Europaparlamentet
2019-2024

Plenarhandling

B9-0305/2021

2.6.2021

FÖRSLAG TILL RESOLUTION

till följd av frågan för muntligt besvarande B9-0000/2021

i enlighet med artikel 136.5 i arbetsordningen

om EU:s strategi för cybersäkerhet för ett digitalt decennium
(2021/2568(RSP))

Cristian-Silviu Buşoi
för utskottet för industrifrågor, forskning och energi

B9-0305/2021

Europaparlamentets resolution om EU:s strategi för cybersäkerhet för ett digitalt decennium
(2021/2568(RSP))

Europaparlamentet utfärdar denna resolution

– med beaktande av det gemensamma meddelandet av den 16 december 2020 från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik *EU:s strategi för cybersäkerhet för ett digitalt decennium* (JOIN(2020)0018),

– med beaktande av kommissionens förslag av den 16 december 2020 till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, och upphävande av direktiv (EU) 2016/1148 (COM(2020)0823),

– med beaktande av kommissionens förslag av den 24 september 2020 till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, (COM(2020)0595),

– med beaktande av kommissionens förslag av den 12 september 2018 till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (COM(2018)0630),

– med beaktande av kommissionens meddelande av den 19 februari 2020 *Att forma EU:s digitala framtid* (COM(2020)0067),

– med beaktande av Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten)[1],

– med beaktande av direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG[2],

– med beaktande av Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation[3],

– med beaktande av Europaparlamentets och rådets förordning (EU) nr 1290/2013 av den 11 december 2013 om reglerna för deltagande och spridning i Horisont 2020 – ramprogrammet för forskning och innovation (2014–2020) och om upphävande av

[1] EUT L 151, 7.6.2019, s. 15.
[2] EUT L 153, 22.5.2014, s. 62.
[3] EUT L 321, 17.12.2018, s. 36.

förordning (EG) nr 1906/2006[4],

– med beaktande av Europaparlamentets och rådets förordning (EU) nr 1291/2013 av den 11 december 2013 om inrättande av Horisont 2020 – ramprogrammet för forskning och innovation (2014–2020) och om upphävande av beslut nr 1982/2006/EG[5],

– med beaktande av Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240[6],

– med beaktande av Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag[7],

– med beaktande av Budapestkonventionen om it-relaterad brottslighet av den 23 november 2001 (ETS nr. 185),

– med beaktande av sin resolution av den 16 december 2020 om en ny strategi för europeiska små och medelstora företag[8],

– med beaktande av sin resolution av den 25 mars 2021 om en EU-strategi för data[9],

– med beaktande av sin resolution av den 20 maj 2021 om formandet av EU:s digitala framtid och att få bort hindren för en fungerande digital inre marknad och förbättra användningen av AI för europeiska konsumenter[10]

– med beaktande av sin resolution av den 21 januari 2021 om överbryggande av den digitala klyftan mellan könen och kvinnors deltagande i den digitala ekonomin[11],

– med beaktande av sin resolution av den 12 mars 2019 om säkerhetshot kopplade till Kinas ökande teknologiska närvaro i EU och möjliga åtgärder på EU-nivå för att minska dem[12],

– med beaktande av frågan till kommissionen om EU:s strategi för cybersäkerhet för ett digitalt decennium (O-000037/2021 – B9-0000/2021),

– med beaktande av artiklarna 136.5 och 132.2 i arbetsordningen, och av följande skäl:

A. Den digitala omställningen är ett viktig strategisk prioritering för unionen som oundvikligen också innebär större utsatthet för cyberhot.

B. Antalet uppkopplade enheter, såsom maskiner, sensorer och industriella komponenter

[4] EUT L 347, 20.12.2013, s. 81.
[5] EUT L 347, 20.12.2013, s. 104.
[6] EUT L 166, 11.5.2021, s. 1.
[7] EUT L 207, 6.8.2010, s. 1.
[8] Antagna texter, P9_TA(2020)0359.
[9] Antagna texter, P9_TA(2021)0098.
[10] Antagna texter, P9_TA(2021)0261.
[11] Antagna texter P9_TA(2021)0026.
[12] Antagna texter P8_TA(2019)0156.

och nätverk som ingår i sakernas internet fortsätter att öka. 2024 förväntas 22,3 miljarder enheter vara förbundna genom sakernas internet, vilket gör att risken för cyberattacker ökar.

C. Tekniska framsteg – såsom kvantdatorteknik – och den ojämna tillgången till dessa, kan komma att utgöra ett problem för cybersäkerheten.

D. Genom covid-19-krisen har cyberriskerna inom vissa kritiska branscher blivit tydliga, i synnerhet inom hälso- och sjukvården, och åtgärder som distansarbete och social distansering har ökat vårt beroende av digital teknik och uppkoppling. Samtidigt ökar cyberattackerna medan cyberbrottsligheten har blir allt mer avancerad med bland annat spionage och sabotage och intrång i och manipulering av IKT-system, IKT-strukturer och IKT-nätverk genom skadliga och olagliga installationer.

E. Hybridhoten ökar, vilket även inkluderar desinformationskampanjer och cyberattacker mot infrastruktur, ekonomiska processer och demokratiska institutioner. Dessa hot är på väg att bli ett allvarligt problem inom såväl cybervärlden som den fysiska världen och riskerar att påverka demokratiska processer såsom val, lagstiftningsförfaranden, brottsbekämpning och rättsväsende.

F. Vi blir allt mer beroende av internets kärnfunktioner och grundläggande internettjänster för kommunikation, värdskap, applikationer och data, medan marknaden för detta koncentreras mer och mer till allt färre företag.

G. Förmågan att genomföra samordnade överbelastningsattacker (DDOS-attacker) ökar, och därför bör motståndskraften inom internets kärnfunktioner ökas parallellt.

H. Säkerhetsberedskapen och medvetenheten bland företag, i synnerhet små och medelstora företag och enmansföretag, är fortsatt låg och det råder brist på kvalificerad arbetskraft (arbetskraftsunderskottet har ökat med 20 % sedan 2015). De traditionella rekryteringskanalerna uppfyller inte efterfrågan, inbegripet för ledande och tvärdisciplinära befattningar. Nästan 90 % av dem som arbetar med cybersäkerhet världen över är män, och den konstanta bristen på jämn könsfördelning begränsar talangpoolen ytterligare[13].

I. Cybersäkerheten är heterogen mellan medlemsstaterna och incidentrapporteringen och informationsutbytet mellan dem är varken systematisk eller heltäckande, samtidigt som inte heller den potential som finns i informations- och analyscentralerna för att utbyta information mellan den offentliga och privata sektorn utnyttjas till fullo.

J. Det saknas enighet på EU-nivå om samarbete kring underrättelser om cyberhot och kollektiva svar på cyber- och hybridattacker. Det är tekniskt och geopolitiskt mycket svårt för en medlemsstat att på egen hand vidta motåtgärder mot cyberhot och cyberattacker, i synnerhet sådana av hybridkaraktär.

K. Gränsöverskridande datadelning och global datadelning är viktiga för värdeskapandet förutsatt att integriteten, de immateriella rättigheterna och äganderätten säkerställs.

[13] Europeiska revisionsrätten *Utmaningar för en ändamålsenlig EU politik för cybersäkerhet*, briefingdokument, mars 2019.

Efterlevnaden av utländska datalagar skulle kunna utgöra ett cyberhot mot europeisk data eftersom företag som verkar i olika regioner är föremål för överlappande skyldigheter oavsett var deras data kommer ifrån.

L. Cybersäkerheten är en global marknad värd 600 miljarder euro, vilket förväntas öka snabbt, och unionen är nettoimportör av produkter och lösningar.

M. Det finns en risk att den inre marknaden fragmenteras på grund av nationell cybersäkerhetslagstiftning och bristen på horisontell lagstiftning om cybersäkerhetskrav för maskinvara och programvara, inklusive anslutna produkter och applikationer.

1. Europaparlamentet välkomnar de initiativ som kommissionen har tagit i det gemensamma meddelandet med titeln *EU:s strategi för cybersäkerhet för ett digitalt decennium*.

2. Europaparlamentet vill se en utveckling av säkra och tillförlitliga nät- och informationssystem, infrastruktur och förbindelser i hela unionen.

3. Europaparlamentet vill att målet ska vara att alla internetanslutna produkter i unionen, inklusive produkter för konsument- och industriändamål och hela de leveranskedjor som gör dem tillgängliga, ska ha inbyggd säkerhet, vara motståndskraftiga mot cyberincidenter och snabbt kunna åtgärdas när sårbarheter upptäcks. Parlamentet välkomnar kommissionens planer på att föreslå en horisontell lagstiftning om cybersäkerhetskrav för uppkopplade produkter och tillhörande tjänster, och begär att man i denna lagstiftning ska harmonisera nationella lagar för att undvika en fragmentering av den inre marknaden. Parlamentet begär att den befintliga lagstiftningen (cybersäkerhetsakten, den nya lagstiftningsramen och förordningen om standardisering) ska beaktas för att undvika tvetydigheter och fragmentering.

4. Europaparlamentet uppmanar kommissionen att bedöma behovet av ett förslag om en horisontell reglering med cybersäkerhetskrav för applikationer, programvara, inbyggd programvara och operativsystem till 2023, vilket ska bygga på EU:s regelverk för riskhanteringskrav. Parlamentet betonar att föråldrade applikationer, programvara, inbyggd programvara och operativsystem (föråldrade på så sätt att de inte längre får regelbundna programfixar och säkerhetsuppdateringar) utgör en icke försumbar andel av alla uppkopplade enheter, vilket innebär en cybersäkerhetsrisk. Kommissionen uppmanas att inkludera denna aspekt i sitt förslag. Parlamentet föreslår att förslaget ska innehålla en skyldighet för tillverkarna att i förväg informera om en minimiperiod under vilken de kommer att stödja programfixar och uppdateringar så att köpare kan göra välgrundade val. Parlamentet anser att tillverkarna måste utgöra en del av programmet för samordnad information om sårbarheter i enlighet med NIS 2-direktivet

5. Europaparlamentet understryker att cybersäkerhet bör integreras i digitaliseringen. Parlamentet vill därför att digitaliseringsprojekt som finansieras av unionen ska inkludera krav på cybersäkerhet. Parlamentet välkomnar stöd för forskning och innovation inom cybersäkerhet, i synnerhet när det gäller omstörtande teknik (såsom kvantdatorteknik och kvantkryptografi) vars framväxt kan leda till en destabilisering av den internationella balansen. Dessutom behövs det ytterligare forskning om postkvantalgoritmer som en cybersäkerhetsstandard.

6. Europaparlamentet anser att digitaliseringen av vårt samhälle innebär att alla branscher är sammankopplade och att bristerna i en bransch kan hämma de övriga. Parlamentet kräver därför att cybersäkerhetsstrategierna ska införlivas i EU:s digitala strategi och EU-finansieringen, samt att de ska vara samstämda och interoperabla mellan de olika branscherna.

7. Europaparlamentet efterlyser en konsekvent användning av EU-medel när det gäller cybersäkerhet och relaterad infrastrukturutbyggnad. Kommissionen och medlemsstaterna uppmanas att se till att utnyttja cybersäkerhetsrelaterade synergier mellan olika program, i synnerhet Horisont Europa-programmet, programmet för ett digitalt Europa, EU:s rymdprogram, EU:s facilitet för återhämtning och resiliens, InvestEU och FSW, samt att fullt ut utnyttja kompetenscentrumet och nätverket för cybersäkerhet.

8. Europaparlamentet påminner om att kommunikationsinfrastruktur utgör en hörnsten i all digital verksamhet och att säkerställa säkerheten i denna är en strategisk prioritering för unionen. Parlamentet stöder utvecklingen av EU:s cybersäkerhetscertifiering för 5G-nätverk. Parlamentet välkomnar EU:s verktygslåda för 5G-cybersäkerhet och uppmanar kommissionen, medlemsstaterna och industrin att öka sina ansträngningar för att skapa säkra kommunikationsnät, inklusive åtgärder för hela leveranskedjan. Parlamentet uppmanar kommissionen att undvika inlåsning till vissa leverantörer och att förbättra nätverkssäkerheten genom att främja initiativ som stärker virtualiseringen och övergången till molntjänster för nätverkens olika delar. Parlamentet vill se en snabb utveckling av nästa generations kommunikationsteknik med inbyggd cybersäkerhet som en grundläggande princip och där skyddet av integriteten och personuppgifterna säkerställs.

9. Europaparlamentet upprepar vikten av en ny, robust säkerhetsram för EU-kritisk infrastruktur i syfte att värna om EU:s säkerhetsintressen och bygga vidare på befintlig kapacitet att agera vid risker, hot och tekniska förändringar.

10. Europaparlamentet uppmanar kommissionen att förbereda bestämmelser för att säkerställa tillträde, tillgänglighet och integritet i den öppna kärnan av internet och därmed även stabiliteten i cyberrymden, i synnerhet när det gäller EU:s tillgång till det globala systemet för rot-DNS. Parlamentet anser att sådana bestämmelser ska inkludera åtgärder för att få fler leverantörer och därmed motverka den nuvarande risken för att man måste förlita sig på de få företag som dominerar marknaden. Parlamentet välkomnar förslaget om ett europeiskt domännamnssystem (DNS4EU) som ett sätt att öka motståndskraften i internets kärnfunktioner. Kommissionen ombeds att utvärdera hur man inom DNS4EU skulle kunna utnyttja den senaste tekniken, säkerhetsprotokollen och kunskaperna om cyberhot för att skapa ett snabbt, säkert och motståndskraftigt domännamnssystem för hela Europa. Parlamentet påminner om behovet av att bättre skydda gränssnittsprotokollet (BGP) för att förhindra BGP-kapningar och om sitt stöd för en flerpartsmodell för internetstyrning, där cybersäkerhet skulle utgöra en av kärnfrågorna. Parlamentet understryker att EU bör påskynda införandet av IPv6 och uppskattar modellen med öppen källkod, som har visat sig vara effektiv och ändamålsenlig som grund för internets funktion. Parlamentet förespråkar därför att den används.

11. Europaparlamentet erkänner behovet av att öka kriminaltekniken inom cybersäkerheten för att bekämpa brottslighet, cyberbrott och cyberattacker, inklusive statsstödda attacker, men varnar för oproportionerliga åtgärder som äventyrar EU-medborgarnas integritet och yttrandefrihet på internet. Parlamentet påminner om behovet av att slutföra revisionen av det andra tilläggsprotokollet till Budapestkonventionen om it-brottslighet, som har potential att öka beredskapen mot cyberkriminalitet.

12. Europaparlamentet uppmanar kommissionen och medlemsstaterna att slå samman sina resurser för att öka EU:s strategiska motståndskraft, minska dess beroende av utländsk teknik samt stärka dess ledarskap och konkurrenskraft när det gäller cybersäkerhet inom hela den digitala leveranskedjan (inklusive databehandling i moln, processorteknik, integrerade kretsar (chips), ultrasäker uppkoppling, kvantdatorteknik och nästa generations nätverk).

13. Europaparlamentet anser att planen för en ultrasäker sammankopplingsinfrastruktur är ett viktigt instrument för säkerheten i känslig digital kommunikation. Parlamentet välkomnar meddelandet om utvecklingen av ett europeiskt rymdbaserat globalt och säkert kommunikationssystem som integrerar kvantkrypteringsteknik. Parlamentet påminner om att det behövs mer arbete tillsammans med Europeiska unionens rymdprogrambyrå och Europeiska rymdorganisationen för att säkerställa Europas rymdverksamhet.

14. Europaparlamentet beklagar att metoderna för informationsdelning kring cyberhot och cyberincidenter inte har anammats av den privata och offentliga sektorn. Parlamentet uppmanar kommissionen och medlemsstaterna att öka förtroendet och minska hindren för informationsutbyte om cyberhot och cyberattacker på alla nivåer. Parlamentet välkomnar de insatser som har gjorts i vissa branscher och efterlyser ett branschöverskridande samarbete eftersom sårbarheten sällan är sektorsspecifik. Medlemsstaterna måste samarbeta på europeisk nivå för att effektivt kunna dela sina senaste kunskaper om cybersäkerhetsrisker. Parlamentet vill se att medlemsstaterna inrättar en gemensam arbetsgrupp för cyberunderrättelseverksamhet för att främja informationsutbytet i EU och det Europeiska ekonomiska området samt i synnerhet förhindra storskaliga cyberangrepp.

15. Europaparlamentet välkomnar det planerade inrättandet av en gemensam cyberenhet för att stärka samarbetet mellan EU:s organ och de myndigheter i medlemsstaterna som ansvarar för att förebygga, avvärja och svara på cyberattacker. Parlamentet uppmanar medlemsstaterna och kommissionen att stärka cyberförsvarssamarbetet ytterligare och utveckla forskningen för att ha den senaste cyberförsvarskapaciteten.

16. Europaparlamentet påminner om betydelsen av den mänskliga faktorn i cybersäkerhetsstrategin. Parlamentet efterlyser fortsatta insatser för att öka medvetenheten om cybersäkerhet, cyberhygien och cyberkunnighet.

17. Europaparlamentet understryker vikten av att ha en robust och konsekvent säkerhetsram för att skydda all EU-personal, alla data, alla kommunikationsnät och alla informationssystem, samt att ha beslutsprocesser mot cyberhot som bygger på heltäckande, konsekventa och homogena regler och vederbörlig styrning. Parlamentet vill se att man frigör tillräckliga resurser och tillräcklig kapacitet, vilket även inkluderar

vid förstärkningen av mandatet för CERT-EU och när det gäller de pågående diskussionerna om definitionen av gemensamma bindande regler om cybersäkerhet för EU:s alla institutioner, organ och byråer.

18. Europaparlamentet vill se en mer utbredd användning av frivilliga certifierings- och cybersäkerhetsstandarder, eftersom de utgör viktiga verktyg för att förbättra den allmänna cybersäkerhetsnivån. Parlamentet välkomnar inrättandet av den europeiska certifieringsramen och det arbete som europeiska gruppen för cybersäkerhetscertifiering har lagt ner. Parlamentet uppmanar Enisa och kommissionen att göra det obligatoriskt att tillämpa EU-lagstiftningen för att nå nivån ”hög” när de utarbetar EU-ordningen för cybersäkerhetscertifiering av molntjänster.

19. Europaparlamentet understryker att efterfrågan på arbetskraft inom cybersäkerhet bör åtgärdas genom att man fortsätter att satsa på utbildning för att minska kunskapsluckan. Särskild uppmärksamhet bör ägnas åt att undanröja könsklyftan, som också finns i denna sektor.

20. Europaparlamentet erkänner behovet av att ge bättre stöd till mikroföretag och små och medelstora företag för att öka deras förståelse för alla it-säkerhetsrisker och informera dem om vilka möjligheter det finns att förbättra cybersäkerheten. Enisa och de nationella myndigheterna uppmanas att utveckla självtestportaler och bästa praxis-vägledningar för mikroföretag och små och medelstora företag. Parlamentet påminner om behovet av utbildning och tillgång till särskild finansiering för säkerheten i dessa entiteter.

21. Europaparlamentet uppdrar åt talmannen att översända denna resolution till kommissionen och rådet samt till medlemsstaternas regeringar och parlament.