Strategi för cybersäkerheten i Finland

Statsrådets principbeslut 24.1.2013

INNEHÅLL

1. Inledning 1

2. Vision om cybersäkerheten 3

3. Ledningen av cybersäkerheten och en nationell handlingsmodell 4

4. Strategiska riktlinjer för cybersäkerheten 6

BILAGA Begrepp och definitioner 12

Säkerhets- och försvarskommittén
Södra Magasinsgatan 8
PB 31, 00131 HELSINGFORS

www.yhteiskunnanturvallisuus.fi/sve

Layout: Tiina Takala/puolustusministeriö
Tryckeri: Forssa print, 2013

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

1. INLEDNING

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.

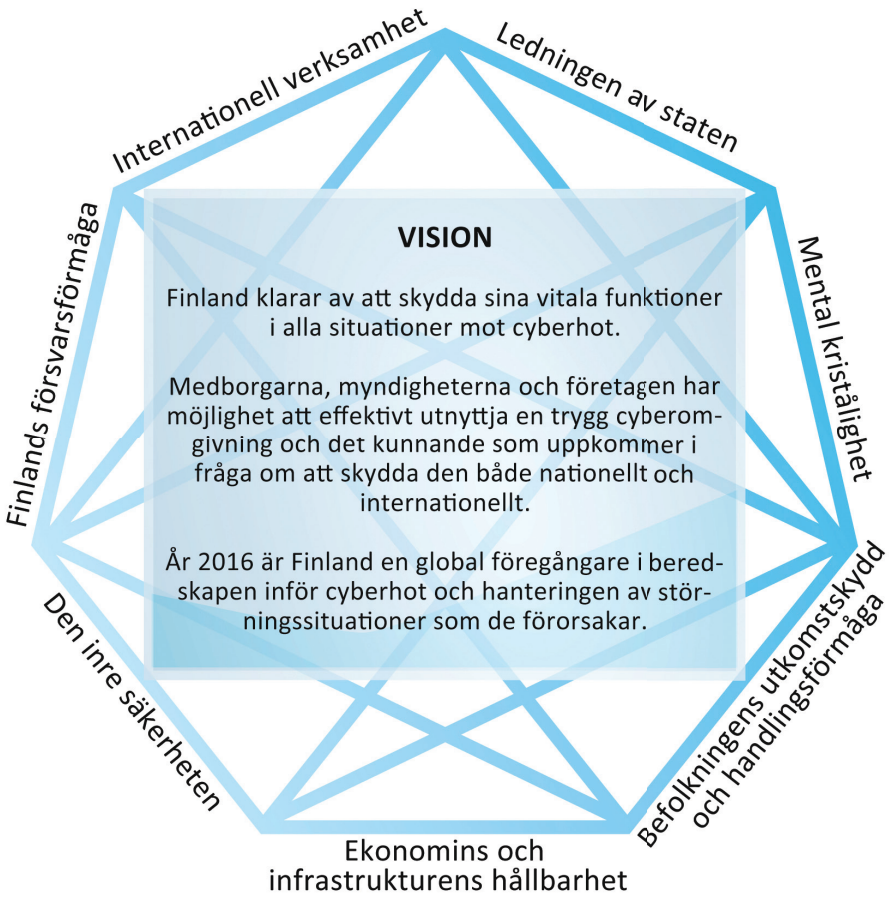
2. VISION OM CYBERSÄKERHETEN

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.yhteiskunnan turvallisuus.fi/sve