ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 30.9.2010
COM(2010) 517 окончателен

2010/0273 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. ОСНОВАНИЯ И ЦЕЛИ НА ПРЕДЛОЖЕНИЕТО

Целта на предложението е да замени Рамково решение 2005/222/ПВР от 24 февруари 2005 г. относно атаките срещу информационните системи[1]. Както се отбелязва в съображенията на рамковото решение, то имаше за цел подобряване на сътрудничеството между съдебните и другите компетентни органи, в това число полицията и други специализирани правоприлагащи служби на държавите-членки, чрез сближаване на нормите на наказателното право в сферата на атаките срещу информационните системи. С него законодателството на ЕС започна да третира нарушения като незаконен достъп до информационни системи, незаконна намеса в такива системи и незаконната намеса в данните им, и бяха въведени специфични правила относно отговорността на юридическите лица, съдебната компетентност и обмена на информация. От държавите-членки се изиска да вземат необходимите мерки за прилагане на разпоредбите на рамково решение до 16 март 2007 г.

На 14 юли 2008 г. Комисията публикува доклад за прилагането на рамковото решение[2]. В заключенията на доклада се отбелязва, че е постигнат значителен напредък в повечето държави-членки и че степента на прилагане е сравнително висока, но че в някои държави-членки това прилагане все още не е завършено. Освен това в доклада се заявява, че „неотдавнашните атаки в цяла Европа след приемането на рамковото решение очертаха няколко нови вида заплахи, по-специално възникването на масови едновременни атаки срещу информационни системи и увеличаване на престъпната употреба на така наречените „ботнет“. Тези атаки не са били в центъра на вниманието, когато рамковото решение е било прието. Като реакция на тези събития Комисията ще обмисли действия за намиране на по-добър отговор на заплахите (за обяснение на това какво е ботнет вж. следващия раздел).

Важността на предприемането на допълнителни действия за засилване на борбата срещу престъпленията в кибернетичното пространство беше подчертано в Хагската програма за укрепване на свободата, сигурността и правосъдието в Европейския съюз от 2004 г., както и в Програмата от Стокхолм от 2009 г. и в съответния ѝ план за действие[3]. Освен това в наскоро представената Програма в областта на цифровите технологии за Европа[4] — първата водеща инициатива, приета в рамките на стратегията „Европа 2020“, се призна необходимостта от справяне на европейско равнище с възникването на нови форми на престъпност, по-специално престъпленията в кибернетичното пространство. В тази област на действие, в която доверието и сигурността са от основно значение, Комисията се ангажира с мерки за борба с атаките в кибернетичното пространство срещу информационните системи.

На международно равнище Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, подписана на 23 ноември 2001 г., се приема за най-пълния международен стандарт до този момент, тъй като осигурява цялостна и

---

1 ОВ L 69, 16.3.2005 г., стр. 68.

2 Доклад от Комисията до Съвета въз основа на член 12 от Рамково решение на Съвета от 24 февруари 2005 г. относно атаките срещу информационните системи - COM (2008) 448.

3 ОВ C 198, 12.8.2005 г., ОВ C 115, 4.5.2010 г. , COM (2010) 171, 20.4.2010 г.

4 Съобщение на Комисията - COM (2010) 245, 19.5.2010 г.

съгласувана рамка, обхващаща различните аспекти, свързани с престъпленията в кибернетичното пространство[5]. До този момент конвенцията е подписана от всички 27 държани-членки, но е ратифицирана само от 15[6]. Конвенцията влезе в сила на 1 юли 2004 г. ЕС не е страна по конвенцията. Като се има предвид важността на този инструмент, Комисията настойчиво насърчава останалите държави-членки на ЕС да ратифицират Конвенцията възможно най-бързо.

- **Общ контекст**

Що се отнася до престъпленията в кибернетичното пространство, основната причина за това явление е уязвимостта, произтичаща от редица фактори. Недостатъчният отговор от страна на механизмите за правоприлагане допринася за разпространението на тези явления, а трудностите стават по-големи поради факта, че някои форми на престъпления надхвърлят националните граници. Докладването на информация за този вид престъпност е често незадоволително, отчасти защото някои престъпления остават незабелязани, и отчасти, тъй като жертвите (икономически оператори и предприятия) не съобщават за престъпленията поради опасения от лоша репутация и опасения, че бъдещите бизнес перспективи ще бъдат засегнати от оповестяването на тяхната уязвимост.

Освен това различията в националното наказателно право и процедури могат да доведат до разлики в разследването и наказателното преследване, което води до различия в начина, по който се разглеждат тези престъпления. Развитието на информационните технологии изостря тези проблеми, като улеснява производството и разпространението на инструменти („злонамерен софтуер“ и „ботнет“), като същевременно предоставя анонимност на извършителите на престъпления и размива отговорността между различните национални юрисдикции. Поради трудностите за започване на наказателното преследване, организираната престъпност може да трупа значителни печалби с малък риск.

В това предложение се вземат предвид новите начини за извършване на престъпленията в кибернетичното пространство, по-специално използването на ботнет. Терминът „ботнет“ означава мрежа от компютри, които са били заразени от злонамерен софтуер (компютърен вирус). Такава мрежа от заразени компютри („зомбита“) може да бъде активирана за извършване на определени действия, като атакуване на информационни системи (кибератаки). Тези „зомбита“ могат да бъдат контролирани от друг компютър - често без знанието на потребителите на заразените компютри. Този „контролиращ“ компютър е познат още като „командно-контролен център“. Лицата, които контролират този център, са сред нарушителите, тъй като те използват заразените компютри, за да започнат атаки срещу информационни системи. Много е трудно извършителите да бъдат проследени, тъй като компютрите, които образуват ботнет и извършат атаката могат да се намират на различно място от самия престъпник.

Атаките от един ботнет често се извършват в големи мащаби. Широкомащабни са тези атаки, които могат или да бъдат извършени посредством инструменти, засягащи голям брой информационни системи (компютри), или атаки, които причиняват значителни

---

[5] Конвенция на Съвета на Европа за престъпленията в кибернетичното пространство, Будапеща, 23.11. 2001 г., CETS n° 185.

[6] За преглед на ратификациите на конвенцията (CETS n° 185), вж.: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

щети, изразяващи се например в прекъснати системни услуги, финансови разходи, загуба на лични данни и т.н. Щетите, причинени от широкомащабни атаки оказват огромно въздействие върху функционирането на самата цел и/или засягат нейната работна среда. В този контекст под „голям ботнет“ се разбира, ботнет, който е в състояние да причини сериозни щети. Трудно е ботнетите да бъдат определени от гледна точка на големината им, но се смята, че при най-големите наблюдавани ботнети се извършват между 40 000 и 100 000 свързвания (т.е. заразени компютри) за период от 24 часа[7].

- **Действащи разпоредби в областта на предложението**

На ниво ЕС с рамковото решение се въвежда минимално ниво на сближаване на законодателствата на държавите-членки за инкриминиране на редица престъпленията в кибернетичното пространство, включително незаконния достъп до информационни системи, незаконната намеса в такива системи и незаконната намеса в данните им, както и подбудителството, подпомагането и опитите за извършване.

Въпреки че разпоредбите на рамковото решение като цяло са приложени от държавите-членки, в решението има редица недостатъци поради тенденцията към увеличаване на размера и броя на престъпленията (кибератаки). С него законодателствата се сближават само за ограничен брой престъпления, но не се отговоря напълно на потенциалната заплаха за обществото от широкомащабните атаки. В решението не се отчита в достатъчна степен тежестта на престъпленията и на санкциите срещу тях.

Други инициативи на ЕС и действащи или планирани програми до известна степен допринасят за справяне с проблемите, свързани с кибератаките или с въпроси като сигурността на мрежовата сигурност и безопасността на интернет потребителите. Те включват действия, подкрепяни от програмите „Предотвратяване и борба с престъпността“[8], „Наказателно правосъдие“[9], „По-безопасен интернет“[10] „Инициатива за критична информационна инфраструктура“[11]. В допълнение към рамковото решение, друг правен инструмент от значение е Рамковото решение 2004/68/ПВР относно борбата със сексуалната експлоатация на деца и детската порнография.

На административно ниво практиката на заразяване на компютри и превръщането им в „ботнет“ вече е забранена съгласно правилата на ЕС за защита на неприкосновеността на личния живот и данните[12]. По-специално националните административни агенции вече си сътрудничат в рамките на Контактната мрежа на органите, отговарящи за борбата със спама (CNSA). Съгласно тези правила държавите-членки са длъжни да забранят прихващането на съобщения, изпращани по обществени електронни съобщителни мрежи и обществено достъпни електронни съобщителни услуги, ако прихващането е извършено без съгласието на съответните потребители или без законово разрешение.

---

7 Броят на свързванията за 24 часа е общотоприетата мерна единица за оценка на големината на ботнетите.

8 Вж.: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Вж.: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Вж.: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Вж.: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Директива за правото на неприкосновеност на личния живот и електронни комуникации (ОВ L 201, 31.7.2002 г.), изменена с Директива 2009/136/ЕО (ОВ L 337, 18.12.2009 г.).

Настоящото предложение е в съответствие с тези правила. Държавите-членки следва да обърнат внимание на подобряването на сътрудничеството между административните и правоприлагащите органи в случаите, подлежащи както на административни, така и наказателни санкции.

- **Съгласуваност с други политики и цели на Съюза**

Целите са в съответствие с политиките на ЕС за борба с организираната престъпност, за укрепване на устойчивостта на компютърните мрежи, за защита на критичната информационна инфраструктура и за защитата на данните. Целите са в съответствие и с Програмата за по-безопасен интернет, създадена за насърчаване на по-безопасното използване на интернет и новите онлайн технологии и за борба срещу незаконното съдържание.

Предложението бе подложено на задълбочено разглеждане, за да се гарантира, че разпоредбите му са напълно съвместими с основните права и по-специално със защитата на личните данни, свободата на изразяване и на информацията, правото на справедлив съдебен процес, презумпцията за невинност и правото на защита, както и на принципите на законност и пропорционалност на престъпленията и наказанията.

2. КОНСУЛТАЦИЯ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

- **Консултация със заинтересованите страни**

Бяха преведени консултации с широк кръг експерти в тази област в определен брой срещи, посветени на разнообразни аспекти на борбата срещу престъпленията в кибернетичното пространство, включително и на последващи съдебни действия (наказателно преследване) на тези престъпления. Сред тях имаше по-конкретно представители на правителствата на държавите-членки и на частния сектор, специализирани съдии и прокурори, международни организации, европейски агенции и експертни органи. Редица експерти и организации изпратиха впоследствие документи и информация.

Основните послания в резултат на консултацията са следните:

– необходимостта за ЕС да предприеме действия в тази област;

– необходимостта да се инкриминират формите на престъпления, които не са включени в сегашното рамково решение, по-конкретно новите форми на кибератаки (ботнети);

– необходимостта от премахване на препятствията пред разследването и наказателното преследване на трансгранични случаи;

Информацията и становищата, получени по време на консултацията, бяха взети предвид в оценката на въздействието.

Събиране и използване на експертни становища

Външни експертни становища бяха получени на различните срещи със заинтересованите страни.

Оценка на въздействието

Бяха разгледани различни варианти на политиката като средство за постигане на целта.

- Вариант на политиката (1): запазване на статуквото/без нови действия от страна на ЕС

Този вариант означава, че ЕС няма да предприеме по-нататъшни действия за борба с този конкретен вид престъпления в кибернетичното пространство, т.е. атаките срещу информационни системи. Очаква се сегашните действия да продължат по-специално програмите за укрепване на защитата на критичната информационна инфраструктура и подобряване на публично-частното сътрудничество срещу престъпността в кибернетичното пространство.

- Вариант на политиката (2): разработка на програма за по-енергични усилия за противодействие на атаките срещу информационните системи посредством незаконодателни мерки

В допълнение към програмата за защита на критичната информационна инфраструктура, незаконодателните мерки биха били насочени към трансграничното правоприлагане и публично-частното партньорство. Целта на необвързващите правни инструменти следва да е насърчаването на още по-координирани действия на ниво ЕС, включително засилване на съществуващата за правоприлагащите органи мрежа от звена за контакт, които са на тяхно разположение 24 часа в денонощието и седем дни в седмицата, създаване на мрежа на ЕС от публично-частни звена за контакт, в които да участват експерти по престъпления в кибернетичното пространство и правоприлагащите органи, разработка на типово споразумение на ЕС за нивото на обслужване при сътрудничество в областта на правоприлагането с операторите от частния сектор, както и подкрепа за организирането на програми за обучение, предназначени за правоприлагащите органи и посветени на разследването на престъпленията в кибернетичното пространство.

- Вариант на политиката (3): целенасочена актуализация на правилата на рамковото решение (нова директива, която да замени сегашното рамковото решение), която да отговори на заплахата от широкомащабни атаки срещу информационни системи (ботнети), а когато тези атаки са извършени с прикриване на истинската самоличност на извършителя и нанасят щети на законния собственик на идентичността—да повиши ефективността на звената за контакти по правоприлагане в държавите-членки, както и да реши проблема с липсата на статистически данни за кибератаки.

В този вариант се предвижда въвеждане на специфично целево (т.е. ограничено) законодателство за предотвратяване на широкомащабни атаки срещу информационни системи. Такова „подсилено“ законодателство може да се придружава с незаконодателни мерки за укрепване на оперативното трансгранично сътрудничество срещу такива атаки, което би улеснило прилагането на законодателните мерки. С тези

мерки се цели да се подобри готовността, сигурността и устойчивостта на особено важната информационна инфраструктура, както и обмена на добри практики.

- Вариант на политиката (4): въвеждане на всеобхватно законодателство на ЕС срещу престъпленията в кибернетичното пространство

Този вариант би довел до ново всеобхватно законодателство на ЕС. В допълнение към въвеждането на необвързващи мерки съгласно варианта на политиката 2, както и актуализацията според вариант на политиката 3, с вариант 4 ще се решат и други правни проблеми, свързани с използването на интернет. Тези мерки биха обхванали не само атаките срещу информационните системи, но и проблеми като финансовите престъпления в кибернетичното пространство, незаконно съдържание в интернет, събирането/съхранението/прехвърлянето на електронни доказателства и по-подробни правила относно юрисдикцията. Законодателството ще действа успоредно с Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство и ще включва споменатите по-горе придружаващи незаконодателни мерки.

- Вариант на политиката (5): актуализация на Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство

За този вариант ще се изисква съществено предоговаряне на сегашната конвенция, а това е продължителен процес и е в противоречие със сроковете за действие, предложени в оценката на въздействието. На международно равнище не изглежда да има готовност за предоговаряне на конвенцията. Следователно актуализацията на конвенцията не може да се приеме за осъществим вариант, тъй като с него не спазват сроковете за действие.

Предпочитан вариант на политиката: комбинация от незаконодателни мерки (вариант 2) с целенасочена актуализация на рамковото решение (вариант 3)

След анализ на икономическото и социалното въздействие, както и на въздействието върху основните права, варианти 2 и 3 представляват най-добрият подход към проблемите и позволяват да бъдат постигнати целите на предложението.

При изготвянето на предложението Комисията извърши оценка на въздействието.

3. ПРАВНИ ЕЛЕМЕНТИ НА ПРЕДЛОЖЕНИЕТО

- **Обобщение на предлаганите мерки**

С директивата се отменя Рамковото решение 2005/222/ПВР, но в нея ще се запазят сегашните му разпоредби и ще бъдат включени следните нови елементи:

– Относно материалното наказателно право като цяло в директивата:

А. се наказват производството, продажбите, доставките за употреба, вноса, разпространението или друга форма на предоставяне на устройства/ инструменти, предназначени за извършване на престъпленията.

Б. се включват утежняващи обстоятелства:

- на широкомащабния аспект на атаките — ботнети или други подобни инструменти, ще се отговори с въвеждането на ново утежняващо вината обстоятелство, в смисъл че актът на създаване на ботнет или на подобен инструмент ще бъде утежняващ фактор при извършване на престъпленията, посочени в съществуващото рамково решение;

- когато такива атаки са извършени с прикриване на истинската самоличност на извършителя и нанасят щети на законния собственик на идентичността. Всички такива правила ще трябва да отговарят на принципите на законност и пропорционалност на престъпленията и наказанията и да бъдат в съответствие с действащото законодателство за защита на личните данни[13];

В. се въвежда престъплението „незаконно прихващане“;

Г. се въвеждат мерки за подобряване на европейското сътрудничество в областта на наказателното правосъдие чрез укрепване на съществуващата структура от звена за контакт, които са достъпни 24 часа в денонощието и седем дни в седмицата[14];

- предлага се задължение за отговор в определен срок на искане за съдействие от оперативните звена за контакт (посочени в член 14 от директивата). В Конвенцията за престъпленията в кибернетичното пространство няма задължителна разпоредба от този вид. Целта на тази мярка е да се гарантира, че звената за контакт отговарят в определен срок дали са в състояние да предложат решение по искането за съдействие и докога запитващото звено за контакти може да очаква такова решение да бъде намерено. Действителното съдържание на решенията не е уточнено.

Д. се разглежда необходимостта да бъдат предоставяни статистически данни за престъпленията в кибернетичното пространство, като държавите-членки се задължават да направят необходимото за въвеждане на подходяща система за записване, производство и предоставяне на статистически данни за престъпленията, посочени в действащото рамково решение и за нововъведеното престъпление „незаконно прихващане“.

В дадените в директивата определения на престъпленията, изброени в членове 3, 4, 5 (незаконен достъп до информационни системи, незаконна намеса в системите и незаконната намеса в данните) се съдържа разпоредба, която позволява, в процеса на транспониране на директивата в националното законодателство, да се инкриминират само „случаи, които не са маловажни“. Този елемент на гъвкавост има за цел да позволи на държавите-членки да не обхващат случаи, които биха попаднали *in abstracto* в основното определение, но за които се счита, че не вредят на защитения правен интерес, например, по-специално деяния на млади хора, които се опитват да докажат

---

[13] Като например Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации, ОВ L 201, 31.7.2002 г., стр. 37, в процес на преразглеждане), а също и общата директива 95/46/ЕС за защита на данните.

[14] Създадена с конвенцията и Рамково решение 2005/222/ПВР относно атаките срещу информационните системи.

своите познания в областта на информационните технологии. Тази възможност да се ограничи обхватът на инкриминирането обаче не следва да води до въвеждане на допълнителни съставни елементи на престъпленията, освен тези, които са вече включени в директивата, защото това ще доведе до положение, при което се обхващат единствено престъпления, извършени при утежняващи обстоятелства. В процеса на транспониране държавите-членки следва да се въздържат по-специално от добавяне на допълнителни съставни елементи към основните престъпления, като например конкретното намерение да се извлекат незаконни облаги от престъпленията или наличието на конкретна последица като например причиняването на значителни щети.

- **Правно основание**

Член 83, параграф 1 от Договора за функционирането на Европейския съюз[15].

- **Принцип на субсидиарност**

Принципът на субсидиарност се прилага към действията на Европейския съюз. Целите на предложението не могат да бъдат постигнати в достатъчна степен от държавите-членки поради следните причини:

Престъпленията в кибернетичното пространство и по-специално атаки срещу информационните системи имат значително трансгранично измерение, което личи най-вече от широкомащабните атаки, като свързващите елементи на дадена атака често са разположени на различни места и в различни страни. Това изисква действия на равнище ЕС, и по-специално подобаващ отговор на сегашната тенденция на широкомащабни атаки в Европа и в света. За действия на ниво ЕС и за актуализиране на Рамково решение 2005/222/ПВР се призовава също в заключенията на Съвета от ноември 2008 г.[16], тъй като целта за ефективна защита на гражданите от престъпленията в кибернетичното пространство не може да бъде постигната в достатъчна степен от държавите-членки.

Чрез действия на Европейския съюз целите на предложението ще бъдат изпълнени по-добре поради следните причини:

С предложението ще се постигне по-нататъшно сближаване на материалното наказателно право на държавите-членки и на приложимите процедури, което ще има благоприятно въздействие върху борбата срещу тези престъпления. На първо място, така ще се попречи на нарушителите да се преместят в държави-членки с по-снизходително законодателство срещу кибератаките. На второ място, общите определения ще дадат възможност за обмен на информация, събиране и сравняване на съответните данни. На трето място, нараства и ефективността на превантивните мерки в целия ЕС и ефективността на международното сътрудничество.

Поради това предложението е в съответствие с принципа на субсидиарност.

---

15 ОВ C 83, 30.3.2010 г., стр. 49

16 „Съгласувана работна стратегия и практически мерки в борбата с киберпрестъпността“, 2987-мо заседание на Съвета по правосъдие и вътрешни работи, Брюксел, 27—28 ноември 2008 г.

- **Принцип на пропорционалност**

Предложението е в съответствие с принципа на пропорционалност поради посочената по-долу причина:

Директивата се ограничава до необходимия минимум с оглед постигане на тези цели на европейско равнище и не надхвърля необходимото за тази цел, като взема предвид необходимостта от точно наказателно законодателство.

- **Избор на инструменти**

Предлаган инструмент: директива.

Други средства не биха били подходящи поради следната причина.

Според правното основание се изисква директива.

Незаконодателни мерки и саморегулиране биха подобрили ситуацията в определени области, където прилагането е особено важно. В други области обаче, където от решаващо значение е изработването на ново законодателство, ползите биха били малки.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Отражението на предложението върху бюджета на Съюза е слабо. Повече от 90 % от очакваните разходи в размер на 5,913 млн. EUR ще бъдат поети от държавите-членки, като има възможност за кандидатстване за финансиране от страна ЕС с цел намаляване на разходите.

5. ДОПЪЛНИТЕЛНА ИНФОРМАЦИЯ

- **Отмяна на съществуващо законодателство**

Приемането на предложението ще доведе до отмяна на съществуващото законодателство.

- **Териториален обхват**

Адресати на настоящата директива са държавите-членки в съответствие с Договорите.

2010/0273 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 83, параграф 1 от него,

като взеха предвид предложението на Европейската комисия[17],

след като представиха проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет,

като взеха предвид становището на Комитета на регионите,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Основната цел на директивата е да сближи правилата относно наказателното право на държавите-членки в сферата на атаките срещу информационни системи и да подобри сътрудничеството между съдебните и другите компетентни органи, в това число полицията и други специализирани правоприлагащи служби на държавите-членки.

(2) Атаките срещу информационните системи, по-специално в резултат на заплахата от организираната престъпност, представляват засилваща се опасност, а съществува и растяща загриженост от вероятни атаки по терористични или политически подбуди срещу информационните системи, които са част от критичната инфраструктура на държавите-членки и на Съюза. Това представлява заплаха за постигането на едно по-безопасно информационно общество и за изграждането на пространство на свобода, сигурност и правосъдие и следователно налага ответна реакция на равнището на Европейски съюз.

(3) Има доказателства за наличието на тенденция към все по-опасни и постоянни широкомащабни атаки срещу информационните системи, които са от решаващо значение за държавите или за определени функции в публичния или частния сектор. Тази тенденция се придружава от разработка на все по-усъвършенствани

[17] ОВ С […], […] г., стр. […].

инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки.

(4) Приемането на общи определения в тази област, по-конкретно за информационните системи и компютърните данни, е важно, за да се осигури последователен подход в държавите-членки при прилагането на директивата.

(5) Необходимо е да бъде постигнат общ подход към елементите, съставляващи престъпления, като незаконния достъп до информационни системи, незаконната намеса в такива системи, незаконната намеса в данните и незаконното прихващане, се обявят за общи престъпления.

(6) Държавите-членки следва да предвидят наказания за атаките срещу информационните системи. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи.

(7) Целесъобразно е да се предвидят по-строги санкции, когато атаката срещу дадена информационна система е извършена от организирана престъпна група, както е определено в Рамково решение на Съвета 2008/841/ПВР от 24 октомври 2008 г. относно борбата с организираната престъпност[18], когато атаката е широкомащабна, или когато престъплението е извършено с прикриване на истинската самоличност на извършителя и нанася щети на законния собственик на идентичността. Подходящо е също така да се предвидят по-сериозни наказания в случаите, когато такава атака е причинила сериозни щети или е засегнала съществени интереси.

(8) В заключенията на Съвета от 27—28 ноември 2008 г. се посочва, че следва да се разработи нова стратегия с участието на държавите-членки и Комисията, като се вземе предвид съдържанието на Конвенцията на Съвета на Европа от 2001 г. за престъпленията в кибернетичното пространство . Конвенцията е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и срещу атаките срещу информационните системи. Тази директива се основава Конвенцията.

(9) Като се има предвид различните начини, по които могат да бъдат извършени атаките, и с оглед на бързите промени в хардуера и софтуера, настоящата директива се отнася до „инструменти“, които могат да бъдат използвани за извършване на престъпленията, изброени в нея. Към инструментите се числи, например, зловредният софтуер, включително ботнети, използвани за извършване на кибератаки.

(10) Настоящата директива няма за цел да наложи наказателна отговорност за деяния извършени без престъпно намерение като, например, разрешените изпитвания или защитата на дадена компютърна система.

(11) С директивата се засилва значението на мрежите, като тази на Г—8 или Съвета на Европа, съставена от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата с цел обмен на информация относно оказване на незабавно съдействие за разследвания и производства по

[18] ОВ L 300, 11.11.2008 г., стр. 42.

престъпления, свързани с информационни системи или данни, или за събиране на доказателства в електронна форма за престъпления. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни атаки, държавите-членки следва да реагират незабавно на спешни искания, отправени по тази мрежа от звена за контакт. Такова съдействие следва да включва улесняването или прякото вземане на мерки като, например: предоставяне на технически консултации, опазване на данни, събирането на доказателства, предоставяне на правна информация и намирането на заподозрени лица.

(12) Необходимо е да се съберат данни за престъпления по настоящата директива, за да се добие по-цялостна представа за проблема на съюзно равнище и по този начин да се допринесе за изготвянето на по-ефективни отговори. Освен това данните ще помогнат на специализираните агенции като Европол и Европейската агенция за мрежова и информационна сигурност да оценят по-добре мащаба на престъпленията в кибернетичното пространство и състоянието на мрежовата и информационната сигурност в Европа.

(13) Значителните пропуски и различия в законите на държавите-членки в тази област могат да препятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят ефективното полицейско и съдебно сътрудничество в тази област. Транснационалният характер на съвременните информационни системи, които функционират отвъд националните граници, предполага, че атаките срещу тези системи често имат трансгранично измерение, което показва още веднъж спешната необходимост от осъществяване на действия за сближаване на наказателното право в тази област. Освен това координирането на наказателното преследване по дела за атаки срещу информационни системи ще стане по-лесно с приемането на Рамково решение 2009/948/ПВР на Съвета относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства.

(14) Понеже целите на настоящата директива, а именно да се гарантира, че атаките срещу информационните системи във всички държави-членки се наказват с ефективни, пропорционални и възпиращи наказания, както и подобряването и насърчаването на сътрудничеството между съдебните системи чрез премахването на потенциалните усложнения, не могат да бъдат постигнати в достатъчна степен от държавите-членки, тъй като правилата трябва да бъдат еднакви и съвместими, и следователно могат да бъдат по-добре постигнати на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, посочен в член 5 от Договора за Европейския съюз. Настоящата директива не надхвърля необходимото за постигането на тези цели.

(15) Всички лични данни, обработвани в контекста на прилагането на настоящата директива, трябва да бъдат защитени в съответствие с правилата за защита на данните, определени в Рамковото решение на Съвета 2008/977/ПВР от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси[19] за дейностите по обработка, които попадат в неговия обхват, както и в Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000

[19] ОВ L 350, 30.12.2008 г., стр. 60.

година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни[20].

(16) В настоящата директива се зачитат основните права и се съблюдават принципите, признати по-специално в Хартата на основните права на Европейския съюз, а именно защитата на личните данни, свободата на изразяване и на информацията, правото на справедлив съдебен процес, презумпцията за невинност и правото на ефективна правна защита, както и принципите на законност и пропорционалност между престъпления и наказания. По-специално, настоящата директива има за цел да осигури пълното спазване на тези права и принципи и трябва да бъде прилагана в съответствие с това.

(17) [В съответствие с членове 1, 2, 3 и 4 от Протокола относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, приложен към Договора за функционирането на Европейския съюз, Обединеното кралство и Ирландия са уведомили за желанието си да участват в приемането и прилагането на настоящата директива] ИЛИ [Без да се засяга член 4 от Протокола относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, Обединеното кралство и Ирландия няма да участват в приемането на настоящата директива и следователно няма да бъдат обвързани с нея и няма да я прилагат].

(18) В съответствие с членове 1 и 2 от Протокола относно позицията на Дания, приложен към Договора за функционирането на Европейския съюз, Дания не участва в приемането на настоящата директива и следователно не е обвързана с нея и няма да я прилага,

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

Член 1
Предмет

С директивата се определят престъпленията в областта на атаките срещу информационните системи и се установяват минимални правила за налагане на наказания за такива престъпления. С нея се цели също създаването на общи разпоредби за предотвратяване на подобни атаки и подобряване на европейското сътрудничество в областта на наказателното правосъдие.

Член 2
Определения

За целите на настоящата директива се прилагат следните определения:

а) „информационна система“ означава всяко устройство или група от свързани или подобни устройства, едно или повече от които, съобразно дадена програма, извършват автоматична обработка на компютърни данни, както и

[20] ОВ L 8, 12.1.2001 г., стр. 1.

компютърните данни, съхранявани, обработвани, извличани или пренасяни от тези устройства с цел оперирането с тези данни и използването, защитата и поддръжката им;

б) „компютърни данни“ означава представянето на факти, информация или понятия във форма, удобна за обработка в информационни системи, включително и програмите, задаващи указания на информационни системи за изпълнение на определени функции;

в) „юридическо лице“ означава всеки субект, притежаващ такъв статус съгласно приложимото законодателство, с изключение на държави или други публични органи при упражняване на държавна власт, както и на публични международни организации;

г) „неправомерен“ означава достъп или намеса, който/която не е разрешен/а от собственика или от други притежатели на права върху системата или части от нея, или е забранен/а по силата на националното законодателство.

Член 3

Незаконен достъп до информационни системи

Държавите-членки предприемат необходимите мерки, за да гарантират, че всеки умишлен неправомерен достъп до цялата информационна система или до части от нея е наказуем като престъпление поне в случаите, в които то не се счита за леко.

Член 4

Незаконна намеса в система

Държавите-членки гарантират, че всяко умишлено сериозно възпрепятстване или спиране на функционирането на информационна система чрез неправомерно въвеждане, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или спиране на достъпа до компютърни данни е наказуемо като престъпление поне в случаите, в които то не се счита за леко.

Член 5

Незаконна намеса в данни

Държавите-членки гарантират, че всяко умишлено изтриване, увреждане, влошаване, променяне, скриване или спиране на достъпа до компютърни данни в дадена информационна система е наказуемо като престъпно деяние поне в случаите, в които престъплението не се счита за леко.

Член 6

Незаконно прихващане

Държавите-членки приемат необходимите законодателни мерки, за да гарантират, че извършеното с технически средства умишлено прихващане на непублични компютърни данни, изпращани до дадена информационна система, от нея или в нейните рамки,

включително електромагнитните емисии от информационна система, пренасящи такива компютърни данни, се наказва като престъпление, когато е извършено неправомерно.

Член 7

Инструменти, използвани за извършване на престъпления

Държавите-членки приемат необходимите мерки, за да гарантират, че производството, продажбата, доставянето за употреба, вносът, притежаването, разпространението или друга форма на предоставяне на изброеното по-долу, се наказва като престъпление, когато е направено умишлено и неправомерно с цел извършване на престъпленията, посочени в членове 3—6:

а) устройство, включително компютърна програма, конструирано или адаптирано главно за извършване на престъпление, посочено в съответствие с членове 3–6;

б) компютърна парола, код за достъп или други подобни данни, с чиято помощ може да се получи достъп до информационна система или до част от нея,

Член 8

Подстрекателство, съучастничество и опит за извършване на престъпление

1. Държавите-членки гарантират, че подстрекателството, подпомагането и съдействието за извършване на престъпленията, посочени в членове 3—7, са наказуеми като престъпления.

2. Държавите-членки гарантират, че опитът за извършване на престъпленията, посочени в членове 3—6, е наказуем като престъпление.

Член 9

Санкции

1. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—8, са наказуеми с ефективни, пропорционални и разубеждаващи наказания.

2. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—7, се наказват с лишаване от свобода за максимален срок не по-малък от *две години*.

Член 10

Утежняващи обстоятелства

1. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—7, се наказват с лишаване от свобода за максимален срок не по-малък от пет години, когато те са извършени в рамките на престъпна организация, както е определено в Рамково решение 2008/841/ПВР.

2. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—6, се наказват с лишаване от свобода за максимален срок не по-малък от пет години, когато те са извършени чрез използване на инструменти, предназначени за започване на атаки, засягащи значителен брой информационни системи, или на атаки, причиняващи значителни щети като, например, прекъснати системни услуги, финансови разходи или загуба на лични данни.

3. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—6, се наказват с лишаване от свобода за максимален срок не по-малък от пет години, когато те са извършени с прикриване на истинската самоличност на извършителя и нанасят щети на законния собственик на идентичността.

Член 11

Отговорност на юридически лица

1. Държавите-членки вземат необходимите мерки, за да гарантират, че юридическите лица могат да бъдат подведени под отговорност за престъпленията, посочени в членове 3─8, извършени в тяхна полза от лице, което действа самостоятелно или като част от орган на юридическото лице и което заема ръководна длъжност в това юридическо лице, въз основа на едно от следните:

а) право да представлява юридическото лице;

б) право да взема решения от името на юридическото лице;

в) правомощие да упражнява контрол в рамките на юридическото лице.

2. Държавите-членки вземат необходимите мерки, за да гарантират, че юридическите лица могат да бъдат подведени под отговорност, когато липсата на надзор или контрол от страна на лице, посочено в параграф 1, е направила възможно извършването от негово подчинено лице на някое от престъпленията, посочени в членове 3─8, в полза на това юридическо лице.

3. Отговорността на юридическите лица съгласно параграфи 1 и 2 не изключва образуването на наказателни производства срещу физически лица, които са извършители или съучастници на престъпления, посочени в членове 3─8.

Член 12

Наказания спрямо юридически лица

1. Държавите-членки предприемат необходимите мерки, за да гарантират, че юридическото лице, подведено под отговорност съгласно член 11, параграф 1, подлежи на наказания, които са ефективни, пропорционални и възпиращи, които включват глоби по наказателното право и друг вид глоби и може да включват други санкции, като например:

а) лишаване от правото да се ползва от обществени облаги или помощи;

б) временно или постоянно лишаване от правото да упражнява търговска дейност;

в) поставяне под съдебен надзор;

г) съдебна ликвидация;

д) временно или постоянно затваряне на предприятия, използвани за извършване на престъплението.

2. Държавите-членки предприемат необходимите мерки, за да гарантират, че юридическите лица, подведени под отговорност съгласно член 11, параграф 2, ще бъдат наказани с ефективни, пропорционални и възпиращи наказания или мерки.

Член 13
Компетентност

1. Държавите-членки създават своя юрисдикция за престъпните деяния, посочени в членове 3—8, когато престъплението е извършено:

а) изцяло или отчасти на територията на съответната държава-членка или

б) от неин гражданин или от лице, което обичайно пребивава на територията на съответната държава-членка; или

в) в полза на юридическо лице, чието главно управление е разположено на територията на съответната държавата-членка.

2. При създаването на юрисдикция в съответствие с параграф 1, буква а) държавите-членки гарантират, че тази юрисдикция разглежда случаи, при които:

а) нарушителят извършва престъплението, когато се намира физически на територията на съответната държава-членка, независимо дали престъплението е насочено срещу информационна система, намираща се на нейна територия; или

б) престъплението е насочено срещу информационна система, намираща се на територията на съответната държава-членка, независимо дали нарушителят се намира физически на нейна територия, когато го извършва.

Член 14
Обмен на информация

1. За целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8, и в изпълнение на изискванията относно защитата на данни, държавите-членки използват съществуващата мрежа от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. Държавите-членки гарантират също, че разполагат с процедури,

чрез които да отговарят на спешни искания в максимален срок от осем часа. В този отговор се посочва поне дали, кога и под каква форма ще бъде отговорено на искането за помощ.

2. Държавите-членки информират Комисията за определеното от тях звено за контакт относно обмена на информация за престъпления, посочени в членове 3—8. Комисията съобщава тази информация на другите държави-членки.

Член 15
Контрол и статистика

1. Държавите-членки гарантират наличието на система за записване, производство и предоставяне на статистически данни за престъпленията, посочени в членове 3—8.

2. Като минимум посочената в параграф 1 статистика обхваща броя на посочените в членове 3—8 престъпления, за които е докладвано на държавите-членки, и последващи мерки по тези доклади. В нея се посочва също на годишна база броят на разследваните случаи, за които е докладвано, броят на лицата, срещу които е повдигнато обвинение, и броят на осъдените лица за престъпленията, посочени в членове 3—8.

3. Държавите-членки предават на Комисията събраните по този член данни. Те правят също необходимото консолидираният преглед на тези статистически отчети да бъде публикуван.

Член 16
Отмяна на Рамково решение 2005/222/ПВР

С настоящото се отменя Рамково решение 2005/222/ПВР, без да се засягат задълженията на държавите-членки относно сроковете за транспониране в националното законодателство.

Позоваванията на отменението рамково решение се считат за позовавания на настоящата директива.

Член 17
Транспониране

1. Държавите-членки въвеждат в сила законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата директива, не по-късно от [2 години след приемането]. Те незабавно съобщават на Комисията текста на тези разпоредби и прилагат таблица на съответствието между разпоредбите и настоящата директива. Когато държавите-членки приемат тези разпоредби, в тях се съдържа позоваване на настоящата директива или това позоваване се извършва при официалното им публикуване. Условията и редът на позоваване се определят от държавите-членки.

2. Държавите-членки съобщават на Комисията текста на основните разпоредби от националното законодателство, които те приемат в областта, уредена с настоящата директива.

Член 18
Докладване

1. До [ЧЕТИРИ ГОДИНИ СЛЕД ПРИЕМАНЕТО] и на всеки три години след това Комисията представя на Европейския парламент и на Съвета доклад за прилагането на директивата в държавите-членки, който съдържа и всяко необходимо предложение.

2. Държавите-членки изпращат на Комисията цялата информация, необходима за изготвянето на посочения в параграф 1 доклад. Информацията съдържа подробно описание на законодателните и незаконодателните мерки в приложение на настоящата директива.

Член 19
Влизане в сила

Настоящата директива влиза в сила на двадесетия ден след публикуването ѝ в *Официален вестник на Европейския съюз*.

Член 20
Адресати

Адресати на настоящата директива са държавите-членки в съответствие с Договорите.

Съставено в Брюксел,

За Европейския парламент	*За Съвета*
Председател	*Председател*