Становище на Европейския икономически и социален комитет относно „Предложение за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 и Предложение за директива на Европейския парламент и на Съвета относно издръжливост на критичните субекти“

[COM(2020) 823 final — 2020/0359 (COD) — COM(2020) 829 final — 2020/0365 (COD)]

(2021/C 286/28)

Докладчик: **Maurizio MENSI**

Консултация	Европейски парламент, 21.1.2021 г. — 11.2.2021 г.
	Съвет: 26.1.2021 г. и 19.2.2021 г.
Правно основание	Член 114 от Договора за функционирането на Европейския съюз
Компетентна секция	„Транспорт, енергетика, инфраструктури, информационно общество“
Приемане от секцията	14.4.2021 г.
Приемане на пленарна сесия	27.4.2021 г.
Пленарна сесия №	560
Резултат от гласуването	
(„за“/„против“/„въздържал се“)	243/0/5

1. **Заключения и препоръки**

1.1. ЕИСК оценява положените от Комисията усилия за повишаване на устойчивостта на публичните и частните субекти срещу заплахите, произтичащи от кибер- и физически атаки и инциденти и споделя необходимостта от укрепване на промишлеността и иновационния капацитет на ЕС по приобщаващ начин, в съответствие със стратегия, основана на четири стълба: защита на данните, основни права, безопасност и киберсигурност.

1.2. ЕИСК отбелязва обаче, че предвид целесъобразността и чувствителността на целите, преследвани от двете предложения, регламентът като инструмент би бил за предпочитане пред директивата. Не личат ясно, обаче, основанията, поради които Комисията е решила да не включи тази възможност в различните разглеждани варианти.

1.3. ЕИСК отбелязва, че някои разпоредби в двете предложения за директива се припокриват, тъй като са тясно свързани и се допълват, като в едното се разглеждат предимно аспекти на киберсигурността, а в другото — на физическата сигурност. Ето защо призовава да се прецени възможността двете предложения да бъдат обединени в един единствен текст, за да се постигне опростяване и функционална концентрация.

1.4. Комитетът приветства предложения подход за преодоляване на разграничението между оператори на основни услуги и доставчици на цифрови услуги, предвидено в първоначалния вариант на Директивата за МИС, но подчертава предоставените възможности по отношение на приложното ѝ поле за по-прецизни и ясни индикации за определяне на субектите, които са длъжни да спазват директивата. По-специално, би трябвало да бъдат определени по-точно разграничителните критерии между „съществени“ и „значими“ субекти, както и изискванията, които трябва да бъдат изпълнени, за да се избегне това, различните подходи на национално равнище да доведат до пречки пред конкуренцията и свободното движение на стоки и услуги, с риск да се навреди на предприятията и да се засегне търговския обмен.

1.5. ЕИСК счита, че поради обективната сложност на системата, предвидена в двете предложения, е важно Комисията да изясни точно обхвата на двата законодателни пакета, особено когато различни разпоредби допринасят за уреждане на един и същ случай или въпрос.

1.6. Комитетът подчертава, че яснотата на всяка законодателна разпоредба е неотменима цел, заедно с целите за намаляване на бюрокрацията и фрагментираността, като се опростяват процесите, изискванията за сигурност и задълженията за уведомяване за инциденти. И за тази цел може да стане подходящо, в полза на гражданите и предприятията, двете предложения за директива да бъдат обединени в един единствен текст, като се избегне понякога сложното тълкуване и прилагане.

1.7. ЕИСК признава основната роля, подчертана в предложението за директива, на управителните органи на „съществените“ „и „значимите“ субекти, чиито членове трябва редовно да преминават специални курсове за обучение, за да придобият знания и умения, достатъчни за познаване, управление на различните киберрискове и оценяване на тяхното въздействие. В това отношение се счита, че в предложението трябва да се посочи минималното съдържание на такива знания и умения,за да се предоставят насоки на европейско равнище относно това кои умения за обучение се считат за подходящи и да се избегне съдържанието на различните курсове за обучение да бъде различно в отделните държави.

1.8. ЕИСК изразява съгласие с възложената важна роля на ENISA в цялостната институционална и оперативна структура на киберсигурността на европейско равнище. Във връзка с това счита, че в допълнение към доклада за състоянието на киберсигурността в Съюза, който се изготвя на всеки две години, този орган трябва да публикува в интернет редовна и актуализирана информация за инцидентите, свързани с киберсигурността, в допълнение към предупрежденията за отделните сектори, за да предостави допълнителен полезен информационен инструмент, който да даде възможност на заинтересованите страни, засегнати от Директивата за МИС 2 да защитават по-добре своите предприятия.

1.9. ЕИСК приветства предложението задачата за създаване на европейски регистър на уязвимостите да бъде възложена на ENISA и счита, че докладването относно уязвимостта и по-сериозните инциденти трябва да стане задължително, а не доброволно, така че да се превърне в полезен инструмент и за възложителите в рамките на различните процедури по възлагане на обществени поръчки на европейско равнище, включително за продуктите и технологиите за 5G.

2. **Общи бележки**

2.1. На 16 декември 2020 г. беше представена новата стратегия на ЕС за киберсигурността заедно с две законодателни предложения: преразглеждане на Директива (ЕС) 2016/1148 ([1]) относно киберсигурността на мрежите и информационните системи (МИС 2) и нова директива относно устойчивостта на критичните субекти (УКС). Стратегията, ключов елемент на съобщението „Изграждане на цифровото бъдеще на Европа“ ([2]), на Плана за възстановяване на Европа и на Стратегията на ЕС за Съюза на сигурност, е насочена към укрепване на колективната устойчивост на Европа срещу киберзаплахите и гарантиране, че всички граждани и предприятия могат да се възползват от надеждни и сигурни цифрови услуги и инструменти.

2.2. Съществуващите мерки на равнището на ЕС, насочени към защита на услугите и критичните инфраструктури от кибер- и физически рискове, трябва да бъдат актуализирани. С нарастване на цифровизацията и взаимосвързаността продължават да се променят рисковете, свързани с компютърната сигурност. Ето защо е необходимо действащата регулаторна рамка да бъде преразгледана съгласно логиката на стратегията на ЕС за сигурността, като се преодолее разделението между онлайн и офлайн и подхода, основан на строго разграничаване.

2.3. Двете предложения за директива засягат широк кръг от сектори и разглеждат настоящи и бъдещи онлайн и офлайн рискове, произтичащи от престъпни кибератаки, природни бедствия и други инциденти и като се извлича поука от текущата пандемия, която показа, че общества и икономики, зависещи все повече от цифрови решения, са уязвими и изложени на растящи и бързо променящи се киберзаплахи, особено за групите, изложени на риск от социално изключване, като например хората с увреждания. Това накара ЕС да предложи действия за опазване на глобално и отворено, но основано на солидни гаранции за сигурност киберпространство, технологичен суверенитет и лидерство, като се изгради оперативен капацитет, който чрез повишено сътрудничество може да предотвратява, възпира и реагира на евентуалните заплахи, при зачитане на прерогативите на държавите членки в областта на националната сигурност.

3. **Предложение за преразглеждане на Директивата за мрежова и информационна сигурност**

3.1. С Директива (ЕС) 2016/1148, пръв „хоризонтален“ законодателен инструмент на ЕС в областта за киберсигурността, се целеше подобряване на устойчивостта на мрежовите и информационните системи в Съюза срещу кибернетичните рискове. Въпреки постигнатите добри резултати, Директивата за МИС все пак показа някои ограничения, когато цифровата трансформация на обществото, ускорена от кризата с COVID-19, разшири спектъра на заплахите, като повиши уязвимостта на нашите общества, които стават все по-взаимозависими при значителни и непредвидими рискове. Възникнаха нови

([1]) ОВ L 194, 19.7.2016 г., стр. 1.
([2]) COM(2020) 67 final.

предизвикателства, изискващи адекватни и новаторски реакции. Резултатите от широката консултация, проведена със заинтересованите страни, разкриха недостатъчното равнище на киберсигурността на европейските предприятия, несъгласуваното прилагане на правилата от страна на държавите в различните сектори и липсата на разбиране на основните заплахи и предизвикателства.

3.2. Предложението за Директива за МИС 2 е тясно свързано с други две инициативи: предложението за регламент относно сектора на финансовите услуги, в който се използват цифровите технологии (акт относно оперативна устойчивост при цифровите технологии, DORA), и предложението за Директива относно устойчивостта на критичните субекти(УКС), което разширява за нови сектори приложното поле на Директива 2008/114/ЕО ([3]) относно енергетиката и транспорта, като се съсредоточава например върху здравния сектор и субектите, които извършват научноизследователска дейност и разработване на лекарствени продукти. Директивата относно устойчивостта на критичните субекти, чието секторно приложно поле е идентично с това на Директивата за МИС 2 за съществените субекти (приложение 1 към Директивата за МИС 2), премества фокуса си от защитата на материалните активи към устойчивостта на субектите, които ги управляват и преминава от определянето на европейските критични инфраструктури с трансгранично измерение към определяне на критичните инфраструктури на национално равнище. Директивата за МИС 2 също е съгласувана със и допълва други действащи регулаторни инструменти като Европейския кодекс за електронни съобщения, Общия регламент относно защитата на данните и Регламента относно електронната идентификация и удостоверителните услуги.

3.3. С предложението за директива за МИС 2 в съответствие с Програмата за пригодност и резултатност на регулаторната рамка (REFIT) се цели да се намалят регулаторните тежести за компетентните органи и разходите на публичните и частните субекти за привеждане в съответствие и да се осъвремени референтната правна рамка. Освен това с него се засилват наложените на предприятията изисквания за сигурност, разглежда се въпросът за сигурността на веригите за доставки, оптимизират се задълженията за докладване, въвеждат се по-строги мерки за надзор за националните органи и се проявява стремеж за хармонизиране на режимите за санкции в държавите членки.

3.4. Директивата за МИС 2 допринася също така за засилване на обмена на информация и сътрудничеството в областта на управлението на кибернетичните кризи на национално и европейско равнище. Преодолява се разграничението между оператори на съществени услуги и доставчици на цифрови услуги, предвидено в Директивата за МИС. Приложното ѝ поле включва средно големи предприятия от сектори, определяни въз основа на тяхната важност за икономиката и обществото. Тези субекти, публични или частни, се подразделят на „съществени“ и „значими“ и подлежат на различни режими на надзор. На държавите членки все пак се предоставя възможността да разглеждат и по-малки субекти с високорискови профили.

3.5. Предвидена е нова мрежа от оперативни центрове за сигурност на равнището на ЕС, управлявани от изкуствен интелект (ИИ), които ще представляват същински „щит за киберсигурност“, способен да открива сигналите за кибератака достатъчно време предварително, за да може да се реагира преди да бъдат нанесени вреди. Значението на изкуствения интелект за киберсигурността е подчертано и в доклада относно изкуствения интелект (ИИ) на Комисията за национална сигурност на САЩ (NSCAI), представен на 1 март 2021 г. В резултат на това държавите членки и операторите на критичните инфраструктури ще могат да имат пряк достъп до информацията относно заплахите в рамките на европейска мрежа за сигурност от гледна точка на разузнаването във връзка с евентуални заплахи.

3.6. Комисията разглежда и проблемът със сигурността на веригите за доставки и на отношенията с доставчиците: държавите членки, в сътрудничество с Комисията и ENISA, могат да извършват координирани оценки на рисковете на критичните вериги за доставки въз основа на успешно приетия подход за 5G мрежите, предвиден в препоръката от 26 март 2019 г. ([4]).

3.7. С предложението се укрепват и оптимизират задълженията за предприятията, свързани със сигурността и докладването, като се налага общ подход за управление на рисковете с минимален списък за прилагане на основни елементи за сигурност. Предвидени са по-точни разпоредби относно процеса на уведомяване за инцидентите, относно съдържанието на докладите и сроковете. В това отношение предложението предвижда двуетапен подход: предприятията имат на разположение 24 часа да представят кратък първоначален доклад, последван от подробен окончателен доклад в рамките на един месец.

([3]) ОВ L 345, 23.12.2008 г., стр. 75.
([4]) ОВ L 88, 29.3.2019, стр. 42.

3.8. Предлага се държавите членки да определят националните органи, отговарящи за управлението на кризи, с конкретни планове и нова мрежа за оперативно сътрудничество — Европейска мрежа за връзка на организациите при кибернетични кризи („EU — CyCLONe“). Засилена е ролята на групата за сътрудничество при определянето на стратегическите решения и е създаден регистър за откритите в ЕС уязвимости, управляван от ENISA; освен това са подобрени обменът на информация и сътрудничеството, включително оперативното, между органите на държавите членки по отношение на управлението на киберкризите.

3.9. Въведени са по-строги мерки за надзор за националните органи, по-стриктни изисквания за прилагане и се цели хармонизиране на режимите за санкции във всички държави членки.

3.10. Във връзка със санкциите предложението за директива изготвя списък с административни санкции в случай на нарушаване на задълженията за управление на рисковете, свързани с компютърната сигурност и комуникацията. Предвидени са разпоредби относно отговорността на физическите лица на представителни или ръководни длъжности в дружествата, които попадат в приложното поле на директивата. В това отношение с предложението се подобрява начинът, по който ЕС предотвратява, управлява и реагира на инциденти и на широкомащабни кризи на компютърната сигурност, като се предвиждат ясни отговорности, подходящо планиране и повишено сътрудничество на равнището на ЕС.

3.11. Държавите членки са в състояние да следят съвместно за прилагането на стандартите на ЕС и да си помагат взаимно в случай на трансгранични проблеми, да установяват по-структуриран диалог с частния сектор, да координират оповестяването на уязвимости, открити в софтуера и хардуера, продавани на вътрешния пазар и да оценяват по координиран начин рисковете за сигурността и заплахите, свързани с новите технологии, както в случая с 5G.

4. **Предложението за директива относно устойчивостта на критичните субекти**

4.1. През 2006 г. ЕС създаде Европейската програма за защита на критичната инфраструктура (EPCIP), а през 2008 г. прие Директивата за европейските критични инфраструктури (ЕКИ), която се прилага за секторите на енергетиката и транспорта. Както в приетата от Комисията Стратегия на ЕС за Съюза на сигурност за периода 2020—2025 г. ([5]), така и в наскоро приетата Програма за борба с тероризма се подчертава, че е важно да се гарантира устойчивостта на критичните инфраструктури на физически и цифрови рискове. Все пак както извършената през 2019 г. оценка относно прилагането на Директивата за ЕКИ, така и резултатите от оценката на въздействието на разглежданото предложение показаха, че действащите европейски и национални мерки не гарантират в достатъчна степен, че операторите са в състояние да се справят с настоящите рискове. Ето защо Съветът и Парламентът отправиха призиви към Комисията да преразгледа настоящия подход за защита на критичните инфраструктури.

4.2. В Стратегията на ЕС за Съюза на сигурност, приета от Комисията на 24 юли 2020 г., беше призната растящата взаимосвързаност и взаимозависимост между физическите и цифровите инфраструктури, подчертавайки необходимостта от по-съгласуван и последователен подход между Директивата за ЕКИ и Директивата за МИС. В този смисъл предложението за директива (УКС), чиято обективна референтна рамка е същата като на Директивата за МИС 2 относно съществените субекти, разширява първоначалното приложно поле на Директива 2008/114/ЕО, ограничено до енергетиката и транспорта, за да включи изброените сектори: банково дело, инфраструктури на финансовите пазари, здравеопазване, питейна вода, отпадъчни води, цифрови инфраструктури, публична администрация и космическо пространство, като предвижда и ясни отговорности, подходящо планиране и повишено сътрудничество. Във връзка с това е необходимо да се създаде референтна рамка за всички рискове и да се подкрепят държавите членки в усилията да се гарантира, че критичните субекти са в състояние да предотвратяват, да устояват и да поемат последиците от инцидентите, независимо от факта, че рисковете произтичат от природни опасности, инциденти, тероризъм, вътрешни заплахи или извънредни ситуации, свързани с общественото здраве, като настоящата.

4.3. Всяка държава членка е длъжна да приеме национална стратегия за гарантиране на устойчивостта на критичните субекти, да извършва редовни оценки на риска и на тази основа да идентифицира критичните субекти. От своя страна критичните субекти са длъжни да извършват оценки на риска, да приемат подходящи технически и оперативни мерки за повишаване на устойчивостта и да уведомяват националните органи за инцидентите. Субектите, които предоставят услуги на най-малко една трета от държавите членки или най-малко в една трета от тях, подлежат на специален надзор, който включва специални мисии за подпомагането им, организирани от Комисията.

4.4. В предложението за директива (УКС) се предвиждат различни форми на подкрепа в полза на държавите членки и критичните субекти, преглед на рисковете на равнището на ЕС, най-добрите практики и методи, освен образователна дейност и учения за изпитване на устойчивостта на критичните субекти. Системата за трансгранично сътрудничество предвижда също така *ad hoc* експертна група, Групата за устойчивост на критичните субекти, форуми за стратегическото сътрудничество и обмена на информация между държавите членки.

([5]) COM(2020) 605 final.

5. **Предложения за промени в съответното законодателно предложение.**

5.1. ЕИСК оценява положените от Комисията усилия за повишаване на устойчивостта на публичните и частните субекти срещу заплахите, произтичащи от кибер- и физически атаки. Това придобива особено значение и важност с оглед на бързата цифрова трансформация, предизвикана от извънредната ситуация във връзка с COVID-19. Изразява съгласие и с това, че е необходимо, както е посочено в съобщението „Изграждане на цифровото бъдеще на Европа“, Европа да се възползва от предимствата на цифровата ера и да укрепи своята промишленост, особено по отношение на малките и средните предприятия, а така също и иновационния си капацитет по приобщаващ начин в съответствие със стратегия, основана на четири стълба: защита на данните, основни права, безопасност и киберсигурност като съществени предпоставки за изграждане на общество, което се основава на силата на данните.

5.2. Все пак, в светлината на резултатите от оценката на въздействието и на консултацията, която предшестваше предложението за МИС 2, с оглед на многократно подчертаната цел да се избегне фрагментираността на приетите на национално равнище правила, както е предвидено и в съобщението от 4 октомври 2017 г. относно прилагането на директивата за МИС ([6]), ЕИСК подчертава, че не стават ясни основанията, поради които Комисията не е счела за необходимо да предложи приемането на регламент вместо директива дори сред разгледаните варианти.

5.3. ЕИСК отбелязва, че някои разпоредби в двете предложения за директива се припокриват, тъй като са тясно свързани и се допълват, като в едното се разглеждат предимно аспекти на киберсигурността, а в другото — на физическата сигурност. Отбелязва се също, че критичните субекти, посочени в Директивата относно устойчивостта на критичните субекти (УКС), обхващат едни и същи сектори и съвпадат със „съществените“ субекти, посочени в Директивата за МИС 2 ([7]). Освен това всички критични субекти, обхванати от Директивата относно УКС, подлежат на задължения в областта на киберсигурността по директивата за МИС 2. Освен това в двете предложения се предвиждат редица „мостови“ клаузи за гарантиране на свързването: разпоредби за засилено сътрудничество между органите, обмен на информация относно дейностите по надзор, уведомяване на органите, отговарящи за Директивата за МИС 2 относно определянето на критичните субекти по смисъла на Директивата относно УКС, както и редовни заседания на съответните групи за сътрудничество най-малко веднъж годишно. Двете предложения имат едно и също правно основание, член 114 от ДФЕС, чиято цел е функционирането на единния пазар чрез сближаване на националните разпоредби, както е тълкуван ex multis от Съда на ЕС в решението му по дело C-58/08, Vodafone и други. Ето защо се призовава за разглеждане на възможността двете предложения да бъдат обединени в един единствен текст с цел опростяване и функционална концентрация.

5.4. Комитетът приветства подхода за преодоляване на разграничението между оператори на основни услуги и доставчици на цифрови услуги, предвидено в първоначалния вариант на Директивата за МИС, но подчертава предоставените възможности по отношение на приложното ѝ поле за по-прецизни и ясни индикации за определяне на субектите, които са длъжни да спазват директивата. Всъщност, освен позоваванията, които се съдържат в приложения I и II, Директивата за МИС 2 изисква редица различаващи се помежду си критерии, включващи деликатни качествени и количествени оценки, които могат да се прилагат диференцирано на национално равнище с риск да се повтори ситуацията на фрагментираност, която трябваше да се избегне с разглежданото законодателно действие. В действителност изглежда важно да се избегне това, подходите, различаващи се на национално равнище да се превърнат в пречки за конкуренцията и свободното движение на стоки и услуги, с риск да се причинят вреди на предприятията и да се възпрепятства търговският обмен.

5.5. В Директивата за МИС 2 се предвижда критичните оператори в секторите, считани в разглежданото предложение за „съществени“, да бъдат и обект на общи задължения за укрепване на устойчивостта с особено внимание към заплахите, различни от киберзаплахите по смисъла на Директивата относно УКС. В последната обаче изрично се посочва, че същата не се прилага за въпросите, разглеждани в Директивата за МИС 2. Всъщност в Директивата относно УКС се предвижда, че тъй като компютърната сигурност е разгледана в достатъчна степен в Директивата за МИС, уредените от нея въпроси следва да бъдат изключени от приложното ѝ поле, без да се засяга специалният режим за субектите от сектора на цифровите инфраструктури. След това в Директивата относно УКС се подчертава, че субектите, принадлежащи към сектора на цифровите инфраструктури, се основават главно на мрежови и информационни системи и попадат в приложното поле на Директивата за МИС 2, в която се разглежда и физическата сигурност на тези системи като част от техните задължения за управление на риска, свързан с киберсигурността и уведомяването. В същото време в Директивата относно УКС се посочва, че не е изключено към тях да могат да се прилагат специални нейни разпоредби.

5.6. Ето защо в този сложен контекст ЕИСК счита, че е наложително Комисията да изясни точно обхвата на двата законодателни пакета, особено когато разпоредбите допринасят за уреждане на един и същ случай или въпрос.

5.7. Яснотата на всяка законодателна разпоредба, още повече когато е включена в обширни и подробни текстове като разглежданите, трябва да бъде на всяко равнище неотменима цел, заедно с целите за намаляване на бюрокрацията и фрагментираността, като се опростяват процесите, изискванията за сигурност и задълженията за уведомяване за инциденти.

([6]) COM(2017) 476 final.
([7]) Приложение 1 (ОВ L 194, 19.7.2016 г., стр. 1).

Необходимо е също така да се избегне увеличаването на органите, отговарящи за конкретни задачи, да възпрепятства ясното определяне на техните правомощия, като осуети постигането на преследваните цели. По тази причина може да стане подходящо, в полза на гражданите и предприятията, двете предложения за директива да бъдат обединени в един единствен текст, като се избегне понякога сложното тълкуване и прилагане.

5.8. На определени места в Директивата за МИС 2 се споменават разпоредби за други правни инструменти, както в случая с Директива (ЕС) 2018/1972 ([8]) за установяване на Европейски кодекс за електронни съобщения, чието приложение се регулира от критерия за специфичния характер. Някои разпоредби на тази директива са изрично отменени (член 40 и член 41), докато други трябва да се прилагат подобно на гореспоменатия принцип без да се предоставят разяснения по този въпрос. Във връзка с това ЕИСК изразява желание всяко съмнение да бъде разсеяно, за да се избегнат проблеми с тълкуването. По отношение на системата от санкции ЕИСК подкрепя и целта на Комисията за хармонизиране на техния режим в случай на неспазване при управлението на риска, в контекста на по-добър обмен на информация и сътрудничество на равнището на ЕС.

5.9. ЕИСК признава основната роля, подчертана в предложението за директива, на управителните органи на „съществените“ и „значимите“ субекти в стратегията за киберсигурност и в управлението на риска, тъй като от тях се изисква да одобряват мерки за управление на риска, да наблюдават тяхното изпълнение и да реагират на всяко несъответствие. Във връзка с това се предвижда членовете на тези органи редовно да преминават специални курсове за обучение, за да придобият достатъчно знания и умения, да познават, управляват различните киберрискове и оценяват тяхното въздействие. При това се счита, че в предложението трябва да се посочи съдържанието на такива знания и умения, така че да се предоставят насоки на европейско равнище относно това кои умения за обучение се считат за подходящи, за да отговорят на посочените в предложението изисквания и да се избегне изискванията и съдържанието на различните курсове за обучение да бъде различно в отделните държави.

5.10. ЕИСК изразява съгласие с възложената важна роля на ENISA в цялостната институционална и оперативна структура на киберсигурността на европейско равнище. Във връзка с това тя счита, че в допълнение към доклада за състоянието на киберсигурността в Съюза, този орган би трябвало да публикува в интернет актуализирана информация за инцидентите, свързани с киберсигурността, както и предупреждения за отделните сектори. Това би било полезен начин за предоставяне на информация, за да се даде възможност на заинтересованите страни, засегнати от МИС 2, да защитят по-добре своите предприятия.

5.11. ЕИСК изразява съгласие, че достъпът до вярна и своевременна информация относно уязвимостите, отнасящи се за информационните и телекомуникационните продукти и услуги, допринася за подобрено управление на риска, свързан с киберсигурността. В това отношение източниците на публично достъпна информация относно уязвимостите представляват важен инструмент за националните компетентни органи, ЕРИКС, предприятията и потребителите. Поради тази причина ЕИСК одобрява предложението да се възложи на ENISA задачата за създаване на европейски регистър на уязвимостите, където съществените и значимите субекти и техните доставчици могат да предоставят информацията, така че да се позволи на останалите потребители да предприемат подходящите ограничаващи мерки. Освен това счита, че това докладване, що се отнася до най-големите уязвимости и инциденти, трябва да стане задължително, а не доброволно, така че да се превърне в полезен инструмент и за възложителите в рамките на различните процедури по възлагане на обществени поръчки на европейско равнище, включително за продуктите и технологиите за 5G. В този случай подобен регистър би съдържал елементи, които да могат да се използват при оценка на офертите, за целите на проверката на тяхното качество и надеждността на европейските и неевропейските договарящи се страни по отношение на сигурността на продуктите и услугите, които са предмет на търга, в съответствие с посоченото в препоръката относно киберсигурността на 5G мрежите от 26 март 2019 г. Регистърът следва също да гарантира, че съдържащата се в него информация се предоставя така, че да се избегне всякаква дискриминация.

Брюксел, 27 април 2021 г.

Председател
на Европейския икономически и социален комитет
Christa SCHWENG

([8]) ОВ L 321, 17.12.2018 г., стр. 36.