Yttrande från Ekonomiska och sociala kommittén om ”Meddelande från kommissionen till rådet, Europaparlamentet, ’Ekonomiska och sociala kommittén och Regionkommittén – Nät- och informationssäkerhet: förslag till en europeisk strategi’”

(2002/C 48/07)

Den 7 juni 2001 beslutade kommissionen att i enlighet med artikel 262 i EG-fördraget rådfråga Ekonomiska och sociala kommittén om ovannämnda meddelande.

Sektionen för transporter, energi, infrastruktur och informationssamhället, som fick uppdraget att förbereda ärendet, antog sitt yttrande den 6 november 2001. Föredragande var Daniel Retureau.

Vid sin 386:e plenarsession den 28–29 november 2001 (sammanträdet den 28 november 2001) antog Ekonomiska och sociala kommittén följande yttrande med 113 röster för, 2 emot och 3 nedlagda röster.

1. Inledning

1.1. Uppbyggnaden av interna nät inom företag, förvaltningar och andra organ samt uppkopplingen av dessa och privatpersoner på Internet fortgår i allt snabbare takt. Taket kommer snart att nås om ett snabbare Internet [1] inte snart växer fram eller om ett nytt system för tilldelning av namn för toppdomäner inte inrättas.

1.2. Samhället, ekonomin, myndigheterna och den nationella säkerheten (både civil och militär) har blivit beroende av att deras sinsemellan hopkopplade nät är välfungerande och pålitliga. I framtiden kommer detta beroende att öka ytterligare. Beroendet hänför sig också till bredbandsspektrumet, informationsinnehållet och i många fall även till konfidentiella uppgifter eller till möjligheten att säkert fastställa identiteten hos dem som är uppkopplade.

1.3. Nät- och informationssäkerheten är framdeles en strategisk fråga av högsta vikt och bör bli föremål för en samordnad och enhetlig politik mellan EU:s medlemsstater och på global nivå.

1.4. Kommissionen gör i meddelandet en djupgående analys av problemen och nuläget. ESK anser att analysen är väl uppbyggd och ger upphov till en rad åtgärdsförslag.

2. Kommissionens förslag

2.1. Tanken med kommissionens meddelande är att införa en gemensam metod för frågor i anslutning till nätsäkerhet och säker överföring av information i EU. Syftet är att försöka uppnå en lika hög skyddsnivå i alla medlemsstater, att systemen skall vara kompatibla, att det offentliga skall tillhandahålla de behövliga säkerhetstjänsterna gällande Internet och att fastställa medlemsstaternas lagstiftande roll.

2.2. Det gäller att säkerställa en form av ”minsta” säkerhetsnivå för näten och de privata Internetanslutningarna samt för kopplingarna mellan dessa. En säkerhetskultur måste utvecklas i syfte att gynna en allmän medvetenhet om problem och lösningar.

2.3. Det är den svagaste länken som är avgörande för säkerheten som helhet, och den ökande förekomsten av höghastighetsuppkopplingar (ADSL, kabel) och permanenta uppkopplingar på Internet, även bland privatpersoner, ger upphov till nya krav på säkerhet. Detsamma gäller elektronisk handel där konsumenternas personliga uppgifter och betalningsreferenser måste skyddas, vilket även är fallet när det gäller medborgarnas personuppgifter inom den tilltagande elektroniska myndighetsverksamheten.

2.4. Det är även nödvändigt att införa en tillräckligt harmoniserad strafflagstiftning för att likvärdigt kunna definiera och bestraffa regelbrott i olika medlemsstater. Sådana brott är intrång, stöld av uppgifter och information, angrepp som ger kontroll över nätverk eller medveten spridning av virus.

2.5. Kommissionen föreslår att ett europeiskt varnings- och stödsystem inrättas och betonar behovet av utbildning och information såväl inom företag som bland allmänheten. Detta behov står i fokus i meddelandet.

[1] IPv6-normen tillåter 6 000 miljarder IP-adresser.

2.6. Slutligen ges i meddelandet hög prioritet till skydd av privatlivet och av medborgarnas och konsumenternas konfidentiella personuppgifter.

3. **ESK:s synpunkter**

3.1. *Allmänna kommentarer*

3.1.1. ESK ger sitt fulla stöd till de analyser och argument som motiverar en europeisk politisk ram för nät- och informationssäkerhet. ESK bedömer att de föreslagna åtgärderna i huvudsak är relevanta, men vill föra fram vissa synpunkter och förslag.

3.1.2. Internet har inte byggts upp med tanke på elektronisk handel, kontrakt, försäljning av material som omfattas av upphovsrätt (musik, bilder och filmer), överföring av pengar och andra ekonomiska transaktioner som kräver särskild säkerhet. Ursprungligen användes Internet för militära och akademiska ändamål. Internet kunde tillgodose försvarets behov av kryptering med nycklar och universitetens behov av att snabbt sprida icke-kodade forskningsresultat eller vetenskapliga databaser. Av nationella säkerhetsskäl var det ända till år 2000 vanligt att kryptering och export av vissa program var förbjudet för privatpersoner i många länder, särskilt utanför Europa. Lyckligtvis uppmuntrade kommissionen till utveckling av och handel med säkerhetsprodukter som är oundgängliga för företag och myndigheter vid överföringen av sekretessbelagda uppgifter på nätet.

3.1.3. Därefter användes Internet som ett fritt forum som sedermera övergick till att även få ett kommersiellt, ekonomiskt, tekniskt och industriellt syfte. Det blev även en plattform för spel. Till detta skall man lägga de pornografiska webbplatserna som har betydande inkomster. Porren har tillsammans med dataspelen gett upphov till en anmärkningsvärd teknisk utveckling särskilt när det gäller bildkvalitet och hastighet samt anonyma eller icke-anonyma säkra betalningssystem.

3.1.4. Alla dessa användningssätt fortsätter att samexistera och ännu fler utvecklas, men en tilltagande del av näten och Internet utgör grundvalarna för samhällelig och ekonomisk verksamhet och bidrar på ett avgörande sätt till social utveckling och till nationell säkerhet. På detta område krävs säkerhetsåtgärder som står i proportion till överförda uppgifter och transaktioner samtidigt som privatlivet skyddas utan att grundtanken bakom Internet äventyras, nämligen en fri rörlighet för information och ett öppet utbyte av fakta, tankar, vetenskapliga resultat osv.

3.1.5. ESK anser alltså att de säkerhetsåtgärder som vidtas alltid skall stå i proportion till säkerhetskostnaderna, till de säkrade uppgifternas och transaktionernas karaktär och prioritet samt till de berörda användarkategorierna.

3.1.6. ESK delar i huvudsak kommissionens uppfattning om möjliga risker och förhåller sig allmänt positiv till de förslag till lösningar som kommissionen lägger fram. Kommittén delar också kommissionens åsikt om att säkerhet är en dynamisk fråga som förutsätter anpassning och ständig översyn allt eftersom det sker förändringar avseende teknik, programvara och risker. Därför föreslår ESK att den dialog som i anslutning till meddelandet inletts med industrin, användare och ansvariga för nätsäkerhet skall permanentas eller återupptas regelbundet. Det organiserade civila samhället bör fullt ut anslutas till denna dialog såväl med tanke på nät- och informationssäkerhetens återverkningar på vissa medborgerliga grundläggande rättigheter som med tanke på förvaltningens ekonomiska och sociala verksamhet.

3.1.7. I sina färska yttranden om ”Datorrelaterad brottslighet” ([1]) och om ”Skydd av barn/Internet” ([2]) har ESK redan formulerat de grundläggande principer som kommittén omfattar i kampen mot användning av Internet i brottsliga eller kriminella syften, samtidigt som man måste undvika censur, övergripande tillsyn och hinder för yttrandefriheten och för friheten att kommunicera obehindrat på det världsomspännande nätet. Internet faller dock inte utanför lagtillämpningen.

3.1.8. ESK bedömer att alla dimensioner av enskilda användares och konsumenters säkerhet bör inta en mer central ställning i kommissionens beredningsarbete och i den europeiska strategin. Även om en virusattack mot en privatpersons

([1]) Yttrande om ”Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – Ett säkrare informationssamhälle – ökad säkerhet i informationsstrukturen och bekämpning av datorrelaterad brottslighet” (CES 1115/2001). Har inte ännu publicerats i EGT.

([2]) ESK:s yttrande om ett program för skydd av barn på Internet är under arbete.

dator inte får några större direkta återverkningar på ekonomiska intressen eller på allmän säkerhet måste man komma ihåg att vissa virusattacker sker i stor omfattning, sprids vidare via kundernas datorer och lyfts fram av medierna på ett sätt som ibland överdriver den verkliga risken, vilket leder till att medborgarnas tro på Internets fördelar och nytta minskar. Detta har en kraftig negativ inverkan på den elektroniska handelns tillväxtpotential och på e-handeln överlag, samtidigt som framväxten av nya arbetstillfällen hämmas.

3.1.9. Även om skyddet av privatlivet och personliga uppgifter är prioriterade målsättningar har konsumenterna ytterligare rätt att bli skyddade på ett garanterat effektivt sätt mot missbruk av personliga data genom ”spionprogram” (*spyware* och *web bugs*) eller med andra metoder. Man måste även på ett effektivt sätt försöka hindra *spamming*, som innebär massutsändning av oönskad e-post och som ofta är en följd av att personuppgifter missbrukas. Dessa intrång leder till kostnader för offren ([1]).

3.1.10. Skyddet av privatlivet skall gälla samtliga personer i arbetslivet och måste följaktligen inbegripa arbetstagare på alla nivåer inom företagen. De interna säkerhetsreglerna bör förhandlas fram av arbetsmarknadsparterna och vara kända bland alla anställda vid företaget. Detta skall ske med hänsyn till lagstiftningen i respektive medlemsstat. I sammanhanget bör det framhållas att det är viktigt att sådana regler tillämpas enhetligt i enlighet med EU:s stadga om grundläggande rättigheter från toppmötet i Nice och även med avseende på rekommendationen av den 13 september 2001 om europeiska garantier för privatlivet och direktiv 95/46 om skydd av personuppgifter.

3.1.11. Det är alltså oundgängligt att ge privatpersoner och företag effektivare rättsliga medel att ställa operatörer och producenter av programvara till svars ekonomiskt i fall då dessa på basis av skadeståndsansvaret är ansvariga för allvarliga säkerhetsbrister och problem med skydd av information ([2]).

3.1.12. Kommissionen bör enligt ESK i högre grad dra nytta av och sprida kunskap om den positiva roll som s.k. *open source* erbjuder i fråga om resurser och skydd. Open source innebär användarsystem, nätverksprogram och kommunikationsprogram som är kostnadsfria och som användarna fritt kan ändra. Gruppen av open source-programmerare ingriper snabbt för att rätta till fel och åtgärda problem. Kring detta koncept har en viktig ekonomisk sektor för företagstjänster växt fram med stöd av vissa jättar inom IT-industrin. En stor del av världens servrar fungerar generellt sett säkert och stabilt med sådan programvara, samtidigt som det ibland händer att vissa skyddade programvaror bara korrigeras efter en tids försening, till skada för användarna, eller att nya versioner av dessa program med nya funktioner kommer ut på marknaden för tidigt. Viljan att förbättra konkurrenskraften på marknaden eller strävan efter att få fram nyheter till varje pris får ibland dominera över en säkerhetskultur som borde förstärkas hos alla dem som skapar kommersiella eller kostnadsfria program, så att den verkligen integreras i produkterna från första början.

3.1.13. Vidare erbjuder hanteringssystem och skyddade program vars källkod inte har uppgetts inte en tillräcklig garanti för säkerhet och skydd av privatlivet, särskilt med tanke på licensregistrering och nedladdning av programfixar (*patches* – korrigeringar och uppdateringar) via Internet, vilka kan missbrukas i syfte att samla information om kundens system och servern (innehållets uppbyggnad, adresslistor och anslutningar). ESK anser att allt som går utöver registrering av namn och adress för ägaren till programlicensen i syfte att ge denna en aktiveringsnyckel eller en tillfällig kod för tillträde till tjänster skall ses som intrång och förbjudas.

3.1.14. *Fria* program (*free*: kostnadsfria) är en annan garant för sund konkurrens i motsats till de monopolistiska tendenserna på programvarumarknaden och på marknaden för nättjänster, som utvecklas kraftigt.

3.1.15. En allmän öppen licens (*general public licence*, GPL ([3])) bör erkännas och respekteras. Med tanke på Internet anser ESK att särskilda metoder och regler bör utarbetas för immaterialrätt vad gäller programvara och material som finns tillgängligt eller som kan bytas ut via Internet. Det är alltför enkelt att till exempel hänvisa till lagstiftningen om märkning för att hindra yttrandefriheten eller konsumenternas eller löntagarnas frihet att kommentera ett företags politik och förfaranden eller företagets produkter och tjänster. Patent- och märkesrätten verkar vara på väg att nå sina gränser och stöter på tillämpningsproblem när det gäller nätutvecklingen. Därför behövs det särskilda skyddsregler som ännu inte utvecklats i tillräckligt hög grad.

([1]) Se ESK:s yttranden om elektroniska kommunikationsnät (EGT C 123, 25.4 2001, s. 50), om elektronisk handel (EGT C 169, 16.6.1999, s. 36) och om konsekvenserna av elektronisk handel på inre marknaden (EGT C 123, 25.4.2001, s. 1).

([2]) ESK:s yttrande: EGT C 117, 26.4.2000, s. 1.

([3]) Genom GPL fastställs immaterialrätten för upphovsmannen till en programvara som är fritt tillgänglig.

3.1.16. Med beaktande av att försök till intrång och kontrollövertagande eller stöld av känsliga uppgifter främst riktas mot militära och administrativa nät samt företagsnät, uppmanar ESK dessutom EU-institutionerna och samtliga medlemsstater att tillsammans bekämpa alla intrång eller försök till intrång som syftar till militärt, administrativt eller kommersiellt spionage och som motverkar Europas strategiska och ekonomiska intressen.

3.1.17. Säkerhetsåtgärder, övervakning av tillträde, regler och interna protokoll samt tilläggsmateriel (återställningsprogram vid datakrascher, speglade webbplatser och proxyservrar, säkerhetskopiering av data med korta mellanrum och till annan plats) kräver programvara, materiel samt ständig övervakning och uppdatering som utförs av välutbildad personal. Allt detta medför stora kostnader. Såväl otillräcklig teknisk information och medvetenhet som dåliga ekonomiska möjligheter (särskilt inom små och medelstora företag) gör det mycket svårt för offentliga och privata företag och myndigheter att införa säkerhetsåtgärder. De CERT-grupper som skall ge stöd vid virusvarningar och liknande bör vara välutrustade och beakta de små och medelstora företagens behov.

3.2. *Särskilda kommentarer*

3.2.1. Särskilda kommentarer om risker och planerade riskhanteringsmetoder

3.2.1.1. Skydd av privatlivet och bekämpning av datorrelaterad brottslighet och spionage

3.2.1.1.1. Kommittén ställer sig helt och hållet bakom kommissionens prioritering att skydda privatlivet och att se till att personuppgifter förblir konfidentiella. Skyddet av de grundläggande rättigheterna samt informations- och kommunikationsfriheten bör utgöra kärnan i alla strategier för uppgifts- och kommunikationsskydd. Det är också viktigt att slå vakt om skyddet av de kollektiva intressena, framför allt den nationella säkerheten, och se till att våra demokratiska institutioner och offentliga förvaltningar kan fungera normalt. Kommittén delar uppfattningen att man bör utveckla och anpassa metoder för att dessa mål skall kunna uppnås genom lagstiftning, samarbete, forskning och standardisering.

3.2.1.1.2. Om möjligheten till laglig avlyssning skall bibehållas med beaktande av lämpliga rättsliga förfaranden kan kraftfulla krypteringsmetoder omöjliggöra dekryptering. Den organiserade brottsligheten använder sig av de modernaste och säkraste metoderna för att skydda den egna kommunikationen. Ett rättsligt och tekniskt samarbete bör följaktligen utvecklas internationellt på europeisk nivå för att bekämpa organiserad brottslighet och terrorism, något som kommittén betonar i sitt yttrande om kampen mot penningtvätt och datorrelaterad brottslighet ([1]).

3.2.1.1.3. På det konkurrenspolitiska området är det också nödvändigt att hålla koncentrations- och monopoliseringsprocesserna under kontroll med avseende på innehåll (information, kultur m.m.) och de olika sektionerna av ”kanalerna” på Internet. Kommissionen bör också se till att det inrättas en ”ledningsgrupp” för Internet som är mer representativ för dagens 370 miljoner användare och som präglas av större insyn, eftersom dagens månghövdade ”ledningsgrupp” är koncentrerad till Nordamerika och lyder under USA:s handelsdepartement, som bland annat ansvarar för tilldelningen av domännamn och valet av s.k. *registrars* ([2]).

3.2.1.1.4. Operatörerna skall effektivt kunna garantera att man skyddar privatlivet och hemlighåller kundernas identitet med hjälp av materiella övervakningsmetoder och kryptering av kommunikation i linje med uppgifternas betydelse och med beaktande av de tekniska framsteg som gjorts. Operatörernas verksamhet regleras för övrigt av bland annat direktiv 97/66/EG ([3]).

3.2.1.1.5. Användarna skall å sin sida beredas möjlighet att i tillräcklig utsträckning och på ett säkert sätt kryptera känsliga uppgifter som de vill förmedla via Internet. Denna möjlighet är i allmänhet relativt begränsad på grund av otillräckliga resurser och bristfälliga genomförandemetoder. För att de ökade krypterings- och säkerhetsbehoven skall kunna tillgodoses måste man utbilda specialister i tillräcklig omfattning.

3.2.1.1.6. Intrång i datorer och nätverk, oavsett skäl (intellektuell utmaning, personlig hämnd eller viljan att skada, stöld eller övertagande av kontrollen i olika syften) och spridning av datavirus hotar användarnas rättigheter och intressen samt äventyrar skyddet av uppgifter, information och nätverk.

([1]) Se ESK:s yttrande om ett program för skydd av barn på Internet är under arbete. Se ESK:s yttranden om elektroniska kommunikationsnät (EGT C 123, 25.4.2001, s. 50), om elektronisk handel (EGT C 169, 16.6.1999, s. 36) och om konsekvenserna av elektronisk handel på inre marknaden (EGT C 123, 25.4.2001, s. 1).

([2]) Företag som ansvarar för tilldelningen och förvaltningen av vissa domännamn.

([3]) Direktiv om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet (EGT L 24, 30.1.1998).

3.2.1.1.7. Kommittén håller helt och hållet med kommissionen om att olika former av intrång –som i värsta fall kan leda till att andra personer oförmärkt tar kontroll över systemen – kan ge upphov till mycket stora skador. Kommittén anser det dock vara överdrivet att jämställa hackare, *hackers*, (som enbart påvisar säkerhetsbrister utan brottsliga intentioner, vilket kan leda till att bristerna rättas till) med knäckare, *crackers* (som tar sig in i systemen för att skada). Den straffskala som kommissionen kan komma att föreslå måste stå i proportion till det eventuella brottet, som skall definieras exakt och anses vara av allvarlig art, och hänsyn skall tas till gärningsmannens avsikter.

3.2.1.2. Tillämplig gemenskapsrätt och tillgänglig teknik

3.2.1.2.1. Gemenskapsrätten stipulerar att medlemsstaterna skall vidta alla nödvändiga åtgärder för att garantera att de allmänna telenäten upprätthålls vid nätsammanbrott som orsakas av naturkatastrof (direktiv 97/33/EG om samtrafik [1] och direktiv 98/10/EG om taltelefoni [2]). Kommittén föreslår dock att kommissionen genomför en jämförande studie av de åtgärder som vidtagits och dessa åtgärders effektivitet i samtliga medlemsstater.

3.2.1.2.2. Lögnaktiga uttalanden som görs av fysiska eller juridiska personer kan orsaka stor skada. I samband med större transaktioner är det därför nödvändigt att kontrollera att personen verkligen är den man utger sig för att vara och att uppgifterna stämmer.

3.2.1.2.3. SSL- och IPSec-protokollen gör det möjligt att kommunicera på Internet via öppna kanaler med en viss säkerhetsnivå, men ger inte tillräcklig säkerhet. I direktivet om elektroniska signaturer [3] stipuleras att dessa certifikattjänster kan tillhandahållas av en tredje part.

3.2.1.2.4. Denna lösning kännetecknas av samma problem som kryptering, på grund av den kompatibilitet och nyckelhantering som krävs. Privata virtuella nätverk (VPN) kan erbjuda individuella lösningar. För de allmänna näten utgör dock detta problem ett stort hinder.

3.2.1.2.5. Direktivet om elektroniska signaturer är därför ett viktigt styrinstrument och bör utgöra rättslig grund för åtgärder som syftar till att underlätta elektronisk autentisering.

3.2.1.3. Nya utmaningar, nya risker och kostnads-nytto-analys

3.2.1.3.1. Kommittén instämmer i analysen om de nya utmaningar och risker som hänger samman med att tekniken utvecklas allt snabbare samtidigt som antalet Internetterminaler blir både fler och mer diversifierade. Fler terminaler med fast adress är kontinuerligt uppkopplade mot Internet, vilket ökar risken för intrång. Kommittén stöder därför kommissionens förslag att försöka hitta en balans mellan behoven av säkerhet och frihet samt skyddet av näten, skyddet av privatlivet och uppgiftsskyddet.

3.2.1.3.2. Säkrare krypteringsmetoder har inneburit att lagstiftningen anpassats, men för att möjliggöra en kraftfull kryptering har de nya bestämmelserna ofta dragit ut på tiden på grund av olika säkerhetsaspekter. Man kan dock gömma meddelanden med ljud och bild (steganografi) och med hjälp av denna metod kan personer som vill bryta mot lagen utan att bli upptäckta dölja sina meddelanden.

3.2.1.3.3. Flera algoritmer används och dessa blir alltmer sofistikerade. Detta innebär stora problem i hanteringen av krypterade meddelanden enligt olika metoder för olika användare. Även rekommendationen om ett europeiskt system, om ett sådant kan underlätta kommunikationen på inre marknaden, kommer att stöta på problem på grund av de många olika system som används i övriga världen. Detta innebär högre kostnader för säkerhet och hantering, även om vissa effektiva system är allmänna och gratis.

3.2.1.3.4. De kostnader som uppstår om man inte vidtar några säkerhetsåtgärder, i en värld där fler och fler känsliga uppgifter är i omlopp, är dock ännu högre. Säkerheten kommer i viss utsträckning också allt oftare att ingå i själva produkten.

3.2.1.3.5. ESK ser positivt på det europeiska förfarande som föreslås av kommissionen, samtidigt som kommittén är medveten om dess begränsningar. Generella åtgärder måste vidtas i samhället för att man skall kunna komma till rätta med dagens brister på marknaden, med hänsyn till de värden som står på spel.

3.2.1.3.6. Det finns redan rättsliga garantier i EU:s direktiv om uppgiftsskydd och i ramlagstiftningen om telekommunikationer. Dessa åtgärder skall dock vidtas i en verklighet som befinner sig i snabb förändring, oavsett om det gäller konkurrens, nätkonvergens eller globalisering. Marknaden har samtidigt en tendens att inte investera tillräckligt mycket i säkerhetslösningar, på grund av de orsaker som omnämns i meddelandet, även om marknaden för säkerhetslösningar expanderar snabbt runtom i världen.

---

[1] EGT L 199, 26.7.1997.
[2] EGT L 101, 1.4.1998.
[3] Direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer, EGT L 13, 19.1.2000, s. 12.

3.2.1.3.7. Det är sant att marknaden för säkerhetslösningar fortfarande är en ofullkomlig marknad, vilket också kommissionen påpekar. Investeringar i säkerhetslösningar är endast lönsamma om tillräckligt många personer gör en dylik investering. Forskningen kring olika säkerhetslösningar bör därför ske genom samarbete. Om det stora flertalet varor och tjänster även fortsättningsvis skall ha individuella säkerhetslösningar bör man uppmuntra forskning kring standarder som är mer allmänt godkända, kännetecknas av ökad säkerhet och kan tillämpas i olika säkerhetssystem. Kommittén anser att man bör verka för att det utarbetas gemensamma kriterier på internationell nivå i stället för olika certifierings- och autentiseringssystem som kan skapa problem för slutanvändaren.

3.2.1.3.8. För det första bör befintlig EU-lagstiftning genomföras effektivt. Den rättsliga ramen skall vara relevant och effektiv samt kunna anpassas kontinuerligt.

3.2.1.3.9. För det andra bör de åtgärder som föreslagits av kommissionen syfta till att stärka marknadskrafterna, vilka för övrigt håller på att ta form, om dagens marknad inte kan generera tillräckliga investeringar i teknik och säkerhetslösningar.

3.2.1.3.10. Kommunikations- och informationstjänsterna är dessutom gränsöverskridande. Det krävs därför bestämmelser på gemenskapsnivå, så att man kan värna om den inre marknaden för dessa tjänster, tillvarata gemensamma lösningar och agera effektivt på internationell nivå.

3.2.1.3.11. Kommittén instämmer i uppfattningen att investeringar i förbättrad nätsäkerhet innebär både ökade kostnader och större nytta i samhället. Marknadspriset avspeglar inte dessa aspekter på ett korrekt sätt. På kostnadssidan åläggs inte marknadens aktörer att ta ansvar för sitt eget säkerhetsagerande. Kommittén anser att man omedelbart måste rätta till denna brist.

3.2.1.3.12. Kommittén ställer sig också bakom den analys enligt vilken nyttan av säkerhetslösningar inte slår igenom i marknadens pris, även om de investeringar som genomförts av operatörer, leverantörer och serviceföretag är till nytta för såväl företagens kunder som hela ekonomin och den allmänna kommunikationssäkerheten.

3.2.1.3.13. Kommittén anser också att användarna inte är medvetna om samtliga risker samtidigt som många operatörer, försäljare och tjänsteleverantörer har svårt att utvärdera om och i vilken utsträckning man är utsatt för risker. Många nya tjänster, tillämpningar och program har också attraktiva egenskaper, som dock kan innebära ökad riskexponering. Det är viktigt att man testar nya produkter mycket ingående innan dessa släpps ut på marknaden.

3.2.2. Särskilda synpunkter på förslaget till en europeisk strategi

3.2.2.1. Vi är medvetna om att det globala nätet har en inbyggd sårbarhet, särskilt i samband med routing av datapaket, och att det ständigt ökande antalet uppgifter i omlopp inte möjliggör allmänna säkerhetslösningar med filtrering utanför terminalerna. Vi stöder på det hela taget de förslag till åtgärder som ingår i den politiska strategin.

3.2.3. Medvetandehöjande åtgärder

3.2.3.1. Förslagen när det gäller att höja medvetandegraden hos berörda personer och organisationer förefaller rimliga. Säkerhetslösningar för terminaler och elektronisk kommunikation handlar främst om användarnas kunskap om risker och vilken information de fått.

3.2.4. Ett snabbt europeiskt informationssystem

3.2.4.1. Kommittén stöder förslaget om ett snabbt europeiskt varnings- och informationssystem som anger vilka problem som föreligger och hur de skall lösas. Vi stöder även kommissionens andra förslag när det gäller analyser, system för tidig varning, spridning av information och råd samt ett europeiskt och internationellt samarbete. Samtidigt skall man utveckla en anpassad infrastruktur i hela EU med ett effektivt permanent samarbete.

3.2.4.2. När det gäller de rapporter som enligt kommitténs uppfattning inte bara företagen utan även myndigheter och andra organ borde avlägga, kan vi konstatera att det konfidentiella system via vilket man kan rapportera attacker kommer att underlätta informationsutbytet. Det bör dock påpekas att det alltid kommer att finnas läckor eller hackare som offentliggör information, och en snabb kännedom om attackernas art och olika brister, och framför allt vilka åtgärder som vidtagits för att komma till rätta med dem, skulle kunna bygga upp allmänhetens förtroende.

3.2.4.3. Varningssystemen borde enligt kommitténs åsikt även kunna detektera brister i kommersiella program eller gratisprogram samt tekniska eller andra element som kan öppna dörrarna för eventuella attacker. Systemet med tidig varning skulle kunna användas i detta syfte, samt för övervakning av den tekniska utvecklingen och webbplatserna för hackare och angripare samt av olika *underground*publikationer som tar upp användbara metoder eller till och med publicerar ”nyckelfärdiga” program för att skapa virus eller göra intrång som *script kiddies* [1] använder sig av.

3.2.5. Teknikstöd

3.2.5.1. Kommittén bifaller det planerade forskningsstödet. Vi vill emellertid påpeka att kryptering behärskas av högst ett par tiotal experter i världen. Ett större antal av dessa arbetar för NSA [2]. Hur skall man bära sig åt för att få de europeiska experter som kan bidra till att utveckla forskningen att stanna kvar? Vilka medel förfogar vi över i Europa? NSA har ett försprång på 10–15 år och förfogar över instrument för beräkningar (och kryptering) som det förefaller svårt att hinna ikapp omgående. Vilka konkreta – och nödvändigtvis omfattande – medel kommer att ställas till forskningens förfogande [3]?

3.2.5.2. Ett system där hackare och ”informella” experter involveras skulle kunna utgöra ett komplement, i stället för en avvisande, marginaliserande attityd eller det som verkar vara trenden i Europa: en överdriven bestraffning – som borde vara förbehållen riktigt allvarliga brott – av personer som inte direkt skadar andra eller samhället. Samtidigt som straffen för brott som piratkopiering eller terrorism via näten måste vara avskräckande, får straffen inte systematiskt tillämpas på personer som letar efter säkerhetsbrister i syfte att informera programmerare eller nätverksoperatörer så att dessa kan förbättra sitt skydd, i den mån dessa efterforskningar inte syftar till något skadligt som sabotage, stöld av konfidentiella data, anonym användning av nätet, personlig vinning eller spridning av datavirus.

3.2.5.3. Att offentliggöra upptäckter utan att de direkt berörda informeras långt i förväg och utan att de ger sitt samtycke är dock en förkastlig gärning som skall kunna bestraffas i proportion till brottet. Men man bör anstränga sig för att få de personer som inte begår någon förseelse eller något allvarligare brott eller inte orsakar några ekonomiska skador att ta steget innanför lagens gränser och man bör utnyttja deras kompetens till samhällets bästa. Denna unika kompetens skulle på så vis löpa mindre risk att dras till eller utnyttjas av kriminella eller terrorister än om den förblev marginaliserad och kriminaliserad.

3.2.6. Stöd för marknadsorienterad standardisering och certifiering

3.2.6.1. Kommittén instämmer i kommissionens analys att det finns för många standarder och konkurrerande system, och att det utgör hinder för säkerheten och utvecklingen av signaturer och säkra elektroniska betalningsmedel. Vi vill framhålla behovet av gemensamma standarder och kriterier, som gör det möjligt att undvika tröghet på marknaden, samt behovet av kompabilitet.

3.2.6.2. Vi stöder de föreslagna åtgärderna men vill understryka vissa problem som är kopplade till att den ”ledningsgrupp” för Internet som bland annat fastslår standarderna för närvarande är av alltför privat karaktär och inte tillräckligt representativ. Det handlar om ett tidskrävande arbete som fordrar tålamod och samarbete.

3.2.7. Lagstiftning

3.2.7.1. Kommittén stöder förslaget om en specificering vad gäller nätverk och Internet i lagstiftningen för telekommunikation och dataskydd.

3.2.7.2. De föreslagna åtgärderna är välavvägda och kommittén stöder initiativen för att få till stånd en harmoniserad strafflagstiftning och stärka det rättsliga samarbetet mellan medlemsstaterna för att bekämpa den datorrelaterade brottsligheten utan att ifrågasätta avregleringen av handeln med omfattande krypteringsprodukter, som är de enda som kan garantera en effektiv säkerhet. Samarbete av civil och kommersiell natur spelar också en viktig roll i kampen mot den datorrelaterade brottsligheten (finansiella system, skattefusk m.m.).

(1) Unga ”hackarlärlingar” utan tekniska kvalifikationer som enbart kopierar sådant de finner på nätet och i *underground*publikationer.
(2) National Security Agency, USA:s nationella säkerhetsorgan.
(3) ESK:s yttrande om sjätte ramprogrammet för forskning och teknisk utveckling (EGT C 260, 17.9.2001, s. 3).

3.2.7.3. Enligt kommitténs uppfattning bör samarbetet inom det rättsliga området emellertid även utsträckas till internationell nivå, och den europeiska strategin på detta område bör bli föremål för åtgärder inom den föreslagna politiska strategin. Kommittén noterar med tillfredsställelse att kommissionen inom de närmaste veckorna kommer att lägga fram ett formellt förslag i detta ärende.

3.2.8. Säkerheten i myndigheternas system

3.2.8.1. Kommittén stöder de planerade åtgärderna eftersom ett stort antal uppgifter som hanteras av de offentliga myndigheterna är av personlig karaktär, men även med tanke på att myndigheternas webbplatser kan utgöra mål för terroristattacker samt av inrikes- och utrikespolitiska skäl, vilket *Code Red* (ett polymorft virus) och *Nimda* nyligen visade. Kommissionen bör se de senaste attackmotiven som ännu ett skäl att ytterligare säkra sina egna och medlemsstaternas webbplatser och officiella nät.

3.2.9. Internationellt samarbete

3.2.9.1. Det är enligt kommitténs uppfattning en viktig men svår och känslig fråga för den europeiska politiken för nät- och informationssäkerhet som skapar problem när det gäller den interna solidariteten, utrikespolitiken och den gemensamma säkerhetspolitiken samt när det gäller styrningen av sammankopplade nätverk och Internet.

3.2.9.2. Förslaget till åtgärder på detta område innebär att man skall fullfölja och utveckla samarbetet inom de olika internationella organen i fråga om nätsäkerhet, och det är diplomatiskt och allmänt formulerat.

3.2.9.3. Kommittén anser emellertid att man även borde fortsätta diskussionen i lämpliga internationella organ samt inom den transatlantiska dialogen och ta upp frågor om säkerhet, kompabilitet mellan krypteringsnycklar och krypteringssystem samt problem med vissa standarders eventuella svagheter som somliga har kännedom om men som inte avslöjats. Det vore även önskvärt med ett nära samarbete i frågor som internationell överföring av personuppgifter och rättsligt och civilt samarbete mot databrottslighet, dvs. effektiva säkerhetslösningar och en överskådlig och balanserad hantering av det globala nätet vars strategiska betydelse anses vara väsentlig för vår livsföring och levnadsstandarden i våra samhällen. OECD arbetar med nätsäkerhet och är ett viktigt organ för internationellt samarbete på detta område. Det är bråttom att finna praktiska lösningar på internationell nivå.

3.2.9.4. Kommissionens förslag att inrätta ett EU-forum för samtliga berörda parter i syfte att diskutera problem och lägga fram lösningar för institutionerna stöds och betraktas som mycket viktigt av kommittén.

4. **Slutsatser**

4.1. Det finns relativt effektiva lösningar i form av hårdvara och program som ständigt utvecklas liknande dem som beskrivs i kommissionens meddelande. Dessutom kan en fils integritet säkerställas genom användning av en algoritm för numerisk märkning som är unik och som anger att den överförda filen inte varit föremål för några ändringar.

4.2. Enligt vår uppfattning är information och utbildning kärnan i alla säkerhetsstrategier, annars kommer tillgängliga lösningar inte att användas på rätt sätt. Information och utbildning kan också öka det övergripande förtroendet för systemet om alla regelbundet vidtar nödvändiga försiktighetsåtgärder och företagen gör erforderliga investeringar i säkerhetslösningar för sina system.

4.3. Kostnaderna för säkerhet är dock mycket höga och bristen på kompatibla lösningar är ett stort hinder. *Open source* skulle här kunna vara en lösning eftersom det stimulerar konkurrens och efterbildande.

4.4. Om man inte snabbt finner en lösning på dessa problem inom EU och på internationell nivå – EU bör inta en plats i styrningen av Internet – kommer det att fortsätta att inverka negativt på utvecklingen av *e*Europe, den elektroniska handeln samt när det gäller ledningen av företag, de allmännyttiga tjänsterna och den offentliga förvaltningen.

4.5. För nätsäkerhetens skull är det under alla omständigheter nödvändigt att få till stånd en allmän tillämpning av skyddsåtgärder och ett effektivt och välavvägt stöd, antingen det rör sig om programvarulösningar för privatpersoner (regelbundet uppdaterade virusskydd) eller kombinerade lösningar som är mer eller mindre krävande för andra användare (brandväggar, övervakning av portar för extern kommunikation, separation (DMZ [1]), *shields* och andra typer av teknik, lämpliga program och hårdvaror).

---

[1] DMZ: DeMilitarized Zone, en buffertzon som isolerar det interna nätverket.

4.6. Brottspåföljder i avskräckande syfte ligger inom medlemsstaternas ansvarsområde, men kommittén anser att det åligger kommissionen att föreslå en övergripande och enande ram för att fastställa brottspåföljder på gemenskapsnivå och för att få till stånd ett internationellt rättsligt samarbete.

4.7. Marknadsföringen av vissa produkter som kan innehålla avsiktliga *backdoors* [1], som det ibland tar flera år att upptäcka, bör uppmärksammas och medföra sanktioner liksom spionprogram (*spyware*) som ofta finns i demonstrationsprogram, vissa gratisprogram och vissa system för on-line-licensregistreringar.

4.8. Även brister som inte är avsiktliga tar tid att korrigera och kan utnyttjas som *backdoors* av insatta personer.

4.9. Särskilda oberoende, opartiska, representativa nationella myndigheter – antingen det är fråga om organ som redan finns och vars uppgifter bör utökas eller organ som inte finns men bör skapas (exempelvis i kandidatländerna, som bör involveras) – bör följa upp dessa säkerhetsproblem så att de kan bidra till att utarbeta rekommendationer och standarder för att skydda de grundläggande rättigheterna. Lagstiftningsprojekt under beredning kräver i själva verket en mer ingående analys för att kampen mot terrorismen skall kunna förenas med principerna om den personliga friheten som bör bevaras.

4.10. Enligt ESK:s uppfattning bör Internet under alla omständigheter förbli flexibelt och lättillgängligt och även i fortsättningen utgöra ett område för informations- och kommunikationsfrihet i ett öppet och demokratiskt samhälle, samtidigt som det görs allt säkrare för användarna och erbjuder många olika och allt fler legala former av användning av näten och Internet.

[1] Dolda ingångar.

Bryssel den 28 november 2001.

Ekonomiska och sociala kommitténs

ordförande

Göke FRERICHS