Evropski parlament
2019-2024

SPREJETA BESEDILA

P9_TA(2021)0286

Strategija EU za kibernetsko varnost v digitalnem desetletju

Resolucija Evropskega parlamenta z dne 10. junija 2021 o strategiji EU za kibernetsko varnost v digitalnem desetletju (2021/2568(RSP))

Evropski parlament,

– ob upoštevanju skupnega sporočila Komisije in visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 16. decembra 2020 z naslovom Strategija EU za kibernetsko varnost v digitalnem desetletju (JOIN(2020)0018),

– ob upoštevanju predloga Komisije z dne 16. decembra 2020 za direktivo Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 (COM(2020)0823),

– ob upoštevanju predloga Komisije z dne 24. septembra 2020 za uredbo Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014 (COM(2020)0595),

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

– ob upoštevanju sporočila Komisije z dne 19. februarja 2020 z naslovom Oblikovanje digitalne prihodnosti Evrope (COM(2020)0067),

– ob upoštevanju Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti)[1],

– ob upoštevanju Direktive 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES[2],

---

1 UL L 151, 7.6.2019, str. 15.
2 UL L 153, 22.5.2014, str. 62.

– ob upoštevanju Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah[1],

– ob upoštevanju Uredbe (EU) št. 1290/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o pravilih za sodelovanje v okvirnem programu za raziskave in inovacije (2014–2020) – Obzorje 2020 ter za razširjanje njegovih rezultatov in o razveljavitvi Uredbe (ES) št. 1906/2006[2],

– ob upoštevanju Uredbe (EU) št. 1291/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o vzpostavitvi okvirnega programa za raziskave in inovacije (2014–2020) – Obzorje 2020 in razveljavitvi Sklepa št. 1982/2006/ES[3],

– ob upoštevanju Uredbe (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa za digitalno Evropo in razveljavitvi Sklepa (EU) 2015/2240[4],

– ob upoštevanju Direktive 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza[5],

– ob upoštevanju Budimpeške konvencije o kibernetski kriminaliteti z dne 23. novembra 2001 (ETS št.185),

– ob upoštevanju svoje resolucije z dne 16. decembra 2020 o novi strategiji za evropska mala in srednja podjetja[6],

– ob upoštevanju svoje resolucije z dne 25. marca 2021 o trajnostni strategiji za kemikalije[7],

– ob upoštevanju svoje resolucije z dne 20. maja 2021 o oblikovanju demografski prihodnosti Evrope: odprava ovir za delovanje enotnega digitalnega trga in izboljšana uporaba umetne inteligence za evropske potrošnike[8],

– ob upoštevanju svoje resolucije z dne 21. januarja 2021 o zapolnitvi digitalnega razkoraka med spoloma: udeležba žensk v digitalnem gospodarstvu[9],

– ob upoštevanju svoje resolucije z dne 12. marca 2019 o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možnih ukrepih na ravni EU za njihovo zmanjšanje[10],

– ob upoštevanju vprašanja Komisiji o strategiji EU za kibernetsko varnost v digitalnem

---

1 UL L 321, 17.12.2018, str. 36.
2 UL L 347, 20.12.2013, str. 81.
3 UL L 347, 20.12.2013, str. 104.
4 UL L 166, 11.5.2021, str. 1.
5 UL L 207, 6.8.2010, str. 1.
6 Sprejeta besedila, P9_TA(2020)0359.
7 Sprejeta besedila, P9_TA(2021)0098.
8 Sprejeta besedila, P9_TA(2021)0261.
9 Sprejeta besedila, P9_TA(2021)0026.
10 UL C 23, 21.1.2021, str. 2.

desetletju (O-000037/2021 – B9-0024/2021),

– ob upoštevanju člena 136(5) in člena 132(2) Poslovnika,

A. ker je digitalna preobrazba ključna strateška prednostna naloga Unije, ki je neizogibno povezana z večjo izpostavljenostjo kibernetskim grožnjam;

B. ker se število povezanih naprav, vključno s stroji, senzorji, industrijskimi komponentami in omrežji, ki sestavljajo internet stvari, še naprej povečuje, saj naj bi bilo do leta 2024 z internetom stvari povezanih 22,3 milijarde naprav po vsem svetu, s čimer se bo povečala izpostavljenost kibernetskim napadom;

C. ker bi lahko tehnološki napredek – kot je kvantno računalništvo – in asimetrija pri dostopu do njega pomenila izziv za kibernetsko varnost;

D. ker je kriza zaradi covida-19 še bolj razkrila kibernetske ranljivosti v nekaterih kritičnih sektorjih, zlasti v zdravstvu, in ker so s tem povezani ukrepi dela na daljavo in omejevanja socialnih stikov povečali našo odvisnost od digitalnih tehnologij in povezljivosti, medtem ko so po Evropi vedno številčnejši in bolj izpopolnjeni kibernetski napadi in kibernetski kriminalni napadi, vključno z vohunstvom in sabotažo ter uporabo zlonamernih in nezakonitih načinov za vdiranje v sisteme, strukture in omrežja IKT ter njihovo manipulacijo;

E. ker se število kibernetskih napadov znatno povečuje, kot je razvidno iz nedavnega niza zlonamernih in organiziranih kibernetskih napadov na sisteme zdravstvenega varstva, na primer na Irskem, Finskem in v Franciji; ker ti kibernetski napadi znatno škodujejo zdravstvenim sistemom in oskrbi pacientov ter drugim občutljivim javnim in zasebnim ustanovam;

F. ker hibridne grožnje, vključno z uporabo dezinformacijskih kampanj in kibernetskih napadov na infrastrukturo, gospodarske procese in demokratične institucije, postajajo resen problem v kibernetskem in fizičnem svetu ter lahko vplivajo na demokratične procese, kot so volitve, zakonodajni postopki, kazenski pregon in pravosodje;

G. ker smo vse bolj odvisni od temeljne funkcije interneta in bistvenih internetnih storitev za komunikacijo in gostovanje, aplikacije in podatke, pri katerih je tržni delež vse bolj skoncentriran v vedno manjšem številu podjetij;

H. ker se povečujejo zmogljivosti porazdeljenih napadov za zavrnitev storitve in bi bilo zato treba hkrati povečati odpornost jedra interneta;

I. ker sta pripravljenost in ozaveščenost na področju kibernetske varnosti pri podjetjih, zlasti MSP in posameznikih, še vedno nizki in ker primanjkuje kvalificiranih delavcev (od leta 2015 se je vrzel v delovni sili povečala za 20 %), tradicionalni načini zaposlovanja pa ne dohajajo povpraševanja, kar velja tudi za vodstvene in interdisciplinarne položaje; ker skoraj 90 % globalne delovne sile na področju kibernetske varnosti predstavljajo moški in ker stalna neuravnotežena zastopanost spolov še dodatno omejuje potencial talentov[1];

---

[1] Informativni dokument Evropskega računskega sodišča o izzivih za uspešno politiko EU za kibernetsko varnost, marec 2019.

J. ker so zmogljivosti za kibernetsko varnost med državami članicami raznolike, poročanje o incidentih in izmenjava informacij med njimi pa ni niti sistematično niti celovito, medtem ko uporaba centrov za izmenjavo in analizo informacij (ISAC) za izmenjavo informacij med javnim in zasebnim sektorjem ne izkoristi svojega potenciala;

K. ker na ravni EU ni dogovora o sodelovanju na področju kibernetskega obveščanja in skupnem odzivanju na kibernetske in hibridne napade; ker države članice tehnično in geopolitično zelo težko same izvajajo protiukrepe proti kibernetskim grožnjam in kibernetskim napadom, zlasti hibridnim;

L. ker sta čezmejna izmenjava podatkov in globalna izmenjava podatkov pomembni za ustvarjanje vrednosti, če so zagotovljeni zasebnost ter pravice intelektualne in industrijske lastnine; ker bi izvrševanje tuje zakonodaje o podatkih lahko pomenilo tveganje za kibernetsko varnost evropskih podatkov, saj za podjetja, ki delujejo v različnih regijah, veljajo prekrivajoče se obveznosti, ne glede na lokacijo podatkov ali njihov izvor;

M. ker je kibernetska varnost svetovni trg v vrednosti 600 milijard EUR, katerega obseg naj bi se hitro povečal, in ker je Unija neto uvoznica izdelkov in rešitev;

N. ker obstaja tveganje za razdrobljenost enotnega trga zaradi nacionalnih predpisov o kibernetski varnosti in pomanjkanja horizontalne zakonodaje v zvezi z bistvenimi zahtevami glede kibernetske varnosti za strojno in programsko opremo, vključno s povezanimi proizvodi in aplikacijami;

1. pozdravlja pobude, ki jih je Komisija predstavila v skupnem sporočilu z naslovom Strategija EU za kibernetsko varnost v digitalnem desetletju;

2. poziva k spodbujanju razvoja varnih in zanesljivih omrežij in informacijskih sistemov, infrastrukture in povezljivosti po vsej Uniji;

3. poziva, naj se določi cilj, da morajo biti vsi z internetom povezani proizvodi v Uniji, tudi za potrošniško in industrijsko uporabo, pa tudi celotne dobavne verige, ki te proizvode dajejo na voljo, varni in odporni na kibernetske incidente, če pa se ugotovi, da imajo šibke točke, morajo biti hitro odpravljene; pozdravlja, da namerava Komisija predlagati horizontalno zakonodajo o zahtevah glede kibernetske varnosti za povezane proizvode in pripadajoče storitve, ter poziva, naj v njej predlaga uskladitev nacionalnih zakonodaj, da bi preprečili razdrobljenost enotnega trga; poziva, naj se upošteva obstoječa zakonodaja (uredba o kibernetski varnosti, novi zakonodajni okvir, uredba o standardizaciji), da bi preprečili dvoumnost in razdrobljenost;

4. poziva Komisijo, naj oceni, ali je potreben predlog za horizontalno uredbo, ki bi do leta 2023 uvedla zahteve glede kibernetske varnosti za aplikacije, programsko opremo, vgrajeno programsko opremo in operacijske sisteme, in sicer na podlagi pravnega reda EU v zvezi z zahtevami za obvladovanje tveganja; poudarja, da zastarele aplikacije, programska oprema, vgrajena programska oprema in operacijski sistemi (tj. ki ne prejemajo več rednih popravkov in varnostnih posodobitev) predstavljajo nezanemarljiv delež vseh povezanih naprav in tveganje za kibernetsko varnost; poziva Komisijo, naj v svojem predlogu obravnava ta vidik; predlaga, naj v predlog vključi obveznost za proizvajalce, da vnaprej sporočijo minimalno obdobje, v katerem bodo zagotavljali varnostne popravke in posodobitve, da bodo kupci lahko sprejemali premišljene

odločitve; meni, da se morajo proizvajalci vključiti v program usklajenega razkrivanja šibkih točk, kot je določeno v predlogu direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji;

5. podarja, da bi morala biti kibernetska varnost vključena v digitalizacijo; zato poziva, naj projekti digitalizacije, ki jih financira Unija, vključujejo zahteve glede kibernetske varnosti; pozdravlja podporo raziskavam in inovacijam na področju kibernetske varnosti, zlasti v zvezi s prelomnimi tehnologijami (kot sta kvantno računalništvo in kvantna kriptografija), ki bi lahko destabilizirale mednarodno ravnovesje; poleg tega poziva k nadaljnjim raziskavam o postkvantnih algoritmih kot standardu kibernetske varnosti;

6. meni, da digitalizacija naše družbe pomeni, da so vsi sektorji med seboj povezani in da lahko slabosti v enem sektorju ovirajo druge; zato vztraja, da je treba politike kibernetske varnosti vključiti v digitalno strategijo EU in financiranje EU ter da morajo biti skladne in interoperabilne v vseh sektorjih;

7. poziva k usklajeni uporabi sredstev EU v zvezi s kibernetsko varnostjo in uvedbo s tem povezane infrastrukture; poziva Komisijo in države članice, naj zagotovijo izkoriščanje sinergij, povezanih s kibernetsko varnostjo, med različnimi programi, zlasti programom Obzorje Evropa, programom za digitalno Evropo, vesoljskim programom EU, mehanizmom EU za okrevanje in odpornost, programom InvestEU in instrumentom za povezovanje Evrope, ter naj v celoti izkoristijo strokovni center in mrežo za kibernetsko varnost;

8. želi spomniti, da je komunikacijska infrastruktura temelj vseh digitalnih dejavnosti in da je zagotavljanje njene varnosti strateška prednostna naloga Unije; podpira razvoj certifikacijske sheme EU za kibernetsko varnost za omrežja 5G; pozdravlja nabor orodij EU za kibernetsko varnost tehnologije 5G ter poziva Komisijo, države članice in industrijo, naj si še naprej prizadevajo za varna komunikacijska omrežja, tudi z ukrepi, ki se bodo nanašali na celotno dobavno verigo; poziva Komisijo, naj prepreči vezanost na ponudnika in poveča varnost omrežja s podpiranjem pobud, ki bodo krepile virtualizacijo in prenos različnih sestavnih delov omrežij v oblak; poziva k hitremu razvoju komunikacijskih tehnologij naslednje generacije, pri katerih bo vgrajena kibernetska varnost temeljno načelo in ki bodo zagotavljale varstvo zasebnosti in osebnih podatkov;

9. poudarja, da je treba vzpostaviti nov, trden varnostni okvir za kritične infrastrukture EU, da bi zaščitili varnostne interese EU in nadgradili obstoječe zmogljivosti za ustrezen odziv na tveganja, grožnje in tehnološke spremembe;

10. poziva Komisijo, naj pripravi določbe za zagotovitev dostopnosti, razpoložljivosti in celovitosti javnega jedra interneta ter s tem stabilnosti kibernetskega prostora, zlasti v zvezi z dostopom EU do svetovnega korenskega sistema DNS; meni, da bi morala v te določbe vključiti ukrepe za diverzifikacijo dobaviteljev, da bi se zmanjšalo sedanje tveganje odvisnosti od maloštevilnih podjetij, ki prevladujejo na trgu; pozdravlja predlog za evropski sistem domenskih imen (DNS4EU) kot orodje za odpornejše jedro interneta; poziva Komisijo, naj oceni, kako bi lahko ta sistem uporabljal najnovejše tehnologije, varnostne protokole in strokovno znanje o kibernetskih grožnjah, da bi vsem Evropejcem ponudili hiter, varen in odporen sistem domenskih imen; želi spomniti, da je treba bolje zaščititi protokol mejnih usmerjevalnikov, da bi preprečili

njihovo zlorabo; želi spomniti, da podpira model upravljanja interneta z več deležniki, pri čemer bi morala biti kibernetska varnost ena od osrednjih tem; poudarja, da bi morala EU pospešiti izvajanje internetnega protokola IPv6; priznava, da je odprtokodni model osnova za delovanje interneta in da se je izkazal za učinkovitega in uspešnega; zato spodbuja njegovo uporabo;

11. priznava, da je treba povečati forenziko kibernetske varnosti v boju proti kriminalu, kibernetski kriminaliteti in kibernetskim napadom, vključno z napadi pod pokroviteljstvom države, vendar svari pred nesorazmernimi ukrepi, ki bi ogrožali zasebnost in svobodo govora državljanov EU pri uporabi interneta; opozarja, da je treba zaključiti revizijo drugega dodatnega protokola k Budimpeški konvenciji o kibernetski kriminaliteti, ki bi lahko povečal pripravljenost na tovrstno kriminaliteto;

12. poziva Komisijo in države članice, naj združijo svoja sredstva za povečanje strateške odpornosti EU, zmanjšanje njene odvisnosti od tujih tehnologij ter spodbujanje njenega vodilnega položaja in konkurenčnosti na področju kibernetske varnosti v digitalni dobavni verigi (vključno s shranjevanjem in obdelavo podatkov v oblaku, procesorskimi tehnologijami, integriranimi vezji (čipi), ultra varno povezljivostjo, kvantnim računalništvom in omrežji naslednje generacije);

13. meni, da je načrtovana ultra varna infrastruktura za povezljivost pomemben instrument za varnost občutljivih digitalnih komunikacij; pozdravlja napovedani razvoj globalnega varnega vesoljskega komunikacijskega sistema EU, ki bo vključeval tehnologije kvantnega šifriranja; opozarja, da si je treba v sodelovanju z Agencijo Evropske unije za vesoljski program (EUSPA) in Evropsko vesoljsko agencijo (ESA) nenehno prizadevati za zagotavljanje evropskih vesoljskih dejavnosti;

14. poudarja, da zasebni in javni sektor nista dobro sprejela praks izmenjave informacij v zvezi s kibernetskimi grožnjami in incidenti; poziva Komisijo in države članice, naj povečajo zaupanje in zmanjšajo ovire za izmenjavo informacij o kibernetskih grožnjah in kibernetskih napadih na vseh ravneh; pozdravlja prizadevanja nekaterih sektorjev in poziva k medsektorskemu sodelovanju, saj se šibke točke redko nanašajo le na en sektor; poudarja, da morajo države članice združiti moči na evropski ravni, da bi učinkovito izmenjevale svoje najnovejše znanje o tveganjih za kibernetsko varnost; spodbuja oblikovanje delovne skupine držav članic za kibernetsko obveščevalno dejavnost, da bi spodbudili izmenjavo informacij v EU in evropskem gospodarskem prostoru, zlasti za preprečevanje obsežnih kibernetskih napadov;

15. pozdravlja načrtovano ustanovitev skupne kibernetske enote za povečanje sodelovanja med organi EU in organi držav članic, pristojnimi za preprečevanje kibernetskih napadov, odvračanje od njih in odzivanje nanje; poziva države članice in Komisijo, naj še povečajo sodelovanje na področju kibernetske obrambe in izvajajo raziskave najsodobnejših zmogljivosti za kibernetsko obrambo;

16. želi spomniti, kako pomemben je človeški faktor pri strategiji za kibernetsko varnost; poziva k nadaljnjim prizadevanjem za širjenje ozaveščenosti o kibernetski varnosti, vključno s kibernetsko higieno in kibernetsko pismenostjo;

17. poudarja pomen trdnega in doslednega varnostnega okvira za zaščito vsega osebja, podatkov, komunikacijskih omrežij in informacijskih sistemov EU ter postopkov odločanja pri boju proti kibernetskim grožnjam, ki temeljijo na celovitih, doslednih in

homogenih pravilih ter ustreznem upravljanju; poziva, naj se zagotovijo zadostna sredstva in zmogljivosti, tudi zaradi okrepitve mandata skupine CERT-EU in glede na potekajoče razprave o opredelitvi skupnih zavezujočih pravil o kibernetski varnosti za vse institucije, organe in agencije EU;

18. poziva k širši uporabi prostovoljnega certificiranja in standardov kibernetske varnosti, saj so pomembna orodja za izboljšanje splošne ravni kibernetske varnosti; pozdravlja vzpostavitev evropskega certifikacijskega okvira in delo Evropske certifikacijske skupine za kibernetsko varnost; poziva agencijo ENISA in Komisijo, naj pri pripravi Evropske certifikacijske sheme za kibernetsko varnost za storitve v oblaku razmisli o obvezni uporabi prava EU v zvezi z „visoko“ ravnjo zanesljivosti;

19. poudarja, da je treba nadaljevati prizadevanja na področju izobraževanja in usposabljanja in tako povpraševanje po delovni sili na področju kibernetske varnosti uskladiti z odpravo vrzeli v znanjih in spretnostih; poziva, naj se posebno pozornost nameni odpravi razlik med spoloma, ki so prisotne tudi v tem sektorju;

20. priznava, da je treba bolj podpreti mikro, mala in srednja podjetja, da bi bolje razumela vsa tveganja za informacijsko varnost in priložnosti za izboljšanje svoje kibernetske varnosti; poziva agencijo ENISA in nacionalne organe, naj razvijejo portale za samotestiranje in vodnike z dobrimi praksami za mikro, mala in srednja podjetja; želi spomniti, kako pomembna sta usposabljanje in dostop do namenskih sredstev za varnost teh subjektov;

21. naroči svojemu predsedniku, naj to resolucijo posreduje Komisiji, Svetu ter vladam in parlamentom držav članic.