KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 22.5.2007
KOM(2007) 267 endelig

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET OG REGIONSUDVALGET

Hen imod en generel politik til bekæmpelse af cyberkriminalitet

{SEK(2007) 641}
{SEK(2007) 642}

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET OG REGIONSUDVALGET

Hen imod en generel politik til bekæmpelse af cyberkriminalitet

1. INDLEDNING

1.1. Hvad er cyberkriminalitet?

Et af de vigtigste aspekter ved sikkerheden i informationssystemerne, som får større og større betydning i vores samfund, er bekæmpelse af cyberkriminalitet. Da der ikke er vedtaget en definition af cyberkriminalitet, bruges begreber som "cyberkriminalitet", "computerkriminalitet", "computerrelateret kriminalitet" eller "high tech-kriminalitet" ofte i flæng. I denne meddelelse forstås ved cyberkriminalitet: "kriminelle handlinger, som begås under anvendelse af elektroniske kommunikationsnet og informationssystemer eller er rettet mod sådanne net og systemer".

I praksis anvendes begrebet cyberkriminalitet om tre kategorier af kriminelle aktiviteter. Den første kategori dækker **traditionelle former for kriminalitet** som for eksempel svig eller falskneri, men i forbindelse med cyberkriminalitet tænkes der specielt på kriminalitet, der begås via elektroniske kommunikationsnet og informationssystemer (i det følgende benævnt: elektroniske net). Den anden kategori vedrører offentliggørelse af **ulovligt indhold** via elektroniske medier (bl.a. materiale med seksuel misbrug af børn eller tilskyndelse til racehad). Den tredje kategori omfatter **kriminalitet, der udelukkende er rettet mod elektroniske net**, dvs. angreb mod informationssystemer, denial of service og hacking. Disse former for angreb kan også være rettet direkte mod centrale kritiske infrastrukturer i Europa og påvirke eksisterende alarmeringssystemer på mange områder, hvilket kan få katastrofale følger for hele samfundet. Fælles for disse kategorier af kriminalitet er, at de kan foregå i stor målestok og med en stor geografisk afstand mellem den kriminelle handling og følgerne heraf. Derfor er de tekniske aspekter af anvendte efterforskningsmetoder ofte de samme. Det er disse fælles træk, der vil blive fokuseret på i denne meddelelse.

1.2. Seneste udvikling inden for cyberkriminalitet

1.2.1. Generelt

Kombinationen af kriminelle aktiviteter, der hele tiden udvikler sig, og manglen på pålidelige oplysninger gør det vanskeligt at få et eksakt billede af situationen, som den er nu. Der er dog visse generelle tendenser:

- Antallet af cyber-lovovertrædelser er stigende, og de kriminelle aktiviteter bliver mere og mere sofistikerede og internationaliserede[1]

[1] Hovedparten af det, der siges i denne meddelelse om nuværende tendenser, er taget fra en undersøgelse, som skulle vurdere indvirkningen af en meddelelse om cyberkriminalitet, og som var bestilt af Kommissionen i 2006 (kontrakt nr. JLS/2006/A1/003).

- Der er klare tegn på, at organiserede kriminelle grupper i stigende grad er involveret i cyberkriminalitet

- Men antallet af europæiske retsforfølgelser, der er baseret på et grænseoverskridende politisamarbejde, stiger ikke.

1.2.2. Traditionel kriminalitet inden for elektroniske net

De fleste lovovertrædelser kan begås ved hjælp af elektroniske net, og der er forskellige former for svig og forsøg på svig, som er særligt udbredt og i stigende grad benyttes inden for elektroniske net. Instrumenter som identitetstyveri, phising[2], spam og ondsindede koder kan benyttes til at begå svig i stor målestok. Ulovlig national og international internetbaseret handel er også blevet et stigende problem. Der er blandt andet tale om handel med narkotika, udryddelsestruede arter og våben.

1.2.3. Ulovligt indhold

Der er et stigende antal netsider med ulovligt indhold tilgængelige i Europa, og de dækker materiale med seksuel misbrug af børn, opfordring til terroristhandlinger, ulovlig forherligelse af vold, terrorisme, racisme og fremmedhad. Det er ekstremt vanskeligt at håndhæve loven over for sådanne netsider, da ejerne og administratorerne af siderne ofte opholder sig i andre lande end mållandet og ofte uden for EU. Siderne kan flyttes meget hurtigt, også uden for EU's område, og definitionen af ulovlighed er forskellig fra det ene land til det andet.

1.2.4. Kriminalitet, som kun angår elektroniske net

Angreb i stor målestok mod informationssystemer eller organisationer og enkeltpersoner (ofte gennem såkaldte botnet[3]) er blevet mere og mere almindelige. Der har også på det seneste været flere tilfælde af systematiske, velkoordinerede, direkte og omfattende angreb mod en stats kritiske informationsinfrastruktur. Med de nye teknologier og den hurtige sammenkædning af informationssystemer, som har gjort disse systemer mere sårbare, er det blevet et endnu større problem. Angrebene er ofte velorganiserede og bliver brugt til afpresning. Det antages, at der kun sjældent sker indberetning herom, delvis fordi det kan give problemer for virksomheden, hvis det bliver kendt, at den har sikkerhedsproblemer.

1.3. Mål

Der sker hele tiden ændringer, og derfor er det absolut nødvendigt at gøre noget – såvel på nationalt som på europæisk plan – mod alle former for cyberkriminalitet, som udgør en stadig større trussel mod kritiske infrastrukturer, samfundet, erhvervslivet og borgerne. Beskyttelse af fysiske personer mod cyberkriminalitet bliver ofte vanskeliggjort af problemer med at fastslå det kompetente retsområde, med gældende lov, med grænseoverskridende strafforfølgelse eller med anerkendelse og brug af elektronisk bevismateriale. Den grænseoverskridende dimension af cyberkriminalitet, gør det hele endnu vanskeligere. For at imødegå disse trusler har Kommissionen indledt et generelt politisk initiativ, der skal give en bedre koordinering af kampen mod cyberkriminalitet på europæisk og internationalt plan.

---

[2] Phising betyder forsøg på gennem en elektronisk meddelelse på svigagtig vis at ville erhverve følsomme oplysninger som password og kreditkortoplysninger ved at fremstå som en troværdig person.

[3] Botnet er en samling af inficerede maskiner, der kører programmer, som kontrolleres af en bagmand.

Målet er at styrke kampen mod cyberkriminalitet på nationalt, europæisk og internationalt plan. En videreudvikling af en specifik EU-politik har længe været en prioritet for medlemsstaterne og Kommissionen. I initiativet vil der blive fokuseret på strafforfølgelse og kriminallovgivning, og EU's politik vil være et supplement til andre EU-tiltag, der skal forbedre sikkerheden i cyberspace generelt. Der vil her kunne indgå: bedre operationelt politisamarbejde, bedre politisk samarbejde og koordinering mellem medlemsstaterne, politisk og juridisk samarbejde med tredjelande, oplysningskampagner, uddannelse, forskning, bedre dialog med erhvervsliv og mulige, lovmæssige tiltag.

Den politik, der skal bekæmpe og retsforfølge cyberkriminalitet, vil blive defineret og implementeret på en måde, som fuldt ud respekterer grundlæggende rettigheder, især ytringsfrihed, respekt for privatliv og familieliv og beskyttelse af personoplysninger. Inden der tages et lovmæssigt initiativ i denne politik, vil det først blive undersøgt, om det er foreneligt med disse rettigheder, især med EU's charter om grundlæggende rettigheder. Det skal også bemærkes, at alle politiske initiativer af den art vil blive gennemført under fuld hensyntagen til artikel 12 og 15 i det såkaldte e-handelsdirektiv[4], hvor dette retsinstrument finder anvendelse.

Formålet med denne meddelelse er tresidet og kan kort beskrives således:

- At forbedre og lette koordineringen og samarbejdet mellem cyberkriminalitetsafdelinger, andre relevante myndigheder og andre eksperter i Den Europæiske Union

- Sammen med medlemsstaterne, relevante EU-organisationer og internationale organisationer samt andre interessenter at udvikle en sammenhængende ramme for EU's politik til bekæmpelse af cyberkriminalitet

- At skabe bevidsthed om omkostninger og farer ved cyberkriminalitet.

2. EKSISTERENDE RETSINSTRUMENTER I KAMPEN MOD CYBERKRIMINALITET

2.1. Eksisterende instrumenter og tiltag på EU-plan

Denne meddelelse om cyberkriminalitetspolitik konsoliderer og udvikler meddelelsen fra 2001 "Et sikrere informationssamfund: Højnelse af sikkerheden i informationsstrukturerne og bekæmpelse af computerrelateret kriminalitet"[5] (i det følgende benævnt meddelelsen fra 2001). I meddelelsen fra 2001 blev der foreslået materiel- og procesretlige bestemmelser vedrørende såvel indenlandske som grænseoverskridende kriminelle aktiviteter. Det gav anledning til mange vigtige forslag. Det gælder især det forslag, der førte til rammeafgørelse 2005/222/RIA om angreb på informationssystemer[6]. I den forbindelse skal det desuden bemærkes, at der vedtaget anden, mere generel lovgivning, der også dækker aspekter af kampen mod cyberkriminalitet, for eksempel Rådets rammeafgørelse 2001/413/RIA om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter[7].

---

4 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 (EFT C 178, 17.7.200 s. 1).

5 KOM(2000) 890, 26.1.2001.

6 EUT L 69, s. 67.

7 EFT L 149, 16.3.2005,s. 1.

Rammeafgørelse 2004/68/RIA om seksuel udnyttelse af børn[8] er et godt eksempel på, hvor stor vægt Kommissionen lægger på **beskyttelse af børn**, navnlig på bekæmpelse af alle former for materiale med seksuel misbrug af børn, der ulovligt bliver offentliggjort via informationssystemer. Denne horisontale prioritering vil blive fastholdt fremover.

For at tage sikkerhedsudfordringerne for informationssamfundet op har Det Europæiske Fællesskab udviklet en trestrenget strategi for net- og informationssikkerhed: specifikke sikkerhedsforanstaltninger for net og informationer, reguleringsrammen for elektronisk kommunikation og kampen mod cyberkriminalitet. Selv om disse tre aspekter til en vis grad kan behandles hver for sig, gør de mange indbyrdes afhængigheder det nødvendigt med en tæt koordinering. Således vedtog Kommissionen i 2001 en meddelelse om net- og informationssikkerhed med forslag til en EU-strategi[9] samtidig med meddelelsen fra 2001 om cyberkriminalitet. Ifølge direktiv 2002/58/EF om privatlivets fred har udbydere af en offentligt tilgængelig kommunikationstjeneste pligt til at beskytte sine tjenester. Der er også bestemmelser om spyware og spam i direktivet. Politikken vedrørende net- og informationssikkerhed har siden udviklet sig gennem en række tiltag, for nylig med blandt andet en meddelelse om en strategi for et sikkert informationssamfund[10], som skal puste nyt liv i strategien, og som opstiller rammer for videreudvikling og finjustering af en sammenhængende måde at gribe net- og informationssikkerhed an på, og en meddelelse om bekæmpelse af spam, spyware og skadeligt software[11], og i 2004 med oprettelse af ENISA[12]. Hovedformålet med ENISA er at udvikle ekspertise, der kan stimulere samarbejdet mellem den offentlige og den private sektor og yde bistand til Kommissionen og medlemsstaterne. **Forskningsresultater** vedrørende teknologier til sikring af informationssystemer vil også spille en vigtig rolle i kampen mod cyberkriminalitet. Derfor nævnes informations- og kommunikationsteknologier samt –sikkerhed alle som mål for EU's syvende rammeprogram for forskning (FP 7), som vil være operationelt i perioden 2007-2013[13]. En revision af de reguleringsmæssige rammer for elektronisk kommunikation kan resultere i ændringer, der kan gøre de sikkerhedsrelaterede bestemmelser i direktivet om privatlivets fred og forsyningspligtdirektiv 2002/22/EF[14] mere effektive.

2.2. Eksisterende internationale instrumenter

På grund af informationsnettenes globale natur er der ingen politik om cyberkriminalitet, der kan fungere, hvis indsatsen er begrænset til EU. Kriminelle kan angribe informationssystemer eller begå kriminalitet fra en medlemsstat til en anden, men de kan også let gøre det fra steder uden for EU's retsområde. Derfor har Kommissionen deltaget i internationale diskussioner og samarbejdsstrukturer, blandt andet G 8 Lyon-Roma High-Tech Crime Group og Interpol-administrerede projekter. Kommissionen følger især på nært hold arbejdet i 24-timers kontaktnettet for International High-Tech Crime (24/7-nettet)[15], hvor et stort antal stater på hele kloden, herunder de fleste EU-medlemsstater, er medlem. G 8-nettet er en mekanisme,

---

8 EUT L 13, 20.1.2004, s. 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Forordning 460/2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed, (EUT L 77, 13.3.2004, s. 1).
13 Den Europæiske Union har allerede støttet en række væsentlige og succesrige forskningsprojekter under 6. rammeprogram for forskning og teknologisk udvikling.
14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.
15 Se artikel 35 i Europarådets konvention om cyberkriminalitet.

hvormed der hurtigt opnås kontakt mellem deltagende stater, idet kontaktstederne er tilgængelige 24 timer i døgnet for sager, der involverer elektroniske beviser, og for sager, der kræver øjeblikkelig bistand fra politimyndigheder i udlandet.

Det vigtigste europæiske og internationale instrument på dette område må siges at være Europarådets konvention fra 2001 om cyberkriminalitet[16]. Konventionen, som blev vedtaget og trådte i kraft i 2004 indeholder fælles definitioner af forskellige former for cyberkriminalitet og danner grundlag for et fungerende retligt samarbejde mellem kontraherende stater. Den er undertegnet af mange stater, herunder USA og andre ikke-europæiske stater, og af alle EU's medlemsstater. Nogle af medlemsstaterne har dog endnu ikke ratificeret konventionen eller tillægsprotokollen til konventionen vedrørende strafbare handlinger i forbindelse med racisme eller fremmedhad begået via edb-systemer. I betragtning af den betydning, der tillægges konventionen, vil Kommissionen opfordre medlemsstaterne og relevante tredjelande til at ratificere konventionen og overveje muligheden for, at Det Europæiske Fællesskab deltager i konventionen.

3. VIDEREUDVIKLING AF SPECIFIKKE INSTRUMENTER TIL BEKÆMPELSE AF CYBERKRIMINALITET.

3.1. Et større operationelt samarbejde om retshåndhævelse og uddannelsestiltag på EU-plan

En stor svaghed på området frihed, sikkerhed og retfærdighed er manglen på eller underudnyttelsen af de forhåndenværende strukturer til **grænseoverskridende operationelt samarbejde**. Traditionel gensidig bistand har vist sig at være langsom og ineffektiv, når det drejer sig om presserende sager om cyberkriminalitet, og de nye samarbejdsstrukturer er endnu tilfredsstillende. De nationale doms- og politimyndigheder i Europa arbejder nært sammen inden for Europol, Eurojust og andre strukturer, men der er fortsat helt klart behov for at styrke ansvaret og afklare, hvor det ligger. Ifølge høringer gennemført af Kommissionen benyttes disse vigtige kanaler ikke optimalt. En mere koordineret europæisk tilgang er nødt til at være både operationel og strategisk og også omfatte udveksling af oplysninger og bedste praksis.

Kommissionen vil i nær fremtid lægge særlig vægt på **uddannelsesbehov**. Det er en kendsgerning, at der med den teknologiske udvikling skabes et behov for fortsat uddannelse i emner vedrørende cyberkriminalitet for politi- og domsmyndigheder. Der er derfor planer om, at EU skal give mere og bedre koordineret finansiel støtte til multinationale uddannelsesprogrammer. Kommissionen vil også i nært samarbejde med medlemsstaterne og andre kompetente organer som Europol, Eurojust, Det Europæiske Politiakademi (CEPOL) og Det Europæiske Netværk for Uddannelse af Dommere og Anklagere (EJNT) forsøge at koordinere og forbinde alle relevante uddannelsesprogrammer med hinanden.

Kommissionen vil i 2007 organisere et **møde** med eksperter i retshåndhævelse fra medlemsstaterne og fra Europol, CEPOL og EJTN, hvor det skal drøftes, hvordan det strategiske og operationelle samarbejde samt uddannelse til bekæmpelse af cyberkriminalitet kan forbedres i Europa. Et af de punkter, der skal drøftes, vil være oprettelse af både et permanent EU-kontaktsted til udveksling af oplysninger og en EU-uddannelsesplatform

[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

vedrørende cyberkriminalitet. Mødet i 2007 vil være det første i en række af møder, der er planlangt i nær fremtid.

3.2. En styrkelse af dialogen med erhvervslivet

Både den private og den offentlige sektor har interesse i i fællesskab at udvikle metoder til at identificere og afværge skader som følge af kriminelle aktiviteter. Hvis både den private og den offentlige sektor deltager i gensidig tillid og med det fælles mål at begrænse skaderne, kan det være en effektiv måde af fremme sikkerheden på, også når det drejer sig om cyberkriminalitet. De offentligt-private aspekter af Kommissionens cyberkriminalitetspolitik vil, når den tid kommer, blive en del af en planlagt global EU-politik om en dialog mellem den offentlige og den private sektor, som skal dække hele området for europæisk sikkerhed. Denne politik vil især blive anført af et europæisk forum for forskning og innovation på sikkerhedsområdet, som Kommissionen vil oprette om kort tid, og som vil få deltagelse af relevante interessenter fra den offentlige og den private sektor.

Udviklingen af moderne informationsteknologier og elektroniske kommunikationssystemer er i vid udstrækning kontrolleret af private operatører. Det er private selskaber, der udfører trusselsvurderinger, fastlægger programmer til bekæmpelse af kriminalitet og udvikler tekniske løsninger til at forebygge kriminalitet. Erhvervslivet har været meget positivt og forsøgt at hjælpe de offentlige myndigheder i kampen mod cyberkriminalitet, især med at forhindre børnepornografi[17] og andre former for ulovligt indhold på internettet.

Et andet problem er den tilsyneladende mangel på udveksling af oplysninger, ekspertviden og bedste praksis mellem den offentlige og den private sektor. Operatører i den private sektor er ofte tilbageholdende med – fordi de vil beskytte forretningsmodeller og –hemmeligheder - eller har ingen klar juridisk forpligtelse til at indberette eller dele relevante oplysninger om kriminelle hændelser med politimyndighederne. Men sådanne oplysninger kan være nødvendige, hvis de offentlige myndigheder skal kunne udforme en effektiv, hensigtsmæssig politik til bekæmpelse af kriminalitet. Der vil også blive set på muligheden for at forbedre udvekslingen af oplysninger på tværs af sektorer i lyset af gældende regler om beskyttelse af personoplysninger.

Kommissionen spiller allerede en vigtig rolle inden for forskellige offentligt-private strukturer, der tager sig af cyberkriminalitet, for eksempel Fraud Prevention Expert Group (en ekspertgruppe til forebyggelse af svig)[18]. Kommissionen er overbevist om, at der i en effektiv generel politik til bekæmpelse af cyberkriminalitet skal indgå en strategi om samarbejde mellem den offentlige og den private sektor, herunder civilsamfundsorganisationer.

For at opnå et bredere offentligt-privat samarbejde på dette område vil Kommissionen i 2007 afholde en konference for eksperter i retshåndhævelse og repræsentanter for den private sektor, især udbydere af internettjenester[19]. Konferencen vil tage alle de emner op, som anses for at kunne give en merværdi til begge sektorer, men især:

---

17 Et af de seneste eksempler på samarbejde på dette område er samarbejdet mellem politimyndigheder og kreditkortselskaber, hvor sidstnævnte har hjulpet politiet med at opspore købere af børnepornografi på nettet.

18 Se http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 Konferencen kan betragtes som en fortsættelse af det EU-forum, der er er omtalt under punkt 6.4 i meddelelsen om computerkriminalitet.

- Forbedring af det operationelle samarbejde i kampen mod ulovlige aktiviteter og ulovligt indhold på internettet, især på områderne terrorisme, materiale om seksuel misbrug af børn og andre ulovlige aktiviteter, som er særligt følsomme, når det gælder beskyttelse af børn

- Indgåelse af offentligt-private aftaler om på EU-plan at blokere steder, der indeholder ulovligt indhold, især materiale med seksuel misbrug af børn

- Udformning af en europæisk model for deling af nødvendige, relevante oplysninger på tværs af den private og den offentlige sektor, hvor en af overvejelserne vil være, hvordan man kan opnå en atmosfære af gensidig tillid og tage hensyn til alle parters interesser

- Etablering af et net af kontaktsteder for retshåndhævelse i både den private og den offentlige sektor.

3.3. Lovgivning

Det er endnu for tidligt med en generel harmonisering af definitioner på kriminalitet og nationale straffelove på området cyberkriminalitet på grund af de mange former for lovovertrædelse, som er dækket af dette begreb. Et effektivt samarbejde mellem politimyndigheder afhænger ofte af, at der i det mindste findes delvis harmoniserede definitioner på kriminalitet, men det tager lang tid at få harmoniseret medlemsstaternes lovgivning[20]. For visse nøgledefinitioner på kriminalitet er der allerede taget et vigtigt skridt med rammeafgørelsen om angreb på informationssystemer. Som tidligere omtalt har der siden vist sig nye trusler, og Kommissionen følger nøje udviklingen, eftersom det er særdeles vigtigt løbende at vurdere behovet for ekstra lovgivning. Overvågningen af de nye trusler bliver nøje koordineret med det europæiske program til beskyttelse af kritisk infrastruktur.

Det bør dog også nu overvejes at indføre en målrettet lovgivning mod cyberkriminalitet. Et særligt område, hvor det også kan være nødvendigt med lovgivning, vedrører situationer, hvor cyberkriminalitet bliver begået sammen med **identitetstyveri.** Generelt forstås ved "identitetstyveri" brug af en personlig identifikationsoplysning, f.eks. et kreditkortnummer, som et instrument til at begå andre forbrydelser. I de fleste medlemsstater vil en lovovertræder højst sandsynligt blive retsforfulgt for svig eller en anden potentiel forbrydelse snarere end for identitetstyveri, idet førstnævnte anses for at være en mere alvorlig forbrydelse. Identitetstyveri som sådan anses ikke for at være kriminelt i alle medlemsstater. Det er ofte lettere at bevise, at der er begået identitetstyveri end svig, hvorfor det vil være bedre for politisamarbejdet i EU, hvis identitetstyveri bliver kriminaliseret i alle medlemsstater. Kommissionen vil i 2007 begynde at foretage høringer for at vurdere, om lovgivningen er hensigtsmæssig.

---

[20] Dette mere langsigtede mål er allerede blevet omtalt på side 3 i meddelelsen fra 2001.

3.4. Udvikling af statistiske oplysninger

Der er generelt enighed om, at de nuværende oplysninger om kriminalitetens omfang slet ikke er tilfredsstillende, og at der er meget, der skal forbedres, hvis dataene fra medlemsstaterne skal kunne sammenlignes. I Kommissionens meddelelse om *en overordnet og sammenhængende EU-strategi for måling af kriminalitet og strafferetlig behandling deraf: En EU-handlingsplan 2006-2010*[21], er der opstillet en ambitiøs femårsplan til løsning af dette problem. Den ekspertgruppe, der er nedsat i henhold til denne handlingsplan, kan være et passende forum for udvikling af relevante indikatorer, som kan måle omfanget af cyberkriminalitet.

4. VEJEN FREM

Kommissionen vil nu sørge for, at der bliver sat mere fokus på den generelle politik for bekæmpelse af cyberkriminalitet. Da Kommissionens beføjelser på strafferetsområdet er begrænsede, kan denne politik kun blive et supplement til de tiltag, der er i gang i medlemsstaterne og andre organer. De vigtigste tiltag – som hver især indebærer brug af et, flere eller alle de instrumenter, der er omtalt i kapitel 3 – vil også få hjælp gennem finansieringsprogrammet om forebyggelse og bekæmpelse af kriminalitet.

4.1. Bekæmpelse af cyberkriminalitet generelt

- Etablering af et udvidet, operationelt samarbejde mellem de forskellige medlemsstaters politi- og domsmyndigheder, hvilket vil starte med afholdelse af et særligt ekspertmøde i 2007 og kan omfatte oprettelse af et centralt EU-kontaktsted for cyberkriminalitet.

- Øget finansiel støtte til initiativer til bedre uddannelse af politi- og domsmyndigheder i behandling af sager om cyberkriminalitet og forsøg på koordinering af alle multinationale uddannelsestiltag på området ved at oprette en EU-uddannelsesplatform.

- Et større engagement fra medlemsstaternes og alle offentlige myndigheders side med hensyn til at ville træffe effektive foranstaltninger mod cyberkriminalitet og afsætte tilstrækkelige midler til at bekæmpe denne form for forbrydelser.

- Støtte til forskning, der kan være nyttig for bekæmpelse af cyberkriminalitet.

- Afholdelse af mindst én større konference (i 2007) med politimyndigheder og private operatører, navnlig for at indlede et samarbejde i kampen mod ulovlige internetaktiviteter i elektroniske net og opnå en mere effektiv udveksling af ikke-personlige oplysninger og for at følge op på konklusionerne fra denne konference med konkrete offentligt-private samarbejdsprojekter.

- Initiativ til og deltagelse i offentligt-private tiltag, der skal skabe større bevidsthed hos især forbrugerne om omkostningerne og farerne ved cyberkriminalitet uden dermed at undergrave forbrugernes og brugernes tillid ved kun at fokusere på de negative aspekter af sikkerhed.

---

[21] KOM(2006) 437, 7.8.2006.

- Aktiv deltagelse i og fremme af et globalt, internationalt samarbejde om bekæmpelse af cyberkriminalitet.

- Igangsætning af og bidrag og støtte til internationale projekter, som er på linje med Kommissionens politik på dette område, f.eks. projekter, som ledes af G 8 og er i overensstemmelse med landepapirer og regionale strategipapirer (om samarbejdet med tredjelande)

- Konkrete forsøg på at få alle medlemsstater og relevante tredjelande til at ratificere Europarådets konvention om cyberkriminalitet og tillægsprotokollen hertil og at overveje muligheden af, at Fællesskabet deltager i konventionen.

- Undersøgelse i samarbejde med medlemsstaterne af fænomenet med koordinerede, omfattende angreb mod medlemsstaters informationsinfrastruktur for at forhindre og bekæmpe sådanne angreb, blandt andet med koordinerede reaktioner og udveksling af information og bedste praksis

4.2. Kampen mod traditionel kriminalitet i elektroniske net

- En indgående analyse til forberedelse af et forslag til specifik EU-lovgivning om identitetstyveri.

- Udvikling af tekniske metoder og procedurer til bekæmpelse af svig og ulovlig handel på internettet, også gennem offentligt-private samarbejdsprojekter.

- Fortsættelse og udvikling af arbejdet inden for specifikke målområder, blandt andet i ekspertgruppen til forebyggelse af svig i forbindelse med andre betalingsmidler end kontanter i elektroniske net.

4.3. Ulovligt indhold

- Fortsat udvikling af tiltag mod specifikt, ulovligt indhold, især materiale med seksuelt misbrug af børn og opfordring til terrorisme, navnlig ved at følge op på implementeringen af rammeafgørelsen vedrørende seksuel udnyttelse af børn.

- Opfordring til medlemsstaterne om at afsætte tilstrækkelige finansielle ressourcer til arbejdet i retshåndhævelsesorganer, især med henblik på at identificere ofrene for seksuelt misbrug, som er med i det materiale, der distribueres på nettet.

- Igangsættelse af og støtte til aktioner mod ulovligt indhold, som kan tilskynde mindreårige til voldelig og anden alvorlig, ulovlig adfærd, f.eks. visse former for ekstremt voldelige onlinevideospil.

- Indledning og fremme af en dialog mellem medlemsstaterne og med tredjelande om tekniske metoder til bekæmpelse af ulovligt indhold samt om procedurer til at lukke ulovlige websteder, også med henblik på at nå frem til formelle aftaler med nabolande og andre lande om dette problem.

- Udvikling på EU-plan af frivillige aftaler og konventioner mellem offentlige myndigheder og private operatører, især udbydere af internettjenester, med hensyn til procedurer til blokering og lukning af ulovlige internetsteder.

4.4. Opfølgning

I denne meddelelse er der blevet skitseret en række tiltag, der i de næste faser skal forbedre samarbejdsstrukturerne i EU. Kommissionen vil arbejde videre med disse tiltag, vurdere, hvilke fremskridt der gøres med implementeringen af aktiviteterne, og aflægge rapport til Rådet og Parlamentet.