Становище на Европейския икономически и социален комитет относно съвместното съобщение до Европейския парламент и до Съвета: Предложение за политика на ЕС за киберотбрана

(становище по собствена инициатива)

(2023/C 293/04)

Докладчик: **Anastasis YIAPANIS**

Съдокладчик: **Alberto MAZZOLA**

Решение на пленарната асамблея	20.9.2022 г.
Правно основание	Член 52, параграф 2 от Правилника за дейността
	Становище по собствена инициатива
Компетентна секция	Консултативна комисия по индустриални промени (CCMI)
Приемане от секцията	27.3.2023 г.
Приемане на пленарна сесия	14.6.2023 г.
Приемане на пленарна сесия №	579
Резултат от гласуването	
(„за“/„против“/„въздържал се“)	208/1/2

1. **Заключения и препоръки**

1.1. Европейският икономически и социален комитет (ЕИСК) подкрепя предложената политика на ЕС за киберотбрана, но би очаквал на организираното гражданско общество да бъде отредена по-важна роля в разработването на тези предложения. Комитетът смята, че на този етап е трудно да се прецени дали бъдещите инициативи, очертани в съвместното съобщение, ще бъдат приложени и ще постигнат желаните резултати. Той настойчиво приканва институциите на ЕС и държавите членки да дадат приоритет на обявените инициативи и бързо да постигнат напредък по тях.

1.2. ЕИСК подчертава необходимостта от допълнителни мерки за повишаване на способността на ЕС за откриване на киберзаплахи и призовава финансирането за НИРД да бъде насочено към развитието на авангардни способности на ЕС. Сътрудничеството между частния и публичния сектор е от съществено значение и не трябва да бъде еднопосочно. ЕИСК счита, че е необходима координация на равнище ЕС, за да се преодолее фрагментацията и да се гарантират сътрудничество и съвместни инвестиции между държавите членки.

1.3. ЕИСК подкрепя създаването на Координационен център на ЕС за киберотбрана и препоръчва държавите членки да се ангажират постоянно (24 часа/7 дни в седмицата) с бързо реагиране, да оценяват киберготовността и ефективността на механизмите на ЕС за реагиране при киберкризи, с акцент както върху военните способности, така и върху критичните сектори, определени в Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([1]) (Директива МИС 2). Комитетът подкрепя разширяването на мандата на Европейския център за експертни познания в областта на киберсигурността (ECCC), за да подпомага работата на Координационния център на ЕС за киберотбрана.

1.4. За да се засилят стратегическите автономност и суверенитет на Съюза в областта на киберсигурността, ЕИСК счита, че частният сектор следва да разработи или въведе динамична платформа за изпитване и обмен на информация в реално време, за да се установят настоящите пропуски в съществуващите способности. Тя може да се използва и за споделяне на най-добри практики, докладване на киберинциденти и за създаване на списък на ЕС на всички киберпрестъпници.

([1]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

1.5. ЕИСК подчертава необходимостта от по-добра подготовка срещу кибератаки като руските в Украйна, насочени по-специално към критичната инфраструктура. Сътрудничеството между гражданските и военните екосистеми е от решаващо значение за ефективното управление на кризи, оперативната съвместимост и избягването на дублирането на усилия и инвестиции, включително чрез симулирани пробни кибератаки.

1.6. ЕИСК счита, че инвестициите в киберотбрана следва да са приоритетно насочени към защитата на гражданите на ЕС и на критичната инфраструктура, включително чрез използване на надеждни доставчици на хардуер и софтуер. Той настоява за своевременно актуализиране на приоритетите и инвестициите, които да бъдат договорени между ЕС и държавите членки, с участието на съответните заинтересовани страни от частния сектор.

1.7. ЕС трябва да запази и развие необходимия капацитет за гарантиране на сигурността на своята цифрова икономика, общество, демокрация и критични технологии, както и за предоставяне на ключови услуги в областта на киберсигурността. За да се гарантира стратегическата автономност на ЕС, от жизненоважно значение е намаляването на зависимостта от трети държави. ЕИСК счита, че е от съществено значение ЕС да възприеме средносрочен подход към автономността по отношение на ключовите технологии и силно се застъпва за създаването на научноизследователски и производствени съоръжения от установени в ЕС дружества с подходяща европейска промишлена политика, съсредоточена върху автономна киберекосистема.

1.8. МСП следва да получават целенасочена подкрепа и да имат достъп до програми за финансиране, които повишават тяхната устойчивост на кибератаки, както и до помощ, възможности за обучение и образование относно кибернетичните рискове и начините за защита срещу тях. ЕС следва да осигури механизъм за стимулиране, който да насърчава постепенното запознаване на МСП с тези аспекти и развитието на иновативни МСП.

1.9. ЕИСК подкрепя плана за създаване на Академия на ЕС за киберумения и отправя искане към Европейската комисия да координира и финансира широкомащабни програми за обучение и професионално образование, които включват всички държави членки и имат за цел създаването на квалифицирана работна сила за всички агенции и организации, участващи в киберотбраната, както и за частни граждански мрежи.

1.10. Комитетът счита, че повишаването на осведомеността на гражданите относно киберсигурността е от решаващо значение за намаляване на излагането на кибератаки, и призовава за образователни програми в областта на киберсигурността и програми за обучение през целия живот, които да се съсредоточат върху подобряването на киберуменията и знанията. ЕИСК подкрепя включването на киберсигурността във всички бъдещи публични политики на ЕС и информирането на широката общественост за киберзаплахите.

1.11. ЕИСК смята, че силното сътрудничество със съюзниците от НАТО във военните области трябва да се съсредоточи върху цялостна координация и реципрочност, съвместни проекти в областта на научноизследователската и развойната дейност и иновациите, обмен на най-добри практики, големи програми за обучение и симулации на кибератаки, като основната цел е да се разшири капацитетът за съвместно реагиране.

1.12. Комитетът призовава върховния представител да разгледа текущите двустранни кибердиалози и да предприеме допълнителни дискусии с други държави и съответни международни организации за създаване на световна рамка за придържане към международното право в киберпространството, със силен акцент върху реципрочността. Комитетът смята, че тъй като ЕС е солидно базиран на основните демократични свободи, би било подходящо той да поеме водеща роля в международните дискусии относно бъдещето на киберсигурността, особено в рамките на Организацията на обединените нации.

1.13. ЕС следва да заеме твърда позиция срещу всякакъв вид система за социално оценяване в ущърб на гражданите. ЕИСК ясно заявява, че истинската демокрация не може да съществува без ефективна защита на личните данни, и смята, че отговорното и ефикасно управление на данните е от съществено значение за превръщането на хиперсвързаността в конкурентно предимство.

2. **Въведение и общи бележки**

2.1. Цифровата експанзия на обществата е свързана с голям брой заплахи за киберсигурността, породени от модернизацията на технологиите. Броят и сложността на кибератаките нараснаха значително през последните няколко години, което подкопава сигурността както на публичните, така и на частните субекти. Независимо дали става въпрос за софтуер за изнудване, зловреден софтуер, имейл атаки, нарушения на сигурността на данните, дезинформация, разпределени атаки тип „отказ от обслужване“ (DDoS) или други форми на атаки, всички те представляват последователна и постоянна заплаха за сигурността на ЕС като цяло.

2.2. ЕИСК приветства съвместното съобщение относно *„Политика на ЕС за киберотбрана“* ([2]) и смята, че сега е моментът да се действа неотложно и координирано на равнището на ЕС, като се включат както гражданските, така и военните екосистеми в киберпространството и се гарантира подходяща рамка за инвестиции за способности за киберотбрана. Комитетът обаче отбелязва, че съобщението е само заявление за решителност за действие и списък на бъдещите инициативи на ЕС, които следва да бъдат осъществени, и смята, че е невъзможно да се прецени дали тези бъдещи ангажименти действително ще бъдат изпълнени, тъй като бъдещите преговори между съзаконодателите естествено ще повлияят на крайния резултат от плана на ЕС за действие за киберсигурността.

2.3. Руската атака срещу сателитната мрежа KA-SAT, която наруши комуникацията между украинските военни сили, и неотдавнашният скандал с Éric Léandri, с когото някои отбранителни дружества са сключили договор за кибершпионаж от тяхно име, поставят киберсигурността на челно място в списъка на заплахите за сигурността в ЕС. Въпреки че ОРЗД е солиден законодателен акт на ЕС и е в сила от няколко години, ясно е, че нарастващият обем на наличните данни е уязвим и рискът трети страни да преминат границата на законност се увеличава всеки ден.

2.4. Предвид транснационалния характер на кибератаките е необходима координация на равнище ЕС, за да се намали настоящата фрагментираност и да се гарантира, че държавите членки са готови да си сътрудничат и да инвестират съвместно. Това е особено важно за бъдещи случаи, в които една държава членка би могла да бъде цел на атаки, а всички останали следва да имат възможността да предоставят незабавна подкрепа.

3. **Съвместни действия за по-силна киберотбрана**

3.1. Комитетът взема под внимание обявените амбициозни инициативи за създаване на Координационен център на ЕС за киберотбрана, за разработване на проекта CyDEf-X, за създаване на екипи за бързо реагиране при кибератаки, за разработване на инициатива на ЕС за киберсолидарност и за проучване на разработването на схеми за сертифициране на киберсигурността за ИКТ продукти, услуги и процеси. ЕИСК препоръчва всички държави членки да се ангажират да имат готовност за бързо реагиране 24 часа/7 дни в седмицата, като Координационният център на ЕС участва в оценката и изготвянето на редовни доклади относно киберготовността на държавите членки и ефективността на европейския механизъм за реагиране при киберкризи, като се съсредоточи както върху военните способности, така и върху критичните сектори, определени в Директивата МИС 2. Всяка държава членка следва да разполага със специалисти, специално обучени да интервенират в случай на киберинциденти, и следва редовно да проверява способността си за интервенция в друга държава членка.

3.2. Въпреки че съобщението съдържа дълъг списък с поетапни подобрения, ЕИСК би се надявал да види ясна пътна карта за изпълнението на тези инициативи, с ясно управление и ясни срокове за представяне и приемане. Освен това Комитетът би очаквал на организираното гражданско общество да бъде отредена по-важна роля в разработването на тези предложения.

3.3. ЕИСК смята, че държавите членки трябва да укрепят вътрешния си капацитет да противодействат на киберзаплахите, като се ангажират с проекти за сътрудничество и обменят информация и най-добри практики със своите колеги в други държави членки. Налице е необходимост от бързо осъществяване на инвестиции в способности за киберотбрана и за ускорено внедряване на технологии ([3]) във всички държави членки и в съвместна готовност за откриване на кибератаки, възстановяване след тях и защита срещу тях. За да се подкрепи автономността на Съюза в областта на киберсигурността, Комитетът счита, че частният сектор следва да разработи или въведе динамична платформа за изпитване и обмен на информация в реално време, с акцент върху идентифициране на липсващите понастоящем способности.

3.4. ЕИСК споделя възгледа, че на този етап военните операции в киберпространството следва да останат стриктно от компетентността на държавите членки; Комитетът подкрепя обявеното сътрудничество между военните екипи на ЕС за незабавно реагиране при компютърни инциденти (milCERTs), екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU).

3.5. С наскоро приетата Директива МИС 2 и Директивата относно устойчивостта на критичните субекти (CER) ([4]) вече бяха въведени специфични национални и секторни задължения за рамката на ЕС за киберотбрана. Необходими са допълнителни действия за подобряване на колективния капацитет на ЕС за откриване и ЕИСК призовава за инвестиции в НИРД за развитие на новаторски способности на ЕС.

([2]) Съобщение на Комисията относно „Политика на ЕС за киберотбрана“.

([3]) Като например Ускорителя за иновации в областта на отбраната за Северноатлантическата инициатива (DIANA) на НАТО.

([4]) Директива относно устойчивостта на критичните субекти.

4. **Защита на отбранителната екосистема на ЕС**

4.1. ЕИСК смята, че присъщата сложност и бързо променящите се технологични предизвикателства преобразиха отбранителната екосистема и че киберсигурността се превърна в обща тема и за военния, и за гражданския сектор, както и за гражданите на ЕС. Сътрудничеството между гражданските и военните екосистеми сега е по-важно от всякога и следва да донесе ползи по отношение на по-ефективно управление на кризи, както и непрекъснат напредък и оперативна съвместимост, като се избягва дублирането или умножаването на едни и същи усилия и инвестиции. Държавите членки следва да бъдат готови да провеждат стрес тестове на националната критична инфраструктура с цел оценка и повишаване на устойчивостта на бъдещи кибератаки.

4.2. ЕИСК смята, че инвестициите в киберотбрана трябва, като приоритет, да бъдат насочени към защитата на гражданите на ЕС и на критичната инфраструктура. Предвид бързия темп на цифровата трансформация и бързото развитие на обстановката по отношение на заплахите, Комитетът настоятелно призовава ЕС и държавите членки да договорят своевременно актуализиране на приоритетите и инвестициите, като се провеждат задълбочени консултации със съответните заинтересовани страни от частния сектор. Устройствата за интернет на нещата (ИН) често не са също толкова защитени, колкото традиционните устройства, и ЕИСК призовава да се гарантира минимално равнище на сигурност чрез платформи за идентификация и управление на достъпа (IDAM). Освен това, тъй като сертифицирането е ключов метод за осигуряване на по-високо равнище на сигурност, Комитетът призовава в новия подход на ЕС за сертифициране да се постави по-силен акцент върху сигурността на интернет на нещата.

4.3. ЕС трябва да изгради устойчивост на кибератаките и да създаде ефективно възпиране на злоупотребите в киберпространството. Критичната инфраструктура трябва да бъде защитена срещу кибератаки от всякакъв вид, включително чрез отбранителни системи на ЕС. Комитетът счита, че е от стратегически интерес за ЕС да се гарантира, че Съюзът запазва и развива основния капацитет за гарантиране на сигурността на своята цифрова икономика, общество и демокрация, за постигане на пълен цифров суверенитет като единствен начин за защита на критичните технологии и за предоставяне на ефективни ключови услуги в областта на киберсигурността. Намаляването на зависимостта от трети държави също е от жизненоважно значение за стратегическата автономност на ЕС. ЕИСК счита, че секторните агенции на ЕС (ENISA, ЕААБ, ERA, ЕМА, ЕБО, ЕКА, HADEA и др.) следва да бъдат включени в процеса и да предоставят насоки при разработването на схеми за киберсигурност.

4.4. Пандемията от COVID-19 ускори цифровия преход и превърна традиционния труд в хибриден и/или дистанционен, като създаде нови работни отношения и очаквания, както и нова класа цифрови номади, чийто брой нараства. ЕИСК отбелязва бързите промени на пазара на труда, които доведоха до възприемането от страна на дружествата на архитектурата с „нулево доверие“ чрез решения за IAM (управление на идентифицирането и достъпа) и PAM (управление на привилегирования достъп). Комитетът счита, че този вид управление на ресурсите на дружествата поражда нови решения, свързани с киберзаплахите, и смята, че частният сектор трябва да бъде подкрепян при повишаването на равнището на сигурност на своите иновативни цифрови решения.

4.5. ЕИСК е по-скоро разочарован от изявлението на Комисията, че „[в] сътрудничество с държавите членки би могъл да бъде изготвен план за изпълнение“, и смята, че този план за изпълнение е задължителен. Комитетът смята, че планът следва да бъде изготвен съвместно с държавите членки и приложен възможно най-скоро. Комитетът изразява загриженост във връзка с по-леката позиция, възприета от Комисията, и настоятелно призовава институциите на ЕС и държавите членки да улеснят бързия напредък по обявените инициативи.

5. **Инвестиране в способности за киберотбрана**

5.1. С бързото развитие на технологиите киберпространството се превърна в най-новата област на военни действия след сушата, морето, въздуха и космическото пространство. То също така разкри големи възможности за извършване на престъпления от страна на злонамерени участници в киберпространството — от независими хакери до професионални престъпници и дори държавни субекти.

5.2. Инвестициите в НИРД са от жизненоважно значение и ЕИСК приветства съществуващите специални фондове в рамките на програмата „Цифрова Европа“, Европейския фонд за отбрана, „Хоризонт Европа“ и националните програми за възстановяване. Комитетът обаче би приветствал повече транснационални проекти, насочени към сътрудничество и оперативна съвместимост между системите за киберотбрана във всички държави членки, както и повече полезни взаимодействия между инструментите за финансиране, особено в подкрепа на иновативни МСП.

5.3. Както беше обявено в Стратегията на ЕС за киберсигурност още през 2020 г., Комитетът отбелязва, че крайният срок за създаване на съвместно киберзвено е настоящата година, и очаква новини относно приключването на процеса и готовността на ЕС да реагира на мащабни киберинциденти. ЕИСК очаква то да подобри ситуационната осведоменост на ЕС и цялостния капацитет за реагиране и възстановяване.

5.4. ЕИСК подкрепя разширяването на мандата на ЕССС, за да подкрепя дейността на Координационния център на ЕС за киберотбрана. Освен това тази мрежа би могла да подкрепи европейския цифров суверенитет чрез разработване на конкурентоспособна европейска промишлена база за ключови технологични способности, основана отчасти на работата, извършена от договорни публично-частни партньорства (ПЧП). ПЧП се оказаха най-ефективният подход за подобряване на киберсигурността на цялата цифрова екосистема, но тя не може да бъде еднопосочна: публичните институции трябва също така да споделят своите разузнавателни данни с частния сектор.

5.5. ЕИСК отбелязва, че за да се справи с бъдещите опити за хакерски атаки от квантови компютри, ЕС трябва незабавно да инвестира в авангардни технологии като постквантовата криптография. Комитетът счита, че е абсолютно необходимо Европа да възприеме средносрочен подход към автономността, и силно се застъпва за разработването на научноизследователски и производствени съоръжения от установени в ЕС дружества. ЕИСК счита, че е важно да се увеличат ресурсите на ЕС за научни изследвания и иновации в областта на цифровите технологии и да се подкрепят инвестициите на операторите и доставчиците в нови функции в областта на техническата сигурност, включително свързани с нови тенденции като разширената реалност и метавселената. По-специално, от съществено значение е да се изгради европейска разпределена инфраструктура за изчисления в облак въз основа на европейските правила по теми като съхранението и обработката на данни ([5]).

5.6. На МСП следва да се обърне специално внимание и да им се осигури достъп до програми за финансиране, които повишават тяхната готовност срещу кибератаки, както и до програми за подпомагане, обучение и образование, които им помагат да разберат кибернетичните рискове и как да се защитават. ЕС следва да осигури механизъм за стимулиране, който да насърчава постепенното запознаване на МСП с тези аспекти.

5.7. Комисията изчислява съществуващия недостиг на умения в областта на киберсигурността на половин милион души и ЕИСК оценява предложението за създаване на академия за киберумения. Ясно е, че усилията на равнището на държавите членки не са достатъчни за намаляване на недостига на умения, поради което Комитетът предлага, заедно със стартирането на Академията, Комисията да използва импулса, породен от Европейската година на уменията, и да координира и финансира широкомащабни програми за обучение и програми за ПОО на равнище ЕС, които включват всички държави членки и се съсредоточават върху осигуряването на квалифицирана работна сила за всички агенции и органи, участващи в киберотбраната, както и за частните граждански мрежи. Особено внимание трябва да се обърне на обучението на работната сила, по-специално в областта на науката, технологиите, инженерството и математиката (НТИМ).

5.8. Освен това ЕИСК счита, че е от съществено значение да се повиши осведомеността на гражданите относно киберсигурността, за да се намали експозицията към кибератаки, особено по отношение на основните киберпрестъпления, насочени към населението като цяло. Комитетът призовава за образователни програми в областта на киберсигурността и програми за обучение през целия живот в областта на киберсигурността, които ще се съсредоточат върху подобряването на киберуменията и ще направят киберсигурността по-позната и по-привлекателна за гражданите, особено за по-младото поколение. ЕИСК подкрепя включването на съображения във връзка с киберсигурността във всички бъдещи публични политики на ЕС и информирането на широката общественост за киберзаплахите, включително чрез безплатни програми за обучение на населението като цяло, безплатни информационни приложения за мобилни телефони или чрез повишаване на информираността през най-гледаното телевизионно време. Успоредно с тези действия трябва да се насърчава широко разпространеният културен напредък на всички равнища на обществото в посока подход, ориентиран към киберсигурността.

5.9. ЕИСК счита за изключително важно да се правят оценки на профила на риска на доставчиците и да се прилагат съответните ограничения за онези от тях, които се считат за високорискови, в това число необходимите забрани за ключовите сектори, определени като критични и чувствителни в координираната оценка на риска на равнище ЕС, както и сертифициране на надеждните доставчици на хардуер и софтуер.

6. **Партньорство за справяне с общите предизвикателства**

6.1. Степента на подготвеност за бъдещи кибератаки се различава значително в отделните държави членки. ЕИСК счита, че непосредствената първа стъпка е да се създаде комуникационна платформа за най-добри практики в рамките на ЕС, където най-напредналите в кибернетичното отношение държави членки могат да споделят своите знания с другите държави и да улесняват незабавното им възприемане от другите държави. Това би спомогнало за подобряване на взаимното доверие между националните структури. На второ място, Комитетът счита, че е необходимо по-тясно сътрудничество между държавните и недържавните участници в целия ЕС, за да се подобри киберсигурността на продуктите и услугите в рамките на вътрешния пазар. ЕИСК предлага също така да се създаде обща платформа на ЕС за докладване на киберинциденти, включително черен списък на ЕС на всички активисти в областта на киберпрестъпността.

([5]) Като например Gaia-X, френско-германска инициатива.

6.2. ЕИСК е на мнение, че тясното сътрудничество с нашите съюзници от НАТО във военната област трябва да бъде съсредоточено не само върху изграждането на капацитет и ранното откриване, но и върху съвместните проекти в областта на научноизследователската и развойната дейност и иновациите, споделянето на най-добри практики и обмена между експерти, големите програми за обучение и симулациите на кибератаки. Основната цел следва да бъде да се разшири общият капацитет за реагиране и да се създадат полезни взаимодействия за борба с бъдещите хибридни заплахи след съвместните декларации от Варшава от 2016 г. и Брюксел от 2018 г. Сътрудничеството между ЕС и НАТО все още има редица възможности, които могат да бъдат използвани, а незабавният напредък може да доведе до реална промяна по отношение на гарантирането на сигурността за нашите граждани и общества.

6.3. Комитетът счита, че дискусиите на световно равнище и с нашите международни партньори следва да създадат условия за насърчаване на глобално и отворено киберпространство, което защитава правата на човека, основните свободи и върховенството на закона и се съсредоточава върху разработването на обвързващи международни стандарти в сектори с бързо развитие на цифровите технологии. ЕИСК препоръчва на върховния представител да направи преглед на съществуващите двустранни кибердиалози и да започне допълнителни преговори с други държави и съответни международни организации с цел насърчаване на глобална рамка за прилагане на международното право в киберпространството, въз основа на строго условие за реципрочност.

6.4. Накрая, Комитетът счита, че ЕС е в най-добра позиция да ръководи международните дебати относно бъдещето на киберсигурността, особено в рамките на обсъжданията в рамките на ООН, поради солидната си основа върху основните демократични свободи. ЕС трябва също така да се ангажира в борбата с тоталитарните режими, които извършват мониторинг на данните на гражданите и нарушават техните права и свободи, и следва да се позиционира категорично срещу всякакъв вид система за социално оценяване в ущърб на гражданите. ЕИСК ясно заявява, че не може да съществува истинска демокрация без ефективна защита на личните данни, и счита, че отговорното и ефикасно управление на данните е от жизненоважно значение за превръщането на хиперсвързаността в предимство.

Брюксел, 14 юни 2023 г.

Председател
на Европейския икономически и социален комитет
Oliver RÖPKE