KOMMUNIKATIONSUTSKOTTETS UTLÅTANDE 7/2013 rd

Statsrådets utredning om statsrådets principbeslut om en strategi för cybersäkerheten i Finland

Strategi för cybersäkerheten i Finland

Till utrikesutskottet

INLEDNING

Remiss

Utrikesutskottet sände den 8 februari 2013 statsrådets utredning om statsrådets principbeslut om en strategi för cybersäkerheten i Finland (USP 2/2013 rd) till kommunikationsutskottet för eventuella åtgärder.

Kommunikationsutskottet beslutade den 19 februari 2013 behandla strategin för cybersäkerheten i Finland som eget ärende (LIO 3/2013 rd).

Sakkunniga

Utskottet har hört

- generalsekreterare, överste Aapo Cederberg, säkerhets- och försvarskommitténs sekretariat
- lagstiftningsråd Laura Vilkkonen, kommunikationsministeriet
- lagstiftningsråd Tiina Ferm, inrikesministeriet
- specialrådgivare Yrjö Benson, finansministeriet
- biträdande direktör Erka Koivunen och enhetschef Kirsi Karlamaa, Kommunikationsverket
- dataombudsman Reijo Aarnio, dataombudsmannens byrå, JM
- forskare, doktor i militärvetenskaper Martti Lehto, Jyväskylä universitet
- forskningsdirektör Tatu Koljonen, Statens tekniska forskningscentral
- överombudsman Mikko Kosonen, Jubileumsfonden för Finlands självständighet (Sitra)
- forsknings- och utvecklingsdirektör Jyrki Kasvi, TIEKE Utvecklingscentralen för Informationssamhälle rf
- Chief Research Officer Mikko H. Hyppönen, F-Secure Oyj
- direktör för samhällsrelationer Max Mickelsson, Microsoft Oy
- Director of Cyber Security Jarno Limnell, Stonesoft Corporation
- verkställande direktör Timo Lehtimäki, Suomen Erillisverkot Oy
- Principal Sales Consultant Markku A. Suistola, Symantec
- chef för företagssäkerhetsbyrån Jyrki Hollmén, Finlands Näringsliv
- vice ordförande Ville Oksanen, Electronic Frontier Finland ry EFFI
- beredskapschef Kari Wirman, FiCom
- ordförande Jorma Mellin, Ficix ry.

UTSKOTTETS ÖVERVÄGANDEN

Motivering

Allmänt

Närapå alla centrala och vitala funktioner i det moderna samhället är beroende av fungerande it-system och kommunikationsnät. Det är i dag A och O också för företagen att it- och kommunikationssystemen fungerar. Till följd av detta beroende har kommunikationsnäten och kommunikationstjänsterna blivit ett attraktivt mål för it-attacker, och i krissituationer spelar elektronisk kommunikation en allt viktigare roll. Stödjande sig på erhållen information anser utskottet det sannolikt att samhället blir allt mer beroende av cybermiljön i framtiden.

It-system och kommunikationsnät ger på det hela taget stora fördelar i fråga om effektivitet, kostnader m.m. Men de är också utsatta för risker i cybermiljön som man måste kunna identifiera, bereda sig på och aktivt avvärja i tid. Cybersäkerhet är ett måltillstånd där man kan lita på cybermiljön och säkra de funktioner som är beroende av denna miljö. Ett annat viktigt mål vid sidan av funktionskontinuitet bör vara att tillgodose medborgarnas och företagens rättigheter.

Strategin för cybersäkerhet är ytterst viktig och relevant, menar utskottet. Att strategin genomförs effektivt och samordnat kan under de närmaste åren få positiva effekter för den övergripande säkerheten i Finland och tilltron till cybermiljön.

Strategin innehåller en vision, en allmän handlingsmodell och strategiska riktlinjer med vilka det tänkt att man ska tackla utmaningarna i cybermiljön. Den behandlar enligt utskottets mening emellertid frågorna på ett mycket allmänt plan, och följaktligen måste extra fokus sättas på planeringen och verkställandet av den konkreta genomförandeplanen.

Vitala funktioner är enligt strategin ledningen av staten, internationell verksamhet, Finlands försvarsförmåga, den inre säkerheten, en fungerande ekonomi och infrastruktur, befolkningens försörjning och mental kristålighet. I Säkerhetsstrategi för samhället (2010) anges de viktigaste strategiska insatser som behövs för att skydda samhällsvitala funktioner och det ministerium som primärt har ansvaret för respektive insats. Kommunikationsministeriet har fått i uppdrag att säkerställa att it-system och elektroniska kommunikationssystem fungerar, stödja uppbyggnad och underhåll av larm- och varningssystem och säkerställa kontinuiteten i transporter.

När det gäller cybersäkerheten är även kommunikationsutskottets ansvarsområde och infallsvinkel koncentrerade på en fungerande it- och kommunikationsinfrastruktur och på hur den kan säkerställas. Av cybersäkerhetspaketet ingår i utskottets ansvarsområde bl.a. informationssäkerheten i fråga om öppna kommunikationsnät och nättjänster samt kommunikationstjänster, informationssäkerheten och beredskapen på teleföretag, lagstiftningen om konfidentialitet vid elektroniska kommunikationstjänster och datasekretess, Kommunikationsverkets inklusive det planerade cybercentrets uppgifter och bl.a. cybermiljöns effekter på transportsektorn. Utskottet behandlar i detta utlåtande inte säkerhetsmyndigheternas, såsom försvarets eller polisens, roll eller informationssäkerheten i fråga om statsförvaltningens egna nät eller it-system, eftersom dessa frågor inte hör till utskottet.

Kommunikationsutskottet har behandlat den aktuella strategin även som eget ärende, LIO 3/2013 rd. Utskottet har beslutat behandla dessa två ärenden i ett sammanhang.

Vad är utmärkande för cybermiljön?

Hot och risker förekommer inom alla områden. I den cyberrymd som informationssystemen och kommunikationsnäten utgör är ett visst mått av hot och risker en alldaglig företeelse. Verksamheten och beredskapen måste läggas upp utifrån det faktum att också allvarliga störningar kommer att ske.

Praktiskt taget all internettrafik inom, till och från Finland sker i teleföretagens öppna kommunikationsnät. Kommunikationsnäten är även den primära kanalen för eventuella it-attacker och den väg problemen i cybermiljön sprids. Teleföretagen, de mått och steg dessa vidtar och lagstiftningen om dem spelar alltså en enormt stor roll för cybersäkerheten.

Tekniken för verksamhet i och användning av cybermiljön utvecklas snabbt, men i vilken riktning är svårt att förutsäga många år i förväg. Attackmetoderna följer teknikutvecklingen, gärna med en viss framförhållning. Sårbarheten kan gälla egenskaper och brister i tekniken, människors rutiner eller t.ex. organisationsprocesser.

I cyberrymden kan i princip en aktör med knappa resurser men stora kunskaper vålla stor skada om uppsåtet finns. Dessutom kan tröskeln för otillbörliga eller brottsliga handlingar vara lägre i cybervärlden än i "köttvärlden". Problemmakarna i cybermiljön är i dag ofta proffs, vilket gör det svårare att avvärja hoten. Det vittnar om professionalism om attacken riktar sig mot ett specifikt objekt som attackeraren måste ha haft ingående detaljkännedom om. Det är också troligt att vissa statliga aktörer utsätter företag och samhällsfunktioner för potentiella hot i cybervärlden.

Problemen i cybervärlden kan ha skapats uppsåtligt, men störningar kan också uppstå t.ex. till följd av tekniska fel. Bakom en uppsåtlig cyberattack kan exempelvis ligga strävan efter ekonomisk vinning, industrispionage eller i värsta fall syftet att störa eller rentav lamslå kritiska samhällsfunktioner. Enligt rapport till utskottet har intentionen med merparten av den senaste tidens sabotageprogram varit ekonomisk vinning. Men även aktivism eller rentav ett statsintresse kan vara den utlösande faktorn. Den konkreta avsikten kan vara att stjäla och missbruka uppgifter, förvränga data i it-system, sabotera funktioner m.m. Risker som vanligen drabbar enskilda är identitetsstöld i bedrägerisyfte, t.ex. stöld av person- eller kreditkortsuppgifter. Eventuella attacker kan emellertid också slå mot helt andra funktioner än de avsedda.

Cybermiljön är så komplicerad att det kan vara svårt att avgöra vem som står bakom en attack, vilka alla konsekvenser attacken får eller ens vilket motivet varit till attacken. Särskilt besvärligt är det att bedöma i vilket beroendeförhållande olika sektorer står till varandra och hur de olika sektorerna och den övergripande samhällssäkerheten påverkas av störningarna. För att kunna bedöma effekterna av störningar i cybermiljön torde man också vara tvungen att göra en teknisk analys av attackmetoderna. Utifrån erhållen information konstaterar utskottet att kunskaper om attackmetoder ibland kan förebygga störningar i cybermiljön.

Aktivism har sannolikt varit bevekelsegrunden bakom de flesta överbelastningsattacker som det skrivits om så mycket på senare tid. Men i regel hotar dessa attacker inte exempelvis vitala samhällsfunktioner. Ett potentiellt hot mot kritiska samhällsfunktioner skulle däremot vara om någon kom åt att bryta sig in i eller installera exempelvis ett sabotageprogram i de it-system som funktionen i fråga är beroende av. Därför är det angeläget att inte låta it-, produktions- och styrsystem för t.ex. penningtransaktioner, energibolag, hälso- och sjukvård, industri och logistik ingå i det allmänna kommunikationsnätet, om detta bara låter sig göra. Allmänt tillgängliga e-tjänster eller andra motsvarande banktjänster och liknande webbtjänster är däremot i princip öppna för överbelastningsattacker och måste därför förses med ett tillräckligt skydd.

Utskottet påpekar att enligt sakkunnigyttranden har de numera allt vanligare molntjänsterna med sina utspridda funktioner såväl säkerhetsfördelar som egenskaper som ökar hoten i cybervärlden. Utvecklingslaboratoriet för molntjänster, som sannolikt inleder sin verksamhet 2013, bör lämpligen även befatta sig med dessa frågor, menar utskottet.

Eftersom resurserna är begränsade måste en prioritetslista skapas för de kritiska skyddsobjekten. I prioriteringen bör man utgå från vilka funktioner som mest påverkar vitala och kritiska samhällsfunktioner. Cybersäkerheten är i högsta grad beroende av de öppna kommunikationsnät som förenar it-system med varandra. Om dessa

nät utsätts för allvarliga störningar, får det stora och allvarliga konsekvenser för cybermiljön i övrigt och för beroende funktioner. Också med tanke på informationen och larmgivningen vid störningar att det viktigt att kommunikationsnäten och massmedierna fungerar.

Utskottet understryker att cybersäkerheten i allt väsentligt bygger på informationssäkerhet och framför allt på att alla centrala aktörer använder de informationssäkerhetsprocesser som krävs för att nå målnivån för cybersäkerhet. Det räcker med att en enda aktör struntar i processerna för att cybermiljön ska bli osäker för de övriga aktörerna. Alla centrala aktörer här hemma måste därför ta sitt ansvar för den gemensamma miljön.

Visionen i strategin

Strategins vision är att Finland i alla situationer kan skydda sina vitala funktioner mot cyberhot. Medborgarna, myndigheterna och företagen har möjlighet att både nationellt och internationellt effektivt utnyttja en säker cybermiljö och det kunnande som uppkommer i och med att miljön skyddas.

För medborgarna är det viktigt att en öppen, fri och säker cybermiljö skapas och upprätthålls. För näringslivet bör cybermiljön vara en trygg affärsmiljö. För hela samhället gäller dessutom framför allt att vitala funktioner tryggas. Utskottet tar fasta på visionerna och anser det vara angeläget att alla aktörer har en trygg cybermiljö till sitt förfogande bl.a. för att stödja tillväxt, konkurrensförmåga och innovationer. För att det målet ska nås gäller det att se till att kommunikationsnäten fungerar och är användbara. Självfallet bör man försöka upprätthålla kontinuiteten i våra vitala funktioner under alla omständigheter genom att slå tillbaka hot mot cybermiljön. Utskottet inskärper att det måste vara det främsta målet när strategin genomförs och att adekvata resurser måste hittas för att nå det.

Regeringsprogrammet har som mål att Finland ska vara ett av de ledande länderna när det gäller att utveckla cybersäkerheten. Strategins vision är att Finland 2016 är en global föregångare inom beredskapen inför cyberhot och hanteringen av de störningssituationer som de förorsakar. Målen är ambitiösa men i fråga om tidsplanen inte helt lätta att nå, menar utskottet. Enligt strategin ska man 2013 ta fram program som konkretiserar strategin. Det blir med andra ord knappt om tid för de åtgärder som ska leda fram till målet. Utskottet anser att målen gärna kunde främjas redan innan de olika programmen blir klara och eventuellt samordnas.

Som Finlands styrkor i fråga om cybersäkerheten nämner strategin bl.a. att vi har kunskap och att vårt land är litet, vilket gör oss reaktionssnabba och delvis också ger en tradition av förtroendefullt samarbete och nätverkande mellan privat och offentlig sektor. Det här ger oss ypperliga förutsättningar att som land nå tätpositionen i cybersäkerhet. Styrkorna måste absolut utvecklas och nyttiggöras fullt ut på vägen mot visionen, poängterar utskottet.

Nationell samordning och styrning

För att strategimålen ska nås krävs det framför allt att de operativa programmen för olika sektorer samordnas, att beredskapsåtgärderna koordineras och att ledningsförhållandena är tydliga när störningar inträffar, menar utskottet. Slutresultatet är i många avseenden också beroende av en tillgänglig och tillräcklig finansiering.

Enligt strategin hör ärenden som rör cybersäkerhet i regel till statsrådet, som är högsta ledningsnivå inom denna sektor. För att uppnå cybersäkerhet behövs dels politisk styrning, dels en lämplig fördelning av de begränsade resurserna.

Strategin påverkar i princip inte de olika myndigheternas behörighet. Enligt strategin svarar varje ministerium inom sitt område för att cybersäkerhetsrelaterade ärenden som hör till statsrådet bereds och genomförs. Men särskilt när det gäller polisen och försvarsmakten bör man enligt strategin undersöka om befogenheterna eventuellt behöver ses över. Utskottet poängterar att säkerhetsmyndigheterna kan ha sådana kunskaper som kunde nyttiggöras mer även

inom andra sektorer i cybersäkerhetssyfte. I och med att resurserna är begränsade måste förvaltningarna dela med sig av kunnande och god praxis.

Strategin nämner ofta samordning och behovet av samordning, men anförtror inte den uppgiften åt något särskilt organ. Att utgå från att varje ministerium skaffar sig beredskap för sitt eget förvaltningsområde är ingen liten utmaning. Enligt vad utskottet erfarit trotsar cybermiljön de traditionella förvaltningsgränserna och förvaltningsstrukturerna och kan delvis förpassa dem till historien. Utskottet understryker att cybermiljön inte tar hänsyn till gränsbarriärer mellan stater, för att inte tala om ministerier, och därför krävs det en effektiv styrning och ett ytterst nära samarbete för att kunna hantera säkerheten i den miljön. Enligt de strategiska riktlinjerna (nr 1) ska Finland skapa en modell för effektiv samverkan mellan myndigheter och andra aktörer för att främja den nationella cybersäkerheten och avvärja cyberhoten. Målet är en delad lägesuppfattning och regelbundna samarbetsövningar. Dessutom kommer informationsutbytet mellan myndigheter och näringsliv att främjas genom utveckling av regleringen och samarbetet. Eftersom strategin stannat för att låta myndigheternas uppgifter och uppgiftsgränser i stort sett förbli vid det tidigare, är det angeläget att ta fram effektiva samverkansmodeller för att strategimålen ska kunna nås och strategin genomföras, anser utskottet.

Programmet för att genomföra strategin består av planer som de olika aktörerna och förvaltningarna tar fram och av tvärsektoriella åtgärder som vidtas utifrån dem. Trots det decentraliserade genomförandet och samverkansmodellen gäller det att inom de fastlagda tidsplanerna för måluppfyllelse kunna bilda sig en samlad uppfattning om vilka åtgärder som behövs. Då måste man antingen utse någon som har det tydliga samordningsansvaret eller så måste ministerierna gå in för ett exceptionellt nära samarbete som genuint tar avstamp i den samlade nytta som kan genereras. Det här gäller inte bara i arbetet på verkställighetsprogram utan också i de operativa insatserna, då olika förvaltningar i praktiken måste stödja den huvudansvariga förvaltningen. Samordningen bör också ske så att åtgärderna inte konkurrerar om samma resurser.

Enligt rapport till utskottet har man i den nederländska cyberstrategin redan nått genomförandefasen. Nederländerna har tillsatt ett cybersäkerhetsråd som planerar hur strategin ska genomföras och ansvarar för själva genomförandet. Dessutom har man inrättat (vilket också Finland planerar göra) ett cybersäkerhetscenter. Det nederländska centret har emellertid också getts uppgifter som gäller den operativa ledningen av verksamheten. Dessutom står man i beråd att inrätta ett utbildnings- och övningscentrum för cybersäkerhet. Nederländerna har alltså valt en avsevärt mer centraliserad verksamhets- och ledningsmodell för genomförandet än Finland. Hos oss har respektive ministerium ett självständigt ansvar för sitt förvaltningsområde även i fråga om cybersäkerheten, men i Nederländerna har cybersäkerhetsrådet och delvis också cybersäkerhetscentret en tydlig roll också i den operativa ledningen.

Utskottet ser det som ett stort minus att man i strategin inte angett hela kommandokedjan; effektiviteten i genomförandet kommer sannolikt att bli lidande av det. Vid allvarliga störningar bör alla aktörer ha klart för sig hur det hela ska hanteras och vem som ansvarar för samordningen. Under den fortsatta beredningen är det viktigt att diskutera ledningsstrukturer och ansvarsfördelning och försöka ta fram fungerande processer som gör verksamheten effektiv, understryker utskottet.

Strategin föreslår inga ändringar i resurserna för cybersäkerhetsinsatser och presenterar ingen kostnadskalkyl. Den nöjer sig med att konstatera att ministerierna, ämbetsverken och inrättningarna reserverar de resurser som genomförandet av cybersäkerhetsstrategin förutsätter i sina egna verksamhets- och ekonomiplaner. Som det ekonomiska läget är just nu är det inte särskilt lätt att hitta resurser för nya ändamål. Därför kommer man antagligen att tvingas prioritera även när det gäller strategigenomförandet. Sett i stort anser utskottet att energi- och telekommunikationssektorn hör till de centrala in-

satsområden som kan få ett brett genomslag i samhället. Cybersäkerheten kostar, men genom att satsa på den kan man eventuellt undgå ännu större kostnader.

Strategin förefaller ge beredskapen inför hot något större tyngd än förmågan att reagera i givna situationer och återhämta sig. Som det framhållits för utskottet måste alla relevanta aktörer ha beredskap om man vill nå målen. Framsyn behövs för att kunna agera effektivt när störningar inträffar. Genom att bygga upp beredskap för normala förhållanden bygger man också upp en plattform för insatser under undantagsförhållanden. Man bör redan under normala förhållanden se till att exempelvis informations- och kommunikationssystemen är tillräckligt skyddade och säkrade för att i princip kunna stå emot hot i alla säkerhetslägen. Men att bygga upp beredskap är ofta dyrt, och i och med att cybermiljön är så oförutsägbar kan man aldrig ha den beredskap som behövs för varje enskild situation. Dessutom kan det hända att bl.a. kravet på dataanvändbarhet i informationssystemen leder till att en långt driven beredskap inte är möjlig. Därför är det viktigt med kraftiga satsningar på operativ kapacitet och förmåga att återhämta sig från störningar, menar utskottet.

Strategins infallsvinkel i fråga om förmågan att tåla cyberhot och dimensioneringen av den är att man med denna förmåga ska klara av att skapa en beredskaps- och framförhållningsförmåga som är förenlig med kraven på övergripande säkerhet, ha handlingskapacitet när störningar inträffar och kunna återhämta sig när situationen är över. När verkställighetsprogrammen upprättas vore det bra att helt generellt även diskutera den principiella frågan hur länge man bör förhålla sig till störningar så att man bara koncentrerar sig på att reducera och förhindra skador.

Utskottet påpekar att cybermiljön också bidrar till att fördunkla definitionen av normala förhållanden, störningar, undantagsförhållanden respektive särskilda situationer. Modeller som normalt används i den verkliga världen lämpar sig inte nödvändigtvis för klassificering av problem i cybermiljön och för slutsatser som dras utifrån dem. Den stora utmaningen framöver är att identifiera när och enligt vilka kriterier en störning förvandlas från en störning under normala förhållande till en störning av annan art, vilket i vissa situationer också kan påverka vilken myndighet som då är behörig.

Enligt strategin ska det grundas en säkerhetskommitté, som är ett permanent samarbetsorgan för beredskapen inom området övergripande säkerhet. Om kommitténs uppgifter föreskrivs särskilt. Kommittén ska (riktlinje nr 10) följa och samordna strategigenomförandet. Syftet med samordningen är att undvika överlappande verksamhet, identifiera eventuella brister och försäkra sig om ansvariga parter. I bakgrundspromemorian till strategin står det att kommittén samordnar beredskapen, följer genomförandet av strategin och kommer med förslag till hur den ska utvecklas i framtiden. Men de egentliga besluten i genomförandefasen fattas av ansvarsministeriet. Det torde framför allt handla om ett rådgivande expertorgan, som i bästa fall kan ha en avgörande funktion i en rationell samordning av enstaka åtgärder, beroende på upplägget, menar utskottet. Men på det hela taget är strategin mycket vag när det gäller kommitténs roll, sammansättning och verksamhetsställe.

Viktigt att skapa en lägesbild samt Kommunikationsverkets roll

För ledningen och för hanteringen av störningar är det av största vikt att besluten kan grundas på en samlad, realtida lägesbild formulerad utifrån tillförlitliga uppgifter och analysen av dem. Det blir avsevärt svårare att fatta beslut om man inte kan lita på att uppgifterna är korrekta, tidsenliga och integrerade.

Enligt de strategiska riktlinjerna (nr 2) ska de centrala aktörer som är med och tryggar samhällets vitala funktioner bli mer situationsmedvetna och i detta syfte erbjudas aktuell, samlad och analyserad information om sårbarheter, störningar och konsekvenserna av dem. Strategin föreslår att det för detta ändamål inrättas ett cybersäkerhetscenter i anknytning till Kommunikationsverket. Centret ska betjäna myndigheter, näringslivet och andra aktörer och samverka

med dem. Verksamheten har också en stark internationell dimension som fokuserar på samarbetet kring hotanalys och bedömning av vilka konsekvenser hoten får. Det har visat sig i praktiken att det inte går att agera optimalt vid störningar i cybermiljön, om man inte har tillgång till effektiva internationella samarbetsnätverk.

Cybersäkerhetscentrets primära uppgift är enligt strategin att utforma och distribuera en lägesbild över cybersäkerheten, sammanställa och upprätthålla en riskanalys över cyberhot, stödja myndigheter och den privata sektorn i hanteringen av omfattande störningar i cybermiljön, effektivisera samarbetet och stödja kompetensutveckling. Handlingsmodellen för cybersäkerheten grundar sig på ett effektivt och omfattande system för insamling och analys av information, en gemensam och delad situationsmedvetenhet och ett nationellt och internationellt beredskapssamarbete. Utskottet menar att Cybersäkerhetscentret har sin givna roll inom samtliga delområden och också när det gäller att bädda för operativt samarbete.

Det är i högsta grad befogat att knyta centret till Kommunikationsverket. Verket har redan nu uppgifter som rör bl.a. funktion och säkerhet i fråga om de kommunikationsnät som cybersäkerheten i allt väsentligt vilar på, det besitter den kompetens som behövs och det har internationella kontakter som bl.a. Cert-FI-gruppen byggt upp. Verket är för alla aktörer, även näringslivet, en neutral plats att förlägga centret till och kan därmed medverka till ett välfungerande och förtroendefullt samarbete mellan aktörerna. För att informationen ska löpa smidigt i bägge riktningar krävs ett förtroendefullt samarbete mellan centret och andra aktörer.

Eftersom merparten av den samhällsviktiga kritiska infrastrukturen och verksamheten förvaltas av den privata sektorn, bör centret även ge hög prioritet åt att hjälpa företag att skydda sig mot och avvärja cyberhot. Framför allt bör man försöka se till att lägesbilden är till största möjliga gagn för säkerhetsåtgärderna vid företag som är kritiska för försörjningstryggheten. I initialfasen torde det vara viktigast att reda ut vilken information de olika aktörerna behöver och utifrån det planera centrets verksamhet och rutiner. Centret behöver också stödas av ett engagerat nätverk bestående av de aktörer som bör bereda sig på störningar och attacker i cybermiljön.

Enligt de strategiska riktlinjerna (nr 4) ska det ses till att polisen har effektiva förutsättningar att förebygga, avslöja och reda ut brott som riktar sig mot och utnyttjar cybermiljön. Dessutom (nr 5) ska försvarsmakten skapa en övergripande cyberförsvarsförmåga i sina lagstadgade uppgifter. Utskottet understryker vikten av att man tar fram fungerande modeller för samverkan mellan polisen, försvaret och det planerade cybersäkerhetscentret.

Ur helhetssynpunkt och för att undvika överlappningar är det mycket viktigt att Cybersäkerhetscentrets verksamhet och samarbetet inte bara inriktar sig på teleföretag och privata aktörer som är kritiska för försörjningstryggheten utan också på statliga aktörer. Det är ytterst angeläget att man försöker nå cybersäkerhetsmålen utan onödiga, överlappande och resursslukande funktioner och utan att begränsa informationsutbytet. Enligt reglementet för statsrådet hör datasäkerheten inom statsförvaltningen till finansministeriets ansvarsområde. Det inkluderar också ansvaret för den s.k. GovCert-funktionen som hanterar kränkningar av och hot mot informationssäkerheten inom statskoncernen.

Cybersäkerhetscentret är en källa för kritisk information och kommer därför att vara en intressant måltavla för cyberattacker. Därför gäller det att vara noga med skyddet av centret för att det ska kunna fortsätta fungera och datasekretessen säkerställas.

Utskottet anser att inrättandet av ett cybersäkerhetscenter hör till strategins viktigaste riktlinjer och att det kommer att gagna alla sektorer. Därför måste man absolut se till att centret får så mycket personella och andra resurser att förväntningarna på verksamheten inte kommer på skam, utan att resurserna räcker till en effektiv och trovärdig dygnetruntverksamhet. Resursbehovet bör följas upp, och om uppgifterna ökar till följd av eventuella förändringar i omvärlden bör detta beaktas i resurstilldelningen.

Privataktörernas roll

Den vitala samhällsinfrastrukturen är till övervägande del i privat ägo och används och underhålls utifrån kommersiella premisser. Detta gäller även informationssystem, kommunikationsnät och informationssäkerheten för dem. För att strategimålen ska nås krävs det alltså aktiva tag särskilt från företagsvärlden. Därför är det angeläget att näringslivet är nära involverat när verkställighetsprogrammen upprättas och att man i genomförandet försöker intensifiera det för båda parter nyttiga samarbetet mellan privat och offentlig sektor. Särskilt viktigt är det att försäkra sig om ett uppgiftsflöde i båda riktningarna.

Det är inte bara samarbetet mellan myndigheterna eller mellan offentlig och privat sektor som måste förbättras och intensifieras utan också samarbetet mellan aktörerna inom den privata sektorn. Teleföretag och energiföretag är klart och tydligt beroende av varandra, och dessutom påverkar de andra kritiska samhällsfunktioner. Därför måste i synnerhet samarbetet mellan dem löpa friktionsfritt för att störningar t.ex. i samband med stormar ska kunna hanteras och återhämtningen ske snabbt. Som exempel kan tas energibolagens reparationsberedskap och kännedom om reparationsläget, som spelar en avgörande roll för hur teleföretagens kommunikationsnät och service fungerar.

Enligt de strategiska riktlinjerna (nr 9) tilldelas myndigheterna och näringslivet uppgifter för cybersäkerheten: varje förvaltningsområde ska göra en analys för att identifiera betydelsefulla sårbarheter och hur de hanteras. Analysresultatet läggs till grund för respektive förvaltningsområdens verkställighetsprogram och utgör stöd för de program som upprättas för näringslivet. Strategiriktlinje nr 3 går ut på att man ska utveckla förmågan att upptäcka och avvärja cyberhot och att återhämta sig från störningar hos företag och organisationer av central betydelse för vitala samhällsfunktioner. I praktiken handlar det bl.a. om att de här aktörerna ska ta hänsyn till hoten och hur de negativa effekterna kan minimeras när de upprättar sina säkerhets- och beredskapsplaner. Aktörerna ska utveckla sin störningstålighet så att det inte blir stopp i verksamheten vid exempelvis en cyberattack. Utskottet stöder helhjärtat dessa riktlinjer. När verkställighetsprogrammen upprättas vore det också bra att fundera på med vilken logik och vilka intressen företagen går in för att aktivt genomföra de åtgärder som den nationella strategin kräver. Denna frågeställning kompliceras av att näringslivet internationaliserats, företag som tidigare varit finskägda sålts till utlandet och funktioner utkontrakterats.

När internationella företag funderar på etableringsställe och investeringar tittar de också på hur säker miljön är. Cybersäkerheten kan alltså vara ett stort ekonomiskt plus bl.a. med tanke på investeringar. Här har Finland utan tvekan potential, menar utskottet. Genom att arbeta för visionen får vi inte bara en bättre säkerhet hemmavid utan drar också till oss investeringar. Finland har redan nu kompetens på hög nivå när det gäller den informationssäkerhet m.m. som cybersäkerheten kräver. Med bättre villkor kan denna kompetens användas för att utveckla nya inhemska och eventuellt även exportdugliga produkter och andra former av näringsverksamhet. Under de närmaste åren kommer det att vara livligt på den internationella cybersäkerhetsmarknaden, och det gäller för Finland att försöka få sin del av kakan.

Med tanke på cybersäkerheten vore det enligt utskottets mening bra att titta på kraven för säker upphandling, särskilt avseende leverantörer av kritiska informations- och kommunikationsinfrastrukturer eller program. Utskottet vill även lyfta fram Finlands kommunikationsförbindelser med omvärlden. Om man ser till säkerheten och förbindelsernas störningstålighet kunde det enligt information till utskottet mycket väl vara motiverat att öka de alternativa förbindelserna. Samtidigt kunde det vara nyttigt att diskutera frågan om den geografiska placeringen av vissa högkritiska kommunikationssystem och hur den eventuellt påverkar den övergripande cybersäkerheten.

Enligt de strategiska riktlinjerna (nr 7) ska cyberkunnandet och cyberförståelsen förbättras hos alla samhällsaktörer. För att nå detta mål ska man bl.a. fokusera på anvisningar, utbildning

och övningar, grunda ett spetskompetenskluster och satsa på forskning. Det operativa samarbetet kan i praktiken löpa avsevärt bättre, om det ordnas regelbundna övningar för alla centrala aktörer inom offentlig och privat sektor, poängterar utskottet. Observeras bör att det är inte bara är den inhemska forskningen som behöver främjas, utan det gäller också att aktivt försöka nyttiggöra utländska forskningsresultat.

Medborgaraspekten

Utskottet noterar att strategin är mycket knapphändig när det gäller medborgarnas roll i cybersäkerheten. Cybermiljön bör vara så trygg att medborgarnas rättigheter inte kränks där. Samtidigt påverkas säkerheten i cybermiljön av medborgarnas egna aktiviteter. Cybersäkerhet bidrar till att öka medborgarnas förtroende för miljön, vilket är av fundamental betydelse nu när det blivit allt vanligare med exempelvis e-handel och e-tjänster.

En dimension av cybersäkerheten är att de grundläggande fri- och rättigheterna ska tillgodoses i cybermiljön även i händelse av störningar. Cybersäkerheten bör utformas så att exempelvis skyddet för förtroliga meddelanden eller integritetsskyddet inte kränks. Men man kan i princip se det som så att man genom att främja cybersäkerheten också bidrar till att skydda privatlivet och förtroliga meddelanden. Denna balansgång mellan olika mål och rättigheter är ingen lätt match, men måste göras när strategin genomförs.

Personuppgifter, lösenord och kreditkortsuppgifter kan användas för bedrägeri i cybermiljön. Dem försöker man komma åt genom bl.a. nätfiske (phishing), tangentlogg (keylogger) eller intrång i it-system för tjänster som använder personuppgifter. En av de stora utmaningarna i framtiden är hur medborgarnas e-identitet ska kunna skyddas i cybermiljön; det är något som bör beaktas också när strategin genomförs. Mot den bakgrunden kan det hända att cybermiljön blir mer sårbar om man integrerar databaser innehållande personuppgifter.

Varje aktör i cybermiljön påverkar säkerheten där. Alltså bör all terminalutrustning som medborgarna kopplat till kommunikationsnät kunna skyddas så att den inte t.ex. kan kapas och användas för överbelastningsattacker eller spam eller annars användas för att skada medborgarna själva eller andra aktörer i cybermiljön. Medborgarna bör också kunna använda terminalutrustningen och hantera näten så att exempelvis kommunikationstjänsterna eller kommunikationsnäten inte störs av det. Sannolikt kommer även säkerheten för medborgarnas mobiltelefoner och olika slags mobila terminaler och deras sårbarhet att få en större betydelse för cybersäkerheten än i dag, när dessa till det allmänna kommunikationsnätet kopplade högst olika terminalerna ökar i antal runtom i världen. Men det är trots allt svårt att påverka säkerhetsfunktionerna i apparaterna eller deras operativsystem med renodlat inhemska åtgärder.

Här hemma är det främst ökad utbildning och vägledning som kan påverka medborgarnas agerande och beteende som upplysta användare i cybermiljön, och på den punkten har kommunikationstjänsteleverantören sin egen roll. Det är också viktigt att ta hänsyn till barnen och deras särskilda behov som aktörer i cybermiljön t.ex. i skolornas undervisningsinnehåll. Utbildning är enligt utskottets mening ett kostnadseffektivt sätt att öka cybersäkerheten och medborgarnas användarfärdigheter i cybermiljön.

Utveckling av lagstiftningen

Enligt de strategiska riktlinjerna (nr 8) ska man kartlägga den lagstiftning som påverkar och anknyter till cybermiljön och cybersäkerheten och behovet att utveckla den. Därefter framläggs förslag till hur lagstiftningen kan utvecklas. Ambitionen med förslagen är bl.a. att säkerställa att lagstiftningen ger alla aktörer tillgång till de åtgärder som behövs för att skydda de vitala samhällsfunktionerna. Det här gäller inte minst myndigheternas befogenheter och t.ex. bestämmelserna om behandling av uppgifter och uppgiftsutlämning mellan olika aktörer. Utskottet ser positivt på dessa riktlinjer.

Finland har redan länge använt sig också av lagstiftning för att säkerställa att kommunikationstjänsterna och kommunikationsnäten är driftssäkra och trygga. Teleföretag är enligt 90 § i kommunikationsmarknadslagen (393/2003) skyldiga att sörja för att deras verksamhet fortgår så störningsfritt som möjligt även under sådana undantagsförhållanden som avses i beredskapslagen och vid störningar under normala förhållanden. Bestämmelser om teleföretagens rätt att få ersättning för avsevärda beredskapskostnader finns i 94 § i kommunikationsmarknadslagen. Kommunikationsverket har utfärdat närmare bestämmelser om vad dessa skyldigheter innebär tekniskt sett. Att ha beredskap betyder i praktiken t.ex. att personalen måste utbildas, anläggningar och system skyddas tekniskt eller exempelvis ett reservsystem byggas upp. Teleföretagen ska också rapportera till Kommunikationsverket om fel, störningar och kränkningar av dataskyddet, och verket övervakar att kraven uppfylls. Utskottet menar att teleföretagen redan nu berörs av en tämligen omfattande reglering gällande beredskap, informationssäkerhet och bl.a. skyldighet av rapportera om störningar av olika slag. Teleföretagen spelar en viktig roll för cybersäkerheten, men det är samtidigt högst sannolikt att de tagit i genomsnitt bättre hänsyn till informationssäkerheten i sina funktioner än vad man gjort i många andra kritiska vitala samhällsfunktioner.

Utskottet vill påpeka att bestämmelserna om myndigheternas befogenheter i beredskapslagen, som gäller undantagsförhållanden, blir aktuella först när situationen är ytterst allvarlig. Om det sker t.ex. en allvarlig attack över kommunikationsnäten, är tröskeln för att tillämpa beredskapslagen sannolikt mycket hög. Ett minus med beredskapslagen i cybermiljöhänseende är att det tar tid att ta i bruk befogenheterna. Beredskapslagens befogenhetsmekanism är mycket trög i cybermiljön, där åtgärder måste kunna vidtas snabbt och där störningarna kan få en betydande spridningseffekt på några timmar eller rentav några minuter. Till följd av cybermiljöns karaktär och den hastighet med vilken problemen sprider sig kan t.ex. kommunikationsnätet ha slagits ut efter en allvarlig cyberattack redan i det skedet när man ännu håller på att ta i bruk beredskapslagens befogenheter.

Med undantag för vissa exceptionella fall måste man utgå från lagstiftningen för normala förhållanden när störningar inträffar i cybermiljön. Därför är det med avseende på cybersäkerheten viktigt att man kartlägger vilket behov och vilka möjligheter det finns att ändra lagstiftningen för normala förhållanden. Lagstiftningen får inte lägga onödiga hinder för att värna om säkerheten i cybermiljön, och nödvändig informationsförmedling måste tillåtas för att skydda vitala samhällsfunktioner. Men när man kartlägger ändringsbehoven måste man vara noga med att de grundläggande rättigheterna, såsom skyddet för förtroliga meddelanden och i vidare bemärkelse integritetsskyddet, tillgodoses även i cybermiljön. Det här är enligt utskottet viktigt även med tanke på förtroendet för cybermiljön.

Om det anses behövligt och lämpligt kunde man förutom verksamhet utifrån frivillig samverkan även fundera på om de nuvarande bestämmelserna om informationssäkerhet och rapportering om störningar, som främst gäller teleföretag i egenskap av cybermiljöaktörer, delvis kunde utsträckas till att gälla vissa andra aktörer av relevans för cybersäkerheten eller de vitala samhällsfunktionerna. Utskottet ser ändå att man når målen bättre med frivillig eller avtalsbaserad samverkan än med tvingande lagstiftning.

I och med att störningar i cybervärlden är ett internationellt fenomen måste också de rättsliga förfarandena bli effektivare globalt sett. Till följd av det starka internationella inslaget i cybermiljön med anknytande problem behövs internationellt samarbete på alla nivåer, och när cybersäkerheten förbättras utomlands förbättras också vår cybersäkerhet. De strategiska riktlinjerna (nr 6) utgår från ett aktivt deltagande i internationella organisationer och samarbetsforum när det gäller cybersäkerhet. Särskilt viktigt är det att försöka följa och tillägna sig god internationell praxis och delta aktivt inte minst när ärenden bereds och uppgiftsagendan fastställs på EU-nivå. Det bör observeras att man inom EU håller på att ta fram ett nät- och informationssä-

kerhetsdirektiv och en cyberstrategi, som kan få vissa konsekvenser för verkställighetsprogrammen. Utskottet understryker att Finland måste ta en mycket aktiv roll i beredningen av direktivet.

Cybersäkerhetens effekter på transporter

Trafiken och transporterna hör till de kritiska samhällsfunktionerna. Fungerande transporter är väsentliga för hela samhället och behövs för att myndigheter, företag, industri och medborgare ska kunna fungera och verka. Många vitala samhällsfunktioner är också beroende av att vissa bestämda personer kan ta sig till jobbet under alla omständigheter.

I dagens läge är det i stor utsträckning data- och kommunikationssystem som borgar för att transporterna fungerar och löper smidigt. Vissa transportformer är mer beroende av dessa system än andra, men en allvarlig störning t.ex. i styrsystem eller eldistribution kan medföra stort förfång för funktionerna och säkerheten. Inom transportsektorn finns det också centrala datasystem som någon kan tänkas vara intresserad att göra en attack mot.

Det är ytterst angeläget att utveckla intelligenta transportsystem bl.a. för att det ökar trafiksäkerheten och får trafiken att löpa smidigare. Men i och med att intelligenta transportsystem utvecklas och blir allmännare ökar trafikens beroende av cybermiljön, och beroendet utsträcks också till fordon när fordonstekniken utvecklas.

Det är viktigt, menar utskottet, att man i programmen för genomförande av strategin tar full hänsyn till symbiosen mellan cybermiljö och transportsystem och eventuella sårbarheter på den punkten.

Avslutningsvis

Utskottet ser cybersäkerhetsstrategin som ett stort kliv framåt. Det gäller att noga bevaka hur den genomförs och vilka effekter den får och i förekommande fall vara redo att snabbt lägga om kursen vid förändringar i miljö och hotbilder.

Ställningstagande

Kommunikationsutskottet föreslår

att utrikesutskottet beaktar det som sägs ovan.

Helsingfors den 3 april 2013

I den avgörande behandlingen deltog

ordf. Kalle Jokinen /saml
vordf. Osmo Kokko /saf
medl. Mikko Alatalo /cent
Thomas Blomqvist /sv
Markku Eestilä /saml (delvis)
Ari Jalonen /saf
Jukka Kopra /saml
Merja Kuusisto /sd
Johanna Ojala-Niemelä /sd
Raimo Piirainen /sd
Janne Sankelo /saml
Eila Tiainen /vänst
Ari Torniainen /cent
Reijo Tossavainen /saf
Oras Tynkkynen /gröna
Mirja Vehkaperä /cent.

Sekreterare var

utskottsråd Juha Perttula.