**СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪЮЗ**

**Брюксел, 8 февруари 2013 г. (12.02)**
**(OR. en)**

**6225/13**

**POLGEN 17**
**JAI 87**
**TELECOM 20**
**PROCIV 20**
**CSC 10**
**CIS 4**
**RELEX 115**
**JAIEX 14**
**RECH 36**
**COMPET 83**
**IND 35**
**COTER 17**
**ENFOPOL 34**
**DROIPEN 13**
**CYBER 1**

**ПРИДРУЖИТЕЛНО ПИСМО**

| | |
|---|---|
| От: | Генералния секретар на Европейската комисия, подписано от г-н Jordi AYET PUIGARNAU, директор |
| Дата на получаване: | 7 февруари 2013 г. |
| До: | Г-н Uwe CORSEPIUS, генерален секретар на Съвета на Европейския съюз |
| № док. Ком.: | JOIN (2013) 1 final |
| Относно: | Стратегия на Европейския съюз за киберсигурност - Отворено, безопасно и сигурно киберпространство |

Приложено се изпраща на делегациите документ на Комисията JOIN (2013) 1 final.

Приложение: JOIN (2013) 1 final

ЕВРОПЕЙСКА
КОМИСИЯ

ВЪРХОВЕН ПРЕДСТАВИТЕЛ НА
ЕВРОПЕЙСКИЯ СЪЮЗ ПО
ВЪПРОСИТЕ
НА ВЪНШНИТЕ РАБОТИ И
ПОЛИТИКАТА НА СИГУРНОСТ

Брюксел, 7.2.2013
JOIN(2013) 1 final

# СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

## Стратегия на Европейския съюз за киберсигурност

## Отворено, безопасно и сигурно киберпространство

**СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ**

**Стратегия на Европейския съюз за киберсигурност**

**Отворено, безопасно и сигурно киберпространство**

## 1. ВЪВЕДЕНИЕ

### 1.1. Контекст

През последните две десетилетия интернет и по-общо киберпространството имаха огромно влияние върху всички сфери на обществото. Нашето ежедневие, основните права, социалните взаимодействия и икономиките ни зависят от безупречната работа на информационните и комуникационните технологии. Наличието на едно отворено и свободно киберпространството даде тласък на политическото и социалното приобщаване в световен мащаб; то премахна бариерите между държави, общности и граждани, предоставяйки възможности за взаимодействие и обмен на информация и идеи в световен мащаб; то предостави форум за свободно изразяване на мнения и упражняване на основните права и подкрепи хората в стремежа им за демократични и по-справедливи общества — това стана по особено впечатляващ начин по време на Арабската пролет.

За да остане киберпространството отворено и свободно, към онлайн средата следва да се прилагат същите норми, принципи и ценности, към които ЕС се придържа в останалите области на живота. Основните права, демокрацията и върховенството на закона трябва да бъдат защитени в киберпространството. Свободата и благоденствието ни във все по-голяма степен зависят от един солиден и новаторски интернет, който ще продължи да се развива, ако иновациите в частния сектор и гражданското общество подхранват неговия растеж. Но свободата в онлайн средата изисква също безопасност и сигурност. Киберпространството следва да бъде защитено от инциденти, злонамерени действия и злоупотреби; правителствата също имат важна роля за гарантиране на свободата и безопасността в киберпространството. Правителствата имат редица задачи: да защитават достъпа и откритостта, да зачитат и защитават основните права онлайн и да се грижат за запазване на надеждността и оперативната съвместимост на интернет. Значителна част от киберпространството обаче се притежава и експлоатира от частния сектор и поради това, за да има дадена инициатива успех в тази област, тя трябва да е съобразена с неговата водеща роля.

Информационните и комуникационните технологии се превърнаха в гръбнак на нашия икономически растеж и са ресурс с критично значение за всички икономически сектори. Сега те са в основата на сложните системи, които поддържат функционирането на нашите икономики в ключови сектори като финансите, здравеопазването, енергетиката и транспорта; същевременно много бизнес модели са изградени върху непрекъснатостта на достъпа до интернет и безупречното функциониране на информационните системи.

Чрез завършването на единния цифров пазар Европа би могла да увеличи своя БВП с почти 500 милиарда евро годишно[1], т.е. средно с по 1000 евро на човек. За да могат да се развият новите технологии на базата на свързаността, включително електронните плащания, изчислителните облаци или междумашинните комуникации[2], у гражданите ще трябва да се развие доверие към тях и увереност при употребата им. За съжаление едно проучване[3] на Евробарометър от 2012 г. показва, че почти една трета от европейците не са уверени в своите способности да използват интернет за банкиране или покупки. Преобладаващото мнозинство заявяват също, че избягват да разкриват лична информация онлайн от съображения за сигурност. В рамките на ЕС повече от една десета от потребителите на интернет вече са ставали жертва на онлайн измами.

Последните години показаха, че цифровият свят носи огромни ползи, но е същевременно уязвим. Броят на инцидентите в областта на киберсигурността[4], били те преднамерени или случайни, се увеличава с тревожно темпо, като те биха могли да нарушат функционирането на основни услуги, които ние приемаме за даденост, като водоснабдяването, здравните грижи, електроснабдяването или мобилните услуги. Заплахите могат да имат различен произход, включително да се дължат на криминални, политически мотивирани, терористични или подкрепени от други държави нападения, както и на природни бедствия и непреднамерени грешки.

Икономиката на ЕС вече е засегната от престъпления в киберпространството[5], насочени срещу частния сектор и отделни граждани. Извършителите на киберпрестъпления използват все по-сложни методи за проникване в информационните системи, като си служат с кражби на критични данни или изнудване на предприятия. Засилването на икономическия шпионаж и подкрепяните от трети държави действия в киберпространството представляват нова категория заплаха за правителствата и предприятията от ЕС.

В държави извън ЕС е възможно също правителствата да злоупотребяват с киберпространството, за да осъществяват наблюдение и контрол над собствените си граждани. ЕС може да противодейства на това състояние, като насърчава свободата и осигурява зачитането на основните права в онлайн средата.

Всички тези фактори обясняват защо правителства по света започнаха да разработват стратегии за киберсигурност и да гледат на киберпространството като на все по-важен въпрос от международно значение. Настъпил е моментът ЕС да засили своите действия

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

2 Например насаждения, снабдени със сензори, да съобщават на система за напояване кога имат нужда от вода.

3 Специално проучване на Евробарометър 390 за киберсигурността, 2012 г.

4 Под киберсигурност обикновено се разбират предпазните мерки и действия, които могат да бъдат приложени за предпазване на киберпространството както в гражданската, така и във военната област, от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура или могат да нарушат работата им. Целта на киберсигурността е да се съхрани наличността и целостта на мрежите и инфраструктурата, както и поверителността на информацията, която се съдържа в тях.

5 Под киберпрестъпност обикновено се разбира широк набор от различни престъпни деяния, в които компютри и информационни системи са или основен инструмент, или основна цел. Киберпрестъпността обхваща традиционни престъпления (например измами, фалшифициране и кражба на самоличност), престъпления, свързани със съдържанието (напр. онлайн разпространение на детска порнография или подбуждане към расова омраза), и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ на услуга и зловреден софтуер).

в тази област. Настоящото предложение за стратегия на Европейския съюз за киберсигурност, представяно от Комисията и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност („върховния представител“), очертава вижданията на ЕС в тази област, изяснява ролите и отговорностите и определя необходимите действия въз основата на силна и ефективна защита и насърчаване на правата на гражданите с цел онлайн средата в ЕС да се превърне в най-безопасната онлайн среда в света.

## 1.2. Принципи на киберсигурността

Безграничният и многопластов интернет се превърна в един от най-мощните инструменти за глобален напредък без правителствен надзор или правителствено регламентиране. Въпреки че частният сектор следва да продължи да играе водеща роля в изграждането и оперативното управление на интернет, необходимостта от изисквания относно прозрачността, отчетността и сигурността става все по-явна. В настоящата стратегия се разясняват принципите, от които следва да се ръководи политиката за киберсигурност както в ЕС, така и в международен план.

**Основните ценности на ЕС важат в еднаква степен в цифровия и във физическия свят**

Същото законодателство и норми, които се прилагат в другите области на нашия живот, важат и в киберпространството.

**Защита на основните права, свободата на изразяване на мнение, личните данни и неприкосновеността на личния живот**

Киберсигурността може да бъде надеждна и ефективна само ако се основава на основните права и свободи, залегнали в Хартата на основните права на Европейския съюз, и на основните ценности на ЕС. И обратното, правата на индивида не могат да бъдат обезпечени без сигурни мрежи и системи. За целите на киберсигурността, когато става въпрос за лични данни, всеки обмен на информация следва да е в съответствие със законодателството на ЕС за защита на данните и да отчита в пълна степен правата на личността в тази област.

**Достъп за всички**

Ограниченият достъп или липсата на достъп до интернет, както и цифровата неграмотност поставят гражданите в неблагоприятно положение, като се има предвид голямата степен на навлизане на цифровите технологии във всички дейности на обществото. Всеки трябва да има възможност за достъп до интернет и за безпрепятствен пренос на информация. Целостта и сигурността на интернет трябва да бъдат гарантирани, за да се предостави безопасен достъп за всички.

**Демократично и ефикасно управление с участието на множество заинтересовани страни**

Цифровият свят не се контролира от една-единствена организация. Понастоящем редица заинтересовани страни, много от които са търговски и неправителствени организации, участват в оперативното управление на интернет ресурси, протоколи и стандарти, както и в бъдещото развитие на интернет. ЕС потвърждава значението на

всички заинтересовани страни в настоящия модел на управление на интернет и подкрепя този управленски подход с участието на множество заинтересовани страни[6].

**Споделена отговорност за гарантирането на сигурността**

Нарастващата зависимост от информационните и комуникационните технологии във всички области на човешкия живот доведе до слаби места, които трябва да бъдат правилно определени, внимателно анализирани, отстранени или ограничени. Всички съответни участници, независимо дали са публични органи, представители на частния сектор или отделни граждани, трябва да осъзнаят тази споделена отговорност, да предприемат действия, за да защитят себе си и, ако е необходимо, за да осигурят координиран отговор с цел укрепване на киберсигурността.

## 2. СТРАТЕГИЧЕСКИ ПРИОРИТЕТИ И ДЕЙСТВИЯ

ЕС следва да запази онлайн среда, осигуряваща възможно най-голяма свобода и сигурност за всички. Макар в настоящата стратегия да се признава, че справянето с предизвикателствата пред сигурността в киберпространството е главно задача на държавите членки, в нея се предлагат конкретни действия, които могат да подобрят резултатите на ЕС като цяло. Тези действия са както с краткосрочен, така и с дългосрочен характер и включват различни инструменти на политиките[7] с участието на различни видове участници, били те институции на ЕС, държави членки или промишлеността.

Вижданията на ЕС, представени в настоящата стратегия, са изразени в пет стратегически приоритета, които се отнасят до посочените по-горе предизвикателства:

- постигане на устойчивост на киберпространството
- чувствително намаляване на киберпрестъпността
- разработване на политика за кибернетична отбрана и изграждане на капацитет във връзка с общата политика за сигурност и отбрана (ОПСО).
- разработване на промишлени и технологични ресурси, необходими за киберсигурността
- създаване на последователна международна политика на Европейския съюз относно киберпространството и насърчаване на основните ценности на ЕС.

### 2.1. Постигане на устойчивост на киберпространството

За да подобрят устойчивостта на киберпространството в ЕС, публичните органи и частният сектор трябва да развият своя капацитет и да си сътрудничат ефективно. Опирайки на положителните резултати, постигнати чрез извършените до момента дейности[8], по-нататъшните действия от страна на ЕС могат да помогнат в частност за противодействието на кибернетичните рисковете и заплахи с трансграничен характер и

---

6 Вж. също COM (2009) 277, съобщение на Комисията до Европейския парламент и Съвета — „Управлението на интернет: следващи стъпки“.

7 Действията, свързани с обмен на информация, включваща лични данни, следва да са съобразени със законодателството на ЕС за защита на данните.

8 Вж. препратките в настоящото съобщение, както и в работния документ на службите на Комисията, представляващ оценка на въздействието, придружаващ предложението на Комисията за Директива относно мрежовата и информационна сигурност, по-специално в раздели 4.1.4, 5.2, приложение 2, приложение 6, приложение 8.

да допринесат за координиран отговор в извънредни ситуации. Това ще подпомогне сериозно доброто функциониране на вътрешния пазар и ще засили вътрешната сигурност в ЕС.

Европа ще продължи да бъде уязвима, ако не бъдат положени значителни усилия за увеличаване на публичния и частния капацитет, публичните и частните ресурси и процедури за превенция, откриване и справяне с инциденти, свързани с киберсигурността. Ето защо Комисията разработи политика за мрежова и информационна сигурност (МИС)[9]. **Европейската агенция за мрежова и информационна сигурност (ENISA)** бе създадена през 2004 г.[10], като в процес на договаряне между Съвета и Парламента[11] е нов регламент за укрепване и модернизиране на мандата на ENISA. Освен това Рамковата директива за електронните комуникации[12] изисква от доставчиците на електронни комуникации да прилагат подходящо управление на рисковете за своите мрежи и да докладват за значителните нарушения, свързани със сигурността. Също така законодателството на ЕС в областта на защитата на данните[13] изисква от администраторите на данни да гарантират спазването на изискванията и предпазните мерки за защита на данните, включително мерките, свързани със сигурността, като в областта на обществено достъпните услуги за електронна комуникация администраторите на лични данни трябва да докладват на компетентните национални органи за инциденти, свързани с нарушения на сигурността на личните данни.

Въпреки постигнатия въз основа на доброволни ангажименти напредък все още съществуват празноти в ЕС, по-специално по отношение на националния капацитет, координацията в случай на инциденти с трансграничен характер, както и по отношение на участието на частния сектор и подготвеността за кризи. Настоящата стратегия е придружена от предложение за **законодателен инструмент** с цел по-конкретно:

- да се установят общи минимални изисквания за МИС на национално равнище, които задължават държавите членки да: определят национални компетентни органи за МИС; създадат добре функциониращ екип за незабавно реагиране при компютърни инциденти (CERT); и приемат национални стратегии за МИС и национални планове за сътрудничество в сферата на МИС. Изграждането на капацитет и координацията се отнасят също до институциите на ЕС: екип за незабавно реагиране при компютърни инциденти, отговорен за сигурността на информационните системи на институциите, агенциите и органите на ЕС (CERT-EU) бе създаден с постоянен мандат през 2012 г.;
- да се изградят механизми за координирани действия по превенция, откриване, ограничаване на последствията и отговор, даващи възможност за обмен на информация и взаимна помощ между националните компетентни органи в сферата на МИС. От националните органи, компетентни в сферата на МИС, ще се изисква да

[9] През 2001 г. Комисията прие съобщение, озаглавено „Мрежова и информационна сигурност: предложение за европейски политически подход“ (COM (2001) 298); през 2006 г. тя прие Стратегия за сигурно информационно общество (COM (2006) 251). От 2009 г. насам Комисията прие също План за действие и съобщение относно защитата на критичната информационна инфраструктура (CIIP) (COM(2009)149, одобрен с решение 2009/C 321/01 на Съвета, и COM(2011)163, одобрен в заключенията от срещата на Съвета 10299/11).

[10] Регламент (ЕО) № 460/2004.

[11] COM(2010) 521. Действията, предложени в настоящата стратегия, не водят до изменение на съществуващия или бъдещия мандат на ENISA.

[12] Членове 13а и 13б от Директива 2002/21/ЕО.

[13] Член 17 от Директива 95/46/ЕО; член 4 от Директива 2002/58/ЕО.

гарантират подходящо сътрудничество в ЕС, по-специално на базата на план на Съюза за сътрудничество в сферата на МИС, предназначен за противодействие на киберинциденти, които имат трансграничен характер. Това сътрудничество ще се основава също на напредъка в контекста на Европейския форум за държавите членки (EFMS)[14], в който бяха проведени плодотворни дискусии и обмен относно публичната политика в областта на МИС и който може да бъде включен в механизма за сътрудничество, след като последният бъде създаден.

- да се подобри готовността и ангажираността на частния сектор. Тъй като преобладаващата част от мрежовите и информационните системи са частна собственост и се експлоатират от частния сектор, подобряването на ангажираността на частния сектор е от съществено значение за подобряване на киберсигурността. Частният сектор трябва да разработи на техническо ниво свой собствен капацитет за запазване на устойчивостта на киберпространството и да обменя най-добри практики с другите сектори. Разработените от промишлеността инструменти за реагиране на инциденти, идентифициране на причините и провеждане на разследвания следва да се използват също от публичния сектор.

Въпреки това все още липсват ефективни стимули, които да накарат участниците от частния сектор да предоставят надеждни данни относно наличието на инциденти, свързани с МИС, или относно последиците им, да внедрят култура на управление на риска или да инвестират в решения в областта на сигурността. Поради това предложеният законодателен акт има за цел да гарантира, че участниците в редица ключови области (а именно енергетиката, транспорта, банковото дело, фондовите борси и секторите, играещи съществена роля за ключовите интернет услуги, както и публичните администрации) извършват оценка на рисковете за киберсигурността, пред които са изправени, осигуряват надеждността и устойчивостта на мрежите и информационните системи чрез подходящо управление на риска и обменят събраната информация с националните компетентни органи в сферата на МИС. Разпространението на културата на киберсигурност би могло да увеличи възможностите за бизнес и конкурентоспособността на частния сектор, което евентуално би довело до развитието на пазар в областта на киберсигурността.

Тези икономически субекти ще трябва да докладват на националните компетентни органи в сферата на МИС за инциденти, имащи значително въздействие върху непрекъснатостта на основните услуги и вериги за доставка на стоки, които зависят от мрежовите и информационните системи.

Националните компетентни органи в сферата на МИС следва да си сътрудничат и да обменят информация с други регулаторни органи, в частност с органите, компетентни в областта на защитата на личните данни. Компетентните органи в сферата на МИС на свой ред следва да докладват на правоприлагащите органи за предполагаеми сериозни инциденти от престъпно естество. Националните компетентни органи следва също да публикуват редовно на специално предназначена за целта електронна страница некласифицирана информация за текущи ранни предупреждения за инциденти и рискове, както и за съгласуван отговор. Правните задължения не следва да заместват, нито да възпрепятстват, разгръщането на неофициално и доброволно сътрудничество, включително между публичния и частния сектор, с цел повишаване на сигурността и

[14] Стартът на Европейския форум за държавите членки беше даден с COM (2009) 149 като платформа за насърчаване на дискусии между публичните органи на държавите членки по отношение на практиките на добра политика относно сигурността и устойчивостта на критичната информационна инфраструктура.

обмен на информация и добри практики. По-специално Европейското публично-частно партньорство за устойчивост (EP3R[15]) е солидна и легитимна платформа на равнище ЕС и трябва да бъде развивано по-нататък.

Механизмът за свързване на Европа (МСЕ)[16] ще предостави финансова подкрепа за ключови инфраструктури, които свързват капацитета на държавите членки в сферата на МИС и по този начин улесняват сътрудничеството в рамките на ЕС.

Освен това от съществено значение за изпробване на механизмите за сътрудничество между държавите членки и частния сектор са ученията за действия при инциденти в киберпространството на европейско равнище. Първото учение с участието на държавите членки беше проведено през 2010 г. („Cyber Europe 2010“), а второ учение, в което се включи и частният сектор, беше проведено през октомври 2012 г. („Cyber Europe 2012“). Симулационно учение с участието на ЕС и САЩ беше проведено през ноември 2011 г. („Cyber Atlantic 2011“). За следващите години са планирани допълнителни учения, включително с международни партньори.

**Комисията ще:**

- продължи да осъществява своите дейности, изпълнявани от Съвместния изследователски център в тясно сътрудничество с органите на държавите членки и собствениците и операторите на критични инфраструктури, за идентифициране на уязвимите елементи на европейската критична инфраструктура по отношение на МИС и за насърчаване на развитието на устойчиви системи;

- започне в началото на 2013 г. пилотен проект[17], финансиран от ЕС, за **борба с т.нар. ботмрежи и зловредния софтуер**, с цел да се осигури рамка за координация и сътрудничество между държавите — членки на ЕС, организациите от частния сектор, например доставчиците на интернет услуги, и международните партньори.

**Комисията призовава ENISA да:**

- подпомага държавите членки при разработване на **силен национален капацитет за поддържане на устойчивостта на киберпространството**, по-специално чрез натрупване на експертни познания в областта на сигурността и устойчивостта на системите за промишлен контрол, транспортната и енергийната инфраструктура;

- провери осъществимостта през 2013 г. на идеята за изграждане на екипи за

[15] Стартът на Европейското публично-частно партньорство за устойчивост беше даден с COM (2009) 149. Тази платформа постави начало на работата и насърчи сътрудничеството между публичния и частния сектор за идентифициране на ключовите активи, ресурси, функции и основни изисквания по отношение на устойчивостта, както и нуждите от сътрудничество и механизми за реакция на мащабни смущения, засягащи електронните комуникации.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. МСЕ бюджетен ред 09.03.02 — Мрежи в областта на телекомуникациите (насърчаване на взаимосвързаността и оперативната съвместимост на националните публични услуги онлайн, както и на достъпа до такива мрежи).

[17] CIP-ICT PSP-2012-6, 325188. Той разполага с общ бюджет от 15 милиона евро, като финансирането от ЕС е в размер на 7,7 милиона евро.

незабавно реагиране при компютърни инциденти по отношение на системите за промишлен контрол (ICS-CSIRTs) за ЕС;

- продължава да подпомага държавите членки и институциите на ЕС при провеждането на редовни **паневропейски учения за действия при инциденти в киберпространството**, които ще представляват също оперативната база за участието на ЕС в международни учения за действие при инциденти в киберпространството.

**Комисията призовава Европейския парламент и Съвета да:**

- **приемат** бързо предложението за директива за **общо високо ниво на мрежовата и информационната сигурност (МИС)** на територията на Съюза, разглеждащо националния капацитет и готовността, сътрудничеството на равнище ЕС, разпространението на практики за управление на риска и обмена на информация в областта на МИС.

**Комисията призовава промишлеността да:**

- поеме водеща роля по отношение на **инвестициите** за постигане на високо равнище на киберсигурността и да разработи най-добри практики и механизми за обмен на информация както на равнище сектор, така и с публичните органи, с цел да се гарантира солидна и ефективна защита на активи и индивиди, в частност чрез публично-частни партньорства като EP3R и „Trust in Digital Life“ (Доверие в цифровия живот) (TDL)[18].

**Повишаване на осведомеността**

Гарантирането на сигурността на киберпространството е обща отговорност. Крайните потребители играят ключова роля за гарантирането на сигурността на мрежите и информационните системи: те трябва да бъдат осведомени за рисковете, пред които се изправят в онлайн средата, и да бъдат подготвени да вземат прости мерки за защита.

През последните години бяха разработени редица инициативи, които следва да бъдат продължени. По-конкретно, ENISA взе участие в инициативи за повишаване на осведомеността чрез публикуване на доклади, организиране на работни форуми на експерти и развитие на публично-частните партньорства. Европол, Евроюст и националните органи за защита на данните също работят за повишаване на осведомеността. През октомври 2012 г. ENISA, заедно с някои държави членки, проведе за първи път „Европейски месец на киберсигурността“. Повишаването на осведомеността е една от областите на дейност на работната група ЕС—САЩ по киберсигурността и киберпрестъпленията[19], като темата освен това е от съществено значение в контекста на програмата „По-безопасен интернет“[20] (с ударение върху безопасността на децата в онлайн среда).

---

18 http://www.trustindigitallife.eu/.

19 Работната група, създадена на срещата на върха ЕС—САЩ през ноември 2010 г. (MEMO/10/597), е натоварена със задачата да разработи съвместни подходи за широка гама от въпроси, свързани с киберсигурността и киберпрестъпленията.

20 Програмата „По-безопасен интернет“ финансира мрежа от НПО, които работят в областта на закрилата на децата в онлайн следа, мрежа от правоприлагащи органи, които обменят

**Комисията призовава ENISA да:**

- предложи през 2013 г. пътна карта за въвеждане на „свидетелство за безопасна навигация в интернет от гледна точка на мрежовата и информационната сигурност“ като програма за доброволно сертифициране с цел подобряване на уменията и компетентността на ИТ специалистите (например администратори на интернет страници).

**Комисията ще:**

- организира, с подкрепата на ENISA, **първенство** в областта на киберсигурността през 2014 г., в което студенти ще се съревновават в намирането на решения в областта на МИС.

**Комисията приканва държавите членки[21] да:**

- организират от 2013 г. нататък ежегодно **месец на киберсигурността** с помощта на ENISA и участието на частния сектор с цел да бъде повишена осведомеността на крайните потребители. От 2014 г. месец на киберсигурността ще бъде организиран съгласувано между ЕС и САЩ;

- **да увеличат усилията, полагани на национално равнище за образование и обучение в областта на МИС,** чрез въвеждане на: обучение относно МИС в училищата до 2014 г.; обучение в областта на МИС, разработката на сигурен софтуер и защитата на личните данни за студентите по компютърни науки; базово обучение относно МИС за служители, работещи в публичните администрации.

**Комисията призовава промишлеността да:**

- насърчава **осведомеността относно киберсигурността на всички равнища** както в стопанските практики, така и във връзките си с клиенти. По-специално промишлеността следва да разгледа начини за възлагането на по-голяма отговорност на изпълнителните директори и управителните съвети в областта на киберсигурността.

### 2.2. Чувствително намаляване на киберпрестъпността

Колкото по-голяма част от живота ни преминава в цифровия свят, толкова повече възможности възникват за извършителите на киберпрестъпления. Киберпрестъпността е една от най-бързо разрастващите се форми на престъпност, като всеки ден над един милион души по света стават нейни жертви. Киберпрестъпниците и техните мрежи стават все по-опитни; затова се нуждаем от подходящи оперативни средства и капацитет за борба с тях. Киберпрестъпленията носят високи печалби, крият нисък

информация и най-добри практики във връзка с престъпното използване на интернет с цел разпространение на материали, съдържащи случаи на сексуална злоупотреба с деца, както и мрежа от изследователи, които събират информация за приложения, рискове и последствия на онлайн технологиите за живота на децата.

[21] Също така и с участието на съответните национални органи, включително на компетентните органи в сферата на МИС и органите за защита на данните.

риск и престъпниците често използват анонимността на домейните на интернет страниците. Киберпрестъпността не познава граници — глобалният мащаб на интернет означава, че правоприлагащите системи трябва да приложат координиран и съвместен трансграничен подход, за да отговорят на тази засилваща се заплаха.

**Силно и ефективно законодателство**

ЕС и държавите членки имат нужда от силно и ефективно законодателство за борба с киберпрестъпленията. Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, известна също като Будапещенска конвенция, е обвързващ международен договор, който предоставя ефективна рамка за приемането на национално законодателство.

ЕС вече прие законодателство за киберпрестъпленията, включително и Директива за борбата със сексуалната експлоатация на деца и детската порнография[22] в онлайн среда. Предстои ЕС да приеме също така Директива относно атаките срещу информационните системи, по-специално тези, при които се използват ботмрежи.

**Комисията ще:**

- осигури бързо транспониране и изпълнение на свързаните с киберпрестъпността директиви;
- призове настоятелно държавите членки, които все още не са ратифицирали **Будапещенската конвенция на Съвета на Европа за престъпленията в кибернетичното пространство**, да я ратифицират и да започнат да прилагат нейните разпоредби възможно най-скоро.

**Подобрен оперативен капацитет за борба с киберпрестъпленията**

Развитието на техниките за извършване на киберпрестъпления се ускори рязко: правоприлагащите органи не могат да водят борба с киберпрестъпността, използвайки остарели оперативни инструменти. Понастоящем не всички държави членки на ЕС имат оперативния капацитет, който е необходим, за да дадат ефективен отговор на киберпрестъпленията. Всички държави членки се нуждаят от ефективни национални звена за борба с киберпрестъпността.

**Комисията ще:**

- подпомогне посредством своите програми за финансиране[23] държавите членки **при идентифицирането на евентуални пропуски и ще подсили техният капацитет** за разследване на киберпрестъпността и борба с нея. Освен това Комисията ще подкрепи органите, осъществяващи връзката между изследователските и академичните институции, правоприлагащите органи и частния сектор, по подобие на продължаващата работа с финансираните от Комисията центрове за високи постижения в борбата с

[22] Директива 2011/93/ЕС за замяна на Рамково решение 2004/68/ПВР.

[23] За 2013 г. в рамките на програмата „Предотвратяване и борба с престъпността“ (ISEC). След 2013 г. в рамките на фонд „Вътрешна сигурност“ (нов инструмент в рамките на МФР).

киберпрестъпността, които вече са създадени в някои държави членки;

- координира, заедно с държавите членки, включително с подкрепата на JRC, усилията за определяне на най-добрите практики и най-добрите налични техники за борба с киберпрестъпността (напр. по отношение на разработването и използването на инструменти от криминалистиката или методи за анализ на заплахи);

- работи в тясно сътрудничество с наскоро създадения **в рамките на Европол Европейски център за борба с киберпрестъпността (EC3) и заедно с Евроюст** за съгласуване на тези политически подходи с най-добрите от оперативна гледна точка практики.

**Подобряване на координацията на равнище ЕС**

ЕС може да допълва работата на държавите членки, като улеснява прилагането на координиран подход на сътрудничество, предоставяйки възможности за съвместна работа на правоприлагащите и съдебните органи, публичните и частните заинтересовани страни от ЕС и извън него.

**Комисията ще:**

- подкрепи наскоро създадения **Европейски център по киберпрестъпността** (EC3) като основен европейски център в борбата с киберпрестъпността. Този център (EC3) ще предоставя анализи и проучвания на високо ниво, подкрепя разследвания, осигурява научни познания за съдебни цели, улеснява сътрудничеството, създава канали за обмен на информация между компетентните органи в държавите членки, частния сектор и други заинтересовани страни и постепенно ще поема ролята на говорител на правоприлагащата общност[24];

- подкрепи усилията за подобряване на отчетността на регистраторите на имена на домейни и ще гарантира точността на информацията за собствеността на интернет страници, по-специално въз основа на препоръките за правоприлагане, отправени към Интернет корпорацията за присвоени имена и адреси (ICANN), в съответствие с правото на Съюза, включително правилата за защита на данните;

- продължи да укрепва усилията на ЕС за справяне с практиките на сексуална злоупотреба с деца в онлайн среда, основавайки се на наскоро приетото законодателство. Комисията прие Европейска стратегия за по-добър интернет за децата[25] и заедно с държави от ЕС и извън него постави

[24] На 28 март 2012 г. Европейската комисия прие съобщение, озаглавено „Борбата с престъпността в дигиталната ера: създаване на Европейски център по киберпрестъпност“.

[25] COM(2012) 196 окончателен.

началото на **Глобален алианс срещу сексуалното посегателство над деца в интернет**[26]. Алиансът е механизъм за по-нататъшни действия от страна на държавите членки с подкрепата на Комисията и ЕС3.

**Комисията призовава Европол (ЕС3) да:**

- съсредоточи първоначално своята аналитична и оперативна подкрепа за държавите членки в разследването на киберпрестъпления, така че да помогне на първо място за премахване на престъпните мрежи в киберпространството в областта на сексуалната злоупотреба с деца, измамите при плащания, т.нар. ботмрежи и незаконното проникване в системи;

- изготвя редовно стратегически и оперативни доклади относно тенденциите и възникващите заплахи с цел определяне на приоритети и планиране на разследвания от екипите за борба с киберпрестъпността в държавите членки.

**Комисията призовава Европейския полицейски колеж (CEPOL) в сътрудничество с Европол да:**

- координира разработването и планирането на курсове, чрез които правоприлагащите органи да придобият знания и експертни умения за ефективно справяне с киберпрестъпността.

**Комисията призовава ENISA да:**

- определи основните пречки пред съдебното сътрудничество в областта на разследванията на киберпрестъпления и пред координацията между държавите членки и с трети държави и да подкрепи разследването и съдебното преследване на киберпрестъпленията на оперативно и стратегическо равнище, както и обучението в тази област.

**Комисията призовава Евроюст и Европол (ЕС3) да:**

- си сътрудничат тясно, *inter alia,* чрез обмен на информация, за да се повиши тяхната ефективност в борбата с киберпрестъпността в съответствие със съответните им правомощия и компетентност.

### 2.3. Разработване на политика за кибернетична отбрана и изграждане на капацитет, свързан с рамката на общата политика за сигурност и отбрана (ОПСО)

Усилията в областта на киберсигурността в ЕС включват също аспекта на кибернетичната отбрана. За да се повиши устойчивостта на комуникационните и информационните системи, подкрепящи отбраната и националните интереси на държавите членки в областта на сигурността, изграждането на капацитет за

[26] Заключения на Съвета относно Глобалния алианс срещу сексуално посегателство над деца в интернет (Съвместна декларация на ЕС и САЩ) от 7 и 8 юни 2012 г. и Декларацията относно създаването на Глобален алианс срещу сексуално посегателство над деца в интернет (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

кибернетична отбрана следва да се концентрира в областта на откриването, реагирането и възстановяването от сложни заплахи за киберсигурността.

Като се има предвид, че заплахите са с множество аспекти, полезните взаимодействия между гражданските и военните усилия за защита на критични активи в кибернетичното пространство следва да бъдат засилени. Тези усилия следва да бъдат подкрепени от научноизследователска и развойна дейност, както и чрез по-тясно сътрудничество между правителствата, частния сектор и академичните среди в ЕС. За да се избегне дублирането на усилия, ЕС ще проучи възможностите как ЕС и НАТО могат да допълват взаимно усилията си за подобряване на устойчивостта на критични правителствени, отбранителни и други информационни инфраструктури, от които зависят членовете на двете организации.

**Върховният представител ще се съсредоточи върху следните ключови дейности, като прикани държавите членки и Европейската агенция по отбрана към сътрудничество за:**

- оценяване на оперативните изисквания относно кибернетичната отбрана на ЕС и насърчаване на изграждането на капацитет и технологии за кибернетична отбрана в ЕС, така че да бъдат обхванати всички аспекти на изграждането на капацитет, включително доктрина, ръководство, организация, персонал, обучение, технологии, инфраструктура, логистика и оперативна съвместимост;

- разработване на политическата рамка на ЕС за кибернетична отбрана с цел защита на мрежите, използвани при мисии и операции на ОПСО, включително динамично управление на риска, подобрен анализ на опасностите и обмен на информация. Подобряване на възможностите за военни обучения и учения в областта на кибернетичната отбрана в европейски и многонационален контекст, включително интегриране на елементи на кибернетичната отбрана в настоящите програми на ученията;

- насърчаване на диалога и координацията между гражданските и военните участници в ЕС със специално ударение върху обмена на добри практики, обмена на информация и ранното предупреждение, реагирането при инциденти, оценката на риска, повишаването на осведомеността и определянето на киберсигурността като приоритет;

- осигуряване на диалог с международни партньори, включително НАТО, други международни организации и многонационални центрове за високи постижения, с цел да се осигури ефективна отбранителен капацитет, да се идентифицират областите за сътрудничество и да се избегне дублиране на усилията.

### 2.4. Разработване на промишлени и технологични ресурси за киберсигурността

Европа има отличен капацитет за научноизследователска и развойна дейност, но много от световните лидери, предоставящи новаторски продукти и услуги в областта на ИКТ са разположени извън ЕС. Съществува риск Европа да стане прекомерно зависима не само от ИКТ, произведени някъде другаде, но също така и от решения в областта на сигурността, разработени извън нейните граници. От ключово значение е да се гарантира, че хардуерните и софтуерните компоненти, произведени в ЕС и в трети

държави, които се използват в критични услуги и инфраструктура, и във все по-голяма степен в мобилните устройства, са надеждни, сигурни и гарантират защитата на личните данни.

**Стимулиране изграждането на единен пазар за продукти в областта на киберсигурността**

Високо ниво на сигурност може да бъде гарантирано единствено ако всички участници във веригата на стойността (напр. производители на оборудване, разработчици на софтуер, доставчици на услуги на информационното общество) направят сигурността свой приоритет. Изглежда обаче[27], че все още много от участниците разглеждат сигурността като нещо, много малко различаващо се от допълнително бреме, и търсенето на решения в областта на сигурността е ограничено. Необходими са подходящи експлоатационни изисквания относно киберсигурността, които да се прилагат по протежение на цялата верига на стойността за продуктите на ИКТ, използвани в Европа. Необходими са стимули за частния сектор, за да се гарантира високо равнище на киберсигурността. Например, използването на етикети, които обозначават удовлетворителни показатели по отношение на киберсигурността, ще позволи на предприятията с добри постижения и опит в тази област да постигнат търговска реализация на продуктите си и конкурентно предимство. Освен това задълженията, залегнали в предложената Директива за МИС, ще допринесат значително за засилване на конкурентоспособността на предприятията в обхванатите сектори.

Търсенето на изключително сигурни продукти на европейския пазар също следва да бъде стимулирано. На първо място настоящата стратегия има за цел да засили сътрудничеството и прозрачността по отношение на сигурността на ИКТ продуктите. Тя призовава за създаването на платформа, обединяваща съответните европейски публични и частни заинтересовани страни с цел установяване на добри практики по отношение на киберсигурността по протежение на веригата на стойността и създаване на благоприятни пазарни условия за разработването и внедряването на сигурни решения на основата на ИКТ. Основна задача следва да бъде създаването на стимули за провеждане на подходящо управление на риска и приемане на стандарти и решения в областта на сигурността, както и евентуално създаването на доброволни схеми за сертифициране в ЕС въз основа на вече съществуващи схеми в ЕС и на международно равнище. Комисията ще насърчава приемането на съгласувани подходи сред държавите членки, за да се избегнат несъответствия, водещи до възникването на неблагоприятни условия за предприятията в зависимост от тяхното местоположение.

На второ място, Комисията ще подкрепя разработването на стандарти за сигурност в целия ЕС и ще съдейства на доброволните схеми за сертифициране в областта на изчислителните облаци, като в същото време надлежно взема предвид необходимостта от осигуряване на защита на личните данни. Работата следва да се съсредоточи върху сигурността на веригата на доставки, по-специално в критични икономически сектори (системите за промишлен контрол, енергийната и транспортната инфраструктура). Тази дейност следва да се основава на текущата работа по стандартизация на европейските

[27] Вж. работния документ на службите на Комисията, представляващ оценка на въздействието, придружаващ предложението на Комисията за Директива относно мрежовата и информационна сигурност, раздел 4.1.5.2.

организации за стандартизация (CEN, CENELEC и ETSI)[28], на Групата за координация по киберсигурността (CSCG), а така също и на експертния капацитет на ENISA, Комисията и други заинтересовани участници.

[28] По-специално в рамките на стандарт M/490 относно интелигентните електропреносни мрежи за първия набор от стандарти и референтна архитектура за такива мрежи.

Комисията ще:

- стартира през 2013 г. публично-частна **платформа за решения в областта на МИС** с цел да се създадат стимули за внедряването на сигурни решения на основата на ИКТ и да се подобри равнището на киберсигурността на използваните в Европа продукти на ИКТ;

- предложи през 2014 г. препоръки за гарантиране равнището на киберсигурността по протежение на цялата верига на стойността на ИКТ въз основа на работата на тази платформа;

- проучи как основните доставчици на хардуер и софтуер за ИКТ могат да уведомяват компетентните национални органи относно открити слаби места, които биха могли да имат значително въздействие върху сигурността.

**Комисията призовава ENISA да:**

- разработи в сътрудничество със съответните национални компетентни органи, заинтересованите страни, международните и европейските организации за стандартизация и Съвместния изследователски център на Европейската комисия **технически насоки и препоръки за приемането на стандарти и добри практики за МИС** в публичния и частния сектор;

**Комисията приканва публичните и частните заинтересовани страни да:**

- създадат стимули за разработването и внедряването на **стандарти за сигурност** и технически норми по инициатива на промишлеността, както и за прилагането на принципите за отчитане на изискванията относно сигурността и неприкосновеността на личните данни още на етапа на проектиране от страна на производителите на ИКТ продукти и на доставчиците на ИКТ услуги, включително доставчиците на изчислителни облаци. Новите поколения софтуер и хардуер следва да разполагат с **по-мощни, вградени и удобни** за потребителя функции за сигурност;

- разработят стандарти по инициатива на промишлеността относно показателите на предприятията в сферата на киберсигурността и да подобрят информацията, предоставяна на обществеността, като разработят **етикети за сигурност** или знаци за качество, които подпомагат ориентирането на потребителите на пазара.

**Насърчаване на инвестициите в научноизследователската и развойната дейност и в иновациите**

Научноизследователската и развойната дейност може да подкрепи една силна промишлена политика, да подпомогне възникването на надежден европейски сектор на ИКТ, да стимулира развитието на вътрешния пазар и да намали зависимостта на Европа от чужди технологии. От НИРД се очаква да запълни технологичните празноти в областта на сигурността на ИКТ, да подготви промишлеността за следващото поколение предизвикателства в областта на сигурността, да отчете непрекъснатото развитие на потребителските нужди и да ни осигури предимствата от възможната

двойна употреба на технологии. Тя следва също така да продължи да подпомага развитието на криптографията. Това трябва да бъде допълнено от усилия за превръщане на резултатите от научноизследователската и развойната дейност в търговски решения чрез предоставяне на необходимите стимули и въвеждането на подходящи политически условия.

ЕС трябва да извлече най-доброто от Рамковата програма за научни изследвания и иновации „Хоризонт 2020“[29], която ще започне да се изпълнява през 2014 г. В предложението на Комисията са залегнали конкретни цели за надеждността на ИКТ, както и за борбата с киберпрестъпността, които са в съответствие с тази стратегия. „Хоризонт 2020“ ще подкрепя изследвания в областта на сигурността, свързани с нови информационни и комуникационни технологии; ще предоставя решения за сигурни „от край до край“ ИКТ системи, услуги и приложения; ще осигурява стимули, необходими за изпълнението и приемането на съществуващи решения; и ще допринася за постигането на оперативна съвместимост на мрежовите и информационните системи. Специално внимание на равнище ЕС ще бъде отделено на оптимизирането и по-добрата координация на различните програми за финансиране („Хоризонт 2020“, фонд „Вътрешна сигурност“, бюджет за научноизследователска дейност на Европейската агенция по отбрана, включително Европейската рамка за сътрудничество).

**Комисията ще:**

- използва „Хоризонт 2020“, за да работи по редица теми от областта на неприкосновеността на личния живот и сигурността на ИКТ — от научноизследователската и развойната дейност до иновациите и внедряването. „Хоризонт 2020“ ще разработи също и пособия и инструменти за борба с престъпни и терористични действия в кибернетичната среда;

- създаде механизми за по-добра координация на научноизследователските програми на институциите на Европейския съюз и държавите членки и ще насърчи държавите членки да инвестират повече в научноизследователската и развойната дейност.

**Комисията приканва държавите членки да:**

- разработят до края на 2013 г. добри практики за използване на **покупателната способност на публичните администрации** (например възлагането на обществени поръчки), за да стимулират разработването и внедряването на характеристики в областта на сигурността в продукти и услуги в сферата на ИКТ;

- насърчават ранното участие на промишлеността и академичните среди в разработването и координирането на решения. Това следва да се постигне чрез пълноценно използване на индустриалната база на Европа и свързаните с нея технологични иновации по НИРД, като програмите за научни

[29] „Хоризонт 2020“ е финансовият инструмент за изпълнение на „Съюза за иновации“ – водеща инициатива на стратегията „Европа 2020“, насочена към гарантиране на конкурентоспособността на Европа в световен план. Новата рамкова програма за научни изследвания и иновации в ЕС, която ще е в сила от 2014 г. до 2020 г., ще бъде част от усилието да се създадат нови възможности за растеж и работни места в Европа.

изследвания на граждански и военни организации бъдат координирани;

**Комисията призовава Европол и ENISA да:**

- идентифицират с оглед на развитието на методите за извършване на киберпрестъпления зараждащите се тенденции и нужди относно мерките в областта на киберсигурността, така че да бъдат разработени подходящи инструменти и технологии в служба на криминалистиката.

**Комисията приканва публичните и частните заинтересовани страни да:**

- разработят в сътрудничество със застрахователния сектор **хармонизирани показатели за изчисляване на рисковите премии**, които да позволят на предприятията, направили инвестиции в областта на сигурността, да се възползват от по-ниски рискови премии.

### 2.5. Изграждане на последователна международна политика на Европейския съюз относно киберпространството и насърчаване на основните ценности на ЕС

Запазването на открития характер, свободата и сигурността на киберпространството е глобално предизвикателство, с което ЕС трябва да се заеме съвместно със съответните международни партньори и организации, частния сектор и гражданското общество.

В своята международна политика относно киберпространството ЕС ще се стреми да насърчава откритостта и свободата на интернет както и усилията за разработване на норми на поведение и да прилага съществуващите международни закони в киберпространството. ЕС ще работи също така за преодоляване на цифровото разделение и ще участва активно в международните усилия за изграждане на капацитет в областта на киберсигурността. Международната ангажираност на ЕС по въпросите на киберпространството ще се ръководи от основните ценности на ЕС — човешкото достойнство, свободата, демокрацията, равенството, принципа на правовата държава и зачитането на основните права.

**Включване на въпросите на киберпространството във външните отношения на ЕС и общата външна политика и политика на сигурност**

Комисията, върховният представител и държавите членки следва да формулират една съгласувана международна политика на ЕС по въпросите на киберпространството, която да бъде насочена към увеличаване на ангажираността и по-стабилни отношения с ключови международни партньори и организации, както и с гражданското общество и частния сектор. Следва да бъдат планирани, координирани и проведени консултации на ЕС с международни партньори по въпроси на киберпространството, за да се добави стойност към съществуващите двустранни диалози между държавите — членки на ЕС, и трети държави. ЕС отново ще постави ударението върху диалога с трети държави, по-специално върху отношенията с партньори със сходни разбирания, които споделят ценностите на ЕС. Съюзът ще насърчава постигането на високо ниво на защита на данните, включително в случаите на трансфер на лични данни към трета държава. За да се справи с глобалните предизвикателства в киберпространството, ЕС ще се стреми към по-тясно сътрудничество с организации, които работят в тази област, като например Съвета на Европа, ОИСР, ООН, ОССЕ, НАТО, Африканския съюз, ASEAN и Организацията на американските държави (ОАД). На двустранно равнище

сътрудничество със Съединените щати е от особено значение и ще бъде развивано по-нататък, по-специално в контекста на работната група ЕС—САЩ по киберсигурността и киберпрестъпленията.

Един от основните елементи на международната политика на ЕС относно киберпространството ще бъде насърчаването на свободата и основните права в него. Разширяването на достъпа до интернет следва да подкрепи демократичните реформи и тяхното разпространение в световен мащаб. Нарастването на глобалната свързаност не следва да бъде съпроводено от цензура или масово наблюдение. ЕС следва да насърчава корпоративната социална отговорност[30] и да даде старт на международни инициативи с цел подобряване на глобалното сътрудничество в тази област.

Отговорността за повишаване на сигурността в киберпространството се носи от всички участници в глобалното информационно общество — от гражданите до правителствата. ЕС подкрепя усилията за определяне на норми на поведение в киберпространството, към които следва да се придържат всички заинтересовани страни. Така както ЕС очаква от гражданите да спазват своите граждански задължения, социални отговорности и законодателството в онлайн среда, така и държавите членки следва да спазват нормите и съществуващото законодателство. По въпросите на международната сигурност ЕС насърчава разработването на мерки за изграждане на доверие в киберсигурността с цел повишаване на прозрачността и намаляване на риска от погрешно възприемане на поведението на държавата.

ЕС не призовава за създаване на нови международни правни инструменти по въпросите на киберпространството.

Правните задължения, залегнали в Международния пакт за граждански и политически права, Европейската конвенция за правата на човека и Хартата на основните права на ЕС следва да бъдат спазвани и в онлайн среда. ЕС ще се съсредоточи върху въпроса как да се гарантира, че тези мерки се прилагат и в киберпространството.

С цел справяне с киберпрестъпността Будапещенската конвенция е инструмент, който е отворен за приемане от трети държави. Тя предоставя модел за разработване на национално законодателство в областта на киберпрестъпленията и основа за международно сътрудничество в тази област.

В случай че даден въоръжен конфликт се пренесе в киберпространството, за него ще важат принципите на правото на въоръжените конфликти и, ако е уместно, международното хуманитарно право.

**Разработване на капацитет въз основа на мерките за киберсигурност и устойчивите информационни инфраструктури в трети държави**

Безупречното функциониране на основните инфраструктури, които предоставят и улесняват съобщителните услуги, ще бъде подпомогнато от засиленото международно сътрудничество. Това включва обмен на най-добри практики, обмен на информация, ранно предупреждение, съвместни учения за управление на инцидентите и др. ЕС ще допринесе за постигането на тази цел чрез увеличаване на текущите международни усилия за укрепване на мрежите за сътрудничество относно защитата на критичната

[30] Обновена стратегия на ЕС за периода 2011—2014 г. за корпоративна социална отговорност; COM(2011) 681 окончателен.

информационна инфраструктура (CIIP), включително сътрудничеството с правителства и частния сектор.

Поради липсата на открит, сигурен, оперативно съвместим и надежден достъп не всички части на света се възползват от положителните ефекти на интернет. Поради това Европейският съюз ще продължи да подкрепя усилията на държавите да развият достъпа и използването на интернет за своите народи, така че да гарантират неговата цялостност и сигурност и да се противопоставят ефективно на киберпрестъпността.

**В сътрудничество с държавите членки Комисията и върховният представител ще:**

- работят за постигане на съгласувана международна политика на ЕС по въпросите на киберпространството, за да бъде разширено сътрудничеството с ключови международни партньори и организации, да бъдат включени въпроси на киберпространството в ОВППС, и да се подобри координацията по глобалните въпроси на киберпространството;

- подкрепят разработването на норми на поведение и мерки за изграждане на доверие в областта на киберсигурността; улесняват диалога относно начина на прилагане на съществуващото международно право в киберпространството и насърчават Будапещенската конвенция за справяне с киберпрестъпността;

- подкрепят утвърждаването и защитата на основните права, включително достъпа до информация и свободата на изразяване на мнение, като се съсредоточават върху: а) разработването на нови публични насоки относно свободата на изразяване на мнение в онлайн средата и извън нея; б) мониторинга на износа на продукти или услуги, които могат да бъдат използвани с цел осъществяване на цензура или масово наблюдение в онлайн среда; в) разработването на мерки и инструменти за разширяване на достъпа до интернет, откритостта и устойчивостта с цел да се предотврати цензурата или масовото наблюдение с помощта на комуникационни технологии; г) предоставянето на възможност на заинтересованите страни да използват комуникационните технологии за утвърждаване на основните права;

- работят с международни партньори и организации, частния сектор и гражданското общество за изграждането на глобален капацитет в трети държави с цел да се подобри достъпът до информация и до един отворен интернет, да бъдат предотвратени и да се противодейства на кибернетичните заплахи, включително произтичащите от случайни събития, киберпрестъпления и кибертероризъм, както и да бъде постигната координация на донорите за управление на изграждането на капацитет;

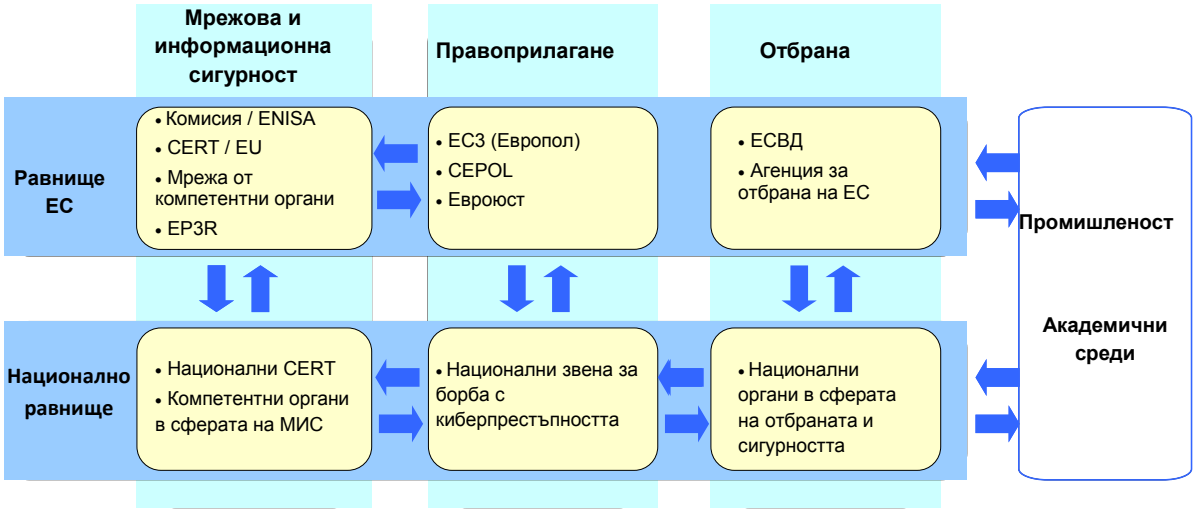
- използват различни инструменти за предоставяне на помощи на ЕС, за да подкрепят изграждането на капацитет в областта на киберсигурността, включително подпомагане обучението на правоприлагащия, съдебния и техническия персонал, насочено към овладяване на киберзаплахите; както и да подкрепят създаването на съответните национални политики, стратегии и институции в трети държави;

- засилят координацията на политиките и обмена на информация чрез международната мрежа за сътрудничество относно защитата на критичната информационна инфраструктура (CIIP), сътрудничеството между компетентните органи в сферата на МИС и други субекти.

## 3. РОЛИ И ОТГОВОРНОСТИ

Във взаимосвързаните цифрови икономики и общества инцидентите в киберпространството не се спират на границите на държавите. Всички участници — от компетентните органи в сферата на МИС, CERT и правоприлагащите органи до промишлеността — трябва да поемат отговорност както на национално, така и на равнище ЕС, и да работят заедно за укрепването на киберсигурността. Тъй като в това сътрудничество могат да се включат различни правни рамки и юрисдикции, основно предизвикателство пред ЕС е да се изяснят ролите и отговорностите на множеството участници.

Като се има предвид сложността на въпроса и разнообразният кръг от участници, един централизиран европейски надзор не е решение. Националните правителства са в най-добра позиция да организират мерките за превенция и реакция на инциденти и атаки в киберпространството и да установят контакти и мрежи с участието на частния сектор и широката общественост в съответствие със своите политически направления и правни рамки. В същото време поради теоретично или практически безграничния характер на рисковете ефективния отговор на национално равнище често налагат участие на равнище ЕС. За да бъде работата по въпросите на киберсигурността всеобхватна, дейностите следва да обхващат три основни стълба — МИС, правоприлагане и отбрана, които от своя страна са част от различни правни рамки:




### 3.1. Координация между компетентните органи в сферата на МИС/екипите за незабавно реагиране при компютърни инциденти, правоприлагащите органи и отбраната

**Национално равнище**

Държавите членки следва вече да имат структури за работа по въпроси на устойчивостта на киберпространството, киберпрестъпността и отбраната, или да изградят такива в резултат от настоящата стратегия; техния капацитет за справяне с инциденти в киберпространството следва да достига изискваното равнище. Въпреки това предвид факта, че редица субекти могат да имат оперативни отговорности за различни аспекти на киберсигурността, и като се има предвид важността на участието на частния сектор, координацията на национално равнище следва да бъде оптимизирана между министерствата. Държавите членки следва да определят в своите национални стратегии относно киберсигурността ролите и отговорностите на различните си национални структури.

Обменът на информация между национални структури, както и с частния сектор, трябва да бъде насърчен, за да се даде възможност на държавите членки и частния сектор да поддържат общо виждане за различните заплахи и с цел по-доброто разбиране на новите тенденции и техники — както на използваните за осъществяване на кибератаки, така и на тези, използвани за ускоряване на ответните действия. Чрез създаването на национални планове за сътрудничество в сферата на МИС, които да се задействат в случай на инциденти в киберпространството, държавите членки следва да бъдат в състояние да разпределят ясно формулирани роли и отговорности и да оптимизират ответните действия.

**Равнище на ЕС**

Точно както и на национално равнище, на равнището на ЕС съществуват редица участници с дейност е във връзка с киберсигурността. ENISA, Европол/ЕС3 и ЕАО са по-специално три агенции, действащи съответно в областта на МИС, правоприлагането и отбраната. Тези агенции имат управителни съвети, в които са представени държавите членки, и предлагат платформи за координация на равнище ЕС.

Координацията и сътрудничеството между ENISA, Европол/ЕС3 и ЕАО ще бъдат насърчавани в редица области, в които те действат съвместно, особено по отношение на анализа на тенденциите, оценката на риска, обучението и обмена на най-добрите практики. Те трябва да си взаимодействат, като същевременно запазват своята специфика. Тези агенции заедно с CERT-EU, Комисията и държавите членки следва да подкрепят развитието на една надеждна общност от технически и политически експерти в тази област.

Неофициалните канали за координация и сътрудничество ще бъдат допълнени от по-структурни връзки. Военният персонал на ЕС и екипът на проекта на ЕАО за кибернетична отбрана могат да се използват като механизъм за координация в областта на отбраната. Програмният съвет на Европол/ЕС3 ще обедини, наред с други участници, Евроюст, Европейския полицейски колеж, държавите членки[31], ENISA и Комисията и ще им даде възможност да споделят своите знания и да гарантират, че действията на ЕС3 се извършват в рамките на партньорство, като се признават допълнителните експертни знания и се зачитат мандатите на всички заинтересовани страни. Новият мандат на ENISA следва да даде възможност за увеличаване на връзките ѝ с Европол и за засилване на обвързаността със заинтересованите страни от промишлеността. Най-важното е, че законодателното предложение на Комисията относно МИС ще създаде рамка за сътрудничество посредством мрежа от национални

[31] Чрез представителство в рамките на работната група на ЕС по киберпрестъпността, която е съставена от ръководителите на звената за киберпрестъпност на държавите членки.

компетентни органи в сферата на МИС и ще позволи обмен на информация между МИС и правоприлагащите органи.

**Международно равнище**

Комисията и върховният представител гарантират, заедно с държавите членки, координирани международни действия в областта на киберсигурността. По този начин Комисията и Върховният представител ще подкрепят основните ценности на ЕС и ще насърчават мирното, открито и прозрачно използване на кибертехнологиите. Комисията, върховният представител и държавите членки се ангажират в политически диалог с международни партньори и с международни организации като ОИСР, Съвета на Европа, ОССЕ, НАТО и ООН.

## 3.2. Подкрепа от страна на ЕС в случай на сериозен инцидент или атака в киберпространството

Вероятно е сериозните инциденти или атаки в киберпространството да имат въздействие върху правителствата, бизнеса или отделни физически лица в ЕС. В резултат на настоящата стратегия, и по-специално на предложената Директива относно МИС, превенцията, откриването и отговора на инциденти в киберпространството следва да се подобри, а държавите членки и Комисията следва да поддържат по-тесен информационен обмен помежду си относно сериозни инциденти или атаки в киберпространството. Въпреки това механизмите за отговор ще бъдат различни в зависимост от естеството, размера и трансграничните последствия от инцидента.

Ако инцидентът нарушава сериозно функционирането на икономиката, Директивата за МИС предлага да се задействат планове за сътрудничество в сферата на МИС на национално равнище или на равнище ЕС, в зависимост от трансграничния характер на инцидента. Мрежата от компетентни органи в сферата на МИС ще се използва в този контекст за споделяне на информация и оказване на подкрепа. Това ще позволи запазването и/или възстановяването на засегнатите мрежи и услуги.

Ако има данни, че инцидентът е свързан с престъпление, Европол/ЕС3 следва да бъде информиран, така че да може, заедно с правоприлагащите органи от засегнатите държави, да започне разследване, да подсигури доказателствата, да разкрие извършителите и накрая да гарантира тяхното съдебно преследване.

Ако има данни, че инцидентът е свързан с кибершпионаж или е подкрепена от друга държава атака или има последствия за националната сигурност, органите на националната сигурност и отбрана ще информират своите съответни партньори, така че последните да знаят, че са обект на нападение и да могат да се защитят. В такъв случай ще бъдат задействани механизми за ранно предупреждение и, ако е необходимо, също процедури по управлението на кризи и други процедури. Особено сериозни инциденти или атаки в киберпространството биха могли да представляват достатъчно основание за държава членка да се позове на клаузата за солидарност на ЕС (член 222 от Договора за функционирането на Европейския съюз).

Ако има опасения, че в резултат на инцидента са застрашени лични данни, в процеса следва да бъдат включени националните органи за защита на данните или националният регулаторен орган в съответствие с Директива 2002/58/ЕО.

И накрая, справянето с инциденти и атаки в киберпространството ще спечели от мрежите за контакти и от подкрепата на международните партньори. Това може да включва технически мерки за ограничаване на последствията, водене на следствие или задействане на механизми за отговор в рамките на управлението на кризи.

## 4. ЗАКЛЮЧЕНИЕ И ПОСЛЕДВАЩИ МЕРКИ

Настоящото предложение за стратегия на Европейския съюз за киберсигурност, предложено от Комисията и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност, очертава виждането на ЕС и действията, необходими за превръщането — на базата на опазването и насърчаването на правата на гражданите — на онлайн средата в ЕС в най-безопасната онлайн среда в света[32].

Тази концепция може да бъде осъществена единствено чрез истинско партньорство с участието на много страни при поемането на отговорност и справянето с бъдещите предизвикателства.

Поради това Комисията и върховният представител приканват Съвета и Европейския парламент да одобрят стратегията и да подпомогнат осъществяването на очертаните действия. Силна подкрепа и ангажираност е необходима също и от страна на частния сектор и гражданското общество, които са ключови участници при подобряването на нашето равнище на сигурност и защитата на правата на гражданите.

Сега е времето да се действа. Комисията и върховният представител са решени да работят заедно с всички участници за постигането на сигурността, необходима за Европа. За да се гарантира, че стратегията се прилага незабавно и се подлага на оценка с оглед на евентуални промени в обстоятелствата, Комисията и върховният представител ще съберат всички заинтересовани страни на конференция на високо равнище след 12 месеца, на която ще бъде направена оценка на напредъка.

[32] Финансирането на стратегията ще стане в рамките на предвидените суми за всяка от съответните области на политиката (МСЕ, „Хоризонт 2020“, фонд „Вътрешна сигурност“, ОВППС и външно сътрудничество, по-специално Инструмент за стабилност), както е посочено в предложението на Комисията за многогодишната финансова рамка за периода 2014—2020 г. (след одобрение от бюджетния орган и съгласно окончателните суми на приетата многогодишна финансова рамка (МФР) за 2014—2020 г.). С оглед на необходимостта да се осигури цялостната съвместимост с броя на наличните щатни бройки за децентрализираните агенции и тавана за децентрализираните агенции във всяка разходна позиция в следващата многогодишна финансова рамка агенциите (СЕПОЛ, ЕАО ENISA, Евроюст и Европол/ЕС3), които са призвани с настоящото съобщение да поемат нови задачи, ще бъдат насърчавани да го правят, доколкото действителният капацитет на агенцията да поеме нарастващите ресурси е установен и всички възможности за преразпределение са идентифицирани.