FÖRVALTNINGSUTSKOTTETS UTLÅTANDE 3/2013 rd

Statsrådets redogörelse: Finlands säkerhets- och försvarspolitik 2012

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

Till utrikesutskottet

INLEDNING

Remiss

Riksdagen remitterade den 7 februari 2012 statsrådets redogörelse för Finlands säkerhets- och försvarspolitik (SRR 6/2012 rd) till utrikesutskottet för beredning och bestämde samtidigt att förvaltningsutskottet ska lämna utlåtande i ärendet till utrikesutskottet.

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

Sakkunniga

Utskottet har hört

- statssekreterare Olli-Pekka Heinonen, statsrådets kansli
- ambassadråd Leena Ritola och utrikessekreterare Laura Kamras, utrikesministeriet
- kanslichef Päivi Nerg, lagstiftningsråd Tiina Ferm och kommodor Markku Halonen, inrikesministeriet
- generalsekreterare för säkerhets- och försvarskommittén Aapo Cederberg, försvarsministeriet
- finansråd Teemu Eriksson, regeringsråd Ismo Mäenpää och datasäkerhetsexpert Aku Hilve, finansministeriet
- trafikråd Mika Mäkilä, konsultativ tjänsteman Timo Kievari och inspektör Harri Uusnäkki, kommunikationsministeriet
- medicinalråd Timo Keistinen, social- och hälsovårdsministeriet
- utvecklingsdirektör Tomi Vuori, Polisstyrelsen
- polisråd, chef Antti Pelttari, skyddspolisen
- direktör Matti Heinonen, Migrationsverket
- generaldirektör Antti Hartikainen och brottsbekämpningschef Sami Rakshit, Tullstyrelsen
- chef för gruppen för säkerhetsövervakning Jarkko Saarimäki, Kommunikationsverket
- biträdande direktör Erka Koivunen, Kommunikationsverket, CERT-FI
- direktör för nödcentralstjänsterna Marko Nieminen, Nödcentralsverket
- direktör Veli-Pekka Nurmi, Centralen för undersökning av olyckor
- direktör Sauli Savisalo, Försörjningsberedskapscentralen
- lärare Juha-Pekka Oksanen, Polisyrkeshögskolan

- kriminalinspektör Jukkapekka Risu, polisinrättningen i Helsingfors
- tf. chef för säkerhets- och beredskapsenheten Matti Koskinen, Helsingfors stad
- chef för befolkningsskyddsenheten Tommi Laurinen, Helsingfors stads räddningsverk
- äldre forskare i informationssäkerhet Jarno Niemelä, F-Secure Oy
- styrelseledamot Mikko Kenttälä, Electronic Frontier Finland ry EFFI
- ledande expert Mika Linna, Finansbranschens Centralförbund rf
- generalsekreterare Kristiina Kumpula, Finlands Röda Kors.

Dessutom har skriftliga utlåtanden lämnats av

— centralkriminalpolisen
— Regionförvaltningsverket i Södra Finland
— Trafiksäkerhetsverket
— Institutet för hälsa och välfärd
— Helsingfors och Nylands sjukvårdsdistrikt
— Finlands Kommunförbund
— Finlands Näringsliv rf
— FiCom rf
— Poliisi-, ulosotto-, syyttäjä- ja maistraattilakimiesten edunvalvontajärjestö PUSH ry
— Gränssäkerhetsunionen rf
— Räddningsbranschens Centralorganisation i Finland ry
— Finlands Polisorganisationers Förbund rf

UTSKOTTETS ÖVERVÄGANDEN

Motivering

Statsrådets redogörelse beskriver utvecklingen i Finlands säkerhetspolitiska omvärld och drar upp linjerna för Finlands säkerhets- och försvarspolitik utifrån ett brett säkerhetsbegrepp. Utskottet har granskat redogörelsen med avseende på den inre säkerheten. I samband med redogörelsen har utskottet även behandlat statsrådets principbeslut om strategin för cybersäkerheten i Finland (USP 2/2013 rd) och ställningstagandena om beslutet ingår i detta utlåtande.

Statsrådets redogörelse för Finlands säkerhets- och försvarspolitik 2012

Tryggandet av ett fungerande samhälle utifrån principen om övergripande säkerhet

Den säkerhets- och försvarspolitiska redogörelsen sträcker sig över regeringsperioderna och är ett centralt styrdokument med bäring på den övergripande säkerheten. Begreppet övergripande säkerhet har definierats i statsrådets principbeslut från december 2012, som även preciserar ansvarsfördelningen mellan de olika förvaltningsområdena och etablerar de grunder för beredskapen som är gemensamma för alla. Utgångspunkten är att samhällets vitala funktioner tryggas genom samverkan mellan myndigheterna, näringslivet, organisationerna och medborgarna. De allmänna principerna för den övergripande säkerheten beskrivs i dokumentet Säkerhetsstrategi för samhället (2010), som bl.a. tar upp hotbilder mot de vitala samhällsfunktionerna och som lägger grunden för beredskaps- och ledningsarbetet i samband med kriser. De konkreta riktlinjerna för verkställandet dras upp i regeringsprogrammet och i olika statsrådsbeslut samt i förvaltningsområdenas verksamhets- och ekonomiplaner och andra strategidokument, däribland programmet för den inre säkerheten.

Det är enligt utskottet motiverat att utgå från begreppet övergripande säkerhet. Redogörelsen beskriver förändringarna i den internationella omvärlden och det ökande ömsesidiga beroendet ur ett flertal perspektiv. Den livligare internationella växelverkan och det ömsesidiga beroendet påverkar invånarnas och samhällenas vardag på många sätt. De ekonomiska effekterna är positiva, men beroendet av varandra ökar samtidigt sårbarheten och gör det svårare att upprätthålla den övergripande säkerheten. För att kunna förebygga och motverka omfattande, gränsöverskridande hot och problem är det viktigt att

bygga upp beredskapen med stöd i de europeiska och globala samarbetsstrukturerna. Med tanke på krisernas och hotens art måste myndighetssamarbetet fördjupas. Det medger samtidigt en effektivare användning av samhällets resurser. Samtidigt ökar näringslivets och frivilligorganisationernas roll i tryggandet av de vitala samhällsfunktionerna. Ett brett säkerhetstänkande som utformats i samverkan stödjer de förebyggande insatserna och gör det lättare att hitta kostnadseffektiva lösningar.

Som ett led i verkställandet av statsrådets principbeslut om den övergripande säkerheten inrättades i januari 2013 en säkerhetskommitté. Denna ersatte den tidigare säkerhets- och försvarskommittén, som bistod det utrikes- och säkerhetspolitiska ministerutskottet och försvarsministeriet i ärenden med anknytning till totalförsvaret. Den nya säkerhetskommittén ska bland annat bistå statsrådet och ministerierna i den beredskap som syftar till att hantera den övergripande säkerheten och i samordningen av denna beredskap. Kommittén är vid behov dessutom sakkunnigorgan i samband med olika störningssituationer i samhället. Det är positivt att kommitténs sammansättning har breddats och får fler representanter för myndigheter som arbetar med inre säkerhet. I kommittén ingår nu också polisöverdirektören, räddningsöverdirektören och Tullens generaldirektör. Dessutom kopplar kommittén in sakkunniga från olika organisationer samt från näringslivet och forskningssamfundet.

Den inre säkerheten ett led i den övergripande säkerheten

De viktigaste uppgifterna inom vår utrikes-, säkerhets- och försvarspolitik är enligt redogörelsen att trygga landets självständighet, territoriella integritet och grundläggande värden, att främja befolkningens säkerhet och välfärd och att upprätthålla ett fungerande samhälle. Säkerhetspolitiken beaktar de gränsöverskridande hoten och inser vikten av internationellt samarbete i arbetet för att förebygga och avvärja hoten. Mot bakgrunden av det breda säkerhetsbegreppet accentueras också det inre tillståndet i samhällena.

Utskottet konstaterar att det inre säkerhetsarbetet har åtskilliga beröringspunkter med den yttre säkerheten och överhuvudtaget med arbetet för att förbättra Finlands säkerhetsmiljö. De mest centrala frågekomplexen inom den inre säkerheten är bekämpningen av terrorism och organiserad brottslighet, stärkandet av gränssäkerheten, kontrollen över migrationsrörelserna, det internationella räddningssamarbetet och övrig krishjälp. Inom dessa områden är Europeiska unionen Finlands centrala referensram. Den finländska medverkan i det europeiska samarbetet kan också bidra till en positiv utveckling av säkerhetsmiljön i unionens närområde.

I och med det ökande ömsesidiga beroendet på det globala planet hör, enligt redogörelsen, staternas externa och interna säkerhet allt närmare ihop. Trots detta får den interna säkerheten relativt lite uppmärksamhet i redogörelsen, som klart fokuserar på försvarspolitiken. Det breda säkerhetsbegreppet förutsätter att vi skyddar oss inte bara mot militära hot, utan detta säkerhetskomplex förutsätter också skydd mot t.ex. brottslighet och olyckor. Även om arbetet för inre säkerhet tar sig konkret uttryck genom programmet för den inre säkerheten, framhåller utskottet att de synpunkter på den inre säkerheten som lyfts fram i detta utlåtande måste behandlas tydligare och i ökad omfattning i de dokument om den övergripande säkerheten som utarbetas hädanefter.

Beredskapen inför visumfriheten mellan EU och Ryssland

Redogörelsen tar upp en central fråga med hänsyn till den inre säkerheten, nämligen beredskapen inför en eventuell visumfrihet mellan EU och Ryssland. Gränsen mellan Finland och Ryssland utgör en del av Europeiska unionens yttre gräns. Finland har förbundit sig att effektivt övervaka denna gräns och att ha ett nationellt gränssäkerhetssystem som uppfyller kraven i EU-lagstiftningen.

Gränstrafiken ökar kraftigt särskilt på de stora gränsövergångarna längs den sydöstra gränsen och i Helsingfors hamn och på Helsingfors-Vanda flygplats. Enligt uppskattning fördubblas

trafiken på den östra gränsen fram till 2018 i jämförelse med 2011 och resenärerna kommer då att vara cirka 20 miljoner. Genom visumfriheten väntas antalet gränspassager stiga till över 30 miljoner. Utskottet konstaterar att en fortsatt smidig och säker trafik förutsätter att trafikledernа och gränsinfrastrukturen förnyas och att gränsmyndigheternas resurser förstärks.

Gränsbevakningsväsendets mest centrala strategiska projekt anknyter till att hantera den växande gränstrafiken och förbereda sig på visumfrihet med Ryssland. Ett utvecklingsprogram för ombyggnad av gränsövergångsställena har tagits fram i samråd mellan de finska och de ryska myndigheterna. Enligt uppgift kräver det ett tilläggsanslag till gränsbevakningsväsendet på cirka 16 miljoner euro under ramperioden. Enligt redovisningen förutsätter främjandet av säkerheten i närområdet att man i god tid bygger upp god beredskap för visumfriheten mellan EU och Ryssland. Utskottet menar att beredskapsarbetet bör lägga tyngden på gränsövervakningen och på resurserna för denna.

Gränsbevakningsväsendet har gått igenom en omfattande omorganisering och genomför dessutom ett ekonomiskt anpassningsprogram. Utskottet har i olika sammanhang fäst uppmärksamhet vid att den ökande gränstrafiken innebär att gränsbevakningsväsendet behöver större anslag (se t.ex. FvUU 14/2012 rd och FvUU 5/2012 rd). Utskottet ser det som positivt att gränsbevakningsväsendets resurser har stärkts i rambeslutet om statsfinanserna för 2015—2017.

Visumfriheten skulle ge verkningar också för andra myndigheter som arbetar med inre säkerhet. Bland annat innebär det för polisens del ökad efterfrågan på trafiksäkerhetstjänster, tillståndstjänster, bekämpning och utredning av brott samt övervakning av utlänningar i inlandet. Utskottet menar att förberedelserna inför visumfriheten bör fokusera på att se till att det finns tillräckliga polistjänster redan då visumfriheten börjar.

Visumfriheten väntas även ha andra återverkningar. Till exempel antas antalet trafikolyckor och andra olyckor som kräver räddningsväsendets hjälp öka i samma proportion som turismen.

Också tullen har på senare år varit tvungen att kraftigt dra ned på verksamheten, vilket påverkat resurserna framför allt vid gränsövergångarna i södra och sydöstra Finland, i hamnarna och på Helsingfors-Vanda flygplats. Tullen medverkar också i gränskontrolluppgifter. Också tullen behöver större satsningar på infrastruktur och personal för att kunna hantera den ökande gränstrafiken och ha beredskap för att visumfrihet införs mellan EU och Ryssland.

Kommunernas och regionernas roll inom den övergripande säkerheten

Som det sägs i redogörelsen är det kommunerna som organiserar de lokala välfärds- och säkerhetstjänsterna. Kommunerna har en central roll inom beredskapen och den övergripande säkerheten, eftersom de organiserar basservicen och många andra vitala funktioner i samhället. Redogörelsens analys av och riktlinjer för det kommunala perspektivet är dock anspråkslösa.

Enligt räddningslagen (379/2011) ansvarar kommunerna i samverkan för räddningsväsendet inom räddningsområdena (det lokala räddningsväsendet). Redogörelsen tar överhuvudtaget inte upp det lokala räddningsväsendets eller räddningsverkens roll i upprätthållandet och utvecklingen av kommunernas och regionernas säkerhet. Det lokala räddningsväsendet ansvarar för räddningsväsendets servicenivå och för att räddningsverkets verksamhet och sotningstjänster ordnas på behörigt sätt. Räddningsverket ska inom sitt område bl.a. sörja för den styrning och rådgivning inom räddningsväsendet som syftar till att förebygga olyckor, för att befolkningen varnas vid tillbud och olyckor samt för de uppgifter som hör till räddningsverksamheten. Räddningsverket ska vidare stödja beredskapsplaneringen i en kommun som hör till räddningsområdet, om detta har överenskommits med kommunen.

Enligt redogörelsen ska samarbetet mellan kommunerna utvecklas med stöd av regionförvaltningen. Utskottet uttalar sitt stöd för ett ökat samarbete mellan kommunerna i syfte att främja säkerheten i regionerna. Samtidigt är det viktigt att ta hänsyn till de regioner och städer som har

en vidare betydelse för den övergripande säkerheten, t.ex. när det gäller att skydda riksomfattande funktioner.

Formuleringarna i redogörelsen är enligt utskottet dock något otydliga. Stödet till kommunernas beredskap har i hög grad skett via räddningsverken. Enligt de sakkunniga inom räddningsbranschen som utskottet hört kan man förvänta sig att kommunerna i allt högre grad kommer att stödja sig på räddningsverken när det gäller att utveckla beredskapen och ta fram lägesbilder samt även för ledningsuppgifter. I lagen om regionförvaltningsverken (896/2009) sägs å andra sidan att regionförvaltningsverken bl.a. ska samordna beredskapen och beredskapsplaneringen, stödja kommunernas beredskapsplanering, ordna beredskapsövningar och stödja behöriga myndigheter i samband med säkerhetssituationer. Begreppet regionförvaltning syftar i regel på regionförvaltningsmyndigheterna, som utöver regionförvaltningsverken omfattar närings-, trafik- och miljöcentralerna.

Det är viktigt med god samordning mellan kommunerna och inom regionerna för att resurserna ska kunna utnyttjas effektivt och för att få till stånd tillräckligt enhetliga handlingsmodeller. Utifrån den styrning inrikesministeriet gett har regionförvaltningsverken inrättat regionala beredskapskommittéer med uppgift att bidra till lägesbilden för regionen, beredskapsplaneringen och i synnerhet att främja samarbetet mellan olika sektorer i fråga om beredskap och säkerhet. Dessutom finns det beredskapskommittéer i landskapen och andra former för beredskapssamarbete mellan kommunerna.

Utskottet understryker att myndigheternas ansvar och uppgifter inom säkerheten måste vara tydliga i fråga om såväl beredskapen och beredskapsplaneringen som agerandet vid hot och störningssituationer. Beredningen av de kommande redogörelserna bör enligt utskottet koppla in också kommunerna och det lokala räddningsväsendet, Nödcentralsverket och organisationerna inom räddningsbranschen, eftersom dessa har en central roll för medborgarna i produktionen av räddningstjänster och tjänster som anknyter till befolkningsskyddet.

Näringslivets och organisationernas betydelse för den övergripande säkerheten

Myndigheterna, näringslivet och organisationerna i Finland har länge bedrivit ett förtjänstfullt samarbete inom skyddet av samhällets vitala funktioner och utvecklingen av den övergripande säkerheten. Enligt utskottet är det motiverat att det finländska samhället även framgent tillämpar denna beredskapsmodell.

En icke ringa utmaning med tanke på den övergripande säkerheten är det ökande ömsesidiga beroendet. Utsattheten för olika störningar har ökat. Att kritiska funktioner är beroende av informations- och kommunikationsnäten gör samhället allt mer sårbart. Beredskapen för nya typer av hot förutsätter ett brett samarbete och ständig utveckling av samarbetsformerna.

Näringslivet får allt större betydelse när det gäller att säkra samhällets vitala funktioner också på regional och lokal nivå. En allt större del av säkerställandet av samhällets vitala funktioner har lagts över på den privata sektorn. Därigenom får också försörjningsberedskapen en allt större roll för den övergripande säkerheten i samhället. I ljuset av detta behandlar redogörelsen näringslivets roll och försörjningsberedskapen tämligen kursivt.

Enligt redogörelsen är avsikten att statsrådet under våren 2013 ska fatta ett nytt beslut om målen för försörjningsberedskapen. I beslutet ska statsrådet fastställa de närmaste årens särskilda insatsområden, varvid man tar hänsyn till de utmaningar som det nya nätverkssamhällets ökande ömsesidiga beroende medför ur ett såväl nationellt som ett internationellt perspektiv. Det är enligt utskottet nödvändigt att beredskapen på lokal och regional nivå ägnas större uppmärksamhet än tidigare.

Organisationerna spelar en stor roll för att upprätthålla och utveckla den övergripande säkerheten. Utskottet poängterar vikten av ständig dialog mellan myndigheterna och organisationerna i inventeringen av risker och hotbilder samt för att upprätthålla hjälpberedskapen.

En bred beredskap som omfattar olika typer av aktörer förutsätter nya handlingsmodeller och noggrann planering av metoderna och rutinerna.

Av central vikt för samarbetet mellan organisationerna och myndigheterna är att organisationerna får en tydlig roll, t.ex. att man fastställer vilka uppgifter som måste utföras i samband med störningssituationer eller undantagsförhållanden och kommer överens om hur de ska utföras. Andra sätt att förbättra samarbetet mellan organisationerna och myndigheterna är ökad utbildning och medvetenhet om problematiken, medverkan i övningar samt uppdrag som bygger på olika partnerskapsarrangemang. Det väsentliga är att myndigheterna lyckas identifiera och slå fast behoven och avgöra vilka som är de lämpligaste aktörerna.

Ur organisationernas synvinkel är det viktigt att myndigheternas ansvarsfördelning och roller är tydliga, så att organisationerna kan ordna sin egen regionala verksamhet på ett kompatibelt vis. I samband med reformer av den offentliga förvaltningen är det särskilt viktigt att tänka på detta och reservera en tillräckligt lång övergångstid, så att beredskapsnivån inte faller.

Den sociala välfärden och förbättringen av säkerhetskompetensen

Enligt redogörelsen stärks säkerheten också genom att man främjar den samhälleliga välfärden och förebygger spänningar, marginalisering och splittring i samhället. Enligt programmet för den inre säkerheten är marginaliseringen fortsatt den största utmaningen i vardagen. Utskottet ser det som viktigt att detta beaktas då man bereder program som syftar till att utveckla den övergripande säkerheten. Den sociala välfärden bidrar till att stärka den mentala kriståligheten i samhället.

Säkerheten stärks även genom höjd handlingsberedskap hos medborgarnas. Utskottet anser i likhet med redogörelsen att det blir allt viktigare att engagera medborgarna i säkerhetsarbetet och höja befolkningens kunskaper. Enligt redogörelsen utvecklas medborgarnas säkerhetsberedskap genom ökad tillgång till information och förbättrad kvalitet på anvisningarna. Organisationerna har en centrall roll i detta. Utskottet betonar vikten av att förbättra såväl den traditionella säkerhetsberedskapen som de färdigheter som krävs i cyberomgivningen. Förbättrade kunskaper och färdigheter hos medborgarna ger också en allmän känsla av säkerhet.

Enligt inkommen utredning har olika typer av gemenskaper fått allt större betydelse för hur individen klarar sig i störningssituationer. Man bör därför fästa uppmärksamhet vid att utveckla beredskapen hos dessa gemenskaper och vid att intensifiera dialogen mellan dem och myndigheterna. Organisationerna kan ha en central roll i detta sammanhang, men det förutsätter att myndigheterna stödjer denna strävan.

Strategin för cybersäkerheten i Finland

Samarbetsmodell för cybersäkerheten

Den nationella strategin för cybersäkerheten har gjorts upp som ett led i strategin för den övergripande säkerheten i samhället. Samhällets vitala funktioner — och IT-samhället i stort — är beroende av att cyberomgivningen är trygg och driftsäker. Med cyberomgivning avses här en omgivning som är avsedd för hantering av information (data) i elektronisk form och som består av ett eller flera informationssystem. I Finland utgör cyberomgivningen och cybersäkerheten övergripande begrepp som täcker bl.a. informationssäkerhet, nätsäkerhet och datasystemsäkerhet.

Cyberhoten utgör en omfattande och mångförgrenad utmaning för den övergripande säkerheten i samhället. Förändringarna i omvärlden är snabba och effekterna av dem svåra att förutse. Att ha beredskap för hot och kunna avvärja dem förutsätter ännu snabbare, mer transparenta och mer samordnade insatser av alla inblandade. För att stärka cybersäkerheten är det därför nödvändigt att skapa en handlingsmodell för samverkan mellan myndigheterna och de övriga aktörerna.

På högsta nivå leds arbetet inom cybersäkerhet av statsrådet. I överensstämmelse med säkerhetsstrategin för samhället svarar de behöriga myndigheterna för hanteringen av störningssituationer och för beredskapen inför situationerna. Säkerhetskommittén samordnar beredskapen och har tillsyn över verkställandet av strategin för cybersäkerheten. Det är enligt utskottet motiverat att den behörighetsfördelning mellan mi-

nisterierna som tillämpas i säkerhetsstrategin för samhället följs också i frågor som gäller cybersäkerheten.

Enligt strategin för cybersäkerheten baserar sig cybersäkerheten 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. Säkerheten främjas också genom medverkan i övningar. Det väsentliga enligt utskottets mening är att man i strategin beaktar parterna utanför förvaltningen, dvs. näringslivet och organisationerna, och att verkställandet av strategin har kopplingar till dem. Till Finlands styrkor hör en gedigen kunskapsbas och en samarbetstradition som bygger på ömsesidigt förtroende såväl inom förvaltningen som mellan den offentliga och den privata sektorn. Den finländska samarbetsmodellen har rönt uppskattning internationellt. Dessa styrkor utnyttjas i strävan att nå de mål som skrivits in i visionen för cybersäkerheten.

Cybersäkerhetscentret

Handlingsmodellen för cybersäkerheten grundar sig på ett effektivt system för insamling och analys av information, gemensam och delad situationsmedvetenhet samt nationellt och internationellt beredskapssamarbete. För att en sammanställd lägesbild över cybersäkerheten ska kunna produceras och upprätthållas, föreslås det i strategin att det inrättas ett cybersäkerhetscenter. Centret ska betjäna myndigheterna, näringslivet och andra aktörer i utvecklingen av cybersäkerheten. Till stöd för beslutsfattandet ska centret ge statsrådets lägesbildscenter en teknisk lägesbild.

Utskottet bedömer att det nya cybersäkerhetscentret kommer att göra det märkbart enklare att skapa en helhetsbild av cybersäkerheten. De olika myndigheterna har varierande lägesbildsfunktioner beroende på och till stöd för deras egna behov. I dag finns det dock ingen i Finland som producerar och upprätthåller en ständigt aktuell, samlad lägesbild för cybersäkerheten och förmedlar den till dem som behöver en sådan. Cybersäkerhetscentret, som kommer att bygga på Kommunikationsverkets grupp CERT-FI, lämpar sig enligt utskottets uppfattning utmärkt för uppgiften. Centret får stöd genom ett nätverk som omfattar alla sådana myndigheter, företag och andra särskilt utsedda parter som har till uppgift att hålla beredskap inför och reagera på kränkningar mot cybersäkerheten. För att säkra att centret lyckas i sin uppgift är det viktigt att varje förvaltningsområde deltar i samarbetet och bär ansvar inom sin egen sektor.

Faktorer som påverkar cybersäkerheten

Den övergripande säkerheten förutsätter att företag och organisationer med avgörande betydelse för de vitala samhällsfunktionerna utvecklar sin förmåga att upptäcka, avvärja och återhämta sig från cyberhot och störningar som äventyrar vitala funktioner. Merparten av datanäten och informationssystemen och av övrig kritisk infrastruktur drivs av privata krafter. Den privata sektorn har också en central roll i identifieringen och bekämpningen av cyberhot och attacker och i reparationen av uppkomna skador. Försörjningsberedskapsorganisationen stöder beredskapsarbetet och kontinuiteten i näringslivet. Utskottet betonar samtidigt vikten av ett genuint och intensivt samarbete mellan den offentliga och den privata sektorn. Utskottet menar att den handlingsmodell som bygger på strategin för cybersäkerheten ger goda förutsättningar för att utveckla samarbetet.

Ur myndighetsarbetets synvinkel är det viktigt att myndigheternas ansvarsfördelning och roller är tydliga, och att myndigheterna har de befogenheter och resurser de behöver. En av de centrala riktlinjerna i strategin är att klarlägga behovet av att utveckla den nationella lagstiftningen för att säkerställa att den ger myndigheterna och andra aktörer möjlighet att förebygga och avvärja cyberhot och skydda samhällets vitala funktioner. I strategin identifierades bland annat behovet av att hitta balans mellan myndigheternas och näringslivets lägesuppfattning, ansvar och verksamhetssätt. I lagstiftningen om cyberomgivningen bör man också beakta förutsättningarna att utveckla affärsverksamhet. Ut-

skottet konstaterar att en säker cyberomgivning och starkt kunnande höjer de finländska företagens konkurrenskraft ute i världen. Samtidigt blir Finland mer attraktivt och kan locka till sig ny affärsverksamhet.

Utöver att utveckla lagstiftningen och den operativa verksamheten är det nödvändigt att aktörerna har de resurser som krävs för att nå upp till och upprätthålla en tillräckligt hög säkerhetsnivå. I fråga om resurserna konstaterar strategin bara att ministerierna, ämbetsverken och inrättningarna reserverar de resurser som genomförandet av cybersäkerhetsstrategin förutsätter i sina egna verksamhets- och ekonomiplaner. Utskottet påpekar att den allt mer tekniskt komplicerade miljön i ökande grad kräver investeringar i tekniska system och specialkompetens hos medarbetarna. Det är viktigt att förvaltningsområdena reserverar resurser särskilt för cybersäkerheten, med tanke på att den under de närmaste åren utgör ett särskilt insatsområde inom säkerhetspolitiken.

I strategin för cybersäkerheten betonas vikten av att de inblandade förmår upptäcka och avvärja cyberhot samt handla snabbt och effektivt i olika störningssituationer. Däremot har planeringen och implementeringen av systemen enligt säkerhetskraven fått mindre uppmärksamhet. Utskottet vill fästa vikt vid det ansvar de som beställer och implementerar systemen — såväl inom den privata som den offentliga sektorn — har för säkerheten i anslutning till informationssystemen. Säkerheten kostar men vi får inte pruta på den. En stärkt cybersäkerhet kräver också utbildning och kompetenshöjning inom säkerhetsfältet. Utskottet menar att cybersäkerhetens betydelse måste betonas särskilt inom områden som inte direkt har fokus på IT men som hanterar processer och datalager som är viktiga för samhället, t.ex. industriautomation, logistik, handel och förvaltning.

Utskottet hänvisar till lagen om säkerhetsutredning (525/2011), där det finns bestämmelser om olyckor och allvarliga tillbud samt även om exceptionella händelser. Med exceptionell händelse avses bland annat händelser som inte är olyckor men som har hotat eller allvarligt skadat samhälleliga basfunktioner. Syftet med säkerhetsutredningar är att öka den allmänna säkerheten. Däremot görs de inte för att klarlägga rättsligt ansvar. Om ett sådant hot som beskrivs i cybersäkerhetsstrategin realiseras och uppfyller kännetecknen för en exceptionell händelse, ska statsrådet fatta beslut om en säkerhetsutredning och tillsätta en oberoende utredningsgrupp. Enligt utskottets mening är det skäl att ta hänsyn till detta vid verkställandet av strategin.

Bekämpningen av cyberkriminalitet

Nätbrottsligheten har blivit ett mycket omfattande brottsområde och har verkningar för såväl stater som företag och enskilda. Cyberkriminalitet avser dels brott som riktar sig till cyberomgivningen, dels brott som utnyttjar cyberomgivningen. Terrorismen och spionaget väntas under kommande år i allt högre grad flytta över till cybermiljön. Också den traditionella organiserade brottsligheten utnyttjar sårbarheterna i datanät och informationssystem. Allt fler brott av traditionellt slag, t.ex. bedrägerier och industrispionage, sker i cyberomgivning. I denna brottsbekämpning räcker det inte att enbart skydda sig, utan det krävs också att det finns risk för att åka fast och att vinningen av brottet fråntas gärningsmännen.

Vid förebyggandet, utredningen och lämnandet till åtalsprövning av brott är polisen behörig myndighet i samarbete med övriga lagövervakande myndigheter. Det är nödvändigt att polisen har tillräcklig behörighet och tillräckliga resurser samt kunnig och motiverad personal för förebyggandet av brott som riktar sig till eller utnyttjar cyberomgivningen samt för den taktiska förundersökningen samt behandlingen och analyseringen av digitalt bevismaterial på ett rättssäkert sätt. Den ständiga utvecklingen inom IT-tekniken kräver — bland annat — ständig utbildning för att upprätthålla kompetensnivån. Det förutsätter ekonomiska satsningar också på utbildning i utlandet.

Hanteringen av cyberstörningar och utredningen av brott förutsätter vidare ständigt samarbete på nationell och internationell nivå mellan de brottsbekämpande myndigheterna, datasäker-

hetsmyndigheterna och den privata sektorn. Polisen samarbetar nära med Cybersäkerhetscentret när det gäller verkställandet av strategin. IT-kriminaliteten är ofta gränsöverskridande och kräver därför internationellt polisiärt och rättsligt samarbete. Varje EU-land har inrättat nätbrottsenheter som har öppet dygnet runt och bidrar till det internationella samarbetet i bekämpningen av cyberbrottsligheten. I januari 2013 öppnades i anslutning till Europol ett europeiskt center för bekämpning av nätbrott, EC3. Centret ska samla expertisen, stödja undersökningen av brott och främja breda lösningar på EU-nivå. Också Interpol har fått ett särskilt center för cyberfrågor.

Enligt erhållen utredning får polisen kännedom om endast en bråkdel av alla brott som sker i näten. Den främsta orsaken till det förmodas vara att ett företag — eller en privatperson — inte nödvändigtvis är medveten om att ha blivit utsatt för ett nätbrott. En annan orsak är att företagen vill sköta utredningen av intrång i sina datanät på egen hand; möjligen med tanke på negativ publicitet eller av rädsla att affärshemligheter röjs. Polisen har i samarbete med Kommunikationsverket och dataombudsmannens byrå utvecklat rådgivningen och anvisningarna i riktning mot företagen. Tanken är att därigenom hjälpa företagen att skapa bättre beredskap mot nätbrott och minimera den skada fullföljda nätbrott medför. Utskottet menar att verkställandet av den nu aktuella strategin för cybersäkerheten stärker dialogen mellan myndigheterna och företagen samt förbättrar företagens möjligheter att identifiera störningssituationer och reagera snabbt på dem.

Höjd informationssäkerhet inom den offentliga förvaltningen

Utvecklandet av de flesta strategiska cybersäkerhetsuppgifterna och de kapaciteter som är förknippade med dem sammanhänger enligt cybersäkerhetsstrategin också med åtgärder vid och resurser från andra ministerier, region- och lokalförvaltning, näringsliv och organisationer.

Inom den offentliga sektorn pågår stora insatser för att utveckla informationssystemen och höja datasäkerheten. Finansministeriets funktion för den offentliga förvaltningens informations- och kommunikationsteknik (JulkICT) svarar för den allmänna utvecklingen och styrningen av den offentliga förvaltningens informationsförvaltning samt för att främja och säkerställa att den offentliga förvaltningens informationssystem är interoperabla. Som bäst pågår arbetet med en IKT-strategi för den offentliga förvaltningen. Syftet med strategin är bl.a. att reducera riskerna i stora IKT-projekt, förkorta genomförandetiderna för IT-systems- och serviceutvecklingsprojekt samt att underlätta införandet av innovativa eller externt framtagna lösningar inom kommunsektorn och statsförvaltningen. Det förutseende säkerhetsarbetet inom statsförvaltningen styrs av statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen (2009) och av programmet för utveckling av informationssäkerheten inom statsförvaltningen 2011—2015. Ledningsgruppen för informationssäkerheten inom statsförvaltningen (VAHTI) utarbetar anvisningar som stöder verkställigheten av bestämmelserna i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010). Dessutom pågår flera projekt för att höja informationssäkerheten inom statsförvaltningen.

Utskottet fäster uppmärksamhet vid att det i de preliminära utredningarna om kommunernas beredskap har konstaterats att telekommunikationen utgör en kritisk faktor i såväl normala förhållanden som vid sådana störningssituationer och undantagsförhållanden som avses i samhällets säkerhetsstrategi. De åtgärdsförslag som ingår i den kommande IKT-strategin för den offentliga förvaltningen omfattar bland annat en utredning av förutsättningarna för ett gemensamt datanät för den offentliga förvaltningen. Ett perspektiv i utredningen skulle vara hur man kan skapa förutsättningar för kommunerna att ha beredskap för att kostnadseffektivt avvärja olika typer av utifrån kommande hot. Kommunerna svarar för ordnandet av omsorgen och många andra vitala samhällsfunktioner. Det är enligt utskottet viktigt att kommunerna och de kommunala säkerhetsmyndigheterna engageras i plane-

ringen av informationssäkerheten, så att de lokala aktörernas behov och resurser inom beredskapen för normala förhållanden och undantagsförhållanden kan beaktas. Det finns också anledning att tänka på att kommunerna och samkommunerna får anvisningar och föreskrifter av flera olika ministerier, vilket understryker vikten av ett samordnande grepp.

Internationellt samarbete och Europeiska unionens cybersäkerhetsstrategi

I strävan att stärka den nationella cybersäkerheten och utveckla kompetensen inom detta fält är det viktigt att Finland och finländska krafter är aktiva i de internationella organisationerna och samarbetsforumen. Finland har självt mycket att ge inom detta område.

En central referensram för Finland är Europeiska unionen, som blivit allt mer aktivt inom cybersäkerheten och som också samarbetar med tredjeländer. Vidare betonar utskottet det nordiska samarbetets roll i arbetet för ökad cybersäkerhet. Euroepiska unionen har utarbetat en cybersäkerhetsstrategi, och avsikten är att rådets slutsatser ska läggas fram ännu under Irlands ordförandeskap. Kommissionen har även gett ett förslag till direktiv om nät- och informationssäkerhet. Europeiska unionens cybersäkerhetsstrategi anlägger ett övergripande grepp som täcker samtliga sektorer och aktörer som är centrala med tanke på cybersäkerheten. Utskottet anser att det är ett motiverat angreppssätt. Det är särskilt viktigt att betona hur viktigt samarbetet mellan den offentliga och den privata sektorn är. Utskottet anser att riktlinjerna i Finlands strategi för cybersäkerheten också stöder Europeiska unionens cybersäkerhetsstrategi.

Ställningstagande

Förvaltningsutskottet föreslår

att lagutskottet beaktar det som sägs ovan.

Helsingfors den 2 april 2013

I den avgörande behandlingen deltog

ordf. Pirkko Mattila /saf
medl. Rakel Hiltunen /sd
Reijo Hongisto /saf
Risto Kalliorinne /vänst
Elsi Katainen /cent
Timo V. Korhonen /cent
Antti Lindtman /sd
Markus Lohi /cent
Outi Mäkelä /saml
Tapani Mäkinen /saml
Markku Mäntymaa /saml
Osmo Soininvaara /gröna
Ulla-Maj Wideroos /sv.

Sekreterare var

utskottsråd Minna-Liisa Rinne.