EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 22.5.2007
KOM(2007) 267 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET OCH EUROPEISKA UNIONENS REGIONKOMMITTÉ

Att införa en allmän politik för kampen mot IT-relaterad brottslighet

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

MEDDELANDE FRÅN KOMMISSIONEN
TILL EUROPAPARLAMENTET, RÅDET
OCH EUROPEISKA UNIONENS REGIONKOMMITTÉ

Att införa en allmän politik för kampen mot IT-relaterad brottslighet

1. INLEDNING

1.1. Vad avses med IT-relaterad brottslighet?

Säkerheten hos de allt mer betydelsefulla informationssystemen i våra samhällen är en mångfacetterad fråga, och kampen mot IT-relaterad brottslighet är en central aspekt av denna. Det saknas en gemensam definition av begreppet IT-relaterad brottslighet, och ord som ”Internetbrottslighet”, ”databrottslighet”, ”datorrelaterad brottslighet” eller ”högteknologisk brottslighet” användas ofta synonymt. I detta meddelande avses med ”IT-relaterad brottslighet” brottsliga handlingar som begås med användning av kommunikationsnät och informationssystem eller som riktas mot sådana nät eller system.

I praktiken avser begreppet IT-relaterad brottslighet tre olika kategorier av brottslig verksamhet. Den första omfattar **traditionella brottsformer** som bedrägeri eller förfalskning, som i detta sammanhang begås med hjälp av elektroniska kommunikationsnät eller informationssystem (nedan kallade ”elektroniska nät”). Den andra kategorin rör offentliggörande av **olagligt innehåll** via elektroniska medier (t.ex. barnpornografiskt material eller hets mot folkgrupp). Till den tredje kategorin hör **brott som uteslutande riktas mot elektroniska nät**, dvs. angrepp mot informationssystem, överbelastningsattacker och olaga intrång i informationssystem (s.k. hackning). Sådana attacker kan också riktas mot samhällsviktig kritisk infrastruktur i Europa och påverka de förvarningssystem som inrättats på många områden, vilket kan få katastrofala följder för hela samhället. Gemensamt för alla dessa brottskategorier är att de kan begås i stor skala och att det geografiska avståndet mellan den brottsliga handlingen och dess följdverkningar kan vara stort. De tekniska aspekterna av de undersökningsmetoder som används är därför ofta desamma. Dessa likheter står i centrum för detta meddelande.

1.2. Den senaste utvecklingen inom IT-relaterad brottslighet

1.2.1. Allmänt

Den IT-relaterade brottsligheten utvecklas konstant och det saknas tillförlitliga uppgifter om den, vilket gör det svårt att skapa en exakt bild av nuläget. Vissa allmänna tendenser kan ändå urskiljas:

- Antalet IT-relaterade brott ökar och brottsligheten blir allt mer sofistikerad och internationaliserad[1].

- Det finns tydliga tecken på att organiserade kriminella sammanslutningar i allt större utsträckning är involverade i IT-relaterad brottslighet.

- Trots detta har antalet åtal som väcks i Europa inom ramen för gränsöverskridande brottsbekämpande samarbete inte ökat.

1.2.2. Traditionella brott via elektroniska nät

De flesta brott kan begås med hjälp av elektroniska nät, och vissa typer av bedrägeri och försök till bedrägeri är särskilt vanliga – och blir allt vanligare – i detta sammanhang. Metoder som identitetsstöld, nätfiske (s.k. phishing[2]), skräppost och saboterande koder kan användas för att begå storskaligt bedrägeri. Olaglig nationell och internationell Internethandel håller också på att bli ett stort problem. Sådan handel kan avse t.ex. narkotika, utrotningshotade arter och vapen.

1.2.3. Olagligt innehåll

En allt större mängd webbplatser med olagligt innehåll är tillgängliga i Europa. Det kan röra sig om barnpornografi, uppmaning till terrorism eller olagligt förhärligande av våld, terrorism, rasism och främlingsfientlighet. Det är extremt svårt att vidta brottsbekämpande åtgärder mot sådana webbplatser, eftersom deras ägare och administratörer oftast befinner sig i ett annat land än det land som åtgärderna riktas mot (ofta utanför EU). Webbplatserna kan flyttas mycket snabbt, även utanför EU:s territorium, och definitionerna av vad som är olagligt varierar avsevärt mellan olika stater.

1.2.4. Brott som riktas mot elektroniska nät

Storskaliga angrepp mot informationssystem eller mot organisationer eller privatpersoner (ofta genom s.k. robotnät eller botnät)[3] har blivit allt vanligare. På senare tid har det också rapporterats om systematiska, storskaliga angrepp direkt mot en stats kritiska IT-infrastruktur. Detta problem har förvärrats av att olika tekniker smälter samman allt mer och informationssystem sammanlänkas i allt snabbare takt, vilket gör systemen mer sårbara. Angreppen är ofta välorganiserade och syftet är utpressning. Sannolikt är rapporteringen om sådana angrepp mycket begränsad, delvis på grund av de affärsmässiga nackdelar som det skulle kunna få om sådana säkerhetsproblemen blev allmänt kända.

---

1 Uppgifterna i detta meddelande om aktuella tendenser har till största delen hämtats ur den analys av konsekvenserna av ett meddelande om IT-relaterad brottslighet som kommissionen lät göra 2006 (kontrakt nr JLS/2006/A1/003).

2 Försök att på bedräglig väg komma över känsliga uppgifter, t.ex. lösenord och kreditkortsuppgifter, genom att uppge sig vara en tillförlitlig person i en elektronisk kommunikation.

3 Ett nätverk av "kapade" datorer som fjärrstyrs genom ett centralt kommando.

1.3. Mål

Mot bakgrund av denna utveckling och med tanke på att den IT-relaterade brottsligheten utgör ett allt större hot mot kritisk infrastruktur, samhället, företag och medborgare finns det ett akut behov av åtgärder mot alla dess former, både nationellt och på EU-nivå. Möjligheten att skydda privatpersoner mot IT-relaterad brottslighet försvåras ofta av frågor som rör fastställande av behörighet, tillämplig lagstiftning, gränsöverskridande brottsbekämpning eller erkännande och användning av bevis i elektronisk form. Dessa svårigheter kommer sig av det faktum att den IT-relaterade brottsligheten till sin natur huvudsakligen är gränsöverskridande. För att kunna bemöta detta hot tar kommissionen nu ett allmänpolitiskt initiativ för att förbättra samordningen på europeisk och internationell nivå när det gäller kampen mot IT-relaterad brottslighet.

Syftet är att intensifiera kampen mot IT-relaterad brottslighet på nationell, europeisk och internationell nivå. Utvecklingen av en särskild EU-politik på detta område har av medlemsstaterna och kommissionen länge setts som en viktig prioritering. Initiativet inriktas på de brottsbekämpande och straffrättsliga aspekterna av denna kamp, och politiken kommer att komplettera andra EU-åtgärder för att förbättra den allmänna säkerheten i cyberrymden. Den skall i slutändan leda till ett bättre fungerande operativt samarbete när det gäller brottsbekämpning, bättre politiskt samarbete och samordning mellan medlemsstaterna, bättre politiskt och rättsligt samarbete med tredjeländer, ökad medvetenhet, utbildning, forskning, en stärkt dialog med industrin samt eventuellt lagstiftningsåtgärder.

Politiken för bekämpning och lagföring av IT-relaterad brottslighet kommer att utformas och genomföras på ett sätt som till fullo respekterar grundläggande rättigheter, särskilt yttrandefriheten, rätten till respekt för privatliv och familjeliv samt skyddet av personuppgifter. Eventuella lagstiftningsåtgärder inom ramen för denna politik kommer först att granskas för att kontrollera att de är förenliga med dessa rättigheter, särskilt Europeiska unionens stadga om de grundläggande rättigheterna. Det bör också noteras att alla sådana initiativ kommer att genomföras med beaktande av artiklarna 12–15 i direktivet om elektronisk handel[4] i den utsträckning detta är tillämpligt.

Syftet med detta meddelande låter sig indelas i tre delmål, som kort kan beskrivas på följande sätt:

- Att förbättra och underlätta samordningen och samarbetet mellan de myndigheter som bekämpar IT-relaterad brottslighet, andra berörda myndigheter och andra experter i EU.

- Att i samordning med medlemsstaterna, berörda EU-organ, internationella organisationer och andra berörda parter utveckla en konsekvent politisk ram för EU i kampen mot IT-relaterad brottslighet.

- Att öka medvetenheten om de kostnader och risker som IT-relaterad brottslighet medför.

---

[4] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (EGT L 178, 17.7.2000, s. 1).

2. BEFINTLIGA RÄTTSLIGA INSTRUMENT I KAMPEN MOT IT-RELATERAD BROTTSLIGHET

2.1. Befintliga instrument och åtgärder på EU-nivå

Genom det här meddelandet om IT-relaterad brottslighet konsolideras och vidareutvecklas meddelandet från 2001 om ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet[5] (nedan kallat ”meddelandet från 2001”). I meddelandet från 2001 föreslogs lämpliga materiella regler och procedurregler för att bekämpa både inhemsk och gränsöverskridande brottslig verksamhet. Meddelandet ledde till flera viktiga förslag, bland annat det som utmynnade i rådets rambeslut 2005/222/RIF om **angrepp mot informationssystem**[6]. I detta sammanhang bör det noteras att vissa aspekter av kampen mot IT-relaterad brottslighet också täcks av annan, mer allmän lagstiftning, t.ex. rådets rambeslut 2001/413/RIF om bekämpning av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter[7].

Rådets rambeslut 2004/68/RIF om bekämpande av sexuellt utnyttjande av barn och barnpornografi[8] är ett exempel på den stora uppmärksamhet som kommissionen ägnar **skydd av barn**, särskilt i samband med kampen mot alla former av olagligt offentliggörande av barnpornografiskt material genom informationssystem, en övergripande prioritering som kommissionen kommer att hålla fast vid även i framtiden.

För att angripa säkerhetsproblematiken i informationssamhället har gemenskapen utvecklat en tredelad strategi för nät- och informationssäkerhet bestående av specifika åtgärder för nät- och informationssäkerhet, en rättslig ram för elektronisk kommunikation samt kampen mot IT-relaterad brottslighet. Dessa tre aspekter kan visserligen i viss mån behandlas var för sig, men de hänger ihop på många punkter, vilket nödvändiggör en nära samordning. Parallellt med meddelandet från 2001 om datorrelaterad brottslighet antogs på det närliggande området nät- och informationssäkerhet ett meddelande från kommissionen med titeln ”Nät- och informationssäkerhet: förslag till en europeisk strategi”[9]. I direktivet (2002/58/EG) om integritet och elektronisk kommunikation fastställs att de som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster är skyldiga att säkerställa att deras tjänster är säkra. Dessutom fastställs bestämmelser om skräppost och spionprogram. Politiken för nät- och informationssäkerhet har sedan dess vidareutvecklats genom en rad åtgärder, av vilka de senaste är meddelandet om en strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande”[10] som syftar till att blåsa nytt liv i strategin och skapa en ram för vidareutveckling av en konsekvent strategi för nät- och informationssäkerhet, meddelandet om skräppost, spionprogram och sabotageprogram[11] samt inrättandet av Europeiska byrån för nät- och informationssäkerhet (ENISA)[12] år 2004. Det viktigaste målet för ENISA är att utveckla sakkunskap för att främja samarbetet mellan den offentliga och den privata sektorn och att bistå kommissionen och medlemsstaterna med stöd och råd.

---

5 KOM(2000) 890; 26.1.2001.
6 EUT L 69, 16.3.2005, s. 67.
7 EGT L 149, 2.6.2001, s. 1.
8 EUT L 13, 20.1.2004, s. 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet, (EUT L 77, 13.3.2004, s. 1).

Forskningsresultat inom säkerhetsteknik för informationssystem kommer också att spela en viktig roll för kampen mot IT-relaterad brottslighet. Följaktligen tas både informations- och kommunikationsteknik och säkerhet upp som mål i EU:s sjunde ramprogram för forskning, som är i kraft under perioden 2007–2013[13]. Den pågående översynen av regelverket för elektronisk kommunikation[14] kan komma att leda till ändringar för att göra de säkerhetsrelaterade bestämmelserna i direktivet om integritet och elektronisk kommunikation och direktiv 2002/22/EG om samhällsomfattande tjänster mer verkningsfulla.

2.2. Befintliga internationella instrument

Eftersom informationsnäten är världsomspännande kan politiken mot IT-relaterad brottslighet omöjligen vara effektiv om den begränsas till att enbart gälla EU. Brottslingar angriper informationssystem eller begår brottsliga handlingar inte bara från en medlemsstat till en annan, utan också med lätthet från platser utanför EU:s jurisdiktion. Därför har kommissionen aktivt deltagit i internationella överläggningar och samarbetsstrukturer, t.ex. G8-ländernas Lyon–Rom-arbetsgrupp mot högteknologisk brottslighet och olika projekt under ledning av Interpol. Kommissionen följer med stor uppmärksamhet arbetet inom nätverket för dygnetruntkontakt i kampen mot högteknologisk brottslighet ("nätverk 24/7")[15], i vilket en rad länder i hela världen deltar, däribland de flesta EU-medlemsstater. G8-nätverket utgör en mekanism för snabba kontakter mellan de deltagande staterna, med dygnetruntöppna kontaktpunkter för ärenden som är relaterade till bevis i elektronisk form eller som kräver omedelbar hjälp från brottsbekämpande myndigheter i ett annat land.

Det absolut viktigaste europeiska och internationella instrumentet på detta område är Europarådets konvention om IT-relaterad brottslighet[16] från 2001. Konventionen antogs och trädde i kraft 2004 och innehåller gemensamma definitioner av olika typer av IT-relaterad brottslighet. Den lägger grunden för ett fungerande rättsligt samarbete mellan de fördragsslutande parterna och har undertecknats av bl.a. Förenta staterna och en rad andra stater utanför Europa liksom av samtliga EU-medlemsstater. Ett antal medlemsstater har dock ännu inte ratificerat konventionen eller dess tilläggsprotokoll om kriminalisering av gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem. Med beaktande av konventionens erkända betydelse kommer kommissionen att uppmuntra medlemsstater och relevanta tredjeländer att ratificera den, och den kommer även att undersöka möjligheterna för Europeiska gemenskapen att ansluta sig till konventionen

---

13 EU har redan inom ramen för sjätte ramprogrammet för forskning och teknisk utveckling understött många relevanta – och framgångsrika – forskningsprojekt.

14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.

15 Se artikel 35 i Europarådets konvention om IT-relaterad brottslighet.

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

3. VIDAREUTVECKLING AV SÄRSKILDA INSTRUMENT FÖR KAMPEN MOT IT-RELATERAD BROTTSLIGHET

3.1. Ett intensifierat operativt samarbete mellan brottsbekämpande myndigheter samt utbildningsinsatser på EU-nivå

En av de största svagheterna på området för rättvisa, frihet och säkerhet är bristen på, eller i förekommande fall underutnyttjandet av, strukturer för ett omedelbart **gränsöverskridande operativt samarbete**. Traditionellt ömsesidigt bistånd har visat sig vara långsamt och ineffektivt när det gäller IT-relaterade brott som kräver ett snabbt ingripande, och nya samarbetsstrukturer är ännu inte tillräckligt utvecklade. Nationella rättsliga och brottsbekämpande myndigheter i Europa samarbetar visserligen genom Europol, Eurojust och andra strukturer, men det finns ett uppenbart behov av att stärka och klargöra ansvarsfördelningen. Samråd som kommissionen hållit tyder på att dessa viktiga kanaler inte används optimalt. EU behöver ett mer samordnat angreppssätt, som måste vara både operativt och strategiskt och även omfatta utbyte av information och bästa metoder.

Kommissionen kommer under den närmaste tiden att fästa särskild vikt vid **utbildningsbehoven**. Man har konstaterat att den tekniska utvecklingen för med sig ett konstant behov av utbildning för de brottsbekämpande och rättsliga myndigheterna i frågor rörande IT-relaterad brottslighet. Ett stärkt och bättre samordnat finansiellt stöd från EU till multinationella utbildningsprogram planeras därför. Kommissionen kommer också att, i nära samarbete med medlemsstaterna och relevanta organisationer som Europol, Eurojust, Europeiska polisakademin (CEPOL) och det europeiska nätverket för rättslig utbildning (European Judicial Training Network, EJNT), arbeta för att alla relevanta utbildningsprogram skall samordnas och knytas samman på EU-nivå.

Kommissionen kommer att ordna ett **möte** för experter på området brottsbekämpning från medlemsstaterna, Europol, CEPOL och EJNT för att diskutera hur det strategiska och operativa samarbetet och utbildningen om IT-relaterad brottslighet kan förbättras i Europa under 2007. Bland annat kommer man att diskutera inrättandet av en permanent EU-kontaktpunkt för informationsutbyte och ett EU-forum för utbildning om IT-relaterad brottslighet. Mötet i år blir det första i en rad planerade möten som skall äga rum inom en nära framtid.

3.2. Stärkt dialog med industrin

Det ligger i både den privata och den offentliga sektorns intresse att gemensamt utveckla metoder för att kartlägga och förebygga skador som vållas av brottslig verksamhet. Ett gemensamt deltagande av den offentliga och den privata sektorn på grundval av ömsesidigt förtroende och med skadebegränsning som gemensamt mål kan utgöra ett effektivt sätt att öka säkerheten, även när det gäller IT-relaterad brottslighet. Dessa två dimensioner av kommissionens politik för kampen mot IT-relaterad brottslighet avses småningom ingå i en övergripande EU-policy för dialog mellan den offentliga och den privata sektorn, som skall täcka samtliga aspekter av säkerheten inom EU. Denna policy kommer att vidareutvecklas av ett forum för europeisk säkerhetsforskning och innovation som kommissionen har för avsikt att inrätta inom kort och som skall föra samman intresserade parter från den offentliga och den privata sektorn.

Utvecklingen av modern informationsteknik och elektroniska kommunikationssystem kontrolleras i stor utsträckning av privata aktörer. Privata företag utför bedömningar av hotbilder, utarbetar program för att bekämpa brott och utvecklar tekniska brottsförebyggande lösningar. Industrin har visat en mycket positiv inställning till att hjälpa de offentliga myndigheterna i kampen mot IT-relaterad brottslighet, särskilt när det gäller att bekämpa barnpornografi[17] och andra typer av olagligt innehåll på Internet.

En annan stor fråga är de uppenbara bristerna när det gäller utbyte av information, sakkunskap och bästa metoder mellan den offentliga och den privata sektorn. Aktörer inom den privata sektorn som vill skydda sina affärsmodeller och affärshemligheter är ofta ovilliga – och har heller inte någon klar juridisk skyldighet – att rapportera brott eller lämna information om brottsfrekvenser till brottsbekämpande myndigheter. Sådan information kan dock vara nödvändig för att myndigheterna skall kunna utforma en effektiv och adekvat brottsbekämpningsstrategi. Möjligheterna att förbättra informationsutbytet mellan de två sektorerna kommer att undersökas även mot bakgrund av gällande regler för skydd av personuppgifter.

Kommissionen spelar redan en viktig roll inom olika offentlig-privata strukturer som bekämpar IT-relaterad brottslighet, t.ex. expertgruppen för förebyggande av bedrägerier[18]. Kommissionen är övertygad om att en effektiv allmän politik för kampen mot IT-relaterad brottslighet också måste inbegripa en strategi för samarbete mellan aktörer inom den offentliga och den privata sektorn, däribland organisationer inom det civila samhället.

För att få till stånd ett bredare samarbete mellan den offentliga och den privata sektorn kommer kommissionen under 2007 att ordna en konferens för brottsbekämpningsexperter och företrädare för den privata sektorn, särskilt Internetleverantörer, där man skall diskutera hur det operativa samarbetet mellan de två sektorerna i Europa kan förbättras[19]. Alla frågor som anses tillföra ett mervärde för bägge sektorerna kommer att tas upp, med tonvikt på följande:

- Förbättring av det internationella samarbetet för bekämpning av olaglig verksamhet och olagligt innehåll på Internet, särskilt när det gäller terrorism, barnpornografi och annan olaglig verksamhet som är särskilt graverande ur ett barnskyddsperspektiv.

- Överenskommelser mellan den offentliga och den privata sektorn för att få till stånd en EU-omfattande blockering av webbplatser med olagligt innehåll, särskilt barnpornografiskt material.

- Utformning av en europeisk modell för utbyte av nödvändiga och relevanta uppgifter mellan de två sektorerna, på grundval av ömsesidigt förtroende och med beaktande av alla parters intressen.

- Inrättande av ett nät av kontaktpunkter för brottsbekämpning inom de två sektorerna.

---

[17] Ett färskt exempel på detta är samarbetet mellan brottsbekämpande myndigheter och kreditkortsföretag, där företagen hjälpt polisen att spåra personer som köpt barnpornografi via Internet.

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

[19] Konferensen kan ses som en förlängning av det EU-forum som beskrivs i avsnitt 6.4 i meddelandet från 2001.

3.3. Lagstiftning

En allmän harmonisering av brottsdefinitioner och nationell strafflagstiftning på området IT-relaterad brottslighet låter sig ännu inte göras på grund av de många olika brottsformer som omfattas av detta begrepp. Eftersom ett fruktbart samarbete mellan brottsbekämpande myndigheter brukar förutsätta att brottsdefinitionerna åtminstone delvis harmoniserats, är ett långsiktigt mål att fortsätta att harmonisera medlemsstaternas lagstiftning[20]. När det gäller vissa centrala definitioner har ett viktigt framsteg redan gjorts i och med rambeslutet om angrepp mot informationssystem. Som nämns ovan har nya hot uppstått sedan dess, och kommissionen följer uppmärksamt utvecklingen i syfte att kontinuerligt utvärdera behovet av ytterligare lagstiftning. Uppföljningen av de nya hoten samordnas med det europeiska programmet för skydd av kritisk infrastruktur.

Det är emellertid också dags att överväga riktad lagstiftning mot IT-relaterad brottslighet. En specifik fråga som man kan komma att behöva lagstifta om rör situationer då IT-relaterad brottslighet begås i samband med **identitetsstöld**. Med identitetsstöld avses vanligen att personliga identitetsuppgifter, t.ex. kreditkortsnummer, används för att begå andra brott. I de flesta medlemsstater blir den som begår ett sådant brott åtalad för bedrägeri eller för något annat brott som begåtts genom identitetsstölden, och inte för identitetsstölden i sig, eftersom de förstnämnda anses vara allvarligare brott. Identitetsstöld är inte ett brott i alla medlemsstater. Det är emellertid ofta lättare att bevisa identitetsstöld än bedrägeri, varför det brottsbekämpande samarbetet inom EU skulle vinna på att identitetsstöld blev straffbelagt i alla medlemsstater. Kommissionen kommer under 2007 att inleda samråd för att bedöma om det är lämpligt att lagstifta om detta.

3.4. Utveckling av statistiska uppgifter

De flesta är överens om att den information om brottsfrekvenser som finns att tillgå är helt otillräcklig och att det finns rum för stora förbättringar i synnerhet när det gäller möjligheterna att jämföra uppgifter från olika medlemsstater. I sitt meddelande av den 7 augusti 2006 *”En övergripande och samordnad EU-strategi för mätning av brottslighet och straffrättskipning: EU:s handlingsplan 2006–2010”*[21] lägger kommissionen fram en ambitiös femårsplan för att råda bot på detta problem. Den expertgrupp som enligt handlingsplanen skall inrättas skulle utgöra ett lämpligt forum för utarbetande av relevanta indikatorer för att mäta förekomsten av IT-relaterad brottslighet.

4. FRAMTIDA UTVECKLING

Kommissionen går nu vidare med sin allmänna politik för kampen mot IT-relaterad brottslighet. Eftersom kommissionens befogenheter på det straffrättsliga området är begränsade kan denna politik endast utgöra ett komplement till de åtgärder som medlemsstaterna och andra organ vidtar. Nedan anges de viktigaste åtgärderna, som alla kommer att innebära att ett, flera eller alla av de instrument som beskrivs i avsnitt 3 används och som också kommer att understödjas genom det särskilda programmet ”Förebyggande och bekämpande av brott”.

---

[20] Detta långsiktiga mål nämns redan i meddelandet från 2001 (s. 3).

[21] KOM(2006) 437, 7.8.2006.

4.1. Kampen mot IT-relaterad brottslighet i allmänhet

- Ett stärkt samarbete mellan medlemsstaternas brottsbekämpande och rättsliga myndigheter. Denna åtgärd kommer att inledas i och med det expertmöte som skall hållas 2007 och kan leda till att det inrättas en central EU-kontaktpunkt för kampen mot IT-relaterad brottslighet.

- Ökat finansiellt stöd till initiativ för bättre utbildning för brottsbekämpande och rättsliga myndigheter när det gäller att handlägga IT-relaterade brott, samt åtgärder för att samordna alla multinationella utbildningsinsatser på detta område genom att inrätta ett europeiskt utbildningsforum.

- Främjande av ett mer beslutsamt åtagande från medlemsstaternas och alla offentliga myndigheters sida att vidta åtgärder mot IT-relaterad brottslighet och anslå tillräckliga resurser för kampen mot denna.

- Stöd till forskning som kan bidra till kampen mot IT-relaterad brottslighet.

- Anordnande av minst en stor konferens (2007) för brottsbekämpande myndigheter och privata aktörer, med det främsta syftet att inleda ett samarbete för bekämpning av olaglig Internetverksamhet inom eller mot elektroniska nät och att främja ett effektivare utbyte av icke-personrelaterade uppgifter, samt uppföljning av slutsatserna från konferensen i form av konkreta samarbetsprojekt mellan den offentliga och den privata sektorn.

- Initiativ till och deltagande i gemensamma åtgärder för den offentliga och den privata sektorn i syfte att öka medvetenheten – särskilt bland konsumenterna – om de kostnader och risker som IT-relaterad brottslighet medför, utan att för den skull undergräva konsumenternas och användarnas förtroende och tillit genom att lägga för stor vikt vid de negativa säkerhetsaspekterna.

- Aktivt deltagande i och främjande av ett övergripande internationellt samarbete för bekämpning av IT-relaterad brottslighet.

- Inledande av, bidrag till och stöd för internationella projekt som överensstämmer med kommissionens politik på detta område, t.ex. projekt under ledning av G8 som är förenliga med land- och regionstrategidokumenten (för samarbete med tredjeländer).

- Konkreta åtgärder för att uppmuntra alla medlemsstater och relevanta tredjeländer att ratificera Europarådets konvention om IT-relaterad brottslighet och dess tilläggsprotokoll samt för att undersöka möjligheterna för gemenskapen att ansluta sig till konventionen.

- Analys, i samarbete med medlemsstaterna, av fenomenet med samordnade och storskaliga angrepp mot medlemsstaters informationsinfrastruktur i syfte att förebygga och bekämpa sådana angrepp, bl.a. genom samordnade motåtgärder, och utbyta information och bästa metoder.

4.2. Kampen mot traditionell brottslighet inom elektroniska nät

- En ingående analys i syfte att utarbeta förslag till specifik EU-lagstiftning mot identitetsstöld.

- Främjande av utvecklingen av tekniska metoder och förfaranden för att bekämpa bedrägeri och olaglig handel på Internet, även genom samarbetsprojekt mellan den privata och den offentliga sektorn.

- Fortsatt arbete och vidareutveckling på specifika områden, t.ex. inom ramen för expertgruppen för förebyggande av bedrägerier när det gäller bekämpning av bedrägeri avseende andra betalningsmedel än kontanter i elektroniska nät.

4.3. Olagligt innehåll

- Vidareutveckling av åtgärder mot specifika typer av olagligt innehåll, särskilt barnpornografi och uppmaning till terrorism, bl.a. genom uppföljning av genomförandet av rambeslutet om bekämpande av sexuellt utnyttjande av barn och barnpornografi.

- Uppmaningar till medlemsstaterna att anslå tillräckliga finansiella medel åt att stärka brottsbekämpande myndigheters arbete. Särskild uppmärksamhet bör här ägnas åt att identifiera offren för barnpornografiskt material som sprids via Internet.

- Inledande av och stöd till åtgärder mot olagligt innehåll som kan påverka minderåriga att begå våldshandlingar eller andra allvarliga former av olagligt beteende, t.ex. vissa typer av extremt våldsamma nätbaserade videospel.

- Inledande och främjande av en dialog mellan medlemsstaterna och med tredjeländer om tekniska metoder att bekämpa olagligt innehåll och om förfaranden för att stänga olagliga webbplatser, eventuellt också med sikte på att ingå formella avtal med grannländer och andra länder om detta.

- Utarbetande av frivilliga avtal och överenskommelser mellan offentliga myndigheter och privata aktörer inom EU, särskilt Internetleverantörer, om förfaranden för att blockera och stänga olagliga webbsidor.

4.4. Uppföljning

I detta meddelande anges vilka åtgärder som bör vidtas härnäst i syfte att förbättra samarbetsstrukturerna inom EU. Kommissionen kommer att arbeta vidare med dessa åtgärder, utvärdera framstegen med genomförandet och rapportera till rådet och parlamentet.