsländerna att utöka förtroen-

det för och säkerheten vid användningen av ICT. Finland deltar i den diskussion om cybersäkerheten som förs i FN-organen och stöder i enlighet med WSIS-åtagandena förstärkandet av samarbetet mellan alla aktörer i frågor som anknyter till säkerheten. Den internationella telekommunikationsunionen ITU främjar också detta mål med sitt initiativ Global Cybersecurity Agenda.

Det arbete som görs inom ramen för Organisationen för ekonomiskt samarbete och utveckling OECD strävar efter att utveckla eller harmonisera medlemsländernas politik på de olika ekonomi- och samhällslivssektorerna. Finland deltar i samarbetet inom OECD i de grupper som gäller informationssäkerhet och integritetsskydd. OECD är en sakkunnigorganisation som stöder det ekonomiska och samhällspolitiska beslutsfattandet i medlemsländerna. OECD har utarbetat rekommendationer om säkerhetsprinciper för datasystemen och datanäten samt gjort en jämförande undersökning av medlemsländernas nationella strategier för cybersäkerhet.

4.6 Utvecklandet av forskning och kunnande samt övningsverksamhet

Cyberkunnandet och cyberförståelsen förbättras hos alla aktörer i samhället.

Målet är att förbättra myndigheternas, näringslivets och medborgarnas förståelse för, kunnande i och färdigheter vad gäller cybersäkerhetens betydelse för ett fungerande samhälle och skapa ett starkt nationellt cyberkompetenskluster. Forskningen i cybersäkerheten utvecklas som en del av den nationella spetsforskningen och en strategisk koncentration av spetskompetens i cybersäkerhet skapas som en del av redan befintliga strukturer. Målet med övningsverksamheten är att förbättra deltagarnas möjligheter att upptäcka sårbarheter i verksamheten och systemen, utveckla kapaciteterna och utbilda personalen. Sektorernas beredskap att agera i situationer där störningar förekommer i vitala funktioner övas regelbundet.

Det kostnadseffektivaste sättet att öka den nationella cybersäkerheten är att förbättra kunnandet. Utökandet av myndigheternas, näringslivets och medborgarnas kännedom om hoten och riskerna i cyberomgivningen förbättrar allas kunnande när det gäller att vidta cybersäkerhetsåtgärder. Med spetsforskningen i branschen skapas ett fundament för utvecklandet av både kunnandet och cybersäkerhetssystemen.

I det finska utbildningssystemet sörjs det för att en så hög kompetensnivå bevaras och utvecklas att man genom att utnyttja den kan trygga och utveckla säkerheten för samhällets vitala funktioner i cyberomgivningen. Studier i baskunskaper och färdigheter i fråga om cybersäkerheten bör ingå på alla utbildningsnivåer. Kraven gällande innehållet i undervisningen om cybersäkerheten bör inbegripas i den allmänbildande grundläggande undervisningen (grundskolan), i yrkesutbildningen och i gymnasieutbildningen samt i högskoleutbildningen.

Förutsättningarna för grundforskning och tillämpad forskning i och innovativ verksamhet gällande cybersäkerheten förstärks vid universiteten och förutsättningarna för

produktutvecklingsarbetet förstärks vid yrkeshögskolorna. Nivån på forskningen i cybersäkerhet höjs och forskningsbetingelserna tryggas för att man kontinuerligt ska kunna producera högklassiga nya innovationer och vetenskapliga genombrott inom både grundforskningen och den tillämpade forskningen. Till exempel utvecklandet av kryptokunnandet stöds så att finska produkter och tjänster kan fås för både inhemsk och internationell användning.

I samband med det redan existerande ICT-SHOK (TIVIT) grundas en tvärvetenskaplig strategisk koncentration av spetskompetens i fråga om cybersäkerhet. Denna koncentration ska erbjuda forskningsenheter på toppnivå och de företag som utnyttjar forskningsrönen ett effektivt sätt att bedriva intensivt och långfristigt samarbete. I koncentrationen realiseras en forskningsstrategi som är flervetenskaplig och utgår från tillämpningar och den fastslås gemensamt av företag, universitet och forskningsinstitut. Resultaten av forskningsstrategin betjänar genomförandet av den nationella strategin för cybersäkerheten och utvecklandet av internationell spetskompetens. Med dessa åtgärder stöds uppkomsten av en ny lönande internationell cybersäkerhetsaffärsverksamhet.

Med tanke på att affärsverksamheter kontinuerligt ska kunna utvecklas är det nödvändigt att sörja för att den högklassiga kompetensen kvarstår i landet. Genom att kompetensen säkerställs möjliggörs vår nationella förmåga att utnyttja cyberomgivningen. Utgående från näringslivets behov bör minst 100 personer omskolas för sektorn under år 2013 i samarbete med 1–2 läroinrättningar. Övergångsutbildningen fortgår på samma nivå under flera år. Så snabbt som möjligt läggs cyber/dataskyddskurser till på schemat i högskolor och yrkeshögskolor. Nybörjarplatserna inom dataskyddssektorn vid de läroinrättningar som ger utbildning inom sektorn utökas liksom också antalet biämneskurser i cybersäkerhet. En professur som koncentrerar sig på cybersäkerhet inrättas omedelbart och med en längre tidtabell utökas antalet professurer som anknyter till cybersäkerheten.

De iakttagelser och erfarenheter som fås vid cyberövningar ger konkret information om hur samhällets vitala funktioner kan tryggas och om den samverkan som behövs. Dessutom fås information om de utvecklingsbehov som de strategiska uppgifterna vid förvaltningsområdena och organisationerna föranleder samt om situationen som helhet vad gäller samhällets beredskap och krisledningsfärdigheter. Genom övningarna testas cybersäkerhetsstrategins principer och handlingsmodeller samt mäts verkställandet av strategin.

Beredskapen på undantagsförhållanden och allvarliga störningssituationer under normala förhållanden bör övas regelbundet. Detta gör det möjligt att bedöma den utveckling av cybersäkerheten som har uppnåtts i Finland och skapa åtgärder som kontinuerligt förbättrar verksamheten. Hoten mot cybersäkerheten förändras med en mycket snabb cykel, vilket gör att all nationell och internationell övningsverksamhet bör vara fortgående och väl organiserad så att verksamheten effektivt stöder den nationella cybersäkerheten.

En framgångsrik cyberövningsverksamhet förutsätter planenlighet och ett klart ledningsansvar. Beredningen och genomförandet av vidsträckta riksomfattande cyberövningar samordnas i enlighet med de principer som har fastslagits i Säkerhetsstrategin för

samhället. Realiserandet av den nationella cybersäkerheten förutsätter en nära samverkan mellan den offentliga förvaltningen och den privata sektorn. För att samhällets totala beredskap ska kunna utvecklas tas också de företag och medborgarorganisationer som är viktiga med tanke på samhällets vitala funktioner med i övningsverksamheten.

Den offentliga förvaltningens och den privata sektorns förmåga att hantera cyberstörningssituationer övas i riksomfattande cyberövningar. Vid dessa övningar testas beredskapen på störningssituationer som anknyter till hotmodellerna i cybersäkerhetsstrategin samt hur väl ledningsarrangemangen och samarbetsarrangemangen fungerar. Övningarnas teman binds till aktuella utmaningar som orsakas av förändringar i cybersäkerhetsomgivningen.

Deltagandet i internationella övningar på flera olika nivåer av verksamheten stöder på ett betydande sätt det nationella utvecklandet av cybersäkerheten, kompetensen i branschen och utvecklandet av verksamhetssätten samt skapandet av internationellt myndighetssamarbete och kontaktnätverk för sakkunniga. Finland bör sträva efter att aktivt påverka strukturen på och genomförandet av övningarna redan i planeringsfasen så att vi vid övningarna kan utveckla det nationella kunnandet och testa vår nationella cyberomgivnings starka sidor och sårbarheter.

5. DET REGELVERK SOM GÄLLER CYBERSÄKERHETEN

5.1 Genom nationell lagstiftning säkerställs förutsättningarna för att effektivt realisera cybersäkerheten.

I cybersäkerheten är det juridiskt fråga om ett nytt fenomen. För cyberhoten är det symtomatiskt att de överskrider staternas gränser. Aktörerna bakom cyberattacker kan variera och det är en utmaning att identifiera dem. Cyberattackernas tekniker är av många slag och snabbt föränderliga samt stadda i utveckling. Cybersäkerheten gäller alla livsområden, förvaltningsområden och samhällets basfunktioner. De grundläggande fri- och rättigheterna och de mänskliga rättigheterna garanterar rätten till integritet och till skydd för förtroliga meddelanden. Vilket juridiskt regelverk som ska tillämpas i en situation med ett cyberhot fastslås enligt cyberhotets ursprung och verksamhetens art.

5.2 Det regelverk som anknyter till cybersäkerheten på internationell och nationell nivå

Förenta nationerna (FN) fastslog på 1990-talet att missbruk av datateknik är ett gränsöverskridande brott. FN har offentliggjort resolutioner i striden mot missbruk av informationsteknologi och i skyddandet av kritisk informationsinfrastruktur.

Inom Europeiska unionen har det upprättats konventioner, rambeslut, direktiv, förslag och meddelanden som behandlar datanätsbrottslighet och bekämpning av sådan, samarbete vid bekämpningen av attacker mot datasystem samt skyddandet av kritisk infrastruktur och informationsinfrastruktur.

Något enhetligt fördrag som skulle täcka alla situationer med cyberhot och binda staterna finns inte. I den internationella juridiken har situationer som utgör cyberhot behandlats splittrat och ur olika synvinklar. Någon enhällighet har inte heller uppnåtts t.ex. i fråga om vad som avses med en cyberattack, ett cyberförsvar eller en cyberkonflikt. På internationell nivå har den juridiska debatten om sakhelheten blivit livligare under de senaste åren. Detta torde komma att leda till att juridiska tolkningar, som gäller bedömningarna av situationer med cyberhot, skapas hos olika parter stater emellan eller i internationella gemenskaper. Det kan antas att dessa tolkningar inte binder staterna juridiskt, men att de visar på de mål som de stater som är med i arrangemangen är beredda att sträva mot.

Användningen av maktmedel i mellanstatliga relationer regleras av FN:s stadga. Användningen av maktmedel är förbjuden med undantag av självförsvar i situationer med ett väpnat angrepp samt deltagande i väpnade sanktioner som verkställs med mandat av säkerhetsrådet. I det internationella samfundet pågår en diskussion och utformandet av tolkningar om huruvida cyberattacker i någon situation kan överstiga tröskeln för ett sådant väpnat angrepp som avses i FN:s stadga på ett sådant sätt att staten har rätt att vidta väpnade motåtgärder. Av suveränitet följer ansvar. Staten måste se till att dess territorium inte används för attacker på en annan stat. Den måste således på sitt eget territorium sträva efter att förhindra också privata parters attacker som riktar sig ut över dess gränser. För cyberoperationer finns inget eget regelverk för användningen av maktmedel.

I den nationella lagstiftningen finns ingen enhetlig reglering gällande cyberhot. Det regelverk som reglerar verksamheten i datanäten är splittrat och närmar sig situationer med cyberhot ur olika synvinklar. Nationellt fastställer de olika förvaltningsområdena cyberhoten ur sin egen synvinkel och befogenheterna är förvaltningsområdesvisa, fastän cyberverksamheten till följd av sin art i allmänhet överskrider förvaltningsområdenas gränser. Beroende på cyberhotets ursprung och verksamhetens art kan samma verksamhet bedömas som en enskild straffrättslig gärning, ett mera vidsträckt terroristbrott eller med tanke på relationerna stater emellan och det militära försvaret. Detta försvårar den juridiska bedömningen av en situation med cyberhot och utformandet av en enhetlig nationell juridisk tolkning av situationen.

På nationell nivå föreskriver vår grundlag att det allmänna ska se till att de grundläggande fri- och rättigheterna och de mänskliga rättigheterna tillgodoses i landet. De grundläggande fri- och rättigheterna ska också skyddas i datanäten. Utökandet av cybersäkerheten kan effektivera t.ex. skyddet för integritet och egendom hos dem som använder nätet. Fungerande datanätsförbindelser kan anses främja också realiserandet av medborgarnas yttrandefrihet. En mera exakt reglering som anknyter till cybersäkerhe-

ten finns i 34 kapitlet i strafflagen, samt i territorialövervakningslagen, beredskapslagen, lagen om försvarstillstånd och lagen om försvarsmakten samt i kommunikationsmarknadslagen och lagen om dataskydd vid elektronisk kommunikation.

Myndigheternas beredskapsskyldighet för att kunna sörja väl för sina uppgifter i alla situationer, vilken avses i beredskapslagen, omfattar också utvecklandet av cyberkapaciteter. En central förutsättning för att befogenheterna enligt beredskapslagen ska få tas i bruk och användas är att sådana undantagsförhållanden som det föreskrivs om i lagen råder. Enligt motiveringarna till lagen kan det vid ett så allvarligt angrepp att det kan jämställas med ett väpnat angrepp som ingår i definitionen på undantagsförhållande, vara fråga också om annat än ett angrepp med traditionella vapen. Angreppet kan t.ex. vara en attack riktad mot landets informationssystem. Ett angrepp kan också syfta på ett angrepp av en icke-statlig aktör, om angreppet är så välorganiserat och omfattande att det är jämförbart med ett angrepp som genomförs av en stat.

5.2 Utvecklandet av lagstiftningen

I sin internationella verksamhet stöder och deltar Finland i utformandet av tolkningar som görs inom ramen för internationell rätt. Syftet med dessa tolkningar är att staka ut riktlinjer för att de rättsliga principer som iakttas i staterna ska vara så enhetliga som möjligt. Samtidigt innebär detta att det inte är tillräckligt att enbart den finska nationella lagstiftningen utvecklas så att den täcker situationer med cyberhot. Finland deltar aktivt i samverkan mellan olika aktörer, där de centrala målen är ett öppet informationsutbyte, att skapa ett gemensamt juridiskt regelverk samt komma överens om ansvarsfördelningen mellan olika aktörer. På detta sätt kan man t.ex. begränsa de situationer där skillnader i de nationella lagarna ger kriminella cyberaktörer möjlighet att förlägga sin verksamhet till sådana stater som passar dem.

Den nationella lagstiftningen bör granskas på ett sådant sätt att den internationella rätt och EU-lagstiftning som hänför sig till cybersäkerheten beaktas. I detta arbete bör de olika förvaltningsområdenas reglering i anknytning till cybersäkerheten, hur aktuell och tillräcklig den är redas ut samt eventuella behov att ändra lagstiftningen kartläggas. Utgångspunkten är att de befogenheter som förutsätts för hantering av cyberstörningssituationer, som äventyrar och skadar samhället, ingår i myndigheternas normala befogenheter. Grundlagen föreskriver att om det allmännas grunder och befogenheter ska föreskrivas i lag.

Lagstiftningen bör utvecklas så att den beaktar de snabbt föränderliga fenomenen i cyberomgivningen och ger möjlighet för behöriga myndigheter inom de olika områdena att genomföra de uppgifter som bestäms för dem. Genom dessa uppgifter tryggas statens självständighet, befolkningens levnadsmöjligheter och säkerhet mot cyberhot som riktar sig mot samhällets vitala funktioner. Cybersäkerheten ska granskas utan att den avskiljs från övriga element som anknyter till säkerheten. Centralt med tanke på att samhället ska

fungera är att i lagstiftningen hitta balans mellan myndigheternas och näringslivets lägesuppfattning, ansvar och verksamhetssätt. I denna granskning ska det också beaktas att Finlands internationella konkurrenskraft tryggas. Den stabila situation gällande cybersäkerheten som råder i landet bidrar till attraktiva verksamhetsbetingelser för näringslivet.

För att de cyberhot som äventyrar statens säkerhet ska kunna avvärjas tas eventuella hinder och begränsningar i lagstiftningen eller sådana som orsakas av förpliktelser i internationella fördrag upp till granskning. Också de förpliktelser granskas som gäller hanteringen av information och som medför olägenheter med tanke på att myndigheter och andra aktörer ska kunna få, överlåta och utbyta sådan information som behövs för att cyberhot ska kunna avvärjas effektivt. I en granskning som gäller insamling och annan hantering av information bedöms dessutom om det finns skäl att för de ansvariga myndigheterna skapa bättre möjligheter än dagens att på förhand samla in, sammanställa och få information om cyberhot och om dem som orsakar sådana. Detta görs på ett sådant sätt att man samtidigt ägnar uppmärksamhet åt integritetsskyddet och skyddet för förtroliga meddelanden, vilka är grundläggande fri- och rättigheter.

För polisverksamheten är det fråga om att få befogenheter i synnerhet för underrättelse och undersökning för att cyberbrottslighet ska kunna förebyggas, upptäckas och avvärjas. För försvarsmaktens del bör de befogenhetsbestämmelser som gäller metoder för cyberpåverkan och cyberunderrättelse klargöras och förbättras i samband med att lagstiftningen revideras. Om befogenheterna eventuellt utvidgas bör i synnerhet de mänskliga rättigheterna och de grundläggande fri- och rättigheterna beaktas och detta gäller också deras konsekvenser för befogenhetsfrågorna t.ex. när rättigheterna att bedriva underrättelse utökas.

6. VERKSTÄLLANDET AV STRATEGIN FÖR CYBERSÄKERHETEN

6.1 Principerna för verkställandet av strategin

Uppgifter och tjänstemodeller som gäller cybersäkerheten samt gemensamma grunder för hanteringen av de krav som cybersäkerheten ställer fastställs för myndigheterna och näringslivets aktörer.

Cybersäkerheten i samhället och tryggandet av de vitala funktionerna grundar sig på ministeriernas strategiska uppgifter och på ett försörjningsberedskapssystem som fungerar i alla säkerhetssituationer. Varje förvaltningsområde svarar för att en cyberriskanalys görs. Med hjälp av analysprocessen blir man medveten om sårbarheterna och kan göra en mognadsanalys. Som resultat av processen får man verkställighetsprogram för varje förvaltningsområde med vilka de behov som påvisats kan tillgodoses. I en närmare planering fastställs de mätare och andra åtgärder som behövs för att cybersäkerheten ska bli bättre. Aktörernas planer och arrangemang gällande beredskapen ska granskas regelbundet och alltid när det sker väsentliga förändringar i samhället eller i säkerhetsmiljön. Den nya Säkerhetskommitté som ska grundas kommer att följa med och sammanjämka verkställandet och utvecklandet av strategin.

Varje aktör i eller sektor av samhället har också sina egna separata cybersäkerhetsuppgifter. Specialuppgifterna fördjupar ur ett cybersäkerhetsperspektiv de strategiska uppgifter, försörjningsberedskapsuppgifter och sektorvisa uppgifter som fastslås i Säkerhetsstrategin för samhället.

För att cybersäkerheten i samhället ska kunna upprätthållas förutsätts korrekt information om beredskapen och handlingsförmågan hos förvaltningsområdena och näringslivet samt om hela samhällets kristålighet och krisberedskap. Bevakningen av hur strategin verkställs bör möjliggöra underhålls- och utvecklingsåtgärder i rätt tid och rätt riktning. Genom bevakningen produceras tidsenlig information för statsledningen om huruvida resurserna har riktats rätt i enlighet med målen i cybersäkerhetsstrategin.

För att cybersäkerheten ska kunna realiseras förutsätts ett konsekvent verkställande av strategins principer också på regional och lokal nivå. Detta förutsätter tillräckligt samarbete mellan olika aktörer och att bästa praxis utnyttjas.

Den gemensamma bevakningen och utvecklingen av verkställandet av strategin samordnas av den kommande Säkerhetskommittén. För statsrådet upprättas en årlig rapport över läget i fråga om verkställandet av strategin.

6.2 De åtgärder som verkställigheten förutsätter

Ministerierna bevakar hur de uppgifter som anknyter till cybersäkerheten samt försörjningsberedskapsarrangemangen inom deras verksamhetsområden realiseras och hur de utvecklas. Bevakningen genomförs som en del av etablerad praxis inom förvaltningsområdena.

Cybersäkerhetscentret producerar i samarbete med sitt nätverk regelbundet för olika myndigheter en rapport om vad som inträffat i cybersäkerhetsomgivningen. Centret utarbetar årligen i samarbete med nätverket en rapport där åtminstone följande helheter behandlas:

- hur inträffade störningssituationer har hanterats och vilka erfarenheter man fått av dem, analyser som gjorts och vilka de ekonomiska konsekvenserna har varit för samhällets vitala funktioner,
- bedömningar av hur beredskapsarrangemangen fungerar och behoven att utveckla dem,
- erfarenheter av förvaltningsområdenas, statsrådets och riksomfattande cyberberedskapsövningar,
- hur verksamheten och kompetensen har utvecklats samt resurstilldelningen.

Vid hanteringen av cyberstörningssituationer är det viktigt att de åtgärder som inletts för att få kontroll över en störningssituation registreras och analyseras så täckande som möjligt. Också analyseringen av s.k. ”nära ögat” –situationer ska fogas till denna bevakning, i synnerhet för att förebygga hot och risker. De lärdomar man kan dra av situationerna och de åtgärder de ger anledning till behandlas i olika samarbetsorgan för att man ska kunna försäkra sig om att bästa praxis utnyttjas.

De upptäckter och erfarenheter som erhålls vid cyberövningar ger konkret information om tryggandet av samhällets vitala funktioner och om den samverkan som behövs. Dessutom får man information om de utvecklingsbehov som förvaltningsområdenas och organisationernas strategiska uppgifter kräver samt om den totala situationen i fråga om samhällets beredskap och krisledningsfärdigheter. Genom övningarna testas cybersäkerhetsstrategins principer och handlingsmodeller samt bedöms hur strategin har verkställts.

Bevakningen av verkställandet av strategin ger också grunder och krav för cybersäkerhetsforskningen och det nationella samarbetet i fråga om den. Nationell och internationell säkerhetsforskning bedrivs och samarbetsformerna utvecklas i enlighet med principerna i den nationella strategin för säkerhetsforskning (2009). Forskning som stöder cybersäkerhetsstrategin produceras i olika forskningsenheter och forskningsinstitut samt i forskningsprogram vid universitet och högskolor.

Upprätthållandet och utvecklandet av cyberstrategin baserar sig på en process med kontinuerligt utvecklande. Cybersäkerhetsstrategin kommer att behandlas i Säkerhetskommittén årligen. Genom detta säkerställs att strategin är tidsenlig och att åtgärderna framskrider. Utgående från den bedömning och analys som gjorts i processen görs eventuella uppdateringar av strategin och verkställighetsprogrammet. De centrala delarna av cybersäkerhetsstrategin inbegrips i säkerhetsstrategin för samhället när den uppdateras nästa gång.

6.3 Resurstilldelning för åtgärderna

Ministerierna, ämbetsverken och inrättningarna inbegriper i sina verksamhets- och ekonomiplaner de resurser som verkställandet av cybersäkerhetsstrategin förutsätter. Riksdagen ger ministerierna anslagsramar, och i dem inbegrips de resurser som cybersäkerhetsåtgärderna förutsätter. Ministerierna planerar sina resursbehov som en del av verkställighetsprogrammen. Företagen beaktar de åtgärder som cybersäkerheten kräver när de fattar beslut om budget och resurstilldelning.

De aktörer som nämns ovan samarbetar med det cybersäkerhetscenter som ska grundas och bildar ett tätt nätverk. Centret kommer att utnyttja det kunnande som finns i nätverket, vilket också påverkar dess egen resurstilldelning. För grundandet av ett cybersäkerhetscenter och för dess verksamhet anvisas ett särskilt tilläggsanslag, vars storlek planeras som en del av den gemensamma verkställighetsplanen. Cybersäkerhetscentret skapas så att det har handlingsförmåga 24/7, vilket enligt en preliminär uppskattning förutsätter cirka tio årsverken och tilläggsresurser på åtminstone en miljon euro.

6.4 Verkställighetsprogrammet och mätning av resultatet

Verkställandet av strategin övervakas och utfallet följs upp.

Verkställandet av fas 1 av cybersäkerhetsstrategin genomförs åren 2013–2015. Under denna tid utarbetas detaljerade beredskaps- och utvecklingsplaner för cybersäkerheten för att regeringsprogrammets mål, att Finland ska vara ett av de ledande länderna när det gäller att utveckla cybersäkerheten, ska nås år 2016. Från år 2016 framåt genomförs cybersäkerhetsstrategin i enlighet med principen om kontinuerlig förbättring. Den budgetering som cybersäkerheten förutsätter genomförs per förvaltningsområde i enlighet med gällande verksamhetsmodell.

Huvudpunkterna i verkställighetsprogrammet är att grunda ett cybersäkerhetscenter, att vidta åtgärder för att ministeriernas strategiska mål ska kunna nås och att göra de ändringar av författningarna som behövs. Som en del av verkställighetsprogrammet utvecklas en mognadsmodell för cybersäkerheten med vilken verksamhetens nivå och utveckling kan mätas.

BILAGA

PROCESSEN MED KONTINUERLIG UTVECKLING AV CYBERSÄKERHETSSTRATEGIN

Målet med den nationella cyberstrategiprocessen är att åstadkomma en verksamhetssättsmodell för kontinuerligt förbättrande, varvid cybersäkerhetsåtgärder i framtiden vidtas effektivare och med större verkan. Strategiprocessen framträder på flera nivåer och den innehåller olika faser. Målet är att skapa en kontinuerlig strategiprocess där processens delar upprepas regelbundet och en kontinuerlig utveckling av verksamheten skapas.

Cybersäkerhetsprocessen (figur 1 i bilagan) innehåller fem faser:

Analysfasen

I strategins analysfas fastslås vår egen ställning, m.a.o. var vi står i förhållande till omgivningen och dess olika element. I cyberstrategin innebär detta att cyberhotomgivningen analyseras och att sårbarheter i samhällets vitala funktioner identifieras samt att de risker som denna helhet medför bedöms. Dessutom bedöms våra egna kapaciteter och brister i dem.

Vid analyseringen av omgivningen identifieras fenomen i cyberomgivningen och görs de definitioner som behövs för strategin samt identifieras befintliga nationella cybersäkerhetsprojekt och de större och mindre projekt som tangerar dem.

Med benchmarking-metoden skaffas information om andra länders cybersäkerhetsstrategier och identifieras i dem den bästa praxis som passar en själv.

Som slutresultat av analysfasen uppkommer en syn som ger vår position i den nationella och internationella cyberomgivningen och ger grunderna för det fortsatta arbetet i form av definitioner och utredningsuppgifter.

Planeringsfasen

I planeringsfasen fastställs en vision över cybersäkerheten, nationella principer och ett cybersäkerhetskoncept. I planeringsprocessen beaktas kapacitetskraven, till buds stående ekonomiska resurser och kunnande. Alternativa planer för hur måltillståndet kan nås utarbetas.

Beslutsfasen

I beslutsfasen jämförs olika alternativ och av alternativen väljs önskat måltillstånd samt ett nationellt verksamhetskoncept och åtgärder för att nå det. Dessutom definieras önskade cyberkapaciteter och åtgärder för att skapa dem.

Produktionsfasen

I produktionsfasen fastställs cybersäkerhetsstrategins uppbyggnad, sättet att presentera saker och cybersäkerhetens konkreta mål och ansvar. I produktionsfasen försäkrar man sig med upprepningar och mellanpresentationer om att det strategiska beslutet kommer till uttryck i den upprättade texten. Utarbetandet av strategin avslutas med att strategin presenteras för uppdragsgivaren och godkänns.

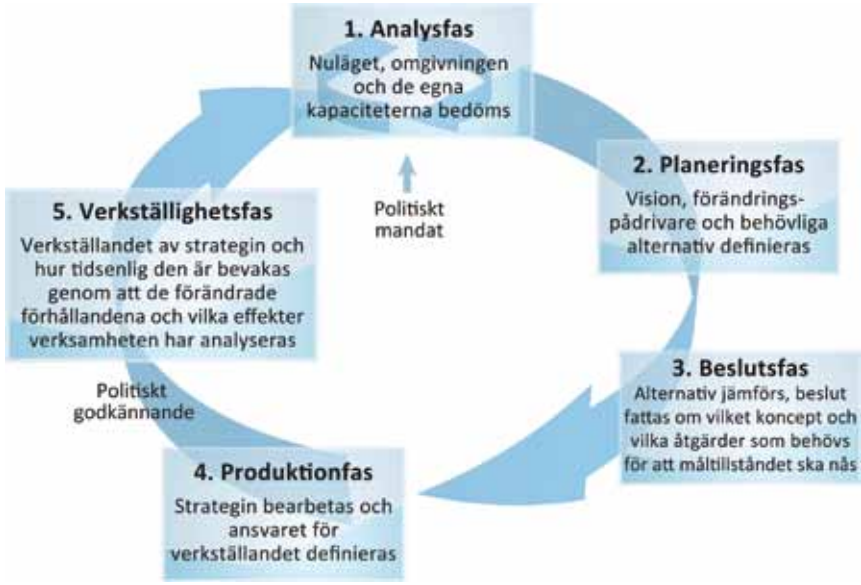
Verkställighetsfasen

De tidigare faserna i strategiprocessen har gett upphov till ett godkänt strategidokument i vilket ingår också dess verkställighetsplan och en plan över hur strategiprocessen ska kunna hållas i kontinuerlig utveckling. I verkställighetsfasen omsätts strategin i praktiken på så sätt att de förslag till åtgärder som presenteras i strategin förankras i praktiska åtgärder på olika nivåer av förvaltningen och organisationerna. För ledning av förändringen skapas ett system för mätning och uppföljning av cybersäkerhetens mogenhet. Med detta system kan det följas upp hur väl verkställigheten lyckas. Genomförandet av verkställigheten bevakas av den kommande Säkerhetskommittén och statsrådet ges årligen en rapport.

I verkställighetsfasen bevakas utvecklingen i cyberomgivningen och stöds förvaltningsområdena vid behov när de realiserar strategins principer. Målet är att upprätthålla en övergripande lägesbild av cyberomgivningen och förändringar i den samt att bevaka hur de kapaciteter utvecklas som förutsätts för att motåtgärder ska kunna vidtas.

Allokeringen av resurser är en viktig del av verkställandet av strategin. Hur resultatrik och verkningsfull verksamheten är, är direkt beroende av de ekonomiska och immateriella resurser som står till buds. Genom regeringens budgetstyrning skapas ramar för resurstilldelning till cybersäkerheten. Ansvarstagande förvaltningsenheter allokerar i enlighet med sin budgetmakt resurser för det praktiska genomförandet av cybersäkerheten såsom t.ex. för skapande av en lägesbild, beredskap, forskning och utvecklande samt för utbildning.

Cybersäkerhetsprocessen representerar en modell med kontinuerlig utveckling, där förändrade förhållanden och verksamhetens verkningsfullhet bevakas och på basis av dessa görs analyser och vid behov uppdateras strategin.



FIGUR 1 i bilagan Processen med kontinuerlig utveckling av cybersäkerheten.

www.yhteiskunnanturvallisuus.fi/sve