

**ОТГОВОРИ НА ЕВРОПЕЙСКАТА КОМИСИЯ ПО СПЕЦИАЛНИЯ ДОКЛАД  
НА ЕВРОПЕЙСКАТА СМЕТНА ПАЛАТА:  
„ВЪВЕЖДАНЕ НА 5G В ЕС: ЗАБАВЯНЕ ПРИ РАЗГРЪЩАНЕТО НА МРЕЖИТЕ  
И НЕРЕШЕНИ ВЪПРОСИ, СВЪРЗАНИ СЪС СИГУРНОСТТА“**

**КРАТКО ИЗЛОЖЕНИЕ**

**Встъпителни бележки на Комисията:**

I. Разгръщането на 5G мрежите по бърз и сигурен начин е основен приоритет за Европейската комисия. Защитата на 5G мрежите от киберзаплахи означава оценяване и смекчаване на заплахите и рисковете. Тези заплахи и рискове бяха установени и оценени съвместно от държавите членки с подкрепата на Комисията и ENISA и въз основа на това беше набелязан набор от всеобхватни мерки за смекчаване на рисковете. При все че работата все още продължава в някои държави членки, голяма част от тях вече са засилили или са в процес на засилване на изискванията за сигурност за 5G мрежите въз основа на инструментариума на ЕС.

Инструментариумът на ЕС е признат като всеобхватна рамка за справяне с рисковете за сигурността на 5G.

Координираните действия в областта на киберсигурността на 5G на равнището на ЕС и инструментариумът на ЕС се вписват в една по-широка европейска рамка за защита на електронните съобщителни мрежи и други критични инфраструктури и допълват съществуващите мерки, като Европейския кодекс за електронни съобщения, рамката за далекосъобщенията, Акта за киберсигурността и Директивата за мрежова и информационна сигурност (Директивата за МИС) и, според случая, правилата за свободно движение, установени в Договора и Хартата на основните права на ЕС.

III. 5G ще играят ключова роля в нашата цифрова икономика и общество през идните години. Необходимо е да гарантираме, че 5G мрежите са сигурни в кибернетично отношение и са устойчиви спрямо нарастващите киберзаплахи и киберинциденти. Ето защо Комисията и държавите членки въведоха процес на координация, насочен към определянето и прилагането на всеобхватна рамка за сигурност на 5G под формата на инструментариум от мерки за намаляване на риска, договорен през януари 2020 г., с цел ефективно справяне с основните рискове за 5G мрежите, като престъпно хакерство, шпионаж и саботаж, по координиран начин. При все че работата все още продължава в някои държави членки, голяма част от тях вече са засилили или са в процес на засилване на изискванията за сигурност за 5G мрежите въз основа на инструментариума на ЕС.

VII. Инструментариумът на ЕС предоставя рамка за насърчаване на съгласуваността на вътрешния пазар, като същевременно се зачитат компетенциите в областта на националната сигурност в тази сфера.

Що се отнася до подхода на държавите членки към високорисковите доставчици, Комисията счита, че ще бъде възможно да се направи окончателна оценка само когато е налице повече информация.

При все че изпълнението е в ход, Комисията работи с държавите членки в рамките на групата за сътрудничество за МИС за насърчаване на привеждането в съответствие и сближаването между националните подходи.

IX. Първо тире — Комисията приема препоръката.

Второ тире — Комисията приема препоръката.

Трето тире — Комисията приема препоръката.

Комисията ще извърши оценката, като вземе предвид националните компетенции.

## ВЪВЕДЕНИЕ

04. Комисията признава съществуването на рискове за сигурността на 5G мрежите, но посочва, че технологията и стандартите за 5G мрежите също могат да доведат до подобряване на сигурността в сравнение с предишните поколения мрежи.

## КОНСТАТАЦИИ И ОЦЕНКИ

30. Въпреки че 4G вече може да обхванат широк спектър от услуги, 5G следва да представляват „мошен скок“ — голяма промяна в сравнение с 4G, така че основното предизвикателство е преходът от 4G към 5G, като 5G мрежите биват разгърнати в целия ЕС. Рискът от цифрово разделение винаги съществува, но е планирано този риск да бъде третиран като приоритет на политиката в рамките на политическата програма „Път към цифровото десетилетие“ във връзка с траекторията, която води към 5G целта за 100 % покритие на всички населени райони до 2030 г., и поради това да се подпомогнат държавите членки да предприемат действия в тази област, особено по отношение на достъпа в селските райони.

32. Обсерваторията за 5G е надежден източник за наблюдение на внедряването на 5G в ЕС и извън него, въпреки появата на някои недостатъци. Службите на Комисията очакват да разполагат с по-актуална информация, която да е на разположение с новия изпълнител.

### Общ отговор на Комисията по точки 48 и 49:

Комисията счита, че изборът на инструмент (препоръка) и подходът на сътрудничество с държавите членки за идентифициране на рисковете и мерките за намаляване на риска са най-подходящият начин на действие за справяне с рисковете за сигурността на 5G по бърз, ефективен и съгласуван начин.

Комисията избра препоръката, както и това да работи в сътрудничество с държавите членки за определяне на рисковете и мерките за смекчаване предвид сложността и хоризонталния характер на темата в рамките на националните компетенции и компетенциите на ЕС, а също и значителното измерение на националната сигурност. Освен това Комисията отчете факта, че държавите членки имат много различен национален контекст (пазарна структура, капацитет в областта на киберсигурността, разузнавателни данни за заплахите и т.н.).

Инструментариумът на ЕС представлява гъвкав инструмент, основан на риска, за справяне с предизвикателствата в областта на сигурността, който позволи своевременното и ефикасно справяне с аспектите на киберсигурността на 5G мрежите.

В своето съобщение „Сигурно внедряване на 5G в ЕС – прилагане на инструментариума на ЕС“ от януари 2020 г. Комисията обяви, че ще предостави подкрепа за прилагането на мерките от инструментариума, свързани с изискванията за сигурност, по-специално по отношение на съответните разпоредби в европейските правила за електронните съобщения, и ще разгледа добавената стойност на евентуални актове за изпълнение, в които се описват подробно техническите и организационните мерки за сигурност, с цел да се допълнят националните правила и да се подобрят ефективността и съгласуваността на мерките за сигурност, наложени на операторите.

### Общ отговор на Комисията по точки 51 и 52:

В контекста на прегледа на препоръката на Комисията, който бе извършен през декември 2020 г., Комисията проведе интервюта с компетентните органи на всички държави членки. Те квалифицираха координираните действия на Европа в областта на киберсигурността на 5G технологиите като своевременни, ефективни и пропорционални. Подходът на сътрудничество между националните органи, Комисията, ENISA и други заинтересовани страни беше снетен за подходящ за справянето с този сложен въпрос. Той даде възможност за навременно определяне на общи цели и методики, като същевременно позволи на държавите членки да адаптират мерките към националните си обстоятелства.

В инструментариума на ЕС и в доклада за напредъка, публикуван от групата за сътрудничество за МИС през юли 2020 г., се препоръчва да се определят планове за изпълнение и/или преходни периоди за онези оператори, които понастоящем използват оборудване на високорискови доставчици или вече са сключили договори с високорискови доставчици преди приемането на инструментариума на ЕС (напр. като се вземат предвид циклите на модернизиране на оборудването, по-специално миграцията от „несамостоятелни“ към „самостоятелни“ 5G мрежи).

55. Комисията взема под внимание забележките, докладвани от Европейската сметна палата.

За да се подпомогне допълнително тяхното изпълнение, критериите от инструментариума за оценка на високорисковите търговци бяха предмет на многобройни обмени между компетентните национални органи в рамките на групата за сътрудничество за МИС, след като беше договорен инструментариумът на ЕС.

56. В инструментариума на ЕС се препоръчва да се вземат предвид рисковите фактори, представени в координираната оценка на риска на ЕС, както и специфичната за всяка държава информация (напр. оценка на заплахата от службите за национална сигурност и др.) за оценката на рисковия профил на доставчиците.

61. Способността на доставчика да гарантира доставките е един от критериите, препоръчани от инструментариума на ЕС, за оценка на рисковия профил на доставчиците. Способността за гарантиране на доставките би могла да бъде засегната и от евентуални търговски санкции, пред които е изправен конкретен доставчик, както е посочено в рисковия сценарий относно „зависимостта“ в координираната оценка на ЕС на риска.

#### Общ отговор на Комисията по точки 70 и 73:

Комисията и държавите членки обменят подробна информация относно прилагането на инструментариума на национално равнище в рамките на групата за сътрудничество за МИС. Що се отнася до публичното оповестяване на непублична информация, това е отговорност на държавите членки.

#### Общ отговор на Комисията по точки 74—76 и каре 5:

Инструментариумът на ЕС предоставя рамка за насърчаване на съгласуваността на вътрешния пазар, като същевременно се зачитат компетенциите в областта на националната сигурност в тази сфера.

Що се отнася до подхода на държавите членки към високорисковите доставчици, Комисията счита, че ще бъде възможно да се направи окончателна оценка само когато е налице повече информация.

При все че изпълнението е в ход, Комисията работи с държавите членки в рамките на групата за сътрудничество за МИС за насърчаване на привеждането в съответствие и сближаването между националните подходи.

#### ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ

81. Разгръщането на 5G мрежите по бърз и сигурен начин е основен приоритет за Европейската комисия. Защитата на 5G мрежите от киберзаплахи означава оценяване и смекчаване на заплахите и рисковете. Тези заплахи и рискове бяха установени и оценени съвместно от държавите членки с подкрепата на Комисията и ENISA и въз основа на това беше набелязан набор от всеобхватни мерки за смекчаване на рисковете. При все че работата все още продължава в някои държави членки, голяма част от тях вече са засилили или са в процес на засилване на изискванията за сигурност за 5G мрежите въз основа на инструментариума на ЕС.

Инструментариумът на ЕС предоставя всеобхватна рамка за справяне с рисковете за сигурността на 5G.

83. 5G представлява „мощен скок“ — голяма промяна в сравнение с 4G, така че основното предизвикателство за избягване на цифровото разделение е преходът от 4G към 5G в целия ЕС.

Спецификациите на 5G обхващат цял набор от показатели за ефективността, по-специално във връзка със случаи на вертикално използване. Това може да включва, наред с другото, изисквания за надеждност, скорост на създаване на услугата, гъвкавост на изпълнението, нива на сигурност.

### **Препоръка 1 — Насърчаване на равномерното и навременно внедряване на 5G мрежите в рамките на ЕС**

Комисията приема препоръката.

а) Комисията ще работи съвместно с държавите членки за разработване на общо определение за очакваното качество на услугите на 5G мрежите. В контекста на цифровото десетилетие и предложеното решение относно програмата за политиката в областта на цифровите технологии до 2030 г. Комисията възнамерява да работи с държавите членки за общ подход към качеството на 5G услугите в ЕС, включително за сравнимостта на измерванията и данните от наблюдението.

Качеството на услугата не включва само скорост и забавяне, а обхваща цял набор от показатели за изпълнение, по-специално във връзка със случаи на вертикално използване.

Комисията възнамерява да работи заедно с държавите членки за определяне на такива измервания, както и да извършва годишни проверки и да дава препоръки за политики, мерки и действия за постигане на пълно 5G покритие до 2030 г.

Програмата за политиката в областта на цифровите технологии ще създаде стабилно управление чрез механизъм за наблюдение и сътрудничество, така че да се гарантира напредък към изпълнението на целите на програмата на политиката, включително внедряването на 5G, и ще препоръча коригиращи действия на държавите членки в това отношение.

б) Комисията приема препоръката.

в) Комисията приема препоръката.

### **Препоръка 2 — Насърчаване на съгласуван подход към сигурността на 5G между държавите членки**

а) Комисията приема препоръката.

Комисията ще оцени заедно с държавите членки необходимостта от по-нататъшни действия или подкрепа, например под формата на насоки, свързани с някои аспекти на инструментариума на ЕС.

б) Комисията приема препоръката.

Наблюдението и докладването ще се извършват от Комисията при пълно сътрудничество с държавите членки и ENISA.

в) Комисията приема препоръката.

### **Препоръка 3 — Разглеждане на въздействието на различните подходи на държавите членки към сигурността на 5G върху ефективното функциониране на единния пазар**

а) Комисията приема препоръката.

б) Комисията приема препоръката.

Комисията ще извърши оценката, като вземе предвид националните компетенции.

Съгласно инструментариума на ЕС държавите членки са тези, които трябва да вземат решение относно точния обхват на съответните ограничения и/или необходимите изключения за ключови активи, определени като критични и чувствителни в координираната оценка на ЕС на риска (напр. функции на основната мрежа, функции по управление и оркестрация на мрежата и мрежови функции за достъп), с цел ефективно смекчаване на установените рискове, като се вземе предвид и оценката на заплахата от националните разузнавателни служби. Държавите членки имат право да предприемат мерки, свързани с националната сигурност, включително потенциални ограничения или изключения на високорискови доставчици.