ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 5.7.2016 г.
COM(2016) 410 final

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

Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността

1. ВЪВЕДЕНИЕ/КОНТЕКСТ

Всеки ден инциденти в сферата на киберсигурността причиняват значителни щети на европейските компании и икономика като цяло и подкопават доверието на гражданите и предприятията в цифровото общество. Кражбата на търговски тайни, на фирмена и лична информация, прекъсванията в предоставянето на услуги, включително такива от първа необходимост, и смущенията в експлоатацията на инфраструктури ежегодно нанасят икономически загуби в размер на стотици милиарди евро[1]. Те могат да имат последици и за основните права на гражданите и обществото като цяло.

Стратегията на Европейския съюз за киберсигурност от 2013 г.[2] (Стратегия на ЕС за киберсигурност) и нейната ключова цел — предстоящото в кратки срокове приемане на Директива относно мрежовата и информационната сигурност (МИС)[3] — както и Директива 2013/40/ЕС относно атаките срещу информационните системи, са до момента ядрото на политическия отговор на Европейския съюз на предизвикателствата в сферата на киберсигурността. Европейският съюз разчита и на специализирани агенции, сред които Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), Европейския център за борба с киберпрестъпността (ЕС3) към Европол и Екипа за незабавно реагиране при компютърни инциденти (CERT-EU). Отскоро се изпълняват и редица секторни инициативи (напр. в секторите на енергетиката и транспорта) за повишаване на киберсигурността в рамките на различни сектори от критично значение.

Независимо от тези действия в положителна посока, ЕС остава уязвим по отношение на киберинциденти. Това би могло да подкопае цифровия единен пазар (ЦЕП) и обществено-икономическия живот като цяло. Въздействието на тези инциденти може да надхвърли границите на икономическата сфера. При хибридни заплахи[4] кибератаките могат да бъдат координирани с други действия за дестабилизиране на определена страна или като предизвикателства към политически институции.

На този фон справянето с мащабни киберинциденти, засягащи няколко държави членки едновременно, може да представлява изключително сериозно предизвикателство за ЕС. В синергия със съобщенията относно борбата с хибридните заплахи и изработването на европейски дневен ред в областта на сигурността[5] Комисията се стреми да идентифицира методи за справяне с динамичните промени в областта на киберсигурността и да прецени необходимостта от допълнителни мерки за подобряване на устойчивостта на ЕС на киберзаплахи и способността ѝ за реакция в случай на инциденти.

---

[1] *Нетни загуби: оценка на щетите в глобален мащаб от икономически киберпрестъпления II: Център за стратегически международни изследвания; юни 2014 г.*

[2] Съвместното съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“, JOIN(2013) 1 окончателен.

[3] Предложение за Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, COM(2013) 48 окончателен.

[4] Съвместно съобщение до Европейския парламент и Съвета: Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз, JOIN(2016) 18 окончателен, 6.4.2016 г.

[5] Съобщение на Комисията до Европейския парламент, Европейския съвет и Съвета: Изпълнение на европейската програма за сигурност с цел борба срещу тероризма и подготвяне на условията за ефективен и истински Съюз на сигурност COM(2016) 230.

Освен това Комисията работи за повишаване на индустриалния капацитет в областта на киберсигурността на Европейския съюз. Макар и Европа да не може да овладее цялата верига на стойността при цифровите технологии, съществува необходимост най-малкото от запазване и развитие на определени ключови способности. Предлагането на продукти и услуги, гарантиращи най-високо ниво на киберсигурност, е добра възможност за сектора на киберсигурността в Европа и би могло да се превърне в силно конкурентно предимство. Според очакванията пазарът на решения, свързани с киберсигурността ще бъде сред най-бързо развиващите се сегменти в сектора на ИКТ[6]. Превръщането на ЕС във водещ играч в тази сфера следва да бъде подкрепено от трайно установена култура на защита на сигурността на данните, включително личните данни, и ефективна реакция в случай на инциденти. Това ще представлява убедителен аргумент в полза на инвестирането в ЕС, допринасяйки по този начин за постигането на амбициозните цели на цифровия единен пазар за растеж и създаване на работни места.

Постигането на горепосочените цели изисква сериозен ангажимент и по-специално:

i) По-тясно и интензивно сътрудничество за укрепване на готовността и за справяне с киберинциденти

Необходимо е съществуващите и договорени механизми за сътрудничество да бъдат укрепени с цел повишаване на устойчивостта и готовността на ЕС, включително за справяне с потенциална общоевропейска криза в областта на киберсигурността. Тези механизми за сътрудничество следва да бъдат всеобхватни по цялата верига на един инцидент — от превенцията до наказателното преследване. Ефективното сътрудничество между държавите членки и практическото изпълнение на изискванията за сигурност от критични оператори създава допълнителна необходимост от предлагане на надеждни технически решения от страна на сектора на киберсигурността.

Същевременно, за да се гарантира устойчивост за най-важните киберактиви на територията на целия ЕС ще се изисква трайно усилие за установяване на междусекторни синергии и включване на изискванията за киберсигурност във всички приложими политики на ЕС. Комисията ще проучи необходимостта от скорошна актуализация на приетата през 2013 г. Стратегия на ЕС за киберсигурност.

ii) Преодоляване на предизвикателствата пред европейския единен пазар на киберсигурност

Стратегията за цифров единен пазар (ЦЕП)[7] признава, че все още съществуват специфични празноти в бързо развиващата се сфера на технологиите и решенията за мрежова сигурност в интернет. Едновременно с това според пазарни проучвания, по отношение на предлагането на продукти и услуги в сферата на киберсигурността, вътрешният пазар на ЕС продължава да бъде географски разпокъсан[8]. Настоящото Съобщение предлага редица пазарно ориентирани мерки на ниво политики, които имат

[6] Вж. Работен документ за служителите на Комисията SWD(2016) 2016.
[7] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Стратегия за цифров единен пазар за Европа, COM/2015/0192 окончателен.
[8] Вж. Работен документ за служителите на Комисията SWD(2016) 216.

за цел запълване на установените празноти и преодоляване на съществуващите предизвикателства пред единния пазар.

iii) Повишаване на индустриалния капацитет в областта на киберсигурността

В Стратегията на ЕС за киберсигурност и Стратегията за ЦЕП Комисията пое ангажимент да насърчи сектора на киберсигурността в ЕС да предлага повече продукти и услуги. В тази връзка Комисията е в процес на приемане на решение, което ще открие възможност за сключване на договорни публично-частни партньорства (ПЧП) в сферата на киберсигурността като стимул за постигането на напредък в създаването на модерна европейска програма за изследвания и иновации в областта на киберсигурността за повишаване на конкурентоспособността.

2. ИЗВЕЖДАНЕ НА СЪТРУДНИЧЕСТВОТО, ЗНАНИЯТА И КАПАЦИТЕТА НА ПО-ВИСОКО НИВО

Стратегията на ЕС за киберсигурност и по-специално предстоящата Директива относно МИС[9] ще очертаят пътя за по-добро сътрудничество между държавите членки на равнище ЕС. Бързото и ефективно изпълнение на директивата ще бъде от ключово значение предвид нарастващата цифровизация на икономическия и обществен живот (и предвид също така компютърните услуги „в облак“, „Интернет на нещата“ и комуникацията „машина-машина“), увеличаващата се трансгранична свързаност и цялостният контекст на бързи промени при киберзаплахите[10]. В този контекст Европейският съюз трябва да бъде подготвен за потенциална мащабна киберкриза[11], включително кибератаки срещу информационни системи с критично значение в няколко държави членки[12].

Следователно сътрудничеството на равнище ЕС е изключително важно за справяне с по-маломащабните, но притежаващи потенциал за бързо разпространение киберинциденти, и с потенциална мащабна кибератака в няколко държави членки. Необходимо е ЕС да интегрира аспектите на киберсигурността в механизмите за управление на кризи. Необходимо е също така да се създадат условия за ефективно сътрудничество и да се изградят механизми за информационен обмен между отделните сектори и държави членки, които да укрепят способността им за реакция и овладяване на подобни инциденти. Освен това съответните механизми следва да функционират съгласувано, подпомагайки по този начин борбата срещу тероризма, организираната престъпност и киберпрестъпността. Това би повишило способността на ЕС да се координира със своите международни партньори, за да може да реагира ефективно на глобалните заплахи и инциденти.

[9] Директивата относно мрежовата и информационната сигурност (МИС) ще изисква от държавите членки да идентифицират редица оператори, предоставящи услуги от първа необходимост в сектори като енергетика, транспорт, финанси и здравеопазване, с цел преодоляване на рисковете за киберсигурността и гарантиране, че определени доставчици на услуги предприемат подходящи мерки за намаляване на подобни рискове.

[10] Вж. Работен документ за служителите на Комисията SWD(2016) 216.

[11] Вж. например Доклада на ENISA: „Общи практики за управление на кризи на равнище ЕС и тяхната приложимост в случай на кибернетични кризи (април 2016).

[12] Вж. Работен документ за служителите на Комисията SWD(2016) 216.

2.1. Максимално оползотворяване на сътрудничеството по линия на МИС и преход към етап 2 от функционирането на Европейската агенция за мрежова и информационна сигурност (ENISA)

Съществен елемент на националните способности, необходими за покриване на изискванията на Директивата относно МИС, са екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), отговорни за предприемането на бързи ответни действия в случай на киберзаплахи и киберинциденти. Те ще формират мрежа (Мрежа на ЕРИКС) с цел насърчаване на ефективното оперативно сътрудничество при конкретни киберинциденти и споделянето на информация относно рисковете. Директивата предвижда и създаването на Група за сътрудничество за подкрепа и улесняване на стратегическото сътрудничество между държавите членки и изграждане на доверие между тях.

Отчитайки естеството и големия брой на киберзаплахите, Комисията насърчава държавите членки да се възползват в максимална степен от съществуващите механизми за сътрудничество по линия на МИС и да продължат да укрепват трансграничното сътрудничество, свързано с готовността за справяне с мащабни киберинциденти. В услуга на едно подобно допълнително сътрудничество за противодействие на значим киберинцидент би бил координираният подход по отношение на сътрудничеството при кризи, почиващ на съгласуваност между отделните елементи на кибернетичната екосистема. Подобен подход може да бъде формулиран в рамките на „модел“, който има за цел постигането на синергии и съгласуваност със съществуващите механизми за управление на кризи[13]. Това предполага необходимост от редовни проверки в рамките на учения за управление на кибернетични и други кризи. Моделът следва да предвижда и съответна роля за органи на равнището на ЕС, сред които ENISA, CERT-EU и Европейския център за борба с престъпленията в киберпространството ЕС3 към Европол, и използването на инструменти, разработени в рамките на мрежата на ЕРИКС. През първата половина на 2017 г. Комисията ще предложи такъв модел на сътрудничество за обсъждане от Групата за сътрудничество, мрежата на ЕРИКС и други заинтересовани страни.

Съществуващият към момента експертен потенциал в областта на киберсигурността в ЕС е разпокъсан и неструктуриран. В подкрепа на механизмите за сътрудничество по линия на НИС информацията следва да бъде съсредоточена в информационен център и леснодостъпна за държавите членки при отправено искане. Подобен център би представлявал централен ресурс, предоставящ на институциите на ЕС и на държавите членки възможност за споделяне на информация, когато е необходимо. Улесненият достъп до по-добре структурирана информация относно рисковете за киберсигурността следва да подпомогне усилията на държавите членки за подобряване на съществуващия капацитет и за съгласуване на практиките, повишавайки цялостната устойчивост на

[13] И по-специално Интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации (IPCR) включително решението относно договореностите за прилагане от страна на Съюза на клаузата за солидарност (24.7.2014 г.) и процесите на вземане на решения в рамките на Общата политика за сигурност и отбрана.

атаки. Комисията, с подкрепата на ENISA, Екипа за незабавно реагиране при компютърни инциденти (CERT-EU) и експертния принос на Съвместния научноизследователски център (JRC), ще съдейства за изграждането на информационен център и ще бъде гарант за неговата устойчивост.

В допълнение на равнище ЕС следва да бъде сформирана редовно заседаваща консултативна група[14] по въпросите на киберсигурността, съставена от експерти и ръководни лица от сектора, както и представители на академичната общност, гражданското общество и други работещи в тази сфера организации. Групата би осигурила на Комисията открит и прозрачен канал за достъп до външна експертна информация, необходима за разработване на стратегии за киберсигурност на ниво политики и предприемане на други потенциални действия в регулаторната сфера или в областта на публичните политики, допълвайки и изграждайки мост към други структури в сферата на киберсигурността[15].

Освен това Комисията е задължена да оцени дейността на ENISA до 20 юни 2018 г. и евентуалното изменяне или подновяването на мандата на Агенцията трябва да получи одобрение до 10 юни 2020 г.[16]. Отчитайки текущата ситуация в сферата на киберсигурността, Комисията цели да постигне напредък в оценката и — в зависимост от нейните резултати — да представи предложение във възможно най-кратки срокове.

За да прецени евентуалната необходимост от изменяне на мандата на ENISA, Комисията ще вземе предвид описаните по-горе предизвикателства в сферата на киберсигурността и цялостните усилия за по-активно сътрудничество и споделяне на знания. Този процес ще направи възможно да се оцени дали не трябва да се укрепят способностите и капацитетът на Агенцията да указва на държавите членки последователна подкрепа за постигане на устойчивост срещу киберзаплахи. Необходимо е при анализа на мандата на ENISA да бъдат отчетени и новите отговорности на Агенцията съгласно Директивата относно МИС, новите цели на политиката в подкрепа на сектора на киберсигурността (Стратегията за ЦЕП и по-специално договорните ПЧБ), нарастващите потребности от обезпечаване на сигурността на критични сектори и новите предизвикателства, свързани с трансгранични инциденти, включително съгласувания отговор на киберкризи.

Комисията:

- ще предложи за обсъждане модел за сътрудничество при мащабни киберинциденти на равнище ЕС през първото полугодие на 2017 г.;
- ще способства за създаването на информационен център в подкрепа на обмена

[14] Екпретната група на Комисията подлежи на действието на хоризонталните правила, установени от Комисията в Решение на Комисията C(2016)3301.

[15] Напр. Платформата за МИС, договорните ПЧП по киберсигурността и секторни платформи, като Платформата на експертите в енергийния сектор по въпросите на киберсигурността (EECSP). Би следвало дейността ѝ да бъде обвързана и с кръглата маса на високо равнище, обявена в Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Цифровизиране на европейската промишленост; оползотворяване в пълна степен на предимствата на цифровия единен пазар (COM(2016) 180 окончателен).

[16] Регламент (ЕС) № 526/2013 за отмяна на Регламент (ЕО) № 460/2004.

на информация между органите на ЕС и държавите членки;
- ще сформира консултативна група на високо равнище по въпросите на киберсигурността;
- ще финализира оценката на ENISA до края на 2017 г., която ще позволи да се оцени необходимостта от евентуално изменяне или продължаване на мандата на Агенцията, с цел краткосрочното изготвяне на предложение.

2.2. Повишаване на усилията за образование, обучение и подготовка в сферата на киберсигурността

Адекватните умения и обучение за предотвратяване на инциденти, свързани с киберсигурността, както и преодоляването и смекчаването на тяхното въздействие са ключови аспекти на усилията за постигане на устойчивост в сферата на киберсигурността.

Понастоящем ENISA, Европейската група за обучение и образование в областта на киберсигурността (ECTEG) в сътрудничество с Европейския център за борба с киберпрестъпността в рамките на Европол и Европейския полицейски колеж (CEPOL) играят важна роля в усилията за изграждане на капацитет — включително за разследване на киберпрестъпления — чрез разработване на ръководства, организиране на обучение и учения в областта на киберсигурността.

Същевременно киберпространството е бързо развиваща се област, в която способностите с „двойна употреба“ играят съществена роля. Това поражда необходимост от развитие на сътрудничество между гражданския и военния сектор и изграждане на синергии в обучението и подготовката за укрепване на устойчивостта и способностите на ЕС за реакция в случай на инциденти.

За да отговори на тази потребност и в продължение на Директивата относно МИС и Рамката за политиката на ЕС за кибернетична отбрана[17], службите на Комисията ще си сътрудничат с държавите членки, Европейската служба за външна дейност (ЕСВД), ENISA и други органи на ЕС[18] за създаване на платформа за образование в областта на киберсигурността, учения и платформа за обучение като стимул за синергии между обученията с гражданска и отбранителна насоченост.

Комисията:

- ще работи в тясно сътрудничество с държавите членки, ENISA, ЕСВД и други свързани органи на ЕС за изграждане на платформа за обучение в сферата на киберсигурността.

[17] Приет от Съвета по външни въпроси на Европейския съюз на 18 ноември 2014 г., Док. 15585/14.

[18] Например Европейският колеж по сигурност и отбрана, Европейският център за борба с киберпрестъпността (EC3), Европейският полицейски колеж (CEPOL) и Европейската агенция по отбрана (EDA).

2.3. Действие за намаляване на междусекторните зависимости и повишаване на устойчивостта на ключови елементи на публичната мрежова инфраструктура

Важен фактор в оценката на риска и въздействието на мащабни киберинциденти е степента на трансгранична и междусекторна зависимост. Сериозен киберинцидент в даден сектор или държава членка може пряко или непряко да окаже влияние върху — или да се разпростре в — други сектори или държави членки.

Трансграничното и междусекторно сътрудничество улеснява обмена на информация и експертни познания, като по този начин повишава степента на готовност и устойчивостта. Комисията подкрепя усилията на различни сектори за по-добро разбиране на съществуващите взаимозависимости чрез Европейската програма за защита на критичната инфраструктура[19].

Същевременно необходима предпоставка за намаляване на междусекторните рискове е способността на всеки отделен сектор да набелязва, да се подготвя и да реагира на кибернетични инциденти. Комисията ще оцени риска, произтичащ от киберинцидентите в силно свързани сектори във и извън националните граници, особено по отношение на секторите в обхвата на Директивата относно МИС, като взема предвид също така и случващото се в международен план[20]. След като направи тази оценка, Комисията ще прецени необходимостта от допълнителни, специфични правила и/или насоки относно готовността на подобни критични сектори за справяне с рисковете за киберсигурността.

На европейско равнище Секторните центрове за споделяне и анализ на информация[21] (ISACs) и съответните Екипи за незабавно реагиране при компютърни инциденти (ЕРИКС) могат да играят ключова роля в подготовката и реакцията в случай на киберинциденти. За гарантиране на ефективен информационен поток относно динамиката на заплахите и улесняване на реакцията в случай на киберинциденти, ISACs следва да бъдат насърчавани да работят съвместно в рамките на мрежата ЕРИКС, създадена съгласно Директивата относно МИС, и с Европейския център за борба с киберпрестъпността в рамките на Европол, CERT-EU, както и със съответните правоохранителни органи.

Обменът на информация между заинтересованите страни и властите в рамките на целия жизнен цикъл на рисковете за киберсигурността изисква участниците да са уверени, че процесът няма да породи правна отговорност за страните. Според наблюденията на Комисията са налице редица безпокойства, които възпират обмена на ценна информация за заплахи между партньорите в отделните сектори или с властите, особено в трансграничен план. Комисията ще положи усилия да разсее подобни безпокойства в интерес на по-ефективния обмен на информация за киберзаплахи.

[19] Вж. Работен документ за служителите на Комисията SWD(2013) 318.
[20] Напр. Пътната карта за киберсигурност, приета от Европейската агенция за авиационна безопасност, Пътната карта за киберсигурност, документи на Международната организация за гражданско въздухоплаване и Международната морска организация.
[21] Вж. например Европейска енергия — Център за споделяне и анализ на информация (ISAC) (www.ee-isac.eu).

Надеждните, гарантиращи поверителност канали за докладване са друг жизненоважен стимул за докладване на кибернетични кражби на търговски тайни от страна на компаниите. Това би направило възможно наблюдението и оценката на претърпените от европейската индустрия щети (включително загуба на приходи от продажби и работни места) и научноизследователски органи. Това ще помогне за разработването на подходящ отговор на ниво политики. Със съдействието на ENISA, Службата на Европейския съюз за интелектуална собственост (EUIPO) и EC3 в рамките на Европол Европейската комисия — в диалог със заинтересованите страни от частния сектор — ще изгради надеждни канали за доброволно докладване на кибернетични кражби на търговски тайни. Това би следвало да позволи събирането на анонимизирана и агрегирана информация на равнище ЕС. Информацията може да бъде споделяна с всички държави членки в полза на дипломатическите усилия и дейностите по повишаване на информираността, в услуга на защитата на нематериалните активи на ЕС срещу кибернетични атаки.

В подкрепа на секторната киберсигурност Комисията ще насърчава и отчитането на киберсигурността при разработването на различни секторни политики на ЕС и по-специално на онези, които имат отношение към киберсигурността.

Не на последно място публичните органи също играят важна роля в проверката на надеждността и способността на ключови интернет инфраструктури да засичат проблеми, да информират отговорните за съответните мрежи страни и, при необходимост, да окажат съдействие за отстраняване на установени слабости. Националните регулаторни органи биха могли да се възползват от капацитета на ЕРИКС, за да сканират редовно публичните мрежови инфраструктури. Въз основа на резултатите те биха могли да насърчават операторите да предприемат действия за отстраняване на пропуски или евентуално констатираните уязвими места.

Европейската комисия ще проучи необходимите законодателни и организационни условия, за да предостави на националните регулаторни органи възможност — в сътрудничество с националните органи в сферата на киберсигурността — да отправят искания до ЕРИКС за провеждане на редовни проверки за уязвими места в националните мрежови инфраструктури. Националните ЕРИКС следва да бъдат насърчавани да работят в сътрудничество по линия на мрежата ЕРИКС в областта на най-добрите практики в наблюдението на мрежите, което ще улесни превенцията на мащабни киберинциденти.

Комисията:

- ще подкрепи установяването на механизъм за европейско сътрудничество между Секторните центрове за споделяне и анализ на информация и тяхната съвместна дейност с ЕРИКС и ще търси начини за премахването на бариерите, които пречат на обмена на информация между участниците на пазара;
- ще проучи стратегическия/системния риск от киберинциденти в силно свързани сектори в рамките на отделните държави и в трансграничен план;
- ще прецени необходимостта и ако сметне за целесъобразно, ще разгледа

приемането на допълнителни правила и/или насоки относно готовността за противодействие на рисковете за киберсигурността за критично важни сектори;
- съвместно с ENISA, EUIPO и EC3 ще изгради надеждни канали за доброволно докладване на кибернетични кражби на търговски тайни;
- ще насърчи въвеждането на мерки за киберсигурност в европейските секторни политики; и
- ще проучи необходимите условия, които ще позволят на националните органи да отправят искания към ЕРИКС за редовни проверки на ключови мрежови инфраструктури.

3. ПРЕОДОЛЯВАНЕ НА ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД ЕВРОПЕЙСКИЯ ЕДИНЕН ПАЗАР ЗА КИБЕРСИГУРНОСТ

Европа се нуждае от висококачествени и оперативно съвместими продукти и решения, свързани с киберсигурността, на приемливи цени. Продуктите и услугите в сферата на сигурността в рамките на единния пазар остават обаче силно разпокъсани географски. От една страна, това затруднява конкуренцията между европейските компании в национален, европейски и глобален мащаб, а от друга, ограничава избора на надеждни и приложими технологии за киберсигурност, достъпни за гражданите и предприятията[22].

Развитието на сектора на киберсигурността в Европа на практика почива основно на търсене от страна на националните правителства, включително за сектора на отбраната. Повечето европейски контрагенти в този сектор са изградили поделения [23], работещи в сферата на киберсигурността. Успоредно с това се наблюдава появата на многобройни иновативни МСП на специализирани пазари или пазарни ниши (напр. системи за криптиране), както и на утвърдени пазари, прилагайки нови бизнес модели (напр. при антивирусния софтуер).

Същевременно компаниите изпитват затруднения в разширяването на дейността си извън границите на съответните национални пазари. Това се дължи основно на липсата на доверие в предлаганите „трансгранични“ решения, констатирано от всички проведени от Комисията консултации[24]. В резултат на това голяма част от договорите за обществени поръчки все още се възлагат в рамките на отделните държави членки и много компании срещат трудности в постигането на икономии от мащаба, които биха повишили конкурентоспособността им както в рамките на вътрешния пазар, така и в глобален мащаб.

Липсата на оперативно съвместими решения (технически стандарти), практики (стандарти за процесите) и приложими на територията на целия ЕС механизми за

[22] Вж. Работен документ за служителите на Комисията.
[23] Вж. Работен документ за служителите на Комисията.
[24] Вж. Работен документ за служителите на Комисията SWD(2016) 216.

сертифициране са други празноти, които оказват влияние върху единния пазар на киберсигурност. В този контекст киберсигурността беше определена като един от приоритетите за стандартизация в сектора на ИКТ за цифровия единен пазар[25].

Ограничените перспективи за растеж на компаниите в сектора на киберсигурността в рамките на единния пазар са причина за големия брой сливания и придобивания от неевропейски инвеститори[26]. Макар тази тенденция да е доказателство за капацитета за иновации на европейските предприемачи в сектора на киберсигурността, тя поражда рискове, водещи до загуба на европейско ноу-хау, на експертни познания и до изтичане на мозъци.

Необходими са неотложни действия за изграждането на по-тясно интегриран единен пазар на продукти и услуги в сферата на киберсигурността, които ще улеснят внедряването на решения с практическа насоченост на достъпна цена.

Бариерите, произтичащи от липсата на доверие сред представителите на отрасъла и институционалната сфера в Европа, могат да бъдат преодолени чрез укрепване на сътрудничеството в ранните етапи на жизнения цикъл на иновациите — в рамките на самия сектор на киберсигурността, между доставчиците и купувачите и в междусекторен план, ангажирайки отраслите, които вече са или е вероятно да станат ползватели на решения, свързани с киберсигурността.

Същевременно разработването на продукти, услуги и технологии с двойна употреба придобива все по-голяма важност в Европа. Ръст бележи броят на разработените в гражданския сектор решения, които се внедряват в сектора на отбраната[27]. В Европейския план за действие в областта на отбраната, който предстои да бъде оповестен, Комисията възнамерява да набележи мерки за по-нататъшното укрепване на синергиите между гражданския и отбранителния сектор на европейско равнище.

3.1. Сертифициране и етикетиране

Сертифицирането играе важна роля в повишаването на надеждността и доверието в продуктите и услугите. Това се отнася в пълна степен и за новите системи, основани на цифрови технологии, които изискват висока степен на сигурност, напр. автомобили, оборудвани с устройства за връзка с интернет и автомобили с автоматично управление, електронно здравеопазване, системи за автоматизирано управление на индустриални процеси (САУИП) или интелигентни мрежи.

Разработват се и национални инициативи на високо равнище за въвеждане на изисквания за киберсигурността на ИКТ компонентите в традиционни инфраструктури, включително сертификационни изисквания. Въпреки своята важност те пораждат риск от фрагментация на единния пазар и проблеми, свързани с оперативната съвместимост. Ефективни системи за сертифициране на ИКТ продукти се прилагат в едва няколко

[25] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на Регионите Приоритети за стандартизацията в областта на ИКТ за цифровия единен пазар (COM(2016) 176/2).
[26] Вж. Работен документ за служителите на Комисията, SWD(2016) 216.

държави членки[28]. За един търговец в сектора на ИКТ това би могло да породи необходимост от преминаване през няколко процеса на сертифициране, за да търгува в различни държави членки. В най-лошия случай ИКТ продукт или услуга, разработени в съответствие със стандартите за киберсигурност в една държава членка, не може да се предлага на пазара на друга.

За постигането на функциониращ общ пазар в областта на киберсигурността въвеждането на евентуална рамка за сертифициране на свързаните със сигурността характеристики на ИКТ продуктите и услугите би следвало да има за цел: (i) покриване на широк спектър от ИКТ системи, продукти и услуги и (ii) приложимост във всички 28 държави членки и (iii) насочване към всички нива в сектора на киберсигурността, отчитайки развитието в международен план.

За тази цел Комисията ще сформира специална работна група по сертифициране на сигурността на продуктите и услугите в сферата на ИКТ, в рамките на която до края на 2016 г. експерти от държавите членки и отрасъла, съвместно с представители на ENISA и Съвместния център за научно-технически изследвания, ще проучат възможността за разработване на предложение за европейска рамка за сертифициране на сигурността в сектора на ИКТ до края на 2017 г. В този контекст Комисията ще направи преглед на Регламент (ЕО) № 2008/765 и разпоредбите относно сертифицирането на Общия регламент за защита на личните данни 2016/679[29].

Процесът ще включва широки консултации и оценка на въздействието. Това ще позволи на Комисията да прецени различните възможности за създаване на рамка за сертифициране на ИКТ продукти и услуги. Комисията ще проучи и възможността за сертифициране на сигурността в сектора на ИКТ в инфраструктурни сектори (напр. самолетостроенето, автомобилостроенето и железопътния сектор), както и специфични механизми за сертифициране и одобрение на готови за въвеждане технологии (напр. такива за контрол в областта на киберсигурността и автоматизираното управление на индустриални процеси[30], „Интернет на нещата“, услугите в облак). По този начин ще бъдат също запълнени установените празноти по линия на споменатата по-горе Европейска схема за сертифициране на сигурността в сектора на ИКТ.

Доколкото е възможно, усилията за сертифициране ще ползват установени международни стандарти и ще бъдат резултат от съвместната работа с международни партньори.

[28] Вж. Работен документ за служителите на Комисията за Групата от висши държавни служители по Споразумението относно информационните системи (Решение на Съвета от 31 март 1992 г. (92/24/ЕИО) и други съществуващи схеми, напр. Гаранцията за търговски продукти в Обединеното кралство и Схемата за сертифициране на сигурността от първо ниво във Франция.

[29] Регламент (ЕО) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни съдържа както кодекс за поведение, който има за цел да допринесе за правилното прилагане на изискванията за защита на личните данни, така и механизми за сертификация, които се основават на всички принципи за защита на личните данни, включително и по-специално на тези, които се отнасят до сигурността при обработката на лични данни.

[30] Вж. Тематична група на Европейската референтна мрежа за защита на критичната инфраструктура (ERNCIP) на https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

Комисията ще разгледа и възможности за най-подходящо интегриране на сертифицирането на сигурността на ИКТ в бъдещо секторно законодателство, включително във връзка с аспекти, свързани с безопасността.

Освен възможните регулаторни решения, Комисията ще проучи и необходимостта от въвеждане на европейска, търговски ориентирана, доброволна и несъздаваща допълнителна административна тежест схема за етикетиране на сигурността на ИКТ продуктите. Тя ще допълва сертифицирането и нейната цел ще бъде да направи по-разбираеми свързаните с киберсигурността характеристики на продуктите с търговско предназначение, повишавайки тяхната конкурентоспособност в рамките на единния пазар и в глобален мащаб. Ще бъдат отчетени и текущите секторни и хоризонтални инициативи, предприети от отрасъла, както от страна на търсенето, така и на предлагането.

Публичните администрации ще участват активно в този процес, за да способстват за използването на единни спецификации и за посочването на изискването за сертифициране в договорите за обществени поръчки. Комисията ще наблюдава и ще докладва относно прилагането на съответните изисквания за сертифициране в сферата на обществените поръчки на национално равнище и по-специално по отношение на секторните системи (енергетика, транспорт, здравеопазване, публична администрация и т.н.).

Комисията:

- ще изготви до края на 2016 г. пътна карта за разработване на проект за Европейска рамка на сертифициране на сигурността в сектора на ИКТ, който да бъде представен до края на 2017 г. и ще оцени практическата възможност и въздействието на въвеждането на европейска, административно необременителна рамка за етикетиране в областта на киберсигурността;
- ще проучи необходимостта от и целесъобразността на действия за запълване на празнотите в сертифицирането на сигурността на ИКТ в рамките на съществуващи секторни механизми за сертифициране/одобряване;
- ще включи, където е подходящо, интегрирането на сертифицирането на сигурността на ИКТ продукти в бъдещи проекти за специфични за сектора законодателни предложения;
- ще стимулира участието на публичните администрации в посока използване на механизми за сертифициране и прилагане на единни спецификации при обществените поръчки; и
- ще наблюдава прилагането на изискванията за сертифициране при възлагането на обществени поръчки и ще докладва относно състоянието на пазара след три години.

3.2. Повишаване на инвестициите в областта на киберсигурността в Европа и подкрепа за МСП

Въпреки разцвета на иновациите в сектора на киберсигурността в Европа, в ЕС все още липсва утвърдена култура на инвестиции в тази сфера. Независимо от големия брой иновативни МСП в този сектор, те често не успяват да разширят своята дейност. Сред причините за това е липсата на леснодостъпно финансиране в ранните етапи на разработване. В Европа компаниите страдат от ограничен достъп до рисков капитал и недостиг на средства за маркетинг за повишаване на видимостта или постигане на съответствие с редица изисквания за стандартизация и съответствие.

Същевременно сътрудничеството между участниците в сектора на киберсигурността е инцидентно и поражда необходимост от допълнителни усилия за повишаване на икономическата концентрация и развитие на нови вериги за създаване на стойност[31].

По-лесният достъп до финансиране е ключово условие за повишаване на инвестициите в киберсигурността в Европа и за подпомагане на МСП. Трябва да бъде подкрепено и развитието на конкурентни на глобално ниво клъстери в сектора на киберсигурността и центрове за високи достижения в рамките на благоприятстващи, регионални екосистеми за цифров растеж. За да се възползва секторът на киберсигурността в максимална степен от тази подкрепа, тя следва да бъде обвързана с изпълнението на стратегии за интелигентна специализация и с прилагането на други инструменти на ЕС.

Комисията ще следва подход, който има за цел максимална осведоменост относно възможностите за финансиране на европейско, национално и регионално равнище в рамките на сектора на киберсигурността (в рамките на хоризонтални инструменти и за конкретни търгове[32]) чрез използване на съществуващи инструменти и канали, напр. мрежата „Enterprise Europe Network“.

Комисията ще допълни тези усилия като проучи в сътрудничество с Европейската инвестиционна банка (ЕИБ) и Европейския инвестиционен фонд (ЕИФ) начините за облекчаване на достъпа до финансиране. Това може да бъде постигнато чрез капиталови и квазикапиталови инвестиции, заеми и гаранции за проекти или насрещни гаранции за посредници, напр. чрез създаването на Платформа за инвестиции в киберсигурност в рамките на Европейския фонд за стратегически инвестиции (ЕФСИ)[33].

Освен това Комисията ще проучи разработването, съвместно със заинтересовани региони и държави членки, на Платформа за интелигентна специализация в сферата на киберсигурността[34]. Това ще улесни координацията и разработването на стратегии за

[31] Вж. Работен документ за служителите на Комисията SWD(2016) 216.

[32] Вж. например многосекторната покана за предложения по програма „Свързана Европа“ от 2016 г. и поканите за предложения 2016 COSMO във връзка с програмата за интернационализация на клъстери.

[33] По линия на Европейския фонд за стратегически инвестиции пряка или непряка подкрепа за индивидуални проекти ще бъде предоставяна чрез инвестиционни платформи. Подобни платформи могат да подпомагат финансирането и на по-малки проекти и да обединяват средства от различни източници, създавайки възможност за диверсифицирани инвестиции с различен географски и тематичен акцент.

[34] Вж. инструментите за интелигентна специализация (RIS3): http://s3platform.jrc.ec.europa.eu/.

киберсигурност и установяването на стратегическо сътрудничество между заинтересовани страни в рамките на регионални екосистеми. Този подход би следвало да отключи потенциала и на съществуващите европейски структурни и инвестиционни фондове за сектора на киберсигурността.

В по-общ план Комисията ще насърчава прилагането на подхода „сигурност още при проектирането“. Тя ще се стреми да гарантира, че всички съфинансирани с европейски средства инвестиции в мащабни инфраструктури с цифров компонент отговарят на изискванията за киберсигурност. Това ще бъде постигнато чрез поетапно въвеждане на съответни програмни правила и изисквания в областта на обществените поръчки.

Комисията:

- ще използва съществуващите инструменти за подкрепа на МСП за повишаване на осведомеността относно съществуващите механизми за финансиране сред представителите на сектора на киберсигурността;
- ще активизира допълнително механизмите и инструментите на ЕС за подкрепа на МСП чрез анализ на синергиите между пазарите на решения, свързани с киберсигурността, с приложение в гражданския и отбранителния сектор[35];
- ще проучи, съвместно с ЕИБ и ЕИФ доколко е практически приложимо да се улесни достъпът до инвестиции, напр. чрез специална Платформа за инвестиции в киберсигурност или други инструменти;
- ще изгради Платформа за интелигентна специализация в сферата на киберсигурността за предоставяне в услуга на държавите членки и регионите, проявяващи интерес към инвестиции в сектора на киберсигурността (RIS3);
- ще насърчава подхода „сигурност още при проектирането“ при съфинансирани със средства на ЕС инвестиции в мащабни инфраструктури с цифров компонент.

4. СТИМУЛИРАНЕ И ПОДПОМАГАНЕ НА ЕВРОПЕЙСКАТА ИНДУСТРИЯ ЗА КИБЕРСИГУРНОСТ ЧРЕЗ ИНОВАЦИИ — СЪЗДАВАНЕ НА ДОГОВОРНИ ПЧП В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

Иновациите и конкурентоспособността на сектора в Европа ще бъдат стимулирани чрез подписването на договорни публично-частни партньорства (ПЧП) в областта на киберсигурността. Договорните ПЧП ще обединяват отраслови и публични ресурси като предпоставка за високи достижения в научноизследователската област и иновациите.

Целта на договорните ПЧП е изграждане на доверие между държавите членки и отрасъла чрез укрепване на сътрудничеството в началните етапи на научноизследователската дейност и иновациите. Друга цел е съгласуването на

[35] Например мрежата „Enterprise Europe Network“ и Европейската мрежа на регионите, свързани с отбраната, ще предоставят нови възможности на регионите за трансгранично сътрудничество в сферата на двойната употреба, включително в областта на киберсигурността, и на МСП, желаещи да установят контакти с други предприятия.

секторите на търсене и предлагане. Това би следвало да предостави на отрасъла възможност да съобрази своите продукти и услуги с бъдещите изисквания на крайните потребители и секторите, които се явяват важни клиенти на решения, свързани с киберсигурността (напр. енергетика, здравеопазване, транспорт и финанси). Това ще улесни тяхното участие във формулирането на общи изисквания за цифрова сигурност и защита на неприкосновеността на личния живот и личните данни за съответните сектори.

Договорните ПЧП в областта на киберсигурността също така ще оптимизират в максимална степен разходването на средства. Това ще бъде постигнато, на първо място, чрез по-добра координация с държавите членки. На второ място, ще бъде поставен по-силен акцент върху няколко технически приоритета като стимул за технологични открития и овладяване на ключови технологии на бъдещето в сферата на киберсигурността. В този контекст разработването на софтуер с отворен код и отворени стандарти може да допринесе за изграждането на доверие и за повече прозрачност, стимулирайки и създаващите нови пазари иновации, и следователно също трябва да се разглежда като част от инвестициите в това договорно ПЧП.

Работата в рамките на договорните ПЧП в областта на киберсигурността ще извлече предимства от синергиите с други европейски проекти и по-специално с такива, които са насочени към усъвършенстване на различни аспекти на сигурността. Това включва „Фабрики на бъдещето“, „Енергийноефективни сгради“, съобщителните мрежи от пето поколение (5G) и ПЧП в сферата на големите информационни масиви[36] и други секторни ПЧП[37], както и инициативата „Интернет на нещата“[38]. Ще бъде насърчавана и тясната съгласуване с Европейския облак за отворена наука и Европейската инициатива за използване на суперкомпютри от ново поколение в областта на квантовите кибернетични технологии (напр. иновации в сферата на разпространение на квантови ключове, квантови компютърни изследвания).

Договорните ПЧП в областта на киберсигурността ще се прилагат в рамките на програма „Хоризонт 2020“[39] — рамковата програма за научни изследвания и иновации на Европейския съюз за периода 2014—2020 г. Те ще разкрият нови възможности за финансиране по линия на двата стълба на програмата — Водещи позиции при базовите и промишлените технологии (LEIT-ICT) и Обществено предизвикателство — Сигурни общества (ОП7). За договорните ПЧП ще бъдат заделени до 450 милиона евро с троен лостов ефект от страна на отрасъла. Решенията, свързани с киберсигурността, следва да бъдат съгласувани с други части на програма „Хоризонт 2020“ (напр. с обществени предизвикателства в енергетиката, транспорта и здравеопазването и с частта за високи постижения по „Хоризонт 2020“). Това ще допринесе за постигането на целите на

[36] Публично-частно партньорство за инфраструктура от пето поколение и публично-частно партньорство в областта на големите масиви данни.
[37] Например Проектът за изследване на управлението на въздушното движение по линия на инициативата „Единно европейско небе“ (SESAR) или прехода към публично-частно партньорство в железопътния сектор.
[38] Алианс за иновации в сферата на инициативата „Интернет на нещата“ (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents

договорните ПЧП в областта на киберсигурността. Съгласуването би следвало да се осъществява на предварителен етап при разработването на секторните стратегии.

Договорните ПЧП ще бъдат прилагани прозрачно, а управлението им ще се основава на открити и гъвкави принципи, които са лесно приспособими към бързо изменящата се среда в сферата на киберсигурността. Тези принципи ще отчитат необходимостта от дискусии между държавите членки относно отражението на технологичните промени върху сигурното и надеждно функциониране на националните и трансграничните инфраструктури. Също така резултатите от това партньорство трябва да бъдат дълготрайни, като предпоставка за постигане на неговите цели.

Договорните ПЧП ще бъдат подкрепяни от Европейската организация за киберсигурност (ECSO), чиито членове ще отразяват многообразието на европейския пазар на решения, свързани с киберсигурността. Сред тях ще има и национални, регионални и местни публични органи, научно-изследователски центрове, представители на академичната общност и други заинтересовани страни.

Комисията:

- ще подпише с отрасъла договорно публично-частно партньорство в областта на киберсигурността, така че то да влезе в сила през третото тримесечие на 2016 г.;
- ще обяви първите търгове за договорни ПЧП в областта на киберсигурността по програма „Хоризонт 2020“ през първото тримесечие на 2017 г.; и
- ще предприеме необходимите действия за съгласуване на договорните ПЧП в областта на киберсигурността със съответните секторни стратегии, инструментите по линия на програма „Хоризонт 2020“ и секторните ПЧП.

5. ЗАКЛЮЧЕНИЕ

В настоящото Съобщение се представят мерки, които имат за цел укрепване на отбранителната способност на Европа срещу кибератаки с цел изграждане на конкурентоспособен и иновативен сектор на киберсигурността в Европа за постигане на целите, огласени в Стратегията на ЕС за киберсигурност и Стратегията за ЦЕП. Комисията приканва Европейския парламент и Съвета да подкрепят настоящия подход.