Európsky parlament
2014-2019

PRIJATÉ TEXTY

P8_TA(2019)0156

Bezpečnostné hrozby súvisiace so zvyšujúcou sa technologickou prítomnosťou Číny v EÚ a prípadné opatrenia na úrovni EÚ na ich znižovanie

Uznesenie Európskeho parlamentu z 12. marca 2019 o bezpečnostných hrozbách súvisiacich so zvyšujúcou sa čínskou technologickou prítomnosťou v EÚ a možných opatreniach na úrovni EÚ na ich zníženie (2019/2575(RSP))

Európsky parlament,

– so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií[1],

– so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii[2],

– so zreteľom na smernicu Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV[3],

– so zreteľom na návrh nariadenia Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“) (COM(2017)0477), predložený Komisiou 13. septembra 2017,

– so zreteľom na návrh nariadenia, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (COM(2018)0630), predložený Komisiou 12. septembra 2018,

– so zreteľom na prijatie nového zákona o národnej spravodajskej službe čínskym Národným ľudovým kongresom 28. júna 2017,

---

1 Ú. v. EÚ L 321, 17.12.2018, s. 36.
2 Ú. v. EÚ L 194, 19.7.2016, s. 1.
3 Ú. v. EÚ L 218, 14.8.2013, s. 8.

– so zreteľom na vyhlásenia Rady a Komisie z 13. februára 2019 o bezpečnostných hrozbách súvisiacich so zvyšujúcou sa čínskou technologickou prítomnosťou v EÚ a možných opatreniach na úrovni EÚ na ich zníženie,

– so zreteľom na skutočnosť, že austrálska vláda prijala reformy bezpečnosti telekomunikačného sektora vlády, ktoré nadobudli účinnosť 18. septembra 2018,

– so zreteľom na svoju pozíciu prijatú v prvom čítaní 14. februára 2019 k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií do Európskej únie[1],

– so zreteľom na svoje predchádzajúce uznesenia o stave vzťahov EÚ a Číny, najmä na uznesenie z 12. septembra 2018[2],

– so zreteľom na oznámenie Komisie zo 14. septembra 2016 s názvom 5G pre Európu: akčný plán (COM(2016)0588),

– so zreteľom na svoje uznesenie z 1. júna 2017 o pripojení na internet pre rast, konkurencieschopnosť a súdržnosť: európska gigabitová spoločnosť a 5G[3],

– so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)[4],

– so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 1316/2013 z 11. decembra 2013 o zriadení Nástroja na prepájanie Európy, ktorým sa mení nariadenie (EÚ) č. 913/2010 a zrušujú nariadenia (ES) č. 680/2007 a (ES) č. 67/2010[5],

– so zreteľom na návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje program Digitálna Európa na obdobie 2021 – 2027 (COM(2018)0434), predložený Komisiou 6. júna 2018,

– so zreteľom na článok 123 ods. 2 a 4 rokovacieho poriadku,

A. keďže EÚ musí presadzovať svoj program v oblasti kybernetickej bezpečnosti s cieľom naplniť svoj potenciál stať sa vedúcim aktérom v oblasti kybernetickej bezpečnosti a využiť to v prospech svojho priemyslu;

B. keďže zraniteľné miesta v sieťach 5G by mohli byť zneužité na ohrozenie IT systémov, čo by mohlo spôsobiť veľmi vážne škody hospodárstvam na európskej a vnútroštátnej úrovni; keďže na minimalizáciu rizík je potrebný prístup založený na analýze rizika v celom hodnotovom reťazci;

C. keďže sieť 5G bude nosným pilierom našej digitálnej infraštruktúry, rozšíri možnosť pripojenia rôznych zariadení do sietí (internet vecí atď.) a prinesie spoločnosti

---

1 Prijaté texty, P8_TA(2019)0121.
2 Prijaté texty, P8_TA(2018)0343.
3 Ú. v. EÚ C 307, 30.8.2018, s. 144.
4 Ú. v. EÚ L 119, 4.5.2016, s. 1.
5 Ú. v. EÚ L 348, 20.12.2013, s. 129.

a podnikom nové výhody a príležitosti v mnohých oblastiach vrátane rozhodujúcich odvetví hospodárstva, ako sú odvetvia dopravy, energetiky, zdravotníctva, financií, telekomunikácií, obrany, kozmického priestoru a bezpečnosti;

D. keďže vytvorenie vhodného mechanizmu na riešenie bezpečnostných výziev by EÚ umožnilo aktívne prijímať opatrenia na stanovenie noriem pre 5G;

E. keďže boli vznesené obavy týkajúce sa predajcov zariadení z tretích krajín, ktorí by mohli predstavovať bezpečnostné riziko pre EÚ v dôsledku právnych predpisov ich krajiny pôvodu, a to najmä po prijatí čínskych zákonov o štátnej bezpečnosti, v ktorých sa stanovujú povinnosti pre všetkých občanov, podniky a ďalšie subjekty, aby spolupracovali so štátom s cieľom zaručiť jeho bezpečnosť, v spojení s veľmi širokým vymedzením národnej bezpečnosti; keďže neexistuje žiadna záruka, že tieto povinnosti sa neuplatňujú extrateritoriálne, a keďže reakcie na čínske právne predpisy sa v jednotlivých krajinách líšili, od bezpečnostných hodnotení až po úplný zákaz;

F. keďže v decembri 2018 český národný orgán pre kybernetickú bezpečnosť vydal varovanie pred bezpečnostnými hrozbami, ktoré predstavujú technológie poskytované čínskymi spoločnosťami Huawei a ZTE; keďže následne české daňové orgány v januári 2019 vylúčili spoločnosť Huawei z verejnej súťaže na vytvorenie daňového portálu;

G. keďže je potrebné dôkladné vyšetrenie, aby sa objasnilo, či uvedené zariadenia alebo akékoľvek iné zariadenia alebo dodávatelia predstavujú bezpečnostné riziká v dôsledku takých prvkov, ako sú napríklad zadné dvierka do systémov;

H. keďže riešenia by sa mali koordinovať a hľadať na úrovni EÚ, aby sa zabránilo vytváraniu rôznych úrovní bezpečnosti a možným medzerám v kybernetickej bezpečnosti, pričom na zabezpečenie silnej reakcie je potrebná koordinácia na globálnej úrovni;

I. keďže výhody jednotného trhu sú spojené s povinnosťou dodržiavať normy EÚ a právny rámec Únie a keďže s dodávateľmi by sa nemalo zaobchádzať inak na základe krajiny ich pôvodu;

J. keďže nariadenie o preverovaní priamych zahraničných investícií, ktoré by malo nadobudnúť účinnosť koncom roku 2020, posilňuje schopnosť členských štátov preverovať zahraničné investície z hľadiska kritérií bezpečnosti a verejného poriadku a vytvára mechanizmus spolupráce, ktorý Komisii a členským štátom umožňuje spolupracovať pri posudzovaní bezpečnostných rizík vrátane rizík pre kybernetickú bezpečnosť, ktoré predstavujú citlivé zahraničné investície, a vzťahuje sa aj na projekty a programy, ktoré sú v záujme EÚ, ako sú transeurópske siete pre telekomunikácie a program Horizont 2020;

1. domnieva sa, že Únia musí zaujať vedúce postavenie v oblasti kybernetickej bezpečnosti, a to prostredníctvom spoločného prístupu založeného na účinnom a efektívnom využívaní odborných znalostí EÚ, členských štátov a priemyslu, pretože rôzne vnútroštátne rozhodnutia by mali negatívny vplyv na digitálny jednotný trh;

2. vyjadruje hlboké znepokojenie nad nedávnymi obvineniami, že zariadenia 5G, ktoré vyvinuli čínske spoločnosti, môžu obsahovať zadné dvierka, ktoré by výrobcom a orgánom umožňovali neoprávnený prístup k súkromným a osobným údajom

a telekomunikáciám z EÚ;

3. je rovnako znepokojený možnou prítomnosťou významných zraniteľných miest v zariadeniach 5G, ktoré vyvinuli títo výrobcovia, keby sa nainštalovali pri zavádzaní sietí 5G v nadchádzajúcich rokoch;

4. zdôrazňuje, že dôsledky pre bezpečnosť sietí a zariadení sú na celom svete podobné, a vyzýva EÚ, aby sa poučila zo skúseností, ktoré sú k dispozícii, a mohla tak zabezpečiť najvyššie normy kybernetickej bezpečnosti; vyzýva Komisiu, aby vypracovala stratégiu, ktorá Európe zabezpečí vedúcu pozíciu v oblasti technológií kybernetickej bezpečnosti a bude zameraná na zníženie európskej závislosti od zahraničných technológií v oblasti kybernetickej bezpečnosti; zastáva názor, že vždy, keď nie je možné zaručiť súlad s bezpečnostnými požiadavkami, sa musia uplatniť primerané opatrenia;

5. vyzýva členské štáty, aby informovali Komisiu o všetkých vnútroštátnych opatreniach, ktoré zamýšľajú prijať, aby bolo možné koordinovať reakciu Únie s cieľom zabezpečiť najprísnejšie normy kybernetickej bezpečnosti v celej Únii, a opätovne zdôrazňuje, že je dôležité upustiť od zavádzania neprimeraných jednostranných opatrení, ktoré by rozdrobili jednotný trh;

6. opätovne zdôrazňuje, že všetky subjekty, ktoré poskytujú zariadenia alebo služby v EÚ, musia bez ohľadu na krajinu pôvodu dodržiavať záväzky v oblasti základných práv a právne predpisy EÚ a členských štátov vrátane právneho rámca týkajúceho sa súkromia, ochrany údajov a kybernetickej bezpečnosti;

7. vyzýva Komisiu, aby posúdila spoľahlivosť právneho rámca Únie s cieľom riešiť obavy týkajúce sa prítomnosti zraniteľných zariadení v strategických odvetviach a základnej infraštruktúre; naliehavo vyzýva Komisiu, aby predložila iniciatívy, v prípade potreby vrátane legislatívnych návrhov, s cieľom včas riešiť všetky zistené nedostatky, pretože Únia je v neustálom procese určovania a riešenia výziev v oblasti kybernetickej bezpečnosti a zvyšovania odolnosti v oblasti kybernetickej bezpečnosti v EÚ;

8. naliehavo vyzýva tie členské štáty, ktoré zatiaľ v plnej miere netransponovali smernicu NIS, aby tak bezodkladne urobili, a vyzýva Komisiu, aby túto transpozíciu pozorne monitorovala s cieľom zabezpečiť, aby sa jej ustanovenia riadne uplatňovali a presadzovali a aby európski občania boli lepšie chránení pred vonkajšími a vnútornými bezpečnostnými hrozbami;

9. naliehavo vyzýva Komisiu a členské štáty, aby zabezpečili riadne uplatňovanie mechanizmov podávania správ zavedených smernicou NIS; konštatuje, že Komisia a členské štáty by sa mali dôkladne zaoberať všetkými bezpečnostnými incidentmi alebo neprimeranými reakciami dodávateľov s cieľom riešiť zistené nedostatky;

10. vyzýva Komisiu, aby posúdila potrebu ďalšieho rozšírenia pôsobnosti smernice NIS na ďalšie kritické odvetvia a služby, na ktoré sa nevzťahujú osobitné odvetvové právne predpisy;

11. víta a podporuje dosiahnutú dohodu o akte o kybernetickej bezpečnosti a posilnení mandátu Agentúry EÚ pre sieťovú a informačnú bezpečnosť (ENISA) s cieľom lepšie podporovať členské štáty v boji proti hrozbám a útokom v oblasti kybernetickej bezpečnosti;

12. naliehavo vyzýva Komisiu, aby agentúru ENISA poverila prioritnou prácou na systéme certifikácie zariadení 5G s cieľom zabezpečiť, aby zavádzanie 5G v Únii spĺňalo najvyššie bezpečnostné normy a bolo odolné voči zadným dvierkam alebo závažným zraniteľnostiam, ktoré by ohrozili bezpečnosť telekomunikačných sietí Únie a závislých služieb; odporúča, aby sa osobitná pozornosť venovala bežne používaným procesom, výrobkom a softvéru, ktoré už len svojou rozšírenosťou majú významný vplyv na každodenný život občanov a hospodárstva;

13. veľmi víta návrhy týkajúce sa centier kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier, ktoré majú pomôcť EÚ udržať a rozvíjať technologické a priemyselné kapacity v oblasti kybernetickej bezpečnosti, ktoré sú potrebné na zabezpečenie digitálneho jednotného trhu; pripomína však, že certifikácia by nemala vylučovať príslušné orgány a prevádzkovateľov z kontroly dodávateľského reťazca s cieľom zaistiť integritu a bezpečnosť ich zariadení, ktoré fungujú v kritických prostrediach a telekomunikačných sieťach;

14. pripomína, že kybernetická bezpečnosť si vyžaduje prísne bezpečnostné normy; požaduje vytvorenie siete, ktorá je zabezpečená automaticky a už v štádiu návrhu; naliehavo vyzýva členské štáty, aby spolu s Komisiou preskúmali všetky dostupné prostriedky na zaistenie vysokej úrovne bezpečnosti;

15. vyzýva Komisiu a členské štáty, aby v spolupráci s agentúrou ENISA poskytli usmernenia o tom, ako riešiť kybernetické hrozby a zraniteľné miesta pri obstarávaní zariadení 5G, napríklad prostredníctvom diverzifikácie zariadení od rôznych dodávateľov alebo zavedenia viacfázových procesov verejného obstarávania;

16. opätovne potvrdzuje svoju pozíciu k programu Digitálna Európa, ktorý subjektom usadeným v EÚ, ale kontrolovaným z tretích krajín ukladá bezpečnostné požiadavky a dohľad Komisie, najmä v prípade činností súvisiacich s kybernetickou bezpečnosťou;

17. vyzýva členské štáty, aby zabezpečili, aby verejné inštitúcie a súkromné spoločnosti, ktoré sa podieľajú na zabezpečovaní riadneho fungovania sietí kritickej infraštruktúry, ako sú telekomunikačné, energetické, zdravotnícke a sociálne systémy, vykonávali príslušné posúdenia rizík, v ktorých zohľadnia bezpečnostné hrozby osobitne spojené s technickými vlastnosťami príslušného systému alebo závislosťou od externých dodávateľov hardvérových a softvérových technológií;

18. pripomína, že súčasný právny rámec pre telekomunikácie poveruje členské štáty, aby zabezpečili, aby telekomunikační operátori zachovávali integritu a dostupnosť verejných elektronických komunikačných sietí zahŕňajúcich podľa potreby šifrovanie bez medzifáz; zdôrazňuje, že podľa európskeho kódexu elektronickej komunikácie majú členské štáty rozsiahle právomoci skúmať výrobky na trhu EÚ a uplatňovať širokú škálu nápravných opatrení v prípade ich nesúladu;

19. vyzýva Komisiu a členské štáty, aby zaradili bezpečnosť medzi povinné aspekty všetkých postupov verejného obstarávania v súvislosti s relevantnou infraštruktúrou na úrovni EÚ aj na vnútroštátnej úrovni;

20. pripomína členským štátom ich povinnosť podľa právneho rámca EÚ, konkrétne smernice 2013/40/EÚ o útokoch na informačné systémy, ukladať sankcie právnickým osobám, ktoré sa dopustili trestných činov, ako sú útoky proti takýmto systémom;

zdôrazňuje, že členské štáty by mali využívať aj možnosť ukladať týmto právnickým osobám ďalšie sankcie, napríklad dočasné alebo trvalé vylúčenie z vykonávania komerčných činností;

21. vyzýva členské štáty, agentúry pre kybernetickú bezpečnosť, telekomunikačných operátorov, výrobcov a poskytovateľov služieb kritickej infraštruktúry, aby Komisii a agentúre ENISA oznámili akékoľvek dôkazy týkajúce sa zadných dvierok alebo iných závažných zraniteľných miest, ktoré by mohli ohroziť integritu a bezpečnosť telekomunikačných sietí alebo viesť k porušeniu práva Únie a základných práv; očakáva, že vnútroštátne orgány pre ochranu údajov, ako aj európsky dozorný úradník pre ochranu údajov dôkladne preskúmajú údajné porušenia ochrany osobných údajov externými dodávateľmi a uložia primerané pokuty a sankcie v súlade s európskymi právnymi predpismi o ochrane údajov;

22. víta nadchádzajúce nadobudnutie účinnosti nariadenia, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií z dôvodov bezpečnosti a verejného poriadku, a zdôrazňuje, že toto nariadenie prvýkrát stanovuje zoznam oblastí a faktorov, ktoré sú dôležité pre bezpečnosť a verejný poriadok na úrovni EÚ, zahŕňajúci komunikácie a kybernetickú bezpečnosť;

23. vyzýva Radu, aby urýchlila prácu na návrhu nariadenia o súkromí a elektronických komunikáciách;

24. opätovne zdôrazňuje, že EÚ musí podporovať kybernetickú bezpečnosť v rámci celého hodnotového reťazca od výskumu až po zavádzanie a využívanie kľúčových technológií, šíriť príslušné informácie a podporovať kybernetickú hygienu a učebné osnovy zahŕňajúce kybernetickú bezpečnosť, a domnieva sa, že popri iných opatreniach bude program Digitálna Európa efektívnym nástrojom na dosiahnutie tohto cieľa;

25. vyzýva Komisiu a členské štáty, aby podnikli potrebné kroky, ktoré zahŕňajú rozsiahle investičné systémy, na vytvorenie prostredia priaznivého pre inovácie v EÚ, ktoré by malo byť dostupné pre všetky podniky v digitálnom hospodárstve EÚ vrátane malých a stredných podnikov (MSP); ďalej naliehavo žiada, aby takéto prostredie umožňovalo európskym predajcom vyvíjať nové výrobky, služby a technológie, vďaka ktorým by boli konkurencieschopní;

26. naliehavo vyzýva Komisiu a členské štáty, aby v nadchádzajúcich diskusiách o budúcej stratégii EÚ voči Číne zohľadnili uvedené požiadavky ako základné predpoklady nato, aby EÚ bola naďalej konkurencieschopná a aby jej digitálna infraštruktúra bola bezpečná;

27. poveruje svojho predsedu, aby postúpil toto uznesenie Rade a Komisii.