KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 26.1.2001
KOM(2000) 890 endelig

**MEDDELELSE FRA KOMMISSIONEN
TIL RÅDET, EUROPA-PARLAMENTET,
DET ØKONOMISKE OG SOCIALE UDVALG OG
REGIONSUDVALGET**

Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet

Resumé

Europas overgang til et informationssamfund kendetegnes af dybtgående forandringer inden for alle aspekter af menneskelivet: på arbejdet, inden for uddannelse og fritidsliv og i den offentlige sektor og inden for industri og handel. De nye informations- og kommunikationsteknologier har en revolutionerende og radikal indvirkning på vores økonomier og samfund. En vellykket overgang til informationssamfundet er af stor betydning for væksten, konkurrenceevnen og beskæftigelsesmulighederne i Europa og har vidtrækkende økonomiske, samfundsmæssige og retlige følgevirkninger.

Kommissionen lancerede *e*Europe-initiativet i december 1999 for at sikre, at Europa høster fordelene ved de digitale teknologier, og at det gryende informationssamfund ikke resulterer i social udstødelse. I juni 2000 vedtog Det Europæiske Råd i Feira en omfattende *e*Europe-handlingsplan og slog til lyd for, at den blev gennemført inden udgangen af 2002. Handlingsplanen lægger stor vægt på netsikkerheden og bekæmpelsen af cyberkriminalitet.

Informations- og kommunikationsinfrastrukturerne er blevet et kritisk element i vores økonomier. Desværre er disse infrastrukturer på visse punkter sårbare og giver nye muligheder for kriminelle aktiviteter. Disse kriminelle aktiviteter kan antage mange forskellige former og krydse mange grænser. Selv om der af forskellige årsager ikke findes nogen pålidelige statistikker, er der ikke meget tvivl om, at disse aktiviteter udgør en trussel for erhvervslivets investeringer og aktiver og for sikkerheden i og tilliden til informationssamfundet. En række eksempler fra den senere tid på manglende adgang til tjenester ("denial of service") og virusangreb har angiveligt anrettet omfattende finansiel skade.

Der er behov for at gribe ind både i form af at forhindre de kriminelle aktiviteter ved at højne sikkerheden i informationsinfrastrukturerne og ved at sikre, at de retshåndhævende myndigheder råder over de rette midler til at skride til handling, samtidig med at den enkeltes grundlæggende rettigheder respekteres fuldt ud.

Den Europæiske Union har allerede taget en række initiativer for at komme skadeligt og ulovligt indhold på Internettet til livs, beskytte intellektuelle ejendomsrettigheder og personoplysninger, fremme elektronisk handel og brug af elektroniske signaturer og fremme transaktionssikkerheden. I april 1998 forelagde Kommissionen resultatet af en undersøgelse om computerrelateret kriminalitet (den såkaldte 'COMCRIME'-undersøgelse) for Rådet. I oktober 1999 konkluderede Det Europæiske Råd på topmødet i Tammerfors, at hightech-kriminalitet skulle inkluderes i bestræbelserne på at nå til enighed om fælles definitioner og sanktioner. Europa-Parlamentet har også slået til lyd for almindeligt acceptable definitioner af computerrelaterede lovovertrædelser og for en effektiv indbyrdes tilnærmelse af lovgivningerne, især af den materielle strafferet. Rådet for Den Europæiske Union har vedtaget en fælles holdning til Europarådets forhandlinger om en konvention om Internetkriminalitet og har vedtaget en række grundlæggende elementer som led i EU's strategi mod hightech-kriminalitet. Nogle af EU-medlemsstaterne har også taget teten i relevante G8-aktiviteter.

Denne meddelelse drøfter, om der er behov for et omfattende politisk initiativ i sammenhæng med de bredere målsætninger for *informationssamfundet* og *frihed, sikkerhed og retfærdighed* og i overensstemmelse med Den Europæiske Unions engagement i forhold til at respektere de grundlæggende menneskerettigheder med henblik på at højne sikkerheden i informationsinfrastrukturerne og bekæmpe cyberkriminalitet, og hvilken form et sådant initiativ skulle have.

På kort sigt finder Kommissionen, at der er et klart behov for et EU-instrument til at sikre, at medlemsstaterne råder over effektive sanktioner til at bekæmpe børnepornografi på Internettet. Kommissionen vil senere i år fremlægge et forslag til en rammeafgørelse, som inden for den bredere sammenhæng af en pakke af foranstaltninger i relation til seksuel udnyttelse af børn og menneskehandel vil omfatte bestemmelser om indbyrdes tilnærmelse af lovbestemmelser og sanktioner.

På længere sigt vil Kommissionen fremlægge lovgivningsforslag for at tilvejebringe en yderligere indbyrdes tilnærmelse af den materielle strafferet inden for hightechkriminalitet. I overensstemmelse med konklusionerne fra Det Europæiske Råd i Tammerfors i oktober 1999 vil Kommissionen tillige overveje mulighederne for gensidig anerkendelse af kendelser afsagt forud for retssager i tilknytning til efterforskning i sager vedrørende Internetkriminalitet.

Sideløbende hermed agter Kommissionen at slå til lyd for, at der oprettes særlige politienheder til bekæmpelse af computerkriminalitet på nationalt plan i de lande, hvor de ikke allerede findes, at støtte passende teknisk uddannelse af personalet i de retshåndhævende myndigheder og at tilskynde til, at der tages initiativer på informationssikkerhedsområdet på EU-plan.

På det tekniske plan og i overensstemmelse med de retlige rammer vil Kommissionen fremme F&U med henblik på at forstå og reducere de sårbare punkter i informationssikkerheden og stimulere formidlingen af knowhow.

Kommissionen agter også at oprette et EU-forum, hvor de retshåndhævende myndigheder, Internetudbyderne, teleoperatørerne, borgerrettighedsorganisationerne, forbrugerrepræsentanter, databeskyttelsesmyndighederne og andre interesserede parter kan mødes med det formål at øge den gensidige forståelse og udbygge det gensidige samarbejde på EU-plan. Forummet skal søge at skærpe offentlighedens opmærksomhed over for de risici, som kriminelle personer frembyder på Internettet, fremme bedste praksis på sikkerhedsområdet, identificere effektive redskaber og procedurer til bekæmpelse af computerrelateret kriminalitet og tilskynde til videreudvikling af advarsels- og krisestyringsmekanismer.

OPFORDRING TIL AT FREMSÆTTE BEMÆRKNINGER TIL DENNE MEDDELELSE

Europa-Kommissionen vil gerne opfordre alle interesserede parter til at fremsætte bemærkninger til de spørgsmål, der behandles i denne meddelelse. Bemærkninger kan frem til den 23.03. 2001 indsendes via e-mail til følgende adresse:

Infso-jai-cybercrime-comments@cec.eu.int

Bemærkningerne vil principielt blive offentliggjort på Internettet, medmindre afsenderen udtrykkeligt anmoder om, at bemærkningerne ikke offentliggøres. Anonyme bemærkninger vil ikke blive offentliggjort. Kommissionen forbeholder sig ret til at undlade at offentliggøre bemærkninger, som den modtager (f.eks. hvis de kan virke stødende). Bemærkningerne vil være tilgængelige via et link på følgende websted:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Forslag vedrørende det tekniske format og nærmere oplysninger om offentliggørelses-politikken vil være tilgængelige på dette websted. Det tilrådes at konsultere dette websted, inden bemærkninger indsendes.

OFFENTLIG HØRING

Europa-Kommissionen vil også afholde en offentlig høring for interesserede parter om de spørgsmål, der behandles i meddelelsen. Denne høring vil blive afholdt den 07.03. 2001. Anmodninger om at modtage opfordring til at komme med indlæg på denne høring kan frem til den 20.02. 2001 indsendes via e-mail til følgende adresse:

Infso-jai-cybercrime-hearing@cec.eu.int

eller pr. brev til følgende adresse:

Europa-Kommissionen
Kontor BU33-5/9
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles
Belgien

Europa-Kommissionen forbeholder sig ret til at foretage en udvælgelse af de parter, som vil blive hørt. Foretages en sådan udvælgelse, vil den være baseret på antallet af anmodninger og ønsket om at opnå den bredest mulige repræsentation af forskellige interesser.

INDHOLDSFORTEGNELSE

1. MULIGHEDER OG RISICI I INFORMATIONSSAMFUNDET

Den stigende prisgunstighed og brug af informationssamfundets teknologier ("Information Society Technologies" (IST)) og globaliseringen af økonomien er vores æras kendetegn. Den fortsatte teknologiske udvikling og den øgede brug af åbne net som f.eks. Internettet gennem de kommende år vil give os store nye muligheder og stille os over for nye udfordringer.

På topmødet i Lissabon i marts 2000 understregede Det Europæiske Råd vigtigheden af overgangen til en konkurrencedygtig, dynamisk og videnbaseret økonomi og opfordrede Rådet og Kommissionen til at udarbejde en *e*Europe-handlingsplan for at udnytte denne mulighed bedst muligt[1]. Handlingsplanen, der er blevet udarbejdet af Kommissionen og Rådet og blev vedtaget på Det Europæiske Råd i Feira i juni 2000, omfatter initiativer til forbedring af netsikkerheden og udformning af en koordineret og sammenhængende strategi til bekæmpelse af cyberkriminalitet inden udgangen af 2002[2].

Informationsinfrastrukturen er blevet en kritisk del af vores økonomiers backbone. Brugerne skal kunne regne med, at informationstjenesterne er tilgængelige, og skal kunne have tillid til, at deres kommunikation og data er beskyttet mod uretmæssig adgang eller uretmæssige ændringer. Indførelsen af elektronisk handel og den fulde virkeliggørelse af informations-samfundet afhænger heraf.

De nye digitale og trådløse teknologier er allerede allestedsnærværende. De giver os friheden til at være mobile og alligevel altid tilsluttet, tilsluttet til et væld af tjenester, som bygger på net efter net. De giver os mulighed for at deltage, for at lære fra os og for at indlære, for at lege og arbejde sammen og for at involvere os i den politiske proces. I takt med at vores samfund bliver mere og mere afhængige af disse teknologier, bliver der større og større behov for effektive praktiske og retlige midler til at medvirke til at styre de tilknyttede risici.

Informationssamfundets teknologier ("Information Society Technologies" (IST)) kan benyttes og bliver benyttet til at udøve og bane vejen for forskellige kriminelle aktiviteter. I hænderne på personer, der handler i ond tro, i ond hensigt eller stærkt uagtsomt, kan disse teknologier blive redskaber for aktiviteter, som udsætter enkeltpersoners liv, ejendom eller værdighed for fare eller beskadigelse eller skader den offentlige interesse.

Den klassiske sikkerhedsmetode tog udgangspunkt i en streng organisatorisk, geografisk og strukturel opdeling af information alt efter graden af følsomhed eller art. Dette er ikke længere praktisk muligt i denne digitale verden, hvor informationsbehandlingen er distribueret, tjenesterne følger mobile brugere, og interoperabilitet mellem systemerne er en given ting. Innovative løsninger, der bygger på de fremvoksende teknologier, træder i stedet for de traditionelle sikkerhedsmetoder. Disse løsninger omfatter brug af kryptering og digitale signaturer, nye adgangskontrol- og autentifikationsværktøjer og softwarefiltre af enhver art[3]. Tilvejebringelsen af sikre og pålidelige informationsinfrastrukturer forudsætter ikke kun en bred vifte af teknologier, men også, at de indsættes korrekt og benyttes effektivt. Nogle af

---

1 Formandskabets konklusioner fra Det Europæiske Råd i Lissabon den 23. og 24. marts 2000, som findes på http://ue.eu.int/en/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.

3 Informationstrømmen filtreres og kontrolleres på alle niveauer; fra firewallen, som ser på datapakker, over filtret, der leder efter inficeret software, og e-mailfiltret, som diskret fjerner spam, til browserfiltret, som blokerer for adgangen til skadeligt materiale.

teknologierne findes allerede, men ofte er brugerne enten ikke klar over, at de findes, eller hvordan de benyttes, eller hvorfor de egentlig er nødvendige.

1.1. Reaktioner på nationalt og internationalt plan

Der begås computerrelateret kriminalitet i hele cyberspace, og den standser ikke ved de konventionelle landegrænser. Den kan i princippet begås alle vegne fra og over for en hvilken som helst computerbruger i verden. Det er almindeligt anerkendt, at for at bekæmpe computerrelateret kriminalitet er det nødvendigt med effektiv handling både på nationalt og internationalt plan[4].

På nationalt plan mangler der ofte stadig omfattende og internationalt orienterede reaktioner på de nye udfordringer, som netsikkerheden og computerkriminaliteten stiller. I de fleste lande fokuserer indgrebene over for computerkriminalitet på den nationale lovgivning (især strafferetten) og lader hånt om alternative forebyggende forholdsregler.

På trods af den indsats, der gøres i internationale og overnationale organisationer, udviser de forskellige nationale lovgivninger over hele verden bemærkelsesværdige forskelle, især hvad angår de strafferetlige bestemmelser om hacking, beskyttelse af forretningshemmeligheder og ulovligt indhold. Der er også betydelige forskelle i henseende til omfanget af de efterforskende myndigheders tvangsbeføjelser (især i forbindelse med krypterede data og efterforskninger i internationale net), udstrækningen af retternes kompetence i straffesager og forholdet mellem tjenesteudbydernes erstatningsansvar på den ene side og indholds-udbydernes erstatningsansvar på den anden. Direktiv 2000/31/EF[5] om elektronisk handel råder bod herpå hvad angår tjenesteudbydernes erstatningsansvar i forbindelse med visse formidlingsaktiviteter. Direktivet forbyder desuden medlemsstaterne at pålægge sådanne formidlende tjenesteudbydere en generel forpligtelse til at overvåge den information, de videregiver eller lagrer.

I internationale og overnationale kredse er der en bred erkendelse af behovet for en effektiv bekæmpelse af computerrelateret kriminalitet, og forskellige organisationer har koordineret eller forsøgt at harmonisere de relevante aktiviteter. Justits- og indenrigsministrene fra G8 vedtog et sæt af principper og en 10-punkts handlingsplan i december 1997, som fik tilslutning på G8-topmødet i Birmingham i juni 1998 og nu er under gennemførelse[6]. Europarådet indledte forberedelserne til en international konvention om Internetkriminalitet i februar 1997 og ventes at færdiggøre denne opgave i 2001[7]. Bekæmpelse af Internet-

---

4 Se f.eks. eEurope-handlingsplanen på
http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm
og erklæringer fra EU-kommissær Antõnio Vitorino på
http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf
og fra den franske premierminister Lionel Jospin på
http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("direktivet om elektronisk handel").

6 EU's Ministerråd (retlige og indre anliggender) gav den 19. marts 1998 sin tilslutning til de ti principper til bekæmpelse af hightechkriminalitet, som G8 havde vedtaget, og opfordrede de EU-medlemsstater, der ikke er G8-lande, til at træffe foranstaltninger til at tilslutte sig netværket.
Findes på European Judicial Network's websted på http://ue.eu.int/ejn/index.htm.

7 Konventionsteksten i udkastform findes på Internettet på to sprog: fransk:
http://conventions.coe.int/treaty/fr/projets/cybercrime.htm og engelsk:
http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

kriminalitet står også på dagsordenen for de bilaterale drøftelser, Europa-Kommissionen har med visse regeringer (uden for EU). Der er blevet opbygget en fælles EU-USA-taskforce for beskyttelse af kritisk infrastruktur[8]. FN og OECD har også været aktive på dette område, og spørgsmålet drøftes i internationale fora som Global Business Dialogue and Trans-Atlantic Business Dialogue[9].

På EU-plan har lovinitiativerne indtil for nylig hovedsagelig taget form af foranstaltninger inden for ophavsret, beskyttelse af den grundlæggende ret til privatlivets fred og databeskyttelse, adgangsstyrede og adgangsstyrende tjenester, elektronisk handel, elektroniske signaturer og især liberalisering af handelen med krypteringsprodukter, som indirekte har relation til computerkriminalitet.

Der er også blevet taget en række betydningsfulde foranstaltninger uden for lovgivningsområdet inden for de seneste 3-4 år. Disse omfatter handlingsplanen mod ulovligt og skadeligt indhold på Internettet, som samfinansierer oplysningskampagner, forsøg med klassificering og filtrering af indhold og hotlines og initiativer til beskyttelse af mindreårige og den menneskelige værdighed i informationssamfundet, på børnepornografiområdet og inden for aflytning af meddelelser til retshåndhævende formål[10]. EU har længe støttet F&U-projekter, der tager sigte på at højne sikkerheden i og tilliden til informationsinfrastrukturer og elektroniske transaktioner, og har for nylig forøget de hertil knyttede bevillinger under IST-programbudgettet. Forskning og operationelle projekter med henblik på fremme af specialuddannelse af retshåndhævende personale samt samarbejde mellem de retshåndhævende myndigheder og erhvervslivet har også fået støtte inden for rammerne af programmer under tredje søjle som STOP, FALCONE, OISIN og GROTIUS[11].

Handlingsplanen for bekæmpelse af organiseret kriminalitet, der blev vedtaget af Rådet (retlige og indre anliggender) i maj 1997 og fik tilslutning fra Det Europæiske Råd i Amsterdam, indeholdt en anmodning om udførelse af en undersøgelse om computerrelateret kriminalitet, som Kommissionen skulle udarbejde inden udgangen af 1998. Denne

---

8 Under den fælles rådgivende gruppe nedsat i medfør af samarbejdsaftalen om videnskab og teknologi mellem EU og USA (EC/US Science and Technology Co-operation Agreement).

9 De Forenede Nationer har udsendt en omfattende "Manual on the prevention and control of computer-related crime", som for nylig er blevet ajourført. I 1983 gennemførte OECD en undersøgelse af muligheden for, at de strafferetlige bestemmelser kunne anvendes og harmoniseres internationalt med henblik på at gøre noget ved problemet med computerkriminalitet og computermisbrug. I 1986 udsendte OECD "Computer-Related Crime: Analysis of Legal Policy", en rapport, som redegjorde for gældende love og forslagene til lovreformer i en række medlemsstater, og anbefalede en minimumsliste af misbrug, som landene burde overveje at forbyde eller straffe ved strafferetlige bestemmelser. Endelig opstillede OECD i 1992 et sæt retningslinjer for sikkerheden i informationssystemer, som skulle lægge det fundament, hvorpå de enkelte lande og den private sektor kunne udforme rammer for sikkerheden i informationssystemer.

10 Rådets henstilling 98/560/EF af 24. september 1998 om udvikling af den europæiske industris konkurrenceevne inden for audiovisuelle tjenester og informationstjenester gennem fremme af nationale rammer, der tager sigte på at opnå en sammenlignelig og effektiv beskyttelse af mindreårige og den menneskelige værdighed; grønbog om beskyttelse af mindreårige og den menneskelige værdighed i forbindelse med audiovisuelle tjenester og informationstjenester, KOM(96) 483, oktober 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm.
Meddelelse fra Kommissionen til Rådet, Europa-Parlamentet, Det Økonomiske og Sociale Udvalg og Regionsudvalget – Ulovligt og skadeligt indhold på Internet (KOM(96) 487 endelig udg.).
Beslutning om Kommissionens meddelelse om ulovligt og skadeligt indhold på Internet (KOM(96) 487 - C4-0592/96).
Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunication (EFT C 329 af 4.11.1996, s. 1– 6).

11 http://europa.eu.int/comm/justice_home/jai/prog_en.htm.

undersøgelse, den såkaldte 'COMCRIME-undersøgelse', blev forelagt af Kommissionen for Rådets tværfaglige arbejdsgruppe mod organiseret kriminalitet i april 1998[12]. Denne meddelelse er til dels en opfølgning af anmodningen fra Rådet (retlige og indre anliggender).

Inden Kommissionen udarbejdede meddelelsen, fandt den det betimeligt at gennemføre uformelle høringer med repræsentanter for medlemsstaternes retshåndhævende myndigheder og databeskyttelsestilsynsmyndigheder[13] og for det europæiske erhvervsliv (primært udbyderne af informationssamfundstjenester og teleoperatørerne)[14].

På basis af analysen og henstillingerne i undersøgelsen, konklusionerne fra høringsprocessen, de nye muligheder i Amsterdam-traktaten og det allerede udførte arbejde i EU, G8 og Europarådet behandler denne meddelelse forskellige muligheder for yderligere initiativer fra EU's side mod computerrelateret kriminalitet. På EU-plan bør de løsninger, der vælges, ikke skabe hindringer for og resultere i fragmentering af det indre marked og heller ikke til foranstaltninger, som undergraver beskyttelsen af de grundlæggende rettigheder[15].

2. SIKKERHEDEN I INFORMATIONSINFRASTRUKTURERNE

I informationssamfundet træder brugerkontrollerede globale net ind på den plads, den ældre generation af nationale kommunikationsnet førhen indtog. En af årsagerne til Internettets succes er, at det har givet brugerne adgang til de allernyeste teknologier. Moores lov[16] forudsiger, at datakraften fordobles hver 18. måned. Kommunikationsteknologien udvikler sig imidlertid endnu hurtigere[17]. Ét resultat heraf er, at mængden af data, der fremføres over Internettet, er blevet fordoblet inden for perioder på mindre end ét år.

De klassiske telefonnet blev bygget og drevet af nationale selskaber. Brugerne havde få valgmuligheder med hensyn til de udbudte tjenester og ingen kontrol over reguleringsmiljøet. De første datanet, der blev udviklet, blev opbygget efter den samme filosofi om et centralt kontrolleret miljø. Sikkerheden inden for disse miljøer afspejlede dette.

Internettet og de andre nye net er meget forskellige herfra, og sikkerhedsproblematikken skal håndteres i konsekvens heraf. Efterforskningen og kontrollen i disse net udføres for det meste

---

12 "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME". Undersøgelsen blev udført af professor U. Sieber fra Würzburgs universitet på kontrakt for Europa-Kommissionen. Rapporten findes i endelig form på: http://www2.echo.lu/legal/en/crime/crime.html.

13 På EU-plan udgøres databeskyttelsestilsynsmyndighederne af artikel 29-databeskyttelsesgruppen, som er et uafhængigt rådgivende organ på EU-plan inden for beskyttelse af privatlivets fred og databeskyttelse, se artikel 29 og 30 i direktiv 95/46/EF.

14 Der blev afholdt to møder med de retshåndhævende myndigheder den 10.12.1999 og den 1.3.2000. Der blev afholdt et møde med repræsentanter for Internetudbyderne den 13.3.2000. Der blev afholdt et møde med et mindre antal persondatabeskyttelseseksperter den 31.3.2000. Et endeligt møde med alle de ovennævnte fandt sted den 17.4.2000. Referat af møderne kan fås ved skriftlig henvendelse til Europa-Kommissionen, kontor INFSO/A5 eller til Europa-Kommissionen, kontor JAI/B2, Wetstraat/rue de la Loi 200, 1049 Bruxelles, Belgien.

15 EU-chartret om grundlæggende rettigheder (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), artikel 6 i traktaten om Den Europæiske Union og Domstolens retspraksis.

16 Bemærkningen tilbage i 1965 fra Gordon Moore, medstifter af Intel, om den hast, hvormed transistor-tætheden i integrerede kredsløb voksede. Denne tæthed bliver nu næsten fordoblet hver 18. måned, og dette har direkte betydning for prisen på og ydeevnen i computerchip. Mange eksperter forventer, at denne udvikling vil vare ved i mindst endnu et årti.

17 Den seneste teknologi gør det muligt for blot ét lyslederkabel at fremføre, hvad der svarer til 100 millioner telefonsamtaler samtidig.

i periferien, hvor brugerne og tjenesterne befinder sig. Kernen i nettet er enkel og effektiv og har til hovedopgave at transmittere data. Der sker kun begrænset verificering eller kontrol af indholdet. Dette sker først ved den endelige destination, hvor bittene bliver til lyden af en stemme, et røntgenbillede eller en bekræftelse på en banktransaktion. Sikkerheden er derfor i væsentlig grad brugernes ansvar, fordi det kun er dem, der kan vurdere værdien af de bit, der sendes eller modtages, og dermed kan afgøre, hvor højt et beskyttelsesniveau der er påkrævet.

Brugermiljøet er derfor en central del af informationsinfrastrukturen. Det er her, der skal træffes sikkerhedstekniske forholdsregler med brugerens tilladelse og deltagelse og ud fra hans eller hendes behov. Dette bliver stadig vigtigere, når man tænker på den voksende vifte af aktiviteter, folk udfører fra én og samme terminal. De arbejder og spiller, de ser tv og foretager bankoverførsler, alt sammen fra det samme apparat.

Der findes mange forskellige sikkerhedsteknologier, og nye teknologier er under udvikling. Fordelene for sikkerheden ved "open source"-udvikling bliver mere og mere åbenbare. Der er blevet udført meget arbejde med formelle metoder og sikkerhedsvurderingskriterier. Det bliver en uundgåelig praksis at benytte kryptering og digitale signaturer, især i betragtning af den stadig større udbredelse af trådløs adgang. Stadig mere varierede autentifikations-mekanismer er påkrævet for at opfylde vores forskellige behov i de miljøer, vi indgår i. I nogle miljøer kan det tænkes, at vi har behov for eller ønsker at bevare anonymiteten. I andre kan det tænkes, at vi har behov for at kunne bevise et bestemt kendetegn uden dog at afsløre vores identitet, f.eks. at der er tale om en voksen, en ansat eller en kunde hos en bestemt virksomhed. Igen i andre situationer kan det tænkes, at det er nødvendigt for os at bevise vores identitet. Softwarefiltre bliver mere og mere avancerede og sætter os i stand til at beskytte os selv eller personer i vores varetægt mod data, som vi ikke ønsker, f.eks. uønsket indhold, spampost, inficeret software og andre former for angreb. Implementeringen og forvaltningen af sådanne sikkerhedskrav på Internettet og i de nye net medfører desuden betydelige udgifter for erhvervslivet og brugerne. Det er derfor vigtigt at fremme innovation og kommerciel udnyttelse af sikkerhedsteknologier og -tjenester.

Den delte infrastruktur for kommunikationsforbindelser og navneservere har naturligvis også sine sikkerhedsaspekter. Datatransmission sker via de fysiske forbindelser, hvorved data dirigeres fra én computer til en anden. Disse forbindelser skal oprettes og beskyttes på en sådan måde, at transmissionen stadig kan lade sig gøre på trods af uheld, angreb og en stadig stigende trafikmængde. Kommunikation afhænger også af kritiske tjenester som dem, der ydes af navneserverne og især det lille antal navnerodservere, der tilvejebringer de nødvendige adresser. Hver af disse komponenter har også behov for passende beskyttelse, som varierer alt efter, hvilken del af navneområdet og brugerbasen der betjenes.

Drevet af målsætningen om større fleksibilitet og lydhørhed over for folks behov er informationsinfrastrukturteknologien blevet mere og mere kompleks med en ofte for utilstrækkelig sikkerhedsmæssig indsats i designfasen. Desuden omfatter denne kompleksitet mere og mere sofistikerede og sammenkoblede softwareprogrammer, som undertiden har svagheder og sikkerhedsmæssige lakuner, som er et nemt bytte ved angreb. I takt med at cyberspace bliver mere og mere komplekst og dets enkeltdele mere og mere sofistikerede, vil der kunne opstå nye og uforudsete sårbare punkter.

Der findes allerede adskillige teknologiske mekanismer til forbedring af sikkerheden i cyberspace, og der udvikles til stadighed nye. Det sikkerhedsmæssige svar skal omfatte foranstaltninger:

- til sikring af kritiske elementer i infrastrukturen gennem indsættelse af offentlig nøgle-infrastrukturer ("public-key infrastructures" (PKI)), udvikling af sikre protokoller osv.

- til sikring af det private og det offentlige miljø gennem udvikling af kvalitetssoftware, firewall, antivirusprogrammer, elektroniske rettighedsforvaltningssystemer, kryptering osv.

- til sikring af autentifikation af autoriserede brugere, brug af smartcard, biometrisk identifikation, elektroniske signaturer, rollebaserede teknologier osv.

Dette forudsætter en øget indsats for at udvikle sikkerhedsteknologi og et øget samarbejde, så der kan sikres den nødvendige interoperabilitet mellem de valgte løsninger gennem aftaler om internationale standarder.

Det er også vigtigt, at de fremtidige konceptuelle sikkerhedsmæssige rammer udgør en integreret del af den samlede arkitektur, der lige fra begyndelsen af designprocessen tager højde for trusler og sårbare punkter. Dette er en anderledes fremgangsmåde end de traditionelle lappeløsninger, som nødvendigvis har måttet benyttes i forsøget på at lukke de smuthuller, der udnyttes af det stadig mere sofistikerede kriminelle miljø.

EU's program for informationssamfundsteknologi ("Information Society Technologies" (IST))[18], især arbejdet vedrørende informations- og netsikkerhed og anden tillidsskabende teknologi[19], udgør rammen for udvikling af den tekniske kapacitet og teknologi, der er nødvendig for at forstå og møde de udfordringer, computerkriminaliteten frembyder. Denne teknologi omfatter tekniske værktøjer til beskyttelse mod krænkelse af den grundlæggende ret til privatlivets fred og af persondata og andre personlige rettigheder og til bekæmpelse af computerkriminalitet. Derudover er der i forbindelse med IST-programmet blev iværksat et driftssikkerhedsinitiativ. Dette initiativ skal medvirke til at opbygge tillid til stærkt indbyrdes forbundne informationsinfrastrukturer og tæt netværkssammenkoblede "embedded" systemer ved at fremme bevidstheden om driftssikkerhed og driftssikkerhedsforbedrende teknologi. En integreret del af dette initiativ er internationalt samarbejde. IST-programmet har opbygget et arbejdssamarbejde med DARPA og NSF og har i samarbejde med det amerikanske udenrigsministerium opbygget en fælles EU-USA-taskforce for beskyttelse af kritisk infrastruktur[20].

Endelig bidrager gennemførelsen af de sikkerhedskrav, som bl.a. følger af EU's databeskyttelsesdirektiver[21], til at højne netsikkerheden og sikkerheden i forbindelse med databehandling.

---

[18] IST-programmet forvaltes af Europa-Kommissionen. Det er en del af det femte rammeprogram, som løber fra 1998 til 2002. Mere udførlige oplysninger findes på http://www.cordis.lu/ist.

[19] Under nøgleaktion 2 - Nye arbejdsmetoder og elektronisk handel.

[20] Under den fælles rådgivende gruppe nedsat i medfør af samarbejdsaftalen om videnskab og teknologi mellem EU og USA (EC/US Science and Technology Co-operation Agreement).

[21] Se artikel 4 i direktiv 97/66/EF (herunder også en forpligtelse til at informere om særlige sikkerhedsricisi) og artikel 17 i direktiv 95/46/EF.

3. COMPUTERRELATERET KRIMINALITET

Moderne informations- og kommunikationssystemer gør det muligt på et hvilket som helst tidspunkt at udføre ulovlige aktiviteter fra et hvilket som helst sted til et hvilket som helst andet sted på jorden. Der findes ingen pålidelige statistikker om den computerrelaterede kriminalitets fulde omfang. De ulovlige indtrængninger, der hidtil er blevet sporet og rapporteret, underdriver formentlig problemets omfang. På grund af systemadministratorernes og brugernes ringe bevidsthed om og erfaring med problemet bliver mange indtrængninger ikke opdaget. Desuden er mange virksomheder på grund af den dårlige omtale og eksponering ikke villige til at rapportere tilfælde af computermisbrug. Mange politistyrker fører ikke statistikker over brugen af computere og kommunikationssystemer i forbindelse med disse og andre forbrydelser. Antallet af ulovlige aktiviteter kan ikke desto mindre forventes at vokse i takt med den øgede brug af computere og net. Der er et klart behov for at indsamle pålidelig dokumentation om omfanget af computerrelateret kriminalitet.

I denne meddelelse er der tale om computerrelateret kriminalitet i den bredeste betydning, nemlig enhver form for kriminalitet, som på den ene eller den anden måde indebærer brug af informationsteknologi. Der er dog forskellige opfattelser af, hvad udtrykket "computer-relateret kriminalitet" omfatter. Udtrykkene "computerkriminalitet", "computerrelateret kriminalitet", "hightechkriminalitet" og "cyberkriminalitet" bruges ofte i flæng til at betegne ét og samme fænomen. Der kan sondres mellem computerspecifik kriminalitet og traditionelle forbrydelser, der begås ved hjælp af computerteknologi. Et aktuelt eksempel herpå findes på toldområdet, hvor Internettet viser sig at blive benyttet som middel til at begå typiske overtrædelser af toldlovene som f.eks. smugling og falskneri. Mens computerspecifik kriminalitet kræver en opdatering af definitionen af kriminalitet i den nationale straffelov, kræver de traditionelle forbrydelser begået ved hjælp af computere øget samarbejde og forbedrede procedureforanstaltninger.

De forudsætter dog alle brug af informations- og kommunikationsnet, som ikke kender nogen grænser, og cirkulation af data, som er uhåndgribelige og ekstremt flygtige. Disse kendetegn betyder, at de eksisterende forholdsregler for at dæmme op for de ulovlige aktiviteter, der udføres på eller ved brug af disse net og systemer, skal tages op til revision.

Mange lande har vedtaget lovgivning til bekæmpelse af computerrelateret kriminalitet. I EU's medlemsstater er en række lovinstrumenter blevet taget i brug. Ud over en rådsafgørelse om børnepornografi på Internettet findes der indtil videre ingen EU-lovinstrumenter, der direkte tager computerrelateret kriminalitet op, men der er en række lovinstrumenter, der indirekte er relevante.

De hovedspørgsmål, der tages op i lovgivningen om computerspecifik kriminalitet på EU- og medlemsstatsplan, er:

Krænkelser af privatlivets fred: Forskellige lande har vedtaget straffelovsbestemmelser om ulovlig indsamling, opbevaring, ændring, videregivelse eller formidling af personoplysninger. I EU er der blevet vedtaget to direktiver, som indebærer en indbyrdes tilnærmelse af medlemsstaternes lovgivning om beskyttelsen af privatlivets fred i forbindelse med

behandling af personoplysninger[22]. Artikel 24 i direktiv 95/46/EF forpligter utvetydigt medlemsstaterne til at vedtage alle passende foranstaltninger for at sikre fuld gennemførelse af direktivets bestemmelser, herunder også sanktioner, som skal finde anvendelse i tilfælde af overtrædelse af bestemmelserne i de nationale love. Den grundlæggende ret til privatlivets fred og beskyttelse af personoplysninger er desuden inkluderet i Den Europæiske Unions charter om grundlæggende rettigheder.

Indholdsrelaterede krænkelser: Spredningen, navnlig via Internettet, af pornografi, især børnepornografi, racistiske ytringer og information, der opfordrer til voldsanvendelse, rejser spørgsmålet om, i hvor høj grad disse handlinger kan imødegås ved hjælp af straffeloven. Kommissionen har forfægtet det synspunkt, at hvad der er ulovligt offline bør også være ulovligt online. Ophavsmanden eller indholdsudbyderen[23] vil kunne ifalde ansvar efter straffeloven. Der er blevet vedtaget en rådsafgørelse til bekæmpelse af børnepornografi på Internettet[24].

Erstatningsansvaret hos formidlende tjenesteudbydere, hvis net eller servere benyttes til transmission eller oplagring af information fra tredjemand, er blevet behandlet i direktivet om elektronisk handel.

Økonomisk kriminalitet, ulovlig indtrængning og sabotage: Mange lande har vedtaget love, som drejer sig om computerspecifik økonomisk kriminalitet og definerer nye lovovertrædelser i tilknytning til ulovlig indtrængning i computersystemer (f.eks. hacking, computersabotage og rundsendelse af viruser, computerspionage, computerfalsk og computerbedrageri[25]) og nye former at begå lovovertrædelser under (f.eks. computermanipulationer i stedet for at bedrage mennesker). Genstanden for kriminaliteten er ofte håndgribelig, f.eks. penge på bankkonti eller computerprogrammer. På nuværende tidspunkt findes der ingen EU-lovinstrumenter vedrørende disse former for ulovlig aktivitet. Hvad forebyggelsen angår, har den nyligt vedtagne forordning om varer med dobbelt anvendelsesformål i væsentlig grad bidraget til at liberalisere adgangen til krypteringsprodukter.

Krænkelser af intellektuelle ejendomsrettigheder: Der er blevet vedtaget to direktiver, ét om beskyttelse af edb-programmer og ét om databaser[26], som har direkte relation til informationssamfundet og fastsætter sanktioner. Rådet har fastlagt en fælles holdning til et direktivforslag om ophavsret og beslægtede rettigheder i informationssamfundet. Det ventes

---

22 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og Europa-Parlamentets og Rådets direktiv 97/66/EF af 15. december 1997 om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren. Artikel 24 i direktiv 95/46/EF forpligter medlemsstaterne til at fastsætte sanktioner, som kan pålægges i tilfælde af overtrædelse af databeskyttelsesbestemmelserne.

23 Indholdsudbyderen må ikke forveksles med tjenesteudbyderen.

24 Rådets afgørelse af 29. maj 2000 om bekæmpelse af børnepornografi på Internettet (EFT L 138 af 9.6.2000, s.1).

25 Medierne har udvist stor opmærksomhed over for de seneste distribuerede "denial of service"-angreb på store websteder og rundsendelsen af den såkaldte "LoveBug"-virus. Dette skal dog ses i perspektiv. "Denial of service"-angreb, hvad enten de er forsætlige eller uforsætlige, og e-mailrelaterede viruser har eksisteret i mange år. "Morris"-ormen og "IBM Xmas-tree"-e-mailen er tidligere eksempler herpå. Der findes produkter og procedurer, som hjælper med til at neutralisere dem. Der findes også et omfattende og godt samarbejde i Internetkredse om at begrænse skaderne fra sådanne hændelser, når de indtræffer. Der er et tilsvarende samarbejde for at begrænse spammingmisbrug.

26 Rådets direktiv 91/250/EØF af 14. maj 1991 om retlig beskyttelse af edb-programmer (EFT L 122 af 17.5.1991, s. 42 – 46).
Europa-Parlamentets og Rådets direktiv 96/9/EF af 11. marts 1996 om retlig beskyttelse af databaser (EFT L 77 af 27.3.1996, s. 20 – 28).

vedtaget i begyndelsen af 2001[27]. Krænkelsen af ophavsretten og beslægtede rettigheder samt omgåelse af de teknologiske forholdsregler, der træffes for at beskytte disse rettigheder, skal sanktioneres. Hvad angår falskneri og piratkopiering, vil Kommissionen inden udgangen af 2000 udsende en meddelelse, der går status over den høringsproces, der blev igangsat med grønbogen fra 1998, og hvori der fremlægges en relevant handlingsplan. Efterhånden som Internettet får større og større betydning kommercielt set, ser man nye tvister opstå omkring domænenavne i forbindelse med pirateri ("cybersquatting"), "warehousing" og "reverse hijacking", og dette følges naturligvis også af opfordringer til at fastsætte regler og procedurer for at søge at løse disse problemer[28].

Problematikken i forbindelse med håndhævelsen af skattebestemmelserne skal også tages op. Kommercielle transaktioner, hvor modtageren af en elektronisk onlinetjeneste befinder sig i EU, vil i de fleste tilfælde give anledning til skattemæssige forpligtelser i det land, hvor tjenesten formodes at være blevet forbrugt[29]. Ved manglende opfyldelse af de skattemæssige forpligtelser udsætter en operatør sig for civilretlige (og i nogle tilfælde strafferetlige) sanktioner, som kan omfatte beslaglæggelse af bankkonti og andre aktiver. Selv om frivillig overholdelse altid er at foretrække, skal sådanne forpligtelser i sidste ende kunne håndhæves. Samarbejde mellem skatteforvaltningerne er et nøgleelement i forbindelse med at opfylde denne målsætning.

Hvis man giver nogle mennesker mulighed for at beskytte deres lovlige transaktioner, giver man også kriminelle de samme midler til at beskytte deres ulovlige transaktioner. De redskaber, som giver os en sikker e-handel, kan også benyttes til at støtte narkohandelen. Der må derfor opstilles nogle prioriteter, og der må foretages nogle valg.

Beskyttelsen af ofrene for computerrelateret kriminalitet skal også omfatte spørgsmål som erstatningsansvar, klagemuligheder og erstatning, som opstår, når der begås computerrelaterede forbrydelser. Opbygningen af tillid afhænger ikke blot af, at den rette teknologi benyttes, men også af, at der stilles tilhørende retlige og økonomiske garantier. Disse spørgsmål skal tages op i forbindelse med hele viften af computerrelaterede forbrydelser.

Der er behov for effektive materielretlige og procesretlige lovinstrumenter, som er indbyrdes tilnærmede på verdensplan eller i det mindste på EU-plan, og som kan yde skadelidte beskyttelse i forbindelse med computerrelateret kriminalitet og bringe lovovertræderne for retten. Samtidig er personlig kommunikation, privatlivets fred og databeskyttelse samt adgangen til og formidlingen af information grundlæggende rettigheder i moderne demokratier. Det er derfor, at det er ønskeligt, at der findes forebyggende foranstaltninger, som kan bringes i anvendelse for at mindske behovet for håndhævende foranstaltninger.

---

27 Fælles holdning fastlagt af Rådet med henblik på vedtagelse af Europa-Parlamentets og Rådets direktiv om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (CS/2000/9512).

28 Meddelelse fra Kommissionen til Rådet og Europa-Parlamentet, "Internettets organisation og administration; politiske aspekter på internationalt og europæisk plan 1998 - 2000", april 2000, KOM(2000) 202.

29 Kommissionen har foreslået en række ændringer af EU's momssystem med det sigte at præcisere, i hvilket land skattetilsvaret falder (KOM(2000) 349 - forslag til Rådets direktiv om ændring af direktiv 77/388/EØF hvad angår merværdiafgiftssystemet for visse tjenesteydelser, der leveres ad elektronisk vej). Forslaget er for øjeblikket til behandling i Rådet og Parlamentet. I nogle tilfælde falder skattetilsvaret på leverandøren, også selv om leverandøren ikke fysisk er etableret i det beskattende land.

Enhver lovforanstaltning, som kan blive nødvendig for at bekæmpe computerrelateret kriminalitet, skal finde den rette balance mellem disse vigtige interesser.

4. MATERIELRETLIGE SPØRGSMÅL

En indbyrdes tilnærmelse af de materielle lovbestemmelser om hightechkriminalitet vil sikre en minimumsbeskyttelse af ofrene for Internetkriminalitet (f.eks. ofrene for børnepornografi), vil bidrage til at opfylde kravet om, at en aktivitet skal være en lovovertrædelse i begge land, inden der kan ydes gensidig retshjælp i forbindelse med en kriminel efterforskning (dobbeltkriminalitetskravet), og vil give større klarhed for erhvervslivet (f.eks. om, hvad der skal anses for at være ulovligt indhold).

Rent faktisk har et EU-lovinstrument, der sikrer en indbyrdes tilnærmelse af den materielle strafferet i relation til computerrelateret kriminalitet, været på EU-dagsordenen siden Det Europæiske Råds møde i Tammerfors i oktober 1999[30]. På topmødet blev hightechkriminalitet indføjet på en begrænset liste over områder, hvor der skulle gøres en indsats for at nå til enighed om fælles definitioner, sigtelser og sanktioner. Dette er inkluderet i henstilling nr. 7 i EU's strategi for det nye årtusind om forebyggelse og bekæmpelse af organiseret kriminalitet, som blev vedtaget af Rådet (retlige og indre anliggender) i marts 2000[31]. Spørgsmålet indgår også i Kommissionens arbejdsprogram for år 2000 og resultattavlen for et EU med frihed, sikkerhed og retfærdighed, som Kommissionen har udarbejdet, og som blev vedtaget af Rådet (retlige og indre anliggender) den 27. marts 2000[32].

Kommissionen har fulgt Europarådets arbejde med konventionen om Internetkriminalitet. Der anføres fire kategorier af strafferetlige lovovertrædelser i det nuværende udkast til Europarådets konvention om Internetkriminalitet: 1) lovovertrædelser i relation til fortroligheden, integriteten og disponibiliteten af computerdata og computersystemer, 2) computerrelaterede lovovertrædelser, 3) indholdsrelaterede lovovertrædelser og 4) ophavsretlige lovovertrædelser og lovovertrædelser inden for hermed beslægtede rettigheder.

En indbyrdes tilnærmelse på EU-plan kunne gå videre end Europarådets konvention, som repræsenterer et minimum af international indbyrdes tilnærmelse. Den vil kunne træde i kraft hurtigere end Europarådets konvention[33]. Den vil bringe computerkriminalitet ind under EU-retten og indføre håndhævelsesmekanismer på EU-plan.

Kommissionen lægger stor vægt på, at EU formår at gribe effektivt ind over for især børnepornografi på Internettet. Kommissionen hilser Rådets afgørelse om bekæmpelse af børnepornografi på Internettet velkommen, men deler Europa-Parlamentets synspunkt om, at der er behov for yderligere initiativer for at sikre større indbyrdes tilnærmelse i de nationale lovgivninger. Kommissionen agter senere i år at fremlægge et udkast til Rådets rammeafgørelse, som vil indeholde bestemmelser om indbyrdes tilnærmelse af lovgivningerne og sanktionerne om børnepornografi på Internettet[34].

---

30 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

31 Forebyggelse og bekæmpelse af organiseret kriminalitet: En EU-strategi for begyndelsen af det nye årtusind (EFT C 124 af 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_en.htm.

33 Europarådets konvention træder først i kraft efter at være blevet ratificeret.

34 Dette initiativ er en del af en pakke af forslag, som også dækker bredere emner i relation til seksuel udnyttelse af børn og menneskehandel, som det blev bebudet i Kommissionens meddelelse om menneskehandel fra december 1998. Teksten til forslaget til Rådets rammeafgørelse er vedlagt meddelelsen fra Kommissionen til Rådet og Europa-Parlamentet om bekæmpelse af menneskehandel og

I overensstemmelse med konklusionerne fra topmødet i Tammerfors vil Kommissionen fremlægge et lovforslag under afsnit VI i traktaten om Den Europæiske Union om indbyrdes tilnærmelse af bestemmelserne om hightechlovovertrædelser. Det vil tage udgangspunkt i de fremskridt, der er gjort i Europarådet og vil især imødekomme behovet for indbyrdes tilnærmelse af lovgivningen om hacking og "denial of service"-angreb. Forslaget vil omfatte standarddefinitioner til brug for Den Europæiske Union på dette felt. Forslaget kunne også gå videre end udkastet til Europarådets konvention ved at sikre, at alvorlige tilfælde af hacking og "denial of service"-angreb straffes med en minimumsstraf i alle medlemsstater.

Desuden vil Kommissionen undersøge mulighederne for at gribe ind over for racisme og fremmedhad på Internettet med henblik på at forelægge et forslag til Rådets rammeafgørelse i henhold til afsnit VI i traktaten om Den Europæiske Union om racisme og fremmedhad både offline og online. I denne forbindelse vil den tage hensyn til den kommende evaluering af medlemsstaternes gennemførelse af den fælles aktion af 15. juli 1996 om initiativer til bekæmpelse af racisme og fremmedhad[35]. Den fælles aktion var et første skridt i retning af at sikre indbyrdes tilnærmelse af adfærden over for kriminelle handlinger i relation til racisme og fremmedhad, men det er nødvendigt med yderligere indbyrdes tilnærmelse inden for EU. Hvor vigtigt og sensibelt dette spørgsmål er, blev sat i relief af en fransk domstols afgørelse den 20. november 2000, der krævede, at Yahoo skulle blokere for franske brugere adgang til websteder, der sælger memorabilia fra nazitiden[36].

Endelig agter Kommissionen at overveje, hvordan bekæmpelsen af den ulovlige narkohandel på Internettet kan effektiviseres, idet vigtigheden af dette spørgsmål blev anerkendt i EU's narkostrategi for 2000-2004, som Det Europæiske Råd i Helsingfors gav sin fulde opbakning[37].

5. PROCESRETLIGE SPØRGSMÅL

Selve karakteren af computerrelaterede lovovertrædelser bringer processuelle spørgsmål frem i rampelyset på den nationale og internationale arena, fordi forskellige nationale suveræniteter, retsområder og lovgivninger gør sig gældende. I højere grad end inden for nogen anden form for grænseoverskridende kriminalitet udgør hastigheden, mobiliteten og fleksibiliten i computerkriminalitet en udfordring for de gældende procedureregler inden for strafferetten.

En indbyrdes tilnærmelse af procedurereglerne vil forbedre beskyttelsen af skadelidte, fordi det sikres, at de retshåndhævende myndigheder har de beføjelser, der er nødvendige for at efterforske lovovertrædelser på deres eget område, og vil sikre, at de kan reagere hurtigt og effektivt på anmodninger om samarbejde fra andre lande.

---

seksuel udnyttelse af børn, to forslag til rammeafgørelser, som offentliggøres sideløbende med denne meddelelse.

35 EFT L 185 af 24.7.1996, s. 5-7. Også tilgængelig på European Judicial Networks websted http://ue.eu.int/ejn/index.htm.

36 Tribunal de Grande Instance de Paris, Ordonnance de Référé afsagt den 20. november 2000, nr. RG 00/05308.

37 Den Europæiske Unions handlingsplan for bekæmpelse af narkotikamisbrug (2000-2004). KOM(1999)239 endelig udg. http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

Det er også vigtigt at sikre, at foranstaltninger truffet på basis af strafferetten, som generelt henhører under medlemsstaternes kompetence og afsnit VI i traktaten om Den Europæiske Union, er i overensstemmelse med kravene i fællesskabsretten. Bl.a. har EF-Domstolen konsekvent statueret, at sådanne lovbestemmelser ikke må diskriminere mod personer, som fællesskabsretten tildeler ret til lige behandling, eller begrænse de ved fællesskabsretten garanterede grundlæggende friheder[38]. Eventuelle nye retshåndhævende beføjelser skal vurderes i forhold til fællesskabsretten og til deres indvirkning på privatlivets fred.

5.1. Aflytning af kommunikation

I EU gælder der et generelt princip om, at kommunikation (og de hertil knyttede trafikdata) er fortrolig. Aflytning er ulovlig, medmindre den er godkendt ved lov, når dette er nødvendigt i særlige tilfælde til begrænsede formål. Dette følger af artikel 8 i den europæiske menneskerettighedskonvention, der omtales i artikel 6 i traktaten om Den Europæiske Union, og nærmere betegnet af direktiv 95/46/EF og direktiv 97/66/EF.

Alle medlemsstater har retlige rammer, som giver de retshåndhævende myndigheder mulighed for at indhente domstolskendelser (eller for to medlemsstaters vedkommende en domstolskendelse med en personlig beføjelse fra en ledende minister) med henblik på aflytning af kommunikation på det offentlige telenet[39]. Denne lovgivning, som skal være i overensstemmelse med fællesskabsretten, for så vidt som denne finder anvendelse, indeholder generelt garantier til beskyttelse af den enkeltes grundlæggende ret til privatlivets fred, f.eks. i form af at begrænse brugen af aflytning til efterforskning af alvorlige forbrydelser, kræve, at aflytning i enkeltsager skal være nødvendig og proportional, eller sikre, at den enkelte informeres om aflytningen, i samme øjeblik dette ikke længere hindrer efterforskningen. I mange medlemsstater indeholder lovgivningen om aflytning bestemmelser, der forpligter (public service)-teleoperatørerne til at give teknisk mulighed for aflytning. En rådsresolution fra 1995 tog sigte på at samordne kravene til aflytning[40].

De traditionelle netoperatører, især dem, der udbyder taletjenester, har tidligere etableret arbejdsrelationer med de retshåndhævende myndigheder med henblik på at bane vejen for lovlig aflytning af kommunikation. Liberaliseringen af telesektoren og den eksplosive vækst i brugen af Internettet har tiltrukket mange nye aktører på markedet, som derved er blevet stillet over for krav om mulighed for aflytning. Spørgsmål vedrørende reguleringen, de tekniske

---

38 Sag C-274/96, Bickel & Franz (1998), Sml. I-7637, punkt 17, sag C-186/87, Cowan (1989), Sml. 195, punkt 19. Bl.a. må de administrative forholdsregler og sanktioner ikke gå videre end til det, der er strengt nødvendigt, kontrolprocedurerne må ikke være udformet således, at de begrænser den ved traktaten garanterede frihed, og de må ikke ledsages af sanktioner, som står i et sådant misforhold til overtrædelsens alvor, at de kommer til at udgøre en hindring for udøvelsen af denne frihed (sag C-203/80, Casati (1981), Sml. 2595, punkt 27.

39 To medlemsstater tillader ikke, at aflyttede meddelelser benyttes som bevismateriale i straffesager.

40 Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation (EFT C 329 af 4.11.1996, s. 1– 6). Bilaget indeholder en liste over retshåndhævende aflytningskrav, som medlemsstaterne blev anmodet om at tage hensyn til ved udformningen og gennemførelsen af relevante nationale politikker og foranstaltninger. I 1998 fremlagde det østrigske formandskab et forslag til en EU-rådsresolution, som skulle udvide resolutionen fra 1995 til at omfatte nye teknologier, herunder Internet- og satellitkommunikation. Forslaget har været debatteret i to udvalg i Europa-Parlamentet, nemlig Udvalget om Borgernes Friheder og Indre Anliggender og Udvalget om Retsvæsen og Borgernes Rettigheder, som nåede til forskellige konklusioner. Førstnævnte udvalg anså resolutionen for at være en præcisering og ajourføring af den gamle og fandt, at den var acceptabel. Sidstnævnte udvalg var stærkt kritisk, både hvad angår de potentielle menneskerettighedskrænkelser og omkostningerne for operatørerne, og afviste EU-Rådets forslag og opfordrede Kommissionen til at udarbejde et nyt forslag, når Amsterdam-traktaten var trådt i kraft. Udkastet til Rådets resolution er ikke i løbet af de seneste måneder blevet aktivt behandlet i Rådet eller dets arbejdsgrupper.

muligheder, fordelingen af udgifterne og den kommercielle indvirkning må drøftes i en dialog mellem regeringen og den berørte sektor samt alle øvrige berørte parter, herunder databeskyttelsestilsynsmyndighederne.

De nye teknologier gør det afgørende, at medlemsstaterne samarbejder, hvis de skal bibeholde deres muligheder for lovlig aflytning af kommunikation. Skulle medlemsstaterne indføre nye tekniske aflytningskrav over for teleoperatørerne og Internettjenesteudbyderne, finder Kommissionen, at disse krav bør koordineres internationalt, så man forhindrer fordrejning på det indre marked, reducerer omkostningerne for erhvervslivet mest muligt og opfylder kravene vedrørende privatlivets fred og databeskyttelse. Kravene bør så vidt muligt være offentlige og åbne og bør ikke svække kommunikationsinfrastrukturen.

Inden for rammerne af EU-konventionen om gensidig retshjælp i straffesager[41] er der blevet aftalt en metode til fremme af samarbejdet om lovlig aflytning[42]. Konventionen indeholder bestemmelser om aflytning af satellittelefonkommunikation[43] og om aflytning af en persons kommunikation på en anden medlemsstats område[44]. Kommissionen finder, at aflytningsreglerne i konventionen om gensidig retshjælp udgør det højest opnåelige på dette stadium. Konventionens ordlyd er teknologineutral; det skal afprøves, hvordan den virker i praksis, inden det kan overvejes at foretage forbedringer. Kommissionen vil vurdere dens gennemførelse sammen med medlemsstaterne, erhvervslivet, brugerne og databeskyttelses-tilsynsmyndighederne for at sikre, at de relevante initiativer er effektive, gennemsigtige og velafbalancerede.

En overdreven og vilkårlig brug af mulighederne for aflytning, især internationalt, vil rejse menneskerettighedsspørgsmål og underminere borgernes tillid til informationssamfundet. Kommissionen ser med stor bekymring på rapporter om påstået misbrug af mulighederne for aflytning[45].

---

41 EFT C 197 af 12.7.2000, s. 1. Konventionen blev vedtaget den 29. maj 2000. Bestemmelserne om aflytning i konventionen gælder kun for EU's medlemsstater og ikke for tredjelande.

42 Konventionen indeholder minimumsgarantier vedrørende beskyttelse af privatlivets fred og personoplysninger.

43 Det oprindelige formål med forhandlingerne var at åbne op for aflytning af personer, der benytter satellittelefoner på den aflyttende medlemsstats område. Teknisk set er det kritiske punkt ved aflytningen af sådan kommunikation satellitjordstationen. Det var derfor nødvendigt at søge teknisk bistand fra den medlemsstat, hvor jordstationen er beliggende. Konventionen giver to muligheder for at løse denne situation: en hurtig procedure for gensidig retlig bistand, som forudsætter en individuel forespørgsel om bistand til den medlemsstat, hvor satellitjordstationen ligger, og en teknisk løsning, som bygger på fjernadgang til satellitjordstationen fra den aflyttende medlemsstat, som ikke forudsætter en individuel forespørgsel.

44 Konventionen udgør også lovrammen for anmodninger om aflytning af en persons kommunikation på en anden medlemsstats område (den medlemsstat, anmodningen er rettet til). I så fald skal både den aflyttende medlemsstat og den medlemsstat, anmodningen er rettet til, indhente aflytningsdommer-kendelser efter deres nationale lovgivning. Endelig opstiller konventionen regler for situationer, hvor den aflyttende medlemsstat har mulighed for at aflytte kommunikation, der foretages af en person på en anden medlemsstats område, uden at der er behov for at søge teknisk bistand fra denne medlemsstat.

45 En lang og udførligt dokumenteret rapport fra Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) om et efterretnings- og aflytningsnetværk benævnt ECHELON blev behandlet ved en offentlig høring i Europa-Parlamentet. Rapporten hævder, at ECHELON blev opbygget til formål i relation til den nationale sikkerhed, men at det også blev benyttet til industrispionage. Europa-Parlamentet har nedsat et midlertidigt udvalg, som skal undersøge sagen og aflægge rapport for plenarforsamlingen inden for et år.

5.2. Opbevaring af trafikdata

For at kunne efterforske og retsforfølge forbrydelser, der begås ved brug af kommunikationsnettene, herunder Internettet, benytter de retshåndhævende myndigheder ofte trafikdata, når disse data opbevares af tjenesteudbyderne til faktureringsformål. Eftersom afstanden og destinationen bliver mindre og mindre bestemmende for prisen for en kommunikation, og tjenesteyderne går over til fakturering til fast pris, vil der ikke længere være behov for at opbevare trafikdata til faktureringsformål. De retshåndhævende myndigheder frygter, at dette vil reducere det potentielle materiale til brug for efterforskningen i straffesager, og slår derfor til lyd for, at tjenesteudbyderne opbevarer visse trafikdata i det mindste i et vist minimumstidsrum, så dataene kan benyttes til retshåndhævende formål[46].

I henhold til EU-direktiverne om beskyttelse af personoplysninger, både principperne om generel begrænsning i direktiv 95/46/EF og de mere specifikke bestemmelser i direktiv 97/66/EF, skal trafikdata slettes eller anonymiseres umiddelbart efter leveringen af teletjenesten, medmindre de er nødvendige til faktureringsformål. Når der er tale om teletjenester til fast pris eller til gratis afbenyttelse, har tjenesteudbyderne principielt ikke lov til at opbevare trafikdata.

Ifølge EU's databeskyttelsesdirektiver må medlemsstaterne vedtage lovforanstaltninger med henblik på at begrænse rækkevidden af forpligtelsen til at slette trafikdata, hvis dette er en nødvendig foranstaltning af hensyn til bl.a. forebyggelse, efterforskning, opklaring og retsforfølgning i straffesager eller af ulovlig brug af telekommunikationssystemet[47].

Enhver national lovforanstaltning, som kan åbne mulighed for opbevaring af trafikdata til retshåndhævende formål, skal dog opfylde visse betingelser: de foranstaltninger, der påtænkes truffet, skal være passende, nødvendige og proportionale, som det kræves i fællesskabsretten og i international ret, bl.a. i direktiv 97/66/EF og direktiv 95/46/EF, den europæiske menneskerettighedskonvention af 4. november 1950 og Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger. Dette er særlig relevant for foranstaltninger, som indebærer, at der rutinemæssigt ville blive opbevaret data om en stor del af en given befolkning.

Nogle medlemsstater er i færd med at tage lovinitiativer, der tillader eller stiller krav til tjenesteudbyderne om at opbevare visse kategorier af trafikdata, som ikke er nødvendige til faktureringsformål, efter at tjenesten er leveret, men som anses for nyttige for efterforskningen i straffesager.

Disse initiativer varierer betydeligt i omfang og form, men de bygger alle på den idé, at der skal kunne stilles flere data til disposition for de retshåndhævende myndigheder, end hvad der ville være tilfældet, hvis tjenesteudbyderne kun behandlede data, som er strengt nødvendige af hensyn til leveringen af tjenesten. Kommissionen er ved at vurdere disse foranstaltninger ud fra gældende fællesskabsret.

---

[46] Disse ville omfatte efterforskning i straffesager, som ikke har forbindelse med computere eller kommunikationsnettene, men hvor dataene kan være en hjælp til at opklare forbrydelsen.

[47] Artikel 14 i direktiv 97/66/EF og artikel 13 i direktiv 95/46/EF.

Europa-Parlamentet er lydhørt i spørgsmål vedrørende privatlivets fred og går generelt ind for en stærk beskyttelse af personoplysninger. I forbindelse med drøftelserne om bekæmpelse af børnepornografi på Internettet har Europa-Parlamentet imidlertid givet udtryk for, at der skulle være en generel forpligtelse til at opbevare trafikdata i tre måneder[48].

Dette illustrerer den vigtige sammenhæng, hvori et ømtåleligt emne som opbevaring af trafikdata drøftes, og den udfordring, de politiske beslutningstagere står over for i forsøget på at finde den rette balance i denne forbindelse.

Kommissionen finder, at enhver løsning af den komplicerede problematik med opbevaring af trafikdata bør være velbegrundet, proportional og sikre en rimelig balance mellem de forskellige implicerede interesser. Det er kun ved at forene statens, erhvervslivets, databeskyttelsestilsynsmyndighedernes og brugernes ekspertise og kapacitet, at det vil kunne lykkes at opfylde disse mål. Det vil være yderst ønskeligt med en sammenhængende approach, hvis man skal opfylde målsætningerne om både effektivitet og proportionalitet, og hvis man skal undgå en situation, hvor både de retshåndhævende myndigheder og Internetmiljøet bliver stillet over for et sammensurium af forskelligartede tekniske regler og lovrammer.

Der findes helt andre og betydningsfulde spørgsmål, der skal tages i betragtning. På den ene side har databeskyttelsestilsynsmyndighederne tilkendegivet, at det mest effektive middel til at mindske uacceptable risici for privatlivets fred og samtidig anerkende behovet for en effektiv retshåndhævelse er, at trafikdata principielt ikke kun bør kunne opbevares til retshåndhævende formål[49]. På den anden har de retshåndhævende myndigheder erklæret, at opbevaring af en minimumsmængde af trafikdata i et minimumstidsrum efter deres opfattelse er nødvendig som en hjælp til efterforskningen i straffesager.

Erhvervslivet har en interesse i at samarbejde om bekæmpelsen af forbrydelser som hacking og computerfalsk, men bør ikke stilles over for foranstaltninger, som er urimeligt bekostelige. Den økonomiske virkning af foranstaltninger af enhver aft skal nøje analyseres og sammenholdes med foranstaltningens effektivitet i bekæmpelsen af Internetkriminalitet, så det undgås, at Internettet bliver dyrere og derved mindre økonomisk overkommeligt for brugerne. Der må sikres en passende sikkerhed for opbevarede trafikdata.

Under alle omstændigheder spiller erhvervslivet en nøglerolle ved at medvirke i processen til skabelse af et sikrere informationssamfund. Brugerne bør have tillid til sikkerheden i informationssamfundet og føle sig beskyttet mod kriminalitet og krænkelser af privatlivets fred.

Kommissionen giver sin fulde opbakning til og slår til lyd for en konstruktiv dialog mellem de retshåndhævende myndigheder, erhvervslivet, databeskyttelsesmyndighederne og forbrugerorganisationerne samt andre parter, som kan være impliceret. Inden for rammerne af

---

48 Lovgivningsmæssig beslutning med Europa-Parlamentets udtalelse om udkast til fælles aktion vedtaget af Rådet på grundlag af artikel K.3 i traktaten om Den Europæiske Union om bekæmpelse af børnepornografi på Internettet, ændring 17 (EFT C 219 af 30.7.1999, s. 68 ff., s. 71).

49 "Omfattende efterforskende eller generel overvågning skal være forbudt … det mest effektive middel til at mindske uacceptable risici for privatlivets fred og samtidig anerkende behovet for en effektiv retshåndhævelse er, at trafikdata principielt ikke kun bør kunne opbevares til retshåndhævende formål, og at den nationale lovgivning ikke bør forpligte teleoperatørerne, teletjenesteudbyderne og Internet-udbyderne til at opbevare trafikdata i længere tid, end hvad der er nødvendigt af faktureringshensyn", henstilling 3/99 af 7. september 1999 udstedt af gruppen vedrørende databeskyttelse nedsat ved artikel 29, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

det foreslåede EU-forum (se punkt 6.4 i denne meddelelse) opfordrer Kommissionen alle implicerede parter til at give højeste prioritet til en indgående drøftelse af det komplicerede spørgsmål om opbevaring af trafikdata med henblik på at finde passende, afbalancerede og proportionale løsninger, som fuldt ud respekterer den grundlæggende ret til privatlivets fed og databeskyttelse[50]. Kommissionen vil derefter på basis af resultatet af dette arbejde kunne vurdere behovet for at træffe lovforanstaltninger eller andre foranstaltninger på EU-plan.

5.3. Anonym adgang og brug

Eksperter inden for retshåndhævelse har udtrykt bekymring for, at anonymitet kan føre til manglende ansvarliggørelse og i alvorlig grad forringe mulighederne for at fange visse forbrydere. Anonym brug af mobiltelefoni er mulig i nogle lande via taletidskort (ikke i andre). Anonym adgang til og brug af Internettet tilbydes af nogle tjeneste- og adgangsudbydere, bl.a. re-mailere og Internetcaféer. Der findes også en grad af anonymitet i systemet med dynamisk Internetadressetildeling, hvor adresser ikke tildeles brugerne permanent, men kun i den tid, en given opkobling tager.

I deres drøftelser med Kommissionen er nogle af erhvervslivets repræsentanter ikke gået ind for fuld anonymitet, til dels af hensyn til deres egen sikkerhed, bekæmpelsen af bedrageri og netintegriteten. London Internet Exchange har peget på nogle retningslinjer for bedste praksis, som den har udstedt, og som har vist sig nyttige i UK[51]. Andre repræsentanter for erhvervslivet og eksperter på privatlivsfredsområdet har fremført, at uden anonymitet er det ikke muligt at garantere de grundlæggende rettigheder.

Artikel 29-databeskyttelsesgruppen (artikel 29 i direktiv 95/46/EF) har udstedt en henstilling om spørgsmålet om anonym brug af Internettet[52]. Den betragter anonymitet på Internettet som et centralt dilemma for regeringer og internationale organisationer. På den ene side er muligheden for at forblive anonym af afgørende betydning, hvis den fundamentale ret til privatlivets fred og ytringsfriheden skal bevares i cyberspace. På den anden strider muligheden for at deltage og kommunikere online uden at afsløre sin identitet mod den vifte af initiativer, der er under udformning inden for andre nøgleområder af samfundspolitikken, f.eks. bekæmpelsen af ulovligt og skadeligt indhold, finansielt bedrageri og ophavsretskrænkelser. Naturligvis er den konflikt, der tilsyneladende er mellem forskellige samfundsmæssige målsætninger, ikke af ny dato. I forbindelse med de mere traditionelle, offline kommunikationsmidler som brev- og pakkepost, telefon, aviser og radio- og tv-spredning er der opnået en balance mellem disse forskellige målsætninger. Den udfordring, de politiske beslutningstagere står over for i dag, består i at sikre, at denne balance, som garanterer basale rettigheder, samtidig med at den giver mulighed for proportionale restriktioner i disse rettigheder i begrænsede og specificerede tilfælde, bibeholdes i den nye Internetsammenhæng. Af central betydning for denne balance er omfanget af og restriktionerne i en persons mulighed for at deltage online på anonym vis.

I sluterklæringen fra ministerkonferencen i Bonn om globale informationsnet den 6.-8. juli 1997 blev det fastslået, at princippet burde være, at hvor brugeren kan vælge at forblive anonym offline, skal dette valg også være muligt online. Der er derfor klart enighed

---

50 Som inkorporeret i den europæiske menneskerettighedskonvention (artikel 8, retten til privatlivets fred), Den Europæiske Unions charter om grundlæggende rettigheder, EU-traktaten og EF's databeskyttelsesdirektiver.

51 http://www.linx.net/noncore/bcp/.

52 Gruppen vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger. Henstilling 3/97 - Anonymitet på Internettet. Vedtaget af gruppen den 3. december 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

om, at aktivitet på net skal vurderes ved brug af de grundlæggende retsprincipper, der gælder andre steder. Internettet er ikke en anarkistisk ghetto, hvor samfundets regler ikke gælder. Tilsvarende bør regeringers og offentlige myndigheders muligheder for at begrænse individets rettigheder og overvåge potentielt ulovlig adfærd dog ikke være bedre i offentlige net, end de er i offlineverdenen udenfor. Kravet om, at indskrænkninger i de grundlæggende rettigheder og friheder skal være behørigt begrundede, nødvendige og proportionale set i forhold til andre samfundspolitiske målsætninger, skal også gælde i cyberspace.

I artikel 29-databeskyttelsesgruppens henstilling er det nøje anført, hvordan dette kan opnås i konkrete tilfælde (f.eks. i forbindelse med e-mail, nyhedsgrupper osv.)[53]. Kommissionen deler gruppens synspunkter.

5.4. Praktisk samarbejde på internationalt plan

På det seneste har verdensomspændende koordinerede retshåndhævelsesaktioner som f.eks. Starburst og Cathedral over for pædofiliringe demonstreret værdien af koordinerede internationale aktioner fra de retshåndhævende myndigheders og domstolenes side, såvel i form af at udveksle information på et tidligt stadium som i form af at forhindre, at de andre ringmedlemmer får et praj, når der foretages arrestationer og beslaglæggelser. Internettet har også vist sig at være et værdifuldt og effektivt redskab i forbindelse med politi- og toldmæssigt efterforskningsarbejde, hvor det benyttes som et middel til at begå traditionelle forbrydelser som falsknerier og smugling. På den anden side har disse aktioner også blotlagt de store retlige og operationelle problemer, som de retshåndhævende myndigheder og domstolene stilles over for ved styringen af aktioner af denne art, bl.a. indsamling af bevismateriale på tværs af landegrænserne eller *commission rogatoire*, identifikation af ofre og de mellemstatslige politiorganisationers rolle (især Interpol og Europol).

Inden for det praktiske internationale samarbejde får internationale informationsudvekslingsnet større og større betydning for politi- og toldmyndighederne.

Inden for G8 er der blevet oprettet et 24-timers/7-dages informationsnet for kontaktpunkter i de retshåndhævende myndigheder, som allerede er funktionsdygtigt. Hovedformålet med det er at modtage og besvare hastende anmodninger om samarbejde i sager, der involverer elektronisk bevismateriale. Nettet har været benyttet med succes i en række sager. EU's Ministerråd (retlige og indre anliggender) gav på sit møde den 19. marts 1998 sin tilslutning til de ti principper for bekæmpelse af hightechkriminalitet, som var blevet vedtaget af G8, og opfordrede de EU-medlemsstater, der ikke er medlem af G8, til at tilslutte sig nettet[54]. Kontaktpunkterne skal samarbejde direkte og være et supplement til de eksisterende strukturer for gensidig bistand og de eksisterende kommunikationskanaler[55].

---

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

54 Ud over G8-medlemmerne har fem EU-medlemsstater hidtil tilsluttet sig G8's 24-timers/7-dages net.

55 På verdenskonferencen i Stockholm den 28. august 1996 om kommerciel seksuel udnyttelse af børn blev det foreslået at inddrage Interpol i de nævnte net. EU-Ministerrådets afgørelse om bekæmpelse af børnepornografi på Internettet forudser også, at Europol inddrages på dette område.

Udkastet til Europarådets konvention påregner også, at der oprettes et net af denne art. Et 24-timers/7-dages net af kontaktpunkter omtales også i Rådets afgørelse om bekæmpelse af børnepornografi på Internettet og i EU's fælles holdning til udkastet til Europarådets konvention om Internetkriminalitet[56] samt i Rådets afgørelse, der giver sin tilslutning til G8's handlingsplan[57], men der er endnu ikke taget nogen konkrete initiativer i EU-sammenhæng.

Kommissionen finder, at i betragtning af behovet for passende ekspertise og hurtig handling på dette felt bør Rådets intentioner gennemføres snarest muligt. En forudsætning for, at et net af denne art kan blive en succes, er dog, at det bemandes med både retligt og teknisk kvalificeret personale, hvilket indebærer en passende medarbejderuddannelse.

Der er et tilsvarende behov for at intensivere samarbejdet og informationsudvekslingen mellem toldmyndighederne. De eksisterende former for samarbejde bør udbygges, og der bør udvikles nye måder at styre fælles operationer og udveksle information på. Under behørig hensyntagen til databeskyttelseskravene er der en voksende konsensus blandt toldmyndighederne om, at der bør oprettes internationale informationsnet for yderligere at udbygge informationsudvekslingen. Det er også nødvendigt at investere øgede ressourcer på dette område, både med henblik på at opgradere computersystemerne og med henblik på at uddanne medarbejderne, så toldmyndighederne kan udføre deres opgaver mere effektivt.

5.5. Procedureretlige beføjelser og værneting

Indenlandsk har de retshåndhævende myndigheder, når de nødvendige lovfæstede betingelser én gang er opfyldt, behov for at kunne søge efter og beslaglægge data lagret i computere hurtigt nok til at forhindre, at bevismateriale i straffesager tilintetgøres. De retshåndhævende myndigheder mener, at de bør besidde tilstrækkelige tvangsmidler til inden for deres myndighedsområde at søge i computersystemer og beslaglægge data, beordre enkeltpersoner til at udlevere nærmere angivne computerdata og beordre eller sikre hurtig opbevaring af specifikke data under de normale retsgarantier og i overensstemmelse med de normale retsprocedurer. I den aktuelle situation har garantierne og procedurerne imidlertid ikke været genstand for indbyrdes tilnærmelse.

Der kan opstå problemer, hvis de retshåndhævende myndigheder i forbindelse med adgang til en computer opdager, at der er en række computere og netværk impliceret, som ligger spredt over hele det pågældende land. Situationen kompliceres meget mere, hvis en retshånd-hævende myndighed ved søgningen i en computer eller simpelthen i forbindelse med en efterforskning opdager, at den opnår adgang til data eller har behov for at opnå adgang til data, der befinder sig i et eller flere forskellige lande. Der står i så fald vigtige suverænitets-, menneskerettigheds- og retshåndhævelsesinteresser på spil, som skal afvejes mod hinanden.

De eksisterende retlige redskaber til brug for det internationale samarbejde på det strafferetlige område, nemlig gensidig retshjælp, er formentlig ikke hensigtsmæssige eller tilstrækkelige, fordi det normalt tager flere dage, uger eller måneder at effektuere denne hjælp. Der er behov for en mekanisme, hvorved lande kan efterforske lovovertrædelser og indhente bevismateriale hurtigt og effektivt eller i det mindste ikke miste vigtigt bevis-

---

[56] Artikel 1, stk. 4, i den fælles holdning: "Medlemsstaterne bør støtte, at der fastsættes bestemmelser, der letter det internationale samarbejde, herunder bestemmelser om gensidig retshjælp i videst muligt omfang. Konventionen bør lette og fremme samarbejdet i forbindelse med edb-relaterede og edb-støttede strafbare handlinger. Denne form for samarbejde kan omfatte oprettelse af retshåndhævelses-kontaktpunkter, der fungerer døgnet rundt, og som supplerer de eksisterende strukturer inden for gensidig retshjælp."

[57] Findes på European Judicial Networks websted http://ue.eu.int/ejn/index.htm.

materiale i tværnationale retshåndhævelsesprocedurer på en måde, som er forenelig med principperne om national suverænitet og beskyttelsen af de forfatningsmæssige rettigheder og menneskerettighederne, herunder privatlivets fred.

Blandt de nye forslag, der er under overvejelse i forbindelse med udkastet til Europarådets konvention om Internetkriminalitet med henblik på at løse disse problemer, kan nævnes, at opbevaring af data skal kunne berordres som en hjælp ved konkrete efterforskningsopgaver. Andre spørgsmål som grænseoverskridende eftersøgning og beslaglæggelser frembyder vanskelige og hidtil uløste problemer. Der er klart behov for yderligere drøftelser mellem alle implicerede parter, før det kan overvejes at iværksætte konkrete initiativer.

G8-undergruppen om hightechkriminalitet har drøftet spørgsmålet om grænseoverskridende eftersøgning og beslaglæggelser og er i afventning af en efterfølgende mere permanent aftale nået til enighed om en række foreløbige principper[58]. Blandt de vigtige spørgsmål, der drøftes i denne sammenhæng, er navnlig spørgsmålet om, hvorvidt hurtig eftersøgning og beslaglæggelse i bestemte situationer er mulig, inden den stat, hvori eftersøgningen foregår, orienteres, og der skal opstilles passende garantier for respekt af de grundlæggende rettigheder. I EU-Ministerrådets fælles holdning til udkastet til Europarådets konvention om Internetkriminalitet indtager ministrene en åben holdning til dette spørgsmål[59].

I forbindelse med computerrelateret kriminalitet er det også vigtigt, at der er klare regler for, hvilket land der har retten til at indlede retsforfølgning. Det skal især forhindres, at der ikke er noget land, der har denne ret. Hovedreglerne, der foreslås i udkastet til Europarådets konvention, er, at der etableres værneting i en stat, når lovovertrædelsen begås på dens område eller af en af dens statsborgere. Hvis mere end ét land påberåber sig retten til retsforfølgning, skal de implicerede lande rådføre sig med hinanden med henblik på at fastslå, hvor det er mest hensigtsmæssigt at etablere værneting. Meget i denne sammenhæng afhænger af et effektivt bilateralt eller multilateralt samarbejde. Kommissionen vil fortsætte med at overvåge dette spørgsmål for at se, om der er behov for yderligere handling på EU-plan.

Kommissionen, som både har deltaget i drøftelserne i Europarådet og G8, erkender, at disse procedureretlige spørgsmål er komplekse og vanskelige. Et effektivt samarbejde inden for EU om bekæmpelse af Internetkriminalitet er imidlertid et afgørende element i opnåelsen af et sikrere informationssamfund og etableringen af et område med frihed, sikkerhed og retfærdighed.

Kommissionen agter at fortsætte sine høringer med alle implicerede parter gennem de kommende måneder med udgangspunkt i dette arbejde. Spørgsmålet vil også blive taget op i den bredere sammenhæng af arbejdet med at gennemføre konklusionerne fra Det Europæiske Råd i Tammerfors i oktober 1999. Topmødet i Tammerfors anmodede bl.a. Rådet og

---

58 Kommuniké fra G8-landenes ministerkonference om bekæmpelse af grænseoverskridende organiseret kriminalitet, Moskva, 19.-20. oktober 1999 (se http://www.usdoj.gov/criminal/cybercrime/action.htm og også http://www.usdoj.gov/criminal/cybercrime/principles.htm.

59 EFT L 142 af 5.6.1999, s. 2: "Med forbehold af forfatningsmæssige principper og særlige beskyttelses-foranstaltninger, der tager sigte på i passende omfang at respektere andre staters suverænitet, sikkerhed, offentlige orden eller andre væsentlige interesser, kan det på betingelser, der skal fastlægges nærmere i konventionen, i undtagelsestilfælde og især hvis sager er af hastende karakter, eventuelt komme på tale at foretage en grænseoverskridende edb-søgning med henblik på efterforskning af en grov strafbar handling, f.eks. hvis det er nødvendigt for at forebygge ødelæggelse eller ændring af bevismateriale vedrørende den grove strafbare handling eller for at forebygge, at der begås en strafbar handling, der vil kunne resultere i en persons død eller medføre alvorlige personskader".

Kommissionen om senest i december 2000 at vedtage et program med foranstaltninger til gennemførelse af princippet om gensidig anerkendelse af domstolsafgørelser. Kommissionen har allerede udsendt en meddelelse om gensidig anerkendelse af endelige afgørelser i straffesager[60]. Som led i sit bidrag til gennemførelsen af den del af programmet med foranstaltninger, der vedrører håndhævelsen af afgørelser afsagt forud for retssager, vil Kommissionen overveje muligheden for gensidig anerkendelse af afgørelser afsagt forud for retssager i forbindelse med efterforskning af Internetkriminalitet med henblik på at fremlægge et lovgivningsforslag i henhold til afsnit VI i traktaten om Den Europæiske Union.

5.6. Værdien af computerdata som bevismateriale

Selv i tilfælde, hvor de retshåndhævende myndigheder har opnået adgang til computerdata, som synes at udgøre bevismateriale, har de brug for at kunne hente og autentificere disse data for at kunne bruge dem i forbindelse med efterforskningen og retsforfølgningen i straffesager. Dette er ikke nogen let sag, fordi elektroniske data er flygtige og nemme at manipulere, forfalske, beskytte teknisk eller slette. Den disciplin, der beskæftiger sig med dette problem, er edb-retsvidenskaben**,** som beskæftiger sig med udvikling og brug af videnskabelige protokoller og procedurer til at søge i computere og analysere og fastslå autenciteten i data, som er blevet hentet.

Efter anmodning fra G8's eksperter har den internationale organisation for edb-bevismateriale ("International Organisation of Computer Evidence" (IOCE)) indvilliget i at udarbejde anbefalinger til standarder omfattende definition af fælles termer, identifikationsmetoder og identifikationsteknikker, som vil kunne benyttes, og udarbejdelse af et fælles format til retsvidenskabelige anmodninger. EU bør tilknyttes dette arbejde både via medlemsstaternes særlige computerkriminalitetsefterforskningsorganer og via den F&U, der støttes via det femte rammeprogram (IST-programmet).

6. IKKE-LOVGIVNINGSMÆSSIGE FORANSTALTNINGER

Passende lovgivning på både nationalt og internationalt plan er nødvendig, men ikke i sig selv tilstrækkelig til effektivt at bekæmpe computerrelateret kriminalitet og netmisbrug. En række supplerende ikke-lovgivningsmæssige tiltag er også påkrævet som et supplement til lovgivningsforanstaltningerne. De fleste er nævnt i anbefalingerne i COMCRIME-undersøgelsen, og G8 har foreslået en række tiltag i sin 10-punkts handlingsplan, og de har fået bred opbakning fra alle parter i den uformelle høringsproces, der gik forud for udarbejdelsen af denne meddelelse. De omfatter bl.a.:

- oprettelse på nationalt plan af særlige politienheder for bekæmpelse af computer-kriminalitet i de lande, hvor de ikke allerede findes
- forbedret samarbejde mellem de retshåndhævende myndigheder, erhvervslivet, forbrugerorganisationerne og databeskyttelsesmyndighederne
- fremme af passende erhvervs- og EU-ledede initiativer, bl.a. inden for sikkerheds-produkter.

Spørgsmålet om kryptering vil formentlig være af stor betydning i denne sammehæng. Kryptering er et vigtigt redskab til at sikre implementering og indførelse af nye tjenester,

---

60 KOM(2000) 495, Bruxelles, den 26. juli 2000.

herunder elektronisk handel, og kan yde et væsentligt bidrag til forebyggelse af kriminalitet på Internettet. Kommissionens politik i relation til kryptering blev fastlagt i meddelelsen om sikkerhed og tillid i elektronisk kommunikation fra 1997[61], hvori Kommissionen bebudede, at den vil forsøge at afskaffe alle restriktioner på den frie bevægelighed for alle krypteringsprodukter inden for Det Europæiske Fællesskab. Meddelelsen fastslog endvidere, at eventuelle nationale restriktioner på krypteringsprodukters frie bevægelighed skal være forenelige med fællesskabsretten, og at Kommissionen vil undersøge, om sådanne nationale restriktioner er begrundede og proportionale, navnlig i forhold til traktatens bestemmelser om fri bevægelighed, Domstolens retspraksis og kravene i databeskyttelsesdirektiverne. Kommissionen erkender dog, at kryptering også kan frembyde nye og vanskelige udfordringer for de retshåndhævende myndigheder.

Kommissionen ser derfor med tilfredshed på den nyligt vedtagne reviderede forordning om varer med dobbelt anvendelse, som i høj grad var medvirkende til at liberalisere krypteringsprodukter, samtidig med at den erkendte, at dette skulle følges op af en bedre dialog mellem brugerne, erhvervslivet og de retshåndhævende myndigheder. Kommissionen agter på sin side at fremme denne dialog på EU-plan via det foreslåede EU-forum for højteknologikriminalitet. Hvis sikkerhedsprodukter, herunder kraftige krypteringsprodukter, var tilgængelige overalt i EU og efter behov var certificeret i forhold til aftalte evalueringskriterier, ville dette både forbedre mulighederne for at forebygge kriminalitet og øge brugernes tillid til processerne i informationssamfundet.

6.1. Særlige enheder på nationalt plan

Eftersom nogle computerrelaterede kriminelle handlinger frembyder komplekse tekniske og retlige problemstillinger, er det afgørende, at der oprettes særlige enheder på nationalt plan. Sådanne særlige enheder bør bestå af kyndige medarbejdere fra forskellige tjenester (politiet og domstolene) og bør udstyres med passende tekniske faciliteter og fungere som hurtige kontaktpunkter med henblik på:

- hurtigt at besvare forespørgsler om information om formodede lovovertrædelser. Der skal fastsættes fælles formater for udveksling af information af denne art, selv om drøftelserne på G8-ekspertplan har vist, at dette muligvis ikke er nogen let opgave i betragtning af forskellene i de nationale retstraditioner

- at fungere som national og international retshåndhævelsesgrænseflade for hotlines[62], der modtager klager om ulovligt indhold fra Internetbrugere

- at forbedre og/eller udvikle særlige computerefterforskningsteknikker med henblik på opklaring, efterforskning og retsforfølgning af computerrelaterede kriminalitet

---

61 KOM(97) 503.

62 Hidtil findes der kun hotlines i nogle få lande. Eksempler herpå er Cybertipline i USA og Internet Watch Foundation (IWF) i UK, som siden december 1996 har drevet en telefon- og e-mailhotline, som borgerne kan benytte til at indberette materiale på Internettet, som de anser for at være ulovligt. IWF vurderer, om materialet er ulovligt, og underretter Internettjenesteudbyderne og politiet. Der findes også overvågningsorganer i Norge (Redd Barna), Nederlandene (Meldpunt), Tyskland (Newswatch, FSM og Jugendschutz), Østrig (ISPAA) og Irland (ISPAI). Inden for rammerne af EU's Daphne-program er Childnet International for øjeblikket ved at gennemføre et projekt, som har direkte tilknytning til dette spørgsmål ("International Hotline Providers in Europe Forum"). UNESCO's ekspertmøde i Paris i januar 1999 gav også sin støtte og opmuntring til nationale hotlines og opbygning af netværk af hotlines eller et internationalt "elektronisk vagttårn".

- at fungere som videnscenter om spørgsmål vedrørende Internetkriminalitet med det formål at formidle bedste praksis og erfaring.

Inden for EU har nogle medlemsstater allerede oprettet disse specialenheder, der specifikt beskæftiger sig med computerrelateret kriminalitet. Kommissionen finder, at oprettelsen af sådanne specialenheder hører under medlemsstaternes ansvarsområde, og opfordrer kraftigt medlemsstaterne til at tage skridt hertil. Anskaffelsen af den seneste hardware og software til disse enheder og uddannelsen af medarbejderne medfører betydelige omkostninger og forudsætter en prioritering og politiske beslutninger på rette niveau i statsadministrationen[63]. Den erfaring, allerede eksisterende enheder i medlemsstaterne har indhøstet, kan være til stor nytte. Kommissionen vil opfordre til, at der sker en udveksling af erfaringer på dette område.

Kommissionen finder også, at Europol kan yde yderligere merværdi på EU-plan via koordinering, analyse og anden bistand til specielenhederne i medlemsstaterne. Kommissionen vil derfor støtte, at Europols ansvarsområde udvides til at dække cyberkriminalitet.

6.2. Specialuddannelse

Der er behov for en betydelig indsats for at tilvejebringe en løbende specialuddannelse af politiets og domstolenes ansatte. Den computerrelaterede kriminelle teknik og kapacitet ændrer sig meget hurtigere end inden for de mere traditionelle områder af kriminel aktivitet.

Nogle medlemsstater har taget initiativ til at opbygge hightechuddannelse af de retshåndhævende myndigheders ansatte. Disse lande kan yde rådgivning og vejledning til medlemsstater, som endnu ikke har taget lignende initiativer.

Der er blevet iværksat individuelle projekter i denne forbindelse – i form af udveksling af erfaringer, seminarer om de fælles udfordringer, de relevante personalegrupper vil blive stillet over for – med støtte fra programmer, der forvaltes af Kommissionen (bl.a. STOP-, FALCONE- og GROTIUS-programmerne). Kommissionen vil fremlægge forslag til andre aktiviteter på dette område, herunder computer- og onlineuddannelse.

Europol har i november 2000 taget initiativ til at være vært for et 1-uges uddannelsesprogram for retshåndhævende personale fra medlemsstaterne, som især skal fokusere på børnepornografiproblematikken. Emnet for disse uddannelsesprogrammer kunne udvides til at omfatte computerrelateret kriminalitet generelt. Interpol har også været aktiv på dette felt i en årrække. Blandt de relevante initiativer kan nævnes muligheden af at udsende et større antal praktikanter.

G8 har taget initiativer, der giver mulighed for, at de retshåndhævende myndigheder kan udveksle erfaringer og opbygge fælles efterforskningsteknikker ud fra konkrete sager. Et yderligere initiativ på uddannelsesområdet ventes taget i andet halvår af 2001. De EU-medlemsstater, der deltager i G8, kan videregive disse erfaringer til de øvrige medlemsstater.

Hvad angår specielt bekæmpelsen af børnepornografi på Internettet, vil oprettelsen og førelsen af et centralt digitalt bibliotek af børnepornografiske billeder på internationalt plan (som skal gøres tilgængeligt på Internettet til de retshåndhævende specialenheder i medlemsstaterne - med de nødvendige betingelser og restriktioner hvad angår adgangen og

---

63 Om USA's erfaringer på dette felt, se Michael A. Sussmanns "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", Duke Journal of Comparative and International Law, bind 9, foråret 1999, s. 464.

beskyttelsen af privatlivets fred) være en hjælp i forbindelse med søgningen efter ofre og lovovertrædere, bestemmelsen af lovovertrædelserne art og specialuddannelsen af politifolk[64].

6.3. Bedre information og fælles registreringsregler

Et harmoniseret sæt af regler for politiets og domstolenes registrering og opbygning af de rette redskaber til statistisk analyse af computerkriminalitet vil være en hjælp for politiet og domstolene til bedre at opbevare, analysere og evaluere den formelle information, der indhentes på dette område, der er under stadig forandring.

Set fra den private sektors synspunkt er sådanne statistikker også påkrævet for at opnå den rette vurdering af de implicerede risici og opstille cost-benefit-analyser af forvaltningen af dem. Dette er af betydning ikke blot af operationelle grunde (f.eks. for at afgøre, hvilke sikkerhedsforholdsregler der skal træffes), men også af forsikringsmæssige grunde.

En database om retsforskrifterne om computerkriminalitet, som udgjorde en del af COMCRIME-undersøgelsen, er ved at blive ajourført og gjort tilgængelig for Kommissionen. Kommissionen vil overveje at forbedre databasens indhold (inkluderer love, retsafgørelser og litteratur) og anvendelighed**.**

6.4. Samarbejde mellem de forskellige aktører: EU-forummet

Et effektivt samarbejde mellem de statslige myndigheder og den implicerede sektor inden for de fastsatte lovrammer anses for at være et afgørende element i enhver offentlig politik til bekæmpelse af computerrelateret kriminalitet[65]. Repræsentanter for de retshåndhævende myndigheder har indrømmet, at de ikke altid har været tilstrækkelig klare og præcise med, hvad de har behov for fra tjenesteudbyderne. Repræsentanter for sektoren har udtrykt en generelt positiv holdning over for et bedre samarbejde med de retshåndhævende myndigheder, men har understreget behovet for at sikre en passende balance mellem beskyttelsen af borgernes grundlæggende rettigheder og friheder, især deres ret til privatlivets fred[66], behovet for at bekæmpe kriminalitet og de økonomiske byrder, der lægges på tjenesteudbyderne.

Sammen kan sektoren og de retshåndhævende myndigheder øge bevidstheden i offentligheden om den fare, lovovertrædere på Internettet udgør, fremme bedste praksis på det sikkerhedsmæssige område og udvikle effektive kriminalitetsbekæmpende redskaber og

---

64 Et meget vellykket initiativ i denne sammenhæng har været "Excalibur"-projektet, som blev udviklet af den svenske nationale kriminalefterretningstjeneste med økonomisk støtte fra Europa-Kommissionen under STOP-programmet. Projektet blev etableret i samarbejde med politimyndighederne i Tyskland, UK, Nederlandene og Belgien samt Europol og Interpol. Andre projekter gennemført af det tyske BKA (det såkaldte "Perkeo") og det franske indenrigsministerium ("Surfimage"-projekter, som også fik støtte under STOP-programmet) skal også tages i betragtning.

65 I et kommuniké, der blev vedtaget i Washington den 9./10. december 1997 om principperne bag og en 10-punkts handlingsplan til bekæmpelse af højteknologikriminalitet, erklærede G8's justits- og indenrigsministre, at "det er industrien, der udformer, etablerer og vedligeholder disse globale netværk og har hovedansvaret for udarbejdelsen af tekniske standarder. Det påhviler derfor industrien at spille en rolle i forbindelse med at udvikle og distribuere sikre systemer, som kan spore computermisbrug, opbevare elektronisk bevismateriale og bistå ved lokaliseringen og identificeringen af lovovertrædere". Rådets afgørelse om bekæmpelse af børnepornografi på Internettet understreger behovet for, at medlemsstaterne fører en konstruktiv dialog med industrien og gennem løbende kontakt med den samarbejder ved at udveksle erfaringer.

66 Som fastsat i EU's databeskyttelsesdirektiver, Europarådets menneskerettighedskonvention og Europarådets konvention 108 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger og de relevante nationale love.

procedurer. Der er allerede taget relevante initiativer i en række medlemsstater, hvoraf UK Internet Crime Forum formentlig er det ældste og mest vidtrækkende[67].

Kommissionen hilser disse initiativer velkommen og finder, at de bør fremmes i alle medlemsstater. Kommissionen agter at oprette et EU-forum, hvor de retshåndhævende myndigheder, Internettjenesteudbyderne, teleoperatørerne, borgerrettighedsorganisationer, forbrugerrepræsentanter, databeskyttelsesmyndighederne og andre interesserede parter kan samles med det formål at forbedre samarbejdet på EU-plan. I første række indebærer dette, at der skal udpeges embedsmænd af medlemsstaterne, at der skal udnævnes teknologi- og privatlivsfredseksperter af artikel 29-databeskyttelsesgruppen, og at der skal findes erhvervs- og forbrugerrepræsentanter i nært samarbejde med erhvervs- og forbrugerorganisationerne. På et senere stadium vil EU-forummet omfatte repræsentanter for de relevante nationale initiativer.

EU-forummet vil fungere på åben og gennemsigtig vis, de relevante dokumenter vil blive offentliggjort på et websted, og alle interesserede parter vil modtage opfordring til at fremsætte bemærkninger.

EU-forummet vil blive opfordret til bl.a. at overveje følgende områder:

- etablering efter behov af døgnåbne kontaktpunkter mellem de offentlige myndigheder og den implicerede sektor

- udarbejdelse af et passende standardformat for anmodninger med henblik på retshåndhævelse om information fra sektoren og øget brug af Internettet fra de retshåndhævende myndigheders side i kommunikationen med tjenesteudbyderne

- fremme af udviklingen og/eller implementeringen af adfærdskodekser og bedste praksis og udveksling af sådanne kodekser mellem sektoren og de offentlige myndigheder[68]

- fremme af informationsudveksling om udviklingen inden for højteknologikriminalitet mellem de forskellige parter, især sektoren og de retshåndhævende myndigheder

- vurdering af mulighederne for at inkludere retshåndhævende hensyn i udviklingen af ny teknologi

- fremme af videreudviklingen af alarm- og krisestyringsmekanismer med henblik på at forebygge, identificere og håndtere trusler eller forstyrrende hændelser i informationsinfrastrukturerne

- efter behov ydelse af et ekspertbidrag til arbejdet i Rådet og andre internationale fora, f.eks. Europarådet og G8

- fremme af samarbejde mellem de berørte parter, herunder om de principper, de retshåndhævende myndigheder, sektoren og brugerne er fælles om (f.eks. aftalememoranda og kodekser for god praksis i overensstemmelse med de retlige rammer).

---

67 Internet Crime Forum blev oprettet i 1997 og omfatter politifolk, embedsmænd fra indenrigsministeriet, repræsentanter for databeskyttelsesmyndighederne og repræsentanter for Internetsektoren; det afholder plenarmøder 3-4 gange om året og har en række stående arbejdsgrupper.

68 For så vidt angår adfærdskodeks for artikel 27 af Direktiv 95/46/EC (det kunne for eksempel omfatte områder, der falder under Direktiv 97/66/EC så som interceptions), er Artikel 29 Databeskyttelses arbejdsgruppen og de nationale overvågende myndigheder for databeskyttelse involveret.

6.5. Direkte tiltag fra sektorens egen side

I vid udstrækning er bekæmpelsen af computerrelateret kriminalitet i det bredere samfunds egen interesse. Hvis forbrugerne skal have tillid til elektronisk handel, må og skal foranstaltninger til forebyggelse af computerrelateret kriminalitet være et accepteret element i god forretningsskik. Mange erhvervssektorer, f.eks. banksektoren, elektronisk kommunikation, kreditkortsektoren og ophavsretssektoren, og deres kunder er potentielle ofre for computerrelateret kriminalitet. Virksomhederne beskytter naturligt nok deres egne navne og varemærker og spiller derved en rolle i bedrageribekæmpelsen. Organisationer, der repræsenterer software- og audiosektoren (f.eks. British Phonographic Industry - BPI), har team, der efterforsker pirateri (herunder også Internetrelateret pirateri). Internettjenesteudbydere i en række medlemsstater har oprettet hotlines til brug for indberetning af ulovligt og skadeligt indhold.

Kommissionen har støttet nogle af disse initiativer ved at tilskynde til, at de deltager i EU's F&U-rammeprogram, Internethandlingsplanen[69] og afsnit VI-programmer som f.eks. STOP og DAPHNE.

Bedste praksis på disse områder vil blive udvekslet inden for rammerne af EU-forummet.

6.6. EU-støttede FTU-projekter

I FTU-programmet for informationssamfundsteknologi (IST), som er en del af det femte rammeprogram for 1998 - 2002, lægges der vægt på udvikling og indsættelse af tillidsskabende teknologi. Tillidsskabende teknologi omfatter både informations- og netsikkerhedseknologi samt tekniske værktøjer og metoder, der er egnede til at beskytte mod misbrug af den grundlæggende ret til privatlivets fred og databeskyttelse og beskyttelse af andre personlige rettigheder og bekæmpe computerkriminalitet.

IST-programmet, især arbejdet vedrørende *Informations- og netsikkerhed og anden tillidsskabende teknologi* under nøgleaktion 2 - *Nye arbejdsmetoder og elektronisk handel*, udgør rammerne for udvikling af den kapacitet og teknologi, der er nødvendig for at forstå og håndtere de teknologiske udfordringer, der knytter sig til forebyggelsen og bekæmpelsen af computerkriminalitet, og sikre, at sikkerheds- og privatlivsfredskravene kan opfyldes på EU-plan, i det virtuelle miljø og på individuelt plan.

For at imødegå de udfordringer, der knytter sig til tillidsproblematikken, på en ordentlig måde, herunder forebyggelsen og efterforskningen af computerkriminalitet, er der også blevet iværksat et driftssikkerhedsinitiativ som led i IST-programmet. Initiativet har til formål at bidrage til at skabe og sikre tillid til de stærkt forbundne informationsinfrastrukturer og til tæt netværkssammenkoblede "embedded" systemer ved at øge bevidstheden om driftssikkerhed og driftssikkerhedsskabende teknologi. En integreret del af dette initiativ er internationalt samarbejde. Under IST-programmet er der blevet opbygget et arbejdssamarbejde med DARPA og NSF og i samarbejde med det amerikanske udenrigsministerium en fælles taskforce om beskyttelse af kritisk infrastruktur inden for rammerne af den fælles rådgivende gruppe for EU og USA under samarbejdsaftalen om videnskab og teknologi[70].

---

[69] Yderligere oplysninger om Internethandlingsplanen: Handlingsplan til fremme af en sikrere brug af Internettet findes på http://158.169.50.95:10080/iap/.

[70] Yderligere oplysninger om IST-programmet findes på http://www.cordis.lu/ist.

Kommissionen Fælles Forskningscenter (FFC), som har støttet driftssikkerhedsinitiativet under IST-programmet, vil fokusere sine bestræbelser på at udvikle passende og harmoniserede foranstaltninger, indikatorer og statistikker i samarbejde med andre interesserede parter, herunder Europol. Formålet hermed vil være at udvikle en passende klassifikation af og forståelse for ulovlige aktiviteter, deres geografiske spredning, deres vækstrate og effektiviteten i de foranstaltninger, der træffes for at bekæmpe dem. FFC vil efter behov inddrage andre forskningsgrupper og integrere deres indsats og resultater. Det vil føre et websted på Internettet om problematikken og aflægge beretning om fremskridtet med sit arbejde for EU-forummet.

7. KONKLUSIONER OG FORSLAG

Forebyggelse og effektiv bekæmpelse af computerrelateret kriminalitet forudsætter, at en række betingelser er til stede, nemlig:

- rådighed over forebyggende teknologi. Dette forudsætter passende lovrammer, som giver plads og incitamenter til innovation og forskning. Offentlig finansiering kan begrundes til støtte for udvikling og indsættelse af passende sikkerhedsteknologi

- bevidsthed om de potentielle sikkerhedsrisici og måderne at bekæmpe dem på

- hensigtsmæssige materielle og processuelle lovbestemmelser, både hvad angår indenlandske og tværnationale kriminelle aktiviteter. De nationale materielle straffelovsbestemmelser bør være tilstrækkelig brede og bør effektivt kriminalisere alvorlige computerrelaterede misbrug og fastsætte bestemmelser om afskrækkende sanktioner, bør bidrage til at løse dobbeltkriminalitetsproblemer[71] og bør tjene til fremme af internationalt samarbejde. Når de retshåndhævende myndigheder har et behørigt begrundet behov for hurtigt at søge i computersystemer og beslaglægge eller på sikker vis kopiere computerdata inden for deres område for at kunne efterforske computerrelateret kriminalitet, skal der findes procedureregler, som giver mulighed herfor i henhold til principperne og undtagelserne i fællesskabsretten og i overensstemmelse med den europæiske menneskerettighedskonvention. Kommissionen finder, at de aflytningsbestemmelser, der er nået enighed om i konventionen om gensidig retshjælp i straffesager, er det højest opnåelige på det nuværende stade. Kommissionen vil fortsat vurdere gennemførelsen i samarbejde med medlemsstaterne, sektoren selv og brugerne for at sikre, at de relevante initiativer er effektive, gennemsigtige og velafbalancerede

- rådighed over et tilstrækkeligt antal veluddannede og veludrustede medarbejdere i de retshåndhævende myndigheder. Der vil yderligere blivet skubbet på for at etablere et tæt samarbejde med Internettjenesteudbyderne og teleoperatørerne inden for uddannelsesområdet

- forbedret samarbejde mellem alle de implicerede aktører: brugerne og forbrugerne, de pågældende erhvervssektorer, de retshåndhævende myndigheder og databeskyttelsesmyndighederne. Dette er af kritisk betydning ved efterforskningen af computerkriminalitet og for beskyttelsen af den offentlige sikkerhed. Virksomhederne i sektoren har behov for at operere inden for klare regler og forpligtelser. Regeringerne bør erkende, at de retshåndhævende myndigheders behov kan lægge byrder på

---

[71] I tilfælde, hvor en kriminel efterforskning kræver bistand fra myndighederne i andre lande, er det i mange retssystemer en forudsætning for visse typer gensidig retshjælp og udvisning, at handlingen er strafbar i begge lande.

virksomhederne, og bør derfor tage rimelige skridt til at mindske disse byrder mest muligt. Samtidig bør virksomhederne inkorporere hensyn vedrørende den offentlige sikkerhed i deres forretningspraksis. Dette vil i stigende grad kræve et aktivt samarbejde og støtte fra den enkelte bruger og forbruger

- løbende erhvervs- og samfundsledede initiativer. Hotlines, som allerede findes til indberetning af tilfælde af ulovligt og skadeligt indhold, kan udvides til at omfatte andre typer misbrug. Selvregulering inden for sektoren og et tværtjenstligt aftalememorandum kunne inddrage den bredest mulige vifte af interesserede parter og spille en flersidet rolle i forbindelse med at medvirke til at forebygge og bekæmpe computerkriminalitet og skabe øget bevidsthed og tillid

- resultaterne af og potentiellet i F&U bør udnyttes i vidst muligt omfang. Den strategiske fokus skal ligge på en økonomisk overkommelig og effektiv sikkerhedsteknologi og anden tillidsskabende teknologi og politiske initiativer på EU-plan.

Foranstaltninger, der vil skulle aftales i EU, bør dog tage højde for, at ansøgerlandene gradvis bringes ind under EU's regi og det internationale samarbejde på dette felt, og bør forhindre, at de bliver benyttet som tilflugtssted for computerkriminalitet. Det bør overvejes at involvere repræsentanter for disse lande i alle eller nogle af de relevante EU-møder.

Kommissionens forslag kan opdeles i følgende områder.

7.1. Lovgivningsforslag

Kommissionen vil fremsætte lovgivningsforslag under afsnit VI i traktaten om Den Europæiske Union om:

- indbyrdes tilnærmelse af medlemsstaternes lovgivning om lovovertrædelser på børnepornografiområdet. Dette initiativ er en del af en pakke af forslag, som også vil dække bredere emner i tilknytning til seksuel udnyttelse af børn og menneskehandel, som det blev bebudet i Kommissionens meddelelse om menneskehandel fra december 1998. Et sådant forslag vil ligge fuldt på linje med Europa-Parlamentets forsøg på at omdanne det østrigske initiativ til en rådsafgørelse om børnepornografi til en rammeafgørelse, der forudsætter indbyrdes tilnærmelse af medlemsstaternes lovgivning. Det er også i overensstemmelse med konklusionerne fra Tammerfors og EU's strategi for det nye årtusinde for bekæmpelse af organiseret kriminalitet. Dette er allerede en del af resultattavlen for oprettelsen af et område med frihed, sikkerhed og retfærdighed

- yderligere indbyrdes tilnærmelse af den materielle strafferet inden for området højteknologikriminalitet. En sådan tilnærmelse vil omfatte lovovertrædelser som hacking og "denial of service"-angreb. Kommissionen vil også undersøge mulighederne for at gribe ind over for racisme og fremmedhad på Internettet ved at fremsætte forslag til en rammeafgørelse under afsnit VI i traktaten om Den Europæiske Union, som skal dække racistisk og xenofobisk aktivitet såvel offline som online. Endelig vil problemet med narkotika på Internettet også blive vurderet

- anvendelse af princippet om gensidig anerkendelse af retsafgørelser afsagt forud for retssager i forbindelse med efterforskning af cyberkriminalitet og fremme af efterforskning af computerrelateret kriminalitet, hvori mere end én medlemsstat er involveret, med passende garantier vedrørende de grundlæggende rettigheder. Forslaget ligger i forlængelse

af det overordnede program af foranstaltninger for gensidig anerkendelse, som omtaler behovet for at overveje forslag om fremlæggelse og indefrysning af bevismateriale.

Behovet for foranstaltninger, bl.a. i form af et specifikt lovgivningsinitiativ, om spørgsmålet om opbevaring af trafikdata vil blive vurderet af Kommissionen som led i andre høringer på basis af resultatet af det arbejde, der vil blive udført af det foreslåede EU-forum på dette område.

7.2. Initiativer i anden form end lovgivning

Der foreslås initiativer på en række områder:

- Kommissionen vil oprette og fungere som formand for et EU-forum, som skal samle de retshåndhævende myndigheder, tjenesteudbyderne, netoperatørerne, forbrugergrupper og databeskyttelsesmyndighederne med det formål at intensivere samarbejdet på EU-plan gennem øget offentlig opmærksomhed omkring de risici, som kriminelle på Internettet frembyder, fremme af bedste praksis inden for IT-sikkerhed, udvikling af effektive kriminalitetsbekæmpende værktøjer og procedurer til bekæmpelse af computerrelateret kriminalitet samt fremme af videreudviklingen af alarm- og krisestyringsmekanismer. Dette vil være en EU-udgave af tilsvarende succesfulde fora, som i forvejen findes i visse medlemsstater. I de medlemsstater, hvor sådanne fora ikke findes, opfordrer Kommissionen disse lande til at oprette dem. Samarbejdet mellem disse forskellige fora vil blive fremmet og stimuleret via EU-forummet

- Kommissionen vil fortsat fremme sikkerhed og tillid i sammenhæng med *e*Europe-initiativet, Internethandlingsplanen, IST-programmet og det næste FTU-rammeprogram. Dette vil bl.a. indebære fremme af produkter og tjenester, der frembyder et passende sikkerhedsniveau, og fremme af en mere liberaliseret brug af kraftig kryptering via en dialog mellem alle de berørte parter

- Kommissionen vil fremme yderligere projekter under eksisterende programmer til støtte for uddannelsen af de ansatte i de retshåndhævende myndigheder i højteknologikriminalitet og for forskning i computeranvendelse til retsvidenskabelige formål

- Kommissionen vil overveje at stille finansiering til rådighed for en forbedring af indholdet og anvendeligheden af databasen over medlemsstaternes nationale love, som omhandles i COMCRIME-undersøgelsen, og vil iværksætte en undersøgelse for at få et bedre billede af karakteren og omfanget af computerrelateret kriminalitet i medlemsstaterne.

7.3. Initiativer i andre internationale fora

Kommissionen vil fortsætte med at spille sin fulde rolle som koordinator mellem medlemsstaterne i andre internationale fora, hvor Internetkriminalitet står på dagsordenen, bl.a. Europarådet og G8. Kommissionens initiativer på EU-plan vil i fuldt omfang tage hensyn til de fremskridt, der sker i andre internationale fora, og Kommissionen vil samtidig søge at sikre en indbyrdes tilnærmelse inden for EU.

* * * * *

FINANSIERINGSOVERSIGT

1. FORANSTALTNINGENS BETEGNELSE

Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet.

2. BUDGETPOST

B5 302

B5 820

B6 1110, B6 2111, B6 1210

3. RETSGRUNDLAG

EF-traktatens artikel 95, 154 og 155 samt EU-traktatens artikel 29 og 34.

4. BESKRIVELSE AF FORANSTALTNINGEN

4.1. Foranstaltningens generelle formål

Kommissionen vil oprette og lede et EU-forum, hvor de retshåndhævende myndigheder, internetudbydere, teleselskaber, borgerrettighedsorganisationer, forbrugerrepræsentanter, databeskyttelsesmyndighederne og andre interesserede kan mødes med det formål at øge den gensidige forståelse og udbygge det gensidige samarbejde på EU-plan. Forummet skal søge at skærpe offentlighedens opmærksomhed over for de risici, som kriminelle personer frembyder på Internettet, fremme bedste praksis på sikkerhedsområdet, identificere effektive redskaber og procedurer til bekæmpelse af computerrelateret kriminalitet og tilskynde til videreudvikling af advarsels- og krisestyringsmekanismer. De relevante dokumenter vil blive offentliggjort på et websted.

4.2. Foranstaltningens varighed og nærmere bestemmelser for dens forlængelse/fornyelse

2001-2002. I 2002 vil man tage stilling til, om Forummet skal fortsætte.

5. KLASSIFIKATION AF UDGIFTERNE/INDTÆGTERNE

5.1. Ikke-obligatoriske udgifter

5.2. Opdelte bevillinger

6. UDGIFTERNES/INDTÆGTERNES ART

Møder: refusion af eksperters rejseudgifter			
B5 302A	2001		27 000 EUR
B5 302A	2002		40 500 EUR
Forummets drift, vedligeholdelse af websted			
B6 1110	2001	JRC Missioner	10 000 EUR
B6 2111	2001	JRC Specifikke bevillinger (diverse)	15 000 EUR
B6 1210	2001	JRC Generalomkostninger	50 000 EUR
B6 1110	2002	JRC Missioner	10 300 EUR
B6 2111	2002	JRC Specifikke bevillinger (diverse)	15 450 EUR
B6 1210	2002	JRC Generalomkostninger	51 500 EUR
Undersøgelser af specifikke emner			
B6 2111	2001	JRC Specifikke bevillinger (undersøgelser)	25 000 EUR
B6 2111	2002	JRC Specifikke bevillinger (undersøgelser)	25 750 EUR
I alt	2001 + 2002		270 500 EUR

7. FINANSIELLE VIRKNINGER

7.1. Beregningsmetode for de samlede omkostninger ved foranstaltningen (fastlæggelse af gennemsnitsomkostningerne pr. enhed)

Refusion af mødedeltageres rejseudgifter. Der er planlagt 2 møder i 2001 og 3 i 2002. 15 eksperter fra hvert møde vil få rejseudgifter refunderet. Gennemsnitlige udgifter pr. person anslås til 900 EUR.

Omkostningerne, både personaleomkostninger og specifikke omkostninger, til infrastruktur og administrativ og teknisk bistand svarer til antallet af ansatte, der beskæftiger sig med de pågældende aktiviteter. Budgettet til undersøgelserne beregnes på grundlag af 2 undersøgelser om året af ca. 1 mandemåned hver.

8. FORHOLDSREGLER MOD SVIG (OG FORVENTEDE RESULTATER HERAF)

Rutinemæssig kontrol. Der påtænkes ingen yderligere forholdsregler.

9. OPLYSNINGER OM COST/EFFECTIVENESS

9.1 Specifikke og kvantificerbare mål, målgruppe

At øge den gensidige forståelse og udbygge det gensidige samarbejde på EU-plan for forskellige interessegrupper. Målgrupper: retshåndhævende myndigheder, internetudbydere, teleselskaber, borgerrettighedsorganisationer, forbrugerrepræsentanter, databeskyttelses-myndigheder og andre interesserede.

9.2 Begrundelse for foranstaltningen

Formålet med Forummet er at øge den gensidige forståelse og udbygge det gensidige samarbejde på EU-plan mellem forskellige interessegrupper. Forummet vil søge at skærpe offentlighedens opmærksomhed over for de risici, som kriminelle personer frembyder på Internettet, fremme bedste praksis på sikkerhedsområdet, identificere effektive redskaber og procedurer til bekæmpelse af computerrelateret kriminalitet og tilskynde til videreudvikling af advarsels- og krisestyringsmekanismer.

9.3 Overvågning og evaluering af foranstaltningen

Kommissionen vil tilrettelægge og lede Forummets møder og deltage i drøftelserne. Kommissionen vil forvalte Forummets websted. Behovet for at fortsætte Forummet i 2003 og derefter vil blive vurderet i 2002.

10 UDGIFTER TIL ADMINISTRATION

Behovet for menneskelige ressourcer vil blive dækket med det nuværende personale.

10.1 Antal stillinger

Type stilling	Personale til forvaltning af initiativet		Kilde		Varighed
	Permanente stillinger	Midlertidige stillinger	GD's nuværende ressourcer	Yderligere ressourcer	
A-tjenestemænd eller midlertidigt A-ansatte B C	 0,05	 0,75 0,15	 1,75 0,15 0,05		om året i 2 år
Andre ressourcer					
I alt	0,05	1,9	1,95		

10.2 Samlet finansiel virkning af menneskelige ressourcer

	Beløb	Beregning (2001 - 2002)
Tjenestemænd	421 200 EUR	2 år x 108 000 EUR x 1,95 ansatte