Försvarsutskottets yttrande 1999/2000:FöU5y

Ett informationssamhälle för alla

1999/2000
FöU5y

Till trafikutskottet

Trafikutskottet har berett försvarsutskottet tillfälle att yttra sig över proposition 1999/2000:86 *Ett informationssamhälle för alla,* jämte motioner.

Försvarsutskottet

Regeringens överväganden och förslag

Regeringen anser att regler och system på IT-området bör vara sådana att de skapar förtroende genom att vara

- säkra, förutsägbara och teknikneutrala,
- internationella,
- skydda individens integritet.

Det finns *olika begrepp* som beskriver säkerhet kring elektronisk informationshantering. Informationssäkerhet, som är det övergripande begreppet, omfattar IT-säkerhet (traditionell datasäkerhet) och administrativ säkerhet som är relaterad till hantering av information i olika verksamheter.

Begreppet IT-säkerhet används för att beskriva skydd av information i informationsbehandlande tekniska system. IT-säkerhet kan delas upp i ADB-säkerhet (bearbetning och lagring) och kommunikationssäkerhet.

Fortsättningsvis kommer huvudsakligen det vidare begreppet informationssäkerhet att användas. I följande avsnitt behandlas även ämnesområdet informationsoperationer. Informationsoperationer är samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. Det kan ske genom att utnyttja egen information och egna informationssystem samtidigt som dessa också måste skyddas. Ett viktigt inslag är att påverka beslutsprocesser och beslutsfattande.

Det finns både *offensiva* och defensiva informationsoperationer. De genomförs i politiska, ekonomiska och militära sammanhang. Exempel på informationsoperationer är t.ex. informationskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.

Defensiva informationsoperationer är samordnade och samlade åtgärder i fred, kris och krig avseende policy, operationer, personal och teknik för att

skydda och försvara information, informationssystem och förmåga till rationellt beslutsfattande.

Regeringens förslag

Regeringens förslag är att ansvaret för informationssäkerheten även fortsättningsvis skall ligga hos de myndigheter, företag och organisationer som har det normala verksamhetsansvaret.

Enligt *regeringens bedömning* bör för den närmaste framtiden tre områden prioriteras: skydd mot informationsoperationer, ett säkrare Internet samt elektroniska signaturer och annan säkerhetsteknik. En tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring bör utformas.

Bakgrunden till regeringens förslag är att riksdagen med anledning av 1996 års IT-proposition gav regeringen till känna sin syn på behovet av ett mer samlande och samordnande ansvar för IT-säkerhetsfrågorna än för närvarande (bet. 1995/96:TU19, rskr. 1995/96:282). I det sammanhanget skulle behovet av att koordinera Sveriges medverkan i det internationella IT-säkerhetsarbetet beaktas. Riksdagen ansåg vidare att regeringen skulle återkomma till riksdagen med en utvecklad strategi på IT-säkerhetsområdet, där regeringen preciserar statens ansvar och anger hur säkerhetsarbetet inordnas i det nationella handlingsprogrammet för IT samt hur säkerhetsarbetet bör organiseras.

Regeringens syn på arbetet har breddats från IT-säkerhet till informationssäkerhet och informationsoperationer. Under år 1999 har regeringen behandlat informationsoperationer och informationssäkerhet i propositionerna Förändrad omvärld – omdanat försvar (prop. 1998/99:74) och Det nya försvaret (prop. 1999/2000:30).

Arbetet med att organisera ett mer samlande och samordnande ansvar för informationssäkerhetsfrågor

Regeringen har i propositionen Det nya försvaret (prop. 1999/2000:30) konstaterat att informationssäkerhetsarbetet måste ske hos de myndigheter, företag och organisationer som har det normala verksamhetsansvaret. Att respektive myndighet vidtar åtgärder för att säkerställa detta faller därmed inom ramen för det departements ansvarsområde under vilket myndigheten etc. lyder.

Sedan riksdagen begärde att regeringen ytterligare skulle samla och samordna arbetet inom IT-säkerhetsområdet (prop. 1995/96:125, bet. 1995/96:TU19, rskr. 1995/96:282) har frågan breddats och flera utredningar har belyst området. Såväl arbetsgruppen om informationskrigföring och Statskontoret har i rapporter understrukit vikten av en bättre samordning av IT-säkerhetsarbetet och skyddet mot informationskrigföring.

Regeringen delar utredningarnas bedömningar att *samordningen behöver förbättras*. Frågan om vad samordningsansvaret bör omfatta, och hur det skall organiseras, behandlas *inom ramen för en utredning* om det civila försvaret och beredskapen mot svåra påfrestningar på samhället i fred. Regeringen har beslutat om direktiv (dir. 1999:63) för en särskild utredare med

uppgift att lämna förslag till principer för att åstadkomma en förbättrad helhetssyn när det gäller planeringen för civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred.

Utredaren skall bl.a., efter analys av nuvarande ansvars- och rollfördelning, föreslå hur utformningen av en tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring bör utformas. Det är naturligt att i detta samarbete beakta frågan om Sveriges medverkan i det internationella arbetet inom området.

Ansvarsfördelning

I dag ingår IT-system eller ett beroende av IT-system i nästan all verksamhet i samhället. Arbetet med IT-omställningen inför år 2000 har tydligt visat detta. I dagens samhälle är det i princip omöjligt att urskilja informationssystem och därmed informationssäkerheten ur den dagliga verksamheten.

Vad gäller verksamhetsansvar, att varje myndighet ansvarar för den egna verksamhetens informationssäkerhet, finner regeringen att Statskontorets förslag är vad som gäller för närvarande och ser ingen anledning att ändra detta. Varje myndighet har ett självständigt förvaltningsansvar.

Utöver detta uppmärksammas informationssäkerhetsfrågorna alltmer både i totalförsvarsplanering och när det gäller beredskapen för svåra påfrestningar på samhället i fred.

Staten ställer krav på myndigheter som skall kunna bedriva verksamhet under höjd beredskap genom beredskapsförordningen. Detta innebär att myndigheterna måste ha fungerande system även i fred.

Informationssäkerhetsarbetet i det nationella handlingsprogrammet

För den närmaste framtiden har regeringen valt att i det nationella handlingsprogrammet prioritera tre områden:

- skydd mot informationsoperationer,
- ett säkrare Internet samt
- elektroniska signaturer och annan säkerhetsteknik.

Regeringen kommer även fortsättningsvis att följa utvecklingen inom området och vid behov prioritera nya eller andra områden i informationssäkerhetsarbetet.

Skydd mot informationsoperationer

Regeringens arbete med informationssäkerhet bör bl.a. syfta till att *öka skyddet mot informationsoperationer.*

Det är nödvändigt med ett fortsatt och fördjupat arbete kring frågor som rör skyddet mot informationsoperationer, informationssäkerhet och IT-säkerhet. Gränsdragningen mellan vad som är att betrakta som åtgärder för att motstå informationskrigföring (eller andra informationsoperationer) och

åtgärder för att öka IT-säkerheten är enligt regeringen diffus. Utvecklingen inom området informationskrigföring ställer ökade krav på den grundläggande IT-säkerheten i samhället.

Det är viktigt för Sverige att aktivt stödja internationella avtal och regler inom detta område som snabbt internationaliseras. Informationsoperationer och informationskrigföring har bl.a. behandlats i Förenta nationerna, en G8-kommitté och i EU:s ministerråd.

Ett säkrare Internet

Regeringens arbete skall bidra till ett säkrare Internet. Regeringen anser att ett säkrare Internet skulle innebära en snabb och effektiv höjning av säkerheten för många aktörer i samhället.

Under de senaste åren har användningen av Internet ökat mycket kraftigt. Stora grupper av användare har blivit beroende av Internet som kommunikations- och informationsväg. Informationsutbytet mellan myndigheter, företag och medborgare ökar dramatiskt. Myndigheter och företag använder i allt större utsträckning elektroniska tjänster och Internet för tjänster och förmedling av information. Alltfler hushåll använder Internet för att kommunicera med varandra, med myndigheter, med sina arbetsplatser och med företag. Regeringen menar att *en säker infrastruktur för Internet* utgör en viktig del i arbetet med samhällets informationssäkerhet.

Elektroniska signaturer och annan säkerhetsteknik

Med den ökande kommunikationen ökar exponeringen av den information som hanteras. Hoten mot informationssystemen och kraven på säkerheten i dessa ökar och ändrar karaktär.

Den ökade användningen av elektronisk kommunikation innebär krav på system som medger säker identifiering, att ett meddelande inte har förändrats under överföringen, samt att man skall kunna skydda information från insyn. För att uppnå detta kan olika former av krypteringsteknik användas.

Staten kan skapa förutsättningar för en ökad användning av säkerhetsteknik genom att undanröja eventuella legala hinder. Det är viktigt att den offentliga förvaltningen med gemensamma ansträngningar börjar använda system för säker elektronisk kommunikation och driver på denna utveckling i samhället. Regeringen anser att användning av krypteringsteknik för att åstadkomma säkra elektroniska kommunikationer utgör en viktig del av arbetet för att förbättra samhällets informationssäkerhet.

Motionerna

Moderata samlingspartiet anser i *motion T28 (m parti)* att säkerhetsmedvetandet är lågt i såväl offentlig som privat sektor. Den enda metod som står till buds för att skapa säkerhet i en öppen digital miljö som Internet är användning av kryptering. Med stark kryptering når signaturer och nycklar den säkerhetsnivå som det digitala samhället behöver.

Sverige bör under sitt ordförandeskap i EU ta initiativ till en konferens om åtgärder och arbete i Europa för att skydda den kritiska digitala infrastrukturen. Elektroniska signaturer är en viktig beståndsdel i de elektroniska affärerna, men förtroendet för och bruket av dessa uppstår inte via lagstiftning.

Kristdemokraterna delar i *motion T24 (kd kommitté)* regeringens uppfattning att den myndighet eller organisation som har verksamhetsansvar också ansvarar för informationssäkerheten. Det innebär inte att regeringen saknar ett sammanhållande ansvar för att koordinera det internationella IT-säkerhetsarbetet. Regeringen bör snarast ta initiativ med anledning av Domännamnsutredningens förslag samt påskynda arbetet med elektroniska signaturer.

Folkpartiet liberalerna anser i *motion T29 (fp kommitté)* att det är viktigt att känslig information hanteras på ett sådant sätt att riskerna för intrång i personlig och affärsmässig integritet blir så små som möjligt. Regeringens förslag till ansvar för informationssäkerheten är lika rimligt som okontroversiellt; informationssäkerheten kan inte betraktas som något annat än en normal del av verksamheten. Folkpartiet föreslår *(yrkande 1*) att det skall ställas krav på revision av IT-säkerheten på alla myndigheter som hanterar information som är känslig för enskilda, företag, organisationer eller för samhället i stort. IT-revisionen bör utföras av experter som är fristående från de myndigheter som granskas.

I *motion T25* av Bengt-Göran Hansson (s) betonas att behovet av ett sammanhållande organ för säkerhetsfrågor kommer att öka mycket kraftigt ju fler som blir användare och ju snabbare den tekniska utvecklingen blir. Skall regering och riksdag kunna hålla jämna steg med den mycket snabba utvecklingen blir det nödvändigt att myndigheter, organisationer och företag i Sverige snarast bildar ett IT-institut för utveckling och säkerhet, samt att någon statlig myndighet får till ansvar att vara samordnare i säkerhetsfrågor.

Försvarsutskottets överväganden

Hotet mot informationssamhället har fått ökad betydelse i takt med att samhällsviktiga system och funktioner blir beroende av informationsteknik. Den internationella utvecklingen inom området har tydligt visat *att hela samhället berörs* – inte bara den offentliga förvaltningen. Hela samhällets beroende och dess sårbarhet har därför även en stor säkerhetspolitisk betydelse. Utgångspunkten för beredskap och skyddsåtgärder är inte primärt knutet till skyddet av Sveriges territorium utan i högre grad till behovet att skydda svenska intressen och nationella tillgångar, t.ex. en funktionssäker samhällsviktig infrastruktur, såväl i fred som i kris och krig. En nationell samordning och ett sektorsövergripande ansvar för planering och exekutiva åtgärder blir därmed nödvändigt.

*Regeringe*n pekar i propositionen på att det finns både offensiva och defensiva informationsoperationer. De genomförs i politiska, ekonomiska och militära sammanhang. Exempel på informationsoperationer är t.ex. informat-

ionskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.

Enligt försvarsutskottets mening behöver begreppen i den säkerhetspolitiska dimensionen utvecklas. Sålunda bör man skilja på *informationsoperationer* å ena sidan och *informationskrigföring* i kris och krig å den andra sidan. Informationsoperationer kan förekomma i hela spektrumet fred–kris–krig medan informationskrigföring enligt utskottets mening är en militär aktivitet riktad mot vårt militära försvar och därmed i huvudsak är Försvarsmaktens ansvar.

I sitt yttrande (1995/96:FöU4y) över 1996 års IT-proposition till trafikutskottet framhöll *försvarsutskottet* att det saknades ett uttalat samlat ansvar för sårbarhets- och säkerhetsaspekterna på departements- eller myndighetsnivå för informationstekniken. Ett betydande antal myndigheter inom staten har viktiga uppgifter och stor kompetens inom IT-säkerhetsområdet – var och en dock inom sitt speciella ansvarsområde. Ingen myndighet har emellertid av regeringen getts ett sammanhållet ansvar för helheten och för att ha en samlad överblick inom området. Försvarsutskottet anförde mot denna bakgrund följande:

– Utskottet anser för sin del att den av regeringen aviserade arbetsgruppen för att följa hot- och sårbarhetsaspekterna är otillräcklig med hänsyn till de krav som numera bör ställas, dels mot bakgrund av vad riksdagen uttalat under 1987/88 års riksmöte, dels mot bakgrund av den vidgade hotbilden och den betydelse som samhällets infrastruktur har både i fred, kriser och i krig – särskilt lednings- och informationssystemen. Regeringen har anledning att inför propositionen om 1996 års försvarsbeslut på nytt överväga frågorna om informationsteknikens särskilda betydelse för totalförsvaret och hur en hög säkerhet för denna skall ordnas redan i fred. Utskottet har vidare inhämtat att regeringen under hösten 1996 avser att genom en proposition lämna riksdagen förslag i anledning av Hot- och riskutredningens förslag. Med hänsyn till ämnets särskilda betydelse förordar utskottet emellertid att riksdagen ger regeringen i uppdrag att organisera ett mer samlande och samordnande ansvar för IT-säkerhetsfrågorna än för närvarande. I det sammanhanget bör behovet av att koordinera Sveriges medverkan i det internationella IT-säkerhetsarbetet beaktas. Utskottet anser vidare att regeringen bör återkomma till riksdagen med en utvecklad strategi på IT-säkerhetsområdet, där regeringen preciserar statens ansvar och anger hur säkerhetsarbetet inordnas i det nationella handlingsprogrammet för IT samt hur säkerhetsarbetet bör organiseras. Vad utskottet nu har anfört bör riksdagen som sin mening ge regeringen till känna.

Trafikutskottet delade försvarsutskottets uppfattning att informationstekniken har genomgripande effekter på samhällets säkerhet och sårbarhet. Enligt trafikutskottets uppfattning borde därför riksdagen som sin mening ge regeringen till känna vad försvarsutskottet i sitt yttrande anfört dels om organisationen av ett mer samlande och samordnande ansvar för IT-säkerhetsfrågorna, dels om att regeringen bör återkomma till riksdagen med en utvecklad strategi på området.

Försvarsutskottet anslöt sig i samband med den *säkerhetspolitiska kontrollstationen våren 1999* till regeringens bedömning om behovet av en sammanhållen strategi för informationskrigföring och samhällets IT-säkerhet. Utskot-

tet ansåg att det krävdes ett samlat grepp om detta nya område och att ansvaret på myndighetsnivå måste definieras och läggas fast. Utskottet påtalade behovet av att komma i gång snabbt med det fortsatta arbetet.

Försvarsberedningen har vid flera tillfällen behandlat frågan om hoten mot informationssäkerheten, senast i rapporten Ds 1999:55 *Europas säkerhet – Sveriges försvar.*

I rapporten framhåller försvarsberedningen bl.a. följande:

– Försvarsberedningen vill avslutningsvis betona att det är nödvändigt med ett fortsatt och fördjupat arbete kring frågor som rör skyddet mot informationsoperationer och IT-säkerhet. Det krävs ett samlat grepp om detta nya område och ansvaret på myndighetsnivå måste snarast definieras och läggas fast. Detta är viktigt inte minst mot bakgrund av att olika myndigheter i brist på styrning agerar självständigt till förfång för möjligheten att få till stånd en samlad lösning. Frågan om samhällets sårbarhet i detta hänseende är säkerhetspolitiskt av stor betydelse. Försvarsberedningen avser därför noga följa utvecklingen inom detta område och hur regeringens arbete fortskrider.

Regeringen anmäler i propositionen att frågan om vad samordningsansvaret bör omfatta, och hur det skall organiseras, behandlas *inom ramen för en utredning* om det civila försvaret och beredskapen mot svåra påfrestningar på samhället i fred. Regeringen har beslutat om direktiv (dir. 1999:63) för en särskild utredare med uppgift att lämna förslag till principer för att åstadkomma en förbättrad helhetssyn när det gäller planeringen för civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred.

Utredaren skall bl.a., efter analys av nuvarande ansvars- och rollfördelning, föreslå hur utformningen av en tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring bör utformas. Det är naturligt att i detta samarbete beakta frågan om Sveriges medverkan i det internationella arbetet inom området.

Regeringen har i de ursprungliga direktiven förutsatt att utredaren skulle lämna en delrapport senast den 1 april år 2000 om informationskrigföring och IT-säkerhet. Enligt vad utskottet erfarit kommer delrapporten att lämnas under början av år 2001. Tidsutdräkten är beklaglig. Därmed ökar risken för att den föreliggande bristen på nationell styrning som nu råder kommer att leda till en försvårad samordning över sektorsgränserna.

Försvarsutskottet delar regeringens uppfattning att ansvaret för informationssäkerheten även fortsättningsvis skall ligga hos de myndigheter, företag och organisationer som har det normala verksamhetsansvaret. Ställningstagandet är – som anförs i motion T29 – okontroversiellt. Informationssäkerheten kan inte betraktas som något annat än en normal del av verksamheten. Denna ordning är emellertid inte tillräcklig. Tvärsektoriella hot kräver tvärsektoriella lösningar. Ansvarsfrågorna i ett mer nationellt perspektiv måste nu äntligen klaras ut. Det är utskottets mening att den utredare som nu arbetar måste lämna förslag till hur en tvärsektoriell samordning för IT-säkerhet och skydd mot informationskrigföring i Sverige bör utformas.

Utskottet erinrar om riksdagens tidigare tillkännagivande i frågan (bet. 1995/96:TU19). Försvarsutskottet utgår således från att regeringen snarast därefter återkommer till riksdagen med förslag som redovisar de konkreta åtgärder – och eventuella författningsförslag – som behövs för ett mer samlat ansvarstagande för Sveriges informationssäkerhet än hittills.

Stockholm den 27 april 2000

På försvarsutskottets vägnar

Henrik Landerholm

I beslutet har deltagit: Henrik Landerholm (m), Tone Tingsgård (s), Karin Wegestål (s), Stig Sandström (v), Åke Carnerö (kd), Olle Lindström (m), Rolf Gunnarsson (m), Ola Rask (s), Håkan Juholt (s), Berit Jóhannesson (v), Anna Lilliehöök (m), Lars Ångström (mp), Erik Arthur Egervärn (c), Runar Patriksson (fp), Laila Bäck (s), Berndt Sköldestig (s) och Amanda Agestav (kd).

Innehållsförteckning

Elanders Gotab, Stockholm 2000