КОМИСИЯ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ

Брюксел, 22.5.2007
COM(2007) 267 окончателен

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА И ЕВРОПЕЙСКИЯ КОМИТЕТ НА РЕГИОНИТЕ

„Към основна политика по отношение на борбата с престъпленията в кибернетичното пространство“

{SEC(2007) 641}
{SEC(2007) 642}

**СЪОБЩЕНИЕ НА КОМИСИЯТА
ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА
И ЕВРОПЕЙСКИЯ КОМИТЕТ НА РЕГИОНИТЕ**

„Към основна политика по отношение на борбата с престъпленията в кибернетичното пространство“

1. ВЪВЕДЕНИЕ

1.1. Какво представлява престъплението в кибернетичното пространство?

Сигурността на нарастващите по значимост в съвременното общество информационни системи обхваща много аспекти, от които борбата срещу престъпленията в кибернетичното пространство представлява основен елемент. Без общоприето понятие за престъпление в кибернетичното пространство, понятията „престъпление в кибернетичното пространство“, „компютърно престъпление“, „свързано с компютрите престъпление“ или „престъпление в сферата на високите технологии“ се използват често като взаимозаменяеми. За целите на настоящото съобщение под „престъпление в кибернетичното пространство“ следва да се разбира „престъпни деяния, извършени посредством използване на електронни съобщителни мрежи и информационни системи или срещу такива мрежи и системи“.

В действителност, понятието „престъпление в кибернетичното пространство“ се отнася до три категории престъпни деяния. Първата обхваща **традиционните видове престъпление** като измама или фалшификация, въпреки че в контекста на престъпленията в кибернетичното пространство тази категория се отнасят по-конкретно до престъпления, извършени посредством електронни съобщителни мрежи и информационни системи (наричани по нататък: електронни мрежи). Втората се отнася до публикуването в електронна медия на **незаконно съдържание** (например материали - детска порнография или подбуждащи расова омраза). Третата включва **престъпленията, характерни единствено за електронните мрежи**, например атаки срещу информационни системи, отказ на услуга и чужд достъп (хакерство). Тези видове атаки могат да бъдат насочени също срещу изключително важни инфраструктури в Европа и да засегнат, с потенциално гибелни последици за цялото общество, съществуващите в много райони системи за бърза тревога. Общото за всички категории на престъпление е това че, те могат да бъдат извършени в масов мащаб и да има голямо географско разстояние между престъпното деяние и последиците от него. В резултат на това, техническите аспекти на прилаганите методи за разследване често са същите. Настоящото съобщение се съсредоточава върху тези прилики.

1.2. Последни тенденции на развитие в областта на престъпленията в кибернетичното пространство

1.2.1. Обща характеристика:

Комбинацията от постоянно развиващи се престъпни дейности и липсата на сигурна информация затруднява получаването на точна представа за настоящата ситуация. Независимо от това се очертават някои общи характеристики.

- Броят на престъпленията в кибернетичното пространство нараства и престъпните дейности стават все по-усложнени и излизат извън границите на една държава[1].

- Ясни показатели говорят за нарастващо участие на организирани престъпни групи в престъпленията в кибернетичното пространство.

- Въпреки това, броят на европейските съдебни преследвания, осъществени въз основа на трансграничното сътрудничество в правоприлагането не се увеличава.

1.2.2. Традиционни престъпления в електронните мрежи

Повечето от престъпленията могат да се извършат посредством използването на електронни мрежи. Особено честа и растяща форма на престъпление в електронните мрежи са измамата и опита за измама. Кражба на самоличност, фишинг[2], нежелани съобщения (спам) и зловредни кодове са средства, които могат да се използват за извършването на измама в големи размери. Незаконната национална и международна търговия по Интернет също се очертава като нарастващ проблем. Това включва търговията с наркотици, със застрашени видове и с оръжия.

1.2.3. Незаконно съдържание

В Европа нараства броят на достъпните интернет страници с незаконно съдържание, обхващащо материали с детска порнография, подбуждане към терористични действия, незаконно възхваляване на насилието, тероризма, расизма и ксенофобията. Дейността на правозащитните органи срещу такива интернет страници е изключително трудна, тъй като тези страници се притежават и подготвят от хора, които се намират в държави, различни от целевата държава и най-често извън ЕС. Страниците могат да бъдат много бързо преместени и извън територията на ЕС, а определенията за незаконно действие се различават значително в отделните държави.

1.2.4. Престъпления, характерни единствено за електронните мрежи

Атаките в големи мащаби (често наричани „ботнет“[3]) срещу информационните системи или срещу организации или отделни лица изглежда стават все по-широко разпространени. Също така отскоро се наблюдават случаи на системни, добре координирани преки атаки в голям мащаб срещу ключова държавна информационна инфраструктура. Това, съчетано със съвместяващите се технологии и все по-скоростната връзка на информационни системи, прави тези системи по-уязвими. Атаките са често са добре организирани и използвани с цел изнудване. Може да се предположи, че огласяването е ограничено, донякъде поради търговските загуби, които могат да възникнат, ако се даде гласност на проблемите със сигурността.

---

1 Повечето от твърденията в съобщението относно настоящите тенденции на развитие са взети от Изследването за определяне на значимостта на съобщението върху престъпленията в кибернетичното пространство, поръчано от Комисията през 2006 г. (Договор № JLS/2006/A1/003).

2 „Фишинг“ означава опитите да се придобие чувствителна информация, като пароли и данни от кредитни карти, като измамникът се представя подвеждащо като лице, на което може да се има доверие.

3 „Ботнет“ означава сбора от заразени машини, стартиращи програми под обща команда

1.3. Цели

С оглед на тази променяща се среда, е необходимо спешно да се предприемат действия, както на национално, така и на европейско ниво, срещу всички форми на престъпления в кибернетичното пространство, които представляват нарастваща заплаха за ключови инфраструктури, обществото, търговията и гражданите. Защитата на отделни лица срещу престъпленията в кибернетичното пространство е често възпрепятствана от проблеми, свързани с определянето на компетентния правораздавателен орган, приложимото право, трансгранично правоприлагане или признаване и използването на електронни доказателства. Тези трудности изпъкват особено на фона на трансграничния характер на престъпленията в кибернетичното пространство. Отчитайки тези заплахи, Комисията открива инициатива за изработването на основна политика за подобряване на координацията на европейско и международно ниво в борбата с престъпленията в кибернетичното пространство.

Целта е да се засили борбата с престъпленията на национално, европейско и международно ниво. Държавите-членки и Комисията отдавна определят като приоритет понататъшното развитие на конкретна политика на ЕС. Инициативата ще се концентрира върху правоприлагането и върху наказателноправните аспекти на тази борба, като политиката ще допълва други действия на ЕС за подобряване на сигурността изобщо в кибернетичното пространството. Политиката ще обхваща евентуално: подобрено оперативно сътрудничество в правоприлагането; по-добро политическо сътрудничество и координация между държавите-членки; политическо и правно сътрудничество с трети страни; привличане на общественото внимание; обучение; научноизследователска дейност; засилен диалог с производителите и възможни законодателни действия.

Политиката за борба и наказателно преследване на престъпленията в кибернетичното пространство ще бъде изготвена и прилагана по начин, напълно зачитащ основните права, и по-специално свободата на изразяване, зачитането на личния и семейния живот и защитата на лични данни. Всяко законодателно действие, предприето в контекста на тази политика, ще бъде детайлно анализирано преди това за съвместимост с тези права и по-конкретно с Хартата на ЕС за основните права. Следва да се отбележи също, че всички подобни инициативи по тази политика ще се осъществяват, като напълно се спазват членове 12 и 15 от т.нар. директива за електронна търговия[4], за сферите, където се прилага този правен инструмент. Целта на това съобщение може да бъде разделена на три основни оперативни насоки, които могат да се обобщят както следва:

- да се подобри и улесни координацията и сътрудничеството между отделите за борба с престъпленията в кибернетичното пространство, другите отговорни органи и експерти в Европейския съюз;

[4] Директива 2000/31/ЕО на Европейския парламент и Съвета от 8 юни 2000 г. за някои правни аспекти на услугите от информационното общество, и в по-специално на електронната търговия във вътрешния пазар (ОВ L 178, 17.7.2000, стр.1).

- да се разработи, в сътрудничество с държавите-членки, съответните международни организации, организациите на ЕС и други заинтересовани страни съгласувана правна рамка на политиката на ЕС относно борбата с престъпленията в кибернетичното пространство;

- да се насочи общественото внимание към загубите и опасностите, на които ни излагат престъпленията в кибернетичното пространство.

2. СЪЩЕСТВУВАЩИ ПРАВНИ ИНСТРУМЕНТИ ЗА БОРБА СРЕЩУ ПРЕСТЪПЛЕНИЯТА В КИБЕРНЕТИЧНОТО ПРОСТРАНСТВО

2.1. Съществуващи инструменти и действия на ниво ЕС

Настоящото съобщение относно престъпленията в кибернетичното пространство консолидира и доразвива Съобщението от 2001 г. относно създаването на по-безопасно информационно общество чрез подобряване на сигурността на информационните инфраструктури и чрез борба със свързаната с компютри престъпност[5] (наричано по нататък: Съобщението от 2001 г.) Съобщението от 2001 г. предлага подходящи материални и процесуални норми относно националните и трансгранични престъпни дейности. От негопоследваха няколко важни предложения. По-специално, това включва предложението довело до Рамковото решение 2005/222/ПВР относно атаките срещу информационните системи[6]. В тази връзка, следва да се отбележи също, че бяха приети други по-общи законодателни мерки относно борбата срещу престъпленията в кибернетичното пространство като Рамково решение 2001/413/ПВР относно борбата срещу измамата и фалшификацията на безкасови средства на разплащане[7].

Рамковото решение 2004/68/ПВР относно сексуалната експлоатация на деца[8] е добър пример за специалното внимание на Комисията към **защитата на детето** и по-специално във връзка с борбата срещу всички видове материали, показващи сексуално посегателство върху деца, незаконно публикувани посредством използването на информационни системи. Защитата на детето ще продължи да бъде хоризонтален приоритет и в бъдеще.

За да се справи с предизвикателствата пред сигурността в информационното общество, Европейската общност е развила подход относно мрежовата и информационната сигурност, включващ три елемента: специфични мрежи и мерки за сигурност на информация, регулаторна рамка за електронни съобщения и борба срещу престъпленията в кибернетичното пространство. Независимо че, тези три аспекта могат до известна степен да бъдат разработени отделно, многобройните взаимовръзки налагат тясно координиране. В свързаната с това област на мрежова и информационна сигурност, Съобщението на Комисията от 2001 г. относно мрежовата и информационната сигурност: предложение за изготвяне на политика на ниво ЕС[9], е прието едновременно със съобщението от 2001 г. относно престъпленията в

---

5 COM(2000) 890, 26.1.2001.
6 ОВ L 69 от 16.3.2005 г., стр. 67
7 ОВ L 149 от 2.6.2001 г, стр. 1.
8 ОВ L 13 от 20.01.2004 г., стр. 44.
9 COM(2001) 298.

кибернетичното пространство. Директивата 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации предвижда като задължение на доставчиците на обществено достъпни услуги в електронните съобщения да обезпечат сигурността на тези услуги. Тя съдържа също разпоредби срещу спам и шпионски софтуер. Политиката за мрежовата и информационната сигурност се развива от този момент нататък посредством няколко действия, последните от които са Съобщението относно Стратегията за сигурно информационно общество[10] , предвиждащо обновена стратегия и предвиждаща рамка за доразвиване и детайлно уреждане на съгласуван подход към мрежовата и информационната сигурност, Съобщението относно борбата срещу нежеланите съобщения (спам), шпионски и зловреден софтуер[11], както и създаването на Европейска агенция за мрежова и информационна сигурност (ЕАМИС)[12] през 2004 г. Основната цел на ЕАМИС е да се специализира в стимулирането на сътрудничеството между публичния и частния сектор и да подпомогне Комисията и държавите-членки. Резултатите от научните изследвания върху технологии за сигурността на информационните системи ще изиграят също важна роля в борбата срещу престъпленията в кибернетичното пространство. Съобразно с това, информационните технологии и технологиите на съобщенията, както и сигурността са посочени като цели в Седмата рамкова програма на ЕС за научни изследвания (FP 7), която ще действа в периода 2007-2013[13]. Прегледът на регулаторната рамка за електронни съобщения може да доведе до изменения, които да засилят ефективността на разпоредбите относно сигурността, предвидени в Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации и в Директивата за универсалната услуга 2002/22/ЕО[14].

2.2. Съществуващи международни инструменти

Поради глобалния характер на информационните мрежи, каквато и да е политика относно престъпленията в кибернетичното пространство не може да бъде ефикасна, ако усилията се ограничат в рамките на ЕО. Престъпниците могат да атакуват информационните системи или да извършат престъпление не само от една държава-членка в друга, но намирайки се извън юрисдикцията на ЕО. Затова, Комисията участва активно в международните обсъждания и структури-за сътрудничество, например Групата на Г 8 на Лион-Рим относно престъпления в сферата на високите технологии и администрирани от Интерпол проекти. По-специално, Комисията следи отблизо работата на мрежата за 24-часова връзка относно международни престъпления в сферата на високите технологии (мрежата 24/7)[15]в която членуват голям брой държави от целия свят, включително и повечето от държавите-членки. Мрежата на Г-8 представлява механизъм за ускоряване на контактите между участващите страни с 24-часова връзка за случаи, при които са необходими електронни доказателства и които изискват спешна помощ от чуждестранни правоприлагащи органи.

---

10 COM(2006) 251.

11 COM(2006) 688.

12 Регламент 460/2004 г. създаващ Европейска агенция за мрежова и информационна сигурност , (ОВ L 77, 13.3.2004, стр. 1.).

13 В Европейският съюз все още действа 6-тата Рамкова програма за научни изследвания и технологично развитие, подкрепяща определен брой значими и успешни научноизследователски проекти.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

15 Виж член 35 от Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство.

Съобразно с това, основният европейски и международен инструмент в тази област е Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство[16]. Конвенцията, която е приета и влязла в сила през 2004 г., съдържа общи определения на различни видове престъпления в кибернетичното пространство и полага основите на работещо сътрудничество между правораздавателните органи на договарящите се държави. Тя е подписана от много държави, включително Съединените американски щати и други неевропейски държави, както и от всички държави-членки. Все пак, много от държавите-членки все още не са ратифицирали конвенцията или допълнителния протокол към нея относно прояви на расизъм и ксенофобия, извършени чрез компютърни системи. Предвид общоприетата значимост на конвенцията, Комисията ще насърчава държавите-членки и съответните трети държави да ратифицират конвенцията и ще разгледа възможността Европейската общност да стане страна по конвенцията.

3. По-нататъшно развитие на специфични инструменти в борбата с престъпленията в кибернетичното пространство

3.1. Засилване на оперативното сътрудничество в правоприлагането, както и на обучението, провеждано на ниво ЕС

Липсата или недостатъчното използване на структури за незабавно реагиране в **трансграничното оперативно сътрудничество** остава основния недостатък в пространството на свобода, сигурност и правосъдие. Традиционната взаимопомощ се оказва слаба и неефективна при спешни случаи на престъпления в кибернетичното пространство, а все още не са достатъчно развити нови структури за сътрудничество. Докато националните съдебни и правоприлагащи органи в Европа си сътрудничат тясно посредством Европол, звеното „Европейско правосъдие“ и други структури, то съществува очевидна необходимост от засилване и изясняване на техните правомощия. Предприетите от Комисията консултации показват, че тези изключително важни канали не са използвани оптимално. Задължителен е по-координиран европейски подход, едновременно оперативен и стратегически и обхващащ също обмяната на информация и най-добри практики.

В близко бъдеще, Комисията ще наблегне, най-вече на необходимостта от **обучение.** Общоизвестно е, че технологичното развитие налага нуждата от непрекъснато обучение на правоприлагащите и съдебните органи по въпросите, свързани с престъпленията в кибернетичното пространство Затова се предвижда засилена и по-добре координирана финансова подкрепа от страна на ЕС на многонационални програми за обучение. Комисията ще работи в тясно сътрудничество с държавите-членки и другите компетентни органи като Европол, Евроюст, Европейския полицейски колеж (ЕПК) и Европейската мрежа за съдебно обучение (EMCO) за координацията и съгласуването на ниво ЕС на всички програми за обучение в областта.

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

Комисията ще организира **среща** на експерти от правоприлагащите органи на държавите-членки, от Европол, ЕПК и ЕМСО, за да се обсъди как да се подобрят стратегическото и оперативно сътрудничество и обученията относно престъпленията в кибернетичното пространство в Европа през 2007 г. Освен всичко друго, ще се обмисли и създаването на платформа на ЕС за обучение по проблемите на престъпленията в кибернетичното пространство и на постоянна връзка на ЕС за обмен на информация. Срещата през 2007 г. ще бъде първата от поредицата срещи, планирани в близко бъдеще.

3.2. Засилване на диалога с производителите

Както частният, така и публичният сектор имат интерес от съвместното разработване на методи за откриване и предотвратяване на вредите, настъпили в резултат на престъпните деяния. Участието и на частния и на публичния сектор, основано на взаимното доверие и на общата цел за намаляване на вредите, обещава да бъде ефективен начин за нарастване на сигурността и в борбата срещу престъпленията в кибернетичното пространство. Публично-частният аспект на политиката на Комисията относно престъпленията в кибернетичното пространство ще бъде по-нататък част от планираната глобална политика на ЕС за диалога между публичния и частния сектор, като обхваща сигурността в Европа изобщо. Тази политика ще бъде по-специално доразвита от Европейския форум за научни изследвания на сигурността и иновациите, който Комисията планира да създаде скоро и който ще обедини съответните заинтересовани лица от публичния и частния сектор.

Развитието на модерни информационни технологии и електронни системи на съобщения е напълно контролирано от частните оператори. Частните предприятия извършват оценка на заплахата, изготвят програми за борба срещу престъпленията и разработват технически решения за предотвратяването им. Производителите са положително настроени и подкрепят държавните органи в борбата с престъпленията в кибернетичното пространство, и особено в усилията им да се противопоставят на детската порнография[17] и другите видове незаконно съдържание в Интернет.

Друг проблем представлява очевидната липса на обмен на информация, на експертни познания и на добри практики между публичния и частния сектор. Операторите от частния сектор често, за да защитят търговската тайна и информация, не желаят или нямат ясно формулирано законно задължение да докладват или съобщават на правоприлагащите органи съответната информация за извършените престъпления. Въпреки това, тази информация е нужна, за да могат държавните органи да изготвят ефективна и подходяща политика за борба срещу престъпността. Възможностите да се подобри обмена на информация между публичния и частния сектор също ще бъдат взети предвид с оглед на съществуващите правила за защита на личните данни.

---

[17] Скорошен пример на сътрудничество в тази област е това между правоприлагащите органи и дружествата, издаващи кредитни карти, посредством което последните помогнаха на полицията да проследи купувачите онлайн на детска порнография.

Комисията вече играе важна роля в различни публично-частни структури, занимаващи се с престъпленията в кибернетичното пространство като например Експертната група за предотвратяване на измамата[18]. Комисията е убедена, че ефективната основна политика за борба с престъпленията в кибернетичното пространство трябва да включва и стратегия за сътрудничество между операторите от публичния и частния сектор, включително организации на гражданското общество.

За да се постигне по-разширено публично-частно сътрудничество в тази област, през 2007 г., Комисията ще организира конференция, предназначена за експерти в правоприлагането и за представители на частния сектор, особено на доставчиците на Интернет услуги, на която да се обсъди как да подобри публично-частното оперативно сътрудничество в Европа[19]. Конференцията ще засегне всички въпроси от интерес за двата сектора, но по-конкретно:

- подобряване на оперативното сътрудничество в борбата с незаконните деяния и съдържание в Интернет, по-специално в областта на тероризма, както и във връзка с материалите, представляващи сексуално посегателство върху деца и други незаконни деяния, които са изключително деликатни от гледна точка на защита на детето;

- инициране на публично-частни споразумения, които имат за цел спирането на уебсайтове в целия ЕС, съдържащи незаконно съдържание, особено материали със сексуално посегателство върху деца;

- създаване на европейски модел за разпространяване на съответната необходима информация в целия частен и в целия публичен сектор, като един от аргументите за това е да се създаде атмосфера на взаимно доверие и да се отчетат интересите на всички страни;

- изграждане в частния и в публичния сектор на мрежа от точки за контакт относно правоприлагането

3.3. Правна уредба

Все още не е уместно да се хармонизират съставите на престъпления и националните наказателни законодателства относно престъпленията в кибернетичното пространство, тъй като престъпленията обхващат различни видове нарушения. Тъй като ефективното сътрудничество между правоприлагащите органи често зависи от наличието на поне частично хармонизирани определения на престъпните състави, по-нататъшното хармонизиране на законодателствата на държавите-членки[20] остава дългосрочна цел. С рамковото решение относно атаките срещу информационни системи, се предприе важна стъпка относно някои основни престъпни състави. Както е описано по-горе, впоследствие се появиха нови заплахи и Комисията следи отблизо тяхното развитие, като има предвид колко важно е непрекъснатото оценяване на нуждата от допълнителна правна уредба. Наблюдението на нововъзникващите заплахи е тясно

---

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

19 Конференцията може да се смята като продължение на форума в ЕС, представен в раздел 6.4 от Съобщението относно компютърните престъпления.

20 Тази дългосрочна цел вече беше посочена на страница 3 от Съобщението от 2001 г.

координирано в рамките на европейската програма за защита на ключовата инфраструктура.

Въпреки това, сега трябва да се помисли и за специална правна уредба на престъпленията в кибернетичното пространство. Специфичен проблем, изискващ вероятно правна уредба е случаят, когато престъпление в кибернетичното пространство е извършено заедно с **кражба на самоличността**. Най-общо под „кражба на самоличността“ се разбира използването на лични идентификационни данни, например като номер на кредитна карта, за да се извършат други престъпления. В повечето държави-членки е по-вероятно срещу престъпника да бъде образувано наказателно производство за измама или за друго престъпление, извършено чрез кражба на самоличността, отколкото за кражба на личността, като последното се квалифицира като по-тежко престъпление. Кражбата на самоличността като такава не е инкриминирана във всички държави-членки. Често е по-лесно да се докаже престъплението кражба на самоличността, отколкото измама, така че сътрудничеството между правоприлагащите органи на ниво ЕС би имало повече полза, ако кражбата на самоличност се инкриминира във всички държави-членки. През 2007 г. Комисията ще започне консултации, за да прецени дали е уместно да се създаде правна уредба.

3.4. Развитие на статистическите данни

Общоприето становище е, че съществуващата информацията за често срещаните престъпления далеч не е достатъчно адекватна и по-специално, че са необходими сериозни подобрения, за да се сравняват данните между държавите-членки. Амбициозен петгодишен план за решаване на този проблем се съдържа в Съобщението на Комисията относно *разработване на съгласувана и цялостна стратегия на ЕС за определяне нивото на престъпността и ефективността на наказателното правосъдие. План от 7.8.2006 г. за действие на ЕС за периода 2006-2010 г.*[21] Образуваната, съгласно този план за действие, експертна група би могла да бъде подходящия форум за разработване на съответните показатели за отчитане на мащаба на престъпленията в кибернетичното пространство.

4. ПЕРСПЕКТИВИ

Понастоящем Комисията ще доразвива основна политика за борба срещу престъпленията в кибернетичното пространство. Поради ограничените правомощия на Комисията в наказателното право, тази политика може да бъде само допълнение към действията, предприети от държавите-членки и други органи. Най-важните действия, всяко от които включва употребата на един, няколко или на всички инструменти, посочени в глава 3, ще бъдат също подкрепени чрез финансовата програма „Предотвратяване и борба с престъпността“:

[21] COM(2006) 437, 7.8.2006.

4.1. Борбата с престъпления в кибернетичното пространство най-общо:

- Комисията: ще установи по-активно оперативно сътрудничество между правоприлагащите и съдебните органи на държавите-членки, чието начало ще се постави на организираната през 2007 г. среща на експерти от тези органи и което може да включва създаването на централен контактен пункт относно престъпленията в кибернетичното пространство;

- ще увеличи финансовата помощ за инициативи, насочени към подобряване на квалификацията на служители от правоприлагащите и съдебните органи във връзка с разглеждането и решаването на дела за престъпленията в кибернетичното пространство и към координиране на всички многонационални програми за обучение в тази област, чрез създаването на платформа на ЕС за обучение;

- ще стимулира ангажираността на държавите-членки и на всички държавни органи да предприемат ефективни мерки срещу престъпленията в кибернетичното пространство и да отпуснат достатъчно средства за борба с тях;

- ще подкрепи научните изследвания, които са полезни за борбата с престъпленията в кибернетичното пространство;

- ще организира поне една голяма конференция (през 2007 г) за правоприлагащите органи и частните оператори, най-вече за да инициира сътрудничеството в борбата с незаконните интернет дейности в и срещу електронните мрежи, за да стимулира по-ефективен обмен на информацията, която не е лична, както и за да доразвие заключенията от тази конференция с конкретни проекти за сътрудничество между публичния и частния сектор;

- ще поема инициативата и ще участва в публично-частни дейности, които целят да повишат осведомеността на потребителите за загубите и за опасностите на престъпленията в кибернетичното пространство, като едновременно с това не се съсредоточава върху отрицателните страни на сигурността за да не подкопава доверието на потребителите;

- ще участва активно и ще стимулира глобално международно сътрудничество в борбата с престъпленията в кибернетичното пространство;

- ще инициира, съдейства и подкрепя международни проекти, които са в съответствие с политиката на Комисията в тази област, като например проекти, осъществени от Г-8 и съвместими с държавните и регионални стратегически документи (относно сътрудничеството с трети страни);

- ще предприеме конкретни действия за насърчаване на всички държави-членки и съответните трети страни да ратифицират Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство и допълнителните протоколи към нея, както и ще разгледа възможността Общността да стане страна по конвенцията.

- ще проучи, заедно с държавите-членки, феномена на координираните и широкомащабни атаки срещу информационната инфраструктура на държавите-членки, за да ги предотврати и да се бори с тях, включително чрез координирани ответни действия, обмен на информация и добри практики.

4.2. Борбата с традиционните престъпления в електронните мрежи:

- Комисията ще инициира задълбочени анализи, за да подготви предложение за специална правна уредба на ЕС относно кражбата на самоличност;

- ще стимулира,посредством проекти за сътрудничество между публичния и частния сектор, разработването на технически методи и процедури за борба с измамата и с незаконната търговия по Интернет;

- ще продължи да работи в специфични целеви области, като борбата с измамата с безкасови средства на разплащане в електронните мрежи в рамките на Експертната група за предотвратяване на измамата.

4.3. Незаконно съдържание

- ще продължи да развива дейности срещу специфично незакоконно съдържание, особено по отношение на материалите, представящи сексуално посегателство върху деца и подбуждащи към тероризъм, най-вече чрез проследяване на изпълнението на Рамковото решение относно сексуалната експлоатация на деца;

- ще прикани държавите-членки да отпуснат достатъчно финансови средства в подкрепа на работата на изпълнителните агенции, като се обърне особено внимание на идентифициране на жертвите на материалите, показващи сексуално посегателство, разпространявани онлайн;

- ще поема инициатива и ще подкрепи дейности срещу незаконното съдържание, което може да подбуди непълнолетните към насилие или друго тежко незаконно деяние, например като някои видове онлайн видео игри, съдържащи изключително насилие;

- ще открие и насърчи диалог между държавите-членки и с трети страни относно техническите методи за борба с незаконно съдържание, както и относно процедурите за спиране на незаконни уебсайтове, също с оглед на възможното постигане на официални споразумения по тези въпроси със съседни и други държави;

- ще работи за сключването на доброволни споразумения и конвенции на ниво ЕС между държавните органи и частни оператори, по-специално доставчици на интернет услуги относно процедурите за спиране и закриване на незаконните интернет страници.

4.4. Последващи действия

В това съобщение бяха очертани като следващи стъпки много дейности за подобряване структурите за сътрудничество в ЕС. Комисията ще доразвие тези дейности, ще оцени напредъка по изпълнението им и ще докладва на Съвета и на Парламента.