Sisäasiainministeriö E-KIRJELMÄ SM2007-00479

Kartila Marja 04.10.2007

Eduskunta
Suuri valiokunta

Viite

Asia
EU/OSA; Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi (komission tiedonanto tietoverkkorikollisuudesta)

U/E-tunnus:EUTORI-numero:

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys, joka koskee komission tiedonantoa neuvostolle, Euroopan parlamentille ja alueiden komitealle tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi.

Poliisiylitarkastaja Marja Kartila

LIITTEET SM2007-00392, 10089/07 Crimorg 102 ja ADD 2 suomeksi ja ruotsiksi sekä ADD 1 englanniksi

Asiasanat	oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, STM, TH, TM, VM, VNEUS

Sisäasiainministeriö EU-OHJE SM2007-00392

Kartila Marja 27.08.2007

Asia
EU/OSA; komission tiedonanto tietoverkkorikollisuudesta

Kokous

Liitteet Viite

EUTORI/Eurodoc nro:

U-tunnus / E-tunnus:

Käsittelyn tarkoitus ja käsittelyvaihe:

Tiedonanto esiteltiin artikla 36 komitean kokouksessa 18.7.2007. Seuraavaksi asiaa käsitellään neuvoston työryhmässä sekä Euroopan neuvoston ja artikla 36 komitean yhteiskokouksessa kuluvan vuoden marraskuussa.

Asiakirjat:

10089/07 CRIMORG 102 + ADD 1 ja ADD 2

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

Käsittelijä(t):

Marja Kartila/SM p. 160 42850
Lena Andersson/OM p. 1606 7725
Mari Herranen/LVM p. 160 28305

Suomen kanta/ohje:

Suomi pitää tiedonantoa hyvin valmisteltuna ja riittävän laaja-alaisena. Suomi hyväksyy siinä esitetyt eri näkökohdat tietoverkkorikollisuuden aiheuttamista uhista ja ne toimenpide-ehdotukset, joiden avulla tietoverkkorikollisuutta tulee torjua.

Suomen mukaan lainvalvontaviranomaisten rajat ylittävä operatiivinen yhteistyö vaatii tehostamista. Osittain tämä voidaan toteuttaa komission ehdottamalla tavalla tehostamalla nykyisten kanavien

käyttöä ja koordinoimalla paremmin yhteistyötä Euroopan tasolla. Tiedonannossa mainitut mahdolliset lainsäädäntöä koskevat uudistukset voivat myös osaltaan tehostaa lainvalvontayhteistyötä.

Suomessa on tähän mennessä jo ryhdytty toimenpiteisiin tiedonannossa esitettyjen toimenpiteiden kohdalla, jotka koskevat yhteistyötä elinkeinoelämän kanssa sekä tilastojen kehittämistä (kts. jäljempänä Muut mahdolliset asiaan vaikuttavat seikat).

Suomi yhtyy siihen tiedonannon näkemykseen, että komission tulisi selvittää, tarvitaanko lainsäädäntöä erityisesti tilanteessa, jossa kyseessä on väärän henkilöllisyyden käyttö. Komission on syytä selvittää, missä maassa väärän henkilöllisyyden pelkkä käyttö (tunnusluvut, sähköiset tunnisteet jne) hyötymistarkoituksessa on jo nykyisin maksuliikenteen tai sähköisen kaupankäynnin yhteydessä rangaistavaa ja missä maissa ei. Lisäksi tulisi pyrkiä selvittämään se, missä muissa kuin kaupankäyntiin tai maksuliikenteeseen liittyvissä yhteyksissä väärää henkilöllisyyttä voidaan pyrkiä hyödyntämään.

Suomi katsoo myös, että kaikkien EU:n jäsenmaiden tulisi ratifioida Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus, kuten komissio ehdottaa. Suomessa sopimus tuli voimaan 1.9.2007. Tämän lisäksi tulevaisuudessa olisi syytä soveltaa tehokkaammin myös YK:n järjestäytyneen rikollisuuden vastaista yleissopimusta, jotta järjestäytyneeseen verkkorikollisuuteen voitaisiin vaikuttaa globaalisti. YK:n sopimus täydentää käytettävissä olevaa sopimusverkostoa tarjoten maailmanlaajuisen yhteistyöjärjestelmän, joka sisältää määräyksiä kansainvälisestä, viranomaisten välisestä keskinäisestä tiedonvaihdosta.

Pääasiallinen sisältö:

1. Johdanto

1.1. Mitä tietoverkkorikollisuus on?

Tiedonannossa termillä tietoverkkorikollisuus tarkoitetaan rikollista toimintaa, joka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai rikoksia, jotka kohdistuvat näihin verkkoihin tai järjestelmiin. Tietoverkkorikollisuus voidaan jakaa kolmeen eri ryhmään: perinteinen rikostyyppi (petos tai väärennys), sähköisen viestimen laiton sisältö (esim. lapsipornografia) ja itse sähköisiin verkkoihin kohdistuva rikos (palvelunesto ja hakkerointi). Viimeksi mainitut rikokset voivat olla suunnattuja kohti Euroopan elintärkeää infrastruktuuria aiheuttaen tuhoisia seurauksia koko yhteiskunnalle. Yhteistä kaikille rikostyypeille on, että ne voidaan tehdä laajassa mittakaavassa ja rikoksen ja sen vaikutusten välinen maantieteellinen etäisyys voi olla suuri. Mainittujen rikosten tutkinnassa käytettävät tekniikat ovat usein samoja ja nämä yhteiset piirteet ovat tiedonannon keskeinen aihe.

1.2. Viimeaikaiset kehityspiirteet tietoverkkorikollisuudessa

Tietoverkkorikollisuuden tämänhetkisestä tilanteesta on vaikea saada tarkkaa kuvaa, sillä rikollinen toiminta muuttuu jatkuvasti eikä luotettavia tietoja ole olemassa. Joitakin kehityssuuntauksia voidaan erotella: tietoverkkorikollisuus lisääntyy koko ajan ja muuttuu kehittyneemmäksi ja kansainvälisemmäksi, järjestäytyneiden rikollisryhmien on todettu sotkeutuneen tietoverkkorikollisuuteen ja lisäksi on todettu, että syytteiden määrä Euroopan tasolla ei ole noussut.

1.2.2. Perinteiset rikokset

Useat perinteiset rikokset (petos ja petoksen yritys) voidaan tehdä käyttäen sähköistä verkkoa. Laajamittaista petollista toimintaa voidaan harjoittaa muun muassa identiteettivarkauden, phishingin ja

spamien avulla. Myös laajentunut internet-kauppa aiheuttaa kasvavaa ongelmaa (huumekauppa, uhanalaiset lajit ja aseet).

1.2.3. Laiton sisältö

verkkosivustojen laittomaan sisältöön on erittäin vaikea puuttua lainvalvonnan keinoin, koska sivujen omistajat ja hallinnoijat ovat usein muussa maassa kuin kohdevaltiossa, usein myös EU:n ulkopuolella. Tiedostot voidaan siirtää nopeasti, minkä lisäksi laittomana sisällön määritelmä vaihtelee valtiosta toiseen.

1.2.4. Sähköiseen verkkoon kohdistuvat rikokset

Laajamittaiset hyökkäykset tietojärjestelmiä, organisaatioita tai yksityishenkilöitä vastaan ovat nykyään hyvin yleisiä. Myös systemaattisia, hyvin järjestettyjä ja laajamittaisia hyökkäyksiä valtioiden elintärkeää infrastruktuuria vastaan on havaittu viimeaikoina, järjestelmän haavoittuvuuden vuoksi. Teknologian yhdenmukaistuminen ja tietojärjestelmien yhä etenevä yhteen liittäminen aiheuttaa haavoittuvuutta. Hyökkäyksistä ei aina raportoida viranomaisille.

1.3. Tavoitteet

Yksilöiden suojaaminen tietoverkkorikollisuutta vastaan on hankaloitunut ja se on johtunut ongelmista, jotka liittyvät toimivaltaisen valtion määrittelyyn, sovellettavan lain valintaan, lainvalvontaviranomaisten rajat ylittävään toimintaan ja vastavuoroiseen tunnustamiseen sekä sähköisen todisteluaineiston arviointiin. Tietoverkkorikollisuuden rajat ylittävän luonteen vuoksi nämä ongelmat korostuvat. Komissio haluaa lanseerata yleisen poliittisen aloitteen parantaakseen eurooppalaista ja kansainvälistä koordinaatiota tietoverkkorikollisuuden vastustamisessa. Painopiste tulee olemaan lainvalvontatyössä ja rikosoikeudellisessa työssä ja politiikan tarkoitus on täydentää muita EU-tason toimenpiteitä. Toimenpiteet sisältävät muun muassa yhteistyö kolmansien maiden kanssa, tietoisuuden herättäminen, koulutus sekä vahvistettu dialogi teollisuuden kanssa.

Toimenpiteet tullaan toteuttamaan kunnioittaen perusoikeuksia, erityisesti ilmaisuvapaus, yksityisyyden suoja ja henkilötietosuoja. Mahdolliset lainsäädäntöaloitteet arvioidaan Perusoikeuskirjan määräykset ja sähköistä kaupankäyntiä koskevat säännökset huomioiden.

Tämän tiedonannon tavoite voidaan jakaa kolmeen operatiiviseen osaan seuraavasti:

- parantaa ja helpottaa tietoverkkorikoksia tutkivien yksiköiden, muiden relevanttien viranomaisten ja muiden asiantuntijoiden välistä koordinaatiota ja yhteistyötä.
- kehittää yhtenäinen tietoverkkorikollisuutta vastustavaa EU-politiikan puitteistoa EU:n jäsenmaiden, EU:n ja muiden kansainvälisten järjestöjen ja osallisten kesken.
- lisätä tietoisuutta tietoverkkorikollisuuden aiheuttamista kustannuksista ja vaaroista.

2. Olemassa olevat lainsäädäntöinstrumentit tietoverkkorikollisuutta vastaan

2.1. EU:n säädökset ja toimet

Tiedonannossa on lueteltu olemassa olevat EU-tason ja kansainväliset lainsäädäntöinstrumentit. Tiedonanto täydentää vuonna 2001 annettua tiedonantoa *Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä*, jonka johdosta tehtiin useita aloitteita. Muun muassa puitepäätös 2005/222/JHA, joka koskee tietojärjestelmiin kohdistuvia iskuja, perustuu em. tiedonantoon. Puitepäätös 2004/68/JHA, joka koskee lasten

seksuaalista hyväksikäyttöä, on hyvä esimerkki horisontaalisesta välineestä, joka kieltää kaikenlaisen lasten seksuaalista hyväksikäyttöä koskevan materiaalin julkaisemisen käyttäen tietojärjestelmiä.

Komissio on kehittänyt kolmiosaisen lähestymistavan verkkojen ja tietojen turvaamiseksi: erityiset suojaamismenetelmät, lainsäädännölliset toimet ja verkko ja tietoturvallisuuteen: verkko- ja tietoturvallisuutta koskevat erityistoimenpiteet, sähköisen viestinnän sääntelypuitteet ja tietoverkkorikollisuuden torjunta. Kaikkia näitä voidaan kehittää toisistaan erillään, mutta tietyt riippuvuustekijät edellyttävät tiivistä koordinointia. Esimerkiksi vuonna 2001 laadittiin sekä tietoverkkorikollisuutta koskeva tiedonanto että verkostoa ja tietoturvallisuutta koskeva tiedonanto. Vuonna 2004 perustettiin Asetuksen (EY) N:o 460/2004:n nojalla ENISA (=European Network and Information Security Agency, Euroopan verkko- ja tietoturvavirasto). Sen tarkoituksena on tehostaa julkisen ja yksityisen sektorin välistä yhteistyötä sekä antaa apua komissiolle ja jäsenmaille. EU:n seitsemäs tutkimusta koskeva puiteohjelma vuosille 2007-2013 sisältää tietoa ja tiedonvaihtoa sekä tietoturvallisuutta koskevan osion.

2.2. Kansainväliset sopimukset

Tietoverkkorikollisuutta vastustavat toimenpiteet eivät voi rajoittua vain EU:n sisään. Komissio on osallistunut aktiivisesti mm. G8-maiden työhön ja Interpolin asianomaisiin projekteihin. Merkittävin eurooppalainen ja kansainvälinen instrumentti on Euroopan neuvoston piirissä tehty tietoverkkorikollisuutta koskeva yleissopimus. Sopimus, joka astui voimaan vuonna 2004, sisältää yhteiset määritelmät useille tietoverkkorikollisuuden muodoille ja velvoittaa oikeusviranomaiset keskinäiseen yhteistyöhön. Sopimuksen ovat kaikkien EU:n jäsenmaiden lisäksi allekirjoittaneet USA ja useita Euroopan ulkopuolisia maita. Useat EU:n jäsenmaat eivät ole vielä ratifioineet sopimusta tai sen lisäpöytäkirjaa, joka koskee tietojärjestelmien avulla tehtyjen rasististen ja muukalaisvastaisten rikosten säätämistä rangaistaviksi teoiksi. Komissio rohkaisee jäsenmaita ratifiointiin ja harkitsee Euroopan yhteisön mahdollisuuksia liittyä sopimukseen.

3. Eräiden tietoverkkorikollisuutta koskevien instrumenttien edelleen kehittäminen

3.1. Lainvalvontaviranomaisten operatiivisen yhteistyön vahvistaminen ja EU:n yhteiset koulutushankkeet

Suurin heikkous on nopean rajat ylittävän operatiivisen yhteistyön rakenteen puute tai sen vajavainen käyttö. Perinteinen keskinäinen avunanto on liian hidas menettelytapa tietoverkkorikollisuusjutuissa eikä uutta yhteistyörakennetta ole vielä riittävästi kehitetty. Erityisesti tulee tutkia sitä, miten Europolia, Eurojustia ja muita rakenteita voitaisiin hyödyntää tehokkaammin ja tarkentaa niiden välisiä vastuita. Koordinoidumman eurooppalaisen lähestymistavan tulee olla sekä operatiivinen että strateginen sekä kattaa myös tiedonvaihdon ja parhaat käytänteet.

Komissio tulee jatkossa painottamaan koulutusta. Sen tulee olla jatkuvaa, koska teknologia kehittyy ja muuttuu jatkuvasti. Koulutusta koskevaan rahoitukseen tullaan kiinnittämään huomiota ja EU-tason koordinaatio Europolin, Eurojustin, CEPOLin ja EJNT:n välillä tulee toteuttaa.

Komissio tulee järjestämän jäsenmaiden lainvalvonta-asiantuntijoille sekä Europolin, CEPOLin ja EJNT:n edustajille kokouksen, jossa pohditaan, miten voidaan parantaa strategista ja operatiivista yhteistyötä sekä tehostaa koulutusta. Myös erityisten yhteyspisteiden perustamista harkitaan. Tämä kokous on yksi siitä kokoussarjasta, joka tulevaisuudessa järjestetään.

3.2. Tehostetaan vuoropuhelua elinkeinoelämän kanssa

Sekä julkisella että yksityisellä sektorilla on yhteinen intressi kehittää keinoja, joilla voidaan torjua rikollista toimintaa. Dialogi yksityisen ja julkisen sektorin välillä on osa EU politiikkaa. Piakkoin perustettava Eurooppalainen turvallisuuden tutkimus- ja innovaatiofoorumi tulee kokoamaan relevantit osapuolet kummaltakin puolelta. Yksityiset operaattorit ovat merkittävä tekijä uhka-arviointien tekemisessä, rikoksentorjunnan vastaisten ohjelmien laatimisessa ja teknisten ratkaisujen kehittämisessä rikoksentorjuntaa varten. Yksityisen ja julkisen sektorin välistä tietojen, asiantuntemuksen ja parhaiden käytänteiden vaihtoa tulee parantaa. Yksityinen sektori ei aina ole halukas tai sillä ei ole lakimääräistä velvollisuutta ilmoittaa rikoksista. Yritysten motiivina on liiketoimintamallien ja -salaisuuksien suojeleminen. Tietojenvaihdon parantamisen yhteydessä tulee ottaa huomioon tietosuojasäännökset.

Komissio järjestää vuoden 2007 aikana konferenssin julkiselle ja yksityiselle sektorille, erityisesti Internet- palvelujen tarjoajille, jossa voidaan pohtia yhteistyön parantamiskeinoja. Konferenssin aiheita ovat: yhteistyön parantaminen (erityinen terrorismi, lasten seksuaalinen hyväksikäyttö ja muut lasten suojelua koskevat asiat), aloite julkisen ja yksityisen sektorin väliselle yhteistyölle, joka koskee laittomien sivujen sulkemista, tietojenvaihdon parantaminen ja yhteyspisteverkoston luominen.

3.3. Lainsäädäntö

Jäsenvaltioiden lainsäädäntöjen harmonisointi ei ole ajankohtainen johtuen hyvin erilaisesta säätelystä jäsenmaissa. Harmonisointi on pitkän aikavälin tavoite. Keskeisimpien rikosten yhtenäinen määrittely on hoidettu puitepäätöksessä, joka koskee hyökkäyksiä tietojärjestelmiä vastaan. Kehittyvien rikostrendien seuranta on hoidettu eurooppalaisessa ohjelmassa elintärkeän infrastruktuurin suojelusta.

Lainsäädäntöä saatetaan kuitenkin tarvita erityisesti tilanteissa, jossa tietoverkkorikollisuuteen liittyy väärän henkilöllisyyden käyttö. Tällä tarkoitetaan tilanteita, joissa toisen henkilön yksityisiä tietoja käytetään luvatta muiden rikosten tekemiseen. Useissa jäsenvaltioissa väärän henkilöllisyyden käyttö rangaistaan usein petoksena tai se ei ole rangaistavaa lainkaan. Yhtäläinen lainsäädäntö jäsenmaissa helpottaisi lainvalvontaviranomaisten välistä yhteistyötä. Komissio aloittaa vuonna 2007 kuulemisen siitä, onko yhtäläinen lainsäädäntö tältä osin tarpeen.

3.4. Tilastotietojen kehittäminen

Yhtäläiset tilastot ovat olennaisia tietojen vertailukelpoisuuden kannalta. Tätä asiaa käsittelee komission 5-vuotinen, kattava ja koherentti EU-strategia rikosten ja rikollisuuden mittaamisesta vuosille 2006-2010, joka perustuu vuonna 2006 annettuun tiedonantoon.

4. Jatkotoimet

4.1. Tietoverkkorikollisuuden torjunta

Operatiivisen yhteistyön parantaminen lainvalvonta- ja oikeusviranomaisten välillä, joka aloitetaan vuonna 2007 asiantuntijakokouksella sekä perustetaan mahdollisesti tietoverkkorikollisuutta koskeva EU:n yhteyspiste. Tietoverkkorikollisuuden vastaista työtä tuetaan rahoitusohjelmilla. Jäsenvaltioiden tulee sitoutua tietoverkkorikollisuuden vastustamiseen ja antaa lainvalvontaviranomaisille riittävät resurssit. Ilmiötä tulee tutkia myös tieteellisesti. Vuonna 2007 järjestetään lainvalvontaviranomaisten ja yksityisen sektorin konferenssi, jonka konkluusioiden pohjalta laaditaan yhteistyöprojekti. Yleistä tietoisuutta tietoverkkorikollisuudesta parannetaan. Osallistutaan globaaliin yhteistyöhön ja tuetaan muita kansainvälisiä projekteja, jotka ovat yhdenmukaisia komission ehdotusten kanssa (esim. G8). Jäsenmaita rohkaistaan ratifioimaan Euroopan neuvoston tietoverkkorikollisuuden vastainen

yleissopimus sekä harkitaan yhteisön liittymistä siihen. Tutkitaan koordinoituja ja laajamittaisia hyökkäyksiä jäsenvaltioiden tietoinfrastruktuuria vastaan niiden vastustamiseksi, tietojen jakamiseksi ja parhaiden käytäntöjen jakamiseksi.

4.2. Perinteiset rikokset sähköisissä verkoissa

Väärän henkilöllisyyden käytön osalta komissio selvittää erityisen EU-lainsäädännön tarpeen. Edistetään teknisten metodien ja prosessien kehittämistä, joiden avulla tietoverkkorikoksia estetään. Työtä erityisalueilla jatketaan, kuten esimerkiksi petostenvastainen työryhmä, joka käsittelee muiden maksuvälineiden kuin käteisrahan välityksellä sähköisissä verkoissa tapahtuvien petosten ehkäisemiseksi.

4.3. Laiton sisältö

Jatketaan terrorismirikosten ja lasten seksuaalista hyväksikäyttöä koskevien rikosten vastaisia toimia. Jäsenmaiden tulisi antaa tarvittavat resurssit lainvalvontaviranomaisten työhön. Nuoria vahingoittavaa laitonta materiaalia sisältäviä, kuten esim. väkivaltaiset videopelit, sivuja tulee vastustaa. Kolmansien maiden kanssa käytävää dialogia laittomasta sisällöstä ja sivujen sulkemisesta tulee kehittää. Vapaaehtoisia sopimuksia julkisen ja yksityisen sektorin välillä mm. sivujen sulkemisesta tulee kehittää.

4.4. Seuranta

Tiedonannon useat toimenpiteet yhteistyörakenteen parantamiseksi ovat seuraava askel. Komissio vie toimenpiteitä eteenpäin, seuraa niiden toteutumista ja raportoi neuvostolle ja Euroopan parlamentille.

Asiakirjat ADD 1 ja ADD 2 sisältävät vaikuttavuusarvioinnin ja sen yhteenvedon:

Asiakirjoissa suositellaan ryhdyttäväksi laatimaan yleistä tietoverkkorikollisuuden vastaista ohjelmaa.

Kansallinen käsittely:

EU-6 11.9.2007.

Eduskuntakäsittely:

Käsittely Euroopan parlamentissa:

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

Rikoslain 38. luku sisältää tietoverkkorikoksia koskevia säännöksiä: tässä luvussa säädetään muun muassa viestintäsalaisuuden loukkauksesta, tietoliikenteen häirinnästä, tietomurrosta sekä suojauksen purkujärjestelmärikoksesta. Rikoslain 34 luvussa säädetään rangaistavaksi vaaran aiheuttaminen tietojärjestelmälle ja tietoverkkorikosvälineen hallussapito. Rikoslain 35 luvun 1 §:n 2 momentissa kriminalisoidaan (tieto)vahingonteko. Maksuvälinepetoksena säädetään rangaistavaksi rikoslain 37 luvussa maksuvälineen käyttö ilman sen laillisen haltijan lupaa.

Maksuvälineellä tarkoitetaan myös PIN-koodeja, tunnuslukuja, salasanoja ja sähköiseen kaupankäyntiin tarkoitettuja sähköisiä tunnisteita (HE 38/1997 vp s. 5/I), joiden luvaton käyttö taloudellisen hyödyn hankkimiseksi on säännöksen nojalla rangaistavaa.

Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen määräykset ovat tulleet voimaan Suomessa 1.9.2007. Tässä yhteydessä rikoslaki saatettiin vastaamaan EU:n puitepäätöstä tietojärjestelmiin kohdistuvista hyökkäyksistä, koska puitepäätös sisältää määräyksiä samoista asioista kuin yleissopimus. Rikoslakiin lisättiin uudet tietojärjestelmän häirintää, tietoverkkorikosvälineen hallussapitoa sekä törkeää tietomurtoa koskevat rangaistussäännökset. Pakkokeinolain 4 lukuun lisättiin uusi säännös, joka koskee datan säilyttämismääräystä, jolla turvataan datan säilyminen muuttamattomana rikostutkintaa varten.

Taloudelliset vaikutukset:

Taloudellisia vaikutuksia ei voida tässä vaiheessa arvioida, koska komissio ei ole vielä antanut asiaa koskevia ehdotuksia.

Muut mahdolliset asiaan vaikuttavat tekijät:

Suomessa on kiinnitetty jo aiemmin huomiota tiedonannon kohteisiin 2. (vuoropuhelu elinkeinoelämän kanssa) ja 4. (tilastotietojen kehittäminen):

Menestyksellinen suojautuminen rikoksilta edellyttää realistista uhka-arviota. Yhteistyö yritysten kanssa on tärkeää, sillä poliisin hallussa oleva tieto voi olla edesauttaa yritysten suojautumista uusilta rikosilmiöiltä. Toisaalta yritykset pystyvät havaitsemaan hallitsemissaan verkoissa rikosilmiöitä, jotka eivät muuten tulisi poliisin tietoon. Yhteistyö julkisen ja yksityisen sektorin välillä perustuu vuonna 2003 hyväksyttyyn valtioneuvoston periaatepäätökseen kansallisesta tietoturvastrategiasta. Sisäasiainministeriö on asettanut vuonna 2005 yhteistyössä oikeusministeriön, Elinkeinoelämän keskusliiton ja Keskuskauppakamarin kanssa kansallisen yhteistyöryhmän yritysturvallisuuden parantamiseksi. Yhteistyöryhmän puitteissa laadittiin Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi, joka kattaa myös tietoverkkorikostorjunnan toimenpiteitä.

Verkkorikollisuus on mitä suurimmassa määrin piilorikollisuutta: Verkkorikoksen havaitsevat asianomistajat eivät useinkaan ilmoita siitä poliisille. Toisaalta asianomistaja itse ei välttämättä edes havaitse rikosta. Tilastointiteknisistä syistä poliisilla ei ole ollut ilmoitettujenkaan rikosten osalta tarkkaa jatkuvaa kuvaa tietoverkkorikoksista. Keskusrikospoliisi ryhtyy selvittämään syksyllä 2007 tilannekuvan tuottamista verkon ajankohtaisista rikosilmiöistä. Lähteinä tullaan käyttämään poliisin järjestelmiä, muilta viranomaisilta saatua rikostiedustelutietoa että avoimista lähteistä saatavaa tietoa, jota poliisi pystyy jalostamaan rikosilmiöiden näkökulmasta.

Asiasanat	oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, STM, TH, TM, VM, VNEUS

EUROOPAN UNIONIN NEUVOSTO

Bryssel, 30. toukokuuta 2007 (02.07)
(OR. en)

10089/07

CRIMORG 102

SAATE

Lähettäjä:	Euroopan komission pääsihteerin puolesta Jordi AYET PUIGARNAU, johtaja
Saapunut:	24. toukokuuta 2007
Vastaanottaja:	Javier SOLANA, pääsihteeri, korkea edustaja
Asia:	Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle – Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi

Valtuuskunnille toimitetaan oheisena komission asiakirja – KOM(2007) 267 lopullinen

Liite: KOM(2007) 267 lopullinen

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 22.5.2007
KOM(2007) 267 lopullinen

KOMISSION TIEDONANTO NEUVOSTOLLE, EUROOPAN PARLAMENTILLE JA ALUEIDEN KOMITEALLE

Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi

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

KOMISSION TIEDONANTO
NEUVOSTOLLE, EUROOPAN PARLAMENTILLE
JA ALUEIDEN KOMITEALLE

Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi

1. JOHDANTO

1.1. Mitä tietoverkkorikollisuus on?

Nyky-yhteiskunnassa yhä tärkeämmäksi muuttuvien tietojärjestelmien turvallisuuteen liittyy useita kysymyksiä, joista keskeisimpiä on tietoverkkorikollisuuden torjunta. Koska tietoverkkorikollisuudelle ei ole sovittu yhteistä määritelmää, ’tietoverkkorikollisuutta’, ’tietokonerikollisuutta’ sekä ’huipputeknologiaa käyttävää rikollisuutta’ käytetään usein samassa merkityksessä. Tässä tiedonannossa tietoverkkorikollisuudella tarkoitetaan rikoksia, jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin.

Käytännössä tietoverkkorikollisuus voidaan jakaa kolmeen alaryhmään. Ensimmäinen ryhmä kattaa **perinteiset rikollisuuden muodot**, kuten petokset ja väärentämisen. Tietoverkkorikollisuuden yhteydessä tähän kuuluvat erityisesti rikokset, jotka on tehty käyttäen sähköisiä viestintäverkkoja ja tietojärjestelmiä (’sähköiset verkot’). Toiseen ryhmään kuuluu **laittoman sisällön** (mm. lapsen seksuaalista hyväksikäyttöä esittävän tai rotuvihaan yllyttävän materiaalin) julkaiseminen sähköisissä viestimissä. Kolmas ryhmä käsittää **rikokset, joita esiintyy ainoastaan sähköisissä verkoissa**, kuten hyökkäykset tietojärjestelmiä vastaan, palvelunesto ja hakkerointi. Tämäntyyppiset hyökkäykset saattavat kohdistua myös elintärkeisiin eurooppalaisiin infrastruktuureihin ja vaikuttaa nopeisiin hälytysjärjestelmiin monilla aloilla, millä voi olla katastrofaaliset seuraukset koko yhteiskunnan kannalta. Kaikille edellä mainituille rikostyypeille on yhteistä se, että rikoksia voidaan tehdä laajassa mittakaavassa ja että itse rikoksen ja sen vaikutusten välinen maantieteellinen etäisyys voi olla suuri. Sen vuoksi kaikkien mainittujen rikosten tutkinnassa käytetään usein samanlaisia teknisiä menetelmiä. Nämä yhteiset piirteet ovat tiedonannon keskeinen aihe.

1.2. Tietoverkkorikollisuuden viimeaikainen kehitys

1.2.1. Yleistä

Tietoverkkorikollisuuden tämänhetkisestä tilanteesta on vaikea saada tarkkaa kuvaa, sillä rikollisten toiminta muuttuu jatkuvasti ja toisaalta luotettavia tietoja ei ole riittävästi saatavilla. Joitakin yleisiä kehityssuuntauksia voidaan kuitenkin hahmotella:

- Tietoverkkorikollisuus lisääntyy jatkuvasti, ja rikollisten toiminta on yhä kehittyneempää ja samalla kansainvälisempää.[1]

- Selvät todisteet viittaavat siihen, että tietoverkkorikollisuudessa on yhä useammin mukana järjestäytyneitä rikollisryhmiä.

- Lainvalvontaviranomaisten rajat ylittävään yhteistyöhön perustuvien syytetoimien määrä ei kuitenkaan lisäänny Euroopassa.

1.2.2. Perinteinen rikollisuus sähköisissä verkoissa

Useimmat rikokset on mahdollista tehdä sähköisiä verkkoja hyödyntäen. Erityisen yleisiä ovat erityyppiset petokset ja niiden yritykset. Esimerkiksi väärän henkilöllisyyden käyttöä, phishing-hyökkäyksiä[2], roskapostia ja haittaohjelmia voidaan hyödyntää suurimittaisissa petoksissa. Kasvavan ongelman muodostaa myös esimerkiksi huumausaineiden, uhanalaisten eläinten ja aseiden laiton kansallinen ja kansainvälinen kauppa Internetin välityksellä.

1.2.3. Laiton sisältö

Euroopassa on yhä enemmän verkkosivustoja, jotka käsittävät laitonta sisältöä, kuten lasten seksuaalista hyväksikäyttöä, tai kannustavat terroritekoihin tai ihannoivat väkivaltaa, terrorismia, rasismia ja muukalaisvihaa. Tällaisiin sivustoihin on erittäin vaikea puuttua lainvalvonnan keinoin, sillä sivustojen omistajat ja ylläpitäjät ovat usein sijoittautuneet muualle kuin kohdemaihin, monesti myös EU:n ulkopuolelle. Lisäksi sivustoja voidaan siirtää hyvin nopeasti, myös EU:n ulkopuolelle, ja toisaalta laittoman sisällön määritelmä vaihtelee huomattavasti valtiosta toiseen.

1.2.4. Ainoastaan sähköisissä verkoissa tapahtuvat rikokset

Laajamittaiset hyökkäykset tietojärjestelmiä tai organisaatioita ja yksityishenkilöitä vastaan (usein botnet-verkkojen[3] välityksellä) ovat nykyään hyvin yleisiä. Lisäksi viime aikoina on havaittu järjestelmällisiä, koordinoituja ja laajamittaisia hyökkäyksiä, jotka kohdistuvat suoraan valtioiden kriittisiin tietoinfrastruktuureihin. Ongelmia on pahentanut teknologian yhdenmukaistuminen ja tietojärjestelmien yhä enenevä yhteen liittäminen, mikä tekee niistä entistä haavoittuvampia. Hyökkäykset ovat usein hyvin suunniteltuja, ja niiden tarkoituksena on kiristää rahaa. Hyökkäyksistä raportoidaan viranomaisille todennäköisesti hyvin harvoin, osittain siksi että turvallisuusongelmien julkitulosta saattaisi olla yrityksille haittaa.

---

[1] Suurin osa tietoverkkorikollisuuden kehityssuuntauksia koskevista tiedoista on peräisin komission vuonna 2006 tilaamasta tutkimuksesta *Study to assess the impact of a communication on cyber crime* (sopimus nro JLS/2006/A1/003).

[2] Phishing tarkoittaa yritystä hankkia laittomasti henkilökohtaisia tietoja, kuten salasanoja ja luottokorttitietoja, esiintymällä sähköisessä viestintätapahtumassa luotettavana henkilönä.

[3] Botnet tarkoittaa useiden kaapattujen tietokoneiden verkkoa, joka voidaan yhdellä komennolla ohjata suorittamaan tiettyjä ohjelmia.

1.3. Tavoitteet

Muuttuvat olosuhteet edellyttävät nopeaa toimintaa sekä jäsenvaltioiden että Euroopan tasolla kaikenlaisen tietoverkkorikollisuuden torjumiseksi, sillä kyseiset rikokset muodostavat yhä suuremman uhan kriittisille infrastruktuureille, yhteiskunnalle, liike-elämälle ja kansalaisille. Yksilöiden suojelemista tietoverkkorikollisuudelta hankaloittavat usein seikat, jotka liittyvät toimivaltaisen tuomioistuimen määrittämiseen, sovellettavaan lainsäädäntöön, lainvalvontaviranomaisten rajatylittävään toimintaan sekä sähköisen todistusaineiston keräämiseen ja hyödyntämiseen. Nämä vaikeudet korostuvat sen takia, että tietoverkkorikollisuus on luonteeltaan olennaisesti rajat ylittävää. Ratkaistakseen ongelmat komissio käynnistää aloitteen, jonka tarkoituksena on parantaa tietoverkkorikollisuuden torjunnan koordinaatiota Euroopan ja kansainvälisellä tasolla.

Aloitteella pyritään tietoverkkorikollisuuden torjunnan vahvistamiseen jäsenvaltioiden, Euroopan ja kansainvälisellä tasolla. Jäsenvaltiot ja komissio ovat todenneet jo kauan sitten, että on ensiarvoisen tärkeää kehittää EU:lle oma toimintalinja tietoverkkorikollisuuden torjumiseksi. Aloitteessa keskitytään tietoverkkorikollisuuden torjunnan lainvalvonta- ja rikosoikeudellisiin näkökohtiin, ja sillä täydennetään muita EU:n toimia, joilla pyritään parantamaan yleisesti turvallisuutta kyberavaruudessa. EU:n yleisen toimintalinjan on tarkoitus käsittää seuraavanlaisia toimia: käytännön lainvalvontayhteistyön parantaminen, jäsenvaltioiden poliittisen yhteistyön ja koordinaation tehostaminen, poliittinen ja oikeudellinen yhteistyö EU:n ulkopuolisten maiden kanssa, tiedottaminen, koulutus ja tutkimus, vuoropuhelun tehostaminen elinkeinoelämän kanssa sekä mahdolliset säädösaloitteet.

Tietoverkkorikollisuuden torjuntaa ja syytteeseenpanoa koskeva yleinen toimintalinja määritellään ja pannaan täytäntöön perusoikeuksia ja erityisesti sananvapautta, yksityis- ja perhe-elämää sekä henkilötietojen suojaa kunnioittaen. Jos toimintalinjan yhteydessä tehdään säädösaloitteita, on ensin tutkittava, että ne vastaavat mainittuja oikeuksia ja ovat sopusoinnussa erityisesti Euroopan unionin perusoikeuskirjan kanssa. Lisäksi on huomattava, että kaikki aloitteet pannaan täytäntöön sähköistä kaupankäyntiä koskevan direktiivin[4] 12–15 artiklan mukaisesti, niiltä osin kuin kyseistä säädöstä sovelletaan.

Tiedonannon tavoite voidaan jakaa kolmeen keskeiseen toimintalohkoon, jotka voidaan tiivistää seuraavasti:

- parannetaan ja edistetään koordinointia ja yhteistyötä tietoverkkorikollisuutta tutkivien yksiköiden sekä muiden viranomaisten ja asiantuntijoiden kesken EU:ssa

- kehitetään EU:lle yhtenäiset poliittiset puitteet tietoverkkorikollisuuden torjunnalle yhteistyössä jäsenvaltioiden, asianomaisten EU:n elinten, kansainvälisten organisaatioiden ja muiden sidosryhmien kanssa

- tiedotetaan tietoverkkorikollisuuden aiheuttamista kustannuksista ja siihen liittyvistä vaaroista.

---

[4] Euroopan parlamentin ja neuvoston direktiivi 2000/31/EY, annettu 8 päivänä kesäkuuta 2000, tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista (EYVL L 178, 17.7.2000, s. 1).

2. TIETOVERKKORIKOLLISUUDEN TORJUNTAA KOSKEVAT SÄÄDÖKSET

2.1. EU:n säädökset ja toimet

Tässä tietoverkkorikollisuutta koskevassa tiedonannossa lujitetaan ja kehitetään edelleen vuonna 2001 annettua tiedonantoa *Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä*[5] ('vuoden 2001 tiedonanto'). Vuoden 2001 tiedonannossa ehdotetaan asiasisältöä ja menettelyjä koskevia asianmukaisia säännöksiä, joilla pyritään torjumaan sekä valtioiden sisällä että niiden välillä tapahtuvaa rikollisuutta. Tiedonannon pohjalta on tehty useita tärkeitä säädösaloitteita, kuten puitepäätös 2005/222/YOS[6] tietojärjestelmiin kohdistuvista hyökkäyksistä. Tässä yhteydessä on huomattava, että lisäksi on annettu muuta, yleisluonteisempaa lainsäädäntöä, joka liittyy tietyltä osin tietoverkkorikollisuuden torjuntaan, kuten puitepäätös 2001/413/YOS[7] muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta.

Neuvoston puitepäätös 2004/68/YOS[8] lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta kuvastaa hyvin sitä, että komissio on asettanut etusijalle lasten suojelun ja pyrkii estämään kaikenlaisen lasten seksuaalista hyväksikäyttöä koskevan aineiston julkaisemisen tietojärjestelmissä. Tämä horisontaalinen tavoite säilyy keskeisellä sijalla myös tulevaisuudessa.

Euroopan yhteisö on kehittänyt tietoyhteiskuntaan kohdistuvien turvallisuushaasteiden ratkaisemiseksi kolmiosaisen lähestymistavan verkko- ja tietoturvallisuuteen: verkko- ja tietoturvallisuutta koskevat erityistoimenpiteet, sähköisen viestinnän sääntelypuitteet ja tietoverkkorikollisuuden torjunta. Vaikka näitä kolmea lähestymistapaa voidaan myös kehitellä erikseen, ne liittyvät siinä määrin toisiinsa, että toiminta edellyttää läheistä koordinointia. Komissio julkaisi vuonna 2001 verkko- ja tietoturvallisuutta koskevan tiedonannon *Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi*[9] samanaikaisesti tietokonerikollisuutta koskevan tiedonannon kanssa. Sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY velvoitetaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat huolehtimaan palvelujen turvallisuudesta. Lisäksi direktiivi käsittää säännöksiä, joissa kielletään roskaposti ja vakoiluohjelmat. Verkko- ja tietoturvallisuuden alalla on sen jälkeen toteutettu useita toimia, joista viimeisimpiä ovat tiedonanto *Turvallisen tietoyhteiskunnan strategia*[10], jossa esitellään uudistettu strategia ja määritetään puitteet verkko- ja tietoturvallisuutta koskevan yhdenmukaisen lähestymistavan kehittämiseksi ja määrittämiseksi, tiedonanto *Roskapostin sekä vakoilu- ja haittaohjelmien torjunta*[11] sekä Euroopan verkko- ja tietoturvaviraston perustaminen[12] vuonna 2004. Euroopan verkko- ja tietoturvaviraston keskeinen tavoite on kehittää asiantuntemusta, tehostaa yhteistyötä julkisen ja yksityisen sektorin välillä sekä tukea komissiota ja jäsenvaltioita. Tärkeä merkitys tietoverkkorikollisuuden torjunnassa on lisäksi **tutkimustuloksilla**, joita saadaan turvallisten tietojärjestelmien teknologisen kehittämisen

---

5 KOM(2000) 890, 26.1.2001.
6 EUVL L 69, 16.3.2005, s. 67.
7 EYVL L 149, 2.6.2001, s. 1.
8 EUVL L 13, 20.1.2004, s. 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Asetus (EY) N:o 460/2004 Euroopan verkko- ja tietoturvaviraston perustamisesta (EUVL L 77, 13.3.2004, s. 1).

alalla. Tieto- ja viestintäteknologiat sekä turvallisuus onkin määritelty EU:n seitsemännen tutkimuksen puiteohjelman tavoitteiksi. Ohjelmaa sovelletaan vuosina 2007–2013[13]. Sähköisen viestinnän sääntelypuitteiden tarkistaminen saattaa johtaa siihen, että sähköisen viestinnän tietosuojadirektiivin ja yleispalveludirektiivin 2002/22/EY[14] niitä säännöksiä, jotka liittyvät turvallisuuteen, muutetaan turvallisuuden parantamiseksi.

2.2. Kansainväliset sopimukset

Koska tietoverkot ovat maailmanlaajuisia, tietoverkkorikollisuutta koskeva toimintapolitiikka ei voi olla tehokasta, jos toimet rajoittuvat pelkästään EU:n alueelle. Paitsi että rikolliset voivat hyökätä tietojärjestelmiä vastaan tai tehdä rikoksia jossakin jäsenvaltiossa toisesta jäsenvaltiosta käsin, rikollista toimintaa on helppo harjoittaa myös EU:n toimivalta-alueen ulkopuolelta. Sen vuoksi komissio on ollut aktiivisesti mukana asiaa käsittelevissä kansainvälisissä neuvotteluissa ja yhteistyöhankkeissa, kuten G8-maiden perustamassa ympärivuorokautisessa tietoverkostossa huipputeknologiaan liittyvän rikollisuuden torjumiseksi (*G8 Lyon-Roma High-Tech Crime Group*) ja Interpolin johtamissa projekteissa. Komissio seuraa erityisen tarkasti huipputeknologiaa hyödyntävän kansainvälisen rikollisuuden tutkintaan erikoistuneita tahoja varten luodun 24-tuntisen jokapäiväisen verkoston[15] toimintaa. Verkostoon kuuluu useita maita ympäri maailman. Myös useimmat EU:n jäsenvaltiot ovat verkoston jäseniä. G8-maiden perustama tietoverkosto puolestaan antaa osanottajavaltioille mahdollisuuden luoda keskinäinen yhteys ympärivuorokautisten yhteyspisteiden välityksellä asioissa, joihin liittyy sähköistä todistusaineistoa tai joissa tarvitaan pikaisesti muiden maiden lainvalvontaviranomaisten apua.

Tärkein eurooppalainen ja kansainvälinen väline tietoverkkorikollisuuden torjunnassa lienee vuonna 2001 tehty tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus[16]. Vuonna 2004 hyväksytyssä ja voimaan tulleessa yleissopimuksessa esitetään tietoverkkorikollisuuden eri lajien yhteiset määritelmät ja luodaan perusta sopimusvaltioiden väliselle toimivalle oikeudelliselle yhteistyölle. Yleissopimuksen ovat allekirjoittaneet useat maat, esimerkiksi Yhdysvallat sekä moni muu Euroopan ulkopuolinen maa. Myös kaikki EU:n jäsenvaltiot ovat allekirjoittaneet yleissopimuksen. Sen sijaan kaikki jäsenvaltiot eivät ole vielä ratifioineet yleissopimusta tai sen lisäpöytäkirjaa, joka koskee tietojärjestelmien avulla tehtyjen rasististen ja muukalaisvastaisten rikosten säätämistä rangaistaviksi teoiksi. Koska yleissopimus on merkittävä asiakirja, komissio aikoo kannustaa jäsenvaltioita ja tiettyjä EU:n ulkopuolisia maita ratifioimaan yleissopimuksen ja harkitsee Euroopan yhteisön liittymistä yleissopimukseen.

---

13 Euroopan unioni on tukenut useita tärkeitä ja onnistuneita tutkimushankkeita jo kuudennesta tutkimuksen ja teknologian kehittämisen puiteohjelmasta.

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

15 Katso tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen 35 artikla.

16 Http://conventions.coe.int/treaty/en/treaties/html/185.htm.

3. ERÄIDEN TIETOVERKKORIKOLLISUUDEN TORJUNTAA KOSKEVIEN VÄLINEIDEN KEHITTÄMINEN

3.1. Lainvalvontaviranomaisten operatiivisen yhteistyön vahvistaminen ja EU:n yhteiset koulutushankkeet

Suurimpia puutteita vapauden, turvallisuuden ja oikeuden alueella on se, ettei käytössä ole rakenteita, jotka mahdollistaisivat nopean **rajatylittävän operatiivisen yhteistyön**, tai jos onkin, niitä ei hyödynnetä riittävästi. Perinteinen keskinäinen avunanto on osoittautunut nopeaa toimintaa vaativan tietoverkkorikollisuuden kohdalla liian hitaaksi ja tehottomaksi keinoksi, eikä uusia yhteistyöjärjestelyjä ole vielä kehitetty riittävästi. Vaikka jäsenvaltioiden oikeus- ja lainvalvontaviranomaiset tekevät läheistä yhteistyötä Europolin, Eurojustin ja muiden organisaatioiden puitteissa, on EU:ssa selvästi tarvetta vahvistaa ja selkeyttää vastuualueita. Komission selvitysten perusteella vaikuttaa siltä, ettei olemassa olevia kanavia hyödynnetä parhaalla mahdollisella tavalla. Euroopassa tarvitaan paremmin koordinoitua lähestymistapaa, jonka on oltava sekä operatiivinen että strateginen ja lisäksi käsitettävä tietojen ja parhaiden käytänteiden vaihtaminen.

Komissio aikoo lähitulevaisuudessa korostaa erityisesti **koulutuksen** tarvetta. On todettu, että teknologian kehitys edellyttää lainvalvonta- ja oikeusviranomaisten jatkuvaa kouluttautumista tietoverkkorikollisuutta käsittelevissä aiheissa. Sen takia EU:n aikookin lisätä taloudellista tukeaan monikansallisille koulutusohjelmille ja koordinoida tukea aiempaa tehokkaammin. Lisäksi komissio pyrkii yhteistyössä jäsenvaltioiden ja muiden toimivaltaisten tahojen, kuten Europolin, Eurojustin, Euroopan poliisiakatemian (CEPOL) ja Euroopan juridisen koulutusverkoston (EJNT) kanssa koordinoimaan ja sovittamaan yhteen EU:n tasolla kaikkia keskeisiä koulutusohjelmia.

Komissio aikoo järjestää vuonna 2007 jäsenvaltioiden, Europolin, CEPOLin ja EJNT:n lainvalvonta-asiantuntijoiden **kokouksen**, jossa on määrä keskustella strategisen ja operatiivisen yhteistyön sekä tietoverkkorikollisuutta koskevan koulutuksen parantamisesta Euroopassa. Asialistalla ovat muun muassa EU:n pysyvän yhteyspisteen luominen tietojenvaihtoa varten ja tietoverkkorikollisuutta koskevan EU:n koulutusfoorumin perustaminen. Vuoden 2007 kokous aloittaa useiden lähitulevaisuudessa järjestettävien tapaamisten sarjan.

3.2. Tehostetaan vuoropuhelua elinkeinoelämän kanssa

Sekä yksityinen että julkinen sektori hyötyvät siitä, että ne kehittävät yhdessä menetelmiä rikollisuuden aiheuttamien haittojen tunnistamiseksi ja ehkäisemiseksi. Yksityisen ja julkisen sektorin yhteistyö, joka perustuu molemminpuoliseen luottamukseen ja yhteiseen tavoitteeseen eli haittojen vähentämiseen, vaikuttaa tehokkaalta keinolta lisätä turvallisuutta, myös tietoverkkorikollisuuden torjunnassa. Tietoverkkorikollisuutta koskevan komission toimintapolitiikan osat, jotka liittyvät julkisen ja yksityisen sektorin suhteisiin, on aikanaan tarkoitus sisällyttää suunnitteilla olevaan julkisen ja yksityisen sektorin vuoropuhelua koskevaan EU:n politiikkaan, joka kattaa koko Euroopan turvallisuustilanteen. Kyseistä politiikkaa on tarkoitus kehitellä erityisesti turvallisuusalaa koskevassa eurooppalaisessa tutkimus- ja innovointifoorumissa, jonka komissio aikoo käynnistää piakkoin ja johon odotetaan mukaan keskeisiä toimijoita julkiselta ja yksityiseltä sektorilta.

Modernin informaatioteknologian ja sähköisten viestintäjärjestelmien kehittäminen on pääasiassa yksityisten toimijoiden vastuulla. Yksityiset yritykset suorittavat uhkien arviointia, luovat rikostentorjuntaohjelmia ja kehittävät teknisiä ratkaisuja rikollisuuden ehkäisemiseksi. Elinkeinoelämä on suhtautunut hyvin myönteisesti viranomaisten avustamiseen tietoverkkorikollisuuden torjunnassa, varsinkin lapsipornografian[17] ja muun Internetissä olevan laittoman sisällön kohdalla.

Toinen ongelma liittyy siihen, että julkinen ja yksityinen sektori eivät vaihda keskenään tietoja, asiantuntemusta ja parhaita käytänteitä. Julkisen sektorin toimijat ovat usein haluttomia ilmoittamaan lainvalvontaviranomaisille rikoksista, eikä laki myöskään selkeästi velvoita niitä tähän. Yritysten motiivina on liiketoimintamallien ja -salaisuuksien suojeleminen. Tiedot voivat kuitenkin olla tarpeen, jotta viranomaiset voivat toteuttaa tehokasta ja asianmukaista rikostentorjuntapolitiikkaa. Kun harkitaan mahdollisuuksia parantaa tietojen vaihtoa yksityisen ja julkisen sektorin välillä, on lisäksi otettava huomioon henkilötietojen suojaa koskevat säännöt.

Komissio on keskeisessä asemassa erilaisissa tietoverkkorikollisuuteen liittyvissä julkisen ja yksityisen sektorin yhteistyöjärjestelyissä, kuten petostentorjunnan asiantuntijaryhmässä[18]. Komissio on vakuuttunut siitä, että tietoverkkorikollisuuden torjuntaa koskevaan tehokkaaseen toimintapolitiikkaan on sisällyttävä julkisen ja yksityisen sektorin yhteistyöstrategia, joka kattaa myös kansalaisjärjestöt.

Varmistaakseen julkisen ja yksityisen sektorin laaja-alaisen yhteistyön komissio aikoo järjestää vuonna 2007 lainvalvonta-alan asiantuntijoiden ja julkisen sektorin edustajien, erityisesti Internet-palveluntarjoajien konferenssin, jossa keskustellaan keinoista parantaa julkisen ja yksityisen sektorin välistä käytännön yhteistyötä Euroopassa.[19] Konferenssissa käsitellään kaikkia aiheita, jotka voivat tuoda lisäarvoa julkiselle ja yksityiselle sektorille. Asialistalla ovat erityisesti seuraavat toimet:

- Parannetaan käytännön yhteistyötä Internetin välityksellä tapahtuvien rikosten ja Internetissä levitettävän laittoman sisällön torjumiseksi erityisesti terrorismin, lasten seksuaalista hyväksikäyttöä esittävän materiaalin ja muiden erityisesti lastensuojelun kannalta erityisen haitallisten rikosten osalta.

- Pyritään aikaansaamaan julkisen ja yksityisen sektorin välisiä sopimuksia, joiden tavoitteena on sulkea laitonta aineistoa ja erityisesti lasten seksuaalista hyväksikäyttöä koskevaa materiaalia sisältävät sivustot EU:n alueella.

- Luodaan eurooppalainen malli tarpeellisten ja tärkeiden tietojen jakamiseksi yksityisen ja julkisen sektorin kesken molemminpuolisen luottamuksen ilmapiirissä ja kaikkia osapuolia hyödyttäen.

- Luodaan verkosto, joka käsittää julkisen ja yksityisen sektorin lainvalvonnasta vastaavat yhteyspisteet.

---

17 Tuore esimerkki alan yhteistyöstä on lainvalvontaviranomaisten ja luottokorttiyhtiöiden yhteistyöhanke, jossa yhtiöt auttoivat poliisia jäljittämään Internetin kautta lapsipornoa hankkivia henkilöitä.

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

19 Konferenssin voidaan katsoa olevan jatkoa tietokonerikollisuutta koskevan tiedonannon 6.4 kohdassa mainitulle EU:n keskustelufoorumille.

3.3. Lainsäädäntö

Tietoverkkorikollisuuteen liittyvien rikosten määritelmien ja kansallisten rikoslainsäädäntöjen yhtenäistäminen ei ole vielä toistaiseksi tarkoituksenmukaista, sillä tietoverkkorikollisuus kattaa hyvin monentyyppisiä rikoksia. Koska lainvalvontaviranomaisten tehokas yhteistyö kuitenkin edellyttää usein ainakin jossain määrin yhtenäisiä rikosten määritelmiä, on jäsenvaltioiden lainsäädännön yhtenäistäminen pitkän aikavälin tavoite[20]. Eräiden keskeisten rikosten määrittelyssä tapahtui merkittävää edistystä, kun puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä hyväksyttiin. Kuten edellä on kuvattu, tietoverkkorikollisuuden alalla on sittemmin ilmestynyt uusia uhkia, joiden kehittymistä komissio seuraa tarkasti voidakseen arvioida, tarvitaanko uusia säädösaloitteita. Uusien uhkien seuranta on sovitettava yhteen Euroopan elintärkeiden infrastruktuureiden suojaamisohjelman kanssa.

Nyt olisi kuitenkin oikea aika harkita myös lainsäädäntöä, joka kohdistuu nimenomaan tietoverkkorikollisuuteen. Lainsäädäntöä saatetaan tarvita erityisesti tilanteessa, jossa tietoverkkorikollisuuteen liittyy **väärän henkilöllisyyden käyttö**. Tällä tarkoitetaan yleensä sitä, että toisen henkilön yksityisiä tietoja, kuten luottokortin numeroa, käytetään luvatta muiden rikosten tekemiseen. Useimmissa jäsenvaltioissa rikollinen asetettaisiin tällaisessa tapauksessa todennäköisesti syytteeseen petoksesta tai jostakin muusta rikoksesta eikä väärän henkilöllisyyden käytöstä, sillä edellistä pidetään vakavampana rikoksena. Väärän henkilöllisyyden käyttöä ei ole edes määritelty rikokseksi kaikissa jäsenvaltioissa. Usein on kuitenkin helpompi näyttää toteen väärän henkilöllisyyden käyttö kuin petos, joten EU:n lainvalvontayhteistyön kannalta olisi parempi, jos väärän henkilöllisyyden käyttö määriteltäisiin rikokseksi kaikissa jäsenvaltioissa. Komissio käynnistää vuonna 2007 kuulemisen arvioidakseen, tarvitaanko asiassa lainsäädäntöä.

3.4. Tilastotietojen kehittäminen

Kaikki tahot tunnustavat yleisesti, että rikollisuuden yleisyydestä ei ole tällä hetkellä saatavilla riittävästi tietoa. Erityisesti olisi tehostettava tietojen vertailua jäsenvaltioiden välillä. Komission 7. elokuuta 2006 antamassa tiedonannossa *Rikollisuuden ja rikoslainkäytön mittaamista koskeva kattava ja johdonmukainen EU:n strategia: EU:n toimintasuunnitelma vuosiksi 2006–2010*[21] luonnosteltiin kunnianhimoinen viisivuotissuunnitelma ongelman ratkaisemiseksi. Toimintasuunnitelman mukaisesti perustettu asiantuntijaryhmä voisi kehittää asianmukaiset indikaattorit tietoverkkorikollisuuden laajuuden selvittämiseksi.

4. TULEVAT TOIMET

Komissio aikoo kehittää tietoverkkorikollisuuden torjuntaa koskevaa yleistä politiikkaa. Koska komission toimivaltuudet rikosoikeuden alalla ovat rajalliset, yleisellä politiikalla ainoastaan täydennetään jäsenvaltioiden ja muiden tahojen toimia. Tärkeimpiä toimenpiteitä, joista kukin käsittää vähintään yhden 3 luvussa mainitun välineen käytön, tuetaan rikollisuuden ehkäisemistä ja torjuntaa koskevasta rahoitusohjelmasta.

---

[20] Tavoite on mainittu jo vuoden 2001 tiedonannon sivulla 3.

[21] KOM(2006) 437, 7.8.2006.

4.1. Tietoverkkorikollisuuden torjunta

- Vahvistetaan jäsenvaltioiden lainvalvonta- ja oikeusviranomaisten operatiivista yhteistyötä esimerkiksi järjestämällä vuonna 2007 asiantuntijoiden kokous ja mahdollisesti perustamalla tietoverkkorikollisuutta koskeva EU:n yhteyspiste.

- Lisätään rahoitustukea aloitteille, joilla pyritään parantamaan lainvalvonta- ja oikeusviranomaisten koulutusta tietoverkkorikosten käsittelyssä, ja ryhdytään koordinoimaan alalla järjestettävää monikansallista koulutusta perustamalla EU:n koulutusfoorumi.

- Kannustetaan jäsenvaltioita ja viranomaisia sitoutumaan tietoverkkorikollisuuden torjuntaan ja antamaan riittävät resurssit rikosten ehkäisemiseen.

- Tuetaan tutkimusta, josta on hyötyä tietoverkkorikollisuuden torjunnassa.

- Järjestetään ainakin yksi suuri lainvalvontaviranomaisten ja yksityisen sektorin toimijoiden konferenssi (vuonna 2007) erityisesti Internetin välityksellä sähköisissä verkoissa tapahtuvien ja sähköisiin verkkoihin kohdistuvien rikosten torjuntaa koskevan yhteistyön aloittamiseksi ja automaattisen tietojenvaihdon tehostamiseksi sekä pannaan konferenssissa sovittuja asioita täytäntöön käynnistämällä julkisen ja yksityisen sektorin yhteistyöhankkeita.

- Tehdään aloitteita sellaisten julkisen ja yksityisen sektorin yhteistyöhankkeiden käynnistämiseksi, joilla pyritään tiedottamaan kuluttajille tietoverkkorikollisuuden aiheuttamista kustannuksista ja siihen liittyvistä vaaroista, sekä osallistutaan näihin hankkeisiin; samalla on huolehdittava siitä, ettei kuluttajien ja käyttäjien luottamusta heikennetä liikaa keskittymällä pelkästään turvallisuuden kielteisiin näkökohtiin.

- Osallistutaan aktiivisesti kansainväliseen yhteistyöhön tietoverkkorikollisuuden torjumiseksi sekä tuetaan tällaista yhteistyötä.

- Käynnistetään, rahoitetaan ja tuetaan kansainvälisiä hankkeita, kuten G8-maiden käynnistämiä projekteja, jotka ovat yhdenmukaisia komission toimintapolitiikan sekä maa- ja aluekohtaisten strategia-asiakirjojen kanssa (jälkimmäinen koskee EU:n ulkopuolisten maiden kanssa tehtävää yhteistyötä).

- Ryhdytään käytännön toimiin, joilla pyritään kannustamaan kaikkia jäsenvaltioita ja tiettyjä EU:n ulkopuolisia maita ratifioimaan tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus ja sen lisäpöytäkirja, sekä harkitaan yhteisön liittymistä yleissopimukseen.

- Tutkitaan yhdessä jäsenvaltioiden kanssa jäsenvaltioiden tietoinfrastruktuureihin kohdistuvia koordinoituja ja laajamittaisia hyökkäyksiä niiden ehkäisemiseksi ja torjumiseksi; tämä käsittää toimien yhtenäistämisen sekä tietojen ja parhaiden käytänteiden vaihtamisen.

4.2. Sähköisissä verkoissa tapahtuvan perinteisen rikollisuuden torjunta

- Käynnistetään perusteellinen arviointi ehdotuksen valmistelemiseksi väärän henkilöllisyyden käyttöä koskevaksi EU:n säädökseksi.

- Edistetään Internetissä tapahtuvien petosten ja laittoman kaupan torjuntaan tähtäävien teknisten menetelmien kehittämistä, myös julkisen ja yksityisen sektorin yhteistyöhankkeita.

- Jatketaan ja kehitetään toimintaa tietyillä erityisalueilla: esimerkiksi petostentorjunnan asiantuntijaryhmän toiminta muiden maksuvälineiden kuin käteisrahan välityksellä sähköisissä verkoissa tapahtuvien petosten ehkäisemiseksi.

4.3. Laiton sisältö

- Kehitetään toimenpiteitä laittoman sisällön, varsinkin lasten seksuaalista hyväksikäyttöä koskevan ja terrorismiin kannustavan materiaalin poistamiseksi erityisesti huolehtimalla lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta annetun neuvoston puitepäätöksen täytäntöönpanosta.

- Kehotetaan jäsenvaltioita myöntämään riittävät varat lainvalvontaviranomaisten toiminnan tehostamiseksi erityisesti Internetissä levitettävän seksuaalista hyväksikäyttöä kuvaavan materiaalin uhrien tunnistamiseksi.

- Käynnistetään ja tuetaan toimia sellaisen laittoman sisällön torjumiseksi, joka saattaa kannustaa alaikäisiä väkivaltaan ja muuhun vakavaan laittomaan käyttäytymiseen; tämä koskee eräitä hyvin väkivaltaisia Internet-pelejä.

- Käynnistetään ja tuetaan vuoropuhelua niin jäsenvaltioiden kesken kuin jäsenvaltioiden ja EU:n ulkopuolisten maiden välillä erilaisista teknisistä keinoista torjua laitonta sisältöä sekä menetelmistä laittomien verkkosivustojen sulkemiseksi; lisäksi vuoropuhelun tavoitteena on mahdollisesti saada aikaan naapurimaiden ja muiden maiden kanssa asiaa koskevat viralliset sopimukset.

- Kehitetään EU:n tasolla viranomaisten ja yksityisen sektorin toimijoiden, erityisesti Internet-palveluntarjoajien vapaaehtoisia sopimuksia, jotka koskevat menettelyjä laittomien verkkosivustojen käytön estämiseksi ja sivustojen sulkemiseksi.

4.4. Seuranta

Tässä tiedonannossa on esitelty useita toimenpiteitä, joilla pyritään jatkossa tehostamaan EU:n yhteistyöjärjestelyjä. Komissio aikoo kehittää toimenpiteitä edelleen, arvioida toiminnan täytäntöönpanossa tapahtuvaa edistystä sekä raportoida siitä neuvostolle ja Euroopan parlamentille.

EUROPEISKA UNIONENS RÅD

Bryssel den 30 maj 2007 (2.7)
(OR. en)

10089/07

CRIMORG 102

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
mottagen den:	24 maj 2007
till:	Javier SOLANA, generalsekreterare/hög representant
Ärende:	Meddelande från kommissionen till Europaparlamentet, rådet och Europeiska unionens regionkommitté – Att införa en allmän politik för kampen mot IT-relaterad brottslighet

För delegationerna bifogas kommissionens dokument – KOM(2007) 267 slutlig.

Bilaga: KOM(2007) 267 slutlig

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.

COUNCIL OF THE EUROPEAN UNION

Brussels, 30 May 2007

10089/07
ADD 1

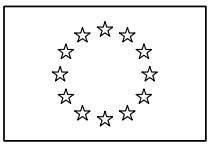
CRIMORG 102

ADDENDUM TO COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	247 May 2007
to:	Mr Javier SOLANA, Secretary-General/High Representative
Subject:	Commission Staff Working Document *Accompanying document to the* Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime = Impact Assessment Report

Delegations will find attached Commission document SEC(2007) 642.

Encl.: SEC(2007) 642



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.5.2007
SEC(2007) 642

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS

Towards a general policy on the fight against cyber crime

IMPACT ASSESSMENT REPORT

{COM(2007) 267 final}
{SEC(2007) 641}

Lead DG:

Justice, Freedom and Security

Commission Legislative Work Programme reference:

2007/JLS/010

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Background

After the last Commission Communications on network and information security[1] and cyber crime[2] were adopted in 2001, the use of the Internet has exploded, and the appearances of new phenomena and new techniques have created a situation of increased insecurity.

In its **Legislative and Work Programme 2007**, the Commission considered that a comprehensive update of the Commission's cyber crime policy has become necessary and therefore envisaged the preparation of a Communication on European Cyber crime policy.

The Commission adopted two Communications on security and privacy in the Information society in May[3] and November[4] 2006 respectively. Those Communications and other prevention oriented documents have been taken into account in the present Impact Assessment and in the initial planning for the Communication on the fight against cyber crime. It is hard to draw an exact dividing line between the area of network and information security and the area of fight against cyber crime, since no effective crime repression policy can be established without an effective prevention and general security policy supporting it, and vice versa. However, to be brief, it can be considered that this cyber crime communication and its impact assessment build on a criminal law enforcement perspective and therefore concentrate principally, but not exclusively, on third pillar issues.

The assessment of problem areas and the possible policy options presented in this Impact Assessment are based on extensive formal and informal consultations with experts and other stakeholders, mainly - but not exclusively - inside Europe.

During the consultation process it became clear that there is not much data or statistics available. This is due to many factors, but especially to the cross-border and global character of cyber crime, the difficulty to establish that such crimes have taken place and the lack of reporting of such crimes. A true picture of cyber crime incidents in Europe is

---

1 Communication on Network and Information Security: Proposal for an EU policy approach - COM(2001) 298.

2 Communication on enhancing creating a Safer Information Society by improving the security of information infrastructures and combating computer related crime - COM(2000) 890.

3 Communication on a strategy for a Secure Information Society – "Dialogue, partnership and empowerment" - COM(2006) 251.

4 Communication on Fighting spam, spyware and malicious software - COM(2006) 688.

thus very hard to establish. Little statistical data is available and existing data gives a rather disparate picture of the situation at EU-level. The preparations for this report already at an early stage made it clear that no quantitative method could be used and that the only method available to assess the impacts would consist in a qualitative consultation of stakeholders. The lack of quantitative data is due to the fact that cyber crime incidents are rarely reported to law enforcement authorities. In particular companies that have been victims of such crimes fear negative impacts if knowledge of the vulnerability of their information and communication technology systems becomes public.

This lack of data (and details on the current state of national legislations) was thus one of the main reasons why the Commission in 2006 decided to order a study from an external contractor. This external study[5], which was established in the period July-October 2006, constitutes the main support for this impact assessment report. The problems and objectives assessed were defined by the contractor in close consultation with the Commission and on the basis of a desk analysis of appropriate analytical methods and applicable legal documents. The core of the study was carried out through numerous interviews with relevant stakeholders (i.e. European Commission officials, law enforcement bodies, national prosecutors, Internet service providers, Internet security providers, specialists and companies facing specific risks, network and information security associations, public and private cyber crime experts, civil organisations, universities and consumer associations). Subsequently, the Commission services have informally consulted different stakeholders and especially Member States experts[6] in order to confirm the conclusions made in the external study. These consultations confirmed that there is a global consensus among practically all stakeholders regarding the EU needs in this field. Although there is a lack of reliable and quantifiable data, the consultations thus provided a sufficient evidence base for identifying problems and corresponding objectives, and assessing available policy options.

On the basis of these activities, the Commission is preparing a new general policy initiative, consisting of a Communication on the fight against cyber crime at EU level. The present impact assessment report will thus principally deal with strategic policy choices. Part of the strategic options that will be assessed are more specific, operational actions, which are not in all cases of relevance for immediate policy purposes, but could fit into the strategy in a longer term perspective.

1.2. State of play: presentation of existing instruments

For the purpose of this Impact Assessment, the following legislative and non-legislative measures have especially been analysed, particularly in relation to possible "gaps" which will be discussed below. It should be underlined that the list below only described the most important instruments. Many other relevant legal and other acts exist, and can be of relevance for the Commission policy against cyber crime.

---

5 Study to Assess the Impact of a Communication on Cyber Crime prepared by Yellow Window Management Consulting (Contract No. DG 2006/JLS D 2/03).

6 Such as the members of the Europol High Tech Crime Experts group.

The **Council of Europe Convention on cyber crime**[7] (hereafter: the CoE Convention) is no doubt the most important and comprehensive international instrument in this field, but its significance depends also on its application as it has by 1 March 2007 entered into force only in ten Member States[8] and nine non EU Member States. The CoE Convention aims to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive- and procedural law and for jurisdiction. The objectives of the policy outlined in this report will complement and not duplicate what has already been decided through the Convention. It should be underlined that the Convention only covers a number of specific legal and procedural questions, whereas the planned EU anti-cyber crime policy will cover cyber crime from a global perspective.

In comparison with the CoE Convention, the **Framework Decision on Attacks against Information Systems**[9] places emphasis rather on approximation of criminal law improving cooperation between judicial and other authorities, calling for the use of existing networks of operational points.

The **Framework Decision on combating terrorism**[10] currently does not contain direct references to cyber terrorism, but can be of relevance.

The **Council Decision to Combat Child Pornography on Internet**[11] calls Member States to promote and facilitate investigation and prosecution, to encourage internet users to report to competent authorities, to use the existing points of contact, to cooperate with Europol and Interpol and also to build up dialogues with the industry.

The **Directive on Electronic Commerce**[12] is important concerning issues of responsibility as it excludes any obligation of network operators to monitor the information they transmit or store. **The Directive on privacy and electronic communications**[13], besides containing provisions on spam, envisages also an obligation for service providers to take measures to safeguard security and to inform users in case of particular risk of breach of security of the network. **The Directive on the retention of data**[14] is particularly relevant for the purpose of prevention, investigation, detection and prosecution of criminal offences as it ensures at EU level that certain data, in the course of the supply of communications services, are retained for a certain period of time.

All the instruments just presented, including the CoE Convention, have in common that they cover only some aspects of the fight against cyber crime. The initiative discussed in

---

7 Council of Europe Convention on Cyber crime, 2001: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

8 Bulgaria, Cyprus, Denmark, Estonia, France, Hungary, Lithuania, the Netherlands, Romania and Slovenia.

9 Framework Decision on attacks against information systems (2005/222/JHA).

10 Framework Decision on combating terrorism (2002/475/JHA).

11 Council Decision of 29 May 2000 to combat child pornography on the Internet (2000/375/JHA).

12 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the Internal Market.

13 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

14 Directive 2006/24/EC on the retention of data generated of processed in connection of the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

the present report aims at a more strategic and horizontal perspective, covering the whole range of the cyber crime problem area.

1.3. The Impact Assessment Board

On 9 March 2007, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. In the opinion, the Board in brief stated that:

- A more focused analysis should be presented of the problem, objectives and policy options, giving particular attention to the justification for EU action and providing a realistic picture of its likely added value
- The definition of problems and objectives should be clarified, ranked and focused
- The presentation of policy options should be simplified and strengthened as regards the subsidiarity and value added aspects
- A clearer discussion of economic and social impacts was advisable

The present version of the Impact Assessment report has been completely restructured and significantly redrafted, with a view to taking these recommendations fully into account. However, the recommendation to rank the objectives has only been followed to the extent possible. The objectives of this policy are very closely connected to each other and not interchangeable; a ranking between them can thus only be of tentative character.

2. PROBLEM DEFINITION

2.1. Overall problem

The rapid development of Internet and other information systems has given rise to a completely new economic sector and to new rapid flows of information, products and services across the internal and external borders of the EU. This has obviously had numerous positive effects for consumers and citizens. The new sector also contributes considerably to economic growth in many areas in Europe. However, the same development has also opened many new possibilities for criminals. A pattern of new criminal activities against the Internet, or with the use of information systems as a criminal tool, is clearly discernible. These criminal activities are in permanent evolution, and legislation and operational law enforcement have obvious difficulties in keeping pace. The intrinsic cross-border character of this new type of crime also creates a need for improved cross-border law enforcement cooperation.

In section 2.2 below, eight strategic problem areas will be used in order to explain the overall problem more in detail. It should be noted that the consultations undertaken in view of the present report indicated strikingly converting views from all stakeholders – be they law enforcement authorities or private companies – regarding current EU problems in this field.

2.2. Strategic problem areas in detail

2.2.1. The growing vulnerability to cyber crime risks for society, business and citizens

The importance of the internet is growing as companies and organisations are interlinked and become more and more depending on communication systems, especially the internet. Due to new spam techniques and enlarged spam volumes and to other new phenomena such as phishing, botnets, malware, theft of codes and of different personal information, insecurity has increased and the level of trust has been reduced. The fight against cyber crime is one of the most important factors in the efforts to strengthen security, but also one of the most difficult. Besides the difficulties of discovering crimes and the cross-border nature of cyber crime, the determination of the competent jurisdiction and applicable law, the cross-border enforcement and the recognition and use of electronic evidence enhances difficulties to prevent and prosecute crime.

It can be assumed that the continuously enhanced globalisation and interoperability of information systems will make the cyber environment even more vulnerable, although new security techniques and strategies may also complete the picture in compensating for this increased vulnerability.

2.2.2. An increased frequency and sophistication of cyber crime offences

The lack of information on cyber crime in Member States makes it difficult or even impossible to identify and quantify the crime level. The external study mentioned above has given some indicative data only. In the absence of reliable global statistics, the following general indicative trends in cyber crime can however be discerned:

- New sophisticated techniques are increasingly used by criminals
- Cyber crime attacks are more and more often targeted at specific groups of victims
- Crimes, particularly fraud, are increasingly often committed with the help of identity thefts and phishing[15]
- The most serious threat lately seems to be the appearance of so called botnets, which make it possible to, for example, infect a large number of computers in order to use a whole network to commit crimes at a large scale
- A trend towards more organised crime on the Internet, focused only on financial profit, has been observed

As an indicative example of the increased frequency in one particularly serious form of crime, the publication of child sexual abuse material, it should be underlined that the UK-based Internet Watch Foundation has estimated that the number of sites with this type of illegal material has increased with 1 500 percent in the period 1997-2005.

[15] Phishing signifies attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.

2.2.3. The lack of a coherent EU-level policy and legislation for the fight against cyber crime

As EU integration continues, the need for better coordination of criminal policies is accentuated. This is true in particular for the field of fight against cyber crime. All Member States have national policies against cyber crime or certain aspects of cyber crime. There are also different multinational projects to interconnect these policies. These projects often concern particular aspects of the problem area, such as the fight against child pornography or the fight against illegal trade. Despite the existence of organs and structures such as the Europol High Tech Crime group, it can not be claimed that an elaborated coherent horizontal policy in Europe on the fight against cyber crime exists. A continuing situation of uncoordinated policies in Europe would increase the problem by leading to fragmented anti cyber-crime actions, a state of affairs which could potentially be exploited by criminals.

The risk that criminals would exploit differences between Member States is even more concrete when it comes to differences in legislation. Criminals may choose to set up shop in a country in which a specific activity is punished more mildly or is not even criminalized. In view of studying this problem, a preliminary analysis of **legal gaps** in and between Member States has been carried out through the external study, but the analysis of this very complex issue must be deepened before any final conclusions can be drawn. The analysis has been done on the basis of the CoE Convention, which is probably the most comprehensive legal act that exists in this field.

In this context, it should be noted that to date, two different approaches have been applied to the definition of cyber crime. The first approach considers only computer- or network-specific crimes. The second approach includes also computer- or network-related crimes, thus covering also traditional crimes committed with the support of a computer or over a network. According to the first approach, legislation needs to include only computer- or network-specific crimes because non- computer- or network-specific crimes are often sufficiently covered by the provisions against traditional crimes. The second approach deems necessary the adoption of specific provisions for computer- or network-related crimes, taking into account the principle prohibiting the interpretation of penal law through analogy, and demanding a precise definition of acts that are considered to be crimes. When legal gaps between Member States are analyzed, this difference in approaches must be kept in mind. In view of the rapid evolution of cyber crime and the increase in the different types of cyber crimes that are being perpetrated, it is important to consider a development of a categorisation of cyber crimes that finds the right balance between these two approaches.

Regarding the *substantive legislation*, there is a constant need to monitor crime definitions in order to make sure that they are still valid, considering the quick technology changes and new emerging crime types. Definitions need to be as technology neutral as possible. One example is the notion of "*computer system*" in the CoE Convention, which has given rise to some problems such as the exclusion, according to the case-law in some states, from the sphere of application, of mobile telephones or other wireless technology. In the Framework Decision 2005/222/JHA, the notion "*information system*", which should be more technology neutral, has been used instead. Considerable general differences between Member States still exist in formal crime definitions. It is however hard to make any conclusion on the basis of this, since the lack of explicit

legislation does not always mean that there is no law (in the form of case-law or other non codified regulation). For example in many Member States computer *fraud and forgery* fall under traditional terms of criminal law, and no specific legislation is then considered to be needed.

A specific problem concerns *identity theft*, which is often used as an instrument to commit crimes. In many Member States, identity theft as such is not criminalised, which may lead to considerable problems in cross-border law enforcement and judicial cooperation. It has also been confirmed by stakeholders that the legal means to fight identity theft before another crime is committed are, partly for this reason, limited. It should be considered that identity theft is the core activity of many cyber crimes, and that cyber criminals find it relatively easy to steal identities.

Generally speaking national legislations are rarely uniform, or even close to harmonized, regarding *content-related offences.*

Specific *procedural measures* are provided by the CoE Convention, such as preservation of stored computer data, production order, search and seizure of stored computer data, or real-time collection of computer data, but the Convention has not been ratified by all Member States, and the majority of them still apply general procedural provisions to cyber crimes. Many stakeholders have underlined a need for European procedural rules defining types of data, modalities to preserve and produce evidence.

The conclusion would be that many differences exist between legislations within the EU and that this may cause a problematic situation in Europe.

2.2.4. Specific difficulties in operational law enforcement cooperation regarding cyber crime

The fight against cyber crime often implies a need to act very quickly against a criminal activity. Criminals may often change web addresses, Internet services providers or user names, especially when there is a risk of intervention from law enforcement authorities. If the criminal activities are to be stopped, there is thus often a clear need of extremely rapid action and information exchange, often border-crossing. The current procedures for intra-European and international law enforcement cooperation are not adapted to the fight against cyber crime in this respect. It should be noted that the difficulties in this context are not a result of EU integration, but rather of intrinsic cross-border technologies and the general impact of globalization. The borders of the EU are very seldom the borders of cyber crime activities.

As a consequence of the technical evolution, criminals are now using with fast networks allowing them to commit crimes over different national judicial territories in a very short period of time and also to eliminate evidence, just as quickly. Due to the cross border nature of cyber crime, criminals can also easily obtain significant comparative advantages in relation to law enforcement authorities. In addition to the fact that cyber criminals do not have to be present physically while committing the crime, weak or nonexistent legislation or a lack of law enforcement specialists on cyber crimes can give criminals an advantage. Law enforcers also have the problem of getting used to continuous new forms of crime, of handling the increasing number of cases and of reacting quickly within the national jurisdiction as well as across other jurisdictions.

The pressure on the system is enhanced by the time consuming procedures that are necessary to access data, to separate relevant from irrelevant data and to secure electronic evidence. The procedures which law enforcers need to use to get relevant information are also perceived to be much too slow. As an example, the fact that law enforcement in one country can not directly contact a network operator in another state, even though a crime in their own state may have been committed via the foreign operator, makes work very difficult.

There are a number of organisations and mechanisms, such as Interpol, the G8 and Council of Europe 24/7 contact points, Europol, CEPOL and Eurojust, which are dealing with trans-border crimes. Theoretically, international cyber crime could be handled by these bodies. However, experience shows that this does not often happen. It would thus seem that good structures exist, but that they are not used in anything close to an optimal way.

2.2.5. The need to develop competence and technical tools: Training and research

The fast evolution in cyber criminality means that there is also a situation of increased need for training at all concerned levels. It should be noted that there is a global need for training of the entire population, but the present point of focus will be on analysing training needs for law enforcement and judicial authorities. Due to the fact that technology is changing extremely quickly, there is an obvious need for continuous training not only for specialised units, but also for any police officer, judge or prosecutor who could be confronted with cyber crime activities. The cross-border character of cyber crime makes it easy for criminals to move their activities from one state to another at short notice. Criminal activities may be moved to states considered to have weak law enforcement in this area. Already for this reason, there is a clear European interest in making sure that law enforcement authorities in all Member States are sufficiently trained to meet the cyber crime threat.

Closely linked to the training issue is the need to build on and take forward relevant research in this area. In particular the development of technological tools to trace criminals and victims and to prevent or stop criminal cyber activities need to be promoted.

2.2.6. The lack of a functional structure for cooperation between important stakeholders in the public and the private sector

Industry has often shown a very positive attitude towards assisting public authorities in the fight against cyber crime, but the public authorities are very often not aware of programmes and actions run by the private sector, which could in fact serve as an important support to traditional law enforcement and crime prevention activities. There are very few initiatives in Europe to centralise existing information platforms.

Public authorities and law enforcement are also not always informed of criminal attacks against private companies. Private sector operators are often, in order to protect business models and secrets, reluctant to report or share information on crime incidences with law enforcement authorities. However, such information is needed if the public authorities are to be able to formulate an efficient and well-adjusted anti-crime policy. The willingness of companies to report criminal incidents may be linked to the fact of whether or not police officers make an official case out of each report they receive, or to

the fact that the perception is such that police cannot follow-up on reported crimes anyhow.

One other main problem regarding the fight against cyber crime is the lack of adequate statistics. Individual users do not report incidents, because often they are not aware of the attack, do not care about it, do not know where and how to report or simply they do not want to inform authorities. Nonetheless, it is important to note that the analysis conducted has shown that companies in general do appreciate the advantages of better exchanges of information. Indeed, raising customer awareness can enable the consumers to protect themselves more effectively, or to better accept the needs as well as the cost and possible inconveniences of higher protection. Information on victims may also highlight security problems in certain sectors, which in turn may improve policy and legislation makers' understanding of the need to protect those particular sectors.

It should be noted that there is a generally satisfactory operational cooperation between network operators and web hosts and law enforcement bodies concerning closing down of web sites, especially those containing child pornography, and the blocking of crime-related communication between specific users. In spite of the lack of clear provisions on shutting down sites, network operators frequently close down such web pages on their own initiative. In many cases cyber crimes and criminals can hardly be detected unless the private sector cooperates with law enforcement authorities. There is thus a public interest in having network operators taking an active part in investigations and in legal proceedings. The role of network operators is especially important in relation to blocking specific web sites with illegal content or which are used to support botnets, as they are in a special position regarding communications on the Internet. It should also be noted that investigations are often pursued by private companies, without the knowledge of the authorities.

It can thus be stated, as a conclusion, that a clear and urgent need and scope for improvement of the cooperation between the public and the private sector in this field has been identified. An effective programme for the fight against cyber crime can only be truly effective if it includes a strategy for cooperation between the public sector, especially law enforcement authorities, and private sector operators. For this, an atmosphere of trust and confidence is needed.

2.2.7. Unclear system of responsibilities and liabilities

A specific issue regarding both possible EU legislation and EU public-private relations in the fight against cyber crime concern the responsibilities and liabilities of different actors in cyber space. The lack of clear responsibilities of all actors has been identified as a problem area in Europe. Even if the fight against cyber crime is the object of this report, it should be noted that repression is not possible without prevention, and that prevention is indeed the top priority in terms of efficiency. Setting clear responsibilities for all actors in the cyber world would represent enormous advantages for all those involved, whether they are victims or law enforcers and prosecutors. Four main categories of actors could be considered: (1) end users, (2) providers of services directly linked to Internet, (3) providers of e-services and (4) manufacturers of hardware or software tools etc. Network operators, in particular, have a clear technical capacity to identify and prevent a large number of cyber crime offences, but also manufacturers of software could make their products crime proof.

2.2.8. The lack of awareness of the risks emanating from cyber crime

The financial and social risks emanating from cyber crime attacks can be enormous. It appears that these risks are not known widely enough or are partly neglected. This is also due to the reluctance to report crime (referred to in section 2.2.6). The lack of reliable data and statistics[16] is likely to contribute to lack of awareness of the risks emanating from cyber crime, especially among particularly vulnerable potential victims, such as small companies, organisations and individual citizens. There is a general need to better protect all users of electronic information systems, and this can mainly be done if awareness of existing risks is enhanced. Campaigns should especially be directed towards consumers and other identified potential vulnerable victim groups. It is however important that awareness raising programmes do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security.

2.3. Who is affected?

Cyber crime affects all sectors of society, and a policy to counter it will also be visible practically everywhere. Considering that the number of citizens using private computers is very high, most individual citizens – already in their capacity of potential victims – may also be affected by any initiative in the area of fight against cyber crime.

There are however also clear indications pointing at increased criminal activity directed against specific groups of victims. As an example, it would seem that phishing and other tools used to commit fraud crimes appear to be used in a more targeted fashion against more vulnerable potential victim groups, such as very young persons or small companies with less developed financial control mechanisms. An effective anti cyber crime policy could thus have clear beneficial effects for these groups. In the short term, the main public stakeholders of an EU level policy against cyber crime would be all authorities with an anti-cyber crime programme, *ie* mainly law enforcement authorities.

2.4. Does the EU have a right to act?

Given the scope and magnitude of security threats, a need to tackle the threats from cyber crime persists and may be growing. Security issues connected to cyber crime have a global dimension and cannot therefore be dealt with only at national level. The threat is international, and so must be at least a part of the answer. It is beyond any doubt that the fight against cyber crime will continue to be most important and effective at a national level, but there is a clear need to interlink and possibly complement national efforts at the European level.

The EU actions discussed in this impact assessment report will not go beyond what is required and what is clearly adding value at the EU-level. Already the limited EU legal competence in this field implies that the main feature of all planned EU actions in the short term will be of a coordinating nature. The fight against cyber crime will also in the future primarily be a responsibility of Member States, and the scale of EU intervention will remain limited. However, the benefits of EU-level coordination in this field should

---

[16] Proposals for an improved framework for collection of data can be found in the Communication on a strategy for a Secure Information Society – Dialogue, partnership and empowerment - COM(2006) 251.

not be underestimated. Operational law enforcement work against cross-border criminal activities would be considerably facilitated and a more structured exchange of information and best practices could provide a clear added value for national law enforcement bodies. Such efforts could also create synergies and, in turn, add a clear value also at EU level. The intrinsic international and cross-border character of cyber crime is proof enough that actions are needed both at global international and at EU-level. The Commission, fully respecting the subsidiarity principle, is ideally placed to coordinate such actions, in close cooperation with Member States and other international organisations. It should again be underlined that the EU level policy can at this point in time only be a supplement to national and other international policies. A reinforced EU coordination should mainly be regarded as a limited but nevertheless very important contribution to the national and global actions against cyber crime.

The policy to be outlined in this report will include a number of future and more concrete actions, including the organisation of conferences, the setting up of formal or informal networks, as well as legislation. Those future actions will be assessed in time, in order to certify that they add value at EU-level before they are undertaken. In the same way, the legal bases for these actions will be defined later after a close study of the content of the particular actions.

3. OBJECTIVES

The overall strategic objective of the proposed policy, based on the problems identified above, can be summarized as follows:

- To strengthen and better coordinate the fight against cyber crime at national, European and international level

This overall strategic objective can be divided into the following six strategic level objectives, presented in a tentative order of priority:

- To improve operational cross-border law enforcement actions against cyber crime in general and against serious forms of cyber crime in particular, and to improve exchange of information, intelligence and best practices between law enforcement agencies in Member States and beyond

- To identify and create operational instruments for cooperation and common goal-setting between the public and the private sector and to improve the exchange of information, intelligence and best practices for the fight against cyber crime between the public and the private sector at EU level

- To establish a political platform and structures for the development of a consistent EU Policy on the fight against cyber crime, in cooperation with the Member States and competent EU and international organisations, and to make existing legal and institutional frameworks more effective, also by clarifying responsibilities and liabilities for all relevant actors

- To meet the growing threat from serious forms of cyber crime by promoting skills, knowledge and technical tools; including actions to strengthen relevant training and research

- To raise overall awareness of the threat of cyber crime, especially among consumers and other vulnerable groups of potential victims, while avoiding to undermine the trust and confidence of consumers and users by focusing only on negative aspects of security

An EU policy against cyber crime would need to include all these strategic objectives, since they are closely interlinked and could hardly be followed separately in an effective way. The priority order tentatively set out above thus only has a limited validity. All policy options discussed in the present report will thus be attempts to address all these objectives.

4. STRATEGIC POLICY OPTIONS

4.1. Formulation of policy options

Any policy for the fight against cyber crime will, due to the nature of the subject-matter, be of a multi-faceted nature. To be truly effective, the police must combine traditional law enforcement activities with other instruments, such as self-regulatory elements and the setting up of structures for cooperation between different stakeholders. A number of problem areas and strategic objectives for the present initiative have been presented above. To reach these objectives, a number of different and combined actions are needed.

There are many possible ways to address the problems described above. The Commission services have considered a number of concrete actions, which are complementing each other rather than constituting completely separate alternatives. These policy options are presented in more detail in the preparatory external study. In order to choose a concrete coherent policy for the next few years, a policy which will be presented in a Communication planned for adoption in 2007, the objectives set out above have resulted in four "option packages" (hereafter: general policy options), each including a number of specific potential actions.

All of these general policy options, except the first one ("status quo"), include elements which will contribute to all of the objectives presented in section 3 above. In brief, the second option concentrates on the setting up of a regulatory framework and new formal structures, the third looks at informal and self-regulatory networks and action, whereas the fourth general policy option is a combination of regulatory and informal measures. The options packages have been discussed with public and private external stakeholders, who have in general agreed on the choices proposed in this report.

4.2. The four general policy options

4.2.1. General policy option 1: Status quo/no major new action at all

This option would mean that no general horizontal action is taken in this field by the Commission now. This would imply that:

- The Commission would continuously assess the need for targeted legislation or policy action and take appropriate action when needed

The Commission would continue to play its role as policy initiator and propose legislation when needed, but no horizontal strategy for this activity in the area of fight against cyber crime would be launched.

- The Commission would follow existing EU and international structures projects against cyber crime

The Commission would continue to actively participate in the European efforts to strengthen network and information security. It would also continue to actively follow external work, for example in the Council of Europe or in the G 8 Roma-Lyon High Tech Crime Group.

- The Commission would continue to initiate new projects in targeted fields of interest for the fight against cyber crime, but would not take any horizontal policy initiative

The Commission would also in the future support different projects through its financial programmes, especially the programme "Prevention of and Fight against crime".

4.2.2. General policy option 2: General legislation

This option would mean that a policy to gradually propose a general regulatory framework for the fight against cyber crime is adopted. Such a policy would imply that:

- The Commission would systematically propose harmonized or unified crime definitions, especially for the EU but also at the international level

The Commission is already active in this area; although only with regard to specific single crimes. As an example of efforts to harmonize crime definitions, the Framework Decision on Attacks against cyber crime can be mentioned. No global strategy to generalise this effort has however existed. The action suggested would mean that actions to achieve harmonized or unified crime definitions in the whole field of fight against cyber crime would be undertaken.

- The Commission would propose common minimum standards for criminalization and penalties in the EU

The Commission is already active in this area, in basically the same way as described above regarding harmonized and unified crime definitions. No global strategy to make this effort general has however existed. The action suggested would mean that actions to achieve minimum standards of criminalization and minimum penalties in the whole field of fight against cyber crime in the EU would be undertaken.

- Generally applicable rules on responsibilities and liabilities - in particular rules imposing legal obligations for network operators, producers and consumers to take specific security measures to fight cyber crime - would be proposed

The Commission would in this case consider strengthening the obligation for the network operators to remove or to disable access to the information when they are aware or have knowledge of illegal activity or information.

- Formal platforms for the area of public-private cooperation as well as the area of training and research would be created

The Commission would in this case propose or take a formal decision to set up a specific public-private platform. This formalized structure, which could take the form of networks or expert groups, would be provided with their own rules of procedure, and would also deal with awareness raising issues.

- A formal law enforcement network would be created

The Commission would in this case propose or take a formal decision to set up a new body dealing permanently with EU coordination of the operational fight against cyber crime. Training and research issues would also be handled by this body. A continuous analysis of potential legal gaps and EU legislative needs could also be within the remit of the group, which could be given the competence to formulate recommendations.

4.2.3. General policy option 3: Creation of informal cyber crime and public-private networks, combined with the setting up of voluntary schemes for certification of products and services at different levels

This option would mean that the Commission, alone or together with other institutions, would formally set up networks or expert groups of cyber crime. This would imply that:

- An informal body of law enforcement cyber crime experts would be set up

The Commission would, through the organisation of regular dedicated meetings, set up an informal network of law enforcement experts. The network would be asked to informally coordinate operational law enforcement activities and of creating a informal coordination points all over Europe, dealing also with areas such as exchange of information and best practices as well as training and research issues in the very specific field of fight against cyber crime. The network could build on, and coordinate with, existing structures, such as the Europol High Tech Crime or the Council of Europe/G 8 24/7 network. The network would thus also be in contact with international partners.

- An informal platform/network of public and private cyber crime experts would be set up

The Commission would set up or contribute to the setting up of an informal but permanent platform of law enforcement experts as well as private sector network and information security experts. The network would complement the network mentioned in the point above and the two networks should be closely coordinated. In particular, the network would have the task of creating models for the exchange of sensitive non-personal information between the sectors. It could also be linked to public and private actors in neighbouring countries.

4.2.4. General policy option 4: A coherent strategic approach

This option would mean that a coherent strategy for the fight against cyber crime is introduced at EU-level. The main feature would be the setting up of a strategic framework for the EU-level policy against cyber crime, with the general objective of

achieving a better guidance on concrete actions and an optimization of existing means. Other important operational features of this strategy would be:

- An improved EU-level law enforcement cooperation

This would in particular include actions to improve exchange of information and best practices between Member States, training for law enforcement and judicial authorities (with the possible setting up of a permanent EU training platform and the increased use of existing and future financing programmes to support multi-national training initiatives in the field of fight against cyber crime), awareness raising campaigns among law enforcement personnel and support for relevant research. Expenditures for existing coordinating instruments in the EU would be increased.

- The introduction of a strategic structure for public-private cooperation against cyber crime

The Commission would take a pro-active role in networking and the setting up of public-private task forces and working groups, which would be given the task of addressing common cyber crime problems. These efforts would also contribute to an atmosphere of confidence, facilitating common goal-setting.

- The promotion of the establishment of a framework for global international cooperation in the relevant field

The Commission would take action to strengthen global international cooperation. Efforts should be made both to make existing instruments, such as those developed by the Council of Europe and G 8, more effective, and to develop new instruments or cooperation structures. Efforts would also be made to make existing international instruments more efficient.

- Targeted legislative measures when this is needed

The need for new legislation would be continuously assessed. In the short term, rules on a minimum penal legislation on identity theft would be proposed. Reflections on the possibility to introduce additional rules on responsibilities and liabilities would also be launched by the Commission. In the longer term, further legislation with a view to harmonising relevant criminal and criminal procedural law, both within the EU and internationally, would remain an objective.

5. ASSESSMENT OF POLICY OPTIONS

The general policy options have been assessed on the basis of a number of set criteria (see below). It should again be underlined that the direct impacts of the proposed strategies are limited, and that specific actions undertaken later within the framework of one of these strategies will be assessed separately at that point. It should also be noted that the view has been taken that the anti-cyber crime policy actions examined will not have any noticeable environmental impact; that issue will thus not be assessed.

5.1. General policy option 1: Status quo/no major new action at all

5.1.1. Social impacts

The main direct consequences of a "no new action" scenario regarding law enforcement would be that law enforcement authorities and prosecutors would continue to encounter important problems in cooperating effectively across borders and that cyber criminals could continue to actively exploit these differences between jurisdictions and possibly actively seek out "free havens". The fight against cyber crime and especially prevention efforts would thus continue to be fragmented and no horizontal approach aiming at finding synergies and structures for horizontally exchanged information and best practices would be established. Anti-cyber crime activities in the EU would risk an emerging internal incoherence. As regards relevant training and research, the situation would continue to be fragmented, with different, uncoordinated initiatives.

No global initiative to interlink public and private efforts to fight cyber crime would be achieved. Public authorities would continue to lack sufficient information on what is done in the private sector, which would reduce the possibilities to formulate an adequate policy in this field. The global responses to cyber crime from all legal actors would continue to be fragmented.

The absence of a horizontal legislative strategy could contribute to increasing the risk of a continuing or even growing legal uncertainty at EU-level. Existing and emerging gaps in legislation and differences in Member States' legislation would lead to a continuous and sometimes even growing legal insecurity for potential cyber crime victims.

The lack of any horizontal initiative would also produce a clear risk of a growing feeling of insecurity in the EU. This could also affect the further development of Information Society industry - and thereby also the employment market - negatively. The position of vulnerable potential crime victim groups, such as consumers and small companies, would also risk being weakened, especially when new cyber crime phenomena emerge.

5.1.2. Economic impacts

The "no new action" option would not produce any direct economic impacts. However, there are clear indications that the costs resulting from cyber crime are already high for industry citizens and society in general. These costs would continue to be high or increase. It could thus be argued that this option is expensive, in that the present state of lack of coordination and unclear responsibilities probably increases costs at all levels in society. Growing disparities in legislation – due to new crime phenomena leading to even more disparate legislation in Member States – could also create additional administrative burdens for all stakeholders. In particular multinational private sector operators would have to carry increased costs if they had to adapt to completely different legislation in each Member State in which they are active.

5.1.3. Costs for public administration

No new costs would occur for public administrations.

5.1.4. Degree of coherence with policy objectives

This general option would only meet the objectives outlined in section 3 above to a lesser degree.

5.1.5. Added value and respect of the subsidiarity principle

No new action that could add value would be taken. It should be recalled, however, that this option leaves the door open for continued targeted activities, but the added value of such activities would need to be assessed separately.

5.1.6. Feasibility

A "no new action" option is obviously feasible from a theoretical point of view. However, a decision not to take any horizontal action in this field would risk strong political criticism already in the near future. As regards the lack of a horizontal legislative policy, there are very important, sometimes insoluble, political and legal problems surrounding any attempt to achieve common categorization of crime definitions or harmonised definitions, and a no new action policy would for this reason possibly be the most feasible solution.

5.1.7. Conclusion

Due to the reasons explained below, this option would clearly not be enough in relation to existing challenges. The impacts of the "no new action" option are in principle limited, but it is difficult to assess whether there is a risk of this option leading to a significant impact as the future types of crime are by definition not known. The potential long-term negative impact of a "no new action" scenario is very high, taking into account the current and growing importance of this type of crime

5.2. General policy option 2: General legislation

5.2.1. Social impacts

As regards harmonized or unified crime definitions and common minimum standards for criminalization and penalties, one social impact would be the general improvement of legal certainty and increased likelihood of covering all types of cyber crime. Cross-border operational and jurisdictional cooperation would also be facilitated considerably. A negative social impact linked to this option could possibly be perceived regarding the general political atmosphere (see feasibility below). A more uniform law would possibly fail to take regional and cultural specificities into account.

5.2.2. Economic impacts

This policy option could produce a considerable economic impact in the long perspective. A higher degree of legal certainty may provide important advantages on the Information Society market, which could be economically advantageous for all stakeholders. Filling existing legal gaps would improve the potential of repression, which would strengthen the prevention side. This, in turn, could result in considerable positive economic impacts in society. At the same time, the introduction of a number of new

European legal measures, in particular as regards responsibilities and liabilities, might however also entail a significant implementation costs for companies.

5.2.3. Costs for public administration

There are no direct costs associated with this option. The indirect costs connected to the preparation and implementation of new legislation could be substantial. These costs would need to be separately assessed later, depending on the specificities of every single proposal for new legislation.

5.2.4. Degree of coherence with policy objectives

A common legal framework would facilitate intra EU and international operational cooperation. On the basis of the framework, a functional public-private cooperation, relevant training and specific awareness raising campaigns could also be achieved. This general option would no doubt also permit the creation of a truly consistent EU policy with a more effective legal and institutional framework. From a theoretical standpoint, this general policy option is thus fully consistent with the objectives set out.

5.2.5. Added value and respect of the subsidiarity principle

All general legislative initiatives in this field would add a clear European value in that a common European regulatory framework would be established. This would have clear positive impacts for the Internal market, and thereby also for the economic development of the sector in question. The legal security of all stakeholders and the protection of consumers and other potential victims would also clearly be strengthened. On the other hand, it can be questioned whether such a general initiative would not go too far with regard to the subsidiarity principle. It is true that every single legislative proposal would have to be assessed in relation to this principle, but it is possible that the general strategy as such would need to be adjusted in order to be consistent with subsidiarity requirements.

5.2.6. Feasibility

The feasibility is open to question, as a significant resistance both from Member States and from private sector operators can be expected. The main barrier against this type of legislation may be the difficulty in formulating a penal law which is in accordance with national legal practices and traditions. A risk to criminalise non-damaging activities, by failing to take regional specificities into account, also exists. However, if the general strategy were adjusted at the political level, it cannot be excluded that a solution can be found in the long term, especially considering the importance of the problem.

5.2.7. Conclusion

This policy option could only be pursued very carefully and in the long-term perspective. Detailed legal feasibility studies and long political negotiations would be necessary. The impacts of this option may be very important, but in view of the small likelihood of making real progress in the short term, this option becomes uncertain in the short term perspective. It can also be questioned whether the policy objectives would met as effectively at the level of the actual implementation of the policy actions as they are at a political and theoretical level. Should this policy option prevail, the risk would be that the

operational level of fight against cyber crime would not be sufficiently involved in strategic political choices and decisions. Considering the important, associated impacts, the role of the Commission in this respect would also need to be clarified. It could possibly also be claimed that similar results could be achieved with less penetrating measures. However, it should be kept in mind that many legislative proposals are already under way at EU level in areas related to network and information security. One example is the review of the Regulatory Framework for electronic communications which might result in amendments to the security-related provisions of the ePrivacy Directive 2002/58/EC and the Universal Service Directive 2002/22/EC.

5.3. General policy option 3: Creation of informal cyber crime and public-private networks, combined with the setting up of voluntary schemes for certification of products and services at different levels

5.3.1. Social impacts

The social impact of the setting up of a law enforcement network would be high, as this would in the long run certainly increase the number of EU-wide joint operations and prosecutions against cyber criminals. A secondary effect of this could possibly be a slow tendency to further adapt national laws to suit EU harmonisation. The positive impacts for law enforcers and prosecutors would be significant, helping to eliminate many restrictions on international cooperation between law enforcers and prosecutors across the EU. Resources would thus be used more efficiently in the repression process.

Subsequently, an increased level of security would in particular have positive effects on the protection of potential victim groups and the further development of Information Society industry. A negative effect could be that new structures could add confusion to the EU situation, insofar as the role of already existing bodies would become more unclear.

The creation of a public-private network could also possibly have important social impacts of the same sort as those just described. Impacts to be considered could be better coherence inside the EU, improved prevention, better awareness, higher efficiency in repression and higher level of trust in e-commerce. In addition, an atmosphere of cooperation, common goal-setting and mutual confidence between all stakeholders – in the private as well as in the public sector – could be achieved. This, in turn, could lead to important synergies and a more effective global strategy in the fight against cyber crime.

5.3.2. Economic impacts

The economic impact is linked mainly with the efficiency of law enforcement and prosecution. A likely decrease in cyber crime will entail fewer economic losses for internet users, increase the trust in the internet by those users and thus entail higher revenues for businesses with activities on the internet. Consumers would also be better protected. The negative economic impact, if any, would be negligible.

5.3.3. Costs for public administration

Costs for public administrations would be fairly moderate. The European Union would finance the different networks, but the costs could be limited to the organisation of a few

meetings a year and some administrative support. The establishment of two networks could possibly be co-financed by the private sector.

5.3.4. Degree of coherence with policy objectives

The general policy option would meet the objectives regarding operational law enforcement cooperation and public-private structures very well. This would probably also contribute to making existing legal and institutional frameworks more effective. It can also be assumed that the objectives regarding promoting skill, knowledge and risk awareness would be met through the work of the different networks described. Since these networks would be rather flexible and informally organised, it could however be questioned whether the objective of pursuing a consistent EU policy would be met in an optimal way through this policy option.

5.3.5. Added value and respect of the subsidiarity principle

The setting up of both networks would clearly add European value. It should however be underlined that the system as well as the networks will only operate in the European environment, and not replace similar instruments at national level. The Commission will in any case take action in this field only if, and insofar as, the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. It is open to question whether formal expert groups are required and if the need could in reality not be covered by less formal structures.

5.3.6. Feasibility

The setting up of the two networks is probably easy to achieve. It could however take considerable efforts to make them operational and make sure that they add concrete value.

5.3.7. Conclusion

This policy option looks very interesting from a strategic point of view, even if the added value and the concrete impacts are hard to foresee. The risk is that the new network structures would achieve few concrete results. The Commission should be ideally placed for coordinating self-regulatory actions in the relevant field but, in the framework of this policy option, more in the role of coordinator and facilitator that that of strategic leader.

5.4. General policy option 4: A coherent strategic approach

5.4.1. Social impacts

As regards EU-level law enforcement cooperation, positive impacts of some importance are expected for the coordination of investigations and prosecutions, the efficiency of the system and the reduction of the time needed to complete the cases. As the scope would be the EU, to the extent that Member States believe that a part of the problem of cyber crime is better dealt with at an EU level than at the national level, the efforts to bring these measures about will be less cumbersome than similar measures to bring about global cooperation or harmonisation of laws. The impact will however again mainly be

on cyber crime operations within the EU. Therefore there is a risk that criminal activities would shift outside the EU, but continue to target crime victims in the EU. The impact of operational cooperation in individual cases would be high, as this could be expected to significantly increase the number of prosecutions against cyber criminals. Such cooperation could fall within the remit of Europol, Eurojust and CEPOL, and demand efforts which are limited to these institutions. As concerns EU-level relevant training and research, the impacts would firstly touch upon law enforcers and prosecutors, who would gain in competence and knowledge. The measure would eventually contribute not only to more harmonisation and cooperation inside the EU, but also to better international cooperation.

The social impacts relating to private companies, which take part in the public-private networks and conferences, are not easy to predict. It is however beyond doubt that private and public sector, network operators and law enforcement, would benefit considerably in terms of exchange of information and best practices and assist each other in countering illegal activities, especially in the fight against illegal content on the Internet. In the longer term, this could contribute to strengthening the protection of potential victims and the Information Society industry.

If existing international instruments were used more effectively, this could have enormous positive impacts on the repression of cyber crime in the countries concerned, within the EU as well as outside. Positive impacts could be expected especially with regard to the collaboration between EU and non-EU law enforcers and prosecutors. One negative side effect that can be envisaged is that criminal organizations may move away from countries cooperating with the EU and set up shop in other countries further away, but at international level the option does not imply negative impacts for cooperating countries. An increased level of security could be the overall result, which could in particular have positive effects on the protection of potential victim groups and the further development of Information Society industry.

The social impact of targeted legislation, well assessed and adapted to concrete needs, would probably only be positive in that more legal certainty is achieved. In addition, more extensive and possibly burdensome legislation regarding cyber crime could be avoided.

5.4.2. Economic impacts

The economic impact of a strengthened EU-level law enforcement cooperation is expected to be positive both for the EU and its neighbouring area and at global level, as a decrease in cyber crime would entail fewer losses for internet users, increased trust in the internet by those users and thus higher revenues for businesses with activities on the internet. Few negative economic impacts can be foreseen, with the possible exception of negative economic impacts for countries located outside the EU neighbouring area, as criminal activities may move there as a result. Indeed, it could entail more efficiency regarding investments made in EU bodies, which would be better valorised. With specific regard to the objective of strengthening existing structures, the present institutions may only be able to play a more pro-active role if their financial and human resources are increased. If this measure is not well implemented and financed, it could have the negative impact that these institutions would lose their focus on other policy areas which fall under their remit.

The potential positive economic impact of an EU training and/or research initiative could be significant and cover various dimensions. It would especially help to valorise investments and make them sustainable and to improve knowledge in law enforcement bodies and in the judicial system. The exact economic impact of the initiative is not easy to define as it will be quite indirect, for example through increased efficiency of law enforcement processes and a more efficient split in resource utilisation between the private and public sector for an equivalent result.

Economic impacts of actions to increase EU-level public-private cooperation are hard to predict and must be studied further. The costs of the preliminary study and the costs of institutionalizing information sharing and assembling statistics from different national data bases would certainly be high. On the other hand, if more information could be gathered successfully and if patterns of cyber crime could be identified, this would certainly help in curbing costs emanating from cyber crime.

The strategy to introduce targeted and well assessed legislation could lead to a situation where the possibilities to concentrate efforts on where they are really needed would be increased. This would in turn reduce costs in general. The risk that too many efforts are made at a horizontal level - at the cost of possible concrete and effective projects at a sector-specific, national or regional level - would be minimized.

5.4.3. Costs for public administration

The first direct costs for public administrations incurred would be for increased financial resources which might have to be made available for EU-level cooperation structures and training programmes. Another cost which public administrations might incur would be linked to a study needed in order to understand the factors which until now prevented existing institutions deploying their full powers with pro-active initiatives, and taking relevant measures. There are not likely to be other costs for the public sector, or for other stakeholders.

The cost of the concrete actions, which would be decided at a later stage within the framework of the strategy, would have to be assessed separately at that time, when the concrete actions have been defined in detail. It could however be assumed that the direct costs for public administrations for this option would continue to be limited.

5.4.4. Degree of coherence with policy objectives

This general policy option would fully meet all strategic objectives set out in section 3 above.

5.4.5. Added value and respect of the subsidiarity principle

Coordination of cross-border law enforcement as well as public-private cooperation would add a clear European value, by spreading knowledge of best practices and by making sure that resources are well used. The limited legislation which will be part of this policy will only be proposed if such an added value can clearly be established. The Commission, in cooperation with Member States and other partners, is well placed to coordinate this policy. It will in any case take action in this field only if, and insofar as, the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central, regional or local level, but can rather, by reason of the scale or

effects of the proposed action, be better achieved at Union level. The implementation of certain actions may however be taken at national, sectoral or regional level. The added value of any concrete action subsequent to the adoption of the strategy will be assessed separately.

5.4.6. Feasibility

The success of this general policy option also depends mainly on the willingness of Europol, Eurojust and CEPOL to take on more responsibility in the area of cyber crime, and on Member States to accept that these institutions do indeed get more responsibility. The feasibility appears to be high; existing instruments have already been accepted by Member States and an overwhelming majority of stakeholders would certainly welcome this policy option. Efforts to strengthen public private cooperation and EU and international cooperation in general would also, it seems, be generally acceptable. The political possibility to adopt targeted legislation to support this policy, for example by strengthening Europol, is not assessed in this report. Some resistance can be expected from some Member States and from some national law enforcement bodies and prosecutors, as the criminal domain is still considered part of the "core" of the national culture.

5.4.7. Conclusion

This policy option presents a number of most relevant strategic level actions. Very few negative impacts or major obstacles can be discerned. On the negative side, it could be argued that the direct impacts of the policy are rather modest. This however only goes for the short term perspective; very important impacts may follow when adequate implementation measures are taken. The resulting concrete impacts however remain hard to foresee in detail, since the strategic level will have to be implemented operationally at a later stage. All impacts will be assessed then.

5.5. Choice of policy option

Already a preliminary analysis, on the basis of the assessments made here above and opinions expressed during the Commissions' own informal and formal stakeholder consultations, has clearly pointed at option 4 as the best alternative. Option 4 is also clearly the option which best responds to the general objectives indicated in section 2.4 above.

The option to take no action at all in this field does not seem to be viable. A passive approach would be likely to result in numerous bilateral cooperation projects on the fight against cyber crime continuing to exist without any possibility to take advantage of a horizontal exchange of best practices or synergy effects. General legislation to create new EU bodies, to harmonize crime definitions and to clarify responsibilities and liabilities of all stakeholders could be interesting, but an analysis of the political situation has clearly shown that proposals for general and horizontal legislation would stand very small chances to be adopted. Furthermore, very few of the stakeholders consulted believed that this can be the most important priority now. General legislation may however still be of relevance in a long-term perspective. The creation of new informal structures for the EU-level law enforcement or public-private cooperation might also be a good idea in a long term perspective, but all stakeholders seem to agree that the existing structures are sufficient, even if they urgently need to be made more effective. As a result of the

analysis, the preference has thus been given to option 4, "a coherent strategy". It should be noted that that option does not exclude that a formal structure is created (option 3) or that general legislation (option 2) is adopted later. The preferred option does in fact mean that the doors for new actions are held open.

The preparatory analysis and the discussions held clearly show that the "coherent strategy" is the option which is most likely to achieve the objective of making Europe more secure with respect to the cyber crime threat. Such a strategy is likely to have significant positive impacts on the fight against cross-border cyber crime, since the competencies and roles of all involved in the fight will be clarified and strengthened. It would also contribute to a better dialogue and understanding between the public and private sectors, which in turn could have many positive side effects. From an economic point of view, the preferred option may lead to important synergy effects, decreased level of harm from criminal activities and decreased costs for individual security programmes.

It is however likely that it will take a few years for the expected effects under the chosen option to materialise. It is thus hard to assess all its potential impacts now. This is even more the case since the concrete details of the policy remain to be decided. It will thus be necessary to assess the specific impacts of concrete elements of the policy at a later stage.

6. DATA PROTECTION AND FUNDAMENTAL RIGHTS ISSUES

A number of the options mentioned above could affect fundamental rights, such as the right to respect for private and family life and the right to data protection. When the exact conditions of implementations of preferred options have been settled, an assessment of the impacts of these options with respect to fundamental rights should thus be done.

The Commission is of the opinion that the options presented above, if implemented correctly, would in principle not have a negative impact on fundamental rights. It can however not be excluded that negative effects could occur, depending on the specific modalities and conditions of the implementation. The Commission is taking this risk seriously and will make sure that the policy on the fight and prosecution of cyber crime will be defined and implemented in a manner which fully respects fundamental rights, in particular the freedom of expression, the right to respect for private and family life and the protection of personal data. Any legislative action which will be taken in the framework of this policy will be scrutinised for compatibility with the Charter of Fundamental Rights, in accordance with the Commission Communication on the compliance with the Charter in Commission legislative proposals adopted in 2005 - COM(2005) 172.

7. THE PREFERRED POLICY OPTION: THE MAIN ASPECTS OF THE POLICY AND IMPACTS

The option consisting of a coherent strategy on the fight against cyber crime has thus been chosen. This strategy will give the European Commission a central coordinating role in Europe. With regard to its limited competence in this field, it is clear that the Commission will play this role only when a clear added value can be established. The Commission will closely coordinate all actions with Member States and other competent bodies. The concrete policy can be divided into four main policy areas or instruments:

7.1. Improved European law enforcement cooperation

The main feature of this policy instrument is a proactive policy in reinforcing the structures for operational law enforcement cooperation. The Commission will launch a reflection on how this cooperation can be strengthened and improved. This will mainly be done through the organisation of a European law enforcement conference, and possibly – if this is considered necessary after initial discussion – through a decision to set up a specific task force/working group. The discussions may also lead to a formal proposal to strengthen existing structures, especially the high-tech crime work at Europol and Eurojust. The policy instrument includes actions to improve exchange of information and best practices, initiatives to improve training and awareness-raising within law enforcement authorities.

7.2. Increased European public-private cooperation

This policy instrument aims at strengthening existing public-private cooperation against cyber crime and to create new public-private projects. The Commission will organise a major conference in order to consider how cooperation can be strengthened concerning areas such as the fight against illegal content (such as child pornography and incitement to terrorism) on the Internet, Botnets and other illegal activities. The Commission will especially promote an atmosphere of confidence between the sectors, which could facilitate effective and rapid actions against illegal activities. The Commission will also support ad hoc initiatives for better cooperation against specific problems. This policy instrument also includes exchange of information and best practices, initiatives to improve training, relevant research and awareness-raising in both the public and private sector.

7.3. International cooperation

This policy instrument aims at better coordinating EU actions against cyber crime with external and international initiatives. In fact, cyber crime in Europe is a phenomenon which may originate or have its effects far beyond the borders of the EU. A global approach is thus especially needed when it comes to the fight against this type of crime. The Commission will promote a common European approach to international cooperation in this field and also take a proactive role in international projects such as the ones initiated by Interpol, the Council of Europe or the G 8 Roma-Lyon High-tech crime group. The policy instrument also includes exchange of information and best practices and initiatives to improve training and relevant research.

7.4. Legislation

As has been made clear above, no general legislation on the fight against cyber crime can be expected to be effective at this moment. However, legislation can be an effective instrument when the three policy instruments just mentioned prove insufficient. Targeted legislative actions may also prove to be appropriate or needed in specific areas. As an example, the Commission will consider an initiative regarding European legislation against identity theft in 2007. Legislative action could also include developing a regulation on the responsibility of different actors in the relevant sector.

8. MONITORING AND EVALUATION

In order to measure progress made in the strategy for the fight against cyber crime described above, it is necessary to follow-up and monitor the process. This is also needed in order to decide whether legislative measures, which would be more general in nature, would be more appropriate than the instruments suggested here.

The preferred option discussed above is an EU strategy mainly consisting of reinforced dialogue and cooperation networks. The success of such actions is by its nature very hard to measure, but this is also due to the limited competences at the EU level. Most work against cyber crime will still be carried out at the national level and the specific effects of EU action will be hard to define and measure. One part of the strategy, however, consists of a number of actions planned to be taken in the period 2007-2009. The Commission will assess how these actions have been implemented and report to the Council and the Parliament in 2010.

Depending on the outcome of discussions at the conferences foreseen in 2007 and developments in the field of fight against cyber crime, the Commission may also decide to propose new legislative or other targeted actions. Specific impact assessments such actions will then be carried out as appropriate.

As for the global strategy, the following preliminary set of key indicators could be considered:

- The number of successful meetings and conferences organised in the relevant area
- The quantified and qualitatively perceived change in exchanged strategic information in this field between national law enforcement authorities
- The quantified and qualitatively perceived change in exchanged strategic information in this field between the public and the private sector

EUROOPAN UNIONIN NEUVOSTO

Bryssel, 30. toukokuuta 2007 (03.07)
(OR. en)

10089/07
ADD 2

CRIMORG 102

LISÄYS SAATTEESEEN

Lähettäjä:	Euroopan komission pääsihteerin puolesta Jordi AYET PUIGARNAU, johtaja
Saapunut:	24. toukokuuta 2007
Vastaanottaja:	Javier SOLANA, pääsihteeri, korkea edustaja
Asia:	Komission yksiköiden valmisteluasiakirja *Oheisasiakirja asiakirjaan:* Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle – tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi = vaikutustenarviointi: tiivistelmä

Valtuuskunnille toimitetaan oheisena komission asiakirja SEC(2007) 641.

Liite: SEC(2007) 641

EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 22.5.2007
SEK(2007) 641

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

Oheisasiakirja asiakirjaan:

KOMISSION TIEDONANTO
NEUVOSTOLLE, EUROOPAN PARLAMENTILLE
JA ALUEIDEN KOMITEALLE

Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi

VAIKUTUSTENARVIOINTI: TIIVISTELMÄ

{KOM(2007) 267 lopullinen}
{SEK(2007) 642}

TIIVISTELMÄ

1. JOHDANTO

Internetin käyttö on lisääntynyt räjähdysmäisesti viime vuosina, ja uusien ilmiöiden ja tekniikoiden käyttöönotto on lisännyt turvattomuutta.

Komissio katsoi **vuoden 2007 lainsäädäntö- ja työohjelmassaan**, että tietoverkkorikollisuutta koskeva komission politiikka on uudistettava perusteellisesti, ja ilmoitti sen vuoksi antavansa tiedonannon tietoverkkorikollisuutta koskevasta EU:n politiikasta.

Kuulemismenettelyn aikana kävi ilmi, että asiaa koskevat tiedot ja tilastot ovat puutteelliset. Sen vuoksi komissio tilasi vuonna 2006 asiasta **ulkopuolisen tutkimuksen**[1], johon tämä vaikutustenarviointi etupäässä perustuu.

Valmistelutyön aikana komissio on analysoinut useita säädöksiä ja muita toimenpiteitä erityisesti löytääkseen nykyisten sääntelypuitteiden aukot. On huomattava, että komissio on asettanut etusijalle **tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen**[2] (’yleissopimus’) ja **puitepäätöksen tietojärjestelmiin kohdistuvista hyökkäyksistä**[3], sillä mainitut asiakirjat ovat sekä aineellisen oikeuden että prosessioikeuden kannalta kattavimmat välineet.

Komissio valmistelee näiden toimien pohjalta uutta yleistä toiminta-aloitetta, joka käsittää tiedonannon tietoverkkorikollisuuden torjunnasta EU:n tasolla. Tässä vaikutustenarvioinnissa käsitellään siis lähinnä strategisia kysymyksiä.

Komissio on sitoutunut huolehtimaan siitä, että tietoverkkorikollisuuden torjuntaa ja syytteeseenpanoa koskeva toimintalinja määritellään ja pannaan täytäntöön perusoikeuksia ja erityisesti sananvapautta, yksityis- ja perhe-elämää sekä henkilötietojen suojaa kunnioittaen. Tässä yhteydessä otetaan lisäksi huomioon vuonna 2005 annettu komission tiedonanto *Perusoikeuskirjan noudattaminen komission lainsäädäntöehdotuksissa* [KOM(2005) 172].

---

1 *Study to Assess the Impact of a Communication on Cyber Crime,* Yellow Window Management Consulting (sopimus nro DG 2006/JLS D 2/03).

2 Vuonna 2001 tehty tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

3 Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä.

2. ONGELMAT JA TAVOITTEET

Internetin ja muiden tietojärjestelmien nopea kehitys on synnyttänyt kokonaan uuden taloudenalan ja johtanut tietojen, tuotteiden ja palvelujen nopeaan siirtymiseen EU:n sisä- ja ulkorajojen yli. Tällä on luonnollisesti ollut useita myönteisiä seurauksia kuluttajien ja kansalaisten kannalta. Sama kehityssuuntaus on kuitenkin luonut myös paljon uusia mahdollisuuksia rikollisille. Nykyään on selvästi havaittavissa uusi rikollisuuden suuntaus, joka kohdistuu Internetiin ja toisaalta hyödyntää tietojärjestelmiä välineenä. Nämä uudet rikollisuuden muodot muuttuvat jatkuvasti, joten lainsäätäjän ja lainvalvojien on vaikea pysyä niiden jäljillä. Lisäksi tietoverkkorikollisuuden kansainvälinen luonne edellyttää rajat ylittävän lainvalvontayhteistyön kehittämistä.

Ongelmaa voidaan tarkastella lähemmin seuraavien kahdeksan strategisen ongelma-alueen kautta:

- yhteiskunnan, liike-elämän ja kansalaisten lisääntyvä alttius tietoverkkorikollisuuden riskeille
- tietoverkkorikosten lisääntyminen ja kehittyminen
- tietoverkkorikollisuuden torjuntaa koskevan johdonmukaisen EU:n politiikan ja lainsäädännön puute
- tietoverkkorikollisuutta koskevan operatiivisen lainvalvontayhteistyön erityisongelmat
- tietämyksen ja teknisten välineiden vajavuus: tarve kehittää koulutusta ja tutkimusta
- toimivien järjestelyjen puuttuminen julkisen ja yksityisen sektorin keskeisten toimijoiden yhteistyötä varten
- velvollisuuksien ja vastuiden epäselvä määrittely
- puutteellinen tietämys tietoverkkorikollisuuden aiheuttamista riskeistä

On huomattava, että kaikki sidosryhmät – sekä lainvalvontaviranomaiset että yritykset – esittivät tätä raporttia varten järjestetyissä kuulemisissa hämmästyttävän yhteneviä näkemyksiä EU:n nykyisistä ongelmista tällä alalla.

2.1. Keitä ongelma koskee?

Tietoverkkorikollisuus koskettaa kaikkia yhteiskunnan osa-alueita, ja sen torjumiseen tähtäävä politiikka tulee väistämättä näkymään lähes kaikkialla yhteiskunnassa. Koska useimmilla kansalaisilla on käytössään tietokone, kaikki tietoverkkorikollisuuden torjunnan alalla tehtävät aloitteet vaikuttavat lähes kaikkiin kansalaisiin – jo pelkästään siitä syystä, että he ovat tietoverkkorikosten mahdollisia uhreja.

On kuitenkin olemassa selviä viitteitä siitä, että rikolliset kohdistavat toimintansa yhä enemmän tiettyihin kohderyhmiin. Tehokkaasta tietoverkkorikollisuuden torjuntapolitiikasta voisikin olla selvää hyötyä kyseisille ryhmille. Asia koskettaa läheisesti tietoyhteiskuntaan liittyvää elinkeinoelämää ja koko tietoyhteiskuntaa, sillä turvallisuuden parantamisella ja turvallisen ilmapiirin luomisella voi olla huomattavat myönteiset taloudelliset vaikutukset.

2.2. Onko EU:lla valtuudet toimia?

Koska tietoverkkorikollisuuteen liittyvät turvallisuusuhat ovat hyvin yleisiä ja laajoja, on niiden torjuminen ensiarvoisen tärkeää. Turvallisuusongelmat ovat maailmanlaajuisia, eikä niitä voida siksi ratkaista pelkästään yksittäisten valtioiden tasolla. Koska uhka on kansainvälinen, myös sen torjuminen edellyttää ainakin osittain kansainvälistä toimintaa. On selvää, että tietoverkkorikollisuuden torjunta on jatkossakin tärkeintä ja tehokkainta kansallisella tasolla. Sen lisäksi on kuitenkin tarpeen koordinoida ja mahdollisesti täydentää kansallisia toimia Euroopan tasolla.

2.3. Tavoitteet

Suunnitteilla olevan politiikan strateginen yleistavoite voidaan tiivistää edellä lueteltujen ongelmien pohjalta seuraavasti:

Vahvistetaan ja koordinoidaan tietoverkkorikollisuuden torjuntaa kansallisella, Euroopan ja kansainvälisellä tasolla.

Tämä strateginen yleistavoite voidaan jakaa seuraaviin viiteen osatavoitteeseen, jotka on lueteltu alustavassa tärkeysjärjestyksessä:

- Parannetaan rajat ylittäviä operatiivisia lainvalvontatoimia tietoverkkorikollisuuden ja erityisesti sen vakavien muotojen torjumiseksi sekä tehostetaan tietojen, tiedustelutiedon ja parhaiden käytänteiden vaihtoa lainvalvontaviranomaisten kesken sekä jäsenvaltioiden sisällä että niiden välillä.

- Kehitellään ja luodaan operatiivisia välineitä julkisen ja yksityisen sektorin yhteistyötä sekä yhteisten tavoitteiden määrittämistä varten ja parannetaan tietoverkkorikollisuuden torjuntaan liittyvien tietojen, tiedustelutiedon ja parhaiden käytänteiden vaihtoa julkisen ja yksityisen sektorin välillä EU:n tasolla.

- Perustetaan poliittinen foorumi ja muita rakenteita tietoverkkorikollisuuden torjuntaa koskevan EU:n politiikan kehittämiseksi yhteistyössä jäsenvaltioiden ja toimivaltaisten EU:n elinten sekä kansainvälisten organisaatioiden kanssa ja tehostetaan voimassa olevia oikeudellisia ja institutionaalisia puitteita, myös selkeyttämällä velvollisuuksien ja vastuiden jakoa kaikkien toimijoiden välillä.

- Torjutaan tietoverkkorikollisuuden vakavien muotojen aiheuttamaa kasvavaa uhkaa parantamalla taitoja, tietoja ja teknisiä välineitä; tämä käsittää toimet koulutuksen ja tutkimuksen lisäämiseksi.

- Lisätään erityisesti kuluttajien ja muiden tietoverkkorikoksille alttiiden ryhmien tietämystä tietoverkkorikollisuuden aiheuttamasta uhasta.

3. STRATEGISET TOIMINTAVAIHTOEHDOT

Tietoverkkorikollisuuden monimuotoisuus edellyttää, että myös sen torjuntaa koskevan toimintapolitiikan on oltava monitahoista. Ollakseen mahdollisimman tehokasta sen on käsitettävä perinteisten lainvalvontatoimien ohella muita välineitä, kuten itsesääntelyä ja eri sidosryhmien välisiä yhteistyöjärjestelyjä. Edellä on kuvattu useita ongelma-alueita ja tämän aloitteen strategisia tavoitteita. Tavoitteiden saavuttaminen edellyttää useita erilaisia ja koordinoituja toimia. Komissio on muotoillut laajojen kuulemismenettelyjen pohjalta neljä yleistä toimintavaihtoehtoa, joista kukin käsittää useita erityistoimia.

3.1. Toimintavaihtoehto 1: tilanne jatkuu ennallaan / ei merkittäviä uusia toimia

Jos tämä vaihtoehto valitaan, komissio ei tässä vaiheessa ryhdy asiassa yleisiin horisontaalisiin toimiin. Tämän vaihtoehdon mukaan:

- Komissio jatkaa kohdennetun lainsäädännön tai toimintapolitiikan tarpeen arvioimista ja ryhtyy tarvittaessa asianmukaisiin toimiin.

- Komissio seuraa käynnissä olevia EU:n ja kansainvälisiä hankkeita, jotka liittyvät tietoverkkorikollisuuden torjuntaan.

- Komissio käynnistää uusia hankkeita tietoverkkorikollisuuden torjunnan kannalta keskeisillä aloilla, mutta ei tee lainkaan horisontaalisia aloitteita.

3.2. Toimintavaihtoehto 2: yleinen lainsäädäntö

Tässä vaihtoehdossa aletaan toteuttaa politiikkaa, jonka mukaan EU:ssa otetaan asteittain käyttöön yleiset sääntelypuitteet tietoverkkorikollisuuden torjuntaa varten. Tällainen politiikka käsittäisi esimerkiksi seuraavat toimet:

- Komissio ehdottaa systemaattisesti yhdenmukaisia tai yhtenäisiä rikosten määritelmiä erityisesti EU:ta varten mutta myös kansainvälisellä tasolla.

- Komissio ehdottaa EU:n yhteisiä vähimmäisstandardeja, jotka koskevat kriminalisointia ja rangaistusten määräämistä.

- Luodaan viralliset foorumit julkisen ja yksityisen sektorin yhteistyötä sekä koulutusta ja tutkimusta varten.

- Perustetaan lainvalvontaviranomaisten virallinen verkosto.

3.3. Toimintavaihtoehto 3: luodaan julkisen ja yksityisen sektorin epävirallisia verkostoja tietoverkkorikollisuuden torjuntaa varten

Tässä vaihtoehdossa komissio perustaa joko yksin tai muiden toimielinten kanssa tietoverkkorikollisuuden asiantuntijoiden verkostoja tai ryhmiä sekä ottaa käyttöön vapaaehtoisen turvallisuusmerkintäjärjestelmän operaattoreita, tuottajia ja kuluttajia varten. Vaihtoehto käsittää esimerkiksi seuraavat toimet:

- Perustetaan tietoverkkorikollisuuteen erikoistuneiden lainvalvonta-alan asiantuntijoiden epävirallinen ryhmittymä.

- Perustetaan tietoverkkorikollisuuteen erikoistuneiden julkisen ja yksityisen sektorin asiantuntijoiden epävirallinen foorumi/verkosto.

3.4. Toimintavaihtoehto 4: johdonmukainen strateginen lähestymistapa

Tämän vaihtoehdon mukaan EU:n tasolla otetaan käyttöön johdonmukainen strategia tietoverkkorikollisuuden torjumiseksi. Siihen kuuluisi keskeisenä osana strategisten puitteiden luominen tietoverkkorikollisuuden torjuntaa koskevalle EU:n politiikalle. Yleisenä tavoitteena olisi koordinoida käytännön toimia entistä tehokkaammin ja optimoida nykyisten välineiden käyttö. Muita strategian keskeisiä toimia ovat:

- Parannetaan lainvalvontayhteistyötä EU:n tasolla.

- Otetaan käyttöön strategiset järjestelyt tietoverkkorikollisuuden torjuntaan tähtäävää julkisen ja yksityisen sektorin yhteistyötä varten.

- Edistetään kansainvälisten yhteistyöpuitteiden luomista.

- Tehdään tarvittaessa kohdennettuja säädösaloitteita.

4. TOIMINTAVAIHTOEHTOJEN ARVIOINTI JA TOIMINTAVAIHTOEHDON VALINTA

4.1. Arviointi

Yleisiä toimintavaihtoehtoja arvioitiin seuraavin perustein:

- yhteiskunnalliset vaikutukset

- taloudelliset vaikutukset

- hallinnolliset kustannukset

- yhdenmukaisuus poliittisten tavoitteiden kanssa

- lisäarvo ja subsidiariteettiperiaatteen noudattaminen

- toteutettavuus

Arvioinnin tulokset olivat lyhyesti seuraavat:

4.1.1. Toimintavaihtoehto 1

Tätä toimintavaihtoehtoa ei pidetty riittävänä nykyisten haasteiden ratkaisemiseksi. ”Ei uusia toimia” -vaihtoehdon vaikutukset ovat periaatteessa rajalliset. On kuitenkin vaikea arvioida, onko tällä vaihtoehdolla mahdollisesti merkittäviä haittavaikutuksia tulevaisuudessa, koska tietoverkkorikollisuuden tulevista kehityssuuntauksista ei ole tietoa. Tämän vaihtoehdon potentiaaliset negatiiviset vaikutukset ovat pitkällä aikavälillä hyvin suuret, sillä tietoverkkorikollisuus on jo nykyisinkin hyvin laajaa ja todennäköisesti kasvaa tulevaisuudessa.

4.1.2. Toimintavaihtoehto 2

Komissio tuli siihen tulokseen, että tätä toimintavaihtoehtoa olisi toteutettava hyvin varovaisesti ja sen vaikutukset näkyisivät vasta pitkällä aikavälillä. Tämä vaihtoehto edellyttää ehdottomasti oikeudellisen toteuttamiskelpoisuuden tutkimista ja pitkiä poliittisia neuvotteluja. Tällä vaihtoehdolla voi olla hyvin merkittävät vaikutukset. Koska on kuitenkin epätodennäköistä, että tämä vaihtoehto edistäisi toimintaa lyhyellä aikavälillä, on vaihtoehto epävarma lyhyen aikavälin kannalta. Lisäksi voidaan kysyä, toteutuisivatko asetetut tavoitteet yhtä tehokkaasti täytäntöönpanon tasolla kuin poliittisella ja teoreettisella tasolla. Jos tämä vaihtoehto valitaan, on vaarana, että tietoverkkorikollisuuden torjunnan käytännön puolta ei oteta riittävästi huomioon strategisessa poliittisessa päätöksenteossa. Koska tämän vaihtoehdon vaikutukset olisivat huomattavat, komission roolia olisi selkeytettävä. Lisäksi samoihin tuloksiin voitaisiin mahdollisesti päästä myös vähemmän intensiivisillä toimilla.

4.1.3. Toimintavaihtoehto 3

Tätä vaihtoehtoa pidettiin hyvin kiinnostavana strategiselta kannalta, vaikka sen tuomaa lisäarvoa ja käytännön vaikutuksia on vaikea ennustaa. Vaarana on, että uudet verkostorakenteet eivät välttämättä johtaisi käytännön tuloksiin. Komissio kykenisi parhaiten koordinoimaan alalla toteutettavia itsesääntelytoimia, mutta tässä vaihtoehdossa komission tehtävänä olisi toimia paremminkin koordinaattorina ja välittäjänä kuin strategisena johtajana.

4.1.4. Toimintavaihtoehto 4

Tämän toimintavaihtoehdon katsottiin käsittävän useita keskeisimpiä strategisia toimia. Vaihtoehtoon liittyy hyvin vähän kielteisiä vaikutuksia tai huomattavia esteitä. Kielteisenä puolena voidaan pitää sitä, että vaihtoehdon välittömät vaikutukset ovat melko vaatimattomat. Tämä pätee kuitenkin ainoastaan lyhyellä aikavälillä. Sen sijaan tällä vaihtoehdolla voidaan aikaansaada hyvin merkittäviä vaikutuksia siinä vaiheessa, kun riittävät täytäntöönpanotoimet on otettu käyttöön. Käytännön vaikutuksia on vaikea ennustaa yksityiskohtaisesti, sillä strateginen puoli pannaan täytäntöön vasta myöhemmässä vaiheessa. Vaikutukset on tarkoitus arvioida vasta siinä vaiheessa.

On korostettava jälleen sitä, että ehdotettujen toimintavaihtoehtojen suorat vaikutukset ovat rajalliset ja että valitun vaihtoehdon puitteissa myöhemmin toteutettavia yksittäisiä toimia on tarkoitus arvioida vasta niiden täytäntöönpanovaiheessa. Tämä arvio on siis vasta alustava.

4.2. Toimintavaihtoehdon valinta

Arvioinnin nojalla selvästi paras vaihtoehto on numero 4. Lisäksi vaihtoehto 4 vastaa ehdottomasti parhaiten edellä 2.4 kohdassa lueteltuja yleisiä tavoitteita.

”Ei toimia” -vaihtoehto ei vaikuta toteuttamiskelpoiselta. Passiivinen lähestymistapa johtaisi todennäköisesti siihen, että maat jatkaisivat lukuisia kahdenvälisiä yhteistyöhankkeitaan tietoverkkorikollisuuden torjunnan alalla, jolloin osapuolet eivät voisi hyödyntää parhaiden käytäntöjen vaihtamista tai synergiaetuja. Uusien EU:n elinten luomista, rikosten määritelmien yhtenäistämistä sekä sidosryhmien velvollisuuksien ja vastuiden määrittelemistä koskeva yleinen lainsäädäntö saattaisi olla hyödyllistä, mutta poliittisen tilanteen arvioinnin perusteella näyttää selvästi siltä, että yleistä lainsäädäntöä ja horisontaalista lainsäädäntöä koskevilla ehdotuksilla on hyvin pienet mahdollisuudet tulla hyväksytyiksi. Lisäksi kuulemiseen osallistuneista sidosryhmistä vain harva piti yleistä lainsäädäntöä ensisijaisena toimintatapana. Yleisellä lainsäädännöllä saattaa kuitenkin olla merkitystä pitkällä aikavälillä. Uusien epävirallisten järjestelyjen käyttöönotto EU:n tasolla tapahtuvaa lainvalvonta-alan tai julkisen ja yksityisen sektorin yhteistyötä varten saattaisi myös olla hyvä ajatus pitkällä aikavälillä, mutta kaikki sidosryhmät näyttävät olevan yhtä mieltä siitä, että nykyiset yhteistyöjärjestelyt riittävät, vaikkakin niitä olisi viipymättä tehostettava. Arvioinnin perusteella etusijalle asetetaan siis vaihtoehto 4: johdonmukainen strategia. Olisi huomattava, että tässä vaihtoehdossa ei ole suljettu pois mahdollisuutta ottaa käyttöön muodollisia rakenteita (vaihtoehto 3) tai antaa myöhemmin yleistä lainsäädäntöä (vaihtoehto 2). Itse asiassa etusijalle asetettu vaihtoehto tarkoittaa sitä, että kaikki uudet toimet ovat mahdollisia.

Alustavan arvioinnin ja keskustelujen pohjalta on käynyt selvästi ilmi, että johdonmukainen strategia on todennäköisesti tehokkain keino strategisten tavoitteiden saavuttamiseksi. Strategialla on todennäköisesti hyvin merkittävät positiiviset vaikutukset tietoverkkorikollisuuden torjuntaan, sillä siinä selkeytetään ja vahvistetaan kaikkien osapuolten valmiuksia ja tehtäviä. Lisäksi strategia tukee tehokkaampaa vuoropuhelua ja lisää ymmärrystä julkisen ja yksityisen sektorin välillä, mikä saattaa puolestaan synnyttää useita myönteisiä sivuvaikutuksia. Valitulla vaihtoehdolla voi olla useita taloudellisia vaikutuksia: huomattavat synergiaedut, rikollisuuden aiheuttamien haittojen väheneminen ja yksityisistä turvaohjelmista koituvien kulujen pieneneminen.

On kuitenkin todennäköistä, että kestää muutaman vuoden, ennen kuin valitun vaihtoehdon vaikutukset alkavat näkyä. Sen takia toimintavaihtoehdon kaikkia mahdollisia vaikutuksia on vaikea arvioida tässä vaiheessa. Tämä johtuu etenkin siitä, että politiikan käytännön yksityiskohdista ei ole vielä päätetty. Toimintapolitiikkaan kuuluvien käytännön toimien vaikutuksia on siis arvioitava myöhemmin.

EUROPEISKA UNIONENS RÅD

Bryssel den 30 maj 2007 (3.7)
(OR. en)

10089/07
ADD 2

CRIMORG 102

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
mottagen den:	24 maj 2007
till:	Javier SOLANA, generalsekreterare/hög representant
Ärende:	Arbetsdokument från kommissionens avdelningar *Medföljande dokument till ett* meddelande från kommissionen till Europaparlamentet, rådet och Europeiska unionens regionkommitté – Att införa en allmän politik för kampen mot IT-relaterad brottslighet = Sammanfattning av konsekvensanalysen

För delegationerna bifogas kommissionens dokument – SEK(2007) 641.

Bilaga: SEK(2007) 641

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 22.5.2007
SEK(2007) 641

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

Medföljande dokument till ett

**MEDDELANDE FRÅN KOMMISSIONEN
TILL EUROPAPARLAMENTET, RÅDET
OCH EUROPEISKA UNIONENS REGIONKOMMITTÉ**

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

SAMMANFATTNING AV KONSEKVENSANALYSEN

{KOM(2007) 267 slutlig}
{SEK(2007) 642}

SAMMANFATTNING

1. INLEDNING

Användningen av Internet har exploderat under senare år och framkomsten av nya fenomen och nya tekniker har skapat en situation med allt större osäkerhet.

Kommissionen anförde i sitt **lagstiftnings- och arbetsprogram 2007** att det krävs en omfattande uppdatering av kommissionens politik på området för IT-relaterad brottslighet och aviserade därför att ett meddelande om IT-relaterad brottslighet skulle utarbetas.

Under det inledande samrådsförfarandet framgick det klart att det saknas uppgifter och statistik, vilket var ett av de främsta skälen till att kommissionen beställde en **extern undersökning**[1] 2006, som konsekvensanalysen till största del bygger på.

Under det förberedande arbetet har kommissionen också analyserat ett antal lagstiftningsåtgärder och andra åtgärder, särskilt vad avser eventuella luckor i den nuvarande lagstiftningsramen. Särskild hänsyn har tagits till **Europarådets konvention om IT-relaterad brottslighet**[2] och **rådets rambeslut om angrepp mot informationssystem**[3], eftersom dessa texter ansågs vara de mest omfattande i fråga om materiell rätt och processrätt.

På grundval av dessa åtgärder håller kommissionen på att utarbeta ett nytt initiativ till allmän politik, nämligen ett meddelande om kampen mot IT-relaterad brottslighet på EU-nivå. Den här konsekvensbedömningen kommer i huvudsak handla om strategiska frågor.

Kommissionen vill i detta sammanhang betona att den strävar efter att utforma och tillämpa politiken för att bekämpa och lagföra IT-relaterad brottslighet på ett sätt som respekterar de grundläggande rättigheterna, särskilt yttrandefriheten, rätten till respekt för privatliv och familjeliv och skyddet av personuppgifter. Det kommer att ske i överensstämmelse med kommissionens meddelande om hur respekten för stadgan om de grundläggande rättigheterna skall upprätthållas i kommissionens lagstiftningsförslag [KOM(2005) 172]

---

1 *Study to Assess the Impact of a Communication on Cyber Crime*, utarbetad av Yellow Window Management Consulting (kontrakt nr DG 2006/JLS D 2/03).

2 Europarådets konvention om IT-relaterad brottslighet från 2001, se http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3 Rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem.

2. PROBLEM OCH MÅL

Den snabba utvecklingen av Internet och andra informationssystem har lett till att en helt ny ekonomisk sektor har skapats och till nya snabba flöden av information, varor och tjänster över EU:s inre och yttre gränser. Detta har naturligtvis haft många positiva följder för konsumenter och medborgare. Samma utveckling har dock även öppnat många nya möjligheter för brottslingar. Man kan tydligt urskilja ett mönster av ny brottslig verksamhet mot Internet eller brottslighet där informationssystem används som ett brottsverktyg. Denna brottsliga verksamhet utvecklas ständigt och det är svårt för lagstiftningen och den operativa brottsbekämpningen att hålla jämna steg med utvecklingen. Eftersom denna nya typ av brottslighet har en inneboende gränsöverskridande karaktär måste även det gränsöverskridande brottsbekämpande samarbetet förbättras.

Följande åtta strategiska problemområden har tagits upp i den närmare undersökningen av det övergripande problemet.

- Samhällets, näringslivets och medborgarnas allt större sårbarhet för IT-relaterad brottslighet.
- Den IT-relaterade brottsligheten blir allt vanligare och alltmera sofistikerad.
- Det saknas en sammanhängande politik och lagstiftning på EU-nivå för kampen mot IT-relaterad brottslighet.
- Det finns särskilda svårigheter med samarbetet kring den operativa bekämpningen av IT-relaterad brottslighet.
- Det finns ett behov av att utveckla kompetens och tekniska verktyg: utbildning och forskning.
- Det saknas en funktionell struktur för samarbetet mellan viktiga aktörer inom den offentliga och den privata sektorn.
- Oklar ansvarsfördelning.
- Bristande medvetenhet om riskerna med IT-relaterad brottslighet.

Det bör noteras att alla berörda parter (såväl brottsbekämpande myndigheter som privata företag) som har lämnat synpunkter under samrådet i samband med denna rapport har varit slående eniga om vilka de nuvarande problemen för EU är på detta område.

2.1. Vem berörs?

IT-relaterad brottslighet berör alla sektorer av samhället och en politik för att bekämpa sådan brottslighet kommer att synas praktiskt taget överallt. Med hänsyn till det mycket stora antal medborgare som använder persondatorer kan varje initiativ för att bekämpa IT-relaterad brottslighet påverka de flesta enskilda medborgare – redan i deras egenskap av potentiella brottsoffer.

Det finns dock även klara tecken på att det finns en ökad brottslig verksamhet som är riktad mot specifika grupper av brottsoffer. En effektiv politik mot IT-relaterad brottslighet måste därför ha tydliga positiva följder för dessa grupper. Verksamheter som har samband med informationssamhället, och informationssamhället i stort, kan förväntas spela en viktig roll i detta sammanhang, med hänsyn till de betydande positiva ekonomiska effekter som kan förväntas uppstå om säkerheten skärps eller om en situation med ökad säkerhet införs.

2.2. Har EU rätt att agera?

Med hänsyn till omfattningen och storleken av säkerhetshoten finns det ett konstant, eventuellt ökande, behov av att avvärja hoten från IT-relaterad brottslighet. Säkerhetsfrågor i samband med IT-relaterad brottslighet har en global dimension och kan därför inte behandlas enbart på nationell nivå. Hotet är internationellt och det måste också åtminstone en del av bemötandet vara. Det råder inga tvivel om att kampen mot IT-relaterad brottslighet även i fortsättningen kommer att föras i första hand och effektivast på nationell nivå, men det finns ett tydligt behov av att sammankoppla och eventuellt komplettera det nationella arbetet på EU-nivå.

2.3. Mål

Det övergripande strategiska målet för den föreslagna politiken, som bygger på de ovan identifierade problemen, kan sammanfattas på följande sätt:

Att stärka och bättre samordna kampen mot IT-relaterad brottslighet på nationell, europeisk och internationell nivå.

Detta övergripande strategiska mål kan delas in i följande fem strategiska delmål. De presenteras i prioritetsordning.

- Att förbättra operativa gränsöverskridande brottsbekämpningsåtgärder avseende IT-relaterad brottslighet i allmänhet och allvarliga former av sådan brottslighet i synnerhet, och att förbättra utbytet av information, underrättelser och bästa metoder mellan brottsbekämpande myndigheter i medlemsstaterna och i länder utanför EU.

- Att identifiera och skapa operativa instrument för samarbete och gemensamt målsättande mellan den offentliga och den privata sektorn och att förbättra utbytet av information, underrättelser och bästa metoder för kampen mot IT-relaterad brottslighet mellan den offentliga och den privata sektorn på EU-nivå.

- Att etablera en politisk plattform och strukturer för utveckling av en konsekvent EU-politik för kampen mot IT-relaterad brottslighet, i samarbete med medlemsstaterna och behöriga EU-organ och internationella organisationer, och att effektivisera befintliga rättsliga och institutionella ramar, även genom att klargöra vilket ansvar alla inblandade aktörer har.

- Att bemöta det växande hotet från allvarliga former av IT-relaterad brottslighet genom att främja kompetens, kunskap och tekniska verktyg, inbegripet åtgärder för att stärka relevant utbildning och forskning.

- Att öka den allmänna medvetenheten om hotet från IT-relaterad brottslighet, särskilt bland konsumenter och andra sårbara grupper av potentiella brottsoffer.

3. VAL AV STRATEGISK POLITIK

All politik för att bekämpa IT-relaterad brottslighet kommer till sin natur att vara mångsidig. För att vara verkligt effektiv måste en sådan politik kombinera traditionell brottsbekämpande verksamhet med andra instrument, t.ex. självreglering och inrättande av strukturer för samarbete mellan olika berörda aktörer. Ett antal problemområden och strategiska mål för detta initiativ har beskrivits ovan. För att uppnå dessa mål måste flera olika och kombinerade åtgärder vidtas. Kommissionen har på grundval av det omfattande samråd som har hållits formulerat fyra alternativ till allmän politik, som vart och ett består av flera specifika åtgärder.

3.1. Alternativ 1: Status quo/ingen viktigare ny åtgärd alls

Detta alternativ skulle innebära att kommissionen i detta skede inte vidtar någon generell övergripande åtgärd. Det skulle innebära följande.

- Kommissionen skulle fortsätta att bedöma behovet av målinriktad lagstiftning eller politisk åtgärd och vidta lämpliga åtgärder när det behövs.

- Kommissionen skulle följa befintliga projekt mot IT-relaterad brottslighet inom EU eller internationellt.

- Kommissionen skulle fortsätta att inleda nya projekt på målinriktade intresseområden för att bekämpa IT-relaterad brottslighet men inte ta några horisontella initiativ.

3.2. Alternativ 2: Generell lagstiftning

Detta alternativ skulle innebära att en politik för att gradvis föreslå en generell lagstiftningsram för kampen mot IT-relaterad brottslighet antas. En sådan politik skulle innebära följande.

- Kommissionen skulle systematiskt föreslå harmoniserade eller enhetliga brottsdefinitioner, särskilt för EU men även på internationell nivå.

- Kommissionen skulle föreslå gemensamma miniminormer för kriminalisering och påföljder inom EU.

- Det skulle skapas formella plattformar på området för samarbete mellan det offentliga och det privata och inom utbildning och forskning.

- Ett formellt nätverk för brottsbekämpning skulle skapas.

3.3. Alternativ 3: Skapande av informella nätverk och nätverk mellan den offentliga och den privata sektorn

Detta alternativ skulle innebära att kommissionen, ensam eller tillsammans med andra institutioner, formellt skulle inrätta nätverk eller grupper för experter på området för IT-relaterad brottslighet och kombinera denna åtgärd med att införa ett frivilligt system för säkerhetscertifiering för operatörer, producenter och konsumenter. Detta skulle innebära följande.

- Det skulle inrättas ett informellt organ för experter inom bekämpning av IT-relaterad brottslighet.
- Det skulle inrättas informell plattform för/ett informellt nätverk av offentliga och privata experter inom IT-relaterad brottslighet.

3.4. Alternativ 4: Ett sammanhängande strategiskt tillvägagångssätt

Detta alternativ skulle innebära att en sammanhängande strategi för kampen mot IT-relaterad brottslighet införs på EU-nivå. Det främsta inslaget i denna strategi skulle vara att det inrättades en strategisk ram för EU:s politik mot IT-relaterad brottslighet, med den generella målsättningen att uppnå bättre vägledning för konkreta åtgärder och en optimal användning av befintliga medel. Andra viktiga operativa inslag i denna strategi skulle vara följande.

- Ett bättre samarbete inom brottsbekämpningen på EU-nivå.
- Införande av en strategisk struktur för samarbete mellan det offentliga och det privata mot IT-relaterad brottslighet.
- Främjande och inrättande av en ram för globalt internationellt samarbete på området.
- Målinriktade lagstiftningsåtgärder när det behövs.

4. BEDÖMNING AV DE OLIKA ALTERNATIVEN OCH VAL AV POLITIK

4.1. Bedömning

De olika alternativen till allmän politik har bedömts utifrån följande kriterier:

- Konsekvenser för samhället
- Ekonomiska konsekvenser
- Kostnader för de offentliga myndigheterna
- Grad av överensstämmelse med politiska mål
- Mervärde och respekt för subsidiaritetsprincipen
- Genomförbarhet

Slutsatserna av bedömningen var i korthet följande:

4.1.1. Alternativ 1

Detta alternativ ansågs vara klart otillräckligt för att ta itu med de befintliga utmaningarna. Följderna av alternativet ”ingen ny åtgärd” är i princip begränsade, med det är svårt att bedöma om det finns en risk för att detta alternativ får betydande konsekvenser, eftersom det inte går att veta vilka framtida brottstyper som kommer att uppstå. De potentiella negativa följderna av att ingen åtgärd vidtas är mycket stora, med hänsyn till att denna brottsform är betydande och kommer att växa ytterligare.

4.1.2. Alternativ 2

Slutsatsen blev att detta alternativ endast kunde användas med stor försiktighet och på lång sikt. Det skulle kräva detaljerade genomförbarhetsstudier och långdragna politiska förhandlingar. Effekterna av detta alternativ kan vara mycket stora, men med hänsyn till att det inte är sannolikt att några verkliga framsteg skulle göras på kort sikt, är alternativet osäkert i ett kortsiktigt perspektiv. Det kan också ifrågasättas om de politiska målsättningarna skulle uppnås lika effektivt i det faktiska genomförandet av de politiska åtgärderna som på politisk och teoretisk nivå. Om man skulle välja detta alternativ finns det risk för att den operativa sidan av kampen mot IT-relaterad brottslighet inte skulle vara tillräckligt delaktig i de strategiska politiska valen och besluten. Eftersom detta alternativ skulle få betydande konsekvenser skulle även kommissionens roll i detta hänseende behöva klargöras. Det skulle eventuellt också kunna hävdas att liknande resultat skulle kunna uppnås med mindre ingripande åtgärder.

4.1.3. Alternativ 3

Detta alternativ bedömdes vara det mest intressanta ur strategisk synvinkel, även om mervärdet och de konkreta verkningarna är svåra att förutse. Risken är att de nya nätverken skulle uppnå få konkreta resultat. Kommissionen skulle vara mycket lämpad att samordna självreglerande åtgärder på området men skulle inom ramen för detta alternativ spela rollen av en samordnare och medlare snarare än en strategisk ledare.

4.1.4. Alternativ 4

Detta alternativ ansågs erbjuda en rad högst relevanta strategiska åtgärder. Endast mycket få negativa effekter eller hinder kan urskiljas. En nackdel kan vara att de direkta verkningarna är ganska blygsamma. Det gäller dock bara på kort sikt, eftersom mycket viktiga verkningar kommer att kunna uppnås om lämpliga genomförandeåtgärder vidtas. Det är dock svårt att i detalj förutse vilka de konkreta verkningarna kommer att bli, eftersom de strategiska aspekterna kommer att behöva genomföras på det operativa planet i ett senare skede. Alla verkningar kommer att bedömas då.

Det bör återigen betonas att de direkta verkningarna av de föreslagna strategierna är begränsade och att specifika åtgärder som vidtas senare inom ramen för någon av dessa strategier kommer att bedömas separat i det skedet. Den bedömning som nu görs är därför preliminär.

4.2. Val av politik

I analysen har alternativ 4 klart framstått som det bästa alternativet. Alternativ 4 är också tydligt det alternativ som bäst svarar mot de generella mål som anges i avsnitt 2.4 ovan.

Alternativet att inte vidta åtgärder alls på detta område förefaller inte hållbart. En passiv hållning skulle troligtvis leda till att det även i fortsättningen skulle pågå ett stort antal bilaterala samarbetsprojekt i kampen mot IT-relaterad brottslighet, utan möjligheter att dra fördel av ett horisontellt utbyte av bästa metoder eller synergieffekter. Generell lagstiftning för att skapa nya EU-organ som skall harmonisera brottsdefinitioner och klargöra olika aktörers ansvar skulle kunna vara ett intressant alternativ, men en analys av den politiska situationen har tydligt visat att det finns mycket små utsikter till att förslag till generell och horisontell lagstiftning skulle antas. Vidare var det bara ett fåtal av de aktörer som uttalade sig under samrådet som ansåg att detta är den viktigaste prioriteringen just nu. Generell lagstiftning kan dock fortfarande vara relevant i ett långsiktigt perspektiv. Skapande av nya informella strukturer för brottsbekämpningen på EU-nivå eller samarbete mellan det offentliga och det privata kan också vara en god idé på lång sikt, men alla berörda aktörer verkar vara eniga om att de befintliga strukturerna är tillräckliga, även om det finns ett brådskande behov av att effektivisera dem. Analysen har således lett till slutsatsen att alternativ 4, ”en sammanhängande strategi”, är att föredra. Det bör noteras att det alternativet inte utesluter att en formell struktur skapas (alternativ 3) eller att generell lagstiftning (alternativ 2) antas senare. Det valda alternativet innebär att man håller dörren öppen för nya åtgärder.

De förberedande analyserna och diskussionerna visar tydligt att alternativet ”en sammanhängande strategi” ger störst sannolikhet för att de strategiska målen för politiken kommer att kunna uppnås. En sådan strategi har sannolikt betydande positiva verkningar för kampen mot gränsöverskridande IT-relaterad brottslighet, eftersom alla inblandades kompetens och roller kommer att klargöras och stärkas. Den skulle också bidra till att uppnå en bättre dialog och förståelse mellan den offentliga och den privata sektorn, vilket i sin tur skulle ge många positiva sidoverkningar. Ur en ekonomisk synvinkel kan detta alternativ leda till betydande synergieffekter, till att brottslig verksamhet ger mindre skadliga verkningar och till att kostnaderna för enskilda säkerhetsprogram sänks.

Det är dock troligt att det kommer att ta några år innan de förväntade effekterna av det valda alternativet inträder. Det är därför svårt att i detta skede bedöma alla potentiella verkningar, särskilt som de konkreta detaljerna i politiken ännu inte har fastställts. Det kommer därför att bli nödvändigt att bedöma de specifika effekterna av de konkreta inslagen i politiken i ett senare skede.