Evropski parlament
2014-2019

Dokument zasedanja

B8-0153/2019

6.3.2019

PREDLOG RESOLUCIJE

ob zaključku razprave o izjavah Sveta in Komisije

v skladu s členom 123(2) Poslovnika

o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možnih ukrepih na ravni EU za njihovo zmanjšanje
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
v imenu skupine EFDD

B8-0153/2019

Resolucija Evropskega parlamenta o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možnih ukrepih na ravni EU za njihovo zmanjšanje
(2019/2575(RSP))

Evropski parlament,

– ob upoštevanju sporočila Komisije z dne 14. septembra 2016 z naslovom Povezljivost za konkurenčen enotni digitalni trg – evropski gigabitni družbi naproti (COM(2016)0587) in „Akcijski načrt za 5G v Evropi“ (COM(2016)0588),

– ob upoštevanju spremenjenega predloga Komisije za uredbo Evropskega parlamenta in Sveta z dne 29. januarja 2016 o dostopu blaga in storitev tretje države do notranjega trga javnih naročil Unije ter postopkih za podporo pogajanjem o dostopu blaga in storitev Unije do trgov javnih naročil tretjih držav (COM(2016)0034),

– ob upoštevanju Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[1] (direktiva o varnosti omrežij in informacij),

– ob upoštevanju predloga uredbe Evropskega parlamenta in Sveta z dne 13. septembra 2017 o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti) (COM(2017)0477),

– ob upoštevanju Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah[2],

– ob upoštevanju predloga Komisije za uredbo Evropskega parlamenta in Sveta z dne 12. septembra 2018 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov (COM(2018)0630),

– ob upoštevanju rešitve spora pred STO (WT/DS549/6) z dne 1. junija 2018 glede nekaterih ukrepov, ki jih je Kitajska uvedla v zvezi s prenosom tuje tehnologije na Kitajsko,

– ob upoštevanju svojega stališča, sprejetega v prvi obravnavi dne 14. februarja 2019, o predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvira za pregled neposrednih tujih naložb v Evropski uniji[3],

– ob upoštevanju sedanjih pogajanj med EU in Kitajsko o celovitem sporazumu o naložbah,

[1] UL L 194, 19.7.2016, str. 1.
[2] UL L 321, 17.12.2018, str. 36.
[3] Sprejeta besedila, P8_TA(2019)0121.

– ob upoštevanju člena 123(2) Poslovnika,

A. ker je nedavni napredek na področju informacijskih in komunikacijskih tehnologij (IKT), vključno s telekomunikacijami pete generacije (5G) utrl pot proizvodnji, distribuciji in izkoriščanju blaga in storitev ter interakciji med napravili in med državljani, javnimi upravami in drugimi socialno-ekonomskimi akterji, zaradi česar imajo potencial za spodbuditev evropskega gospodarstva;

B. ker so kibernetska varnost na področju IKT, varstvo občutljivih informacij, spoštovanje pravic posameznikov in zaščita pred zunanjimi kibernetskimi grožnjami osnovni pogoji za zagotavljanje tehnološke suverenosti državljanov EU, s tem pa zagotovitev blaginje in podpore demokraciji v EU;

C. ker raziskave in preskušanje omrežij 5G stežka ostajajo v koraku z mednarodnim pritiskom za njihovo uvedbo in trženje, hkrati pa vrsta znanstvenih študij sproža pomisleke in negotovost v zvezi z njihovo varnostjo in zaščitenostjo, zlasti kar zadeva elektromagnetno onesnaževanje za zdravje ljudi in okolje;

D. ker je zagotavljanje kibernetske varnosti za omrežja 5G nov in kompleksen izziv, saj so virtualizirana in decentralizirana, njihova vrednostna veriga pa je razdrobljena in zelo specializirana, od proizvodnje do odpošiljanja, namestitve, konfiguracije, delovanja in posodobitev programske opreme; ker mora EU zapolniti vrzeli v kibernetski varnosti pri svoji kritični infrastrukturi, med drugim v sektorjih telekomunikacij, energije, prometa, zdravja, obrambe in varnosti;

E. ker naloge zagotavljanja varnih in zavarovanih omrežij 5G ne morejo izpolniti posamezni proizvajalci ali operaterji sistemov, temveč je zanjo potrebno učinkovito usklajeno delovanje vseh zadevnih nacionalnih in mednarodnih organov;

F. ker bi EU lahko vodila razvoj tehnologij kibernetske varnosti, tako da bi podprla evropska podjetja v tem sektorju in spodbujala vse spremembe v vrednostni verigi, ki bi lahko zmanjšale odvisnost EU od tuje tehnologije;

G. ker EU pripravlja vrsto ukrepov za zagotavljanje kibernetske varnosti, vključno z direktivo o varnosti omrežij in informacij ter uredbo o kibernetski varnosti, ki bi ju bilo treba hitro izvajati in stalno spremljati, da bi se zagotovilo ohranjanje njune učinkovitosti ob vseh potrebnih posodobitvah in pregledih;

H. ker se je povečala prisotnost kitajskih in drugih ponudnikov tehnologije iz tretjih držav na trgu za omrežja 5G v EU, zlasti podjetij v državni lasti ali podjetij, kjer je preglednost pomanjkljiva;

I. ker je vzajemnost eden od najučinkovitejših načinov za izboljšanje enakosti pogojev na svetovni ravni;

J. ker se morajo tuja podjetja spoprijemati s sedanjo vrzeljo v standardih EU za varstvo podatkov med splošno uredbo o varstvu podatkov in različnimi zahtevami nacionalnih zakonodaj;

K. ker se EU in Kitajska pogajata o celovitem sporazumu o naložbah od leta 2013; ker bi

predlagani dogovor pomagal pri reševanju vprašanj dostopa do trga, vzpostavil okvir za zaščito naložb ter določil osnovne delovne in okoljske standarde;

L. ker so se pojavili dokazi, četudi ne dokončni, o pomanjkanju varnosti pri opremi, ki jo dobavljajo dobavitelji iz tretjih držav, tudi iz Kitajske, ki bi lahko ogrozila pravice posameznikov do zasebnosti in varstvo občutljivih informacij v EU;

1. poudarja, da bi bilo treba omrežja 5G uvajati in tržiti v skladu s previdnostnim načelom, vsi socialno-ekonomski akterji pa bi morali predvideti morebitne učinke na varnost in zaščito ter izvajati sorazmerne previdnostne ukrepe, vključno s hitrim razkritjem dejavnikov, ki bi lahko ogrozili javno zdravje ali okolje;

2. poudarja, da bi bilo treba temeljito oceniti socialne in gospodarske učinke omrežij 5G ter tehnologij, ki jih omogoča, od interneta stvari do umetne inteligence, ter da bi bilo treba sprejeti ukrepe, da bo prehod na evropsko gigabitno družbo za vse pravičen in enak ter bo temeljil na etični odgovornosti;

3. poziva Komisijo in države članice, naj oblikujejo inovacijam prijazno okolje, v katerem bodo prodajalci iz EU razvijali nove proizvode, storitve in tehnologije, ter naj podprejo podjetništvo v EU pri uvedbi in trženju varnih in zaščitenih omrežij 5G, hkrati pa naj zagotovijo, da bo njihov potencial dostopen vsem podjetjem v digitalnem gospodarstvu EU, vključno z malimi in srednjimi podjetji;

4. opozarja, da je kibernetska varnost eden od glavnih izzivov, s katerimi se trenutno spoprijema EU, nezmožnost njenega zagotavljanja pa bi lahko povzročila kršenje zasebnosti in temeljnih pravic potrošnikov in proizvajalcev v EU, resno omajala zaupanje državljanov v proizvode in storitve IKT ter na koncu povzročila hudo gospodarsko škodo; poziva k omrežju, ki bo v skladu z načelom privzete in vgrajene varnosti;

5. poziva Komisijo in države članice, naj tesno sodelujejo pri izvajanju strategije EU za kibernetsko varnost ter naj združijo ukrepe EU in nacionalne ukrepe, da bi čim bolj zmanjšale tveganje pomanjkljive varnosti in kršitev varnosti podatkov vzdolž celotne vrednostne verige; meni, da bi taki ukrepi lahko vključevali certificiranje kibernetske varnosti v EU, konfiguracijske zahteve in operacijske postopke in prakse, pa tudi spodbujanje kibernetske higiene in digitalno izobraževanje;

6. meni, da ima agencija EU za kibernetsko varnost (Agencija Evropske unije za varnost omrežij in informacij – ENISA) bistveno vlogo pri analizi morebitnih groženj, ki jih utegnejo pomeniti tuji prodajalci, tudi Kitajska, ter usklajevanju skupnega pristopa držav članic k obravnavanju groženj za kibernetsko varnost in napadov nanjo;

7. poziva Komisijo in države članice, naj hitro izvedejo sveženj ukrepov za krožno gospodarstvo in spodbujajo upravljanje surovin v celotnem življenjskem krogu, pa tudi recikliranje odpadkov, da se izboljša dostop EU do kritičnih surovin, ki so bistvene za visokotehnološke proizvode in nastajajoče inovacije;

8. se mu zdi nujno obravnavati morebitne grožnje za tehnološko varnost, ki jo predstavlja sedanji prodor tujih prodajalcev, tudi Kitajske, na trg EU, in sicer s skupnim pristopom k varnosti in varstvu podatkov med državami članicami;

9. poziva Komisijo in države članice, naj analizirajo in spremljajo varnost tistih sistemov IKT, v katerih so zelo prisotne tehnologije tretjih držav, tudi z izvajanjem testiranj izjemnih situacij;

10. poudarja, da dobaviteljev iz tretjih držav ne bi smeli diskriminirati na podlagi države izvora, a bi morali upoštevati preglednost teh podjetij, njihove standarde glede kibernetske varnosti in obstoj vzajemnih pogojev za evropska podjetja v državi izvora, da bi zagotovili enake konkurenčne pogoje;

11. poudarja, da dobavitelji in ponudniki iz Kitajske ali drugih tretjih držav v nobenem primeru ne bi smeli ogrožati pravic posameznikov, ki jih zagotavlja pravo EU, četudi v njihovi državi izvora po nacionalnem pravu veljajo drugačne zahteve;

12. poziva Svet, naj pozitivno oceni ponovno odprtje razprav o novem revidiranem predlogu Komisije o postopku, ki omejuje dostop tujih proizvodov do trga javnih naročil EU, če dostop ni vzajemen;

13. opozarja, kako pomembno je napredovati pri pogajanjih o zakonodajnem sodelovanju na področju digitalne tehnologije s tretjimi državami in zagotoviti njihovo večjo udeležbo v mednarodnih organih za določanje standardov;

14. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu in Komisiji.