Evropský parlament
2014-2019

Dokument ze zasedání

B8-0155/2019

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 na úrovni EU za účelem jejich omezení
(2019/2575(RSP))

Luděk Niedermayer, Angelika Niebler, Ivo Belet, Paul Rübig
za skupinu PPE

B8-0155/2019

Usnesení Evropského parlamentu 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 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 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 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 bezpečnosti telekomunikačního odvětví, které jsou v účinnosti od 18. 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[4],

[1] Úř. věst. L 321, 17.12. 2018, s. 36.
[2] Úř. věst. 194, 19.7.2016, s. 1.
[3] Úř. věst. L 218, 14.8. 2013, s. 8.
[4] Přijaté texty, P8_TA(2019)0121.

– s ohledem na svá předchozí usnesení o vztazích mezi EU a Čínou, zejména na usnesení ze dne 12. září 2018 o situaci v oblasti vztahů mezi EU a Čínou[5],

– 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[6],

– s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 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)[7],

– 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[8],

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

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

A. vzhledem k tomu, že EU musí prosazovat svou agendu týkající se kybernetické bezpečnosti, aby mohla naplnit svůj potenciál stát se vedoucím aktérem kybernetické bezpečnosti a využít tohoto postavení ku prospěchu svého průmyslu;

B. vzhledem k tomu, že by mohlo dojít ke zneužití slabin sítí 5G s cílem ohrozit systémy IT, případně velmi vážně poškodit ekonomiku na evropské úrovni i na úrovni 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 celé naší digitální infrastruktury, neboť rozšíří možnost připojit různá zařízení k sítím (internet věcí apod.), a že společnosti i podnikům přinese tato síť nové výhody a příležitosti v řadě oblastí, mimo jiné i v klíčových odvětvích ekonomiky včetně dopravy, energetiky, zdravotnictví, financí, telekomunikací, obrany, vesmírného průmyslu a bezpečnosti;

D. vzhledem k tomu, že zřízení vhodného mechanismu pro reakce na bezpečnostní problémy by EU poskytlo možnost přijímat aktivní opatření v souvislosti se 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, a to zejména po přijetí čínských zákonů o státní bezpečnosti, které všem občanům, podnikům a dalším subjektům ukládají povinnost spolupracovat se státem na ochraně státní bezpečnosti; vzhledem k tomu, že neexistují žádné záruky toho, že se nejedná

[5] Přijaté texty, P8_TA(2018)0343.
[6] Úř. věst. C 307, 30.8.2018, s. 144.
[7] Úř. věst. L 119, 4.5.2016, s. 1.
[8] Úř. věst. L 348, 20.12.2013, s. 129.

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 vyloučily na základě tohoto varování 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 nainstalovaným přímo v systémech;

H. vzhledem k tomu, že řešení by měla být koordinována a hledána na úrovni EU, aby se zabránilo různým úrovním zabezpečení a potenciálním mezerám v kybernetické bezpečnosti; vzhledem k tomu, 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 v Unii, které má vstoupit v platnost na konci roku 2020, rozšiřuje pravomoci členských států ke kontrole zahraniční investice 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 mají výrobcům a orgánům umožnit nedovolený přístup k datům a telekomunikaci občanů a podniků 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 normy pro kybernetickou bezpečnost; 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;

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 (EU) č. 2016/1148 o bezpečnosti sítí a informačních systémů ve vnitrostátním právu, aby tak bezodkladně učinily, a vyzývá Komisi, aby tento proces pečlivě sledovala, aby bylo zaručeno řádné prosazování těchto ustanovení a lepší ochrana evropských občanů před vnějšími bezpečnostními hrozbami;

9. naléhá na Komisi a členské státy, aby zajistily náležité uplatňování oznamovacích mechanismů zavedených podle směrnice směrnici (EU) č. 2016/1148; konstatuje, že Komise a členské státy by 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 na klíčové sektory a služby, které nejsou pokryty zvláštními právními předpisy (např. síťová infrastruktura);

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. připomíná, že kybernetická bezpečnost klade vysoké požadavky na zabezpečení; vyzývá k vytvoření sítě, která je zabezpečená na úrovni standardního nastavení a výchozího návrhu; naléhavě vyzývá členské státy, aby společně s Komisí přezkoumaly veškeré dostupné prostředky s cílem zajistit vysokou úroveň bezpečnosti;

13. 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 související služby; doporučuje, aby byla zvláštní pozornost věnována obecně užívaným postupům, produktům a softwaru, které mají díky svému velkému rozsahu

významný dopad na každodenní život občanů a na hospodářství;

14. 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, které jsou nezbytné pro zabezpečení jejího jednotného digitálního trhu;

15. opětovně potvrzuje svůj postoj, pokud jde o program 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;

16. 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;

17. připomíná, že současný právní rámec týkající se telekomunikací ukládá členským státům, aby zajistily, aby telekomunikační operátoři postupovali v souladu s integritou a dostupností veřejných sítí elektronických komunikací; zdůrazňuje, že podle evropského kodexu pro elektronické komunikace mají členské státy veškeré pravomoci nezbytné pro vyšetřování a uplatňování širokého spektra nápravných opatření v případě nesouladu výrobků na trhu EU;

18. vyzývá Komisi a členské státy, aby bezpečnost pojaly jako povinné hledisko při veškerých postupech zadávání veřejných zakázek na příslušné infrastruktury na úrovni EU i na vnitrostátní úrovni;

19. vyzývá Komisi a členské státy, aby zvýšily transparentnost a bezpečnost díky vývoji vícefázových postupů zadávání zakázek na infrastrukturu IKT, což by umožnilo, aby se rozlišovalo mezi nabídkami na uspořádání těchto systémů, jejich výrobu, provoz a údržbu i mezi jednotlivými dodavateli technologií;

20. připomíná členským státům, že v rámci trestního práva EU mají povinnost ukládat sankce, zejména pokuty trestní nebo jiné povahy, právnickým osobám, které se dopustily trestných činů, jako jsou útoky na informační systémy, neoprávněné zasahování do informačních systémů nebo neoprávněné zasahování do údajů a protiprávní sledování; zdůrazňuje, že by členské státy měly také využívat možnost ukládat těmto právním subjektům jiné sankce, například dočasný nebo trvalý zákaz provozování obchodní činnosti;

21. 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. 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 podporovala kybernetickou hygienu a vzdělávací osnovy v souvislosti s kybernetickou bezpečností, a je přesvědčen, že pro tento účel bude program Digitální Evropa, vedle jiných opatření, účinným nástrojem;

24. 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 vyzývá také k tomu, aby takové prostředí umožnilo evropským prodejcům vyvíjet nové produkty, služby a technologie, které by jim umožnily být konkurenceschopní;

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