ЕВРОПЕЙСКИ ПАРЛАМЕНТ 2009 - 2014

Документ за разглеждане в заседание

A7-0224/2013

18.6.2013

***I
ДОКЛАД

относно предложението за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Комисия по граждански свободи, правосъдие и вътрешни работи

Докладчик: Моника Холмайер

Легенда на използваните знаци

*	Процедура на консултация
***	Процедура на одобрение
***I	Обикновена законодателна процедура (първо четене)
***II	Обикновена законодателна процедура (второ четене)
***III	Обикновена законодателна процедура (трето четене)

(Посочената процедура се базира на правното основание, предложено в проекта на акт.)

Изменения към проект на акт

Измененията към проекта на акт, внесени от Парламента, се обозначават в ***получер курсив***. Отбелязването в *курсив* е предназначено за съответните технически служби и се отнася до частите от проекта на акт, за които е предложено изменение с оглед изготвяне на окончателния текст (например очевидно грешни или липсващи части в текста на даден език). Предложенията за поправка подлежат на съгласуване със засегнатите технически служби.

Антетката на всяко изменение към съществуващ акт, който проектът на акт има за цел да измени, съдържа трети и четвърти ред, където се посочват съответно съществуващият акт и засегнатата разпоредба от него. Възпроизведените части от разпоредба на съществуващ акт, която Парламентът желае да измени, но която остава непроменена в проекта на акт, се отбелязват с **получер** шрифт. Евентуални заличавания, които засягат такива части от текста се обозначават по следния начин: **[...]**.

СЪДЪРЖАНИЕ

Страница

ПРОЕКТ НА ЗАКОНОДАТЕЛНА РЕЗОЛЮЦИЯ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

относно предложението за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Обикновена законодателна процедура: първо четене)

Европейският парламент,

– като взе предвид предложението на Комисията до Европейския парламент и Съвета (COM(2010)0517),

– като взе предвид член 294, параграф 2 и член 83, параграф 1 от Договора за функционирането на ЕС, съгласно които Комисията е внесла предложението (C7-0293/2010),

– като взе предвид член 294, параграф 3 от Договора за функционирането на ЕС,

– като взе предвид становището на Икономическия и социален комитет от 4 май 2011 г.[1],

– като взе предвид поетия с писмо от xxx ангажимент на представителя на Съвета за одобряване на позицията на Европейския парламент съобразно член 294, параграф 4 от Договора за функционирането на ЕС,

– като взе предвид член 55 от своя правилник,

– като взе предвид доклада на комисията по граждански свободи, правосъдие и вътрешни работи и становищата на комисията по външни работи и на комисията по промишленост, изследвания и енергетика (A7-0224/2013),

1. приема изложената по-долу позиция на първо четене;

2. изисква от Комисията да се отнесе до него отново, в случай че възнамерява да внесе съществени промени в своето предложение или да го замени с друг текст;

3. възлага на своя председател да предаде позицията на Парламента съответно на Съвета и на Комисията, както и на националните парламенти.

Изменение 129
Предложение за директива
–

[1] ОВ C 218, 23.7.2011 г., стр. 130.

ИЗМЕНЕНИЯ, ВНЕСЕНИ ОТ ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ,*

към предложението на Комисията

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

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

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия[1],

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[2],

като взеха предвид становището на Комитета на регионите,

в съответствие с обикновената законодателна процедура,

---

* Изменения: нов или изменен текст се обозначава с получер курсив; заличаванията се посочват със символа ▌.

1 ОВ С […], […] г., стр. […].

2 ОВ С *[...], [...] г.,* стр. *[...].*

като имат предвид, че:

(1) Целта на настоящата директива е да сближи ***наказателното законодателство*** на държавите членки в сферата на атаките срещу информационните системи ***посредством установяването на минимални правила относно квалифицирането на престъпленията и определянето на санкции в тази област и да*** подобри сътрудничеството между ▌ компетентните органи, в това число полицията и други специализирани правоприлагащи служби на държавите членки, ***както и компетентните специализирани агенции на Съюза като Евроюст, Европол и Европейския център по киберпрестъпност към него, както и Европейската агенция за мрежова и информационна сигурност (ENISA)***.

(1a) Информационните системи представляват ключов елемент от политическото, социалното и икономическото взаимодействие в Съюза. Все по-често и в по-голяма степен обществото зависи от подобни системи. Безпроблемното функциониране и сигурността на тези системи в Съюза са от жизненоважно значение за развитието на вътрешния пазар и на конкурентоспособна и иновационна икономика. Осигуряването на подходящи равнища на защита на информационните системи следва да бъде част от цялостна ефективна рамка за превантивни мерки, съпътстваща реакцията на наказателното право спрямо киберпрестъпността.

(2) Атаките срещу информационните системи, по-специално ***атаките, свързани с*** организираната престъпност, представляват засилваща се опасност ***както в ЕС, така и в световен мащаб***, 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 Европейския съюз, ***а също така и по-добра координация и сътрудничество на международно равнище***.

(2a) В Съюза съществува определен брой критични инфраструктури, чието нарушаване или унищожаване би довело до значителни трансгранични последици. От необходимостта да се подобрят способностите за защита на критичните инфраструктури в Съюза става ясно, че мерките срещу кибератаките следва да бъдат допълнени от строги наказателни санкции, отразяващи тежестта на подобни атаки. Като критична инфраструктура могат да се разглеждат разположени в държавите членки активи, системи или части от тях, които са от съществено значение например за поддържането на основните функции на обществото, здравеопазването, безопасността, сигурността, икономическото или социалното благосъстояние на хората, като електроцентрали, транспортни мрежи или правителствени мрежи, и чието нарушаване или унищожаване би имало значително въздействие върху дадената държава членка поради неспособността за поддържане на тези функции.

(3) Има доказателства за наличието на тенденция към все по-опасни и повтарящи се широкомащабни атаки срещу информационните системи, които ***често могат да бъдат*** от решаващо значение за държавите или за определени функции в публичния или частния сектор. Тази тенденция е придружена от разработката на все по-усъвършенствани ***методи, като например създаването и използването на така наречените ботнети, които се характеризират с последващи етапи на престъпното деяние, при които всеки етап поотделно би могъл да създаде сериозна заплаха за обществения интерес. Във връзка с това директивата има за цел, inter alia, да въведе наказателни санкции за етапа на създаване на ботнета, по-конкретно за етапа на установяване на контрол от разстояние върху значителен брой компютри посредством заразяването им със зловреден софтуер чрез целенасочени кибератаки. На по-късен етап заразената мрежа от компютри, която представлява ботнетът, може да бъде активирана без знанието на потребителите на компютрите, за да извърши широкомащабна кибератака, която обикновено е в състояние да причини сериозни щети, както е посочено в настоящата директива. Държавите членки могат да определят кое представлява сериозна щета съгласно националното право и практика, като това може да включва нарушени системни услуги от важно обществено значение или сериозни финансови разходи или загуба на лични данни или чувствителна информация.***

(3а) Широкомащабните атаки могат да предизвикат съществени икономически щети, както поради прекъсването на информационните системи и комуникации, така и поради загуба или промяна на важна от търговска гледна точка поверителна информация или други данни. Особено внимание следва да се обърне на повишаването на осведомеността на иновативните малки и средни предприятия за подобни заплахи и уязвимости, тъй като тези предприятия зависят във все по-голяма степен от правилното функциониране и наличност на информационните системи и често разполагат с ограничени ресурси за информационна сигурност.

(4) Приемането на общи определения в тази област е важно, за да се осигури последователен подход в държавите членки при прилагането на настоящата директива.

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

(5а) Прихващането включва, но не се ограничава непременно до слушането, мониторинга или наблюдението на съдържанието на съобщения и достигането до съдържанието на данни с технически средства пряко, чрез достъп до информационни системи и тяхното използване, или непряко, чрез използване на електронно подслушване или подслушвателни устройства.

(6) Държавите членки следва да предвидят санкции за атаките срещу информационните системи. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи ***и следва да включват лишаване от свобода и/или финансови санкции***.

(6а) Директивата предвижда наказателни санкции най-малкото за случаите, които не се считат за леки. Държавите членки могат да решат какво представлява лек случай в зависимост от своето национално право и практика. Даден случай може да се счете за лек, например ако причинените от престъплението щети и/или рискът, който то поражда за публичните или частните интереси, например по отношение на целостта на компютърната система или компютърните данни или по отношение на неприкосновеността на дадено лице, неговите права и други интереси, са незначителни или от такова естество, че не е необходимо да се налага наказателна санкция в съответната, предвидена в правните разпоредби степен или наказателна отговорност.

(6б) Установяването и докладването на заплахи и рискове, произтичащи от кибератаки, както и на свързаните с тях уязвимости на информационните системи, са елементи, които имат отношение към ефективната превенция и реакция на кибератаките и към повишаването на сигурността на информационните системи. За постигането на тези цели добавена стойност може да има осигуряването на стимули за докладване на пропуски по отношение на сигурността. Държавите членки следва да полагат усилия за предоставянето на възможности, които да позволяват от правна гледна точка откриването и докладването на пропуски по отношение на сигурността.

(7) Целесъобразно е да се предвидят по-строги санкции, когато атаката срещу дадена информационна система е извършена от престъпна организация, съгласно определението в Рамково решение 2008/841/ПВР на Съвета от 24 октомври 2008 г. относно борбата с организираната престъпност[1], ***или*** когато атаката е широкомащабна ***и така е засегнала значителен брой информационни системи или е причинила сериозни щети, включително когато целта на атаката е създаването на ботнет или тя е извършена посредством ботнет, като по този начин е причинила сериозни щети***. Също така е целесъобразно да се предвидят по-строги санкции, когато подобна атака ***е извършена срещу критична инфраструктура***.

(7a) Друг съществен елемент от интегрирания подход срещу киберпрестъпността представлява установяването на ефективни мерки срещу кражбата на самоличност и други престъпления, засягащи самоличността. Евентуалната нужда от действия на ЕС във връзка с този вид престъпни деяния може да се разглежда и в контекста на оценката доколко е необходим цялостен хоризонтален инструмент на ЕС.

(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 престъпления в кибернетичното пространство. Тази конвенция е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и с атаките срещу информационните системи. Настоящата директива се основава на конвенцията. ***Ето защо като приоритет следва да се разглежда приключването на процеса на ратификация на конвенцията от всички държави членки във възможно най-кратък срок.***

[1] ОВ L 300, 11.11.2008 г., стр. 42.

(9) Като се имат предвид различните начини, по които могат да бъдат извършени атаките, и с оглед на бързите промени в хардуера и софтуера, в настоящата директива ***се съдържа позоваване на*** „инструменти“, които могат да бъдат използвани за извършване на престъпленията, изброени в нея. Към инструментите се числи например зловреднияят софтуер, включително ***този, с който могат да се създават*** ботнети, използвани за извършване на кибератаки. ***Макар даден инструмент да бъде подходящ или дори да бъде особено подходящ за извършването на посочените престъпления, той може все пак да се произвежда за законни цели. Поради необходимостта да се избегне инкриминиране на случаите, когато подобни инструменти се произвеждат и предлагат на пазара за законни цели като например изпитване на надеждността на информационни продукти или сигурността на информационни системи, освен изискването за общ умисъл трябва да бъде изпълнено и изискването за пряк умисъл тези инструменти да се използват за извършването на някое от престъпленията, посочени в Директивата.***

I

(10а) Настоящата директива няма за цел да налага наказателна отговорност в случаите, когато са изпълнени обективните критерии за престъпленията, изброени в настоящата директива, но деянията са извършени без престъпно намерение, като при незнание, че достъпът не е разрешен, или при възложено изпитване или защита на информационните системи, например когато дружество или продавач определи дадено лице за изпитване на устойчивостта на системата му за сигурност. В контекста на настоящата директива договорните задължения или споразуменията за ограничаване на достъпа до информационни системи посредством правила за потребителите или условия за използване на услугата, както и трудовите спорове във връзка с достъпа до информационни системи на работодателя и използването им за лични цели, не следва да водят до наказателна отговорност, когато достъпът при такива обстоятелства се счита за неразрешен и това представлява единственото основание за наказателно производство. Настоящата директива не засяга гарантираното от правна гледна точка право на достъп до информация, установено в националното законодателство и законодателството на ЕС, като същевременно тя не може да се използва като освобождаване, което оправдава незаконен и произволен достъп до информация.

(10б) Редица обстоятелства могат да улеснят извършването на кибератаки, като например случаите, когато извършителят в рамките на своята трудова заетост има достъп до системите за сигурност, които са част от засегнатите информационни системи. В контекста на националното право такива обстоятелства следва да бъдат отчетени в подходяща степен в хода на наказателното производство.

(10в) Държавите членки следва да предвидят в националното си право утежняващи вината обстоятелства в съответствие с приложимите правила, предвидени в техните правни системи относно утежняващите вината обстоятелства. Държавите членки следва да гарантират, че съдиите разполагат с възможност да разглеждат тези утежняващи вината обстоятелства при осъждането на нарушителите. Съдията по своя преценка оценява тези обстоятелства заедно с останалите фактически елементи по конкретния случай.

(10г) Настоящата директива не урежда условията, които следва да бъдат изпълнени, за да се упражни компетентност над което и да било от посочените в членове 3—8 престъпления, например съобщаване от страна на жертвата на мястото, където е извършено престъплението, или повдигане на обвинение в държавата, в която е извършено престъплението, или факта, че нарушителят не е бил обект на наказателно преследване на мястото, където е извършено престъплението.

(10д) В контекста на настоящата директива държавите и публичните органи продължават да бъдат задължени да гарантират зачитането на правата на човека и основните свободи в съответствие със съществуващите международни задължения.

(11) С настоящата директива се засилва значението на мрежите, като тези на Г-8 или Съвета на Европа, съставени от звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. ***Подобни звена за контакт следва да бъдат в състояние да осигуряват ефективна помощ и по този начин да улесняват например обмена на подходяща налична информация или предоставянето на технически съвети или правна информация*** за целите на разследвания или производства по престъпления, ***отнасящи се*** информационните системи и ***свързаните данни, с участието на молещата държава членка***. ***За да се осигури гладкото функциониране на мрежите, всяко звено за контакт следва да разполага с капацитет за бързо осъществяване на връзка със звено за контакт на друга държава членка в допълнение, inter alia, към обучен и оборудван персонал***. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни ***кибер***атаки, държавите членки следва да са в състояние да реагират своевременно на спешни искания, отправени по тази мрежа от звена за контакт. ***В подобни случаи може да бъде наложително искането за информация да се придружава от телефон за връзка, за да се гарантира, че замолената държава членка ще обработи своевременно искането и обратната информация ще бъде предоставена в рамките на 8 часа.***

(11a) Сътрудничеството между публичните органи, частния сектор и гражданското общество е от голямо значение за превенцията и борбата с атаките срещу информационните системи. Необходимо е да се насърчава и подобрява сътрудничеството между доставчиците на услуги, производителите, правоприлагащите и съдебните органи при пълно зачитане на принципите на правовата държава. Сътрудничеството може да включва например съдействие от доставчиците на услуги при помощта за съхраняване на евентуални доказателства, при предоставянето на елементи, които да спомогнат за идентифицирането на извършителите, и като крайна мярка, при частичното или пълното спиране в съответствие с националното право, включително националното законодателство и практика, на информационните системи или функции, които са били засегнати или използвани за незаконни цели. Държавите членки следва да обмислят също създаването на мрежи за сътрудничество и партньорство с доставчиците на услуги и производителите за обмен на информация във връзка с нарушенията, които попадат в обхвата на настоящата директива.

I

(12а) Необходимо е да се събират съпоставими данни за нарушенията, посочени в настоящата директива. Съответните данни следва да се предоставят на компетентните специализирани агенции като Европол и Европейската агенция за мрежова и информационна сигурност в съответствие със задачите и информационните им потребности, за да се добие по-цялостна представа за проблема с киберпрестъпността и мрежовата и информационна сигурност на равнището на ЕС и по този начин се допринесе за изготвянето на по-ефективна реакция. Държавите членки следва да предоставят на Европол и Европейския център по киберпрестъпност към него информация за начина на действие на извършителите, за да се извърши оценка на заплахите и стратегически анализ на киберпрестъпността в съответствие с Решение 2009/371/ПВР на Съвета. Предоставянето на информация може да улесни по-доброто разбиране на настоящите и бъдещите заплахи, като допринесе за по-подходящо и целенасочено вземане на решения относно борбата с атаките срещу информационните системи и тяхното предотвратяване.

(12б) В съответствие с настоящата директива Комисията трябва да представи доклад за прилагането ѝ и да направи необходимите законодателни предложения, които евентуално да разширят обхвата на настоящата директива, отчитайки промените в областта на киберпрестъпността. Тези промени могат да включват всяко технологично развитие, което позволява например по-ефективно прилагане в областта на атаките срещу информационните системи или улеснява предотвратяването на подобни атаки или смекчаването на последиците от тях. За тази цел Комисията следва да вземе под внимание наличните анализи и доклади, изготвени от съответните заинтересовани страни, и по-специално от Европол и ENISA.

(12в) С цел ефективна борба с престъпленията в кибернетичното пространство е необходимо също така да се повиши устойчивостта на информационните системи с предприемането на подходящи мерки за по-ефективната им защита от кибератаки. Държавите членки следва да предприемат необходимите мерки за защита на критичните инфраструктури от кибератаки и следва да обмислят защитата на информационните системи и свързаните данни като част от тази защита. Осигуряването на подходящо равнище на защита и сигурност на информационните системи от юридически лица, например във връзка с предоставянето на обществено достъпни електронни съобщителни услуги съгласно действащото законодателство на ЕС относно неприкосновеността на личния живот, електронните съобщения и защитата на данните, представлява съществена част от цялостния подход за ефективна борба срещу киберпрестъпността. Следва да се осигуряват подходящи равнища на защита срещу заплахи и уязвимости, които могат да бъдат разумно идентифицирани, в съответствие със съвременните постижения в конкретните сектори и предвид конкретните ситуации, свързани с обработването на данни. Разходите и тежестта по осигуряване на такава защита следва да бъдат пропорционални на вероятните щети, които евентуална кибератака може да причини на засегнатите лица. Държавите членки се насърчават да предвидят в националното си право подходящи мерки, водещи до отговорност, за случаите, когато юридическо лице явно не е осигурило подходящо равнище на защита срещу кибератаки.

(13) Значителните пропуски и различия в законите ***и наказателните производства*** на държавите членки в областта на атаките срещу информационните системи ▌могат да възпрепятстват 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 имат ***трансгранично*** измерение, което показва още веднъж спешната необходимост от осъществяване на допълнителни действия за сближаване на наказателното право в тази област. Освен това координирането на наказателното преследване по дела за атаки срещу информационни системи следва да бъде улеснено с ***подходящото изпълнение и прилагане*** на Рамково решение 2009/948/ПВР на Съвета относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства. ***В сътрудничество с Европейския съюз държавите членки следва също да се стремят към подобряване на международното сътрудничество по въпросите на сигурността на информационните системи, компютърните мрежи и данни. При всяко международно споразумение, включващо обмен на данни, следва надлежно да се разгледа сигурността на прехвърлянето и съхраняването на данните.***

(13а) По-доброто сътрудничество между компетентните правоприлагащи и съдебни органи в Съюза е изключително важно за ефективната борба срещу престъпленията в кибернетичното пространство. Във връзка с това следва да се насърчава активизирането на усилията за осигуряване на подходящо обучение за съответните органи, за да се подобри разбирането за киберпрестъпността и нейните последици, и за стимулиране на сътрудничеството и обмена на най-добри практики, например чрез компетентните специализирани агенции на ЕС. Целта на подобно обучение, inter alia, следва да бъде повишаването на осведомеността за различните национални правни системи, евентуалните правни и технически предизвикателства при наказателни разследвания или разпределението на области на компетентност между съответните национални органи.

(14) Тъй като целите на настоящата директива, а именно да се гарантира, че атаките срещу информационните системи се наказват във всички държави членки с ефективни, пропорционални и възпиращи санкции, както и да се подобри и насърчи съдебното сътрудничество 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.

I

(15a) Защитата на личните данни е основно право в съответствие с член 16, параграф 1 от ДФЕС и член 8 от Хартата на основните права. Ето защо всяко обработване на лични данни при изпълнението на настоящата директива следва изцяло да зачита съответното законодателство на ЕС относно защитата на данните, прието въз основа на Договорите.

(16) В настоящата директива следва да се зачитат основните ***свободи и*** права и да се съблюдават принципите, признати по-специално в Хартата на основните права на Европейския съюз ***и Европейската конвенция за защита на правата на човека и основните свободи***, включително защитата на личните данни, ***зачитането на личния живот***, свободата на изразяване и на информация, правото на справедлив съдебен процес, презумпцията за невиновност и правото на защита, както и принципите на законност и пропорционалност между престъплението и наказанието. 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 член 3*** 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 вземат участие в приемането и прилагането на настоящата директива ▌ .

(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 не я прилага.

(19) Настоящата директива има за цел да измени и разшири обхвата на разпоредбите на Рамково решение 2005/222/ПВР. Тъй като измененията, които трябва да се направят, са значителни по брой и естество, за по-голяма яснота рамковото решение следва да бъде изцяло заменено по отношение на държавите членки, участващи в приемането на настоящата директива,

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

Член 1

Предмет

Настоящата директива установява минимални правила относно квалифицирането на престъпленията и санкциите в областта на атаките срещу информационните системи. Тя има за цел също да способства за предотвратяването на тези престъпления и да подобри сътрудничеството между съдебните и други компетентни органи.

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 компютърните данни, съхранявани, обработвани, извличани или предавани 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, подходяща 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 статут съгласно приложимото право, с изключение на държави или други публични органи при упражняване на държавна власт, както и на публични международни организации;

г) „неправомерен“ означава ***достъп, намеса, прихващане или всякакво друго действие, посочено в настоящата директива***, което не е разрешено от собственика или от други притежатели на права върху системата или части от нея, или е забранено по силата на националното законодателство.

Член 3

Незаконен достъп до информационни системи

Държавите членки предприемат необходимите мерки, за да гарантират, че ***когато е извършен умишлено,*** неправомерният достъп до цялата информационна система или до части от нея е наказуем като престъпление***, когато е извършен чрез нарушаване на мярка за сигурност*** и поне в случаите, които не се считат за леки.

Член 4

Незаконна намеса в система

Държавите членки предприемат необходимите мерки, за да гарантират, че ▌ сериозното възпрепятстване или спиране на функционирането на информационна система чрез въвеждане, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или спиране на достъпа до компютърни данни е наказуемо като престъпление, когато е извършено ***умишлено и*** неправомерно, поне в случаите, които не се считат за леки.

Член 5

Незаконна намеса в данни

Държавите членки предприемат необходимите мерки, за да гарантират, че ▌ изтриването, увреждането, влошаването, променянето, скриването или спирането на достъпа до компютърни данни в дадена информационна система е наказуемо като престъпление, когато е извършено ***умишлено и*** неправомерно, поне в случаите, които не се считат за леки.

Член 6

Незаконно прихващане

Държавите членки предприемат необходимите мерки, за да гарантират, че ▌ извършеното с технически средства 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, е наказуемо като престъпление, когато е извършено ***умишлено и неправомерно, поне в случаите, които не се считат за леки***.

Член 7

Инструменти, използвани за извършване на престъпления

1. Държавите членки предприемат необходимите ***мерки***, за да гарантират, че производството, продажбата, набавянето за употреба, вносът, ▌ разпространяването или друга форма на предоставяне на изброеното по-долу, е наказуемо като престъпление, когато е извършено умишлено и неправомерно ***с намерение да се използва*** за извършването на което и да било от престъпленията, посочени в членове 3—***6, поне в случаите, които не се считат за леки***:

а) ▌ компютърна програма, проектирана или адаптирана главно с цел извършване на което и да било от престъпленията, посочени в членове 3—6;

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

Член 8

Подбуждане, помагачество и съучастие и опит за извършване на престъпление

1. Държавите членки гарантират, че ***подбуждането***, помагачеството и съучастието ***за извършване на*** някое от престъпленията, посочени в членове 3—7, е наказуемо като престъпление.

2. Държавите членки гарантират, че опитът за извършване на ***престъпленията,*** посочени в ***членове 4—5***, е наказуем като престъпление.

Член 9

Санкции

1. Държавите членки предприемат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—8, са наказуеми с ефективни, ***пропорционални*** и възпиращи санкции.

2. Държавите членки предприемат 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, поне в случаите, които не се считат за леки***.

3. Държавите членки предприемат необходимите мерки, за да гарантират, че когато са извършени умишлено, посочените в членове 4—5 престъпления се наказват с лишаване от свобода за максимален срок, не по-малък от три години, когато значителен брой информационни системи са били засегнати посредством използването на инструмент, посочен в член 7, параграф 1, проектиран или адаптиран главно за тази цел.

4. Държавите членки предприемат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 4—5, се наказват с лишаване от свобода за максимален срок, не по-малък от пет години, когато:

а) са извършени в рамките на престъпна организация, съгласно определението в Рамково решение 2008/814/ПВР, независимо от размера на санкциите, посочени там, или

б) са причинили сериозни щети, или

в) са извършени срещу информационна система, която е част от критична инфраструктура.

5. Държавите членки предприемат необходимите мерки, за да гарантират, че когато престъпленията, посочени в членове 4 и 5, са извършени чрез злоупотреба с лични данни на друго лице, за да се спечели доверието на трето лице, и по този начин са нанесени щети на законния собственик на самоличността, това може да се разглежда съгласно съответните разпоредби на националното право като утежняващо вината обстоятелство, освен ако тези обстоятелства не са вече част от друго престъпление, което е наказуемо съгласно националното законодателство.

I

Член 11

Отговорност на юридическите лица

1. Държавите членки предприемат 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) пълномощие да представлява юридическото лице;

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

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

2. Държавите членки предприемат 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, ***подбудители*** или съучастници в престъпленията, посочени в членове 3—8.

Член 12

Санкции спрямо юридически лица

1. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическо лице, подведено под отговорност съгласно член 11, параграф 1, подлежи на санкции, които са ефективни, пропорционални и възпиращи, включват глоби по наказателното право или 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 структури, използвани за извършване на престъплението.

2. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическо лице, подведено под отговорност съгласно член 11, параграф 2, подлежи на ефективни, пропорционални и възпиращи санкции или мерки.

Член 13

Компетентност

1. Държавите членки установяват компетентността си по отношение на престъпленията, посочени в членове 3—8, когато престъплението е извършено:

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

аа) от техни граждани, поне в случаите, когато деянието се явява престъпление на мястото, където е извършено.

2. При установяването на компетентност в съответствие с параграф 1, буква а) ***дадената държава членка*** гарантира, че тази компетентност обхваща 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.

3. Дадена държава членка уведомява Комисията, когато реши да установи допълнителна компетентност по отношение на престъпления, посочени в членове 3—8, извършени извън нейната територия, например когато:

а) нарушителят има обичайно местопребиваване на територията на съответната държава членка; или

б) престъплението е извършено в полза на юридическо лице, установено на територията на съответната държава членка.

Член 14

Обмен на информация

1. За целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8, ***държавите членки осигуряват наличието на оперативно национално звено за контакт и*** 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 в случай на ***спешно искане да могат в рамките най-много на 8 часа да посочат поне дали на искането за помощ ще бъде отговорено, както и формата и приблизителното време за отговор***.

2. Държавите членки информират Комисията за определеното от тях звено за контакт за целите на обмена на информация за престъпленията, посочени в членове 3—8. Комисията съобщава тази информация на останалите държави членки ***и на компетентните специализирани агенции и органи на ЕС***.

3. Държавите членки предприемат необходимите мерки, за да гарантират наличието на подходящи канали за докладване с цел да се улесни докладването без необосновано забавяне на компетентните национални органи за престъпления, посочени в членове 3—6.

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—***7***.

2. Статистическите данни, посочени в параграф 1, като минимум включват ***съществуващите данни относно*** броя на посочените в членове 3—***7*** престъпления, ***които са регистрирани от*** държавите членки, както и ▌броя на лицата, ***срещу които е възбудено наказателно преследване и които са осъдени*** за престъпления, посочени в членове 3—***7***.

3. Държавите членки предават на Комисията събраните по настоящия член данни. ***Комисията прави необходимото*** консолидираният преглед на тези статистически отчети да бъде публикуван ***и представен на компетентните специализирани агенции и органи на ЕС***.

Член 16

Замяна на Рамково решение 2005/222/ПВР

Рамково решение 2005/222/ПВР ***се заменя по отношение на държавите членки, които участват в приемането на настоящата директива***, без да се засягат задълженията на държавите членки, свързани със ***срока*** за транспониране ***на Рамковото решение*** в националното право.

По отношение на държавите членки, които участват в приемането на настоящата директива, позоваванията на Рамково решение ***2005/222/ПВР*** 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, до [две години от датата на приемане] ▌.

▌

3. Държавите членки съобщават на Комисията текста на разпоредбите, с които се транспонират в националното им право задълженията, наложени им с настоящата директива.

4. Когато държавите членки приемат тези мерки, в тях се съдържа позоваване на настоящата директива или то се извършва при официалното им публикуване. Условията и редът на позоваване се определят от държавите членки.

Член 18

Докладване

▌

До [ЧЕТИРИ ГОДИНИ ОТ ДАТАТА НА ПРИЕМАНЕ] Комисията представя на Европейския парламент и на Съвета доклад за оценка на степента, в която държавите членки са предприели необходимите мерки, за да се съобразят с настоящата директива, придружен при необходимост от законодателни предложения. Във връзка с това Комисията отчита също техническото и правното развитие в областта на киберпрестъпността, по-специално по отношение на обхвата на настоящата директива.

▌

Член 19

Влизане в сила

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

Член 20

Адресати

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

28.11.2011

СТАНОВИЩЕ НА КОМИСИЯТА ПО ВЪНШНИ РАБОТИ

на вниманието на комисия по граждански свободи, правосъдие и вътрешни работи

относно предложението за Директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Докладчик по становище: Кристина Оюланд

КРАТКА ОБОСНОВКА

Становището категорично подкрепя необходимостта от подобряване на обмена на информация, свързана с кибернетичната сигурност между държавите-членки в контекста на нарастващата тревога относно потенциални кибернетични атаки. Заемането с проблемите на кибернетичната сигурност на равнище ЕС и чрез координирани действия на държавите-членки е действително неотложна задача.

Становището подчертава ролята на Комисията за улесняване на насърчаването и координацията на съществуващите инициативи.

Комисията по външни работи и подкомисията по сигурност и отбрана считат, че неотложната необходимост от предприемане на действия и укрепване на координацията на отговорите, инициативите и програмите на равнище ЕС е от съществено значение. Следва да се подкрепи разработването на възможности и засилено сътрудничество за повишаване равнището на информационна сигурност.

Становището подкрепя идеята за назначаване на координатор по въпросите на кибернетичната сигурност в ЕС с цел улесняване на интеграцията и координацията на различните европейски дейности и инициативи на равнище ЕС и посредством институциите на ЕС.

ИЗМЕНЕНИЯ

Комисията по външни работи приканва водещата комисия по граждански свободи, правосъдие и вътрешни работи да включи в доклада си следните изменения:

Изменение 1

Предложение за директива
Съображение 1

Текст, предложен от Комисията	*Изменение*
(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.	(1) Основната цел на директивата е да сближи *разпоредбите на* 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 ***и на Съюза***; ***тази цел е част от общата стратегия на ЕС за борба с организираната престъпност, по-ефективно повишаване на сигурността на информационните мрежи, защита на критични информационни инфраструктури и на данните.***

Изменение 2

Предложение за директива
Съображение 1 а (ново)

Текст, предложен от Комисията	*Изменение*
	***(1а) Информационните системи са съществен елемент на политическото, социалното и икономическото взаимодействие в Съюза. Обществото зависи във все по-голяма степен от информационните системи. Все пак, въпреки големите ползи, които носят, те крият и редица рискове за нашата сигурност, които произтичат от тяхната сложност и уязвимостта им за**

различни видове киберпрестъпност. Следователно сигурността на информационните системи е повод за постоянна загриженост и изисква ефективна реакция от държавите-членки и от Съюза.

Изменение 3

Предложение за директива
Съображение 2

Текст, предложен от Комисията	*Изменение*
(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.	(2) Атаките срещу информационните системи представляват засилваща се опасност. ***Причина за тях може да бъде тероризмът или организираната престъпност, и те могат да бъдат извършени от държави или физически лица.*** 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. ***Трансграничният характер на някои нарушения и относително ниските рискове и разходи за извършителите, в съчетание с потенциално значимите ползи и съответно причинени щети, сериозно увеличава заплахата от подобни атаки.*** Това представлява заплаха за постигането на по-безопасно информационно общество и за изграждането на пространство на свобода, сигурност и правосъдие и следователно налага ответна реакция ***не само*** на равнището на Европейски съюз***, но и от цялата международна общност***.

Изменение 4

Предложение за директива
Съображение 3

Текст, предложен от Комисията	*Изменение*
(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 инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки.	(3) Има доказателства за наличието на тенденция към все по-опасни и постоянни широкомащабни атаки срещу ***информационни*** системи, които са от решаващо значение за ***държавите-членки, за Съюза*** или за определени функции в публичния или частния сектор***, както и на равнище на Съюза***. Тази тенденция се придружава от ***бързата*** разработка на ***компютърните технологии и в резултат на това, на*** все по-усъвършенствани инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки***, някои от които имат огромен потенциал да причинят икономически и социални щети***.

Изменение 5

Предложение за директива
Съображение 4 а (ново)

Текст, предложен от Комисията	*Изменение*
	(4а) Следва да се извърши задълбочена, надеждна и независима оценка на цялостното равнище на заплаха от атаки срещу информационни системи. Институциите на Съюза следва да приспособят своето равнище на информационна сигурност в зависимост от това.

Изменение 6

Предложение за директива
Съображение 4 б (ново)

Текст, предложен от Комисията	*Изменение*
	(4б) Налице е необходимост от координация на равнището на Съюза,

за да се спомогне за интегрирането на различните инициативи, програми и дейности.

Изменение 7

Предложение за директива
Съображение 6

Текст, предложен от Комисията	*Изменение*
(6) Държавите-членки следва да предвидят наказания за атаките срещу информационните системи. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи.	(6) Държавите-членки следва да предвидят наказания за атаките срещу информационните системи***, като част от по-широк набор от национални стратегии, целящи възпирането на атаки от това естество и борбата с тях.*** Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи. ***Предвид трансграничния характер на заплахите е необходимо държавите-членки да съгласуват наказанията си, като по този начин намалят различията по отношение на подхода им към съответните нарушения в Съюза.***

Изменение 8

Предложение за директива
Съображение 8 а (ново)

Текст, предложен от Комисията	*Изменение*
	(8а) Съветът и Комисията следва да призоват държавите-членки, които все още не са ратифицирали Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, незабавно да направят това.

Изменение 9

Предложение за директива
Съображение 11 а (ново)

Текст, предложен от Комисията	*Изменение*
	(11а) Сътрудничеството от страна на органите на управление с частния сектор и с гражданското общество е от основно значение за предотвратяването на кибератаките и борбата срещу тях. Необходимо е с тях да се установи текущ диалог, предвид това, че те използват широко компютърни системи, както и предвид необходимостта от споделяне на отговорността за гарантиране на надеждни и работещи системи. Необходимо е да се повиши информираността сред всички заинтересовани субекти в областта на компютърните системи, така че да се създаде култура на защита на сигурността на данните.

Изменение 10

Предложение за директива
Съображение 11 б (ново)

Текст, предложен от Комисията	*Изменение*
	(11б) С цел укрепване на способностите на държавите-членки за защита срещу кибератаки, следва да се насърчават неотдавнашните инициативи и проекти, отнасящи се до защитата от кибератаки като инициативата в рамките на Европейската агенция по отбрана (ЕАО). Следва да се предвиди по-тясно сътрудничество с ЕАО и със съвместния Център на НАТО за високи научни постижения по киберотбрана, по-специално в областта на изграждането на капацитет и на обучението.

Изменение 11

Предложение за директива
Съображение 12

Текст, предложен от Комисията	*Изменение*
(12) Необходимо е да се събират 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.	(12) Необходимо е да се събират 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. ***Държавите-членки следва да засилят обмена на информация относно кибератаките, с подкрепата на Комисията и на Европейската агенция за мрежова и информационна сигурност.*** Освен това данните ще помогнат на специализираните агенции като Европол и Европейската агенция за мрежова и информационна сигурност да оценят по-добре мащаба ***и въздействието*** на престъпленията в кибернетичното пространство и състоянието на мрежовата и информационната сигурност в Европа. ***По-доброто познаване на настоящите и бъдещите рискове ще направи възможно вземането на по-ефективни решения, целящи възпиране на кибератаките и борба срещу тях или намаляване на причинените от тях щети.***

Изменение 12

Предложение за директива
Съображение 12 а (ново)

Текст, предложен от Комисията	*Изменение*
	(12а) Обменът на информация и публично-частните партньорства (ПЧП) играят съществена роля за

подобряването на кибернетичната сигурност. Следователно Комисията следва да проучи възможностите за реализация на рамки или инструменти за подпомагане на ПЧП да сътрудничат помежду си на национално равнище и на равнището на Съюза, за прилагането на стандарти за качество на информацията с оглед на оперативната съвместимост и за гарантиране на зачитането на основните права, разделението на властите и демократичния контрол.

Изменение 13

Предложение за директива
Съображение 13

Текст, предложен от Комисията	*Изменение*
(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.	(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 ***на равнището на Съюза***. ***Съюзът следва също така да се стреми към засилване на международното сътрудничество в областта на мрежовата сигурност на данните, като си сътрудничи тясно с други организации с компетенции в тази сфера, като Организацията на обединените нации, НАТО, Съвета на Европа или***

ОССЕ и с участието на други заинтересовани международни субекти. 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.

Изменение 14

Предложение за директива
Съображение 16

Текст, предложен от Комисията	*Изменение*
(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.	(16) В настоящата директива ***и във всички области на практическото й прилагане*** се зачитат основните права***,*** и ***по-специално правото на неприкосновеност на личния живот, 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 *невиновност* и правото на ефективна правна защита, както и принципите на *законоустановеност* 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. ***Настоящата директива не нарушава свободния и открит характер на интернет.***

Изменение 15

Предложение за директива
Съображение 16 а (ново)

Текст, предложен от Комисията	*Изменение*
	(16а) В хода на преговорите и сътрудничеството с трети страни, Съветът и Комисията следва да настояват за минимални изисквания за превенция и борба с престъпленията в кибернетичното пространство и кибератаките, както и за минимални изисквания за сигурност на информационните системи.

Изменение 16

Предложение за директива
Съображение 16 б (ново)

Текст, предложен от Комисията	*Изменение*
	(16б) Комисията следва да разгледа възможностите за улесняване и подпомагане на трети страни в техните усилия да развият капацитета си за кибернетична сигурност и кибернетична отбрана.

Изменение 17

Предложение за директива
Член 14 - параграф 2 а (нов)

Текст, предложен от Комисията	*Изменение*
	2а. Комисията подпомага държавите-членки в насърчаването на устойчивостта и стабилността на интернет и предприема други дейности, имащи за цел постигането на информационна сигурност.

Изменение 18

Предложение за директива
Член 14 - параграф 2 б (нов)

Текст, предложен от Комисията	*Изменение*
	2б. Съветът изяснява ролята на Комитета по политика и сигурност и на неговите органи в контекста на действията по отношение на потенциални кибератаки.

Изменение 19

Предложение за директива
Член 14 - параграф 2 в (нов)

Текст, предложен от Комисията	*Изменение*
	2в. Държавите-членки подобряват обмена на информация относно кибернетичната сигурност. Държавите-членки, с подкрепата на Комисията, следва да потърсят взаимодействие с трети страни, по-специално със страните, от които най-често произтичат атаки.

Изменение 20

Предложение за директива
Член 15 - параграф 3

Текст, предложен от Комисията	*Изменение*
3. Държавите-членки предават на Комисията събраните по този член данни. Те правят също необходимото консолидираният преглед на тези статистически отчети да бъде публикуван.	3. Държавите-членки предават на Комисията събраните по този член данни. Те правят също необходимото консолидираният преглед на тези статистически отчети да бъде ***предоставен на Европейския парламент и*** публикуван.

Изменение 21

Предложение за директива
Член 15 - параграф 3 а (нов)

Текст, предложен от Комисията	*Изменение*
	3а. Назначава се координатор на ЕС по въпросите на кибернетичната сигурност с цел да улесни интеграцията и координацията на инициативите, програмите и дейностите на институциите на Съюза.

ПРОЦЕДУРА

Заглавие	Атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
Позовавания	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Водеща комисия Дата на обявяване в заседание	LIBE 7.10.2010 г.
Подпомагаща(и) комисия(и) Дата на обявяване в заседание	AFET 7.4.2011 г.
Докладчик(ци) Дата на назначаване	Kristiina Ojuland 29.3.2011 г.
Дата на приемане	22.11.2011 г.
Резултат от окончателното гласуване	+: 38 –: 8 0: 0
Членове, присъствали на окончателното гласуване	Sir Robert Atkins, Frieda Brepoels, Elmar Brok, Marietta Giannakou, Andrzej Grzyb, Takis Hadjigeorgiou, Anna Ibrisagic, Othmar Karas, Ioannis Kasoulides, Tunne Kelam, Евгени Кирилов, Андрей Ковачев, Eduard Kukan, Krzysztof Lisek, Sabine Lösing, Ulrike Lunacek, Barry Madlener, Francisco José Millán Mon, Annemie Neyts-Uyttebroeck, Raimon Obiols, Justas Vincas Paleckis, Ioan Mircea Paşcu, Cristian Dan Preda, Libor Rouček, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Marek Siwiec, Charles Tannock, Inese Vaidere, Кристиан Вигенин, Sir Graham Watson
Заместник(ци), присъствал(и) на окончателното гласуване	Laima Liucija Andrikienė, Elena Băsescu, Tanja Fajon, Diogo Feio, Monica Luisa Macovei, Emilio Menéndez del Valle, György Schöpflin, Traian Ungureanu, Ivo Vajgl, Renate Weber, Janusz Władysław Zemke
Заместник(ци) (чл. 187, пар. 2), присъствал(и) на окончателното гласуване	Luís Paulo Alves, Sylvie Guillaume, Владимир Уручев

11.11.2011

СТАНОВИЩЕ НА КОМИСИЯТА ПО ПРОМИШЛЕНОСТ, ИЗСЛЕДВАНИЯ И ЕНЕРГЕТИКА

на вниманието на комисията по граждански свободи, правосъдие и вътрешни работи

относно предложението за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Докладчик по становище: Кристиан Елер

ИЗМЕНЕНИЯ

Комисията по промишленост, изследвания и енергетика приканва водещата комисия по граждански свободи, правосъдие и вътрешни работи да включи в доклада си следните изменения:

Изменение 1

Предложение за директива
Съображение 1

Текст, предложен от Комисията	*Изменение*
(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.	(1) ***Целта*** на директивата***, която*** е ***част от общата стратегия на Съюза за борба с организирана престъпност, укрепване на устойчивостта на компютърните мрежи, за защита на критичната информационна инфраструктура и за защитата на данните, е*** да сближи ***разпоредбите на*** 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***, както и Комисията, Евроюст, Европол и Европейската агенция за мрежова и информационна сигурност, да даде възможност за общ и всеобхватен подход на Съюза***.

Изменение 2

Предложение за директива
Съображение 1 а (ново)

Текст, предложен от Комисията	*Изменение*
	(1а) Информационните системи представляват ключов елемент от политическото, социално и икономическо взаимодействие в Европа. Все по-често и в по-голяма степен обществото зависи от подобни системи. Правилното функциониране и сигурността на тези системи в Европа е от жизненоважно значение за развитието на европейския вътрешен пазар, както и на конкурентоспособността и иновационната икономика. Като осигуряват огромни ползи информационните системи същевременно представляват и редица рискове за нашата сигурност поради тяхната сложност и уязвимост за различни видове компютърни престъпления. Следователно сигурността на информационните системи предизвиква постоянна загриженост, която изисква ефективен отговор от страна на държавите-членки и Съюза.

Изменение 3

Предложение за директива
Съображение 2

Текст, предложен от Комисията	*Изменение*
(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.	(2) Атаките срещу информационните системи ***могат да идват от различни извършители, като например терористи, организирани престъпни групи, държави или отделни лица. Те*** представляват засилваща се опасност ***за функционирането на информационните системи в Съюза и на глобално равнище***, а съществува и растяща загриженост от вероятни атаки по терористични или политически подбуди срещу ***информационни*** системи, които са част от критичната инфраструктура на държавите-членки и на Съюза. ***Равнището на посочената заплаха се увеличава значително поради трансграничния характер на определени престъпления и относително малкия риск и разходи за нарушителите, съчетани с огромни печалби, които могат да бъдат придобити и вредите, които могат да бъдат причинени чрез атаките.*** Това представлява заплаха за постигането на по-безопасно информационно общество и за изграждането на пространство на свобода, ***демокрация,*** сигурност и правосъдие***, подкопава създаването на европейски дигитален вътрешен пазар*** и следователно ***изисква*** ответна реакция на ***равнище*** Европейски съюз***, както и на международно равнище, например чрез Конвенцията на Съвета на Европа от 2001 г. за престъпления в кибернетичното пространство.***

Изменение 4

Предложение за директива
Съображение 2 а (ново)

Текст, предложен от Комисията	*Изменение*
	(2а) Неотдавнашни кибератаки, извършени срещу европейски мрежи или информационни системи причиниха съществени вреди на икономиката и сигурността на Съюза.

Обосновка

Имат се предвид кибератаките срещу европейските институции, извършени през март 2011 г., както и многобройните случаи на проникване в европейските схеми за търговия с емисии, които доведоха до кражби на емисии в размер на милиони евро.

Изменение 5

Предложение за директива
Съображение 3

Текст, предложен от Комисията	*Изменение*
(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 инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки.	(3) Има доказателства за наличието на тенденция към все по-опасни и постоянни широкомащабни атаки***, включително атаки за координирано блокиране на услуги,*** срещу информационните системи, които са от решаващо значение за ***международните организации,*** държавите***, за Съюза*** или за определени функции в публичния или частния сектор. ***Подобни атаки могат да предизвикат съществени икономически щети, както поради самото прекъсване на информационните системи и комуникации, така и поради загуба на важна от търговска гледна точка поверителна информация или други данни. Съществува опасност иновационни малки и средни предприятия, които зависят от правилното функциониране и достъпността на информационните системи, като същевременно могат да отделят по-малко ресурси за***

	информационната сигурност, да бъдат особено засегнати. Тази тенденция се придружава от ***бърза*** разработка на ***информационни технологии и оттам на*** все по-усъвършенствани инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки***, като част от тях имат значителен потенциал за причиняване на икономически и социални вреди***.

Изменение 6

Предложение за директива
Съображение 4

Текст, предложен от Комисията	*Изменение*
(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.	(4) Приемането на общи определения в тази област, по-конкретно за информационните системи***, компютърните данни*** и ***престъпления по отношение на информационните системи и*** компютърните данни, е ***от съществено значение***, за да се осигури последователен ***и единен*** подход в държавите-членки при прилагането на директивата.

Изменение 7

Предложение за директива
Съображение 6

Текст, предложен от Комисията	*Изменение*
(6) Държавите-членки следва да предвидят наказания за атаките срещу информационните системи. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи.	(6) ***В допълнение към мерките, предприети от*** държавите-членки***, Съюзът и частният сектор се стремят да повишат сигурността и целостта на информационните системи и да предотвратят атаки, както и да сведат до минимум въздействието от тях, държавите-членки*** следва да предвидят ***както***

	ефективни мерки за предотвратяване на подобни атаки, така и хармонизирани наказания за атаките срещу информационните системи***, които следва да бъдат приети в рамките на по-широкомащабни национални стратегии за възпиране и борба с подобни атаки***. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи. ***Постигането на сближаване при санкциите и наказанията, прилагани от държавите-членки, е необходимо поради често трансграничния характер на заплахите и е насочено към намаляване на различията между държавите-членки, когато става въпрос за престъпления, извършени в рамките на Съюза.***

Изменение 8

Предложение за директива
Съображение 6 а (ново)

Текст, предложен от Комисията	*Изменение*
	(6а) Държавите-членки, Съюзът и частният сектор, в сътрудничество с Европейската агенция за мрежова и информационна сигурност, следва да предприемат стъпки за увеличаване на сигурността и целостта на информационните системи, да предотвратяват атаки и да намаляват въздействието от атаките.

Изменение 9

Предложение за директива
Съображение 8

Текст, предложен от Комисията	*Изменение*
(8) В заключенията на Съвета от 27—28 ноември 2008 г. се посочва, че следва да	(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.

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. ***Съветът и Комисията следва да насърчават държавите-членки, които още не са ратифицирали*** конвенцията***, да направят това възможно най-скоро. Конвенцията*** е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и срещу атаките срещу информационните системи. Тази директива ***взема предвид съответните разпоредби на*** Конвенцията.

Изменение 10

Предложение за директива
Съображение 10

Текст, предложен от Комисията	*Изменение*
(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.	(10) Настоящата директива ***не обхваща действията, предприети с цел да гарантират сигурността на информационните системи, напр. способността на дадена информационна система да устои на престъпни деяния, във вида, в който са определени в настоящата директива, или да премахне инструменти, които са използвани или са предназначени за използване за подобни действия. Директивата също така*** няма за цел да наложи наказателна отговорност за ***случаи, при които обективните критерии, изброени в настоящата директива, са изпълнени, но деянието е извършено*** без престъпно намерение като, например, разрешените изпитвания или защитата на дадена компютърна система.

Обосновка

Като се има предвид, че границата между добросъвестен и недобросъвестен достъп понякога е неясна (автоматични актуализации и т.н.), изменението има за цел да изясни, че функционирането на софтуера за защита против вируси например или инструментите за отстраняване на вируси, или наблюдение на увредени устройства, са изцяло извън обхвата на директивата.

Изменение 11

Предложение за директива
Съображение 11

Текст, предложен от Комисията	*Изменение*
(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 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.	(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 престъпления, свързани с информационни системи или данни, или за събиране на доказателства в електронна форма за престъпления ***или за намерение да се извърши престъпление***. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни атаки, държавите-членки***, Съюзът и Европейската агенция за мрежова и информационна сигурност*** следва да реагират незабавно ***и ефективно*** 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 ***техническа подкрепа, включително по отношение на възстановяване на оперативността на информационната система,*** опазване на данни ***в съответствие с принципите за защита на личните данни***, събирането на доказателства, предоставяне на правна информация***,***

откриване на рискова и/или извлечена информация и намирането ***и установяването*** на ***самоличността на*** заподозрени лица.

Изменение 12

Предложение за директива
Съображение 11 а (ново)

Текст, предложен от Комисията	*Изменение*
	(11а) Сътрудничеството на публичните органи с частния сектор и гражданското общество е от голямо значение за превенцията и борбата с атаките срещу информационните системи. С посочените партньори следва да бъде установен постоянен диалог с оглед на широкото използване от тяхна страна на информационните системи и наложителното с оглед постигане на стабилно и правилно опериране на тези системи споделяне на отговорността. За създаването на култура в областта на сигурността на информационните технологии е важно да се повиши осведомеността на всички заинтересовани лица относно използването на информационните системи.

Изменение 13

Предложение за директива
Съображение 12

Текст, предложен от Комисията	*Изменение*
(12) Необходимо е да се събират 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	(12) Необходимо е да се събират 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. ***Необходимо е***

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***.

държавите-членки, с подкрепата на Комисията и Европейската агенция за мрежова и информационна сигурност, да подобрят обмена на информация относно атаките срещу информационните системи. Освен това данните ще помогнат на специализираните ***органи и*** агенции като ***националните групи за бързо реагиране по въпросите на информационната сигурност,*** 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 ***Съюза, както и да подкрепят държавите-членки при приемането на ответна реакция срещу свързаните с информационната сигурност инциденти***. ***По-доброто познаване на настоящи и бъдещи рискове ще помогне за вземането на по-подходящи решения относно възпирането, борбата или ограничаването на вредите, причинени от атаки срещу информационните системи.***

Изменение 14

Предложение за директива
Съображение 12 а (ново)

Текст, предложен от Комисията	*Изменение*
	***(12а) Докато настоящата директива следва да изпълни приложимите в наказателното право стриктни критерии за правна сигурност и предвидимост, необходимо е също така посредством разпоредбите на настоящата директива относно събирането на данни, обмена на информация и задължението на Комисията редовно да докладва за прилагането им и да представя всяко**

необходимо предложение, да се предвиди гъвкав механизъм, който да позволява адаптирането спрямо бъдещо развитие, което евентуално може да доведе до разширяване на обхвата на настоящата директива. Посоченото бъдещо развитие включва всяко технологично развитие, което позволява, например, по-ефективно прилагане в областта на атаките срещу информационните системи или улеснява предотвратяването или смекчаването на подобни атаки.

Обосновка

Въпреки че оценява въвеждането на наказания, един всеобхватен подход на Съюза за справяне с киберпрестъпността следва не само да се съсредоточи върху ефективното правоприлагане, но и да разработи стратегии и инструменти за предотвратяване на посочените престъпни деяния.

Изменение 15

Предложение за директива
Съображение 12 б (ново)

Текст, предложен от Комисията	*Изменение*
	***(12б) Европейската агенция за мрежова и информационна сигурност следва да играе стратегическа роля в координирането на усилията на държавите-членки и на институциите на ЕС. На ENISA може, например, да бъде възложено да надзирава обмена на информация между тях, действайки по този начин като единно звено за контакт и регистър на инцидентите в областта на кибернетичната сигурност в Съюза. Може също така да й бъде възлагано да централизира статистически данни относно престъпленията, посочени в настоящата директива, на равнището на Съюза, както и да ги използват за основа при изготвянето на доклади относно състоянието на**

информационните системи и сигурността на компютърните данни в Съюза.

Изменение 16

Предложение за директива
Съображение 13

Текст, предложен от Комисията	*Изменение*
(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.	(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 ***на равнище на Съюза*** за сближаване на ***националното наказателно*** право в тази област. ***Също така Съюзът следва да работи за постигането на по-тясно международно сътрудничество в областта на сигурността на мрежовите и информационни системи, което да включва всички заинтересовани международни субекти.*** 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.

Изменение 17

Предложение за директива
Член 1 – параграф 1

Текст, предложен от Комисията	*Изменение*
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***.	С директивата се определят престъпленията в областта на атаките срещу информационните системи и се установяват ***хармонизирани*** минимални правила за налагане на наказания за такива престъпления. С нея се цели също създаването на общи разпоредби ***както*** за предотвратяване, ***така и за борба с*** подобни атаки и ***за*** подобряване на европейското сътрудничество в ***тази област, особено по отношение на наказателното правосъдие***.

Изменение 18

Предложение за директива
Член 2 – буква г)

Текст, предложен от Комисията	*Изменение*
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.	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 ***или европейското*** законодателство.

Изменение 19

Предложение за директива
Член 7 – буква б)

Текст, предложен от Комисията	*Изменение*
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,	б) компютърна парола, код за достъп, ***цифров или материален символ,*** или други подобни данни, с чиято помощ може да се получи достъп до информационна система или до част от нея.

Изменение 20

Предложение за директива
Член 8 – параграф 1 а (нов)

Текст, предложен от Комисията	*Изменение*
	1а. Държавите-членки гарантират, че непозволеното предаване на идентификационни данни на други лица с цел осъществяване на някоя от дейностите, посочени в членове 3–7, съставлява престъпление.

Изменение 21

Предложение за директива
Член 8 – параграф 1 б (нов)

Текст, предложен от Комисията	*Изменение*
	1б. Държавите-членки гарантират, че престъпление по смисъла на членове 3–7, извършено от лице, което в рамките на своята заетост разполага с достъп до системите за сигурност на информационни системи, се третира като утежняващо вината обстоятелството и съставлява престъпление.

Изменение 22

Предложение за директива
Член 10 – параграф 2

Текст, предложен от Комисията	*Изменение*
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	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.

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***, или чувствителна информация***.

Изменение 23

Предложение за директива
Член 13 – параграф 1 – буква в

Текст, предложен от Комисията	*Изменение*
в) в полза на юридическо лице, ***чието главно управление е разположено*** на територията на съответната държавата-членка.	в) в полза на юридическо лице, ***установено*** на територията на тази държава-членка.

Изменение 24

Предложение за директива
Член 14 – параграф 1

Текст, предложен от Комисията	*Изменение*
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***.	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 ***гарантират, че разполагат с оперативно национално звено за контакт и*** използват ***мрежата*** от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата***, както и че предават съответната информация на Комисията и на Европейската агенция за мрежова и информационна сигурност***. Държавите-членки гарантират също, че разполагат с процедури, чрез които да отговарят на спешни искания в максимален срок от

	осем часа. Този отговор ***е ефективен и включва, при необходимост, улесняването или на прякото прилагане на следните мерки: предоставяне на техническа консултация, включително по отношение на възстановяване на оперативността на информационната система, опазване на данни в съответствие с принципите за защита на личните данни, събирането на доказателства, предоставяне на правна информация и намирането и установяването на самоличността на заподозрени лица. Звената за контакт посочват формата и сроковете, в които следва да се предостави отговор на исканията за помощ***.

Изменение 25

Предложение за директива
Член 14 – параграф 2

Текст, предложен от Комисията	*Изменение*
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.	2. Държавите-членки информират Комисията***, Евроюст и Европейската агенция за мрежова и информационна сигурност*** 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.

Изменение 26

Предложение за директива
Член 15 – параграф 3

Текст, предложен от Комисията	*Изменение*
3. Държавите-членки предават на Комисията събраните по този член	3. Държавите-членки предават на Комисията***, Европол и Европейската***

данни. ***Те*** правят също необходимото ***консолидираният*** преглед на тези статистически отчети да бъде публикуван.

агенция за мрежова и информационна сигурност събраните по този член данни ***и*** правят също така необходимото ***периодичен консолидиран*** преглед на тези статистически отчети да бъде публикуван.

Изменение 27

Предложение за директива
Член 18 – параграф 1

Текст, предложен от Комисията	*Изменение*
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.	1. До [ЧЕТИРИ ГОДИНИ СЛЕД ПРИЕМАНЕТО] и на всеки три години след това Комисията, ***след консултация с всички заинтересовани субекти,*** представя на Европейския парламент и на Съвета доклад за прилагането на директивата в държавите-членки, който съдържа и всяко необходимо предложение. ***Всеки доклад посочва и взема предвид всяко необходимо предложение, технически решения, които позволяват по-ефективно прилагане в Съюза в областта на атаките срещу информационните системи, включително технически решения, които могат да послужат за предотвратяване или смекчаване на подобни атаки.***

Изменение 28

Предложение за директива
Член 18 – параграф 2

Текст, предложен от Комисията	*Изменение*
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	2. Държавите-членки ***и Европейската агенция за мрежова и информационна сигурност*** изпращат на Комисията цялата информация, необходима за изготвянето на посочения в параграф 1 доклад. Информацията съдържа подробно описание на законодателните и незаконодателните мерки в

на настоящата директива.

приложение на настоящата директива.

ПРОЦЕДУРА

Заглавие	Атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
Позовавания	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Водеща комисия Дата на обявяване в заседание	LIBE 7.10.2010 г.
Подпомагаща(и) комисия(и) Дата на обявяване в заседание	ITRE 7.10.2010 г.
Докладчик(ци) Дата на назначаване	Christian Ehler 24.11.2010 г.
Разглеждане в комисия	13.4.2011 г. 6.10.2011 г.
Дата на приемане	10.11.2011 г.
Резултат от окончателното гласуване	+: 49 –: 0 0: 1
Членове, присъствали на окончателното гласуване	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Владимир Уручев, Adina-Ioana Vălean
Заместник(ци), присъствал(и) на окончателното гласуване	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ивайло Калфин, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Ţicău
Заместник(ци) (чл. 187, пар. 2), присъствал(и) на окончателното гласуване	Eider Gardiazábal Rubial

ПРОЦЕДУРА

Заглавие	Атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета			
Позовавания	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)			
Дата на представяне на ЕП	30.9.2010 г.			
Водеща комисия Дата на обявяване в заседание	LIBE 7.10.2010 г.			
Подпомагаща(и) комисия(и) Дата на обявяване в заседание	AFET 7.4.2011 г.	BUDG 7.10.2010 г.	ITRE 7.10.2010 г.	
Неизказано становище Дата на решението	BUDG 20.10.2010 г.			
Докладчик(ци) Дата на назначаване	Monika Hohlmeier 9.12.2010 г.			
Разглеждане в комисия	3.2.2011 г.	25.5.2011 г.	12.1.2012 г.	28.2.2012 г.
	27.3.2012 г.	21.6.2012 г.	6.6.2013 г.	
Дата на приемане	6.6.2013 г.			
Резултат от окончателното гласуване	+: –: 0:	36 8 0		
Членове, присъствали на окончателното гласуване	Jan Philipp Albrecht, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Ioan Enciu, Frank Engel, Cornelia Ernst, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Sophia in ‘t Veld, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Светослав Христов Малинов, Véronique Mathieu Houillon, Nuno Melo, Roberta Metsola, Antigoni Papadopoulou, Georgios Papanikolaou, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Заместник(ци), присъствал(и) на окончателното гласуване	Dimitrios Droutsas, Мария Габриел, Evelyne Gebhardt, Станимир Илчев, Franziska Keller, Jean Lambert, Jan Mulder			
Заместник(ци) (чл. 187, пар. 2), присъствал(и) на окончателното гласуване	Jens Nilsson, Sabine Verheyen			
Дата на внасяне	19.6.2013 г.			