Kommittédirektiv

Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system

Dir. 2013:110

Beslut vid regeringssammanträde den 28 november 2013

Sammanfattning

En särskild utredare ges i uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Utredaren ska då

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system,
- föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur,
- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt av sådana som används i förslaget till nationell strategi, och
- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och gällande ekonomiska ramar. De begrepp eller benämningar som används i dessa direktiv ska inte föregripa eller begränsa utredarens arbete.

Uppdraget ska redovisas senast den 1 december 2014.

Bakgrund

Samhällets informationssäkerhet

Målen för Sveriges säkerhet är att värna befolkningens liv och hälsa, samhällets funktionalitet samt vår förmåga att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (propositionen Ett användbart försvar, prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Det finns ingen motsättning mellan frihet och säkerhet utan dessa är ömsesidigt förstärkande. Med utgångspunkt i dessa övergripande mål för vår säkerhet är målen för arbetet med samhällets krisberedskap att minska risker för, och konsekvenser av, allvarliga störningar, kriser och olyckor. Skulle en sådan händelse inträffa bör människors liv, personliga säkerhet och hälsa tryggas samt skador på egendom och miljö begränsas (budgetpropositionen för 2013, prop. 2012/13:1 utg.omr. 6, bet. 2012/13:FöU1, rskr. 2012/13:93-95).

All verksamhet är i dag beroende av fungerande informationssystem. Våra nätverk och system behöver vara säkra och stabila över tid. Näringslivet, offentlig förvaltning och medborgarna måste känna tillit till att de digitala tjänsterna i samhället fungerar. Näringslivet har en betydelsefull roll som den största ägaren och förvaltaren av samhällsviktig informationsinfrastruktur. Konsekvenserna av en allvarlig it-incident skulle med stor sannolikhet genom bl.a. spridningseffekter kunna drabba samhällsviktig verksamhet i flera sektorer. Informationssäkerhet berör således många olika verksamhetsområden bl.a. säkerhets- och utrikespolitiken, försvarspolitiken, näringsfrågor, socialfrågor och brotts-bekämpning. För att nå målen för Sveriges säkerhet är det mot denna bakgrund viktigt att ett systematiskt informations-säkerhetsarbete genomförs på bred front i samhället.

Informationssäkerhet bör vara väl integrerat i arbetet med risk-, sårbarhets- och säkerhetsanalyser. Analyserna behandlar bl.a. samhällets förmåga att motstå och hantera allvarliga händelser och verksamheters ömsesidiga beroendeförhållanden.

Förmåga att hantera it-angrepp är nödvändig främst för att minska risken för, och konsekvenser av, allvarliga it-incidenter som drabbar samhällsviktig verksamhet och kritiska infrastruktursystem. Allvarliga it-incidenter som drabbar dessa system och även förluster av mindre mängder information över tid, kan medföra allvarliga konsekvenser och stora kostnader för samhället oavsett om det sker genom medvetna angrepp, misstag eller av olycka.

Ökad digitalisering

Informationsteknikens utveckling har medfört nya former av kommunikation, datahantering och datalagring vilket också innebär nya former för interaktion mellan individer, organisationer och stater. I allt väsentligt är detta en positiv utveckling. Samtidigt medför it-utvecklingen ett större beroende mellan olika sektorer och verksamheter och därmed också ökade sårbarheter. Detta har utvecklats till en av vår tids mest komplexa frågor.

En ökande hantering av personinformation i informationssystem medför också behov av funktioner för att tillgodose den personliga integriteten.

Den 29 september 2011 beslutade regeringen om *It i människans tjänst – en digital agenda för Sverige*, (N II 2, N2011/342/ITP, m.fl.). Av detta beslut framgår regeringens mål att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Detta mål har också antagits av riksdagen (budgetpropositionen för 2012, prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87).

Den 13 december 2012 beslutade regeringen om *Med medborgaren i centrum. Regeringens strategi för en digitalt samverkande statsförvaltning*, (N II 10, N2012/6402/ITP m.fl.). Genom att samverka digitalt kan myndigheternas kontakter med medborgarna förenklas, innovation och delaktighet stödjas, samtidigt som statsförvaltningens effektivitet och kvalitet ytterligare kan höjas. En viktig utgångspunkt i all utveckling av statsförvaltningens tjänster är att effektivitet och service alltid måste vägas mot skyddet för den enskildes integritet och behov

av sekretesskydd och att medborgarna har tillit till att systemen är säkra.

I dag utgör säkerhet, öppenhet och integritet kopplat till informationssäkerhet en stor utmaning såväl nationellt som internationellt. En allvarlig it-incident, men även långvariga oupptäckta informationsförluster, bedöms kunna få stora konsekvenser för den svenska ekonomin, för samhällsviktig verksamhet, kritisk infrastruktur och för enskilda individer.

Internet används för både civila och militära ändamål och såväl staters som individers och organisationers säkerhet måste tillgodoses. Handel, immaterialrätt, tekniköverföring, nätsäkerhet, frågor om kritisk infrastruktur, demokrati, mänskliga rättigheter, bistånd och it-brott hänger samman med säkerhetspolitiska och försvarspolitiska överväganden och utgör delar av samma problemkomplex. Det medför att en ansats att hantera problem inom området bör koppla samman dessa frågeställningar.

Hot mot elektroniska kommunikationsnät och it-system

Hoten mot elektroniska kommunikationsnät och it-system är mångfacetterade, komplexa, svårdefinierade och föränderliga. Hot utgörs av allt ifrån tekniska fel till den mänskliga faktorn och medvetna handlingar. Utöver detta är det inte ovanligt att t.ex. väderfenomen, naturkatastrofer och olyckor orsakar incidenter med it-inslag.

It-angrepp kan utgöras av intrång som syftar till att störa funktionaliteten, förändra, stjäla eller manipulera information eller helt ta över ett informationssystem. It-angrepp mot samhällsviktig verksamhet och kritisk infrastruktur, såväl statlig som privat, kan också syfta till att begränsa tillgången till information eller funktioner. Ett exempel på sådana angrepp är överbelastningsattacker. En aktör kan också via it-angrepp störa, slå ut eller skaffa sig tillgång till styr- och kontrollsystem samt ledningscentraler för samhällsviktig verksamhet och kritiska infrastrukturer, exempelvis telenät, elnät, transportsystem, finanssystem, va-verk, processindustrier eller militära ledningssystem. Sådana it-angrepp kan förekomma såväl i

fredstid som under kris eller krig och kan användas för att komplettera konventionella militära förmågor. Utvecklingen av militära it-förmågor internationellt innebär att även Sverige måste förhålla sig till nya krav på hur man försvarar sig mot en motståndare som har tillgång till sådana förmågor.

Det sker en ansenlig mängd brottsliga angrepp inriktade på att kompromettera informationssystem för att otillbörligen komma åt information. Spionage sker i ökad omfattning och utförs såväl av stater som av organisationer och enskilda.

Det är tydligt att verksamhetskritisk och känslig information inom både det offentliga och det privata är potentiella mål för olika typer av angrepp. Ett annat hot är att ökande krav på säkerhetsåtgärder i elektroniska kommunikationsnät, it-system och på internet riskerar att leda till inskränkningar av mänskliga rättigheter med stora politiska, sociala och ekonomiska konsekvenser som följd. Särskilt på det internationella planet är detta en oroväckande trend som ofta grundar sig i olika definitioner av begreppet säkerhet och där vissa regimer använder säkerhet som skäl för att kontrollera den egna befolkningen.

Ansvar och samverkan mellan samhällsaktörer

Att öka förmågan att förebygga och hantera allvarliga it-incidenter som drabbar samhällsviktig verksamhet är inte en uppgift för en enskild aktör eller myndighet utan något som privata och offentliga aktörer tillsammans bör bidra till. Nationell och internationell samverkan mellan militära och civila statliga myndigheter, inklusive försvarsunderrättelse-verksamheten, och med kommuner och landsting är en förutsättning för att kunna förebygga, förhindra och hantera dessa risker. Övningar är ett viktigt instrument för att förbättra förutsättningarna för samverkan samt att identifiera, åtgärda och förebygga brister.

Grunden för samhällets krisberedskap är ansvarsprincipen (propositionen Stärkt krisberedskap – för säkerhets skull, prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193-194). Det innebär att den som har ansvar för en verksamhet under normala

förhållanden också har det under allvarliga händelser, kriser eller krig. I ansvarsprincipen ingår även att samverka och samordna sig med andra aktörer i den omfattning som krävs för att effektivt förebygga och hantera en allvarlig händelse.

Internationellt

It-utvecklingen utmanar många traditionella föreställningar om säkerhetspolitikens omfattning, aktörer och logik. Ökat beroende av elektroniska kommunikationsnät och it-system förutsätter internationell samverkan. Internationellt är det viktigt att Sverige har en tydlig inriktning på området för att kunna påverka den säkerhetspolitiska utvecklingen. En stor utmaning i arbetet är staters skilda syn på hotbilder, doktriner och definitioner kopplade till informationssäkerhet. En tydlig skiljelinje är staters olika syn på hur grundläggande mänskliga rättigheter som yttrandefrihet förhåller sig till nationellt definierade säkerhets- och suveränitetsaspekter. För att alla på bästa sätt ska kunna nyttja de möjligheter som informationstekniken ger behöver frihet, öppenhet och säkerhet för användarna baserat på rättsstatsprincipen utgöra en självklar grund för informationssäkerhetsarbetet.

Att kunna upprätthålla en öppen, säker, motståndskraftig och tillförlitlig elektronisk kommunikationsmiljö är betydelsefullt för alla länder, och säkerheten för Sverige är beroende av den globala utvecklingen.

I strategin för Europeiska unionens inre säkerhet (ISS) konstateras att it-brottslighet är ett hot särskilt mot medlemsstaternas informationssystem. EU-kommissionen och utrikestjänsten (EEAS) har presenterat en övergripande europeisk cybersäkerhetsstrategi som berör både EU-interna som EU-externa aspekter av it-frågor (JOIN(2013) 1 final). Den digitala agendan för Europa ägnar ett avsnitt åt it-brottslighet och it-attacker mot informationssystem samt ett avsnitt om tillit och säkerhet. OECD-länderna har antagit flera rekommendationer som berör informationssäkerhet och internetpolicy. Organisationen genomför också analyser av området, bl.a. av

nationella informationssäkerhetsstrategier som under senare år antagits i ett flertal länder.

Uppdraget

Föreslå en strategi och mål för samhällets informationssäkerhet

Myndigheternas arbete med informationssäkerhet ska bedrivas utifrån en nationell strategi som tar sin utgångspunkt i att värna befolkningens liv och hälsa, samhällets funktionalitet samt förmågan att upprätthålla grundläggande värden som demokrati, rättsäkerhet och mänskliga fri- och rättigheter. Att stärka samhällets säkerhet kräver att skyddsvärden, hot och skyddsmedel ses i ett sammanhang. Denna helhetssyn bör genomsyra verksamhet över hela kedjan från orsaksförebyggande och sårbarhetsreducerade till hanterande och återuppbyggande verksamhet.

Informationssäkerhet är en betydelsefull del i arbetet med att nå målen för Sveriges säkerhet och samhällets krisberedskap. Därför bör arbetet med att stärka informationssäkerheten vara en del av det allmänna säkerhets- och krisberedskapsarbetet. För att hålla samman såväl det nationella som det internationella arbetet inom informationssäkerhetsområdet och för att nå Sveriges politiska mål är det viktigt med en nationell strategi som bl.a. tar sin utgångspunkt i en bred säkerhetspolitisk kontext. Strategin ska ta sin utgångspunkt i målen för Sveriges säkerhet och målen för samhällets krisberedskap.

Strategin ska utgå från, och även kunna bidra till, fortsatt utveckling av politiska prioriteringar på området. Strategin ska innehålla övergripande mål samt utgångspunkter för hur aktörer i samhället ska samverka i arbetet med att förebygga, upptäcka, ingripa mot och agera i samband med allvarliga it-incidenter som drabbar samhällsviktig verksamhet.

De övergripande målen ska utformas så att de ger mål, riktlinjer för och prioriteringar som kan ligga till grund för myndigheternas eget informationssäkerhetsarbete. Utredaren ska ta hänsyn till den internationella samverkan som existerar

på området, åtaganden som ålagts Sverige till följd av internationella konventioner samt Sveriges förpliktelser som EU-medlem. Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och it-system ska ses som ett övergripande sammanhållet ramverk för hur arbetet med informationssäkerhet ska bedrivas i Sverige. Det förutsätts att mer nedbrutna detaljerade riktlinjer och handlingsplaner skapas för delområden och sektorer i samhället inklusive det militära försvaret och försvars-underrättelseverksamheten.

Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och it-system ska hantera risker på alla nivåer i samhället. Informations-säkerhetsområdet är tvärsektoriellt och omfattar många aktörer i samhället på lokal, regional och central nivå. Även näringslivet har en stor roll i detta arbete. Till detta kommer också den internationella dimensionen där olika aspekter måste beaktas. Den nationella strategin bör inkludera alla relevanta aspekter och aktörer.

Syftet med strategin ska vara att uppnå ett effektivare och mer samordnat arbete med informationssäkerhet i samhället. Strategin ska vara ett stöd för myndigheternas arbete och kopplas till styrmedel och åtgärder för att åstadkomma ett operativt och verksamt arbete med informationssäkerhet i hela samhället. Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och gällande ekonomiska ramar.

Utredaren ska

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system och
- föreslå övergripande mål för samhällets informations-säkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur.

Inför arbetet med strategin ska utredaren ta del av de nationella strategier som redan tagits fram av ett flertal länder. Utredaren ska också beakta det arbete som sker på informations-säkerhetsområdet inom bl.a. EU, Nato och OECD.

Definiera begrepp inom området

Uttrycket informationssäkerhet används bl.a. i regeringens propositioner, skrivelser och i vissa författningar, t.ex. myndighetsinstruktioner. Internationellt förekommer ”information security” och ”cyber security”. Dessa uttryck används delvis med överlappande betydelse, delvis med olika betydelse utifrån skilda utgångspunkter.

Informationssäkerhet är enligt terminologi för informationssäkerhet (SIS handbok 550 utgåva 3) säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även ansvarighet och oavvislighet).

Informationssäkerhet är även ett legaldefinierat begrepp i säkerhetsskyddslagen (1996:627) där det finns bestämmelser om informationssäkerhet till skydd för rikets säkerhet. Säkerhetsskyddslagstiftningen är för närvarande under översyn och utredningen ska redovisa sitt uppdrag i april 2014 (dir. 2011:94).

Mot bakgrund av en ökad internationalisering och behov av interoperabilitet är även en jämförelse med andra nationer och organisationers syn på definitioner viktig. En särskild utmaning är staters skilda syn på hotbilder, regleringsbehov m.m. inom området som lett till skillnader i definitioner och begreppsanvändning. Begreppet informationssäkerhet kopplas av vissa länder till censur och statlig kontroll av medborgarna.

På senare tid har även andra begrepp börjat användas i det svenska språket, framför allt cybersäkerhet och cyberförsvar men även benämningar som digital säkerhet och it-säkerhet förekommer utan att den närmare innebörden av dessa förklarats.

Det finns således ett behov av att definiera begrepp och reda ut hur de förhåller sig till varandra samt vid behov ensa dessa begrepp för att undvika missförstånd. De begrepp eller benämningar som används i dessa kommittédirektiv ska inte föregripa eller begränsa utredarens arbete i detta avseende.

Utredaren ska

- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt sådana som används i förslaget till nationell strategi.

Utredningsuppdraget omfattar inte att föreslå förtydligande definitioner av begrepp som används inom ramen för säkerhetsskyddslagstiftningen.

Redovisa roller och ansvar på området

Grunden för samhällets krisberedskap är ansvarsprincipen. Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informationssäkerhetsområdet, såväl nationellt som internationellt, och frågorna spänner över en mängd olika områden och nivåer. De statliga myndigheterna bör utveckla sin förmåga att samverka inom informationssäkerhetsområdet. För att underlätta denna förmåga behövs en enhetlig och samlad beskrivning av respektive myndighets ansvar och roll utifrån dagens uppgifter och uppdrag på informationssäkerhetsområdet.

Utredaren ska

- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Konsekvensbeskrivningar

Utredaren ska beskriva eventuella konsekvenser av sina förslag för statliga myndigheter, landsting, kommuner och andra relevanta aktörer som kan beröras.

Om förslagen påverkar kostnaderna eller intäkterna för staten, landstingen, kommunerna eller enskilda ska en beräkning av dessa konsekvenser redovisas och utredaren föreslå finansiering för detta. Om förslagen får samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, landstingen eller kommunerna ska utredaren föreslå en

finansiering. Sådan finansiering ska föreslås ske inom området och gällande ekonomiska ramar.

Om något av förslagen påverkar det kommunala självstyret ska utredaren särskilt redovisa dessa konsekvenser och de särskilda avvägningar som lett till förslagen, i enlighet med bestämmelserna i 14 kap. 2 och 3 §§ regeringsformen.

Samråd och redovisning av uppdraget

Utredaren ska löpande hålla Regeringskansliet (Försvarsdepartementet) informerat.

Vidare ska utredaren hålla sig informerad om och beakta relevant arbete om informationssäkerhetsfrågor som pågår inom Regeringskansliet och i utredningar, som t.ex. Försvarsberedningens arbete. Utredaren ska även hålla sig informerad om och beakta Utredningen om säkerhetsskyddslagen (Ju 2011:14), Utredningen om förbättrad tillgång till personuppgifter inom och mellan hälso- och sjukvården och socialtjänsten (S 2011:13), Sveriges Kommuner och Landstings insatser inom området eSamhället, den Digitala agendan för Sverige, e-förvaltningsstrategin, den europeiska cybersäkerhetsstrategin, kommissionens förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (COM (2013) 48 final), det arbete som pågår inom ramen för regeringens arbete med EU:s digitala agenda, e-förvaltning och allmän uppgiftsskyddsförordning (COM(2012) 11 final) samt andra relevanta internationella dokument. I det fall EU beslutar om direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen ska det beaktas i arbetet med strategin. Utredaren ska också beakta andra länders samt nationella och internationella organisationers strategier för informationssäkerhet. Utredaren bör även beakta nuvarande politik som bedrivs på området.

Uppdraget ska redovisas senast den 1 december 2014.

(Försvarsdepartementet)