|  |  |
| --- | --- |
| Европейски парламент  2014—2019 |  |

**ПРИЕТИ ТЕКСТОВЕ**

P8\_TA(2019)0156

Заплахи за сигурността във връзка с нарастващото технологично присъствие на Китай в ЕС и възможни действия на равнището на ЕС за тяхното намаляване

PE635.406

Резолюция на Европейския парламент от 12 март 2019 г. относно заплахите за сигурността във връзка със засилващото се технологично присъствие на Китай в ЕС и възможни действия на равнището на ЕС за ограничаването им (2019/2575(RSP))

*Европейският парламент,*

— като взе предвид Директива (EС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения[[1]](#footnote-1),

— като взе предвид 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[[2]](#footnote-2),

— като взе предвид Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета[[3]](#footnote-3),

— като взе предвид предложението на Комисията от 13 септември 2017 г. за регламент на Европейския парламент и на Съвета относно ENISA – Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“) (COM(2017)0477),

— като взе предвид предложението на Комисията от 12 септември 2018 г. за регламент за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове (COM(2018)0630),

— като взе предвид приемането от Общокитайското събрание на народните представители на 28 юни 2017 г. на новия закон за националното разузнаване,

— като взе предвид изявленията на Съвета и на Комисията от 13 февруари 2019 г. относно заплахите за сигурността във връзка с нарастващото технологично присъствие на Китай в ЕС и възможни действия на равнището на ЕС за ограничаването им,

— като взе предвид приемането от страна на австралийското правителство на реформи в областта на сигурността на телекомуникационния сектор, които влязоха в действие на 18 септември 2018 г.,

— като взе предвид своята позиция, приета на първо четене на 14 февруари 2019 г., относно предложението за регламент на Европейския парламент и на Съвета за създаване на рамка за скрининг на преки чуждестранни инвестиции в Европейския съюз[[4]](#footnote-4),

— като взе предвид предишните си резолюции относно отношенията между ЕС и Китай, и по-специално тази от 12 септември 2018 г.[[5]](#footnote-5),

— като взе предвид съобщението на Комисията от 14 септември 2016 г., озаглавено „5G за Европа: план за действие“ (COM(2016)0588),

— като взе предвид своята резолюция от 1 юни 2017 г. относно свързаността с интернет за целите на растежа, конкурентоспособността и сближаването: европейското общество в ерата на гигабитовия интернет и технологиите от пето поколение (5G)[[6]](#footnote-6),

— като взе предвид Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/EО (Общ регламент относно защитата на данните)[[7]](#footnote-7),

— като взе предвид Регламент (ЕС) № 1316/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. за създаване на Механизъм за свързване на Европа, за изменение на Регламент (ЕС) № 913/2010 и за отмяна на регламенти (ЕО) № 680/2007 и (ЕО) № 67/2010[[8]](#footnote-8),

— като взе предвид предложението на Комисията от 6 юни 2018 г. за регламент на Европейския парламент и на Съвета за създаване на програмата „Цифрова Европа“ за периода 2021 – 2027 г. (COM(2018)0434),

— като взе предвид член 123, параграфи 2 и 4 от своя Правилник за дейността,

А. като има предвид, че ЕС трябва да даде тласък на своята програма за киберсигурността, за да може да реализира потенциала си да заеме лидерска позиция в областта на киберсигурността и да използва това в полза на своята индустрия;

Б. като има предвид, че уязвимите места в мрежите 5G биха могли да се използват за излагане на риск на информационните системи, което би могло да причини много сериозни вреди на икономиките на европейско и национално равнище; като има предвид, че е необходим подход, основан на анализ на риска по цялата верига за създаване на стойност, за да може рисковете да бъдат сведени до минимум;

В. като има предвид, че мрежата 5G ще бъде гръбнакът на нашата цифрова инфраструктура, като разширява възможностите за свързване на различни устройства към мрежите (интернет на нещата и др.), и ще донесе нови ползи и възможности за обществото и предприятията в много области, включително в централни сектори на икономиката като транспорта, енергетиката, здравеопазването, финансите, далекосъобщенията, отбраната, космическото пространство и сигурността;

Г. като има предвид, че създаването на подходящ механизъм за реагиране на предизвикателствата във връзка със сигурността би дало на ЕС възможност да предприеме активни стъпки за въвеждане на стандарти за 5G;

Д. като има предвид, че бяха изразени опасения относно търговците на оборудване от трети държави, които биха могли да представляват риск за сигурността на ЕС поради законите на тяхната държава на произход, особено след влизането в сила на китайските закони за държавната сигурност, които налагат на всички граждани, предприятия и други субекти задължения за сътрудничество с държавата с цел защита на държавната сигурност, при много широко определение за „национална сигурност“; като има предвид, че няма гаранция, че тези задължения не се прилагат извънтериториално, и като има предвид, че реакциите в различните държави спрямо китайските разпоредби варираха от оценки на сигурността до пълна забрана;

Е. като има предвид, че през декември 2018 г. чешкият национален орган за киберсигурност излезе с предупреждение за заплахи за сигурността, породени от технологиите, доставяни от китайските дружества Huawei и ZTE; като има предвид, че в следствие от това през януари 2019 г. чешките данъчни органи изключиха Huawei от търг за създаване на данъчен портал;

Ж. като има предвид, че е необходимо задълбочено разследване, за да се изясни дали въпросните изделия или каквито и да било други устройства или доставчици създават рискове за сигурността поради някои характеристики, като например скритите възможности за достъп до системите (т.нар. „задни вратички“);

З. като има предвид, че решенията следва да се координират и разглеждат на равнището на ЕС, за да се избегне създаването на различни нива на сигурност и потенциални пропуски в областта на киберсигурността, като същевременно е необходима координация на световно равнище, за да се реагира решително спрямо този проблем;

И. като има предвид, че ползите от единния пазар са свързани със задължението за прилагане на стандартите на ЕС и правната рамка на Съюза, и че доставчиците не следва да бъдат третирани различно въз основа на тяхната държава на произход;

Й. като има предвид, че регламентът относно скрининга на преките чуждестранни инвестиции, който следва да влезе в сила до края на 2020 г., увеличава възможностите на държавите членки да извършват скрининг на чуждестранните инвестиции въз основа на критерии, свързани със сигурността и обществения ред, и създава механизъм за сътрудничество, който позволява на Комисията и на държавите членки да си сътрудничат при оценката на рисковете за сигурността, включително рисковете за киберсигурността, породени от чувствителни чуждестранни инвестиции, а също така обхваща проекти и програми, които представляват интерес за ЕС, като например Трансевропейските мрежи в областта на телекомуникационната инфраструктура и програмата „Хоризонт 2020“;

1. счита, че Съюзът трябва да играе водеща роля в областта на киберсигурността чрез прилагането на общ подход, основан на ефективното и ефикасно използване на експертния опит на ЕС, на държавите членки и на сектора, тъй като многообразието от различни национални решения може да окаже неблагоприятно въздействие върху цифровия единен пазар;

2. изразява дълбока загриженост относно неотдавнашните твърдения, че оборудване 5G, разработено от китайски дружества, може да има вградени „задни вратички“, които предоставят на производителите и на органите възможност за неразрешен достъп до частни и лични данни и съобщения от ЕС;

3. изразява също така загриженост относно потенциалното наличие на значителни уязвими места в оборудването 5G, разработено от тези производители, при евентуалното му инсталиране във връзка с разгръщането на мрежите 5G през идните години;

4. подчертава, че последиците за сигурността на мрежите и оборудването са сходни по целия свят и призовава ЕС да извлече поуки от наличния опит, за да може да гарантира възможно най-високи стандарти на киберсигурност; призовава Комисията да разработи стратегия, която да осигури на Европа водеща позиция в областта на технологиите за киберсигурност и да цели намаляване на зависимостта на Европа от чуждестранни технологии в областта на киберсигурността; изразява становището, че когато спазването на изискванията за сигурност не може да бъде гарантирано, трябва да се прилагат адекватни мерки;

5. призовава държавите членки да информират Комисията за всякакви национални мерки, които възнамеряват да приемат, за да координират реакцията на Съюза, с цел да се гарантират най-високи стандарти за киберсигурност в целия Съюз, и отново изтъква, че е важно държавите да се въздържат от въвеждането на непропорционални едностранни мерки, които биха довели до разпокъсване на единния пазар;

6. отново заявява, че субектите, които доставят оборудване или услуги в ЕС, независимо от тяхната държава на произход, трябва да спазват задълженията, свързани с основните права, правото на ЕС и законодателството на държавите членки, включително правната уредба относно неприкосновеността на личния живот, защитата на данните и киберсигурността;

7. призовава Комисията да извърши оценка на надеждността на правната рамка на Съюза, за да се разсеят опасенията за наличие на уязвимо оборудване в стратегически сектори и опорна инфраструктура; настоятелно призовава Комисията да представи инициативи, включително, когато е целесъобразно, законодателни предложения, с цел своевременно предприемане на мерки във връзка с всякакви установени слабости, тъй като Съюзът е в постоянен процес на идентифициране и справяне с предизвикателствата пред киберсигурността и на повишаване на нейната устойчивост в ЕС;

8. настоятелно призовава онези държави членки, които все още не са транспонирали напълно Директивата за мрежовата и информационната сигурност (МИС), да направят това незабавно, и призовава Комисията да следи отблизо това транспониране, за да гарантира, че разпоредбите се изпълняват и налагат правилно и че за европейските граждани е осигурена по-добра защита от външни и вътрешни заплахи за сигурността;

9. настоятелно призовава Комисията и държавите членки да гарантират, че механизмите за докладване, въведени с Директивата за МИС, се прилагат правилно; отбелязва, че Комисията и държавите членки следва да проследяват внимателно всякакви инциденти във връзка със сигурността или неподходяща реакция от страна на доставчиците, с цел преодоляване на установените пропуски;

10. призовава Комисията да оцени необходимостта от допълнително разширяване на обхвата на Директивата за МИС, така че да бъдат включени и други сектори и услуги от критично значение, които не са обхванати от специфично за сектора законодателство;

11. приветства и подкрепя постигнатото споразумение относно Акта за киберсигурността и укрепването на мандата на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) с цел оказване на по-добра подкрепа на държавите членки за справяне със заплахите за киберсигурността и атаките към нея;

12. настоятелно призовава Комисията да предостави мандат на ENISA да даде приоритет на работата по схема за сертифициране на оборудване 5G, за да се гарантира, че разгръщането на 5G в Съюза отговаря на най-високите стандарти за сигурност и е устойчиво спрямо „задни вратички“ или сериозни уязвими пунктове, които биха застрашили сигурността на далекосъобщителните мрежи и зависещите от тях служби на Съюза; препоръчва да се обърне специално внимание на повсеместно използваните процеси, продукти и софтуер, които поради самия си мащаб оказват значително въздействие върху ежедневието на гражданите и икономиката;

13. горещо приветства предложенията за центрове за компетентност в областта на киберсигурността и за мрежа от национални координационни центрове, проектирани с цел подпомагане на ЕС да запази и развие технологичния и индустриалния капацитет в областта на киберсигурността, който е необходим за осигуряване на цифровия единен пазар; припомня обаче, че сертифицирането не следва да изключва упражняването на контрол от страна на компетентните органи и операторите над веригата на доставки, за да се гарантира почтеността и сигурността на тяхното оборудване, което функционира в чувствителни от гледна точка на сигурността среди и далекосъобщителни мрежи;

14. припомня, че киберсигурността налага високи стандарти за сигурност; призовава за изграждането на мрежа, която да бъде сигурна по подразбиране, още от етапа на проектиране; настоятелно призовава държавите членки, заедно с Комисията, да проучат всички налични средства за осигуряване на високо равнище на сигурност;

15. призовава Комисията и държавите членки, в сътрудничество с ENISA, да предоставят насоки относно начините за справяне с киберзаплахите и уязвимите места при възлагането на обществени поръчки за оборудване 5G, например чрез диверсифициране на оборудването от различни доставчици или чрез въвеждане на многоетапни процедури за възлагане на обществени поръчки;

16. потвърждава своята позиция относно програмата „Цифрова Европа“, която налага изисквания за сигурност и надзор от страна на Комисията върху субекти, установени в ЕС, но контролирани от трети държави, по-специално по отношение на действията, свързани с киберсигурността;

17. призовава държавите членки да гарантират, че публичните институции и частните дружества, които участват в обезпечаването на правилното функциониране на важни инфраструктурни мрежи, като например в сферата на далекосъобщенията, енергетиката, здравните и социалните системи, извършват съответни оценки на риска, като вземат предвид заплахите за сигурността, свързани по-специално с техническите характеристики на съответната система или зависимостта от външни доставчици на хардуерни и софтуерни технологии;

18. припомня, че настоящата правна рамка относно далекосъобщенията изисква от държавите членки да гарантират, че телекомуникационните оператори спазват изискванията за непокътнатост и наличност на обществените електронни съобщителни мрежи, включително, по целесъобразност, криптиране от край до край; подчертава, че съгласно Европейския кодекс за електронни съобщения държавите членки разполагат с широки правомощия да разследват продукти на пазара на ЕС и да прилагат широк набор от средства за правна защита в случай на тяхното несъответствие с правилата;

19. призовава Комисията и държавите членки да превърнат сигурността в задължителен аспект на всички процедури за възлагане на обществени поръчки по отношение на съответната инфраструктура на равнището на ЕС и на национално равнище;

20. припомня на държавите членки за тяхното задължение съгласно правната рамка на ЕС, по-специално Директива 2013/40/ЕС относно атаките срещу информационни системи, да налагат санкции на юридически лица, които са извършили престъпления, като например атаки срещу такива системи; подчертава, че държавите членки следва също така да се възползват от своята способност за налагане на други санкции на тези правни субекти, като например временно или постоянно лишаване от правото да упражняват търговска дейност;

21. призовава държавите членки, агенциите за киберсигурност, далекосъобщителните оператори, производителите и доставчиците на услуги за критична инфраструктура да докладват на Комисията и на ENISA всички доказателства за „задни вратички“ или други сериозни уязвими места, които биха могли да изложат на риск целостта и сигурността на далекосъобщителните мрежи или да нарушат правото на Съюза и основните права; очаква от националните органи по защита на данните, както и от Европейския надзорен орган по защита на данните, да проучват задълбочено сведенията за злоупотреба с лични данни от страна на външни доставчици и да налагат подходящи глоби и санкции, в съответствие с европейското право в областта на защитата на данните;

22. приветства предстоящото влизане в сила на регламента за създаване на рамка за скрининг на преките чуждестранни инвестиции (ПЧИ) по съображения, свързани със сигурността и обществения ред, и подчертава, че с този регламент за първи път се въвежда списък на области и фактори, включително комуникациите и киберсигурността, които са от значение за сигурността и обществения ред на равнището на ЕС;

23. призовава Съвета да ускори работата си по предложението за Регламент за неприкосновеността на личния живот и електронните съобщения;

24. отново заявява, че ЕС трябва да подкрепя киберсигурността по цялата верига на създаване на стойност – от научните изследвания до внедряването и използването на ключови технологии – да разпространява подходяща информация и да насърчава киберхигиената и образователните програми, които включват киберсигурността, и счита че, наред с други мерки, програмата „Цифрова Европа“ ще бъде ефикасен инструмент за това;

25. настоятелно призовава Комисията и държавите членки да предприемат необходимите мерки, включително стабилни инвестиционни схеми, за създаването на благоприятна за иновациите среда в ЕС, която да бъде достъпна за всички предприятия в цифровата икономика на ЕС, включително за малките и средните предприятия (МСП); освен това настоява тази среда да позволява на европейските търговци да разработват нови продукти, услуги и технологии, които биха им позволили да бъдат конкурентоспособни;

26. настоятелно призовава Комисията и държавите членки да вземат предвид горепосочените искания в рамките на предстоящите обсъждания относно бъдещата стратегия „ЕС – Китай“ като предварителни условия, за да може ЕС да запази своята конкурентоспособност и да гарантира сигурността на своята цифрова инфраструктура;

27. възлага на своя председател да предаде настоящата резолюция на Съвета и на Комисията.

1. OВ L 321, 17.12.2018 г., стр. 36. [↑](#footnote-ref-1)
2. OВ L 194, 19.7.2016 г., стр. 1. [↑](#footnote-ref-2)
3. OВ L 218, 14.8.2013 г., стр. 8. [↑](#footnote-ref-3)
4. Приети текстове, P8\_TA(2019)0121. [↑](#footnote-ref-4)
5. Приети текстове, P8\_TA(2018)0343. [↑](#footnote-ref-5)
6. ОВ C 307, 30.8.2018 г., стр. 144. [↑](#footnote-ref-6)
7. ОВ L 119, 4.5.2016 г., стр. 1. [↑](#footnote-ref-7)
8. ОВ L 348, 20.12.2013 г., стр. 129. [↑](#footnote-ref-8)