Evropský parlament
2014-2019

Dokument ze zasedání

B8-0153/2019

6.3.2019

NÁVRH USNESENÍ

předložený na základě prohlášení Rady a Komise

v souladu s čl. 123 odst. 2 jednacího řádu

o bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v EU a o případných opatřeních přijatých na úrovni EU na jejich omezení
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
za skupinu EFDD

B8-0153/2019

Usnesení Evropského parlamentu o bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v EU a o případných opatřeních přijatých na úrovni EU na jejich omezení
(2019/2575(RSP))

Evropský parlament,

– s ohledem na sdělení Komise ze dne 14. září 2016 nazvané „Připojení pro konkurenceschopný jednotný digitální trh – na cestě k evropské gigabitové společnosti“ (COM(2016)0587) a na sdělení „Akční plán 5G pro Evropu“ (COM(2016)0588),

– s ohledem na pozměněný návrh nařízení Evropského parlamentu a Rady ze dne 29. ledna 2016 o přístupu zboží a služeb třetích zemí na vnitřní trh Unie s veřejnými zakázkami a o postupech na podporu jednání o přístupu zboží a služeb Unie na trhy třetích zemí s veřejnými zakázkami (COM(2016)0034),

– s ohledem na směrnici Evropského parlamentu a Rady (EU) č. 2016/1148 ze dne 6. července 2016 o opatřeních pro zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v celé Unii[1],

– s ohledem na návrh nařízení Evropského parlamentu a Rady ze dne 13. září 2017 o agentuře ENISA, „Agentuře EU pro kybernetickou bezpečnost“, a o zrušení nařízení (EU) 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“) (COM(2017)0477),

– s ohledem na směrnici Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace[2],

– s ohledem na návrh nařízení Evropského parlamentu a Rady ze dne 12. září 2018, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, jejž předložila Komise (COM(2018)0630),

– s ohledem na žádost o urovnání sporu podanou ke Světové obchodní organizaci dne 1 června 2018 (WT/DS549/6) týkající se některých opatření uložených Čínou ohledně transferu zahraničních technologií do Číny;

– s ohledem na svůj postoj přijatý v prvním čtení dne 14. února 2019 v souvislosti s návrhem nařízení Evropského parlamentu a Rady, kterým se stanoví rámec pro prověřování přímých zahraničních investic do Evropské unie[3],

– s ohledem na současná jednání mezi EU a Čínou o komplexní dohodě o investicích,

[1] Úř. věst. L 194, 19.7.2016, s. 1.
[2] Úř. věst. L 321, 17.12.2018, s. 36.
[3] Přijaté texty, P8_TA(2019)0121.

– s ohledem na čl. 123 odst. 2 jednacího řádu,

A. vzhledem k tomu, že nedávné pokroky v IKT, včetně páté generace telekomunikací (5G), umožňují nové způsoby výroby, distribuce a zužitkování zboží a služeb a nové způsoby interakce mezi zařízeními a občany, orgány veřejné správy a jinými socioekonomickými činiteli, a tudíž mohou podpořit evropské hospodářství;

B. vzhledem k tomu, že kybernetická bezpečnost v IKT, ochrana citlivých informací a dodržování práv jednotlivce a ochrana před kybernetickými útoky zvnějšku jsou podmínkou pro zajištění technologické suverenity občanů EU a v konečném důsledku přinesou EU blahobyt a podpoří demokracii v EU;

C. vzhledem k tomu, že výzkum a testování sítí 5G jen stěží drží krok s mezinárodním tlakem na zavedení a komercionalizaci sítí 5G, ačkoliv řada vědeckých studií upozornila na obavy a nejistoty v souvislosti s jejich bezpečností a zabezpečením, zejména pokud jde o rizika pro lidské zdraví a životní prostředí související s elektromagnetickým znečištěním;

D. vzhledem k tomu, že kybernetická bezpečnost sítí 5G představuje novou a komplexní výzvu kvůli virtualizované a decentralizované povaze sítí 5G a jejich roztříštěnému a vysoce specializovanému hodnotovému řetězci, od výroby po odeslání, instalaci, nastavení, provoz, údržbu a aktualizaci softwaru; vzhledem k tomu, že EU potřebuje odstranit nedostatky v oblasti kybernetické bezpečnosti mimo jiné ve své kritické infrastruktuře v odvětví telekomunikací, energetiky, dopravy, zdravotnictví, obrany a bezpečnosti;

E. vzhledem k tomu, že zajištění bezpečných a zabezpečených sítí 5G je úkol, který nemůže splnit jednotlivý výrobce nebo provozovatel systému, ale vyžaduje účinná koordinovaná opatření ze strany všech příslušných vnitrostátních a mezinárodních orgánů;

F. vzhledem k tomu, že EU má potenciál stát se předním subjektem ve vývoji technologií kybernetické bezpečnosti tím, že podpoří evropské podniky v tomto odvětví a prosadí veškeré změny v hodnotovém řetězci, které by mohly snížit závislost EU na zahraničních technologiích;

G. vzhledem k tomu, že EU vyvíjí soubor opatření na zajištění kybernetické bezpečnosti, včetně směrnice o bezpečnosti sítí a informačních systémů a aktu o kybernetické bezpečnosti, které by měly být rychle provedeny a průběžně monitorovány s cílem zajistit, aby byly i nadále účinné v průběhu nezbytných aktualizací a přezkumů;

H. vzhledem k tomu, že větší přítomnost poskytovatelů technologií z Číny a jiných třetích zemí je na trhu EU se sítěmi 5G zjevná, zejména pak přítomnost státních nebo netransparentních podniků;

I. vzhledem k tomu, že reciprocita je jedním z nejúčinnějších způsobů, jak dosáhnout pokroku na cestě k rovným podmínkám na celém světě;

J. vzhledem k tomu, že zahraniční společnosti se musejí vypořádat se současnou mezerou v normách EU pro ochranu údajů mezi obecným nařízením o ochraně osobních údajů a

různými požadavky v rámci vnitrostátních právních řádů;

K. vzhledem k tomu, že EU a Čína vyjednávají od roku 2013 o komplexní dohodě o investicích; vzhledem k tomu, že navrhovaná dohoda by pomohla vyřešit otázky spojené s přístupem na trh, vytvořit rámec pro ochranu investic a stanovit základní pracovní a environmentální normy;

L. vzhledem k tomu, že se objevily důkazy, ačkoliv neprůkazné, ohledně bezpečnostních nedostatků v souvislosti se zařízením poskytnutým dodavateli z třetích zemí, včetně Číny, které by mohly ohrozit práva jednotlivce na soukromí a ochranu citlivých informací v EU;

1. zdůrazňuje, že zavedení a komercionalizace sítí 5G by měly být provedeny v souladu se zásadou předběžné opatrnosti a všechny socioekonomické subjekty by měly předjímat bezpečnostní dopady a přijmout přiměřená preventivní opatření, včetně okamžitého sdělení faktorů, které by mohly ohrozit veřejné zdraví nebo životní prostředí;

2. zdůrazňuje, že sociální a hospodářské dopady sítí 5G a technologií, které tyto sítě umožňují, počínaje internetem věcí a konče umělou inteligencí, by měly být důkladně posouzeny a že by měla být přijata opatření, která by umožnila přechod na evropskou gigabitovou společnost takovým způsobem, který by byl spravedlivý a zajišťoval rovnost pro všechny a byl založen na etické odpovědnosti;

3. vyzývá Komisi a členské státy, aby vytvořily prostředí vstřícné k inovacím, které umožní prodejcům EU vyvinout nové produkty, služby a technologie, a aby podpořily podnikatelského ducha EU při zavádění a komercionalizaci bezpečných a zabezpečených sítí 5G a současně zajistily, aby byl jejich potenciál dostupný pro všechny podniky v digitálním hospodářství EU, včetně malých a středních podniků;

4. připomíná, že kybernetická bezpečnost je jednou z hlavních výzev, kterým EU v současnosti čelí, a že selhání v této oblasti by mohlo narušit soukromí a základní práva spotřebitelů a výrobců v EU, vážně ohrozit důvěru občanů ve výrobky a služby v oblasti IKT a v konečném důsledku způsobit vážné hospodářské škody; vyzývá k tomu, aby síť měla standardní nastavení bezpečnosti a byla bezpečná již od fáze návrhu;

5. vyzývá Komisi a členské státy, aby úzce spolupracovaly při provádění strategie kybernetické bezpečnosti EU a aby kombinovaly opatření EU a vnitrostátní opatření s cílem minimalizovat riziko bezpečnostních nedostatků a úniku dat v rámci celého hodnotového řetězce; domnívá se, že tato opatření by mohla zahrnovat certifikaci kybernetické bezpečnosti, požadavky na nastavení a provozní postupy a praxi, jakož i podporu kybernetické hygieny a digitálního vzdělávání;

6. je přesvědčen, že agentura EU pro kybernetickou bezpečnost (Agentura Evropské unie pro bezpečnost sítí a informací – ENISA) plní klíčovou úlohu při analyzování možných hrozeb, jež představují zahraniční prodejci, včetně Číny, a při koordinaci společného přístupu mezi členskými státy s cílem bojovat proti hrozbám a útokům v oblasti kybernetické bezpečnosti;

7. vyzývá Komisi a členské státy, aby rychle provedly balíček týkající se oběhového hospodářství a podpořily řízení surovin v průběhu celého jejich životního cyklu, jakož i

recyklaci odpadu, aby tak zlepšily přístup EU ke kritickým surovinám, které jsou stěžejní pro vyspělé technologické výrobky a pro rodící se inovace;

8. považuje za naléhavé vypořádat se s možnými technologickými bezpečnostními hrozbami, které představuje současná penetrace trhu EU zahraničními prodejci, včetně Číny, tím, že se uplatní společný přístup k bezpečnosti a ochraně údajů mezi členskými státy;

9. vyzývá Komisi a členské státy, aby analyzovaly a monitorovaly bezpečnost těch systémů IKT, v nichž se hojně nacházejí technologie třetích zemí, a to i provedením zátěžových zkoušek;

10. zdůrazňuje, že dodavatelé ze třetích zemí by neměli být diskriminováni na základě země původu, ale že by měla být zohledněna transparentnost těchto společností, jejich normy v oblasti kybernetické bezpečnosti a existence recipročních podmínek pro evropské podniky v zemi původu, aby se zajistily rovné podmínky;

11. zdůrazňuje, že za žádných okolností by dodavatelé a operátoři z Číny nebo ze třetích zemí neměli ohrozit práva jednotlivce zaručená právním řádem EU, a to ani v případě, kdy v jejich zemi původu platí odlišné požadavky podle vnitrostátního práva;

12. žádá Radu, aby skutečně zvážila, zda znovu nezahájí diskuse o novém revidovaném návrhu Komise týkajícím se postupu pro omezení přístupu zahraničních výrobků na trh EU s veřejnými zakázkami v případech, kdy neexistuje reciproční přístup;

13. připomíná význam dalšího zlepšení vyjednávání o spolupráci v oblasti regulace digitálních technologií se třetími zeměmi a zajištění jejich větší angažovanosti v mezinárodních normotvorných orgánech;

14. pověřuje svého předsedu, aby předal toto usnesení Radě a Komisi.