Europa-Parlamentet
2019-2024

VEDTAGNE TEKSTER

P9_TA(2021)0286

EU's strategi for cybersikkerhed for det digitale årti

Europa-Parlamentets beslutning af 10. juni 2021 om EU's strategi for cybersikkerhed for det digitale årti (2021/2568(RSP))

Europa-Parlamentet,

– der henviser til den fælles meddelelse fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik af 16. december 2020 med titlen "EU's strategi for cybersikkerhed for det digitale årti" (JOIN(2020)0018),

– der henviser til Kommissionens forslag af 16. december 2020 til Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (COM(2020)0823),

– der henviser til Kommissionen forslag af 24. september 2020 til om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014 (COM(2020)0595),

– der henviser til Kommissionens forslag af 12. september 2018 til Europa-Parlamentets og Rådets forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre (COM(2018)0630),

– der henviser til Kommissionens meddelelse af 19. februar 2020 med titlen "Europas digitale fremtid i støbeskeen" (COM(2020)0067),

– der henviser til Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed)[1],

– der henviser til Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på

[1] EUT L 151 af 7.6.2019, s. 15.

markedet og om ophævelse af direktiv 1999/5/EF[1],

– der henviser til Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation[2],

– der henviser til Europa-Parlamentets og Rådets forordning (EU) nr. 1290/2013 af 11. december 2013 om reglerne for deltagelse og formidling i "Horisont 2020 – rammeprogrammet for forskning og innovation (2014-2020)" og om ophævelse af forordning (EF) nr. 1906/2006[3],

– der henviser til Europa-Parlamentets og Rådets forordning (EU) nr. 1291/2013 af 11. december 2013 om Horisont 2020 – rammeprogram for forskning og innovation (2014-2020) og om ophævelse af afgørelse nr. 1982/2006/EF[4],

– der henviser til Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240[5],

– der henviser til Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer[6],

– der henviser til Budapestkonventionen om IT-kriminalitet af 23. november 2001 (ETS nr. 185),

– der henviser til sin beslutning af 16. december 2020 om en ny strategi for europæiske SMV'er[7],

– der henviser til sin beslutning af 25. marts 2021 om en europæisk strategi for data[8],

– der henviser til sin beslutning af 20. maj 2021 om Europas digitale fremtid i støbeskeen: fjernelse af hindringerne for et velfungerende digitalt indre marked og forbedring af anvendelsen af AI for de europæiske forbrugere[9],

– der henviser til sin beslutning af 21. januar 2021 om udligning af den kønsbestemte digitale kløft: Kvinders deltagelse i den digitale økonomi[10].

– der henviser til sin beslutning af 12. marts 2019 om sikkerhedstrusler forbundet med den stigende kinesiske teknologiske tilstedeværelse i EU og mulige foranstaltninger på

---

1 EUT L 153 af 22.5.2014, s. 62.
2 EUT L 321 af 17.12.2018, s. 36.
3 EUT L 347 af 20.12.2013, s. 81.
4 EUT L 347 af 20.12.2013, s. 104.
5 EUT L 166 af 11.5.2021, s. 1.
6 EUT L 207 af 6.8.2010, s. 1.
7 Vedtagne tekster, P9_TA(2020)0359.
8 Vedtagne tekster, P9_TA(2021)0098.
9 Vedtagne tekster, P9_TA(2021)0261.
10 Vedtagne tekster, P9_TA(2021)0026.

EU-plan til at mindske dem[1] ,

– der henviser til forespørgsel til Kommissionen om EU's strategi for cybersikkerhed for det digitale årti (O-000037/2021 – B9-0024/2021),

– der henviser til forretningsordenens artikel 136, stk. 5, og artikel 132, stk. 2,

A. der henviser til, at den digitale omstilling er en central strategisk prioritet for Unionen, og som i sagens natur er forbundet med øget eksponering for cybertrusler;

B. der henviser til, at antallet af forbundne enheder, herunder maskiner, sensorer, industrielle komponenter og netværk, der udgør tingenes internet (IoT), fortsat stiger, idet 22,3 mia. enheder forventes at være forbundet med IoT på verdensplan inden 2024, hvilket øger eksponeringen for cyberangreb;

C. der henviser til, at teknologiske fremskridt – f.eks. kvantedatabehandling, og asymmetriske adgangsforhold hertil – vil kunne vende op og ned på cybersikkerhedsområdet;

D. der henviser til, at coronakrisen yderligere har afdækket cyber-sårbarhederne inden for flere kritisk vigtige sektorer, herunder ikke mindst sundhedsvæsenet, og til at de medfølgende foranstaltninger i form af telearbejde og social distancering har øget vores afhængighed af digital teknologi og onlineforbindelser, samtidig med at der over hele Unionen er sket en stigning i antal og grad af udspekulerethed inden for cyberangreb og cyberkriminalitet, herunder spionage og sabotage såvel som indbrud i og manipulation af IT-systemer, -strukturer og -netværk ved hjælp af ondsindede og ulovlige installationer;

E. der henviser til, at antallet af cyberangreb er steget betydeligt, som den seneste række ondsindede og organiserede cyberangreb på sundhedssystemer i bl.a. Irland, Finland og Frankrig vidner om; der henviser til, at disse cyberangreb forårsager betydelig skade på sundhedssystemer og patientpleje samt på andre følsomme offentlige og private institutioner;

F. der henviser til, at hybride trusler er i fremmarch, herunder i form af desinformationskampagner og cyberangreb på infrastruktur, økonomiske processer og demokratiske institutioner, og indebærer stadig mere alvorlige implikationer i både cyberspace og den fysiske verden og fare for, at dette vil påvirke de demokratiske processer såsom valg, lovgivning, retshåndhævelse og justits;

G. der henviser til, at der forekommer en stigende afhængighed af internettets kernefunktion og af essentielle internettjenester til formål som kommunikation og hosting, applikationer og data, for hvilke markedsandelen gradvist koncentreres på stadig færre virksomhedshænder;

H. der henviser til, at mulighederne for at foretage DDoS-angreb (distributed denial of service-angreb) er voksende, og derfor bør kerneinternettets modstandsdygtighed tilsvarende styrkes;

I. der henviser til, at cybersikkerhedsberedskab og -bevidsthed blandt virksomheder,

---

[1] EUT C 23 af 21.1.2021, s. 2.

navnlig SMV'er og enkeltpersoner, fortsat er ringe, at der er mangel på fagkyndig arbejdskraft (hullet i arbejdsstyrken er vokset med 20 % siden 2015) og at de traditionelle rekrutteringskanaler ikke kan følge med efterspørgslen, herunder for ledende og tværfaglige stillinger; der henviser til, at næsten 90 % af den globale arbejdsstyrke inden for cybersikkerhed er mænd, og at den vedvarende mangel på kønsdiversitet begrænser talentmassen yderligere[1];

J. der henviser til, at cybersikkerhedskapaciteter er ulige medlemsstaterne imellem, og at deling af hændelsesrapporter og information mellem dem hverken er systematisk eller tilstrækkeligt omfattende, samtidig med at anvendelse af informationsdelings- og analysecentre til formidling af information mellem den offentlige og den private sektor ikke indfrier sit potentiale;

K. der henviser til. at der ikke findes nogen EU-aftale om efterretningssamarbejde på cyberområdet eller kollektive modtræk over for cyberangreb og hybride angreb; der henviser til, at modforanstaltninger over for cybertrusler og cyberangreb, navnlig af hybrid art, er både teknisk og geopolitisk vanskelige for medlemsstaterne at håndtere på egen hånd;

L. der henviser til, at tværnational datadeling og global datadeling er vigtige for værdiskabelsen, forudsat at der værnes om privatlivets fred og intellektuelle ejendomsrettigheder; der henviser til, at håndhævelsen af udenlandske datalove vil kunne udgøre en cybersikkerhedstrussel mod EU-data i betragtning af, at virksomheder, der opererer inden for flere forskellige geografiske områder, er underlagt overlappende forpligtelser uanset dataenes anbringelses- eller oprindelsessted;

M. der henviser til, at cybersikkerhed udgør et globalt marked på 600 mia. EUR, og at dette beløb forventes at vokse hurtigt, og at Unionen er nettoimportør af produkter og løsninger;

N. der henviser til, at der er risiko for fragmentering af det indre marked på grund af nationale bestemmelser om cybersikkerhed og manglen på horisontal lovgivning vedrørende væsentlige cybersikkerhedskrav til hardware og software, herunder forbundne produkter og applikationer;

1. glæder sig over de initiativer, Kommissionen skitserer i sin fælles meddelelse om EU's strategi for cybersikkerhed for det digitale årti;

2. opfordrer til, at man fremmer udviklingen af sikrede og pålidelige netværks- og informationssystemer, infrastruktur og sammenkobling på tværs af Unionen;

3. opfordrer til at fastsætte som mål, at alle internetforbundne produkter i Unionen, herunder til forbrugere og industriel brug, og langs de forsyningskæder, der gør produkterne tilgængelige, skal være "secured-by-design" (fremstillet med integrerede sikkerhedsmekanismer), modstandsdygtige over for cyberhændelser og hurtigt skal kunne udbedres, når der konstateres sårbarheder; glæder sig over Kommissionens planer om at foreslå horisontal lovgivning om cybersikkerhedskrav for forbundne produkter og tilknyttede tjenester og anmoder om, at en sådan lovgivning foreslår harmonisering af

---

[1] Den Europæiske Revisionsret: Challenges to effective EU cybersecurity policy Briefing Paper, marts 2019.

nationale love for at undgå fragmentering af det indre marked; anmoder om, at der tages hensyn til allerede gældende ret (forordning om cybersikkerhed, de nye lovgivningsmæssige rammer, standardiseringsforordningen) for at undgå tvetydighed og fragmentering;

4. opfordrer Kommissionen til at vurdere behovet for et forslag til en horisontal forordning om indførelse af cybersikkerhedskrav for applikationer, software, indlejret software og operativsystemer inden 2023, der bygger på gældende EU-ret vedrørende krav til risikostyring; fremhæver, at forældede applikationer, software, indlejret software og operativsystemer (dvs. som ikke længere modtager regelmæssige patches og sikkerhedsopdateringer) udgør en ikke ubetydelig andel af alle forbundne enheder og en cybersikkerhedsrisiko; opfordrer Kommissionen til at medtage dette aspekt i sit forslag; foreslår, at forslaget bør omfatte forpligtelser for producenterne til på forhånd at oplyse om de minimumsperioder, hvori de yder sikkerhedspatches og opdateringer, således at køberne kan træffe velunderbyggede valg; mener, at producenterne skal indgå i programmet for koordineret offentliggørelse af sårbarheder som omhandlet i forslaget til NIS2-direktivet;

5. understreger, at cybersikkerhed bør integreres i digitaliseringen; opfordrer derfor til, at digitaliseringsprojekter, der finansieres med EU-midler, skal være omfattet af cybersikkerhedskrav; glæder sig over støtten til forskning og innovation inden for cybersikkerhed, navnlig om disruptiv teknologi (såsom kvantedatabehandling og kvantekryptografi), hvis fremvækst vil kunne forstyrre den internationale balance; opfordrer endvidere til yderligere forskning i post-kvantealgoritmer som en cybersikkerhedsstandard;

6. finder, at digitaliseringen af vores samfund betyder, at alle sektorer er forbundne, således at svagheder i én sektor også vil virke hæmmende på andre; fastholder derfor, at cybersikkerhedspolitikker skal inkorporeres i EU's digitale strategi og finansiering, og at de skal være sammenhængende og interoperable på tværs af sektorerne;

7. opfordrer til sammenhæng i anvendelsen af EU-midler til cybersikkerhedsformål og dermed forbunden opstilling af infrastruktur; opfordrer Kommissionen og medlemsstaterne til at drage omsorg for, at der drages nytte af cybersikkerhedsrelateret synergi mellem forskellige programmer, navnlig Horisont Europa, et digitalt Europa, rumprogrammet, EU's genopretnings- og resiliensfacilitet, InvestEU og Connecting Europe-faciliteten, samt at der gøres fuldt brug af Forskningskompetencecentret for Cybersikkerhed og dets netværk;

8. minder om, at kommunikationsinfrastruktur er hjørnestenen i al digital aktivitet, og at det er en strategisk prioritet for Unionen at tilsikre fuld beskyttelse heraf; bakker op om den igangværende udformning af EU-ordningen for cybersikkerhedscertificering af 5G-net; glæder sig over EU-værktøjskassen for 5G-cybersikkerhed og opfordrer Kommissionen, medlemsstaterne og branchen til at fortsætte deres bestræbelser på at opnå sikrede kommunikationsnetværk, herunder også foranstaltninger beregnet på forsyningskæden i dens fulde udstrækning; opfordrer Kommissionen til at undgå fastlåsning af leverandører og til at udbygge netværkssikkerhed ved at yde opbakning til initiativer, der udbygger virtualisering og "cloud-gørelse" af de forskellige komponenter i netværkene; opfordrer til en skyndsom udvikling af den næste generation af kommunikationsteknologi med integreret cybersikkerhedselementer som et grundlæggende princip og som tilsikrer beskyttelse af privatlivets fred og persondata;

9. gentager, at det er vigtigt at opstille nye, robuste sikkerhedsrammer for EU's kritisk vigtige infrastruktur for at beskytte EU's sikkerhedsinteresser og bygge videre på eksisterende kapaciteter til at reagere hensigtsmæssigt på risici, trusler og teknologiske ændringer;

10. opfordrer Kommissionen til at udarbejde bestemmelser, der skal tilsikre tilgængelighed, rådighed og integritet i den offentlige kerne af internettet og dermed stabilitet ved cyberspace, navnlig for så vidt angår EU's adgang til det globale DNS-rootsystem; mener, at sådanne bestemmelser bør indbefatte foranstaltninger til diversificering af leverandører for dermed at mindske den nuværende risiko for afhængighed af enkelte virksomheder med markedsdominans; glæder sig over forslaget til et EU-domænenavnssystem (DNS4EU) som et middel til at styrke internettets kernes modstandskraft; anmoder Kommissionen om at evaluere, hvordan dette DNS4EU kan anvende de nyeste teknologier, sikkerhedsprotokoller og ekspertise inden for cybertrusler til at tilbyde et hurtigt, sikkert og modstandsdygtigt DNS til alle europæere; minder om nødvendigheden af en bedre beskyttelse af BGP (Border Gateway Protocol) for at forhindre BGP-kapringer; minder om sin opbakning til en interessehaver-inklusiv model for internetstyring, hvor cybersikkerhed vil udgøre en af kernepunkterne; understreger, at EU bør fremskynde implementeringen af IPv6.; anerkender, at open source-modellen, der ligger til grund for internettets funktionsmåde, har vist sig nyttig og effektiv; tilskynder derfor til benyttelse heraf;

11. anerkender behovet for at højne cybersikkerhedskriminalteknik med henblik på at bekæmpe kriminalitet, cyberkriminalitet og cyberangreb, herunder også sager hvor en fremmed statsmagt står bag, men advarer mod uforholdsmæssige foranstaltninger, der vil bringe privatlivets fred og ytringsfriheden for EU's borgere i fare, når de bruger internettet; minder om nødvendigheden af at afslutte revisionen af anden tillægsprotokol til Budapestkonventionen om IT-kriminalitet, som har potentiale til at styrke beredskabet over for cyberkriminalitet;

12. opfordrer Kommissionen og medlemsstaterne til at sammenlægge deres ressourcer for dermed at udbygge EU's strategiske modstandskraft, reducere afhængigheden af fremmed teknologi og fremme dets lederskab og konkurrenceevne inden for cybersikkerhed på tværs af den digitale forsyningskæde (herunder datalagring og -behandling i cloud-steder, CPU-teknologi, integrerede kredsløb (mikrochips), ultrasikret konnektivitet, kvantedatabehandling og næste generation af netværker);

13. anser planen om ultrasikret konnektivitetsinfrastruktur for et vigtigt instrument til beskyttelse af følsom datakommunikation; glæder sig over meddelelsen om, at der skal udvikles et rumbaseret, globalt sikret kommunikationssystem i EU-regi, der vil inkorporere kvantekrypteringsteknologi; minder om, at der fortsat skal gøres bestræbelser på at skabe sikkerhed omkring EU's rumaktiviteter i samarbejde med Den Europæiske Unions Agentur for Rumprogrammet (EUSPA) og Den Europæiske Rumorganisation (ESA);

14. beklager, at informationsdelingspraksis angående cybertrusler og -hændelser ikke er synderligt indarbejdet i hverken den private eller den offentlige sektor; opfordrer Kommissionen og medlemsstaterne til at skabe øget tillid og mindske hindringer for udveksling af oplysninger om cybertrusler og cyberangreb på alle niveauer; glæder sig over den indsats, som er blevet gjort inden for en række sektorer, og opfordrer til tværsektorielt samarbejde, da sårbarheder sjældent er sektorspecifikke; fremhæver, at

medlemsstaterne skal slå sig sammen på EU-niveau for effektivt at kunne dele den senest indhentede viden om cybersikkerhedstrusler; opfordrer til, at der i medlemsstatsregi nedsættes en arbejdsgruppe om cyber-efterretningsarbejde med henblik på at fremme udvekslingen af oplysninger i EU og i det europæiske økonomiske rum, navnlig for at forhindre storstilede cyberangreb;

15. glæder sig over den planlagte oprettelse af en fælles cyber-enhed til styrkelse af samarbejdet mellem EU-organer og medlemsstatsmyndigheder med ansvar for at forebygge, afskrække og sætte ind over for cyberangreb; opfordrer medlemsstaterne og Kommissionen til yderligere at styrke cyberforsvarssamarbejdet og udvikle forskning i de mest avancerede cyberforsvarssystemer;

16. minder om den menneskelige faktors betydning for cybersikkerhedsstrategien; fremhæver, at det fortsat skal gøres en indsats for at højne bevidstheden om cybersikkerhed, herunder cyberhygiejne og cyberfærdigheder;

17. fremhæver betydningen af solide og konsekvente sikkerhedsrammer for at beskytte alt EU-personale, data, kommunikationsnet og informationssystemer samt beslutningsprocesser mod cybertrusler baseret på omfattende, konsekvente og ensartede regler og fyldestgørende styring; opfordrer til, at der stilles tilstrækkelige ressourcer og kapacitet til rådighed, herunder i forbindelse med styrkelsen af CERT-EU's mandat og med hensyn til de igangværende drøftelser om fastlæggelse af fælles bindende regler om cybersikkerhed for alle EU's institutioner, organer og agenturer;

18. opfordrer til øget anvendelse af frivillig certificering og cybersikkerhedsstandarder, eftersom sådanne tiltag udgør vægtige værktøjer til højnelse af det generelle niveau af cybersikkerhed. glæder sig over oprettelsen af den europæiske certificeringsramme og arbejdet i EU-gruppen for cybersikkerhedscertificering; opfordrer ENISA og Kommissionen til i forbindelse med EU-ordningen for cybersikkerhedscertificering af cloud-tjenesteydelser at overveje at indføre obligatorisk anvendelse af EU-retten for så vidt angår garantiniveauet "højt";

19. fremhæver, at det er nødvendigt at indfri efterspørgslen på cybersikkerhedskyndig arbejdskraft for at lukke kvalifikationskløften ved at videreføre bestræbelserne inden for uddannelse og oplæring; opfordrer til, at der især sættes fokus på helt at udligne lønforskellen mellem kønnene, der også findes inden for denne sektor;

20. anerkender behovet for bedre støtte til mikro-, små og mellemstore virksomheder for at øge deres forståelse af alle informationssikkerhedsrisici og muligheder for at forbedre deres cybersikkerhed; opfordrer ENISA og de nationale myndigheder til at udvikle selvtestportaler og retningslinjer for bedste praksis for mikro-, små og mellemstore virksomheder; minder om betydningen af oplæringskurser og adgang til særligt allokerede midler til disse enheders sikkerhed;

21. pålægger sin formand at sende denne beslutning til Kommissionen og Rådet samt til medlemsstaternes regeringer og parlamenter.