Съвет на
Европейския съюз

Брюксел, 7 октомври 2022 г.
(OR. en)

12930/22

LIMITE

CYBER 310
TELECOM 382
COSI 241
COPEN 333
DATAPROTECT 262
IND 372
RECH 514
HYBRID 94
JAI 1244
POLMIL 206
RELEX 1260

БЕЛЕЖКА ПО ТОЧКИ А

От:	Генералния секретариат на Съвета
До:	Съвета
№ предх. док.:	12892/22
Относно:	Проект за заключения на Съвета относно сигурността на веригата за доставки на ИКТ — Одобряване

1. След ориентационен дебат относно сигурността на веригата за доставки на ИКТ, проведен на заседанието на Хоризонталната работна група по въпроси на кибернетичното пространство на 6 юли 2022 г., председателството изготви проект за заключения на Съвета.

2. Целта на настоящия проект за заключения е да се въведе ефикасен начин за използване на наличните инструменти за повишаване на сигурността на веригата за доставки на ИКТ в Европейския съюз и, когато е целесъобразно, да се представят допълнителни инструменти за укрепване на сигурността на веригата за доставки на ИКТ. Необходимостта от повишаване на сигурността на веригата за доставки на ИКТ се откроi особено ярко след някои от кибератаките, предизвикали най-сериозни последици до момента, като SolarWinds и NotPetya, извършени чрез вериги за доставки на ИКТ. Необходимостта от предприемане на мерки се обуславя и от все по-нарастващата зависимост на обществото ни от цифровите технологии и на тясно свързаната с това заплаха от нежелани стратегически зависимости във веригите за доставки на ИКТ, които са от съществено значение за сигурността на нашата цифрова инфраструктура — гръбнака на нашето общество.

3. Проектът за заключения съдържа конкретни действия за укрепване на аспектите, свързани със сигурността на веригата за доставки на ИКТ, на междусекторните инструменти, като например обществените поръчки и рамката за преки чуждестранни инвестиции. В тях е посочен и начинът, по който съществуващите и предстоящите специфични за киберпространството инструменти могат да допринесат за сигурността на веригата за доставки на ИКТ. Тук потенциалът се крие не само в Директивата МИС 2 или в схемите за сертифициране, издадени в рамката, определена с Акта за киберсигурността, но и в неотдавнашното предложение за законодателен акт за киберустойчивост. И накрая, в проекта за заключения се предлага да бъдат използвани механизми за подкрепа за финансиране на изграждането на сигурна цифрова инфраструктура, за подобряване на общото разбиране и осведоменост и за задълбочаване на сътрудничеството с цел повишаване на сигурността на веригата за доставки на ИКТ в ЕС и извън него.

4. По-конкретно, в проекта за заключения се предлага в процедурите за възлагане на обществени поръчки да бъде поставено дължимото ударение върху критериите за подбор, свързани с киберсигурността, и Комисията да бъде приканена да издаде методически насоки, за да насърчи възлагащите органи да поставят подходящ акцент върху практиките на оферентите и техните подизпълнители в областта на киберсигурността. Освен това в проекта за заключения се призовава за създаването на инструментариум за веригата за доставки на ИКТ, който да се състои от общи мерки за намаляване на критичните рискове, свързани с веригата за доставки на ИКТ, и по този начин да се улесни извършването на координирани оценки на риска за критичните вериги за доставки съгласно Директивата МИС2. Включено е и възможно финансиране, позволяващо на организациите да поддържат високо ниво на киберсигурност по отношение на възлагането на обществени поръчки за ИКТ продукти и услуги в цялата верига за доставки.

5. Този проект за заключения на Съвета беше обсъден на заседанията на Хоризонталната работна група по въпроси на кибернетичното пространство на 15 юли, 20 юли, 16 септември и 23 септември 2022 г. На заседанието си от 28 септември 2022 г. хоризонталната работна група постигна съгласие по изменения текст.

6. Корепер обсъди проекта за заключения на Съвета на заседанието си от 7 октомври 2022 г. и одобри текста, поместен в приложението.

7. Съветът се приканва да одобри приложения проект за заключения на Съвета.

ПРИЛОЖЕНИЕ

Проект за заключения на Съвета относно сигурността на веригата за доставки на ИКТ

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

КАТО ПРИПОМНЯ заключенията си относно

– съвместното съобщение от 20 ноември 2017 г. до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“,

– капацитета за киберсигурност и изграждането на способности в ЕС,

– значението на 5G за европейската икономика и необходимостта от смекчаване на рисковете за сигурността, свързани с 5G,

– изграждане на цифровото бъдеще на Европа,

– „Възстановяване, осигуряващо напредък в прехода към една по-динамична, по-издръжлива и по-конкурентоспособна европейска промишленост“,

– киберсигурността на свързаните устройства,

– стратегията на ЕС за киберсигурност за цифровото десетилетие,

– установяването на позицията на Европейския съюз в киберпространството,

– Специален доклад № 03/2022 на Европейската сметна палата, озаглавен „Въвеждане на 5G в ЕС — забавяне в изграждането на мрежите и нерешени въпроси, свързани със сигурността“,

КАТО ПРИПОМНЯ заключенията на Съвета относно

– COVID-19, единния пазар, промишлената политика, цифровите технологии и външните отношения от 1—2 октомври 2020 г.,

– руската военна агресия срещу Украйна, сигурността и отбраната, енергетиката, икономическите въпроси, COVID-19 и външните отношения от 24—25 март 2022 г.,

– Украйна, продоволствената сигурност, сигурността и отбраната, и енергетиката от 30—31 май 2022 г.,

1. Като се има предвид нарастващото значение на геополитиката за киберсигурността, ИЗТЪКВА, че Европейският съюз и неговите държави членки трябва да подхождат към киберсигурността по всеобхватен и стратегически начин. Военната агресия на Русия срещу Украйна доведе до прелом в стратегическата среда и средата на сигурност за Европейския съюз и очерта необходимостта от един по-силен и по-способен Европейски съюз в областта на сигурността и отбраната. Тя показа, че е изключително важно геополитическата среда да се взема предвид по подходящ начин не само когато се реагира на злонамерени действия в киберпространството, но и когато се изгражда и поддържа устойчивостта на информационните и комуникационните технологии (ИКТ). Това е от особено значение за веригите за доставки на ИКТ продукти и услуги (вериги за доставки на ИКТ), които биха могли да бъдат изложени на риск въз основа на геополитическо съперничество, както се вижда от нападението SolarWinds, и засегнати от геополитическо напрежение и нестабилност, както се вижда от заплахата, свързана със зависимостта от руски доставчици на ИКТ по време на военната агресия на Русия срещу Украйна.

2. ОТБЕЛЯЗВА, че естеството на рисковете, свързани с веригата за доставки на ИКТ, състояща се от свързан набор от ресурси и процеси между икономическите оператори (съгласно определението в Регламент (ЕС) 2019/1020), който започва с набавянето на суровини и обхваща производството, преработката, обработването и доставката на ИКТ продукти и услуги, включително предоставянето на подкрепа по време на жизнения цикъл на ИКТ продуктите и услугите, води до уникални предизвикателства и потенциално широкообхватни последици. Освен на рисковете, свързани с липсата на ИКТ продукти, например поради недостиг на суровини от изключителна важност и полупроводници, необходими за тяхното производство, веригите за доставки на ИКТ продукти и услуги са изложени и на други заплахи. По-специално те могат да бъдат обект на действия или злоупотреби от злонамерени субекти по сложни, често скрити начини, които оказват въздействие върху поверителността, целостта и наличността на предаваните и съхраняваните чувствителни данни.

3. Като отчита, че е необходим подход, обхващащ всички рискове, при осигуряването на ИКТ активи, ПРИЗНАВА значението на предложението за директива за устойчивостта на критичните субекти за подобряване на физическата сигурност на критичните субекти и ИЗТЪКВА, че освен повишаването на устойчивостта срещу атаки във веригата на доставки, извършвани чрез киберсредства, е също толкова важно да се укрепят цялостната устойчивост и сигурност на веригите за доставки на ИКТ спрямо цялото разнообразие от рискови фактори като природни събития, срив на системата, вътрешни заплахи или човешки грешки. В този смисъл ОТЧИТА, че сигурността на веригата за доставки на ИКТ обхваща гарантирането на защитата на ИКТ продуктите и услугите, които се произвеждат, доставят, закупуват и използват във веригите за доставки на ИКТ, включително чрез защита на отделните компоненти и предаваните данни.

4. Въз основа на изводите от последиците от стратегическите зависимости на Европейския съюз от руските изкопаеми горива, както и от въздействието на смущенията във веригите за доставки по време на пандемията от COVID-19, по-специално по отношение на фармацевтичните продукти и полупроводниците, където проличаха стратегическите зависимости на ЕС, НАСЪРЧАВА държавите членки да работят за избягване на подобни ситуации на нежелани стратегически външни зависимости във връзка с ИКТ продуктите и услугите. Поради нарастващата цифровизация на обществото и все по-нарастващото използване на ИКТ в критичната инфраструктура, стратегическите външни зависимости, свързани с ИКТ продукти и услуги и техните вериги за доставки, следва непрекъснато да бъдат оценявани и, когато е целесъобразно, да бъдат предприемани мерки.

5. ПРИПОМНЯ, че постигането на стратегическа автономност при запазване на отворена икономика е ключова цел на Съюза, която включва установяване и намаляване на стратегическите зависимости и повишаване на устойчивостта в най-чувствителните промишлени екосистеми и конкретни области, включително цифровата. Това включва разработване и внедряване на стратегически цифров капацитет и инфраструктура, укрепване на способността за вземане на автономни технологични решения и също, като един от основните стълбове, осигуряване на устойчиви и сигурни инфраструктури, продукти и услуги за изграждане на доверие в цифровия единен пазар и в рамките на европейското общество, като същевременно се поддържат отвореността, глобалното сътрудничество с единомислещи партньори и конкурентоспособността и се използват потенциалните ползи от тях. Основните ценности на Европейския съюз са насочени най-вече към запазване на неприкосновеността на личния живот, сигурността, равенството, човешкото достойнство, върховенството на закона и отворения интернет като предпоставки за постигане на ориентирано към човека общество, икономика и промишленост, в които цифровите технологии са водещ фактор.

6. ОТБЕЛЯЗВА, че с оглед на променящата се картина на киберзаплахите, ако се съди по тенденцията в последните години сложни атаки със силно въздействие върху веригата за доставки, като например SolarWinds, Mimecast и Kaseya, да възникват едновременно с възлагането на ИКТ услуги от основно значение на подизпълнители и да стават по-интензивни в резултат на цялостното разчитане на производството, доставката или сервизното обслужване на ИКТ продукти и услуги от трети страни, в бъдеще е силно вероятно да възникват повече атаки към веригата за доставки, които да нанасят съществени вреди на икономиката и обществото. Във връзка с това ИЗТЪКВА значението на повишаването на сигурността и устойчивостта на веригите за доставки на ИКТ за функционирането на единния пазар, както и необходимостта да се гарантира наличността, сигурността и разнообразието на ИКТ продукти и услуги в рамките на единния пазар. Във връзка с това ПРИЗНАВА необходимостта от максимално и рационализирано използване на съществуващите инструменти и подходи на ЕС за постигане на тези цели, както и необходимостта от непрекъснато адаптиране към променящата се картина на киберзаплахите чрез въвеждане на допълнителни подходящи мерки и механизми, включително във връзка с възможните рискове за сигурността на нововъзникващите и революционните технологии. НАСЪРЧАВА държавите членки в това отношение да прилагат основан на риска подход за справяне с развитието на новите технологии.

7. ПРИЗНАВА, че разбирането на постоянно променящата се картина на киберзаплахите, както и на сложността на атаките във веригата за доставки, е от съществено значение за ефективното смекчаване на рисковете, свързани с веригите за доставки на ИКТ. Във връзка с това ИЗТЪКВА необходимостта от адаптиране към новите заплахи чрез активно и непрекъснато наблюдение, анализ и оценка на картината на заплахите във веригата за доставки, от повишаване на осведомеността и натрупване на знания за заплахите и уязвимите места, както и от проактивно предупреждаване на съответните образувания по адаптиран начин. ПРИВЕТСТВА работата на Агенцията на Европейския съюз за киберсигурност (ENISA), свързана със сигурността на веригата за доставки на ИКТ, и по-специално нейния доклад относно картината на заплахите за атаки във веригата за доставки.

МЕЖДУСЕКТОРНИ ИНСТРУМЕНТИ И ПОДХОДИ

8. ПОТВЪРЖДАВА, че е важно държавите членки да разгледат необходимостта от диверсифициране на доставчиците на критични ИКТ, за да се избегне или ограничи създаването на големи зависимости от отделни доставчици, и по-специално от високорискови доставчици, тъй като това увеличава излагането на последиците от потенциални прекъсвания на доставките. ПРИЗНАВА избягването на зависимостта от определен доставчик и диверсификацията на доставчиците на ИКТ за един от важните компоненти за гарантиране на стабилността и сигурността на вътрешния пазар. ПОДЧЕРТАВА необходимостта от насърчаване и прилагане на подходящи стратегии, улесняващи диверсификацията на доставчиците и конкурентоспособността по технологично неутрален начин. Освен това НАСЪРЧАВА включването в законодателството на ЕС на аспекти, свързани с предотвратяването на зависимостта от определен доставчик. Във връзка с това ОТБЕЛЯЗВА предложението за регламент относно хармонизирани правила за справедлив достъп до данни и тяхното използване (Законодателен акт за данните), чиято цел е да се повиши оперативната съвместимост на услугите за обработка на данни и да се премахнат пречките пред смяната на доставчиците на услуги за обработка на данни.

9. ПРИЗНАВА връзката между сигурността на веригата за доставки на ИКТ и обществените поръчки. ПОДЧЕРТАВА необходимостта в процедурите за възлагане на обществени поръчки да бъде отчитано по подходящ начин значението на сигурността на веригата за доставки на ИКТ и когато е целесъобразно, да бъдат налагани обективни и основани на риска критерии за подбор, свързани със способността на оферентите да гарантират високо равнище на сигурност на предоставяните услуги. ПРИЗОВАВА за намиране на правилния баланс между обществения интерес от най-ефективно и справедливо използване на публичните средства, от една страна, и обществения интерес от гарантиране на сигурността на информационните системи и гарантиране на гладкото функциониране на единния пазар, от друга страна. За да се улесни прилагането на съответните правила за възлагане на обществени поръчки с оглед на повишаването на киберсигурността, ПРИКАНВА Комисията да разработи методически насоки до третото тримесечие на 2023 г., за да насърчи възлагащите органи да поставят подходящ акцент върху практиките в областта на киберсигурността на оферентите и техните подизпълнители, както и да оцени и, ако е необходимо, да направи предложения за преразглеждане или допълване на съответното законодателство в областта на обществените поръчки.

10. ОТЧИТА, че преките чуждестранни инвестиции, свързани с ИКТ продукти и услуги, от една страна осигуряват икономически и социални ползи за държавите членки, предприятията и гражданите, но от друга, биха могли да съдържат рискове за сигурността и обществения ред, и ОТБЕЛЯЗВА, че механизмът на ЕС за скрининг на преки чуждестранни инвестиции, заедно със съответните национални системи за скрининг, които осигуряват средства за справяне с тези рискове, също биха могли да се прилагат като полезен инструмент за гарантиране на сигурността и устойчивостта на веригата за доставки на ИКТ, като допринасят за премахването на високорисковите инвестиции, които могат да засегнат тази сигурност и устойчивост. ОТЧИТА, че обменяната и споделяната чрез този механизъм информация, може да помогне на държавите членки да оценят по-добре възможните заплахи за сигурността на веригите за доставки на ИКТ и да предприемат съответните необходими стъпки. ПРИЗОВАВА съответните национални участници също да вземат предвид това измерение на механизма за скрининг, когато е целесъобразно.

11. По отношение на отбраната ПОТВЪРЖДАВА поканата си към Комисията заедно с държавите членки да направи оценка през 2023 г. на рисковете за веригите на доставки на критична инфраструктура в различни области, включително цифровата, свързани с интересите на ЕС в областта на сигурността и отбраната, както и да проучи възможностите за повишаване на киберсигурността в цялата верига за доставки на отбранителната технологична и индустриална база на ЕС. Освен това ПРИКАНВА държавите членки и Комисията да отразяват сигурността на веригата за доставки на ИКТ при изпълнението на ангажиментите и действията по стратегическия компас.

12. Като признава значението на суровините от изключителна важност, както и на всички видове полупроводници като основни градивни елементи на ИКТ продуктите, НАСЪРЧАВА конструктивните преговори по предложението за регламент за създаване на рамка от мерки за укрепване на европейската екосистема в областта на полупроводниците (Законодателен акт за интегралните схеми) и предложението за регламент на Съвета за изменение на Регламент (ЕС) 2021/2085 за създаване на съвместните предприятия в рамките на програмата „Хоризонт Европа“ по отношение на съвместното предприятие „Интегрални схеми“.

СПЕЦИФИЧНИ ЗА КИБЕРПРОСТРАНСТВОТО ИНСТРУМЕНТИ

13. По отношение на телекомуникационната инфраструктура ПРИЗНАВА постиженията на равнището на Съюза за подобряване на сигурността на веригата за доставки на 5G мрежите, по-специално чрез инструментариума на ЕС за киберсигурността на 5G технологиите (Инструментариум на ЕС в областта на 5G). ПРИЗОВАВА държавите членки да продължат да обменят информация относно най-добрите практики и методи за прилагането на мерките, препоръчани в Инструментариума на ЕС в областта на 5G, и в частност да прилагат съответните ограничения за високорискови доставчици на ключови активи, определени като критични и чувствителни в координираната оценка на риска на равнището на ЕС. ИЗТЪКВА, че Инструментариумът на ЕС в областта на 5G представлява гъвкав, основан на риска инструмент за справяне с установените предизвикателства в областта на сигурността, който позволява своевременно и ефективно справяне с аспектите на киберсигурността на 5G технологиите, като същевременно се зачитат компетенциите на държавите членки, и ОТЧИТА, че той е ценен инструмент за по-нататъшно повишаване, при пълна прозрачност, на сигурността на веригата за доставки на телекомуникационните мрежи по координиран начин, който може да послужи като вдъхновение за оценка на риска и инструменти за смекчаване, свързани с други жизненоважни сектори. ПРИПОМНЯ поканата на съответните органи да формулират препоръки въз основа на оценки на риска към държавите членки и Комисията, за да се укрепи устойчивостта на комуникационните мрежи и инфраструктури в рамките на Европейския съюз, включително продължаващото прилагане на Инструментариума на ЕС в областта на 5G.

14. ОТБЕЛЯЗВА значението на оперативно съвместимите подходи, които могат да се справят със зависимостта от определен доставчик и да намалят риска от концентрация, като същевременно подобряват сигурността на веригата за доставки в целия спектър на инфраструктурата и услугите в областта на ИКТ. По-специално във връзка с 5G мрежите ОТЧИТА потенциалните ползи от концепцията за Open RAN в това отношение и едновременно ПРИПОМНЯ доклада относно киберсигурността на Open RAN, публикуван от Групата за сътрудничество за МИС, в който се отбелязва, че тази концепция все още е в процес на разработване и нейната сигурност, прозрачност и стандартизация са на ранен етап на зрялост, и ПОДЧЕРТАВА, че е важно рисковете да се оценяват преди всеки преход към нови стандарти или архитектури.

15. ПОДЧЕРТАВА значението на съществуващите и предстоящите хоризонтални законодателни инструменти в областта на киберсигурността, по-специално Регламента относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии (Акт за киберсигурността), предстоящата директива относно мерки за високо общо ниво на киберсигурност в Съюза (МИС 2), предложението за регламент за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза, както и предложението за регламент относно хоризонталните изисквания за киберсигурност за продукти с цифрови елементи (Законодателен акт за киберустойчивост), за повишаване на сигурността на веригата на доставки на ИКТ. Освен това ОТБЕЛЯЗВА важните промени в специфичните за сектора регламенти в областта на киберсигурността, по-специално бъдещия регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA), който включва надзорна рамка за доставчиците трети страни на услуги в областта на ИКТ, които са от решаващо значение за финансовите субекти. С тези регламенти се въвеждат общи задължения, свързани със сигурността на веригата за доставки, както и подробни и специфични изисквания, които са от значение за съответния сектор. Същевременно ИЗТЪКВА, че доставчиците често предоставят своите продукти и услуги в различни сектори, а не само в един. Поради това е изключително важно да се гарантира, че изискванията за сигурност на веригата за доставки са съгласувани, доколкото е възможно, във всички съответни сектори, особено обхванатите от бъдещата директива за МИС 2, за да се избегнат несъответствия между задълженията, наложени на доставчиците, както и за да се облекчи тежестта за операторите от критичните сектори при оценяването на спазването на тези задължения от страна на доставчиците, като същевременно се вземат предвид секторните особености.

16. ПРИВЕТСТВА предложението за законодателен акт за киберустойчивост като важен законодателен инструмент за постигане на напредък в сигурното разработване на продукти с цифрови елементи и за гарантиране, че киберсигурността се отчита в целия жизнен цикъл на продуктите с цифрови елементи. ОТБЕЛЯЗВА, че предложението за законодателен акт за киберустойчивост има потенциал да допринесе значително за укрепването на сигурността на веригата за доставки на ИКТ. НАСЪРЧАВА конструктивните преговори и своевременното приемане на законодателния акт.

17. Във връзка с това ОТЧИТА текущата работа под ръководството на ENISA съвместно с държавите членки и други заинтересовани страни, която е насочена към предоставяне на ЕС на схеми за сертифициране на ИКТ продукти, услуги и процеси съгласно законодателния акт за киберсигурността, които следва да допринесат за повишаване на цялостното ниво на киберсигурност в рамките на цифровия единен пазар. НАСЪРЧАВА всички заинтересовани страни да участват в подготвителната работа по отделните европейски схеми за сертифициране, за да се изгради доверие в сигурни ИКТ продукти, процеси и услуги и да се укрепи тяхната устойчивост, и ПРИЗОВАВА Комисията бързо да изготви актове за изпълнение относно европейските схеми за сертифициране след приключването на подготвителната работа, по-специално относно европейската схема за сертифициране на киберсигурността, основана на общите критерии. ОТБЕЛЯЗВА, че европейските схеми за сертифициране следва да включват, когато е необходимо, изисквания по отношение на сигурността на веригата за доставки, включително и отношенията с доставчиците.

18. Подчертава необходимостта от цялостно прилагане на всички предстоящи разпоредби за МИС 2, свързани със сигурността на веригата за доставки на ИКТ. Във връзка с това ПОДЧЕРТАВА значението на координираните от ЕС оценки на риска на критичните вериги за доставки (координирани оценки на риска на веригата за доставки), националните политики относно сигурността на веригите за доставки и свързаните с нея мерки за сигурност. ОТБЕЛЯЗВА, че следва да се обърне внимание не само на първите доставчици, но и на съответните подизпълнители по отношение на рисковете за сигурността на първия доставчик или на крайния клиент. За да се улесни прилагането на мерките за управление на риска по веригата за доставки, НАСЪРЧАВА ENISA със съдействието на групата за сътрудничество за мрежова и информационна сигурност (МИС) да извърши преглед на най-добрите налични практики за управление на риска във веригата за доставки и да ги обедини в методически насоки. Освен това НАСЪРЧАВА ENISA да наблюдава инвестициите в сигурността на веригата за доставки на ИКТ на образуванията, регулирани съгласно предстоящата директива за МИС 2.

19. ПОДЧЕРТАВА също така ползите и рисковете от използването на доставчици на управлявани услуги и доставчици на управлявани услуги за сигурност в контекста на сигурността на веригата за доставки. Въпреки че използването на такива доставчици може значително да подобри сигурността в рамките на организациите и да доведе до по-високи нива на киберсигурност, дистанционното управление на ИКТ системите и услугите, съчетано с привилегирован достъп до ИКТ средата на клиентите, от която може да се нуждаят въпросните доставчици, може да доведе до значими каскадни ефекти върху голям брой клиенти, в случай че доставчиците са компрометирани. Поради това е от изключително значение доставчиците на управлявани услуги и доставчиците на управлявани услуги за сигурност да поддържат високо ниво на вътрешна сигурност и сигурност на услугите, които предоставят, както и да възприемат прозрачен подход към клиентите си по отношение на сигурността услугите, които предоставят. Във връзка с това ПРИВЕТСТВА бъдещото включване на тези доставчици в обхвата на предстоящата директива за МИС 2.

20. По отношение на прилагането на механизма за координирани оценки на риска във веригата за доставки съгласно предстоящата директива за МИС 2 ОТБЕЛЯЗВА значението на нетехническите рискови фактори в този контекст, като например неправомерното влияние от страна на трета държава върху доставчиците и доставчиците на услуги, и във връзка с това ОТЧИТА факторите, които могат да се използват за оценка на рисковия профил, както е посочено в координираната оценка на ЕС на риска за киберсигурността при мрежите от пето поколение (5G). ПРИКАНВА Комисията да определи до второто тримесечие на 2023 г., след консултация с групата за сътрудничество за МИС и ENISA, специфичните ИКТ услуги, системи или продукти, които биха могли да бъдат подложени приоритетно на координираните оценки на риска във веригата за доставки.

21. ОТБЕЛЯЗВА, че зависимостта от високорискови доставчици на ИКТ продукти и услуги, използвани за функционирането на критични мрежи и системи, представлява стратегическа заплаха, която трябва да бъде смекчена чрез подходящи политики както на национално равнище, така и на равнището на ЕС, и чрез сътрудничество между държавите членки и с единомислещите международни партньори. За да се улесни смекчаването на този стратегически риск и да се подпомогнат координираните оценки на риска във веригата за доставки, ПРИКАНВА групата за сътрудничество за МИС в сътрудничество с Комисията и ENISA да разработи мерки за намаляване на рисковете в критичните вериги за доставки на ИКТ (инструментариум за веригите за доставки на ИКТ). Инструментариумът за веригите за доставки на ИКТ следва да се основава на сценарии за стратегически заплахи, установени по отношение на веригите за доставки на ИКТ, и да предвижда мерки за реагиране на тези сценарии, като се използва опитът от инструментариума за 5G и опитът, придобит на национално равнище. Инструментариумът следва да допълва по прозрачен начин координираните оценки на риска във веригата за доставки за конкретни ИКТ услуги, системи или продукти съгласно предстоящата Директива за МИС 2, като предлага общи мерки за намаляване на рисковете, подлежащи на адаптиране към конкретните ИКТ услуги, системи или продукти в зависимост от мащаба и въз основа на рисковете, установени в отделните координирани оценки на риска във веригата за доставки.

22. ИЗТЪКВА важната роля на научните изследвания, иновациите, инвестициите и предприемаческите дейности в областта на цифровите технологии и киберсигурността, както и на финансирането на такива дейности, с оглед на избягването на евентуални нежелани стратегически зависимости в бъдеще и укрепването на цялостната устойчивост на веригите за доставки на ИКТ. Във връзка с това ПОДЧЕРТАВА ролята и значението както на стратегическите, така и на изпълнителните функции на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежата от национални координационни центрове, за да се допринесе за максимално увеличаване на въздействието на инвестициите за укрепване на водещата роля на Съюза и отворената му стратегическа автономност в областта на киберсигурността, както и за подкрепа от страна на Съюза на технологичния капацитет и умения и за повишаване на конкурентоспособността на Съюза в световен мащаб. Във връзка с това ПРИЗОВАВА за бързото привеждане в действие на мрежата от национални координационни центрове. ПРИКАНВА мрежата от национални координационни центрове да вземе предвид аспектите на сигурността на веригата за доставки на ИКТ, включително например сигурното разработване на софтуер, в своята стратегическа програма, като същевременно гарантира последователност и взаимно допълване и избягва дублирането на усилия. ПОДКРЕПЯ повишаването на европейската конкурентоспособност в областта на киберсигурността чрез програми за финансиране, като например програмата за научни изследвания и иновации „Хоризонт Европа“, както и програмата „Цифрова Европа“ за укрепване, изграждане и придобиване на съществен капацитет за цифровата икономика, обществото и демокрацията в ЕС.

МЕХАНИЗМИ ЗА ПОДКРЕПА

23. НАСЪРЧАВА засилването на стимулите за предоставяне на финансова подкрепа за мерки, насочени към укрепване на сигурността на веригата за доставки на ИКТ. ПРИЗОВАВА като приоритет и с оглед на предстоящото изпълнение на Директивата за МИС 2, мрежата от национални координационни центрове, Комисията и съответните заинтересовани страни да проучат възможностите за включване на аспекти, свързани със сигурността на веригата за доставки на ИКТ, в предстоящите покани за представяне на предложения в рамките на работните програми в областта на киберсигурността по програма „Цифрова Европа“ и програма „Хоризонт Европа“ или всякакви други подходящи възможности за финансиране. Тези възможности за финансиране следва, наред с другото, да имат за цел да позволят на организациите да подкрепят поддържането на високо ниво на киберсигурност по отношение на възлагането на обществени поръчки за ИКТ продукти и услуги в цялата верига за доставки, по-специално във връзка със замяната на конкретни критични ИКТ услуги, системи или продукти, признати за високорискови в съответствие с бъдещите координирани оценки на риска във веригата за доставки.

24. ОТЧИТА, че глобализацията и специализацията на ИКТ услугите и повишената зависимост от продукти и услуги на трети страни водят до необходимостта от тясно сътрудничество в рамките на ЕС и в международен план при обмена на знания и експертен опит между съответните заинтересовани страни и ги НАСЪРЧАВА да намерят силна и координирана позиция, гарантираща сигурността на веригата за доставки на ИКТ по всеобхватен начин. ПРИЗНАВА също така необходимостта от допълнително проучване на съответните съвременни подходи и техники както за подходяща основна киберхигиена, така и за дългосрочни решения за постигане на сигурни и устойчиви вериги за доставки на ИКТ, както и на най-подходящите начини за тяхното насърчаване и потенциалното им включване в политиката или други инициативи. Във връзка с това ОТЧИТА, че следва да се обърне специално внимание на проучването на ползите и недостатъците на системните решения, като например принципите на нулево доверие, софтуерния „опис на материалите“ и подобни дългосрочни решения. ПРЕПОРЪЧВА за тази цел да се използва групата за сътрудничество за МИС.

25. ОТБЕЛЯЗВА ползите от наблюдението и ефективния обмен на информация относно киберинцидентите и заплахите за предотвратяването, разкриването и смекчаването на последиците от атаки във веригата за доставки. ИЗТЪКВА необходимостта от продължаване на изграждането на доверие между държавите членки за ефективен обмен на такава информация. Във връзка с това ПРИПОМНЯ предложението на Комисията за подпомагане на държавите членки при създаването и укрепването на центрове за операции по сигурността (ЦОС) с цел изграждане на мрежа от такива центрове в целия ЕС, за да се осигури допълнително наблюдение и предвиждане на сигналите за атаки срещу мрежите. ПРИПОМНЯ необходимостта от взаимно допълване и координация в рамките на съществуващите мрежи и механизми, най-вече ИЗТЪКВА в това отношение ролята на мрежата на ЕРИКС и необходимостта от допълнително проучване на потенциала на тези мрежи за насърчаване на ефективна, сигурна и надеждна култура на обмен на информация. ПРИПОМНЯ усилията, предприети от държавите членки и подкрепяни от ЕС, за създаване на секторни, национални и регионални екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) и национални или европейски центрове за споделяне и анализ на информация (ISAC) като част от ефективна мрежа от партньорства в областта на киберсигурността в Съюза.

26. Поради взаимносвързания и глобален характер на заплахите за веригата за доставки на ИКТ ИЗТЪКВА значението на сближаването и повишаването на сигурността на веригата за доставки на ИКТ на световно равнище. С оглед на това ПРЕПОРЪЧВА използването на цифрови партньорства, кибердиалози и други съответни инициативи на ЕС, включително, когато е целесъобразно, споразумения за свободна търговия, за насърчаването на основани на риска оценки на доставчиците на продукти и услуги в областта на ИКТ и използването на надеждни доставчици, както и за създаване на сигурна и иновативна цифрова екосистема, основана на отворени, оперативно съвместими и прозрачни стандарти. Освен това ИЗТЪКВА ОТНОВО визията на партньорствата Global Gateway, както и на Съвета по търговия и технологии ЕС—САЩ и дейностите в рамките на неговите работни групи, за насърчаване на използването на надеждни/невисокорискови доставчици и за разработване на механизъм за финансиране, който да даде възможност за проекти, които правят ИКТ инфраструктурата и услугите в трети държави по-сигурни, устойчиви и надеждни, включително чрез въздържане от финансиране на покупки от ненадеждни/високорискови доставчици по технологично неутрален начин.

27. ПОТВЪРЖДАВА ангажимента си да допринася и насърчава отворено, свободно, глобално, стабилно и сигурно киберпространство и да се придържа към нормите, правилата и принципите за отговорно поведение на държавите в киберпространството, определени в рамката на ООН. Що се отнася по-специално до сигурността на веригата за доставки на ИКТ, ПРИПОМНЯ одобрения от групата на правителствени експерти и групата OEWG към ООН стандарт, който насърчава държавите да предприемат разумни стъпки, за да гарантират целостта на веригата за доставки, включително чрез разработването на обективни мерки за сътрудничество, така че крайните потребители да могат да имат доверие в сигурността на ИКТ продуктите, и да се стремят да предотвратяват разпространението на злонамерени ИКТ инструменти и техники и използването на вредни скрити функции, и ПРИЗОВАВА за широкото му прилагане.