**Evropský parlament**
2014-2019

**PŘIJATÉ TEXTY**

# P8_TA(2019)0156

## Bezpečnostní hrozby související se zvyšující se technologickou přítomností Číny v EU a případná opatření přijatá na úrovni EU na jejich omezení

### Usnesení Evropského parlamentu ze dne 12. března 2019 o bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v EU a o případných opatřeních na úrovni EU za účelem jejich omezení (2019/2575(RSP))

*Evropský parlament*,

– s ohledem na směrnici Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace[1],

– s ohledem na směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[2],

– s ohledem na směrnici Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích proti informačním systémům, kterou se nahrazuje rámcové rozhodnutí Rady 2005/222/SVV[3],

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

– s ohledem na návrh nařízení předložený Komisí dne 12. září 2018, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (COM(2018)0630),

– s ohledem na skutečnost, že dne 28. června 2017 schválilo Všečínské shromáždění lidových zástupců nový zákon o národních zpravodajských službách,

– s ohledem na prohlášení, která vydala Rada a Komise dne 13. února 2019 o

---

1 Úř. věst. L 321, 17.12.2018, s. 36.
2 Úř. věst. L 194, 19.7.2016, s. 1.
3 Úř. věst. L 218, 14.8.2013, s. 8.

bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v EU a o případných opatřeních na úrovni EU za účelem jejich omezení,

– s ohledem na skutečnost, že australská vláda schválila reformy zabezpečení telekomunikačního odvětví, které vstoupily v platnost dne18. září 2018,

– s ohledem na svůj postoj, který byl přijat v prvním čtení dne 14. února 2019, k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví rámec pro prověřování přímých zahraničních investic do Evropské unie[1],

– s ohledem na svá předchozí usnesení o vztazích mezi EU a Čínou, zejména na usnesení ze dne 12. září 2018[2],

– s ohledem na sdělení Komise ze dne 14. září 2016 nazvané „Akční plán 5G pro Evropu“ (COM(2016)0588),

– s ohledem na své usnesení ze dne 1. června 2017 o internetové konektivitě pro růst, konkurenceschopnost a soudržnost: evropské gigabitové společnosti a 5G[3],

– s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)[4],

– s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 1316/2013 ze dne 11. prosince 2013, kterým se vytváří Nástroj pro propojení Evropy, mění nařízení (EU) č. 913/2010 a ruší nařízení (ES) č. 680/2007 a (ES) č. 67/2010[5],

– s ohledem na návrh nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027, jejž předložila Komise dne 6. června 2018 (COM(2018)0434),

– s ohledem na čl. 123 odst. 2 a 4 jednacího řádu,

A. vzhledem k tomu, že EU musí aktivně prosazovat svůj program kybernetické bezpečnosti, aby mohla naplnit svůj potenciál a stát se na tomto poli vůdčím aktérem a tohoto postavení využít ku prospěchu svého průmyslu;

B. vzhledem k tomu, že slabiny sítí 5G by mohly být zneužity k ohrožení systémů IT, což by mohlo velmi vážně poškodit evropskou ekonomiku i ekonomiku jednotlivých států; vzhledem k tomu, že v zájmu minimalizace rizik je nutný přístup založený na analýze rizik v celém hodnotovém řetězci;

C. vzhledem k tomu, že síť 5G bude páteří naší digitální infrastruktury, neboť rozšíří možnosti připojení různých zařízení k sítím (internet věcí apod.), a že společnosti i podnikům přinese nové výhody a příležitosti v řadě oblastí, mimo jiné i v klíčových

---

1 Přijaté texty, P8_TA(2019)0121.
2 Přijaté texty, P8_TA(2018)0343.
3 Úř. věst. C 307, 30.8.2018, s. 144.
4 Úř. věst. L 119, 4.5.2016, s. 1.
5 Úř. věst. L 348, 20.12.2013, s. 129.

odvětvích ekonomiky, např. v dopravě, energetice, zdravotnictví, finančním sektoru, telekomunikacích, obraně, vesmírném průmyslu a bezpečnosti;

D. vzhledem k tomu, že zřízení vhodného mechanismu pro reakce na bezpečnostní problémy by EU umožnilo aktivně přijímat opatření při stanovováním norem pro síť 5G;

E. vzhledem k tomu, že se objevily obavy z prodejců zařízení z třetích zemí, kteří mohou pro EU představovat bezpečnostní hrozbu v důsledku právních předpisů jejich zemí původu, a to zejména po přijetí čínských zákonů o národní bezpečnosti, které všem občanům, podnikům a dalším subjektům ukládají povinnost spolupracovat se státem na ochraně velmi široce definované národní bezpečnosti; vzhledem k tomu, že neexistují žádné záruky ohledně toho, že se nejedná o zákony s extrateritoriálními účinky, a že reakce států na tyto čínské předpisy jsou velmi různé: posouzeními bezpečnosti počínaje a naprostým zákazem konče;

F. vzhledem k tomu, že v prosinci 2018 vydal český Národní úřad pro kybernetickou a informační bezpečnost varování před bezpečnostními hrozbami, které jsou spojené s technologiemi dodávanými čínskými společnostmi Huawei a ZTE; vzhledem k tomu, že v lednu 2019 české daňové orgány na základě tohoto varování vyloučily společnost Huawei z veřejné zakázky na vybudování daňového portálu;

G. vzhledem k tomu, že je nutné důkladně prošetřit, zda zařízení určená pro portál nebo jakákoli jiná zařízení či dodavatelé představují bezpečnostní rizika kvůli prvkům, jako jsou tzv. zadní vrátka nainstalovaná přímo v systémech;

H. vzhledem k tomu, že řešení by měla být koordinována a hledána na úrovni EU, aby se zabránilo rozdílným úrovním zabezpečení a potenciálním mezerám v kybernetické bezpečnosti, a že koordinace je zapotřebí i na celosvětové úrovni, má-li být reakce skutečně účinná;

I. vzhledem k tomu, že výhody jednotného trhu se pojí se závazkem dodržovat normy EU a právní rámec Unie a že s dodavateli by se nemělo zacházet rozdílně podle jejich země původu;

J. vzhledem k tomu, že nařízení o prověřování přímých zahraničních investic, které má vstoupit v platnost na konci roku 2020, rozšiřuje pravomoci členských států ke kontrole zahraničních investic v zájmu bezpečnosti a veřejného pořádku, a zavádí mechanismus spolupráce, v jehož rámci mohou Komise a členské státy spolupracovat při posuzování bezpečnostních rizik, včetně kybernetických hrozeb, spojených s citlivými zahraničními investicemi, a které se vztahuje rovněž na projekty a programy v zájmu EU, jako jsou transevropské telekomunikační sítě a program Horizont 2020;

1. věří, že Unie se musí stát průkopníkem na poli kybernetické bezpečnosti a za tímto účelem zaujmout společný přístup, který bude založen na účelném a účinném využívání odborných vědomostí EU, členských států a příslušných odvětví, protože mozaika různých národních rozhodnutí by poškodila jednotný digitální trh;

2. je velmi znepokojen nedávnými tvrzeními, že do zařízení s podporou 5G, která jsou vyvíjena čínskými firmami, jsou údajně nainstalována zadní vrátka, která by výrobcům a orgánům umožnila nedovolený přístup k soukromým a osobním údajům

a k telekomunikaci EU;

3. stejně tak je znepokojen potenciálními vážnými slabinami zařízení 5G od těchto výrobců, pokud by měla být v příštích letech nainstalována při zahájení provozu sítí 5G;

4. zdůrazňuje, že důsledky, které z toho vyplývají pro bezpečnost sítí a zařízení, jsou na celém světě podobné, a vyzývá EU, aby se poučila z dosavadních zkušeností, aby byla schopna zaručit nejvyšší standardy kybernetické bezpečnosti; vyzývá Komisi, aby vypracovala strategii, která Evropě zajistí vedoucí postavení v oblasti technologií zajišťujících kybernetickou bezpečnost a která bude v oblasti kybernetické bezpečnosti usilovat o snížení naší závislosti na zahraničních technologiích; zastává názor, že kdykoli nelze zaručit dodržování bezpečnostních požadavků, musí být použita odpovídající opatření;

5. vyzývá členské státy, aby informovaly Komisi o všech zamýšlených vnitrostátních opatřeních, aby bylo možné koordinovat reakci na úrovni Unie a tak v celé Unii zajistit nejvyšší standardy kybernetické bezpečnosti, a znovu připomíná, že je důležité zdržet se zavádění neadekvátních jednostranných opatření, která by vedla k rozdrobení jednotného trhu;

6. znovu zdůrazňuje, že všechny subjekty, které v EU nabízejí zařízení nebo služby, musí bez ohledu na svou zemi původu dodržovat povinnosti v oblasti základních práv a unijní i vnitrostátní právní předpisy, včetně právního rámce pro soukromí, ochranu údajů a kybernetickou bezpečnost;

7. vyzývá Komisi, aby posoudila, zda je právní rámec Unie dostatečně propracován, aby řešil obavy spojené s přítomností zranitelných zařízení ve strategicky významných odvětvích a infrastruktuře; naléhá na Komisi, aby představila iniciativy, případně aby předložila i legislativní návrhy, na včasné řešení odhalených nedostatků, neboť Unie se neustále snaží určovat a řešit výzvy spojené s kybernetickou bezpečností a posilovat kybernetickou odolnost v celé EU;

8. naléhá na členské státy, které dosud v plném rozsahu neprovedly směrnici o bezpečnosti sítí a informací ve vnitrostátním právu, aby tak bezodkladně učinily, a vyzývá Komisi, aby tento proces pečlivě sledovala, tak aby bylo zaručeno řádné uplatňování a prosazování těchto ustanovení a lepší ochrana evropských občanů před vnějšími a vnitřními bezpečnostními hrozbami;

9. naléhá na Komisi a členské státy, aby zajistily náležité uplatňování oznamovacích mechanismů zavedených podle směrnice o bezpečnosti sítí a informací; konstatuje, že by Komise a členské státy měly ze všech bezpečnostních incidentů nebo z nevhodných reakcí dodavatelů důkladně vyvozovat závěry, tak aby byly odhalené trhliny odstraněny;

10. vyzývá Komisi, aby posoudila, zda je nutné rozšířit působnost směrnice o bezpečnosti sítí a informací na další klíčové sektory a služby, které nejsou pokryty odvětvovými právními předpisy;

11. vítá a podporuje dohodu, jíž bylo dosaženo ohledně aktu o kybernetické bezpečnosti, a posílení mandátu Agentury EU pro bezpečnost sítí a informací (ENISA) s cílem lépe podporovat členské státy při řešení hrozeb a útoků zaměřených proti kybernetické

bezpečnosti;

12. naléhavě vyzývá Komisi, aby pověřila agenturu ENISA, aby se prioritou její činnosti stal systém certifikace pro zařízení 5G s cílem zajistit, aby zavedení systémů 5G v Unii odpovídalo nejvyšším bezpečnostním standardům a bylo odolné proti skrytým nebo významným zranitelným místům, která by ohrozila bezpečnost telekomunikačních sítí Unie a souvisejících služeb; doporučuje, aby byla zvláštní pozornost věnována běžně využívaným postupům, produktům a softwaru, které mají díky svému rozsahu významný dopad na každodenní život občanů a na hospodářství;

13. s potěšením vítá návrhy týkající se odborných středisek pro kybernetickou bezpečnost a sítě vnitrostátních koordinačních středisek, která byla navržena s cílem pomoci Evropské unii zachovat a rozvinout technologické a průmyslové kapacity v kybernetické bezpečnosti, jež jsou nezbytné pro zabezpečení jejího jednotného digitálního trhu; připomíná však, že by certifikace neměla příslušné orgány a operátory vyloučit z přezkumu dodavatelského řetězce s cílem zajistit integritu a bezpečnost jejich zařízení, které funguje v kritických prostředích a v telekomunikačních sítích;

14. připomíná, že kybernetická bezpečnost vyžaduje vysoké bezpečnostní standardy; vyzývá k tomu, aby síť měla standardní nastavení bezpečnosti a byla bezpečná již od fáze návrhu; naléhavě vyzývá členské státy, aby společně s Komisí přezkoumaly veškeré dostupné prostředky s cílem zajistit vysokou úroveň bezpečnosti;

15. vyzývá Komisi a členské státy, aby ve spolupráci s agenturou ENISA poskytly pokyny ohledně toho, jak bojovat proti kybernetickým hrozbám a zranitelným místům při zadávání zakázek na nákup zařízení 5G, například diverzifikací zařízení od různých prodejců nebo zavedením vícefázových procesů zadávání zakázek;

16. opakuje své stanovisko ohledně programu Digitální Evropa, který ukládá bezpečnostní požadavky a dohled Komise nad subjekty usazenými v Evropské unii, které jsou však kontrolovány ze třetích zemí, zejména pokud jde o činnosti související s kybernetickou bezpečností;

17. vyzývá členské státy, aby zajistily, aby veřejné instituce i soukromé společnosti, které se podílejí na zajišťování řádného fungování sítí kritické infrastruktury, jako jsou telekomunikace, energetika a zdravotní a sociální systémy, provedly příslušné analýzy rizik s přihlédnutím k bezpečnostním hrozbám, které jsou konkrétně spojeny s technickými vlastnostmi příslušného systému, nebo k závislosti na externích dodavatelích hardwarových a softwarových technologií;

18. připomíná, že stávající právní rámec v oblasti telekomunikací ukládá členským státům povinnost zajistit, aby operátoři telekomunikací respektovali integritu a dostupnost veřejných sítí elektronické komunikace, případně včetně používání šifrování mezi koncovými body; zdůrazňuje, že podle evropského kodexu pro elektronické komunikace mají členské státy rozsáhlé pravomoci k prověřování produktů na trhu EU a k uplatňování široké škály prostředků nápravy v případě jejich nesouladu;

19. vyzývá Komisi a členské státy, aby stanovily bezpečnost jako povinný aspekt ve všech zadávacích řízeních pro příslušnou infrastrukturu jak na úrovni EU, tak na vnitrostátní úrovni;

20. připomíná členským státům jejich povinnost v rámci právního rámce EU, zejména směrnice 2013/40/EU o útocích na informační systémy, pokud jde o ukládání sankcí proti právnickým osobám, které se dopustily trestných činů, jako jsou útoky proti těmto systémům; zdůrazňuje, že by členské státy měly také využívat možnost ukládat těmto právním subjektům jiné sankce, například dočasný nebo trvalý zákaz provozování obchodní činnosti;

21. vyzývá členské státy, agentury pro kybernetickou bezpečnost, provozovatele telekomunikačních sítí, výrobce a poskytovatele služeb kritické infrastruktury, aby Komisi a agentuře ENISA oznámili veškeré důkazy o přítomnosti skrytých nebo jiných významných zranitelných míst, jež by mohla ohrozit integritu a bezpečnost telekomunikačních sítí nebo porušit právo Unie a základní práva; očekává, že vnitrostátní orgány pro ochranu údajů a také evropský inspektor ochrany údajů budou podrobně vyšetřovat náznaky porušení zabezpečení údajů ze strany externích prodejců a ukládat odpovídající pokuty a sankce v souladu s evropským právem v oblasti ochrany údajů;

22. vítá nadcházející vstup v platnost nařízení, kterým se stanoví rámec pro prověřování přímých zahraničních investic z důvodu bezpečnosti a veřejného pořádku, a zdůrazňuje, že toto nařízení poprvé uvádí seznam oblastí a faktorů, včetně komunikací a kybernetické bezpečnosti, které jsou relevantní pro bezpečnost a veřejný pořádek na úrovni EU;

23. vyzývá Radu, aby urychlila svou činnost, pokud jde o navrhované nařízení o soukromí a elektronických komunikacích;

24. znovu zdůrazňuje, že je nezbytné, aby EU podporovala kybernetickou bezpečnost v celém hodnotovém řetězci, od výzkumu po zavádění a využívání klíčových technologií, aby šířila příslušné informace a prosazovala kybernetickou hygienu a vzdělávací osnovy zahrnující kybernetickou bezpečnost, a je přesvědčen, že pro tento účel bude program Digitální Evropa, vedle jiných opatření, účinným nástrojem;

25. naléhavě vyzývá Komisi a členské státy, aby učinily nezbytné kroky, včetně odolných investičních programů, s cílem vytvořit v EU prostředí příznivé pro inovace, které by mělo být dostupné všem podnikům v oblasti digitální ekonomiky EU, včetně malých a středních podniků; naléhavě dále vyzývá k tomu, aby toto prostředí umožnilo evropským prodejcům vyvíjet nové produkty, služby a technologie, které by jim umožnily, aby byli konkurenceschopní;

26. naléhavě vyzývá Komisi a členské státy, aby výše uvedené požadavky zohlednily při svých nadcházejících diskusích o budoucí strategii mezi Evropskou unií a Čínou jako podmínky, které jsou nezbytné pro EU, aby zůstala konkurenceschopná, a pro zajištění bezpečnosti její digitální infrastruktury;

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