EUROPA-KOMMISSIONEN

Bruxelles, den 28.3.2012
COM(2012) 140 final

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

Bekæmpelse af kriminalitet i den digitale tidsalder - Oprettelse af et europæisk center til bekæmpelse af it-kriminalitet

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

Bekæmpelse af kriminalitet i den digitale tidsalder - Oprettelse af et europæisk center til bekæmpelse af it-kriminalitet

1. INDLEDNING: EU'S REAKTION PÅ GRÆNSELØS KRIMINALITET

Internettet er blevet en integreret og nødvendig del af vores samfund og økonomi. Firs procent af de unge europæere er via sociale net på internettet[1] i kontakt med hinanden og resten af verden, og der bliver globalt omsat for ca. 8 bio. USD om året i internethandel[2]. En stadig større del af vores hverdagsliv og forretningstransaktioner finder sted på nettet, og det samme er tilfældet med de kriminelle aktiviteter, idet mere end én million mennesker verden over hver dag bliver ofre for it-kriminalitet[3]. It-kriminalitet går lige fra at sælge stjålne kreditkort for så lidt som én euro til identitetstyveri og seksuel udnyttelse af børn og til alvorlige internetangreb mod institutioner og infrastruktur.

De samlede omkostninger for samfundet som følge af it-kriminalitet er betydelige. I en nylig rapport skønnes det, at ofrene verden over mister ca. 388 mia. USD om året som følge af it-kriminalitet, hvilket gør det mere profitabelt end den samlede handel på verdensplan med marihuana, kokain og heroin tilsammen[4]. Selv om sådanne oplysninger bør behandles med forsigtighed, da der er forskellige måder at definere it-kriminalitet på, hvilket kan føre til varierende skøn over omkostningerne, er der dog enighed om, at it-kriminalitet er en meget profitabel form for lavrisikokriminalitet, der bliver stadig mere almindelig og skadelig. I en tid, hvor det er afgørende, at der skabes økonomisk vækst, vil det være vigtigt at optrappe bekæmpelsen af it-kriminalitet for at bevare borgernes og erhvervslivets tillid til sikkerheden ved kommunikation og handel på internettet. Det vil også understøtte vækstmålene i Europa 2020-strategien[5] og den digitale dagsorden for Europa[6].

Den digitale revolution de senere år skyldes først og fremmest friheden på internettet. På internettet findes der nemlig hverken nationale grænser eller en enkelt global kontrolinstans. Samtidig med at vi i henhold til EU's charter om grundlæggende rettigheder fremmer og beskytter friheden på internettet, må vi også stræbe efter at beskytte borgerne mod bander af organiserede kriminelle, der forsøger at udnytte denne åbenhed. Da der ikke findes nogen kriminalitet, der er så grænseløs som it-kriminalitet, er det nødvendigt, at de retshåndhævende myndigheder vedtager en strategi for koordinering og samarbejde på tværs af de nationale grænser sammen med både offentligheden og private aktører. Det er her, EU kan gøre en væsentlig forskel og også gør det.

---

1 Eurostat, Internet Access and Use, 14.12.2010.

2 McKinsey Global Institute, Internet Matters: the Net's sweeping impact on growth, jobs and prosperity. Rapport fra maj 2011, konsulteret den 8.2.2012.

3 Norton Cybercrime Report 2011, Symantec, 7.9.2011, konsulteret den 6.1.2012.

4 Ibid.

5 Europa 2020 - En strategi for intelligent, bæredygtig og inklusiv vækst (KOM(2010) 2020 af 3.3.2010).

6 En digital dagsorden for Europa (KOM(2010) 245 endelig af 26.8.2010).

Den Europæiske Union har udviklet forskellige initiativer for at bekæmpe it-kriminalitet, Direktivet fra 2011 om bekæmpelse af seksuel udnyttelse af børn på internettet og børnepornografi, og et direktiv om angreb på informationssystemer, hvori der fokuseres på at gøre udnyttelsen af værktøjer til it-kriminalitet strafbar, navnlig botnet[7], som forventes vedtaget i 2012. Europol har øget sine aktiviteter til bekæmpelse af it-kriminalitet og spillede en væsentlig rolle i forbindelse med den nylige "Operation Rescue", hvor politiet anholdte 184 mistænkte børnesexforbrydere og identificerede 200 ofre for misbrug af børn i en af de største efterforskninger af sin art med deltagelse af retshåndhævende myndigheder fra hele verden. Takket været Europols analytikeres arbejde med at knække sikkerhedselementerne i en af netværkets centrale computerservere, blev de mistænkte lovovertræderes identitet og aktiviteter afsløret.

Bekæmpelsen af it-kriminalitet, hvor det vigtigste retsinstrument er Europarådets konvention om internetkriminalitet[8], prioriteres fortsat meget højt. Bekæmpelse af it-kriminalitet indgår i EU's politikcyklus for organiseret og grov international kriminalitet[9] og udgør en integreret del af bestræbelserne for at udvikle en overordnet EU-strategi til styrkelse af internet-sikkerheden. EU har også indgået et tæt samarbejde med internationale partnere, f.eks. via løbende møder i EU's og USA's fælles arbejdsgruppe om internetsikkerhed og it-kriminalitet.

Hvis der ses bort fra disse fremskridt, er der stadig adskillige hindringer for at sikre en effektiv efterforskning af it-kriminalitet og retsforfølgelse på europæisk plan, bl.a. grænserne mellem de nationale jurisdiktioner, utilstrækkelig kapacitet til at dele efterretnings-oplysninger, tekniske problemer med at spore dem, der begår it-kriminalitet, uens kapacitet til efterforskning og kriminaltekniske undersøgelser, mangel på uddannet personale og et inkonsekvent samarbejde med andre berørte parter med ansvar for internetsikkerheden. Ved hjælp af stabilitetsinstrumentet forsøger EU også at bekæmpe de hurtigt voksende tværnationale trusler i forbindelse med it-kriminalitet i udviklings- og vækstlande, hvor den nødvendige kapacitet til bekæmpelse af denne form for organiseret kriminalitet ofte mangler.

For at tage disse udfordringer op har Kommissionen meldt ud, at den som prioriteret i strategien for EU's indre sikkerhed har til hensigt at oprette et europæisk center til bekæmpelse af it-kriminalitet[10]. Efter at Kommissionen på Rådets anmodning[11] har gennemført en feasibility-undersøgelse vedrørende oprettelsen af et sådant center[12], foreslår den, at der oprettes et europæisk center til bekæmpelse af it-kriminalitet (EC3), der skal være en del af Europol og fungere som knudepunkt for bekæmpelsen af it-kriminalitet i EU. I denne meddelelse, der bygger på feasibility-undersøgelsen, redegøres der for, hvilke kerne-

---

7 Forslag til Europa-Parlamentets og Rådets direktiv om angreb på informationssystemer (KOM(2010) 517 endelig af 30.9.2010). Botnet er net af computere, der er blevet inficeret af ondsindet software, som kan aktiveres på afstand, så de udfører nærmere bestemte handlinger, herunder it-angreb.

8 Europarådets konvention om it-kriminalitet, Budapest den 23.11.2001, også kendt som Budapestkonventionen. Konventionen ledsages af en tillægsprotokol vedrørende retsforfølgelse af it-aktiviteter, der udspringer af fremmedhad og racisme.

9 I EU's politikcyklus for organiseret og grov international kriminalitet, der dækker årene 2011-2013, er der otte prioriteter, hvoraf den ene er "optrapning af bekæmpelsen af it-kriminalitet og organiserede kriminelle gruppers kriminelle misbrug af internettet".

10 "I 2013 vil EU …….. oprette et center for it-kriminalitet, hvorigennem medlemsstaterne og EU-institutionerne vil kunne opbygge operationel og analytisk kapacitet til efterforskninger og samarbejde med internationale partnere", se Strategien for EU's indre sikkerhed i praksis – Fem skridt hen imod et mere sikkert EU (KOM(2010) 673 endelig af 22.11.2010).

11 Rådets konklusioner om en handlingplan til gennemførelse af den samordnede strategi for bekæmpelse af it-kriminalitet, 3010. samling i Rådet (almindelige anliggender), 26.4.2010.

12 Feasibility study for a European Cybercrime Centre, slutrapport, februar 2012.

funktioner centret skal have, og det forklares, hvorfor det bør placeres inden for rammerne af Europol, og hvordan det kan oprettes. Inden centret kan tages i brug, vil det imidlertid være nødvendigt yderligere at vurdere de ressourcemæssige konsekvenser. Oprettelsen af centret vil på passende vis blive afspejlet i den kommende revision af retsgrundlaget for Europol.

2. FORSLAG OM OPRETTELSE AF ET EUROPÆISK CENTER TIL BEKÆMPELSE AF IT-KRIMINALITET

For at centret kan give en merværdi, samtidig med at der tages hensyn til nærhedsprincippet, foreslås det, at det fokuserer på følgende typer it-kriminalitet:

i) It-kriminalitet, der begås af organiserede grupper, navnlig de typer it-kriminalitet, der giver store ulovlige fortjenester såsom internetbedrageri.

ii) It-kriminalitet, der forårsager alvorlige skader for ofrene såsom seksuel udnyttelse af børn på internettet.

iii) It-kriminalitet (herunder it-angreb), der påvirker infrastruktur og informationssystemer i EU[13].

Da it-kriminalitet hele tiden udvikler sig, bør der også være mulighed for at træffe foranstaltninger som reaktion på medlemsstaternes behov og til at tackle de nye trusler, it-kriminalitet skaber i EU.

2.1. Centrets kernefunktioner og -opgaver

Centret skal have fire kernefunktioner:

a) Tjene som et europæisk knudepunkt for information om it-kriminalitet

Ved at lade centret fungere som et informationsknudepunkt sikres det, at der indsamles oplysninger om it-kriminalitet fra omfattende offentlige, private og åbne kilder for derved at supplere politiets disponible oplysninger. Det skal gradvis lukke de nuværende huller i de foreliggende oplysninger fra de myndigheder, der er ansvarlige for internetsikkerheden og bekæmpelsen af it-kriminalitet. De indsamlede oplysninger skal vedrøre aktiviteter og metoder inden for it-kriminalitet og mistænkte it-kriminelle. De skal være med til at forbedre kendskabet til it-kriminalitet og til at forhindre, opdage og retsforfølge it-kriminalitet, samt til at fremme hensigtsmæssige kontakter mellem retshåndhævende myndigheder, CERT (Computer Emergency Response Team – it-udrykningshold) og specialister inden for informationsteknologisikkerhed i den private sektor. Ved informationsudvekslingen er det nødvendigt, at de aftaler og regler vedrørende fortrolighed, parterne er enedes om, respekteres.

Centrets funktion som informationsknudepunkt er også nyttig, når det drejer sig om at forbedre rapporteringen af it-kriminalitet og informationsudvekslingen. Kommissionen ønsker, at medlemsstaterne gør det obligatorisk, at alvorlig it-kriminalitet rapporteres til de retshåndhævende myndigheder[14]. Det vil gøre det muligt for det nationale politi mere

---

[13] Som defineret i Rådets direktiv 2008/114/EF af 8. december 2008, som på nuværende tidspunkt er ved at blive ændret. Der vil i forbindelse med oprettelsen af centret blive taget hensyn hertil.

[14] F.eks. af den type, der er omhandlet i artikel 3-7 i det fremlagte udkast til direktiv om angreb på informationssystemer (KOM(2010) 517 endelig af 30.9.2010).

konsekvent at fremlægge oplysninger om alvorlig it-kriminalitet for centret, som kan videreformidle dem, således at kolleger i andre medlemsstater, som måske arbejder mod samme mål, kan få kendskab til dem og drage nytte af andres oplysninger i efterforskningen.

Formålet er at forbedre informationsbilledet af it-kriminalitet i Europa over tid, således at der kan udarbejdes strategiske rapporter af høj kvalitet om tendenser og trusler for at øge kendskabet hertil på grundlag af et omfattende talmateriale over kriminalitet, og den operationelle efterretningsaktivitet kan forbedres på grundlag af en database, der bygger på en række kilder.

b) Samle europæisk ekspertise om it-kriminalitet for at hjælpe medlemsstaterne med deres kapacitetsopbygning

Centret for bekæmpelse af it-kriminalitet skal bistå medlemsstaterne med ekspertise og uddannelse for at dæmme op for it-kriminaliteten. Hovedfokus skal være på retshåndhævelse, men aktørerne inden for retsvæsenet bør også tilbydes uddannelse. De eksisterende initiativer fra Europol, CEPOL og medlemsstaterne skal strømlines, efter at der er foretaget en grundig behovsanalyse for at sikre en bedre koordinering og større komplementaritet. Dette uddannelsestiltag skal gå lige fra tilbundsgående teknisk ekspertise til bredere kapacitets-opbygning for politibetjente, anklagere og dommere for at forbedre deres evne til at behandle sager om it-kriminalitet.

Der skal oprettes et kontaktpunkt vedrørende it-kriminalitet med henblik på udveksling af bedste praksis og viden og for at samarbejde med og besvare forespørgsler fra medlemsstaternes og internationale retshåndhævende myndigheder, retsvæsenet, den private sektor og organisationer i civilsamfundet, f.eks. i tilfælde af internetangreb eller nye former for internetsvindel.

Det skal støtte aktiviteterne i ekspertgrupper vedrørende internetkriminalitet og rådgive dem, herunder EU's taskforce vedrørende it-kriminalitet og eksperter i bekæmpelse af seksuel udnyttelse af børn på nettet. Det skal desuden samarbejde om udviklingen af net af ekspertisecentre inden for it-kriminalitet, f.eks. 2Centre, og forskersamfundet.

Centret skal også bistå medlemsstaterne i deres bestræbelser for at udvikle og anvende et system til rapportering af it-kriminalitet på nettet, der er baseret på aftalte standarder, for at videregive rapporteringer fra en række aktører (virksomheder, nationale/statslige it-udrykningsteam, borgere m.fl.) til de nationale retshåndhævende myndigheder og fra sidstnævnte til centret for bekæmpelse af it-kriminalitet.

Centret skal bidrage til og lette udvekslingen af bedste praksis på området strafferet og retshåndhævelse. Det er afgørende, at retsvæsenet effektivt inddrages i bekæmpelsen af it-kriminalitet for derved at forbedre retsforfølgelsen af bagmændene bag grov it-kriminalitet i medlemsstaterne.

c) Yde støtte til medlemsstaternes efterforskning af it-kriminalitet

Centret for bekæmpelse af it-kriminalitet skal yde operationel støtte til efterforskningen af it-kriminalitet, f.eks. ved at fremme oprettelsen af fælles efterforskningsteam inden for it-kriminalitet og udvekslingen af operationelle oplysninger om igangværende undersøgelser.

Det bør også yde kriminalteknisk bistand på højt niveau (faciliteter, lagring, redskaber) og krypteringsekspertise for efterforskning af it-kriminalitet.

d) Blive talerør for europæiske efterforskere inden for it-kriminalitet på området retshåndhævelse og inden for retsvæsenet

Centret for bekæmpelse af it-kriminalitet kan over tid komme til at fungere som et knudepunkt for europæiske efterforskere inden for it-kriminalitet ved at blive talerør for dem i drøftelser med virksomheder inden for informations- og kommunikationsteknologisektoren og andre virksomheder i den private sektor samt forskersamfundet, brugersammenslutninger og organisationer i civilsamfundet om, hvordan it-kriminalitet bedre kan forebygges, og hvordan målrettede forskningsaktiviteter kan koordineres.

Centret skal være en naturlig grænseflade for Interpols aktiviteter på området it-kriminalitet og andre internationale politienheder på samme område. Det kan også koordinere bidrag til igangværende initiativer vedrørende forvaltning af internettet og FN's åbne mellemstatslige ekspertgruppe vedrørende it-kriminalitet.

Centret skal desuden samarbejde med organisationer såsom INSAFE[15] om gennemførelse af offentlige bevidstgørelseskampagner og ajourføringen af dem som følge af ændringer i den type it-kriminalitet, som centrets analyser har identificeret med henblik på at fremme en forsigtig og sikker adfærd på internettet.

2.2. Placering

Som det fremgår af feasibility-undersøgelsen bør Det Europæiske Center til Bekæmpelse af It-Kriminalitet være en del af Europol og placeres i dets eksisterende faciliteter.

Dette har en række fordele: Europol spiller en rolle, som medlemsstaterne og andre berørte parter anerkender, herunder Interpol og internationale retshåndhævende myndigheder, og har allerede mandat til at tage fat på it-kriminalitet[16]. Europols kernefunktion er at bistå med at skabe et mere sikkert Europa til gavn for alle borgere ved at støtte de retshåndhævende myndigheder i EU gennem udveksling og analyse af strafferetlige efterretningsoplysninger.

2.3. Ressourcemæssige konsekvenser

I feasibility-undersøgelsen blev der set nærmere på forskellige ressourcemæssige konsekvenser af at oprette centret. Det vil være nødvendigt at vurdere dette yderligere[17], navnlig i lyset af de øvrige opgaver, Europol skal udføre fremover og mere generelt på baggrund af bemandingen af EU-agenturerne. Vurderingen vil navnlig blive foretaget i forbindelse med revisionen af retsgrundlaget for Europol og den igangværende drøftelse af Kommissionens forslag til en fond for intern sikkerhed. Det er dog allerede tydeligt, at det vil være nødvendigt med udstationeringer fra medlemsstaterne.

Ved vurderingen af de skønnede ressourcer, der er nødvendige, er der tre forhold, Kommissionen skal tage med i sine overvejelser: For det første forventes det, at der vil ske en moderat og ikke en massiv stigning i det samlede antal sager om it-kriminalitet, for det andet

---

15 Europæisk net af oplysningscentre, der fremmer en sikker og ansvarlig brug af internettet og mobiludstyr blandt unge.

16 Rådets afgørelse (2009/371/RIA) af 6. april 2009 om oprettelse af Den Europæiske Politienhed (Europol), artikel 4, stk. 1, sammenholdt med bilaget.

17 Vurderingen skal være kohærent med de overordnede bemandings- og budgetmæssige krav for agenturer i budgettet for 2013 og den næste flerårige finansielle ramme.

vil medlemsstaterne øge deres egen kapacitet til at bekæmpe it-kriminalitet, og for det tredje vil centret for bekæmpelse af it-kriminalitet kun tage sig af bestemte typer it-kriminalitet.

2.4. Forvaltning

Da centret for bekæmpelse af it-kriminalitet skal placeres inden for rammerne af Europol, er det vigtigt at sikre, at de øvrige berørte parter deltager i den strategiske ledelse af centret. Kommissionen foreslår derfor, at der oprettes et programråd for centret inden for rammerne af Europols forvaltningsstruktur, hvis formand er centrets leder. Dette instrument vil give andre berørte parter såsom Eurojust, CEPOL, medlemsstaterne (via deres repræsentanter i EU's taskforce vedrørende it-kriminalitet), ENISA og Kommissionen mulighed for at komme med deres respektive knowhow, uden at det skaber en unødig administrativ byrde. Programrådet kan sørge for, at centret på ansvarlig vis udfører sine aktiviteter og derved sikrer, at de udføres i partnerskab, idet alle berørte parters yderligere ekspertise anerkendes og deres mandat respekteres.

2.5. Samarbejde med vigtige aktører

Centret for bekæmpelse af it-kriminalitet skal koordinere bekæmpelsen af it-kriminalitet og ikke blot muliggøre et samarbejde mellem EU-agenturer, men også fungere som et fælles europæisk kontaktpunkt på dette område.

a) Medlemsstaterne

Hovedformålet er at bistå medlemsstaterne med at bekæmpe it-kriminalitet. Centrets helpdesk for it-kriminalitet og de forventede resultater, f.eks. en mere nøjagtig trusselsanalyse og operationel støtte baseret på flere oplysninger, vil være til gavn for efterforskere på området it-kriminalitet i hele Europa. EU's taskforce for internetkriminalitet skal sikre, at medlemsstaterne via deres repræsentanter kan komme til orde i programrådet. Derudover vil det være nødvendigt, at medlemsstaterne fortsat foretager de nødvendige investeringer i deres nationale strukturer til bekæmpelse af it-kriminalitet, således at de har passende samarbejdsflader med centret.

b) EU-agenturer og andre aktører

De relevante agenturer, navnlig Eurojust, CEPOL og ENISA, samt CERT-EU skal direkte involveres i centrets aktiviteter, ikke blot via deres deltagelse i programrådet, men også via et operationelt samarbejde, når det er relevant og under hensyntagen til deres respektive mandater.

c) Internationale partnere

Centret for bekæmpelse af it-kriminalitet skal stræbe efter at blive et europæisk informations-knudepunkt vedrørende it-kriminalitet og en nyttig samarbejdspartner for internationale partnere på området bekæmpelse af it-kriminalitet. Centret skal i partnerskab med Interpol og vores strategiske partnere rundt omkring i verden stræbe efter at finde bedre og mere koordinerede løsninger i forbindelse med bekæmpelsen af it-kriminalitet og sikre, at der tages hensyn til forhold omkring de retshåndhævende myndigheders indsats ved den videre udvikling af internettet.

d) Den private sektor, forskersamfund og organisationer i civilsamfundet

Det er meget vigtigt at opbygge tilliden mellem den private sektor og de retshåndhævende myndigheder i forbindelse med bekæmpelse af it-kriminalitet. Centret for bekæmpelse af it-kriminalitet skal konsolidere Europols arbejde med eksisterende og nye partnere og etablere pålidelige net og informationsudvekslingsplatforme med erhvervslivet og andre aktører såsom forskersamfundet og organisationer i civilsamfundet. De skal lette informationsudvekslingen mellem de forskellige parter om en lang række spørgsmål, herunder tidlig varsling om internettrusler og fælles løsninger på internetangreb og andre former for it-kriminalitet, der findes på "taskforcemæssig" vis.

Centret skal også bidrage til den bredere indsats, som virksomheder i den private sektor, der har omfattende digitale aktiver, f.eks. banker eller onlinebutikker, gør for at bekæmpe og i højere grad beskytte sig mod it-kriminalitet og gøre ny teknologi mindre sårbar.

Det er i såvel de retshåndhævendes som den private sektors gensidige interesse at få et bedre realtidsbillede af it-kriminalitetstruslen og stræbe efter at sikre en mere effektiv opløsning af net af it-kriminelle ved i højere grad at afsløre, hvordan de fungerer, og hurtigt arrestere dem.

3. EN KØREPLAN FOR OPRETTELSEN AF DET EUROPÆISKE CENTER TIL BEKÆMPELSE AF IT-KRIMINALITET

3.1. Aktiviteter frem til udgangen af 2013

For i første omgang at sikre centrets driftskapacitet vil Kommissionen i tæt samarbejde med Europol undersøge, hvad der er brug for af menneskelige og økonomiske ressourcer for at nedsætte et implementeringsteam frem til udgangen af EU's nuværende finansielle ramme. Dette team kan f.eks. få til opgave at udarbejde centrets kommissorium og organisatoriske struktur og udvikle indikatorer til vurdering af, hvordan det fungerer. Programrådets rolle og funktion vil blive yderligere defineret og vedtaget af de tilknyttede berørte parter.

Med henblik på at få centret til at fungere som et fuldstændigt informationsknudepunkt skal centrets implementeringsteam skabe forbindelser til EU's it-udrykningsteam samt ENISA, når det er relevant (under hensyntagen til deres begrænsede ressourcer). Med henblik på at forbedre rapporteringen af it-kriminalitet vil der blive foretaget en kortlægning heraf for derved at skabe et interoperabelt kort over eksisterende onlinesystemer for rapportering af it-kriminalitet i medlemsstaterne.

Der skal oprettes et kontaktpunkt vedrørende it-kriminalitet. Det skal understøttes af en særlig, sikker onlineplatform for de pågældende parter. De nuværende aktiviteter i Europol, CEPOL og den europæiske gruppe for uddannelse på it-kriminalitetsområdet (ECTEG) kan i koordinering med centret for bekæmpelse af it-kriminalitet og dets programråd vurderes og strømlines. Der skal gennemføres en analyse af uddannelsesbehovene, hvori der også tages hensyn til dommeres og anklageres krav. Med udgangspunkt i denne analyse kan der tilbydes grundlæggende uddannelseskurser vedrørende it-kriminalitet, der er åbne for aktører inden for strafferetssystemet.

Det vil endvidere være nødvendigt med en mere præcis vurdering af de nødvendige menneskelige og økonomiske ressourcer som fastsat i afgørelserne inden for rammerne af den næste flerårige finansielle ramme. Vurderingen vil indgå i den videre udvikling af centret til bekæmpelse af it-kriminalitet.

4. KONKLUSION

Da den organiserede kriminalitet spreder sine aktiviteter ud på internettet, er det nødvendigt at de retshåndhævende myndigheder kan følge trop. EU kan sikre medlemsstaterne og erhvervslivet egnede redskaber til at tackle it-kriminalitet, som udgør en moderne og stadig større trussel, der pr. definition er grænseløs. Hvis de nødvendige menneskelige og økonomiske ressourcer kan sikres, vil et europæisk center til bekæmpelse af it-kriminalitet komme til at fungere som knudepunkt i Europas bekæmpelse af it-kriminalitet ved at samle ekspertisen, støtte de strafferetlige efterforskninger og fremme løsninger på EU-plan, samtidig med at kendskabet til spørgsmål vedrørende it-kriminalitet øges i hele EU. Centret vil som sådan bidrage til at sikre et åbent internet og en lovlig digital økonomi og til at beskytte borgere og erhvervslivet i forbindelse med aktiviteter på nettet.

Rådet opfordres til at godkende dette forslag, og Europa-Parlamentet og andre relevante berørte parter opfordres til at bidrage til udviklingen af centret.