Становище на Европейския икономически и социален комитет относно „Кибератаките в ЕС“

(становище по собствена инициатива)

(2014/C 451/05)

Докладчик: **г-н McDonogh**

На 27 февруари 2014 г. Европейският икономически и социален комитет реши, в съответствие с член 29, параграф 2 от Правилника за дейността си, да изготви становище по собствена инициатива относно

„Кибератаките в ЕС“.

Специализирана секция „Транспорт, енергетика, инфраструктури, информационно общество“, на която беше възложено да подготви работата на Комитета по този въпрос, прие своето становище на 18 юни 2014 г.

На 500-ата си пленарна сесия, проведена на 9 и 10 юли 2014 г. (заседание от 10 юли), Европейският икономически и социален комитет прие настоящото становище със 135 гласа „за“ и 1 глас „против“.

1. **Заключения и препоръки**

1.1 Комитетът би желал на равнището на ЕС да бъде създаден орган за киберсигурност, който да е аналогичен на централния орган за въздухоплавателната индустрия, Европейската агенция за авиационна безопасност (ЕААБ), за да се осигури нужното на равнище ЕС силно лидерство за справяне със сложното изпълнение на ефективна общоевропейска политика за киберсигурност.

1.2 Информираните и уверени в способностите си граждани са изключително важни за добрата киберсигурност в Европа. Образованието на гражданите по въпросите на личната киберсигурност и защита на данните би следвало да е основна част от училищната програма и програмите за обучение на работното място. Освен това ЕС би следвало да стимулира програми и инициативи за обществено осведомяване по тези теми във всички държави членки.

1.3 На предприятията би следвало да се наложи законово изискване, с цел да се защитят от кибератаки, да приемат проактивен подход, включващ сигурни и устойчиви информационни и комуникационни технологии (ИКТ) и обучение на служителите във връзка с политиките за сигурност, каквото изискване съществува и по въпросите в областта на здравето и безопасността.

1.4 Всяка държава членка би трябвало да разполага с организация, чиято задача е да информира, образова и подкрепя сектора на малките и средните предприятия (МСП) по въпроси, свързани с най-добрите практики в киберсигурността. Големите предприятия могат лесно да придобият знанията, от които се нуждаят, но МСП имат нужда от подкрепа.

1.5 Мандатът на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) би следвало да се разшири и да се отпусне финансиране, за да може Агенцията да поеме по-пряка отговорност за програмите за образоване и осведомяване по въпросите на киберсигурността със специална насоченост към гражданите и МСП.

1.6 Предприятията и организациите трябва да повишат осведомеността относно отговорността за киберсигурността на равнище управителен съвет. Директорите на всички организации би следвало да бъдат изрично информирани за потенциалната корпоративна отговорност в резултат на недобри политики и действия в областта на киберсигурността.

1.7 Поради изключително важната си роля за предоставянето на онлайн услуги, всички доставчици на интернет услуги (ДИУ) в ЕС би трябвало да носят специална отговорност за защита на своите клиенти от кибератаки. Тази отговорност би следвало да бъде определена и да залегне в законодателството на равнище ЕС.

1.8 За да се гарантира бърза реализация на огромния потенциал за икономически растеж от динамичното разрастване на компютърните услуги в облак ([1]), на равнище ЕС също би следвало да се налагат специални изисквания и задължения, свързани със сигурността, за доставчиците на облачни услуги.

1.9 Комитетът счита, че доброволните мерки не са достатъчни и поради това е необходимо да се наложат стриктни регулаторни задължения на държавите членки, за да се осигури хармонизирането, управлението и осъществяването на киберсигурността в Европа. Нужно е също така законодателство, за да стане задължително уведомяването за значими инциденти, свързани с киберсигурността, от страна на всички предприятия и организации, а не само от доставчиците на критична инфраструктура. Това би спомогнало за подобряване на действията на Европа в отговор на заплахи, както и за повишаване на знанията и разбирането за кибератаките, за да могат да се разработят по-добри защити.

([1]) ОВ C 24, 28.1.2012 г., стр. 40; ОВ C 76, 14.3.2013 г., стр. 59.

1.10 Комитетът силно препоръчва ЕС да възприеме ориентиран към разработването подход за справяне със заплахата от кибератаки, като се гарантира, че всички използвани в Европа технологии и услуги за предоставяне на достъп до интернет и онлайн услуги са разработени така, че да осигуряват възможно най-добрата защита от кибератаки. Съображенията, свързани с разработването, би следвало да бъдат специално насочени към интерфейса човек — машина.

1.11 ЕИСК би желал европейските организации за стандартизация да разработят стандарти за киберсигурност по същество, които да бъдат разпространени за всички мрежови технологии и услуги в сферата на ИКТ. Тези стандарти би следвало да включат задължителен кодекс за практиките, за да гарантират, че цялото оборудване за ИКТ и интернет услуги, продавани на европейски граждани, отговаря на най-високите стандарти.

1.12 ЕС трябва да действа своевременно, за да гарантира, че всяка държава членка разполага с напълно функциониращ екип за незабавно реагиране при компютърни инциденти (CERT), за да защитава себе си и Европа от кибератаки.

1.13 Комитетът настоява Европейският център за борба с киберпрестъпността (EC3) в Европол да получи допълнителното финансиране, от което се нуждае, за да се бори с киберпрестъпността и да укрепи сътрудничеството между полицейските служби в Европа и със службите извън Съюза, да повиши способността на Европа да залавя и да търси наказателна отговорност от киберпрестъпници.

1.14 В обобщение ЕИСК счита, че политиката на ЕС за киберсигурност трябва да постигне следните конкретни резултати: силно лидерство на ЕС; стратегии за киберсигурност, които повишават сигурността, като същевременно запазват неприкосновеността на личния живот и други основни права; повишаване на осведомеността сред гражданите и насърчаване на проактивни подходи за защита; всеобхватно управление от държавите членки; информирани и отговорни действия от страна на предприятията; задълбочено партньорство между правителствата, частния сектор и гражданите; подходящи равнища на инвестиции; добри технически стандарти и достатъчни инвестиции в НИРДИ; международен ангажимент. За тази цел Комитетът изтъква още веднъж препоръките си във връзка с политиката за киберсигурност, посочени в много предходни становища ([2]) и призовава Комисията да предприеме последващи мерки по действията, поискани в тях.

2. **Обхват на становището**

2.1 Интернет икономиката генерира една пета от ръста на БВП в ЕС, а 200 милиона европейци пазаруват онлайн всяка година. Ние зависим от интернет и свързаните цифрови технологии да подкрепят нашите жизненоважни енергийни, здравни, управленски и финансови услуги. Но критичната цифрова инфраструктура и услуги, които играят толкова първостепенна роля в нашия икономически и социален живот, са изложени на нарастващ риск от кибератаки, застрашаващи нашия просперитет и качество на живот.

2.2 Комитетът е убеден, че нарастващата зависимост на Съюза от интернет и цифровите технологии не е достатъчно подплатена с практики и политики, осигуряващи подходящо равнище на киберсигурност в цяла Европа сега и в бъдеще. Целта на настоящото становище е да подчертае пропуските, които вижда Комитетът в политиката на ЕС по отношение на киберсигурността, и да препоръча подобрения, които повече биха смекчили рисковете от кибератаки.

2.3 Мотивите зад кибератаките могат да варират от много лични, например отмъщение спрямо лице или дружество, до кибершпиониране от държави и кибервойна между страни. При подготовката на настоящото становище беше взето решение обхватът да се стесни и да бъдат разгледани единствено кибератаките с престъпни мотиви, за да може препоръките да бъдат съсредоточени върху проблемите, които предизвикват най-голяма тревога сред повечето членове на Комитета. Сложният политически дебат за кибератаките от държави членки срещу граждани или други държави може да бъде тема за бъдещо становище.

([2]) ОВ C 97, 28.4.2007 г., стр. 21;
ОВ C 175, 28.7.2009 г., стр. 92;
ОВ C 255, 22.9.2010 г., стр. 98;
ОВ C 54, 19.2.2011 г., стр. 58;
ОВ C 107, 6.4.2011 г., стр. 58;
ОВ C 229, 31.7.2012 г., стр. 90;
ОВ C 218, 23.7.2011 г., стр. 130;
ОВ C 24, 28.1.2012 г., стр. 40;
ОВ C 229, 31.7.2012 г., стр. 1;
ОВ C 351, 15.11.2012 г., стр. 73;
ОВ C 76, 14.3.2013 г., стр. 59;
ОВ C 271, 19.9.2013 г., стр. 127;
ОВ C 271, 19.9.2013 г., стр. 133.

2.4 Настоящото становище разглежда единствено кибератаки от киберпрестъпници, водени от финансови мотиви, които представляват преобладаващата група атаки. С приемането на политики и практики за киберсигурност за ефективно справяне с кибератаки с престъпни мотиви се намаляват и рисковете от кибератаки, в основата на които стоят политически или политически мотиви.

2.5 Макар и ЕС да е постигнал добър напредък в изпълнението на действията по доверието и сигурността в Програмата в областта на цифровите технологии и да е разработил широкообхватна стратегия за киберсигурност, в която са заложени повечето от очертаните по-горе цели, трябва да се направи още повече.

3. **Кибератаки и киберсигурност**

3.1 Кибератака е всеки вид нападателно действие, насочено към компютърни информационни системи, инфраструктури, компютърни мрежи и/или лични цифрови устройства чрез различни видове злонамерени действия с цел кражба, промяна или унищожение на даден обект. Обект на атаките могат да бъдат пари, данни или информационни технологии.

3.2 Киберпрестъпниците предприемат кибератаки, за да откраднат пари или данни, да извършат измама, шпионаж, който подлежи на наказателно преследване, или изнудване. Атаките на киберпрестъпността могат да увредят основни мрежи и услуги, от които сме зависими в областта на здравеопазването, безопасността и икономическото благосъстояние, включително правителствени, транспортни и енергийни мрежи.

3.3 Заплахата от кибератаки нараства успоредно с все по-голямата ни зависимост от интернет и цифровите технологии. Според неотдавнашен доклад на Symantec през 2013 г. в световен мащаб общият брой нарушения, свързани с данни, се е повишил с 62 %, което се равнява на над 552 милиона разкрити записа. Тези нарушения често разкриват истински имена, дати на раждане или правителствени идентификационни номера, медицински досиета или финансова информация. Също така 38 % от мобилните потребители са били жертва на мобилна киберпрестъпност през последните 12 месеца.

3.4 Кибератаките могат да имат сериозно въздействие върху отделните предприятия и икономиката на Европа като цяло:

— в доклад за индустрията от 2011 г. се посочва, че в световен мащаб жертвите на кибератаки понасят загуби на стойност около 290 милиарда евро годишно, което означава, че киберпрестъпността е по-доходоносна от световната търговия на марихуана, кокаин и хероин взети заедно.

— Гражданите са под постоянна заплаха от кражба на самоличност чрез кибератаки. През май 2014 г. с еднократна атака от база данни бяха откраднати личните данни на 145 милиона ползватели на eBay. Според изследване на киберсигурността от 2013 г., изготвено от Университета в Кент, само в рамките на една година (в периода 2012-2013г.) онлайн акаунтите на над 9 милиона пълнолетни лица във Великобритания са били жертва на хакерска атака, 8 % от населението е изгубило пари в резултат на киберпрестъпност, а 2,3 % от населението на Обединеното кралство е изгубило над 10 000 британски паунда поради киберпрестъпност.

— През 2011 г. в доклад на британското правителство бе направена оценка, че киберпрестъпността е струвала общо 27 милиарда британски паунда на икономиката на Обединеното кралство:

  — онлайн измами: 1,4 млрд. паунда;

  — кражба на самоличност: 1,7 млрд. паунда;

  — кражба на интелектуална собственост: 9,2 млрд. паунда;

  — шпионаж: 7,6 млрд. паунда;

  — загуба на данни за клиенти: 1 млрд. паунда;

  — (преки) кражби онлайн от предприятия: 1,3 млрд. паунда;

  — изнудване: 2,2 млрд. паунда;

  — данъчни измами: 2,3 млрд. паунда.

— Всяка година кибератаките причиняват огромни икономически щети в Европа. В разходите трябва да бъдат включени:

  — загубата на интелектуална собственост и чувствителни данни;

  — алтернативни разходи, в това число смущения в обслужването и заетостта;

  — щети за имиджа на марката и репутацията на дружеството;

  — санкции и компенсаторни плащания на клиенти (за причинено неудобство или последваща загуба) или договорно обезщетение (за закъснения и пр.);

  — разходи за контрамерки и застраховане;

  — разходи за стратегии за смекчаване на последиците и възстановяване от кибератаки;

  — загуба на търговски приходи и конкурентоспособност;

  — нарушение на търговията и

  — загуба на работни места.

— Според Проучване на нарушенията на информационната сигурност от 2014 г., публикувано от правителството на Обединеното кралство, 81 % от големите дружества и 60 % от МСП са пострадали от нарушение на сигурността през 2013 г.

— Според оценки в същия правителствен доклад средните разходи за най-тежкото нарушение на киберсигурността на голяма организация би могло да достигне до 1 400 000 евро и до 140 000 евро за МСП.

— Дори ако атаките са неуспешни, разходите за смекчаване на последиците от тях бързо нарастват. През 2014 г. световният пазар за информационна сигурност ще отбележи ръст от 8,6 % и стойността му ще надхвърли 73 милиарда щ.д.

3.5 Техниките за кибератаки търпят непрекъснато развитие:

— Кибератаката обикновено включва използването на вектор на атака, чрез който киберпрестъпникът може да придобие достъп до данни за онлайн самоличност, компютър или мрежов сървър, за да постигне злонамерен резултат. Често използвани вектори на атака са USB устройства, приложения в електронната поща, уеб страници, изскачащи прозорци, съобщения в реално време, чат стаи и измами от рода на атаки с фалшива самоличност (фишинг).

— Най-често използваните форми на атака включват използването на зловреден софтуер. Зловредният софтуер е софтуер, който придобива контрол върху цифрово устройство, за да постигне престъпна цел, например да открадне пари или данни за потребителски достъп или да се разпространи в други устройства. Зловредният софтуер включва компютърни вируси (включително червеи и троянски коне), софтуер за изнудване (ransomware), софтуер за наблюдение (spyware), софтуер за рекламни съобщения (adware), фалшив антивирусен софтуер (scareware) и други зловредни програми. Софтуерът за изнудване, например, е особен вид зловреден софтуер, който заключва достъпа до заразената от него компютърна система и иска откуп, за да го отключи отново.

— Зловредният софтуер може също така да превърне даден компютър в бот, свързан с ботмрежа (или зомбирана мрежа) на киберпрестъпник, която той контролира, за да атакува жертвите си.

— Спам атака се нарича деяние, при което престъпник изпраща големи количества нежелани съобщения чрез електронна поща, за да примами жертвата да похарчи пари за фалшиви продукти. За изпращането на повечето спам съобщения се използват ботмрежи.

— Фишинг атаките са опити за кражба на потребителски имена, пароли или данни за кредитни карти по начини, които на пръв поглед вдъхват доверие, така че престъпникът да се сдобие с контрол върху електронната поща, социалната мрежа и банковите сметки на жертвата. Фишинг атаките са особено ефикасни за престъпника, тъй като 70 % от интернет потребителите имат една и съща парола за почти всяка уеб услуга, която използват.

— Киберпрестъпниците понякога използват атаки, свързани с отказ от предоставяне на услуги, за да изтръгнат пари от предприятия или организации. Подобни атаки са опит ресурсите на дадена машина или мрежа да станат недостъпни за потребителите, за които са предназначени, като обектът на атака бъде затрупан с външни искания за връзка, така че да не може да отговори на легитимния трафик, или да отговаря толкова бавно, че на практика да стане неизползваем. В атаките за отказ от предоставяне на услуги престъпниците обикновено отново прибягват до ботмрежи.

3.6 Сред организациите за киберсигурност има консенсус по приоритетните действия, които гражданите и предприятията би трябвало да предприемат, за да се защитят от кибератаки. Тези практики би следвало да бъдат представяни във всяка информационна и образователна програма в областта на киберсигурността.

а. Гражданите

— използват трудни за разбиване, но лесни за запомняне пароли;

— инсталират антивирусен софтуер на нови устройства;

— проверяват настройките за защита на данните в социални медии;

— пазаруват безопасно онлайн, като винаги внимават да проверят дали сайтовете за продажба на дребно онлайн са сигурни; и

— изтеглят софтуер и приложения за актуализиране на софтуер, когато получат известие за това.

б. Предприятията

— изготвят „бял списък“ на приложения;

— използват стандартни, сигурни системни конфигурации;

— актуализират приложния софтуер в рамките на 48 часа;

— актуализират системния софтуер в рамките на 48 часа; и

— намаляват броя на потребителите с администраторски права.

3.7 Малките предприятия често не разполагат с достатъчно IT подкрепа, за да следят потенциалните киберзаплахи, затова се нуждаят от специална помощ, за да се защитават от кибератаки.

3.8 Оповестяването на кибератаките и уязвимите места в системите е изключително важно за борбата с кибератаките, особено при противодействие на т.нар. „атаки в нулевия ден“ (zero-day attacks), т.е. нови разновидности на атаки, които не са известни до този момент на общността, занимаваща се с киберсигурност. Предприятията обаче често не оповестяват кибератаки поради опасения за своята репутация и юридическа отговорност. Тази липса на гласност пречи на способността на Европа да реагира бързо и ефективно на киберзаплахи и да подобри общата киберсигурност чрез процес на взаимно обучение.

3.9 Гражданите и предприятията купуват интернет достъп и услуги чрез доставчици на интернет услуги (ДИУ). Поради първостепенната им роля за предоставянето на онлайн услуги, е изключително важно ДИУ да предоставят на своите клиенти възможно най-високото ниво на защита от кибератаки. ДИУ би следвало не само да гарантират, че собствените им услуги и инфраструктура са разработени и поддържани така, че да предоставят най-високото ниво на киберсигурност, но и да предлагат отлични съвети във връзка с киберсигурността на своите клиенти и да имат въведени специални протоколи, които да съдействат за откриване и противодействие на кибератаки срещу клиенти в момента, в който се провеждат. Това задължение би следвало да бъде определено и да залегне в законодателството на равнище ЕС.

3.10 Ускореното възприемане на компютърните услуги в облак от страна на гражданите и предприятията в Европа е много важно за икономиката на ЕС ([3]). При нарастващото използване на компютърни услуги в облак за лично и бизнес приложение особено важно е Европа да гарантира киберсигурността на доставчиците на облачни услуги. Неяснотите във връзка със сигурността на облачните услуги оказва отрицателно влияние върху темпа на приемане на тази динамична технология. Комитетът би желал ЕС да наложи специални изисквания и задължения за сигурност на доставчиците на облачни услуги в подкрепа на растежа на компютърните услуги в облак в Европа.

([3]) ОВ C 24, 28.1.2012 г., стр. 40; ОВ C 76, 14.3.2013 г., стр. 59.

3.11 Трябва да се положат специални усилия за наемане на служители за сектора на киберсигурността в Европа. Търсенето на работници с висше образование в сферата на информационната сигурност се очаква да нарасне повече от двойно по-бързо спрямо ръста за целия сектор на компютърните технологии. В този контекст Комитетът насочва вниманието на Комисията към успеха на конкурсите в САЩ и в някои държави членки за повишаване на осведомеността по въпросите на киберсигурността и отглеждането на следващото поколение професионалисти в сферата на киберсигурността.

3.12 Една от най-добрите стратегии за защита от кибератаки е да се възприеме ориентиран към разработването подход, като се гарантира, че всички използвани в Европа технологии и услуги за предоставяне на достъп до интернет и онлайн услуги са разработени така, че да осигуряват възможно най-добрата защита от кибератаки. Съображенията, свързани с разработването, би следвало да бъдат специално насочени към интерфейса човек — машина. Това би включвало сътрудничество между производителите на технологии, доставчиците на интернет услуги, секторът за киберсигурност, EC3, ENISA, националните агенции за отбрана и сигурност на държавите членки и гражданите. Организацията на този ориентиран към разработването подход към киберсигурността може да бъде уредена на равнище ЕС от Комисията с евентуална координираща роля за ENISA.

4. **Политика на ЕС за киберсигурността**

4.1 ЕС разработва всеобхватна стратегия ([4]) за повишаване на киберсигурността за гражданите на Европа:

— Стълбът, свързан с доверието и сигурността в Програмата в областта на цифровите технологии, включва 14 действия, насочени към повишаване на киберсигурността и защитата на данните.

— В Директивата относно кибератаките ([5]), която трябва да бъде въведена в националното законодателство до 4 септември 2015 г., са дадени указания относно определенията за престъпления в тази сфера и санкциите за лицата, признати за виновни за тях.

— За да се повишат знанията за киберсигурността и да се улесни трансграничното сътрудничество между държавите членки, ЕС засили правомощията на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

— Съвместно с Интерпол беше създаден Европейски център за борба с киберпрестъпността (EC3), чиято цел е да противодейства на киберпрестъпността.

— Инициативата, свързана със защитата на критичната информационна инфраструктура (CIIP), е насочена към защитата на Европа от кибернетични смущения, включително атаки, чрез повишаване на киберсигурността и устойчивостта в целия ЕС.

— Стратегията за по-добър интернет за децата има за цел да създаде безопасна среда за децата в интернет и да противодейства на онлайн материали за сексуално посегателство над деца и сексуална експлоатация на деца.

— Предложената Директива за мрежова и информационна сигурност (МИС) изисква от държавите членки да въведат капацитет за МИС, напр. добре функциониращ екип за незабавно реагиране при компютърни инциденти (CERT). В нея се уточняват и изискванията за мрежова сигурност и отчитане за доставчици на критична инфраструктура.

4.2 ЕИСК реагира много категорично на предложението на Комисията за Директива за мрежова и информационна сигурност (МИС) ([6]), тъй като предложените мерки бяха преценени като прекалено меки и нямаше да накарат държавите членки да осигурят достатъчна защита на своите граждани и предприятия от кибератаки. Но докато приемаше предложената директива, Парламентът допълнително намали ползата от нея, като строго ограничи приложното ѝ поле до доставчици на „критична инфраструктура“ и по този начин премахна приложението ѝ спрямо търсачки, платформи на социални медии, портали за плащания в интернет и доставчици на компютърни услуги в облак.

4.3 Предложената директива за МИС няма да бъде достатъчна, за да предостави законодателството, необходимо за повишаване на осведомеността и готовността за реакция спрямо кибератаки в ЕС. Комитетът би желал да се приеме ново законодателство, с което уведомяването за всички значими инциденти в сферата на киберсигурността да стане задължително, не само за доставчиците на критична инфраструктура. Липсата на задължително докладване помага на киберпрестъпниците да се възползват от незапознатостта на уязвимите лица с темата.

([4]) JOIN/2013/01 final.
([5]) ОВ L 218, 14.8.2013 г., стр. 8–14.
([6]) ОВ C 271, 19.9.2013 г., стр. 133.

4.4 ЕС би трябвало да обмисли разширяването на правомощията на ENISA за повишаване на запознатостта със заплахата от кибератаки и на способността за реакция в целия ЕС. Вероятно ролята на ENISA би могла да се разшири, така че Агенцията да приеме по-пряка отговорност за образованието и информационните програми в областта на киберсигурността, насочени специално към граждани и МСП.

4.5 Европейският център за борба с киберпрестъпността (EC3) бе създаден в Европол през 2013 г., за да повиши способността на Европа да се бори с киберпрестъпността. EC3 играе ролята на централно звено в Европа за разузнавателна дейност относно престъпността и подкрепя действията и свързаните с кибератаки разследвания на държавите членки. Но в първия си годишен доклад EC3 предупреждава, че настоящите му ресурси вече ограничават напредъка на разследванията и EC3 няма да може да се справи с големите разследвания, които предстоят.

4.6 ЕС би трябвало да поиска от европейските организации за стандартизация — Европейския комитет по стандартизация (CEN), Европейския комитет за стандартизация в електротехниката (CENELEC) и Европейския институт за стандарти в далекосъобщенията (ETSI) — да разработят стандарти за киберсигурност за всеки софтуер или ИКТ хардуер или интернет базирани услуги за продажба в ЕС. Тези стандарти би трябвало непрекъснато да се актуализират, за да се върви в крак с новите заплахи.

4.7 Нужно е законодателство, което да направи задължително уведомяването за значими инциденти, свързани с киберсигурността, от страна на всички предприятия и организации, а не само от доставчиците на критична инфраструктура. Това би спомогнало за подобряване на действията за смекчаване на последиците от заплахи в реално време, както и за повишаване на знанията и разбирането за извършваните кибератаки, като по този начин би съдействало на властите, сектора на киберсигурността, предприятията и гражданите да подобрят киберсигурността и да противодействат на заплахи. За да се насърчи споделянето на информация за кибератаки, всяко законодателство би следвало да предлага подходяща анонимност на предприятията и организациите, предоставящи информация за атака. Би следвало да се обмисли и предоставянето на защита от юридическа отговорност при необходимост.

4.8 Въпреки предприетите от ЕС инициативи, държавите членки имат много различни нива на способности и подготвеност, което води до разпокъсани реакции на кибератаки в целия ЕС. Като се има предвид фактът, че мрежите и системите са взаимосвързани, държавите членки с много неефективен подход спрямо киберсигурността отслабват общата способност на ЕС да се справя с кибератаки. Нужни са мерки, за да бъдат издигнати всички държави членки до приемливо равнище на киберсигурност. Нужно е специално внимание, за да се гарантира, че всяка държава членка е създала напълно функциониращ екип за незабавно реагиране при компютърни инциденти (CERT).

4.9 Както е посочено в негови предишни становища ([7]), ЕИСК смята, че за да се повиши защитата на ЕС от кибератаки, мерките с доброволен характер не вършат работа и че на държавите членки трябва да се наложат силни регулаторни задължения, за да се осигури хармонизирането, управлението и осъществяването на киберсигурността в Европа.

4.10 За да бъде в позиция да предоставя реална и актуализирана защита на гражданите и предприятията от кибератаки, политиката на ЕС в областта на киберсигурността би трябвало да е съсредоточена върху следните действия:

— силно лидерство на ЕС, което въвежда политики, закони и институции в подкрепа на високи нива на киберсигурност в целия ЕС;

— политики за киберсигурност, които повишават индивидуалната и колективната сигурност, като същевременно запазват правото на гражданите на неприкосновеност и други основни ценности и свободи;

— добра осведоменост сред всички граждани за рисковете от използването на интернет и насърчаването на проактивен подход за защита на техните цифрови устройства, самоличност, неприкосновеност и онлайн транзакции;

— всеобхватно управление от всички държави членки, за да се гарантира, че критичните информационни инфраструктури са добре защитени и устойчиви;

— информирани и отговорни действия от страна на всички предприятия, за да гарантират, че системите им за ИКТ са защитени и устойчиви, да защитят своите операции и интересите на своите клиенти;

— проактивен подход от ДИУ за защита на клиентите им от кибератаки;

— задълбочен партньорски подход към киберсигурността в целия ЕС между правителствата, частния сектор и гражданите, на стратегическо и оперативно равнище;

— ориентиран към разработването подход за вграждане на киберсигурността при разработването на интернет технологии и услуги;

([7]) ОВ C 255, 22.9.2010 г., стр. 98; ОВ C 218, 23.7.2011 г., стр. 130; ОВ C 271, 19.9.2013 г., стр. 133.

— подходящо ниво на инвестиции в развиване на знания и умения в областта на киберсигурността, за да се изгради силна работна ръка в сферата на киберсигурността;

— добри технически стандарти за киберсигурност и достатъчно инвестиции в НИРДИ в подкрепа на развитието на силен сектор на киберсигурността и решения от световна класа;

— активен международен ангажимент със страни извън ЕС за развитие на координирана световна политика и отговор на заплахи за киберсигурността.

Брюксел, 10 юли 2014 г.

Председател
на Европейския икономически и социален комитет
Henri MALOSSE