КОМИСИЯ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ

Брюксел, 22.5.2007
SEC(2007) 641

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

Придружителен документ към

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

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

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕ

{COM(2007) 267 окончателен}
{SEC(2007) 642}

ОБОБЩЕНИЕ

1. Увод

Бумът в използването на Интернет през последните години и появата на нови феномени и техники създават нарастваща несигурност.

В своята законодателна и работна програма за 2007 г., Комисията отчита, че е необходима цялостна актуализация на политиката ѝ относно престъпленията в кибернетичното пространство и с тази цел предвижда да изготви предложение за Съобщение относно европейската политика за престъпленията в кибернетичното пространство.

По време на началните консултации стана ясно, че липсва информация и статистически данни и това беше една от основните причини, поради които Комисията поръча през 2006 г. извършването на външно изследване[1] (наричано по-нататък: външното изследване), представляващо основния документ за оценката на въздействието.

В процеса на подготовка, Комисията също анализира много законодателни и незаконодателни мерки, особено по отношение на възможни „пропуски“ в съществуващата регулаторна рамка. Трябва да се подчертае специалното внимание, което се отдава, в тази връзка на **Конвенцията на Съвета на Европа относно престъпленията в кибернетичното пространство**[2] (наричана по-нататък: Конвенция на Съвета на Европа) и на **Рамковото решение относно атаките срещу информационните системи**[3], тъй като тези два документа се считат за най-изчерпателната материална и процесуална правна уредба.

Въз основа на тези дейности, Комисията подготвя нова предложение за основна политика, под формата на Съобщение относно борбата срещу престъпленията в кибернетичното пространство на равнище ЕС. Предмет на настоящата оценка на въздействието са основно стратегически въпроси.

В тази връзка, Комисията подчертава, че ще направи всичко възможно за да гарантира, че политиката за борба и наказателно преследване на престъпленията в кибернетичното пространство ще бъде разработена и изпълнявана по начин, зачитащ напълно основните права, и по-специално свободата на изразяване, правото на неприкосновеност на личния и семейния живот и защитата на лични данни. Това ще се прави в съответствие със Съобщението на Комисията за спазване на Хартата за основните права при изготвяне на законодателните предложения от Комисията, прието през 2005 г. [COM(2005) 172].

---

1 Изследване за оценяване на въздействието на Съобщението относно престъпленията в кибернетичното пространство, изготвено от Yellow Window Management Consulting (Contract №. DG 2006/JHA D 2/03).

2 Конвенция на Съвета на Европа от 2001 г. относно престъпленията в кибернетичното пространство: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3 Рамково решение относно атаките срещу информационни системи (2005/222/ПВР).

2. ПРОБЛЕМИ И ЦЕЛИ

Бързото развитие на Интернет и на другите информационни системи доведе до появата на напълно нов икономически отрасъл и на нови бързи потоци от информация, продукти и услуги, пресичащи вътрешните и външните граници на ЕС. Очевидно, това има многобройни положителни последици за потребителите и гражданите. От друга страна обаче, това развитие отвори много нови възможности за престъпниците. Ясно се очертава модел на нови престъпни деяния срещу Интернет, както и на деяния, при които се използват информационни системи като средство на престъпление. Престъпните деяния непрекъснато се развиват, а законодателството и правоприлагането изпитват очевидни трудности да я догонят. Присъщият трансграничен характер на този нов вид престъпления създава също необходимост от подобряване на трансграниченото сътрудничество в правоприлагането.

За да се проучи подробно цялата проблематика, се вземат предвид следните осем стратегически проблема:

- обществото, бизнеса и гражданите са все по-уязвими към престъпленията в кибернетичното пространство;

- престъпните деяния в кибернетичното пространство стават все по-чести и по-сложни;

- Липсват съгласувани на равнище ЕС политика и законодателство за борба срещу престъпленията в кибернетичното пространство;

- Има специфични трудности в оперативното сътрудничество по правоприлагането в сферата на престъпленията в кибернетичното пространство;

- Необходимо е доразвиване на специални познания и разработване на технически средства: обучения и научноизследователска дейност;.

- липсата на функционална структура за сътрудничество между основните заинтересовани лица от публичния и частния сектор;

- правомощията и отговорностите остават неясни;

- липсва информираност за рисковете, произтичащи от престъпленията в кибернетичното пространство.

Следва да се отбележи, че предприетите с оглед на този доклад консултации, показаха учудващо близки мнения на всички заинтересовани страни, без оглед на това дали са правоприлагащи органи или частни предприятия, по настоящите проблеми на ЕС в тази сфера.

2.1. Кой е засегнат?

Престъпленията в кибернетичното пространство засягат всички сектори на обществото, така че политиката срещу тях ще бъде осезаема практически навсякъде. Като се има предвид, че броят на гражданите, използващи лични компютри, е много висок, повечето частни лица - в качеството им вече на потенциални жертви – също могат да бъдат засегнати от всяка инициатива в борбата с престъпленията в кибернетичното пространство.

Съществуват, обаче, ясни сигнали за нарастваща престъпна дейност, насочена срещу специфични групи от жертви. В тази връзка, една ефективна политика срещу престъпленията в кибернетичното пространство би била категорично от полза на тези групи. При тези обстоятелства, може да се очаква, че индустрията на информационното общество, както и информационното общество най-общо, са основните заинтересовани страни, предвид важните положителни икономически резултати, които могат да се очакват, ако се засили сигурността или ако се установят условия на повишена сигурност.

2.2. Има ли ЕС право да действа?

Предвид обхватът и значимостта на заплахите за сигурността, съществува неотменна дори растяща необходимост да се овладеят тези заплахи от престъпления в кибернетичното пространство се запазва, дори може да нарасне. Проблемите на сигурността, свързани престъпленията в кибернетичното пространство, имат глобални измерения, поради което е невъзможно да се решават на национално ниво. Заплахата е международна, и такава трябва да бъде поне част от ответните мерки. Извън всякакво съмнение е, че борбата срещу престъпленията в кибернетичното пространство ще продължи да бъде най-значителна и най-ефективна на национално ниво, но съществува ясна необходимост националните усилия да се обвържат и евентуално допълнят на европейско равнище.

2.3. Цели

Най-общата стратегическа цел на предлаганата политика, произтичаща от установените по-горе проблеми, може да бъде обобщена както следва:

да се активизира и координира по-добре борбата с престъпленията в кибернетичното пространство на национално, европейско и международно ниво.

Тази обща стратегическа цел може да се раздели на следните пет равностойни стратегически цели, представени в примерен ред по приоритет:

- да се подобрят оперативните трансгранични действия по правоприлагане срещу престъпленията в кибернетичното пространство изобщо и по-специално срещу тежките форми на тези престъпления и да се подобри обмена на информация, на разузнавателни данни и добри практики между правоприлагащите органи в държавите членки и извън тях;

- да се определят и създадат оперативни средства за сътрудничество и за залагането на общи цели за публичния и частния сектор и да се усъвършенства обмена на информация между тези сектори на ниво ЕС, на разузнавателни данни и добри практики в борбата с престъпленията в кибернетичното пространство;

- да се създаде, в сътрудничество с държавите-членки и с компетентни структури на ниво ЕС и международни организации политическа платформа и структури за развитието на последователна политика на ЕС за борбата с престъпленията в кибернетичното пространство и да се усъвършенства съществуващата законова и институционална рамка по-ефективни чрез изясняване на правомощията и отговорностите на всички участници;

- да се отговори на нарастващата заплаха от тежки форми на престъпления в кибернетичното пространство, чрез насърчаване на уменията, познанията и техническите средства; включително и чрез дейности, които да засилят обученията и научноизследователската работа в тази област;

- да се повиши, най-вече сред потребителите и другите уязвими групи на потенциални жертви, общата информираност за заплахата от престъпления в кибернетичното пространство.

3. ВАРИАНТИ ЗА СТРАТЕГИЧЕСКА ПОЛИТИКА

Поради естеството на своя предмет, всяка политика за борба срещу престъпленията в кибернетичното пространство би била многоаспектна. За да бъде истински ефективна, тя трябва да съчетава традиционните правоприлагащи дейности с други инструменти, като елементи на саморегулация и създаване на структури за сътрудничество между различните заинтересовани страни. Много от проблемните области и стратегически цели на настоящата инициатива са представени по-горе. За да се постигнат тези цели, е необходимо, да се предприемат разнообразни и комбинирани действия. Въз основа на предприетите разширени консултации, Комисията е формулирала четири варианта за основна политика, всеки от които представлява набор от специфични действия.

3.1. Вариант 1 за основна политика: Запазване на сегашното положение (status quo)/не се предприемат нови, значими действия

Този вариант би означавал, че понастоящем Комисията няма да предприеме никакво хоризонтално действие в тази област. Това значи, че:

- Комисията ще продължи да оценява нуждата от целево законодателство и когато се налага ще предприеме съответното действие по политиката;

- Комисията ще следи съществуващите на равнище ЕС и международни структурни проекти, насочени срещу престъпленията в кибернетичното пространство;

- Комисията ще продължи да инициира нови проекти в съответните релевантни за борбата срещу престъпленията в кибернетичното пространство области, без да предприема каквато и да хоризонтална инициатива по политиката.

3.2. Вариант 2 за обща политика: Обща правна уредба

Този вариант би означавал, че ще се възприеме политиката да се предложи постепенно приемането на обща регулаторна рамка за борба срещу престъпленията в кибернетичното пространство. Този вариант на политика би означавал, че:

- Комисията системно ще предлага хармонизирани или уеднаквени определения на престъпления, по-специално в рамките на ЕС, но също и на международно ниво.

- Комисията ще предложи минимални общи стандарти за инкриминиране на деяния и за наказания в ЕС.

- Ще бъдат създадени официални платформи за сътрудничеството между публичния и частния сектор, както и за обучение и научни изследвания.

- Официално ще бъде създадена мрежа в областта на правоприлагането .

3.3. Вариант 3 за обща политика: Създаване на неформални публично-частни мрежи и мрежи по въпросите на престъпленията в кибернетичното пространство

Този вариант би означавал, че Комисията, сама или заедно с други институции, ще създаде официално мрежи от експертни групи в областта на престъпленията в кибернетичното пространство, като заедно с това за операторите, производителите и потребителите се въведе схема за доброволно установяване на сигурността. Това би означавало, че:

- Ще бъде създадена неформална организация на експерти в правоприлагането в областта на престъпления в кибернетичното пространство.

- Ще бъде създадена неформална платформа/мрежа на експерти в правоприлагането в частния и публичния сектор при престъпления в кибернетичното пространство.

3.4. Вариант 4 за основна политика: Съгласуван стратегически подход

Този вариант би означавал, че на ниво ЕС ще се въведе съгласувана стратегия за борба с престъпленията в кибернетичното пространство. Нейната основна характеристика би била установяването на стратегическа рамка на политиката на ЕС за борба с престъпленията в кибернетичното пространство, като общата цел е да се направляват по-добре конкретните действия и оптимално да се използват наличните средства. Друга важна функционална характеристика на тази стратегия би била:

- Подобрено сътрудничество в правоприлагането на равнище ЕС

- Създаването на стратегическа структура за сътрудничество между частния и публичния сектор срещу престъпленията в кибернетичното пространство.

- Насърчаване установяването на рамка за глобално международно сътрудничество в съответната област.

- Приемането на законодателни актове в областта, когато е необходимо.

4. ОЦЕНКА НА ВАРИАНТИТЕ ЗА ПОЛИТИКА И ИЗБОР НА ЕДИН ОТ ТЯХ

4.1. Оценка

Вариантите за основна политика бяха оценени въз основа на следните критерии:

- Социални последици.
- Икономически последици.
- Разходи за публична администрация
- Степен на съответствие с целите на политиката
- Допълнителна полза и спазване на принципа на субсидиарност
- Изпълнимост

Изводите от оценката накратко, са:

4.1.1. Вариант 1 за основна политика:

Счете се, че този вариант изобщо не е достатъчен с оглед на съществуващите предизвикателства. Последиците от варианта „да не се предприемат нови действия“ са принципно ограничени, но е трудно да се прецени, дали при него съществува риск от значителни последствия, доколкото бъдещите видове престъпления са по дефиниция неизвестни. Отчитайки настоящото и нарастващо значение на този вид престъпност има много голям риск от потенциално отрицателно въздействие в дългосрочен план на варианта „да не се предприемат нови действия“.

4.1.2. Вариант 2 за основна политика:

Изводът е, че този вариант на политика може да се следва само много внимателно и в дългосрочна перспектива. Необходими са подробни проучвания за правната му изпълнимост и продължителни политически преговори. Последиците от този вариант могат да бъдат много значителни, но с оглед на малката вероятност в краткосрочен план по него да има действителен напредък, той остава несигурен в краткосрочна перспектива. Може също да се постави въпросът, дали целите на политиката могат да бъдат осъществени толкова ефективно при действителното ѝ изпълнение, колкото това изглежда на политическо ниво или на теория. Рискът от избора на този вариант на политика, би бил, че оперативното ниво на борбата срещу престъпленията в кибернетичното пространство няма да участва достатъчно в избора на стратегически политики и решения. Предвид важните взаимосвързани въздействия, е необходимо да се изясни ролята на Комисията в тази връзка. Възможно е също, да се твърди, че сходни резултати биха могли да бъдат постигнати с по-меки мерки.

4.1.3. Вариант 3 за основна политика:

Вариантът за политика би бил оценен като много интересен от стратегическа гледна точка, дори и да е трудно да се предвидят допълнителната му полза и конкретни последици. Риск се крие в това, че новите мрежови структури биха постигнали твърде оскъдни конкретни резултати. Комисията е в най-добра позиция, за да може да координира действията за саморегулация в тази област, но в рамките на този вариант, тя има повече координираща и помощна функция, отколкото тази на стратегически лидер.

4.1.4. Вариант 4 за основна политика:

Счита се, че този вариант на политика представлява набор от най-уместните стратегически действия. Отчитат се много малко отрицателни последици или големи пречки. Критично погледнато може да се твърди, че прякото отрицателно въздействие на политиката е по-скоро ограничено. Това, обаче, важи само в краткосрочна перспектива, тъй като могат да последват значими резултати, в случай, че бъдат предприети адекватни мерки за изпълнение. Трудно е, обаче, да се предвидят в подробности конкретните последици, тъй като стратегическата визия ще бъде оперативно осъществена на по-късен етап. Тогава ще бъдат оценени всички последици.

Отново трябва да се подчертае, че преките последици на предложените стратегии са ограничени и че конкретните действия, предприети на по-късен етап в рамките на една от тези стратегии, ще бъдат оценявани отделно. Това означава, че направената понастоящем оценка е с предварителен характер.

4.2. Избор на вариант на политика

Анализът ясно посочва като най-добра алтернатива вариант 4. Вариант 4 е също вариантът, който най-добре отговаря на общите цели, посочени по-горе в раздел 2.4.

Вариантът да не се предприемат изобщо действия в областта не изглежда надежден. Пасивният подход, вероятно ще доведе до многобройни двустранни проекти за сътрудничество в борбата с престъпленията в кибернетичното пространство, които ще продължават да съществуват, без да се използват преимуществата на хоризонтален обмен на най-добри практики или на съвместно постигнатите резултати. Основно законодателство, уреждащо създаването на нови органи на ЕС, хармонизиране на определенията на съставите на престъпления и изясняване на правомощията и отговорностите на всички участници би представлявало интерес, но анализът на политическата ситуация ясно сочи, че предложения за основно хоризонтално законодателство имат малки шансове да бъдат приети.. Освен това, много малко от консултираните участници вярват че това може да бъде най-важния приоритет понастоящем. Приемането на основно законодателство може обаче да бъде от значение, в дългосрочна перспектива. Създаването, на равнище ЕС, на нови неформални структури по правоприлагане или на сътрудничество между частния и публичния сектор може също да бъде добра идея в дългосрочен план. Изглежда обаче, че всички участници са съгласни, че съществуващите структури са достатъчни, независимо че спешно трябва да станат по-ефективни. Резултатът от анализа е, че се отдава предпочитание на вариант 4 „съгласувана стратегия“ Следва да се отбележи, че вариантът не изключва създаването на по-късен етап на формална структура (вариант

3) или приемането на обща правна уредба (вариант 2). Избраният вариант означава в действителност възможността за нови действия.

Подготвителният анализ и проведените дискусии ясно показват, че „съгласуваната стратегия“ е вариантът, който най-вероятно ще постигане стратегическите цели на политиката. Подобна стратегия вероятно ще има значително позитивно въздействие върху борбата срещу трансграничните престъпления в кибернетичното пространство, тъй като ще се изяснят и утвърдят правомощията и ролята на всички участващи в борбата. Това също ще съдейства за по-добрия диалог и разбирателство между публичния и частния сектор, което на свой ред, би могло да има много положителни странични ефекти. От икономическа гледна точка, избраният вариант може да доведе до важни съвместно постигнати резултати, по-малко вредоносни последици от престъпните деяния и намалени разходи за отделни програми за сигурност.

Вероятно е, обаче, да отнеме няколко години докато настъпят очакваните резултати от избраната да политика. Ето защо, понастоящем е трудно да се оценят всички потенциални въздействия. Това важи с още по-голяма сила, предвид факта, че конкретните подробности на политиката остава да бъдат уточнени. Затова е необходимо, специфичните въздействия на конкретните елементи на политиката да бъдат оценени на по-късен етап.