ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 12.9.2018 г.
SWD(2018) 404 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

ОБОБЩЕНА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

придружаващ

ПРЕДЛОЖЕНИЕ ЗА РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Обобщение

Оценка на въздействието относно: Предложение за създаване на мрежа от експертни центрове и Европейски експертен център за научни изследвания в областта на киберсигурността

А. Необходимост от действия

Защо? Какъв е разглежданият проблем?

Понастоящем ЕС все още не разполага с достатъчно технологичен и промишлен капацитет, за да може да подсигурява самостоятелно своята икономика и своите критични инфраструктури и да се превърне в световен лидер в областта на киберсигурността. Настоящата инициатива има за цел да допринесе за решаването на следните проблеми и свързаните с тях фактори, довели до тази ситуация:

Проблем № 1: недостатъчно равнище на стратегическата и устойчива координация, както и на сътрудничеството между промишлеността, научноизследователските общности в областта на киберсигурността и правителствата при обезпечаване на икономиката, обществото и демокрацията с водещи европейски решения в областта на киберсигурността;

Проблем № 2: недостатъчно финансиране и ограничен достъп до ноу-хау, умения и съоръжения в цяла Европа;

Проблем № 3: само една малка част от резултатите на европейските изследвания и иновации в областта на киберсигурността са се превърнали в годни за пазара решения и са получили широко разпространение в икономиката.

Тези проблеми се дължат на редица фактори, включително на недостатъчното равнище на доверие между различните участници на пазара за киберсигурност, на ограниченията, присъщи на съществуващите механизми за сътрудничество и обединяване на финансирането, на липсата на рамка за съвместни обществени поръчки за скъпа инфраструктура и скъпи продукти/решения в областта на киберсигурността, както и на неизползвания потенциал на пазарните механизми за привличане-отблъскване.

Какво се очаква да бъде постигнато с настоящата инициатива?

Инициативата има за цел да гарантира, че ЕС ще запази и развие съществените (технологични и промишлени) капацитети, за да може самостоятелно да подсигурява своите цифрова икономика, общество и демокрация, както и че държавите членки ще могат да се възползват от най-съвременните решения в областта на киберсигурността и възможности за киберотбрана. Инициативата има за цел също да повиши глобалната конкурентоспособност на предприятията на ЕС в областта на киберсигурността и да осигури достъпа на европейските предприятия от различните сектори до възможности и ресурси, така че киберсигурността да се превърне в тяхно конкурентно предимство. Това следва да бъде постигнато чрез разработване на ефективни механизми за дългосрочно стратегическо сътрудничество между всички значими участници (публичните органи, промишлеността, научноизследователската общност в цивилната и отбранителната област), обединяване на знания и ресурси с цел осигуряване на възможности и инфраструктури за новаторство, стимулиране на широкото разпростиране на европейските продукти и решения в областта на киберсигурността в икономиката и в публичния сектор, подкрепа за стартиращи предприятия и МСП в областта на киберсигурността, както и съдействие за преодоляване на недостига на умения в областта на киберсигурността.

Каква е добавената стойност от действия на равнището на ЕС?

Инициативата ще добави стойност към настоящите действия на национално равнище, като подпомогне създаването на взаимосвързана общоевропейска промишлена и научноизследователска екосистема в областта на киберсигурността. Тя следва да насърчи по-доброто сътрудничество между съответните заинтересовани страни (включително между общностите за киберсигурност в цивилния и отбранителния сектор), за да бъдат използвани по най-добрия начин съществуващите ресурси и експертен опит в областта на киберсигурността, разпръснати из цяла Европа. Тя следва да помогне на ЕС и държавите членки да възприемат активна, дългосрочна и стратегическа перспектива по отношение на промишлената политика в областта на сигурността, която не се изчерпва единствено с научноизследователска дейност и внедряване. Този подход следва да подпомогне не само намирането на принципно нови решения за свързаните с

киберсигурността предизвикателства, пред които се изправят частният и публичният сектор, но също така да подкрепи ефективното внедряване на тези решения. Освен това по този начин ще се даде възможност на съответните научноизследователски и промишлени общности, както и на публичните органи, да получат достъп до ключови капацитети като съоръжения за изпитване и експериментиране, които често са извън възможностите на отделните държави членки поради недостиг на финансови и човешки ресурси. Това ще допринесе също за преодоляването на недостига на умения и за избягването на „изтичането на мозъци", като се осигури достъп за най-добрите таланти до мащабни европейски проекти и по този начин им се предоставят интересни професионални предизвикателства. Всичко, описано по-горе, се приема също така като необходимо условие, за да може Европа да бъде призната за лидер в областта на киберсигурността в световен мащаб.

Б. Решения

Какви законодателни и незаконодателни варианти на политиката бяха разгледани? Има ли предпочитан вариант? Защо?

Бяха разгледани редица варианти на политиката, както законодателни, така и незаконодателни. Следните варианти бяха избрани за задълбочена оценка:

1. **Базов сценарий** — вариант, основан на сътрудничество: предполага продължаване на настоящия подход за изграждане на промишлен и технологичен потенциал в сферата на киберсигурността в ЕС чрез подкрепа на научните изследвания и иновациите и свързаните с тях механизми за сътрудничество в рамките на програмата „Хоризонт Европа";
2. **Вариант 1:** мрежа за компетентност в сферата на киберсигурността с Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, който е оправомощен да предприема мерки в подкрепа на промишлените технологии, както и в сферата на научните изследвания и иновациите;
3. **Вариант 2:** мрежа за компетентност в сферата на киберсигурността с Европейски експертен център за научни изследвания в областта на киберсигурността, които се ограничава до действия единствено в областта на научните изследвания и иновациите.

Сред вариантите, отхвърлени на ранен етап, бяха 1) Без предприемане на действия; 2) Мрежа на базата само на съществуващите експертни центрове, и 3) Използване на вече съществуваща агенция (ENISA, REA или INEA).

С оглед на вече поетото от Комисията общото задължение по отношение на настоящата инициатива, както и с оглед на важната роля, която ще изпълняват държавите членки, основната разлика между двата варианта на политиката, анализирани в подробности, е в тяхното приложно поле, както е посочено в тяхното правно основание: образувание, основаващо се единствено на член 187 от Договора за функционирането на ЕС (вариант 2), би ограничило инициатива в областта на научните изследвания и иновациите и обичайно би предположило финансово участие от страна на частния сектор. От друга страна, образувание, което се основава едновременно на член 187 и член 173 от ДФЕС (вариант 1), би имало по-широк мандат, който ще обхваща наред с другото внедряването, промишлената подкрепа и създаването на по-силни полезни взаимодействия с областта на киберотбраната. Този вариант ще предостави също така по-важна роля на държавите членки — както като участници в процеса на управление, така и като потенциални възложители на обществени поръчки в областта на технологиите за киберсигурност.

Анализът посочва, че вариант 1 е най-подходящ за постигане на целите на инициативата и предлага същевременно най-голямото икономическо, социално и екологично въздействие и най-добрата защита на интересите на Съюза. Сред основните аргументи в полза на този вариант са гъвкавостта, позволяваща различни модели на сътрудничество с общността и мрежата от експертни центрове, насочени към оптимизиране на използването на съществуващите знания и ресурси; възможността за структуриране на сътрудничеството на заинтересованите страни от публичния и частния сектор, произхождащи от всички съответни сектори, включително сектора на отбраната; възможността за създаване на истинска промишлена политика в областта на киберсигурността чрез подкрепа на дейности, свързани не само с научноизследователска и развойна дейност, но и с навлизането на пазара. Не на последно място, вариант 1 позволява също да се повиши съгласуваността, тъй като действа като механизъм за прилагане на свързаното с киберсигурността финансиране по програмите „Цифрова Европа" и „Хоризонт Европа" и

увеличава полезното взаимодействие между цивилните и отбранителните аспекти на киберсигурността във връзка с Европейския фонд за отбрана.

Кой подкрепя отделните варианти?

Резултатите от процесите на консултация и събиране на факти показват, че има ясна необходимост както за промишлените, така и за научните общности, от механизъм, който дава възможност за съгласувана промишлена политика на ЕС в областта на киберсигурността, която да обхваща не само изследователски и развойни дейности, ако Европа иска да се превърне в световен лидер в областта на киберсигурността. В същото време заинтересованите страни подчертаха, че ключът към успеха ще бъде определянето на ясна роля за Центъра по отношение на подкрепата и подпомагането на усилията на Мрежата и съответните общности, както и на приобщаващ, основаващ се на сътрудничество подход към мрежата, с цел да се избегне възникването на нови разделения. Структурата следва също да бъде гъвкава, така че да може лесно да се адаптира, като се има предвид, че киберсигурността представлява бързоразвиваща се среда. В хода на този процес държавите членки изтъкнаха необходимостта да бъдат приобщени всички държави членки и техните съществуващи центрове за високи постижения и експертни центрове, както и да се обърне специално внимание на взаимното допълване на действията. Конкретно във връзка с Центъра държавите членки подчертаха значението на неговата координираща роля в подкрепа на мрежата. Поради това за всяка инициатива на Комисията ще трябва да бъде намерен и съответно отразен в управленските и изпълнителните структури подходящият баланс, за да бъде осигурена ефективна координация на европейско равнище и същевременно да бъде взето предвид развитието на национално равнище.

В. Въздействие на предпочетения вариант

Какви са ползите от предпочетения вариант (ако има такъв; в противен случай — от основните варианти)?

Предпочетеният вариант ще позволи на публичните органи и промишлеността във всички държави членки да предотвратяват и реагират на киберзаплахи по-ефективно, като предлагат и се оборудват с по-сигурни продукти и решения. Това е от значение по-специално за защитата на достъпа до основни услуги (например транспорт, здравеопазване, банкови и финансови услуги). Освен това този вариант ще има положително въздействие върху конкурентоспособността на ЕС и върху МСП, тъй като предполага създаването на механизъм, способен да изгради промишления капацитет на държавите членки и Съюза в областта на киберсигурността и да превърне европейските високи научни постижения в годни за пазара решения, които биха могли да бъдат внедрени във всички сектори на икономиката. Този вариант дава възможност за обединяване на ресурси, с цел да се инвестира в изграждането на необходимите капацитети на равнището на държавите членки и за разработване на общи европейски активи, при което да се реализират икономии от мащаба. Това вероятно ще доведе до увеличаване на достъпността на подобни съоръжения за МСП, промишлените сектори и изследователите, което ще стимулира иновациите и ще съкрати процесите на разработване. По този начин ще се намалят също така разходите на някои предприятия от страната на потреблението и ще им се помогне да превърнат киберсигурността в свое конкурентно предимство. Вариантът позволява да се използват пазарните възможности за продукти с двойна употреба, като дава възможност на отбранителни и цивилни общности да работят заедно по общите предизвикателства. Очаква се също така той да добави стойност към усилията на национално равнище във връзка със справянето с недостига на умения в областта на киберсигурността. На равнище ЕС този вариант позволява също да се подобрят съгласуваността и полезните взаимодействия между различните механизми за финансиране.

Косвено положително въздействие върху околната среда може да се постигне чрез разработването на специални решения за киберсигурност за сектори с потенциално голямо въздействие върху околната среда (например ядрени електроцентрали), което ще помогне да се избегнат потенциалните опустошителни последици от кибератаки срещу този вид инфраструктура.

Какви са разходите за предпочетения вариант (ако има такъв, в противен случай — за основните варианти)?

Разходите във връзка с предпочетения вариант, са свързани главно с разходите за работата на Центъра и на националните координационни центрове. Разходите, свързани с прилагането на различните програми за финансиране (програмата „Цифрова Европа“ и програмата „Хоризонт Европа“), са предмет на отделни

оценки на въздействието.

Какви ще са последиците за предприятията, МСП и микропредприятията?

Европейските предприятия, работещи в областта на киберсигурността, както от страната на търсенето, така и от страната на предлагането, включително МСП и микропредприятия, ще бъдат сред най-силно засегнатите групи от заинтересовани страни. Въпреки че със създаването на Експертния център и Мрежата за тях не възникват регулаторни задължения, то ще разкрие възможности по отношение на намаляването на разходите за проектиране на нови продукти и ще им помогне да получат по-лесен достъп до общността на инвеститорите и да привлекат необходимото финансиране за разгръщането на подходящи за пазара решения. Още по-важен за МСП и микропредприятията се явява достъпът до публично финансирани изследвания и експериментални съоръжения поради факта, че те не разполагат с ресурси за закупуване или пътуване извън границите на своя пазар (а често дори извън ЕС), за да намерят необходимата инфраструктура. Очаква се също така тази инициатива да разкрие нови пазари за европейските МСП и микропредприятия, работещи в областта на киберсигурността. Освен това избраният механизъм ще осигури координация между научните изследвания и промишлеността, като по този начин ще насочи научните изследвания към конкретни нужди на промишлеността. Предоставянето на авангарден експертен опит и инструменти в областта на киберсигурността косвено ще съдейства на стопанските субекти при изпълнението на Директивата за МИС.

Ще има ли значително въздействие върху националните бюджети и администрации?

Инициативата ще даде възможност на държавите членки да координират инвестициите в необходимата инфраструктура в областта на киберсигурността на национално и европейско равнище. Механизмът ще позволи също да се обединяват ресурсите за инструменти и инфраструктури, който иначе биха стрували по-скъпо или не биха били финансово достъпни за отделните държави членки. Този подход ще даде възможност за икономии от мащаба и рационализиране. Финансовото участие на държавите членки във финансирането на Експертния център и съответните действия следва да бъде съобразено с финансовото участие на Съюза.

Ще има ли други значителни въздействия?

Да, инициативата има ясно изразено положително въздействие, тъй като е вероятно тя да увеличи значително капацитета на държавите членки да гарантират самостоятелно сигурността на своите икономики, включително да защитават критични сектори, да повишават конкурентоспособността на европейските предприятия в областта на киберсигурността, както и на предприятия от различни сектори, които ще бъдат в състояние да подсигурят по подходящ начин своите съществуващи активи и да проектират сигурни иновативни продукти, като същевременно намалят свързаните със сигурността разходи за научноизследователска и развойна дейност. В крайна сметка това следва да даде възможност на ЕС да се превърне в лидер при технологиите от следващо поколение в областта на цифровите системи и киберсигурността.

Г. Последващи действия

Кога ще се извърши преглед на политиката?

В правния инструмент ще бъдат включени изрична клауза за мониторинг на ключовите показатели за ефективност (КПЕ), както и клауза за оценка и преглед, чрез които Европейската комисия ще извърши междинна оценка, за да установи въздействието на инструмента и неговата добавена стойност. Впоследствие Европейската комисия ще докладва на Европейския парламент и на Съвета. Въз основа на тази оценка Комисията може да предложи преразглеждане и разширяване на мандата на Експертния център и на Мрежата.