ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 29.1.2020 г.
COM(2020) 50 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

Сигурно внедряване на 5G в ЕС — прилагане на инструментариума на ЕС

1. ***Въведение***

Телекомуникационните мрежи от пето поколение (5G) ще имат основна роля за развитието на европейското общество и икономика. Очаква се те да предоставят огромни икономически възможности и да имат основно значение за цифровата и екологичната трансформация в области като транспорта, енергетиката, производството, здравеопазването, селското стопанство и медиите.

Поради това 5G технологиите ще имат потенциално въздействие върху всички аспекти на живота на гражданите на ЕС. Ето защо киберсигурността на 5G мрежите е от съществено значение не само за защитата на нашите икономики, общества и демократични процеси, но и за осигуряването на надеждна цифрова трансформация в полза на всички граждани на ЕС.

Зависимостта на много услуги с критично значение от 5G мрежите ще направи последиците от системни и широкообхватни смущения особено сериозни и като се има предвид взаимосвързаният характер на цифровите екосистеми, би могла да има значително въздействие отвъд националните граници. В резултат на това гарантирането на киберсигурността на 5G мрежите е въпрос от стратегическо значение за Съюза в момент, когато броят на кибератаките нараства, тяхната сложност е безпрецедентна и те се извършват от широк кръг участници, в частност от държавни или подкрепяни от държавата участници от държави извън ЕС. Що се отнася до сигурността на критичните инфраструктури, например тази за 5G, за първи път беше взето решение да се определи общ европейски подход. Този подход е напълно съобразен с отворения характер на вътрешния пазар на ЕС, доколкото продължават да са изпълнени основаните на риска изисквания на ЕС в областта на сигурността.

На 22 март 2019 г. Европейският съвет призова за съгласуван подход по отношение на сигурността на 5G мрежите. На 26 март 2019 г. Комисията прие Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите[1]. С препоръката държавите членки се призовават да извършат национални оценки на риска и прегледи на националните мерки, да работят съвместно на равнището на ЕС за координирана оценка на риска и да подготвят инструментариум, съдържащ възможни смекчаващи мерки. Настоящото съобщение представлява неразделна част от всеобхватната европейска стратегия на Комисията в областта на цифровите технологии, за която призова Европейският съвет.

2. ***Разгръщане на 5G в ЕС***

Внедряването в Европа на инфраструктурата за 5G мрежи е от основно значение за европейската промишлена стратегия и конкурентоспособност. Комисията определя внедряването на 5G технологиите като основна предпоставка за бъдещите цифрови услуги. През 2016 г. Комисията прие плана за действие за 5G, за да гарантира, че Съюзът разполага с инфраструктурата за свързаност, необходима за неговата цифрова трансформация от 2020 г. нататък и за широкообхватното внедряване в градските райони и по основните транспортни маршрути до 2025 г.[2] В съобщението относно обществото на гигабитов интернет се поставя амбициозната цел да се осигури достъп

[1] Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите, ОВ L 88, 29.3.2019 г., стр. 42—47.

[2] COM (2016) 588 от 14 юни 2016 г. относно 5G за Европа: план за действие.

до мобилен пренос на данни навсякъде, включително в селските и отдалечените райони[3].

Що се отнася до разпределението на честотите, държавите членки са разпределили 16 % от „пионерните“ ленти за 5G[4]. С оглед на правното задължение да се позволи използването на всички 5G „пионерни“ ленти до края на годината през следващите няколко месеца се очакват консултации за редица процедури за разпределяне.

Европа е сред най-напредналите региони в света по отношение на търговското въвеждане на 5G услуги[5]. Понастоящем се очаква до края на 2020 г. първите 5G услуги да бъдат на разположение в 138 европейски града. Първоначалните 5G мрежи, изградени на базата на настоящите мрежови технологии от 4-то поколение (4G) и 5G услуги, се предлагат основно на широката общественост или като подобрение на капацитета и скоростта по отношение на мрежите 4G, или като икономически ефективна безжична алтернатива на фиксираните мрежи[6].

Що се отнася до възможностите за нови услуги между стопански субекти, например в секторите на енергетиката, храните и селското стопанство, здравеопазването, производството или транспорта, Европа напредва добре с инвестиции от порядъка на 1 млрд. евро, включително 300 млн. евро от финансирането на ЕС в контекста на публично-частното партньорство за 5G технологии по линията на „Хоризонт 2020“. Тези инвестиции включват над 160 експериментални широкомащабни внедрявания на 5G технологии, установени в Европа, включително десет трансгранични коридора по протежение на магистрали, предназначени за широкомащабно изпитване на услуги за свързана и автоматизирана мобилност на базата на 5G технологии. Изпитванията включват поддържащи 5G приложения в области, простиращи се от устойчивото здравеопазване и земеделието с ефективно използване на ресурсите на базата на автоматизирана мобилност до интелигентните електрически мрежи и промишленост 4.0. Освен това ЕИБ, с подкрепата на Европейския фонд за стратегически инвестиции, предостави заеми за ускоряване на научноизследователската и развойна дейност в областта на 5G технологията.

Европейският кодекс за електронни съобщения („кодексът“)[7], който ще се прилага от 21 декември 2020 г., е важна основа за създаването на благоприятна среда за инвестиции за 5G мрежи и следващите ги технологии. Освен това програмите за публично финансиране, като например Механизмът за свързване на Европа в

[3] COM(2016)587 „Свързаност за изграждане на конкурентоспособен цифров единен пазар – към европейско общество на гигабитов интернет“.

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Някои от новите функции на 5G ще бъдат въведени следвайки поетапен подход. През първия етап (в краткосрочен или много краткосрочен план) внедряването на 5G ще включва основно „несамостоятелни“ мрежи, при които единствено мрежата за радиодостъп ще е модернизирана до 5G технология, докато останалите ѝ части ще продължават да разчитат на съществуващите 4G опорни мрежи, които ще предоставят на крайните потребители подобрени мобилни широколентови показатели. През следващите етапи (в краткосрочен/средносрочен до дългосрочен план) внедряването на „самостоятелни“ 5G мрежи, включително функции на 5G опорни мрежи, ще наложи и ще доведе с течение на времето до много по-мащабна промяна в архитектурата на мрежата.

[7] Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета за установяване на Европейски кодекс за електронни съобщения (преработена).

цифровата област[8] или европейските структурни и инвестиционни фондове, също ще имат важно значение за подпомагането на бъдещото внедряване на 5G мрежите, по-специално чрез свързването на общините със структури, ползващи 5G, като училища, болници, градове и местни администрации.

Като се имат предвид стратегическите възможности на Европа в областта на 5G услугите за различни сектори, от първостепенно значение ще бъде операторите и доставчиците на услуги да инвестират в усъвършенствани решения за 5G мрежи и услуги. Това ще изисква не само нови 5G мрежи за радиовръзка, но и нови, т. нар. „самостоятелни“ 5G опорни мрежи, за да бъдат предоставени усъвършенствани 5G функции, като например „разделяне на физическата мрежа на логически мрежи“[9] и „периферни изчисления“[10].

Комисията ще продължи напълно да подкрепя успешното разгръщане на 5G в ЕС, включително като се ангажира заедно с държавите членки и заинтересованите страни за използването на възможностите на 5G. Ще се обърне дължимото внимание на съответните здравни аспекти въз основа на принципа на предпазливост[11] в сътрудничество със съответните международни организации и научната общност.

3. Координирана оценка на риска на равнището на ЕС в областта на киберсигурността на 5G мрежите

Работейки съвместно с останалите държави членки в рамките на групата за сътрудничество за МИС[12], всяка държава членка извърши своя собствена национална оценка на риска за своите инфраструктури за 5G мрежи и предаде резултатите на Комисията и ENISA — Агенцията на Европейския съюз за киберсигурност — до началото на юли 2019 г.

Въз основа на тези национални оценки на риска на 9 октомври 2019 г. групата за сътрудничество за МИС, съставена от представители на държавите членки, Комисията и ENISA, публикува доклад за координираната оценка на риска на равнището на ЕС в областта на киберсигурността на 5G мрежите[13]. В него се посочват основните заплахи и участниците в тях, най-чувствителните активи и основните уязвими места (както от техническо, така и от друго естество) по отношение на 5G мрежите. Основавайки се на това, в доклада се набелязват също така редица категории рискове от стратегическо значение от гледна точка на ЕС, илюстрирани чрез конкретни рискови сценарии, които

[8] Предложение за Регламент COM(2018)438 от 6 юни 2018 г. за създаване на Механизма за свързване на Европа и за отмяна на регламенти (ЕС) № 1316/2013 и (ЕС) № 283/2014.

[9] Разделянето на физическата 5G мрежа на логически мрежи позволява висока степен на разграничаване на различните пластове на услугите, използващи една и съща физическа мрежа, като по този начин се увеличават възможностите за предлагане на разграничени услуги по цялата мрежа.

[10] Периферните изчисления са вид разпределени изчисления — парадигма, която предвижда изчисленията и съхраняването на данни да стават по-близо до мястото, където са необходими, с цел да се намали времето за отговор на системата и натоварването на комуникационния канал.

[11] Препоръка на Съвета от 12 юли 1999 г. за ограничаване излагането на населението на електромагнитни полета (0 Hz до 300 GHz) (1999/519/ЕО).

[12] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (директива за МИС). Групата за сътрудничество за МИС е създадена с директивата за МИС с цел да се осигури стратегическо сътрудничество и обмен на информация между държавите — членки на ЕС, в областта на киберсигурността.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

отразяват реалистични комбинации на различните параметри (уязвими места, заплахи и участници в тях) по отношение на различните активи (вж. допълнението).

В допълнение към настоящия доклад и като допълнителен принос към инструментариума, ENISA проведе целенасочено картографиране на заплахите[14], състоящо се от подробен анализ на някои технически аспекти, по-специално идентифициране на мрежовите активи и засягащите ги заплахи.

В доклада за координираната оценка на риска на равнището на ЕС се изтъкват редица аспекти, които са от значение за 5G мрежите. По-специално:

а) Технологичните промени, които се въвеждат с 5G технологиите, ще увеличат общата повърхност, уязвима за атаки, и броя на потенциалните точки на проникване за извършителите:

— Повишената функционалност в периферията на мрежата и по-слабо централизираната архитектура в сравнение с предишните поколения мобилни мрежи означават, че някои функции на опорните мрежи може да са интегрирани в други части на мрежите, което прави съответното оборудване по-чувствително (напр. базови станции или функции MANO).

— Нарасналият дял на софтуера в 5G оборудването води до повишени рискове, свързани с процесите на разработване и актуализиране на софтуера, създава нови рискове от грешки при конфигурацията и отрежда при анализа на сигурността по-съществена роля на решенията, които взема всеки оператор на мобилна мрежа на етапа на внедряване на мрежата.

б) Тези нови технологични характеристики ще увеличат значението на зависимостта на операторите на мобилни мрежи от доставчици, които са трети страни, както и на тяхната роля във веригата на доставки в областта на 5G.

Това от своя страна ще увеличи броя на възможните пътища за извършване на атаки, от които биха могли да се възползват участниците в заплахи, в частност държавни или подкрепяни от държавата участници от държави извън ЕС, поради техните способности (намерения и ресурси) да извършват атаки срещу телекомуникационните мрежи на държавите — членки на ЕС, както и потенциалната сериозност на въздействието на подобни атаки.

В този контекст на повишен риска от излагане на атаки, улеснявани от доставчици, които са трети страни, индивидуалният рисков профил на доставчиците ще стане особено важен, особено когато доставчикът има значително присъствие в рамките на мрежи или райони.

в) Значителната зависимост от един-единствен доставчик увеличава риска от излагане на атаки и последиците от евентуален пробив при този доставчик. Освен това тя задълбочава потенциалния ефект на слабости и уязвими места, както и риска от евентуалното им зловредно използване от участници в заплахи, по-специално

[14] Карта на ENISA относно заплахите за 5G мрежите: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

когато зависимостта е по отношение на доставчик, при който е налице висока степен на риск.

г) Ако се осъществят някои от новите сценарии на употреба, които се очакват за 5G технологиите, 5G мрежите ще се превърнат във важна част от веригата на доставки при много ИТ приложения с критично значение и по този начин не само ще бъдат засегнати изискванията за поверителност и неприкосновеност на личния живот, но също така целостта и достъпността на тези мрежи ще се превърнат в сериозна тема на националната сигурност и сериозно предизвикателство за сигурността от гледна точка на ЕС.

Източник: Координирана оценка на риска на равнището на ЕС

В доклада за координираната оценка на риска на равнището на ЕС се заключава освен това, че тези предизвикателства създават нова парадигма за сигурност, което налага да се направи преоценка на настоящата рамка за политика и сигурност, приложима към сектора на 5G технологиите и неговата екосистема, и да се предприеме необходимото, за да вземат държавите членки необходимите смекчаващи мерки.

С цел да се даде ефективен отговор на установените рискове и да се укрепи сигурността и стабилността на 5G мрежите, се изисква всеобхватен подход, което предполага въвеждането на набор от ключови мерки, както и на свързани подкрепящи действия, които могат същевременно да противодействат на рисковете. Координираната оценка на риска на равнището на ЕС даде основата за определяне на смекчаващи мерки, които могат да бъдат прилагани на национално и европейско равнище.

Заключенията на Съвета от 3 декември 2019 г. подкрепят констатациите на координираната оценка на риска и изтъкват „значението на координирания подход и ефективното прилагане на препоръката, за да се избегне фрагментирането на единния пазар“[15]. За тази цел Съветът призова държавите членки, Комисията и ENISA „да предприемат всички необходими мерки в рамките на своите правомощия, за да гарантират сигурността и целостта на електронните съобщителни мрежи, по-специално на 5G мрежите, и да продължат да утвърждават координиран подход за справяне с предизвикателствата пред сигурността, свързани с 5G технологиите.“

4. Инструментариум на ЕС за киберсигурност на 5G технологиите

На 29 януари 2020 г. групата за сътрудничество за МИС публикува инструментариума на ЕС от мерки за смекчаване на риска[16]. Той съдържа мерки за противодействие на всички рискове, набелязани в координирания доклад за оценка на риска.

Инструментариумът на ЕС определя и описва набор от стратегически и технически мерки и съответни подкрепящи действия за засилване на тяхната ефективност, които могат да се използват за смекчаване на установените рискове. **Стратегическите мерки**

[15] Заключения на Съвета относно значението на 5G за европейската икономика и необходимостта от смекчаване на рисковете за сигурността, свързани с 5G. 3 декември 2019 г., 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

[16] Киберсигурност на 5G мрежите — инструментариум на ЕС от мерки за смекчаване на риска, 29 януари 2020 г. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

обхващат мерки за увеличаване на регулаторните правомощия на органите за контрол относно възлагането на обществени поръчки за мрежи и внедряването на тези мрежи, конкретни мерки за справяне с рисковете, свързани с уязвимости, различни от техническите, както и възможни инициативи за насърчаване на устойчиви и разнообразни вериги на доставки и вериги за създаване на стойност в областта на 5G, с цел да се избегне възникването на системни и дългосрочни рискове от зависимост. **Техническите мерки** включват мерки за укрепване на сигурността на мрежите и оборудването за 5G чрез справяне с рисковете, произтичащи от технологии, процеси, човешки и физически фактори. Освен това за всяка от областите на риск, посочени в координираната оценка на риска на равнището на ЕС, инструментариумът предвижда **планове за смекчаване на риска**, основаващи се на мерките с най-висока ефективност.

Сред тях заключенията относно инструментариума на ЕС, приети от групата за сътрудничество за МИС, препоръчват следния набор от **ключови мерки**, които да се прилагат от всички държави членки и от Комисията:

Заключения в инструментариума на ЕС

В инструментариума на ЕС се определя набор от мерки и действия, които — ако бъдат правилно съчетани и ефективно приложени — дават основата за координиран подход в тази област. Действително, предвид широкия спектър от области на риск, определени в координираната оценка на риска на равнището на ЕС, и тяхното различно естество, няма да е достатъчен един-единствен вид мерки, а ще е необходим набор от мерки, използвани в подходяща комбинация, за да се обхванат всички ключови области на риск.

Въз основа на оценката на възможните планове за смекчаване и на определянето на мерките с най-висока ефективност, в този инструментариум се препоръчва:

1. Всички държави членки следва да гарантират, че разполагат с мерки (включително правомощия за националните органи) да отговорят по подходящ и пропорционален начин на настоящите и бъдещите рискове, и по-специално да гарантират, че са в състояние да ограничават, забраняват и/или налагат специфични изисквания или условия, следвайки основан на риска подход, по отношение на доставките, внедряването и експлоатацията на оборудване за 5G мрежи въз основа на редица съображения, свързани със сигурността.

По-специално те следва:

- *да повишат **изискванията за сигурност** за операторите на мобилни мрежи (напр. строг контрол на достъпа, правила за безопасна експлоатация и наблюдение, ограничения относно възлагането на външни изпълнители на конкретни функции и др.);*

- *да оценяват рисковия профил на доставчиците; на базата на тази оценка **да прилагат съответни ограничения за доставчици, чийто профил се счита за високорисков — включително необходимите изключвания с цел ефективно смекчаване на рисковете — за ключови активи,** определени като критични и чувствителни в координираната оценка на риска на равнището на ЕС (например функции на опорната мрежа, функции по управление и оркестриране на мрежата, както и функции за достъп до мрежата);*

- *да гарантират, че всеки оператор разполага с подходяща стратегия за използване на множество доставчици, за да се **избегне или ограничи всяка значителна зависимост** от един-единствен доставчик (или доставчици със сходен рисков профил), да се осигури подходящ баланс на доставчиците на национално равнище и да се **избегне зависимостта от доставчици, чийто профил се счита за високорисков**; това изисква също да се избягват*

ситуации на „блокиране“ в продуктовия спектър на един-единствен доставчик, включително чрез насърчаване на по-голяма оперативна съвместимост на оборудването.

2. Европейската комисия, съвместно с държавите членки, следва да допринася за:

- *поддържането на разнообразна и устойчива верига на доставки в областта на 5G, за да се избегне дългосрочната зависимост, включително чрез:*

  - *пълноценно използване на съществуващите средства и инструменти на ЕС, по-специално чрез скрининг на потенциални **преки чуждестранни инвестиции** (ПЧИ), засягащи ключови активи в областта на 5G, и чрез избягване на **нарушения** на пазара за доставки на 5G технологии, произтичащи от евентуален дъмпинг или субсидии; както и*

  - *повишаване на **капацитета на ЕС при 5G и по-късни технологии** чрез използване на съответните програми и финансиране от ЕС.*

- *улесняването на координацията между държавите членки по отношение на **стандартизацията** за постигане на конкретни цели в областта на сигурността и разработване на **съответни схеми за сертифициране, валидни в целия ЕС**, с цел насърчаване на по-сигурни продукти и процеси.*

3. За да се гарантира, че този координиран подход ще издържи проверката на времето, следва да се удължи мандатът на групата за сътрудничество за МИС, както и сътрудничеството с други съответни органи и образувания, по-специално с цел:

- *да се преразглеждат периодично с подкрепата на Комисията и ENISA **националните и европейските оценки на риска** относно сигурността на мрежите с 5G и по-късна технология, да се доразвива и привежда в съответствие методиката за оценка и да се предприемат адаптации към развиващата се 5G технология;*

- *да се извършват подробен и редовен **мониторинг и оценка на прилагането** на инструментариума въз основа на структурирано докладване от страна на държавите членки;*

- *да се координира и подпомага изпълнението на **подкрепящи действия**, които изискват сътрудничество на равнището на ЕС, по-специално по отношение на разработването на насоки и обмена на най-добри практики относно различните мерки;*

- *да се подкрепя, когато е целесъобразно и възможно, по-нататъшната координация на равнище ЕС, по-специално с цел по-тясно сближаване **по отношение на техническите и организационните изисквания за сигурност за операторите на мрежи**.*

Източник: Инструментариум на ЕС

Заключенията относно инструментариума показват твърдата решимост на държавите членки да отговорят съвместно на предизвикателствата, свързани със сигурността на 5G мрежите. Това е от основно значение за сигурността в отделните държави членки и целия ЕС, за националните икономики и за вътрешния пазар на ЕС, както и за технологичния суверенитет на Европа. Както координираната оценка на риска, така и инструментариумът на ЕС доказват високата стойност на съвместната работа, извършена в рамките на групата за сътрудничество за МИС, и на активното сътрудничество между представители на всички държави членки, Комисията и ENISA.

Инструментариумът дава възможност за общ подход на ЕС към киберсигурността на 5G технологиите и подкрепя съгласуваността в рамките на вътрешния пазар чрез политиките и координацията на ЕС, както и упражняването на компетенциите на държавите членки, особено по отношение на националната сигурност. Съдържащите се в него мерки и планове за смекчаване позволяват на ЕС да реагира по подходящ, ефективен и пропорционален начин на общите предизвикателства пред киберсигурността на 5G технологиите.

Комисията приветства публикуването на инструментариума на ЕС за киберсигурност на 5G технологиите и напълно подкрепя всички негови заключения, посочени по-горе.

Комисията призовава държавите членки и съответните институции, агенции и други органи на Съюза:

i) да осигурят бързото прилагане на ефективни и подходящи стратегии за смекчаване на риска в целия ЕС в съответствие с инструментариума на ЕС, и

ii) да предприемат всички необходими допълнителни стъпки за осигуряване на координация на равнището на Съюза, включително чрез продължаване на работата в рамките на групата за сътрудничество за МИС и създаване на стабилен механизъм за наблюдение на прилагането на инструментариума на ЕС, за да се гарантира ефективността на мерките и гладкото функциониране на вътрешния пазар.

5. Прилагане на инструментариума

Решимостта на държавите членки да използват пълноценно инструментариума е от съществено значение за прилагането на надежден и успешен европейски подход към сигурността на 5G технологиите. Независимо че държавите членки ще решават съобразно националните обстоятелства относно пригодността на отделните мерки, абсолютно необходимо е **наборът от ключови мерки, препоръчани от групата за сътрудничество за МИС (вж. инструментариума по-горе), да се въведе във всяка държава членка, а някои от мерките — и на равнището на ЕС**, за да се противодействат на установените рискове.

Комисията е готова да продължи да предоставя пълната си подкрепа по време на следващите етапи и призовава държавите членки:

— да предприемат **до 30 април 2020 г.** конкретни и измерими стъпки за прилагане на набора от ключови мерки, препоръчани в заключенията на инструментариума на ЕС;

— да представят **до 30 юни 2020 г.** доклад на групата за сътрудничество за МИС относно състоянието на прилагането на тези ключови мерки във всяка държава членка, основаващ се на данните от редовното докладване и наблюдение, извършвано по-специално в рамките на групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA.

5.1. Съобразен с риска и съгласуван подход към доставчиците на 5G

С оглед на крайната цел да се гарантират сигурността, стабилността и устойчивостта на 5G мрежите държавите членки постигнаха съгласие, че е необходимо да се оценява рисковият профил на отделните доставчици и впоследствие да се прилагат съответни

ограничения за доставчици, които се смятат за високорискови, включително необходимите изключвания с цел ефективно смекчаване на рисковете по отношение на ключови активи, както е посочено в инструментариума. Комисията е готова да окаже подкрепа на държавите членки при прилагането на тези мерки.

За да се подкрепи тяхното прилагане в целия ЕС, координираната оценка на риска на равнището на ЕС и инструментариумът на ЕС предоставят насоки по отношение на 1) оценката на рисковия профил на доставчиците[17] и 2) чувствителността на мрежовите елементи и функции[18], както и на други активи. Координираната оценка на риска на равнището на ЕС и инструментариумът на ЕС обхващат рисковете, свързани с доставчиците на оборудване и услуги за 5G мрежи. Те не обхващат останалите продукти или услуги, които тези или други доставчици могат да предоставят.

Както е определено в параграф 2.37 от координираната оценка на риска на равнището на ЕС, рисковите профили на отделните доставчици могат да бъдат оценени въз основа на няколко фактора.

Оценката на рисковите профили на доставчиците следва да се извършва единствено с оглед на съображенията за сигурност и да се основава на обективни критерии. С цел да се улесни използването на координиран подход при прилагането на тези мерки в инструментариума се препоръчва държавите членки да обменят информация относно националните подходи и най-добри практики. Освен това Комисията е на мнение, че това действие следва да бъде един от първите приоритети в следващия етап на работата, извършвана в рамките на групата за сътрудничество за МИС, заедно с Комисията и ENISA.

Важно е ограниченията по отношение на доставчиците, чийто профил се счита за висок рисков, включително необходимите изключвания с цел ефективно смекчаване на рисковете, както и мерките за избягване на зависимостта от тези доставчици, да се предприемат своевременно. Ако това се прави на най-ранен етап включително, когато е възможно, в рамките на процедурите за лицензиране на 5G честоти, ще се увеличи също предвидимостта за операторите на пазара, което ще допринесе за бързото разгръщане на 5G мрежите и ще гарантира дългосрочната сигурност на 5G мрежите и стабилността на веригата на доставки в областта на 5G.

Същевременно при прилагането на тези мерки на национално равнище могат да се определят различни срокове, когато това е необходимо и оправдано, по-специално, когато е налице висока степен на разпространение на оборудване или услуги на доставчици, оценени като високорискови (напр. с цел да се вземат под внимание циклите за модернизиране на оборудването, по-специално миграцията от „несамостоятелни“ към „самостоятелни“ 5G мрежи). Държавите членки биха могли да обмислят определянето на планове за прилагане, които могат да включват подходящи преходни периоди за съответните оператори на мрежи. В този контекст преходните периоди следва да бъдат определени по такъв начин, че да се запазят или дори засилят стимулите за инвестиране в съвременно мрежово оборудване, включително ускоряване

[17] Параграф 2.37 от координираната оценка на риска на равнището на ЕС.

[18] В параграф 2.21 от координираната оценка на риска на равнището на ЕС са представени основните категории елементи и функции и общото им ниво на чувствителност и са изброени редица ключови елементи, посочени от държавите членки за всяка категория, а в параграфи 2.28 и 2.29 са посочени редица други видове чувствителни активи или области (напр. конкретни образувания или географски райони).

на внедряването на пълноценни („самостоятелни“) 5G опорни мрежи и замяна на съществуващото 4G оборудване в други части на мрежите (напр. в мрежата за радиодостъп), в съответствие с целите на плана за действие за 5G[19].

Освен това, поради сложността на основаващите се на софтуер 5G мрежи, е възможно далекосъобщителните оператори във все по-голяма степен да разчитат на трети страни за изпълнението на определени задачи, като поддръжката и модернизирането на 5G мрежите и софтуера, както и други възложени на външен изпълнител управлявани услуги, в допълнение към доставката на мрежово оборудване. Както е описано в координираната оценка на риска на равнището на ЕС, това представлява източник на сериозен риск за сигурността. Поради това следва да се обърне специално внимание на този аспект. От съществено значение е също така извършването на цялостна оценка за сигурност по отношение на рисковия профил на доставчиците, натоварени с тези услуги, по-специално когато тези задачи не се изпълняват в ЕС. Следва да се предприемат подходящи мерки, включително прилагане на ограничения, по-специално в чувствителните части на 5G мрежите, или необходими изключвания на високорискови субекти в съответствие със смекчаващите мерки от инструментариума, за да се запази дългосрочната цялост на 5G инфраструктурата.

5.2. Ролята на Комисията в подкрепа на прилагането на инструментариума

Комисията ще продължи да подкрепя прилагането на подхода на ЕС по отношение на киберсигурността на 5G технологиите като цяло, както и да предприема конкретни инициативи във връзка с мерките и целите на инструментариума там, където може да добави стойност. Комисията ще използва пълноценно своите правомощия и съответни инструменти, доколкото това е необходимо с оглед на набелязаните съображения относно сигурността. По този начин и като действа съвместно с държавите членки и частния сектор, Комисията се стреми да подкрепя стратегическите мерки, които ще допринесат за гарантиране на технологичния суверенитет и водещата роля на ЕС в бъдещото развитие на мрежовите технологии, технологиите за киберсигурност и всички съответни градивни елементи, от които зависят цялата наша икономика и нашата сигурност.

По-конкретно Комисията ще предприеме следното, за да гарантира прилагането на съответните смекчаващи мерки от инструментариума в областите, попадащи в нейната компетентност:

Гарантиране на киберсигурността на 5G мрежите и на разнообразна верига на стойността в областта на 5G:

— **Сътрудничество в областта на киберсигурността**: ще продължи да предоставя подкрепа на държавите членки за ефективното, координирано и навременно прилагане на националните мерки чрез групата за сътрудничество за МИС.

— **Далекосъобщителни оператори и правила за киберсигурност**: ще подкрепи 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

[19] COM (2016) 588 от 14 септември 2016 г., „5G за Европа: план за действие“.

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.

— **Стандартизация**: ще предприеме действия, за да запази и където е необходимо, да увеличи европейското участие в съответните органи по стандартизация, за да бъдат постигнати целите на Европа в областта на сигурността и оперативната съвместимост. По-специално Комисията, заедно с държавите членки, ще оценява и насърчава техническите спецификации и стандарти, чрез които се дава възможност за оперативна съвместимост между доставчиците на 5G оборудване в различни части на мрежата, включително в заварените мрежи, с цел да се позволи възникването на истинска среда с множество доставчици, например чрез отворени, оперативно съвместими интерфейси.

— **Сертифициране**: ще подкрепи разработването на схеми за 5G сертифициране, насочени към нуждите на 5G мрежите, в съответствие с рамката на ЕС за сертифициране на киберсигурността.

— **Скрининг на преките чуждестранни инвестиции (ПЧИ)**: ще подкрепи прилагането на рамката на ЕС за скрининг, като картографира веригата на стойността в областта на 5G, включително за чувствителни мрежови активи, и извършва редовен мониторинг на ПЧИ по веригата за създаване на стойност. Съгласно графика за скрининг на преките чуждестранни инвестиции (от октомври 2020 г.) Комисията ще упражнява контрол върху чуждестранните инвестиции в областта на 5G в съответствие с насоките, предвидени в Регламент (ЕС) 2019/452, като се съобразява с координираната оценка на риска на равнището на ЕС и инструментариума на ЕС.

— Инструменти за защита на търговията: ще наблюдава всички съответни пазарни тенденции в ЕС и в трети държави и ще защитава на европейския пазар на 5G участниците от ЕС посредством мерки за търговска защита, противодействащи на потенциални практики, нарушаващи търговията (дъмпинг или субсидиране), включително чрез започване на предварителни разследвания, когато е целесъобразно.

— Правила за конкуренция: ще наблюдава функционирането на пазарите за доставка на хардуер и софтуер за 5G технологии, с цел да се гарантира, че те предлагат конкурентни резултати, включително във връзка с евентуално възникване на ситуации на договорно или технологично блокиране.

— **Програми за финансиране от ЕС**: ще гарантира, че участието в програми за финансиране от ЕС в съответните технологични области ще зависи от спазването на изискванията за сигурност, като използва изцяло условията за сигурност в програмите за научни изследвания и иновации и разшири тяхното прилагане, по-специално в „Хоризонт Европа“, програмата „Цифрова Европа“ и Механизма за свързване на Европа 2, в европейските структурни и инвестиционни фондове и в други съответни програми. Подобен подход следва да бъде възприет и в програмите за външно финансиране и финансовите инструменти на ЕС, включително по отношение на финансирането, предоставяно чрез международни финансови институции.

— Обществени поръчки: ще привлече обществени поръчки в областта на 5G мрежите, за да подкрепи набелязаните цели по отношение на сигурността, разнообразието на доставчиците и дългосрочната устойчивост на 5G мрежите; по-специално, ще гарантира, че се вземат надлежно предвид аспектите на сигурността, когато се възлагат

обществени поръчки, свързани с 5G мрежите, в съответствие с правилата на ЕС за обществените поръчки.

— Реагиране при инциденти и управление на кризи (проект) и киберучения: ще се възползва пълноценно от разработването на проекта на ЕС[20] за координирана реакция при мащабни инциденти в областта на киберсигурността. Освен това ще разгледа съвместно с ENISA възможността за провеждане на 5G киберучение, веднага след като пазарът достигне необходимата за това зрелост.

Под ръководството на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност и заместник-председател на Комисията, и на Съвета:

— Рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството (инструментариум за кибердипломация)[21]: В случай на злонамерени действия в киберпространството, които застрашават целостта и сигурността на ЕС, държавите членки се насърчават да използват мерките по общата външна политика и политиката на сигурност от съответната част на инструментариума на ЕС за кибердипломация (включително, ако е необходимо, ограничителни мерки), за да се насърчи сътрудничеството, да се улесни смекчаването на заплахите и да се повлияе върху поведението на потенциалните агресори.

Освен това редица програми ще подпомагат постигането на целите за избягване или ограничаване на риска от дългосрочна зависимост, като насърчават развитието на разнообразен и устойчив пазар на 5G технологии, включително чрез поддържане на капацитета на ЕС във веригата за създаване на стойност при 5G технологии и чрез инвестиции в иновации, в съответствие с международните задължения на ЕС.

Насърчаване на иновации и инвестиции в киберсигурността и технологиите за мрежова инфраструктура:

— Програми за финансиране от ЕС: ще увеличи инвестициите в научни изследвания, иновации и внедряване на мрежовите технологии и техните съответни градивни елементи. Комисията предложи близо 3 милиарда евро инвестиции в областта на киберсигурността в рамките на следващия бюджет на ЕС за периода 2021—27 г. Това включва научни изследвания и иновации по линия на „Хоризонт Европа“ и подкрепа за способностите в областта на киберсигурността по линия на „Цифрова Европа“. По линия на InvestEU също може да се предоставя финансова подкрепа за научноизследователска и развойна дейност в областта на 5G технологиите, както и подкрепа за тяхното внедряване.

Освен това в рамките на следващата програма „Хоризонт Европа“[22] Комисията предлага създаването на институционализирано партньорство на ЕС относно NGI/6G („интелигентни мрежи и услуги“) в сътрудничество с промишлеността и в координация с държавите членки, чиято цел е да завърши внедряването на 5G и най-вече да **подготви почвата за 6G** — следващото поколение мобилни технологии. От

[20] Препоръка на Комисията относно координирана реакция при мащабни киберинциденти и кризи (ЕС 2017/1584).
[21] Заключения на Съвета от 20 ноември 2017 г. (9916/17).
[22] Финансиране може да бъде предоставено и по програмите „Механизъм за свързване на Европа 2.0“ и „Цифрова Европа“.

бюджета на ЕС (2021—27 г.) бяха предложени над 2,5 милиарда евро инвестиции за тази инициатива, които трябва да привлекат поне 7,5 милиарда евро частни инвестиции.

— **Промишлено развитие и внедряване**: ще направи оценка на потенциалните пазарни недостатъци или пропуски по веригата на стойността в областта на 5G, които биха оправдали целенасочени намеси в следващия дългосрочен бюджет или възможен важен проект от общоевропейски интерес (ВПОИ) в областта на киберсигурността, в съответствие с предложенията на форума на високо равнище за ВПОИ. Решението за разработване и създаване на важни проекти от общоевропейски интерес зависи от държавите членки и предприятията. Правилата на ЕС осигуряват благоприятна рамка и Комисията е готова да улесни необходимите контакти и да предостави насоки.

6. Заключение

5G мрежите имат потенциала да създадат редица възможности за европейските граждани, обществото и икономиката. Поради това гарантирането на сигурността и стабилността на 5G мрежите е от основно значение. В същото време заплахите за киберсигурността (включително рискът от намеса на държавни или подкрепяни от държавата участници от държави извън ЕС) са предизвикателство, което се развива и чието значение нараства успоредно с използването на технологии и данни. Пренебрегването на киберсигурността би подкопало доверието в развитието на цифровата икономика и общество и би попречило на ЕС да се възползва в пълна степен от това развитие. Затова реакцията трябва да е съответно адаптирана и засилена.

Използването на координиран и последователен подход към киберсигурността в ЕС по отношение на критични технологии и мрежи е от съществено значение, за да може ЕС да гарантира своя технологичен суверенитет и да поддържа и развива промишления си капацитет. Комисията ще подкрепи напълно прилагането на подхода на ЕС към киберсигурността на 5G мрежите и същевременно ще гарантира, че пазарите на ЕС остават отворени за продукти и услуги, съобразени с развиващите се изисквания за киберсигурност и доверие.

За тази цел е важно ангажиментът на всички заинтересовани страни във връзка със сигурността на 5G технологиите да остане висок, като ще се изисква постоянно сътрудничество между държавите членки, Комисията и ENISA.

Като непосредствена следваща стъпка, както е посочено по-горе, Комисията призовава държавите членки да предприемат бързи действия за ефективно и обективно прилагане на мерките, договорени като част от инструментариума, и да продължат да работят съвместно, с подкрепата на Комисията и ENISA, за осигуряването на координация на равнище ЕС. Успоредно с това Комисията ще стартира всички съответни действия в рамките на своите правомощия, за да подкрепи прилагането на инструментариума от държавите членки и да засили неговото въздействие.

Допълнение: Категории риск (източник: Координирана оценка на риска на равнището на ЕС)

	Категории риск
Рискови сценарии във връзка с недостатъчни мерки за сигурност	*R1: Неправилна конфигурация на мрежите*
	R2: Липса на контрол на достъпа
Рискови сценарии във връзка с веригата на доставка на 5G	*R3: Ниско качество на продуктите*
	R4: Зависимост от отделен доставчик в рамките на отделни мрежи или липса на многообразие на общонационална основа
Рискови сценарии във връзка с начина на действие на основните участници в заплахи	*R5: Държавна намеса чрез веригата на доставки на 5G технологии*
	R6: Зловредно използване на 5G мрежите от организираната престъпност или организирана престъпна група, ориентирано към крайните потребители
Рискови сценарии във връзка с взаимозависимостите между 5G мрежите и други системи с критично значение	*R7: Съществени смущения в работата на критични инфраструктури или услуги*
	R8: Широкообхватен отказ на мрежи, дължащ се на прекъсване на електроснабдяването или на други поддържащи системи
Рискови сценарии във връзка с устройствата за крайни потребители	*R9: Зловредно използване на интернет на нещата*