Európsky parlament
2014-2019

Dokument na schôdzu

B8-0153/2019

6.3.2019

NÁVRH UZNESENIA

predložený na základe vyhlásení Rady a Komisie

v súlade s článkom 123 ods. 2 rokovacieho poriadku

o bezpečnostných hrozbách súvisiacich so zvyšujúcou sa čínskou technologickou prítomnosťou v EÚ a možných opatreniach na úrovni EÚ na ich zníženie
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
v mene skupiny EFDD

B8-0153/2019

Uznesenie Európskeho parlamentu 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 oznámenia Komisie zo 14. septembra 2016 s názvom Pripojenie pre konkurencieschopný jednotný digitálny trh – smerom k európskej gigabitovej spoločnosti (COM(2016)0587) a 5G pre Európu: akčný plán (COM(2016)0588),

– so zreteľom na návrh nariadenia Európskeho parlamentu a Rady z 29. januára 2016 pozmenený Komisiou o prístupe tovaru a služieb tretích krajín na vnútorný trh verejného obstarávania Únie a o postupoch podporujúcich rokovania o prístupe tovaru a služieb Únie na trhy verejného obstarávania tretích krajín (COM(2016)0034),

– 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[1] (smernica NIS),

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

– so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií[2],

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

– so zreteľom na prípad urovnania sporu v rámci WTO (WT/DS549/6) z 1. júna 2018 týkajúci sa určitých opatrení uložených Čínou v súvislosti s transferom zahraničných technológií do Číny,

– so zreteľom na svoju pozíciu prijatú v prvom čítaní 14. februára 2019 o návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií do Európskej únie[3],

– so zreteľom na súčasné rokovania medzi EÚ a Čínou o komplexnej dohode o investíciách,

[1] Ú. v. EÚ L 194, 19.7.2016, s. 1.
[2] Ú. v. EÚ L 321, 17.12.2018, s. 36.
[3] Prijaté texty, P8_TA(2019)0121.

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

A. keďže nedávny pokrok v oblasti IKT vrátane piatej generácie telekomunikačných technológií (5G) umožnil nové spôsoby výroby, distribúcie a realizácie tovarov a služieb a interakciu medzi zariadeniami a medzi občanmi, verejnými správami a inými sociálno-ekonomickými aktérmi, a má preto potenciál podporiť európske hospodárstvo;

B. keďže kybernetická bezpečnosť v IKT, ochrana citlivých informácií, dodržiavanie individuálnych práv a ochrana pred vonkajšími počítačovými hrozbami sú predpokladom pre zabezpečenie technologickej nezávislosti občanov EÚ a v konečnom dôsledku aj pre zabezpečenie prosperity a podpory demokracie v EÚ;

C. keďže výskum a testovanie technológie 5G len ťažko drží krok s medzinárodným tlakom na jej zavádzanie a uvádzanie na trh, zatiaľ čo množstvo vedeckých štúdií vyvoláva obavy a neistotu, pokiaľ ide o jej zabezpečenie, ako aj o bezpečnosť, najmä v súvislosti s rizikami elektromagnetického znečistenia pre ľudské zdravie a životné prostredie;

D. keďže zaručenie kybernetickej bezpečnosti pre siete 5G je novou a zložitou výzvou, a to kvôli virtuálnemu a decentralizovanému charakteru 5G a jeho rozdrobenému a vysoko špecializovanému hodnotovému reťazcu od výroby až po odoslanie, inštaláciu, konfiguráciu, prevádzku, údržbu a aktualizáciu softvéru; keďže EÚ musí vyriešiť nedostatky v oblasti kybernetickej bezpečnosti vo svojej kritickej infraštruktúre v odvetviach telekomunikácií, energetiky, dopravy, zdravotníctva, obrany a bezpečnosti a ďalších;

E. keďže zaručenie zabezpečených a bezpečných 5G sietí je úloha, ktorú nemôžu splniť jednotliví výrobcovia alebo prevádzkovatelia systémov, ale vyžaduje si účinné koordinované konanie všetkých príslušných vnútroštátnych a medzinárodných orgánov;

F. keďže EÚ má potenciál viesť vývoj technológií kybernetickej bezpečnosti prostredníctvom podpory európskych podnikov v tomto odvetví a presadzovaním všetkých zmien v hodnotovom reťazci, ktoré by mohli znížiť závislosť EÚ od zahraničných technológií;

G. keďže EÚ vypracovala súbor opatrení na zabezpečenie kybernetickej bezpečnosti vrátane smernice NIS a aktu o kybernetickej bezpečnosti, ktoré by sa mali urýchlene vykonávať a nepretržite monitorovať, aby sa zabezpečilo, že zostanú účinné aj po všetkých potrebných aktualizáciách a preskúmaniach;

H. keďže na trhu 5G v EÚ sa prejavuje zvýšená prítomnosť čínskych a iných poskytovateľov technológií z tretích krajín, najmä štátnych podnikov alebo netransparentných podnikov;

I. keďže reciprocita je jedným z najúčinnejších spôsobov, ako dosiahnuť pokrok v snahe o vytvorenie rovnakých podmienok na celosvetovej úrovni;

J. keďže zahraničné spoločnosti musia riešiť súčasnú medzeru v normách EÚ v oblasti ochrany údajov medzi všeobecným nariadením o ochrane údajov a rôznymi požiadavkami podľa vnútroštátnych právnych predpisov;

K. keďže EÚ a Čína rokujú o komplexnej dohode o investíciách od roku 2013; keďže navrhovaná dohoda by pomohla vyriešiť otázky prístupu na trh, vytvoriť rámec na ochranu investícií a stanoviť základné pracovné a environmentálne normy;

L. keďže sa objavili dôkazy, hoci nejednoznačné, pokiaľ ide o bezpečnostné nedostatky v zariadeniach, ktoré poskytujú dodávatelia z tretích krajín, vrátane Číny, ktoré by mohli ohroziť práva jednotlivcov na súkromie a ochranu citlivých informácií v EÚ;

1. zdôrazňuje, že zavádzanie a uvádzanie 5G na trh by sa malo uskutočňovať v súlade so zásadou predbežnej opatrnosti so všetkými sociálno-ekonomickými aktérmi, ktorí budú predvídať potenciálne vplyvy na bezpečnosť a ochranu a prijímať primerané preventívne opatrenia vrátane okamžitého odhaľovania faktorov, ktoré by mohli ohroziť verejné zdravie alebo životné prostredie;

2. zdôrazňuje, že sociálne a ekonomické vplyvy sietí 5G a technológií, ktoré umožňujú, od internetu vecí až po umelú inteligenciu, by sa mali dôkladne posúdiť a že by sa mali prijať opatrenia na to, aby sa prechod na európsku gigabitovú spoločnosť uskutočnil spravodlivým a rovnakým spôsobom pre všetkých a na základe etickej zodpovednosti;

3. vyzýva Komisiu a členské štáty, aby pre predajcov z EÚ vytvorili prostredie priaznivé pre inovácie na vývoj nových produktov, služieb a technológií a aby podporovali podnikateľský sektor EÚ pri zavádzaní a uvádzaní zabezpečených a bezpečných technológií 5G na trh, pričom by mali zároveň zabezpečiť, aby bol ich potenciál dostupný pre všetky podniky v digitálnom hospodárstve EÚ vrátane malých a stredných podnikov;

4. pripomína, že kybernetická bezpečnosť je jednou z hlavných výziev, ktorým EÚ v súčasnosti čelí, a že zlyhanie v tejto oblasti by mohlo porušiť súkromie a základné práva spotrebiteľov a výrobcov EÚ, vážne narušiť dôveru občanov v produkty a služby IKT a v konečnom dôsledku spôsobiť vážne hospodárske škody; vyzýva na vytvorenie siete, ktorá je zabezpečená štandardne aj podľa návrhu;

5. vyzýva Komisiu a členské štáty, aby úzko spolupracovali pri vykonávaní stratégie kybernetickej bezpečnosti EÚ a spájali opatrenia EÚ a vnútroštátne opatrenia s cieľom minimalizovať riziko narušenia bezpečnosti a ochrany údajov v celom hodnotovom reťazci; domnieva sa, že medzi takéto opatrenia by mohli patriť certifikácia kybernetickej bezpečnosti EÚ, požiadavky na konfiguráciu a prevádzkové postupy a praktiky, ako aj podpora kybernetickej hygieny a digitálneho vzdelávania;

6. domnieva sa, že agentúra EÚ pre kybernetickú bezpečnosť (Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť – ENISA) by mala zohrávať kľúčovú úlohu pri analyzovaní možných hrozieb vyplývajúcich zo strany zahraničných predajcov vrátane Číny a pri koordinácii spoločného prístupu členských štátov k riešeniu kybernetických hrozieb a útokov;

7. vyzýva Komisiu a členské štáty, aby urýchlene zaviedli balík predpisov o obehovom hospodárstve a posilnili nakladanie so surovinami v rámci ich životného cyklu, ako aj recykláciu odpadu s cieľom zlepšiť prístup EÚ ku kritickým surovinám, ktoré majú zásadný význam pre technologicky vyspelé výrobky a vznikajúce inovácie;

8. domnieva sa, že je naliehavo potrebné riešiť možné technologické bezpečnostné hrozby, ktoré predstavuje súčasný prienik zahraničných predajcov vrátane Číny na trh EÚ, spoločným prístupom k bezpečnosti a ochrane údajov medzi členskými štátmi;

9. vyzýva Komisiu a členské štáty, aby analyzovali a monitorovali bezpečnosť tých systémov IKT, v ktorých sa vo veľkej miere vyskytujú technológie tretích krajín, a to aj vykonávaním stresových testov;

10. zdôrazňuje, že dodávatelia z tretích krajín by nemali byť diskriminovaní na základe svojej krajiny pôvodu, ale že by sa mala zohľadniť transparentnosť týchto spoločností, ich kyberneticko-bezpečnostné normy a existencia podobných podmienok pre európske spoločnosti v ich krajine pôvodu, aby sa zabezpečili rovnaké podmienky;

11. zdôrazňuje, že čínski alebo iní dodávatelia a prevádzkovatelia z tretích krajín by za žiadnych okolností nemali ohroziť práva jednotlivcov zaručené právnymi predpismi EÚ, a to aj v prípade, že v ich krajine pôvodu existujú podľa vnútroštátneho práva iné požiadavky;

12. žiada Radu, aby pozitívne posúdila opätovné otvorenie diskusií o novom revidovanom návrhu Komisie o postupe, ktorým by sa obmedzil prístup zahraničných produktov na trh verejného obstarávania EÚ v prípade, že nie je umožnený vzájomný prístup;

13. pripomína, že je dôležité ďalej zlepšovať rokovania o regulačnej spolupráci v oblasti digitálnych technológií s tretími krajinami a zabezpečiť ich širšie pôsobenie v medzinárodných organizáciách pre normalizáciu;

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