Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om fælles meddelelse til Europa-Parlamentet og Rådet: EU's politik for cyberforsvar

(initiativudtalelse)

(2023/C 293/04)

Ordfører: **Anastasis YIAPANIS**

Medordfører: **Alberto MAZZOLA**

Plenarforsamlingens beslutning	20.9.2022
Retsgrundlag	Forretningsordenens artikel 52, stk. 2
	Initiativudtalelse
Kompetence	Den Rådgivende Kommission for Industrielle Ændringer (CCMI)
Vedtaget i sektionen	27.3.2023
Vedtaget på plenarforsamlingen	14.6.2023
Plenarforsamling nr.	579
Resultat af afstemningen	
(for/imod/hverken for eller imod)	208/1/2

1. **Konklusioner og anbefalinger**

1.1. Det Europæiske Økonomiske og Sociale Udvalg (EØSU) støtter den foreslåede EU-politik for cyberforsvar, men havde forventet, at det organiserede civilsamfund ville få tildelt en mere fremtrædende rolle i udarbejdelsen af disse forslag. EØSU finder det på nuværende tidspunkt vanskeligt at vurdere, om de fremtidige initiativer, der er skitseret i den fælles meddelelse, vil blive gennemført og opnå de ønskede resultater. Udvalget opfordrer indtrængende EU-institutionerne og medlemsstaterne til at prioritere og gå hurtigt videre med de bebudede initiativer.

1.2. EØSU understreger, at der er behov for yderligere foranstaltninger, der kan forbedre EU's evne til at opdage cybertrusler, og opfordrer til, at finansieringen af forskning og udvikling rettes mod udvikling af banebrydende EU-kapacitet. Samarbejde mellem den private og den offentlige sektor er afgørende og må ikke kun gå en vej. EØSU mener, at det er nødvendigt med koordinering på EU-plan for at afhjælpe fragmentering og sikre samarbejde og fælles investeringer mellem medlemsstaterne.

1.3. EØSU støtter oprettelsen af EU's koordinationscenter for cyberforsvar og anbefaler, at medlemsstaterne forpligter sig til hurtig reaktion døgnet rundt og evaluerer cyberberedskabet og effektiviteten af EU's cyberberedskabsmekanismer med fokus på både militære kapaciteter og kritiske sektorer som kortlagt i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([1]) (NIS 2-direktivet). Udvalget støtter udvidelsen af mandatet for Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC), så det kan bistå arbejdet i EU's koordinationscenter for cyberforsvar.

1.4. For at styrke Unionens strategiske autonomi og suverænitet på cybersikkerhedsområdet mener EØSU, at der bør udvikles eller overtages en dynamisk platform for test i realtid og informationsudveksling fra den private sektor med henblik på at afdække de nuværende mangler i den eksisterende kapacitet. Platformen kan også anvendes til at udveksle bedste praksis, indberette cyberhændelser og udarbejde en EU-liste over alle cyberkriminelle.

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

1.5. EØSU fremhæver behovet for et bedre beredskab over for cyberangreb som f.eks. de russiske i Ukraine, der navnlig er rettet mod kritisk infrastruktur. Samarbejde mellem civile og militære økosystemer er afgørende for effektiv krisestyring og interoperabilitet samt for at undgå dobbeltarbejde og dobbeltinvesteringer, herunder gennem simulerede test af cyberangreb.

1.6. EØSU mener, at beskyttelse af EU-borgerne og kritisk infrastruktur bør have første prioritet, når der investeres i cyberforsvar, herunder ved at der anvendes pålidelige hardware- og softwareleverandører. Udvalget insisterer på jævnlige ajourføringer af prioriteter og investeringer, som EU og medlemsstaterne skal nå til enighed om under inddragelse af relevante private interessenter.

1.7. EU skal bevare og udvikle den nødvendige kapacitet til at sikre sin digitale økonomi, sit digitale samfund, sit demokrati og kritiske teknologier og til at levere centrale cybersikkerhedstjenester. For at sikre EU's strategiske autonomi er det afgørende at mindske afhængigheden af tredjelande. EØSU mener, at det er vigtigt, at EU vedtager en strategi for autonomi på mellemlang sigt for så vidt angår nøgleteknologier, og går stærkt ind for, at EU-baserede virksomheder etablerer forsknings- og produktionsfaciliteter, hvilket skal ledsages af en passende europæisk industripolitik, der fokuserer på et selvstændigt cyberøkosystem.

1.8. SMV'er bør modtage målrettet støtte og have adgang til finansieringsprogrammer, der øger deres modstandsdygtighed over for cyberangreb. De bør ligeledes have tilbud om støtte og uddannelse i cyberrisici, og hvordan de kan beskytte sig mod dem. EU bør indføre en incitamentsordning, der fremmer en gradvis udvikling af SMV'ers viden på området og udvikling af innovative SMV'er.

1.9. EØSU støtter planen om at oprette et akademi for cyberfærdigheder og anmoder Kommissionen om at koordinere og finansiere omfattende uddannelses- og erhvervsuddannelsesprogrammer, der omfatter alle medlemsstater og sigter mod at skabe en kvalificeret arbejdsstyrke til alle agenturer og organisationer, der beskæftiger sig med cyberforsvar, samt til private civile netværk.

1.10. Udvalget mener, at det er afgørende at øge borgernes bevidsthed om cybersikkerhed for at mindske eksponeringen for cyberangreb, og efterlyser læseplaner i cybersikkerhed og programmer for livslang uddannelse med fokus på forbedring af cyberfærdigheder og -viden. EØSU støtter, at cybersikkerhed integreres i alle EU's fremtidige offentlige politikker, og at den brede offentlighed informeres om cybertrusler.

1.11. EØSU mener, at et stærkt samarbejde med NATO-allierede på militære områder skal fokusere på fuld koordinering og gensidighed, fælles FUI-projekter, udveksling af bedste praksis, omfattende uddannelsesprogrammer og simuleringer af cyberangreb med det hovedformål at udvide den fælles reaktionskapacitet.

1.12. Udvalget opfordrer den højtstående repræsentant til at gennemgå de nuværende bilaterale cyberdialoger og indlede yderligere drøftelser med andre lande og relevante internationale organisationer med det formål at etablere en verdensomspændende ramme for overholdelse af folkeretten i cyberspace med stor vægt på gensidighed. Udvalget mener, at EU har gode forudsætninger for at gå forrest i internationale drøftelser om den fremtidige cybersikkerhed, navnlig i FN, da Unionen har et stærkt fundament, hvad angår grundlæggende demokratiske frihedsrettigheder.

1.13. EU bør tage klart afstand fra enhver form for socialt pointsystem over for borgerne. EØSU gør det klart, at et ægte demokrati ikke kan eksistere uden effektiv beskyttelse af personoplysninger, og mener, at ansvarlig og velfungerende dataforvaltning er afgørende for at gøre hyperkonnektivitet til en konkurrencemæssig fordel.

2. **Indledning og generelle bemærkninger**

2.1. Den stadig større digitalisering af samfundet medfører en lang række cybersikkerhedstrusler som følge af de teknologiske opgraderinger. Antallet af cyberangreb og deres kompleksitet er vokset betydeligt i de senere år, hvilket undergraver sikkerheden for både offentlige og private enheder. Uanset om vi taler om ransomware, malware, e-mailangreb, brud på datasikkerheden, desinformation, distributed denial of service-angreb (DDoS) eller andre former for angreb, udgør de alle en konsekvent og vedvarende trussel mod EU's sikkerhed som helhed.

2.2. EØSU glæder sig over den fælles meddelelse om *EU's politik for cyberforsvar* ([2]) og mener, at tiden nu er inde til at handle hurtigt og på en koordineret måde på EU-plan, hvilket bør involvere både civile og militære cyberspaceøkosystemer og en passende investeringsramme for cyberforsvarskapaciteter. Udvalget bemærker imidlertid, at meddelelsen blot er en hensigtserklæring og opstiller en liste over fremtidige EU-initiativer, der skal levere resultater. EØSU finder det umuligt at vurdere, om der reelt vil blive fulgt op på disse tilsagn, eftersom fremtidige forhandlinger mellem medlovgiverne naturligvis vil påvirke det endelige resultat af EU's handlingsplan for cybersikkerhed.

2.3. Det russiske angreb på KA-SAT-satellitnetværket, som forstyrrede kommunikationen mellem de ukrainske militære styrker, og den nylige skandale om Éric Léandri, som nogle forsvarsvirksomheder havde engageret til at udøve cyberspionage på deres vegne, sætter cybersikkerhed øverst på listen over sikkerhedstrusler i EU. Selv om den generelle forordning om databeskyttelse er en solid EU-retsakt og har været i kraft i flere år, står det klart, at den stigende mængde data, der er til rådighed, er sårbar, og risikoen for, at tredjeparter overskrider grænsen for det lovlige, bliver større hver dag.

2.4. I betragtning af cyberangrebenes tværnationale karakter er det nødvendigt med koordinering på EU-plan for at mindske den nuværende fragmentering og sikre, at medlemsstaterne er parate til at samarbejde og investere i fællesskab. Dette er især vigtigt i fremtidige tilfælde, hvor én medlemsstat kan være mål for et angreb, og alle andre bør have mulighed for at yde øjeblikkelig støtte.

3. **Fælles handling for at styrke cyberforsvaret**

3.1. Udvalget noterer sig de bebudede ambitiøse initiativer til oprettelse af et EU-koordinationscenter for cyberforsvar, udvikling af CyDEf-X-projektet, oprettelse af cyberberedskabshold, der kan reagere hurtigt, udvikling af et EU-cybersolidaritetsinitiativ og undersøgelse af mulighederne for at udvikle cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer. EØSU anbefaler, at alle medlemsstater forpligter sig til at kunne reagere hurtigt døgnet rundt, og at EU's koordinationscenter inddrages i vurderingen og udarbejdelsen af regelmæssige rapporter om medlemsstaternes cyberberedskab og effektiviteten af den europæiske cyberberedskabsmekanisme med fokus på både militære kapaciteter og kritiske sektorer som kortlagt i NIS 2-direktivet. Hver medlemsstat bør have specialister, der er særligt uddannet til at gribe ind i tilfælde af cyberhændelser, og bør regelmæssigt teste deres interventionskapacitet i andre medlemsstater.

3.2. Selv om meddelelsen indeholder en lang liste over trinvise forbedringer, havde EØSU gerne set en klar køreplan for gennemførelsen af disse initiativer med en klar styring og frister for indgivelse og vedtagelse. EØSU havde desuden forventet, at det organiserede civilsamfund ville få tildelt en mere fremtrædende rolle i udarbejdelsen af disse forslag.

3.3. EØSU er af den opfattelse, at medlemsstaterne er nødt til at styrke deres interne kapacitet for at kunne imødegå cybertrusler og samtidig indgå i samarbejdsprojekter og dele oplysninger og bedste praksis med deres partnere i andre medlemsstater. Der er behov for hurtige investeringer i cyberforsvarskapaciteter og hurtigere udrulning af teknologi ([3]) i alle medlemsstater og i et fælles beredskab, der kan opdage, genoprette efter og forsvare imod cyberangreb. For at styrke Unionens autonomi på cybersikkerhedsområdet mener EØSU, at der bør udvikles eller overtages en dynamisk platform for test og informationsudveksling i realtid fra den private sektor med henblik på at afdække de nuværende mangler i den eksisterende kapacitet.

3.4. EØSU er enig i, at militære cyberoperationer på nuværende tidspunkt udelukkende bør høre under medlemsstaternes kompetence. Udvalget støtter det bebudede samarbejde mellem EU's militære IT-beredskabsenheder (milCERT'er), enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er) og IT-beredskabsenheden under EU's institutioner, organer og agenturer (CERT-EU).

3.5. Det nyligt vedtagne NIS 2-direktiv og direktivet om kritiske enheders modstandsdygtighed (CER) ([4]) har allerede indført specifikke nationale og sektorspecifikke forpligtelser i relation til EU's ramme for cyberforsvar. Der er behov for en yderligere indsats for at forbedre EU's kollektive opdagelseskapacitet, og EØSU efterlyser FoU-investeringer, der skal udvikle banebrydende EU-kapaciteter.

([2]) Meddelelse fra Kommissionen om EU's politik for cyberforsvar.
([3]) F.eks. NATO's forsvarsinnovationsaccelerator for Nordatlanten (DIANA).
([4]) Direktivet om kritiske enheders modstandsdygtighed.

4. **Sikring af EU's forsvarsøkosystem**

4.1. EØSU mener, at den iboende kompleksitet og teknologiske udfordringer i hastig udvikling har ændret forsvarsøkosystemet, og at cybersikkerhed er blevet et fælles interesseområde for både den militære og den civile sektor og for EU-borgerne. Samarbejde mellem civile og militære økosystemer er nu vigtigere end nogensinde og bør give fordele i form af en mere effektiv krisestyring samt løbende fremskridt og interoperabilitet, så man undgår overlapning eller dobbeltarbejde og dobbeltinvesteringer. Medlemsstaterne bør være klar til at gennemføre nationale stresstest af kritisk infrastruktur med henblik på at vurdere og øge modstandsdygtigheden over for fremtidige cyberangreb.

4.2. EØSU mener, at beskyttelse af EU-borgerne og kritisk infrastruktur må have første prioritet, når der investeres i cyberforsvar. I betragtning af den hurtige digitale omstilling og den hastige udvikling i trusselsbilledet opfordrer udvalget kraftigt til, at EU og medlemsstaterne når til enighed om rettidige ajourføringer af prioriteter og investeringer med en grundig høring af relevante private interessenter. Enheder til tingenes internet (IoT) er ofte ikke så godt beskyttet som traditionelt udstyr, og EØSU opfordrer til, at der garanteres et minimumssikkerhedsniveau gennem IDAM-platforme. Eftersom certificering er en vigtig metode til at sikre et højere sikkerhedsniveau, opfordrer udvalget til, at der i den nye EU-certificeringsstrategi lægges større vægt på sikkerheden inden for tingenes internet.

4.3. EU er nødt til at opbygge modstandsdygtighed over for cyberangreb og skabe et cyberforsvar med afskrækkende virkning. Kritisk infrastruktur skal beskyttes mod alle former for cyberangreb, herunder ved hjælp af EU's forsvarssystemer. Udvalget mener, at det er i EU's strategiske interesse at sikre, at Unionen bevarer og udvikler den nødvendige kapacitet til at sikre sin digitale økonomi, sit digitale samfund og sit demokrati og dermed opnå fuld digital suverænitet som den eneste måde at beskytte kritiske teknologier på og levere effektive centrale cybersikkerhedstjenester. Mindre afhængighed af tredjelande er også afgørende for EU's strategiske autonomi. EØSU mener, at sektorspecifikke EU-agenturer (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA osv.) bør inddrages i processen og vejlede om udviklingen af cybersikkerhedsordninger.

4.4. Covid-19-pandemien har fremskyndet den digitale omstilling og omdannet traditionelt arbejde til hybridarbejde og/eller fjernarbejde, hvilket har skabt nye arbejdsrelationer og forventninger samt en ny klasse af stadig flere digitale nomader. EØSU noterer sig de hurtige ændringer på arbejdsmarkedet, som har medført, at virksomheder har indført en »Zero Trust«-arkitektur via IAM- (Identity Access Management) og PAM-løsninger (Privileged Access Management). Udvalget mener, at denne form for forvaltning af virksomhedernes ressourcer resulterer i nye løsninger i forbindelse med cybertrusler, og vurderer, at den private sektor skal have støtte til at styrke sikkerhedsniveauet i virksomhedernes innovative digitale løsninger.

4.5. EØSU er temmelig skuffet over Kommissionens udtalelse om, at »der kan udarbejdes en gennemførelsesplan i samarbejde med medlemsstaterne«, og mener, at en sådan gennemførelsesplan skal være obligatorisk. Udvalget mener, at den bør udarbejdes i fællesskab med medlemsstaterne og gennemføres så hurtigt som muligt. Udvalget er bekymret over, at Kommissionen tager let på spørgsmålet og opfordrer indtrængende EU-institutionerne og medlemsstaterne til at fremme hurtige fremskridt med de bebudede initiativer.

5. **Investeringer i cyberforsvarskapacitet**

5.1. Efterhånden som den teknologiske udvikling skrider hurtigt frem, er cyberspace blevet det nyeste område for krigsførelse, efter land-, sø-, luft- og rumkrig. Udviklingen har også skabt store muligheder for, at ondsindede cyberaktører kan begå forbrydelser. Det gælder lige fra uafhængige hackere til professionelle kriminelle og endda statslige aktører.

5.2. Investeringer i FoU er afgørende, og EØSU glæder sig over de eksisterende øremærkede midler under programmet for et digitalt Europa, Den Europæiske Forsvarsfond, Horisont Europa og de nationale genopretningsprogrammer. Udvalget ser dog gerne flere tværnationale projekter, der fokuserer på samarbejde og interoperabilitet mellem cyberforsvarssystemer i alle medlemsstater, samt flere synergier mellem finansieringsinstrumenter, navnlig i forbindelse med støtten til innovative SMV'er.

5.3. Som bebudet i EU's strategi for cybersikkerhed i 2020 bemærker udvalget, at fristen for at oprette den fælles cyberenhed er i år, og udvalget afventer nyheder om afslutningen af processen og EU's beredskab over for omfattende cyberhændelser. EØSU forventer, at strategien vil forbedre EU's situationsbevidsthed og den overordnede kapacitet til at reagere og komme på fode igen.

5.4. EØSU støtter udvidelsen af mandatet for ECCC, så det kan bistå arbejdet i EU's koordinationscenter for cyberforsvar. Desuden kan dette netværk understøtte den europæiske digitale suverænitet ved at udvikle et konkurrencedygtigt europæisk industrigrundlag for centrale teknologiske kapaciteter, som til dels er baseret på arbejde, der udføres af kontraktlige offentlig-private partnerskaber (OPP). OPP'er har vist sig at være den mest effektive tilgang til forbedring af cybersikkerheden i hele det digitale økosystem, men det kan ikke kun gå en vej: offentlige institutioner skal også dele deres viden med den private sektor.

5.5. EØSU bemærker, at EU for at imødegå fremtidige forsøg på hacking fra kvantecomputere straks er nødt til at investere i banebrydende teknologier såsom post-kvantekryptografi. Udvalget finder det altafgørende, at Europa på mellemlang sigt satser på uafhængighed, og går stærkt ind for, at forsknings- og produktionsfaciliteter udvikles af EU-baserede virksomheder. EØSU mener, at det er vigtigt at øge EU's ressourcer til digital FoU og støtte operatørers og leverandørers investeringer i nye tekniske sikkerhedsfunktioner, hvilket også hænger sammen med nye tendenser såsom augmented reality og metaverse. Det er navnlig vigtigt at opbygge en europæisk distributed cloud-infrastruktur baseret på europæiske regler for områder som datalagring og -behandling ([5]).

5.6. Der bør være særlig opmærksomhed på SMV'er, som bør have adgang til finansieringsprogrammer, der øger deres beredskab over for cyberangreb, samt bistand og uddannelsesprogrammer, som hjælper dem til at forstå cyberrisici, og hvordan de kan beskytte sig mod dem. EU bør indføre en incitamentsordning, der fremmer en gradvis udvikling af SMV'ers viden på området.

5.7. Kommissionen anslår, at der mangler ca. 500 000 kvalificerede arbejdstagere inden for cybersikkerhed, og EØSU værdsætter forslaget om at oprette et akademi for cyberfærdigheder. Det står klart, at indsatsen på medlemsstatsniveau ikke er tilstrækkelig til at mindske manglen på kvalificeret arbejdskraft, så EØSU foreslår, at Kommissionen i tillæg til lanceringen af akademiet udnytter det momentum, som det europæiske år for færdigheder skaber, til at koordinere og finansiere omfattende uddannelsesprogrammer og erhvervsuddannelsesprogrammer på EU-plan, som inddrager alle medlemsstater og fokuserer på at levere en kvalificeret arbejdsstyrke til alle agenturer og organer, der er involveret i cyberforsvar, samt til private civile netværk. Der skal lægges særlig vægt på uddannelse af arbejdsstyrken, navnlig inden for naturvidenskab, teknologi, ingeniørvirksomhed og matematik (STEM).

5.8. EØSU mener desuden, at det er vigtigt at øge borgernes bevidsthed om cybersikkerhed for at mindske eksponeringen for cyberangreb, navnlig i forbindelse med grundlæggende cyberkriminalitet rettet mod befolkningen som helhed. Udvalget efterlyser læseplaner i cybersikkerhed og programmer for livslang uddannelse med fokus på forbedring af cyberfærdigheder, der vil øge kendskabet til cybersikkerhed og gøre dette tema mere attraktivt for borgerne, navnlig den yngre generation. EØSU går ind for at integrere cybersikkerhedsaspekter i alle fremtidige offentlige EU-politikker og informere den brede offentlighed om cybertrusler, herunder gennem gratis uddannelsesprogrammer for den brede befolkning, gratis informationsapps eller informationskampagner på TV i bedste sendetid. En bred kulturel udvikling på alle niveauer i samfundet i retning af en »cybersikkerhedsorienteret« tilgang skal fremmes sideløbende med disse tiltag.

5.9. EØSU mener, at det er nødvendigt at vurdere leverandørers risikoprofil og anvende relevante restriktioner over for leverandører, der anses for at udgøre en høj risiko, herunder nødvendige forbud vedrørende centrale aktiver og applikationer, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering. Der bør desuden gennemføres en certificering af pålidelige hardware- og softwareleverandører.

6. **Partnerskaber for at klare fælles udfordringer**

6.1. Beredskabsniveauet over for fremtidige cyberangreb varierer meget fra medlemsstat til medlemsstat. EØSU mener, at det umiddelbare første skridt må være at oprette en kommunikationsplatform for bedste praksis internt i EU, hvor de medlemsstater, der er kommet længst med hensyn til cybersikkerhed, kan dele deres viden med de øvrige lande og gøre det lettere for dem at anvende denne viden. Dette vil bidrage til at forbedre den gensidige tillid mellem nationale enheder. For det andet mener udvalget, at der er behov for et stærkere samarbejde mellem statslige og ikkestatslige aktører i hele EU om at forbedre cybersikkerheden for produkter og tjenester på det indre marked. EØSU foreslår også, at der oprettes en fælles EU-platform til indberetning af cyberhændelser, herunder en EU-sortliste over alle cyberkriminalitetsaktivister.

([5]) Som f.eks. det fransk-tyske initiativ Gaia-X.

6.2. EØSU er af den opfattelse, at et stærkt samarbejde med vores NATO-allierede på det militære område ikke kun skal fokusere på kapacitetsopbygning og tidlig opdagelse, men også på fælles FUI-projekter, udveksling af bedste praksis og udveksling mellem eksperter, omfattende uddannelsesprogrammer og simuleringer af cyberangreb. Hovedformålet bør være at udvide den fælles reaktionskapacitet og skabe synergier med henblik på at imødegå fremtidige hybride trusler efter de fælles erklæringer fra 2016 i Warszawa og 2018 i Bruxelles. Samarbejdet mellem EU og NATO frembyder stadig en række muligheder, som kan udnyttes, og øjeblikkelige fremskridt kan gøre en reel forskel med hensyn til at garantere vores borgeres og samfunds sikkerhed.

6.3. Udvalget mener, at drøftelser på globalt plan og med vores internationale partnere bør bane vejen for et globalt og åbent cyberspace, der beskytter menneskerettighederne, de grundlæggende frihedsrettigheder og retsstatsprincippet og fokuserer på at udvikle bindende internationale standarder i sektorer med hurtig digital udvikling. EØSU opfordrer den højtstående repræsentant til at gennemgå de eksisterende bilaterale cyberdialoger og indlede yderligere drøftelser med andre lande og relevante internationale organisationer for at fremme en verdensomspændende ramme for anvendelse af folkeretten i cyberspace, baseret på en streng betingelse om gensidighed.

6.4. Endelig mener udvalget, at EU har de bedste forudsætninger for at lede de internationale debatter om den fremtidige cybersikkerhed, navnlig drøftelserne i FN, på grund af Unionens solide fundament bestående af centrale demokratiske frihedsrettigheder. EU skal også engagere sig i bekæmpelsen af totalitære regimer, der overvåger borgernes data og krænker deres rettigheder og frihedsrettigheder, og bør tage stærkt afstand fra enhver form for socialt pointsystem over for borgerne. EØSU gør det klart, at et ægte demokrati ikke kan eksistere uden effektiv beskyttelse af personoplysninger, og mener, at ansvarlig og effektiv dataforvaltning er afgørende for at gøre hyperkonnektivitet til et aktiv.

Bruxelles, den 14. juni 2023.

Oliver RÖPKE
Formand
for Det Europæiske Økonomiske og Sociale Udvalg