Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om »forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148, og forslag til Europa-Parlamentets og Rådets direktiv om kritiske enheders modstandsdygtighed«

(COM(2020) 823 final — 2020/0359 (COD) — COM(2020) 829 final — 2020/0365 (COD))

(2021/C 286/28)

Ordfører: **Maurizio MENSI**

Anmodning om udtalelse	Europa-Parlamentet, 21.1.2021-11.2.2021
	Rådet, 26.1.2021-19.2.2021
Retsgrundlag	Artikel 114 i traktaten om Den Europæiske Unions funktionsmåde
Kompetence	Sektionen for Transport, Energi, Infrastruktur og Informationssamfundet
Vedtaget i sektionen	14.4.2021
Vedtaget på plenarforsamlingen	27.4.2021
Plenarforsamling nr.	560
Resultat af afstemningen	
(for/imod/hverken for eller imod)	243/0/5

1. **Konklusioner og anbefalinger**

1.1. EØSU værdsætter Kommissionens indsats for at øge offentlige og private enheders modstandsdygtighed over for trusler fra hændelser, cyberangreb og fysiske angreb. EØSU er enig i, at det er nødvendigt at styrke EU's industri og innovationskapacitet på en inklusiv måde efter en strategi, der bygger på fire søjler, nemlig databeskyttelse, grundlæggende rettigheder, sikkerhed og cybersikkerhed.

1.2. EØSU påpeger imidlertid, at det som følge af vigtigheden og følsomheden af målene for begge forslag ville have været bedre med en forordning end et direktiv. Det er desuden ikke klart, hvorfor Kommissionen ikke engang nævner dette som en af de overvejede muligheder.

1.3. EØSU bemærker, at nogle af bestemmelserne i de to forslag til direktiver overlapper hinanden. De hænger tæt sammen og supplerer hinanden, idet det ene forslag hovedsagelig omhandler cybersikkerhedsaspekter og det andet fysisk sikkerhed. EØSU opfordrer derfor til, at man overvejer at samle de to forslag i ét dokument med henblik på forenkling og strømlining.

1.4. EØSU bifalder forslaget om at gå bort fra den skelnen mellem operatører af væsentlige tjenester og udbydere af digitale tjenester, der fandtes i det oprindelige NIS-direktiv, men mener dog, at det vil være hensigtsmæssigt, at det defineres mere klart og præcist, hvilke enheder der falder ind under direktivets anvendelsesområde. Især bør kriterierne for differentiering mellem »væsentlige« og »vigtige« enheder og de forpligtelser, de er underlagt, fastlægges mere præcist, så man undgår, at forskellige nationale tilgange skaber hindringer for konkurrencen og den frie bevægelighed for varer og tjenesteydelser, hvilket risikerer at gå ud over virksomhederne og skade handelen.

1.5. Det system, der skitseres i forslaget, er komplekst, hvorfor EØSU finder det vigtigt, at Kommissionen omhyggeligt tydeliggør anvendelsesområdet for de to retsakter, ikke mindst når forskellige bestemmelser regulerer det samme spørgsmål eller den samme enhed.

1.6. EØSU understreger, at klare lovgivningsbestemmelser altid bør være et ufravigeligt mål ligesom mindskelse af bureaukrati og fragmentering gennem forenkling af procedurerne, sikkerhedskravene og pligten til underretning om hændelser. Også i den henseende kunne det være hensigtsmæssigt, at man — til gavn for borgerne og virksomhederne — samler de to forslag til direktiv i ét dokument, så man undgår eventuelle fortolknings- og anvendelsesproblemer.

1.7. EØSU anerkender den afgørende rolle, som ledelsesorganerne for »væsentlige« og »vigtige« enheder spiller, sådan som det understreges i forslaget til direktiv. Medlemmerne af ledelsesorganerne skal regelmæssigt følge specifikke uddannelseskurser for at opnå tilstrækkelig viden og færdigheder til at forstå og håndtere cybersikkerhedsrisici og vurdere deres indvirkning på driften. I den forbindelse bør forslaget præcisere, hvilken viden og hvilke færdigheder der som minimum er tale om, således at der på EU-niveau er en rettesnor for, hvilke uddannelseskvalifikationer der anses for passende, og man undgår, at uddannelseskursernes indhold er forskelligt fra land til land.

1.8. EØSU er enig i, at ENISA institutionelt og operationelt har stor betydning for cybersikkerheden på EU-niveau. EØSU mener derfor, at ENISA i tillæg til den rapport om cybersikkerhedssituationen i Unionen, der skal offentliggøres hvert andet år, også bør offentliggøre regelmæssige og opdaterede oplysninger online om cybersikkerhedshændelser og sektorspecifikke meddelelser, som de enheder, der er omfattet af NIS 2, kan anvende som et yderligere, nyttigt informationsredskab til at beskytte deres egne virksomheder bedre.

1.9. EØSU bifalder forslaget om at give ENISA til opgave at udvikle et europæisk sårbarhedsregister og mener, at rapportering af sårbarheder og af de vigtigste hændelser bør være obligatorisk i stedet for frivillig, så det også bliver et nyttigt instrument for de ordregivende myndigheder i forbindelse med udbudsprocedurer på europæisk plan, bl.a. for produkter og teknologier til 5G.

2. **Generelle bemærkninger**

2.1. Den 16. december 2020 blev den nye EU-strategi for cybersikkerhed præsenteret sammen med to lovgivningsforslag, nemlig revisionen af direktiv (EU) 2016/1148 ([1]) om sikkerhed i net- og informationssystemer (NIS 2) og et nyt direktiv om kritiske enheders modstandsdygtighed. Strategien, som er et nøgleelement i meddelelsen »Europas digitale fremtid i støbeskeen« ([2]), genopretningsplanen for Europa og strategien for EU's sikkerhedsunion, tager sigte på at styrke Europas kollektive modstandsdygtighed over for cybertrusler og sikre, at alle borgere og virksomheder har adgang til pålidelige og sikre digitale tjenester og værktøjer.

2.2. De eksisterende foranstaltninger på EU-niveau, der har til formål at beskytte kritiske infrastrukturer og tjenester mod cyberrisici og fysiske risici, skal ajourføres. Med den stadig mere udbredte digitalisering og indbyrdes forbundethed bliver cybersikkerhedsrisiciene ved med at udvikle sig. Derfor er det nødvendigt at revidere den gældende lovgivning i overensstemmelse med EU's sikkerhedsstrategi, overvinde splittelsen mellem online og offline og nedbryde silotilgangen.

2.3. De to direktivforslag berører en lang række sektorer og omhandler nuværende og fremtidige risici, både online og offline, fra cyberangreb og -kriminalitet til naturkatastrofer og andre hændelser. Dette sker bl.a. på baggrund af erfaringerne fra den aktuelle pandemi, som har blotlagt, hvordan samfund og økonomier, der i stigende grad er afhængige af digitale løsninger, er sårbare og eksponeret for de stadigt flere og hastigt forandrende cybertrusler. Dette gælder ikke mindst grupper i risiko for social udstødelse, f.eks. personer med handicap. EU har derfor foreslået tiltag for at sikre et globalt og åbent cyberspace også fremover, som bygger på solide sikkerhedsgarantier, teknologisk suverænitet og lederskab. Målet er at udvikle operationel kapacitet til at forebygge, modvirke og reagere på eventuelle trusler gennem et mere udbygget samarbejde med respekt for de beføjelser vedrørende den nationale sikkerhed, som henhører under medlemsstaterne.

3. **Forslaget til revision af direktivet om net- og informationssikkerhed**

3.1. Direktiv (EU) 2016/1148 (NIS-direktivet), som var EU's første »horisontale« lovgivningsinstrument vedrørende cybersikkerhed, havde til formål at forbedre Unionens net- og informationssystemers modstandsdygtighed over for cyberrisici. Selv om NIS-direktivet har givet gode resultater, har det også vist sine begrænsninger. Digitaliseringen af samfundet, der er blevet forstærket af covid-19-krisen, har udvidet trusselsbilledet og fremhævet sårbarhederne over for store og uforudsete risici i vores stadig mere indbyrdes afhængige samfund. Der er opstået nye udfordringer, som kræver

([1]) EUT L 194 af 19.7.2016 s. 1.
([2]) COM(2020) 67 final.

passende og innovative løsninger. Resultaterne af den brede høring af de interesserede parter har afdækket det utilstrækkelige cybersikkerhedsniveau i europæiske virksomheder, medlemsstaternes inkonsekvente anvendelse af reglerne på forskellige områder og den mangelfulde forståelse af de vigtigste trusler og udfordringer.

3.2. NIS 2-forslaget hænger tæt sammen med to andre initiativer, nemlig forslaget til forordning om den digitale finansielle sektor (digital operationel modstandsdygtighed, DORA) og forslaget til direktiv om kritiske enheder, som udvider anvendelsesområdet for direktiv 2008/114 ([3]), der omhandler energi og transport, til at omfatte nye områder, som f.eks. sundhedssektoren og de enheder, der forsker i og udvikler lægemidler. Med forslaget til direktiv om kritiske enheder, hvis anvendelsesområde er det samme som NIS 2 om væsentlige enheder (bilag 1 i NIS 2), flyttes fokus fra beskyttelse af fysiske aktiver til modstandsdygtigheden hos de enheder, der forvalter dem, og man går fra at identificere kritisk europæisk infrastruktur med en grænseoverskridende dimension til at identificere kritisk national infrastruktur. NIS 2 hænger også sammen med og supplerer andre gældende lovgivningsinstrumenter såsom den europæiske kodeks for elektronisk kommunikation, den generelle forordning om databeskyttelse og eIDAS-forordningen om elektronisk identifikation og tillidstjenester.

3.3. Forslaget til NIS 2-direktiv har i overensstemmelse med programmet for målrettet og effektiv regulering (REFIT) til formål at mindske den reguleringsmæssige byrde for de kompetente myndigheder og overholdelsesomkostningerne for offentlige og private enheder samt at modernisere referencelovgivningen. Desuden skærpes de sikkerhedskrav, der pålægges virksomhederne, spørgsmålet om forsyningskædernes sikkerhed behandles, rapporteringsforpligtelserne strømlines, og der indføres strengere tilsynsforanstaltninger for de nationale myndigheder. Et andet formål er at harmonisere medlemsstaternes sanktionsordninger.

3.4. NIS 2 bidrager ligeledes til at øge udvekslingen af oplysninger og samarbejdet om cyberkrisestyring på nationalt og europæisk plan. Der skelnes ikke længere mellem operatører af væsentlige tjenester og udbydere af digitale tjenester, sådan som det var tilfældet i NIS-direktivet. Direktivets anvendelsesområde omfatter mellemstore virksomheder i sektorer, der fastlægges på baggrund af deres kritiske betydning for økonomien og samfundet. Disse offentlige og private enheder inddeles i »væsentlige« og »vigtige« enheder, og de er underlagt forskellige tilsynsordninger. Medlemsstaterne har dog mulighed for også at tage mindre enheder i betragtning, hvis de har en høj risikoprofil.

3.5. Der er planer om et nyt netværk af EU-sikkerhedsoperationscentre, som skal styres af kunstig intelligens (AI) og udgøre et reelt »cybersikkerhedsskjold«, der kan opdage tegn på cyberangreb i så god tid, at det er muligt at gribe ind, før skaden sker. Vigtigheden af kunstig intelligens for cybersikkerheden fremhæves desuden i den rapport om kunstig intelligens, som USA's nationale sikkerhedsråd (NSCAI) offentliggjorde den 1. marts 2021. Som følge heraf vil medlemsstaterne og operatører af kritisk infrastruktur kunne få direkte adgang til information om truslerne inden for rammerne af et europæisk sikkerhedsnetværk for trusselsefterretninger.

3.6. Kommissionen tager ligeledes fat på spørgsmålet om forsyningskædernes sikkerhed og forbindelserne til leverandørerne. Medlemsstaterne kan i samarbejde med Kommissionen og ENISA foretage koordinerede risikovurderinger af kritiske forsyningskæder, som det allerede er sket for 5G-net i henhold til henstillingen af 26. marts 2019 ([4]).

3.7. Forslaget styrker og strømliner virksomhedernes sikkerheds- og rapporteringsforpligtelser ved hjælp af en fælles risikostyringstilgang med en minimumsliste over de grundlæggende sikkerhedsforanstaltninger, der skal træffes. Der fastlægges mere præcise bestemmelser om proceduren for underretning om hændelser, rapporternes indhold og frister. I den forbindelse skitseres der i forslaget en rapporteringsproces i to faser: Virksomhederne har 24 timer til at indsende en første sammenfattende rapport, som skal efterfølges af en endelig og detaljeret rapport, inden der er gået en måned.

([3]) EUT L 345 af 23.12.2008 s. 75.
([4]) EUT L 88 af 29.3.2019 s. 42.

3.8. Der lægges op til, at medlemsstaterne udpeger de nationale myndigheder, der skal være ansvarlige for krisestyringen, med specifikke planer og et nyt netværk for operationelt samarbejde, »det europæiske netværk af forbindelsesorganisationer for cyberkriser« (»EU-CyCLONe«). Samarbejdsgruppen skal have en mere fremtrædende rolle i forbindelse med strategiske beslutninger, og der oprettes et register — som forvaltes af ENISA — over de sårbarheder, der konstateres i EU. Desuden øges udvekslingen af oplysninger og samarbejdet mellem medlemsstaternes myndigheder, herunder det operationelle samarbejde om cyberkrisestyring.

3.9. Der indføres strengere tilsynsforanstaltninger for de nationale myndigheder og strengere håndhævelseskrav, og der sigtes mod at harmonisere alle medlemsstaternes sanktionsordninger.

3.10. I den henseende fastlægges der i direktivet en liste over administrative sanktioner for brud på forpligtelserne med hensyn til risikostyring og rapportering vedrørende cybersikkerhed. Der fastlægges bestemmelser om ansvaret hos fysiske personer, som har repræsentative eller ledende stillinger i de virksomheder, der falder ind under direktivets anvendelsesområde. Med forslaget forbedres den måde, hvorpå EU forebygger, håndterer og reagerer på omfattende cybersikkerhedshændelser og -kriser med en klar ansvarsfordeling, hensigtsmæssig planlægning og et større samarbejde på EU-niveau.

3.11. Medlemsstaterne bliver i stand til i fællesskab at overvåge EU-bestemmelsernes gennemførelse, og de hjælper hinanden i tilfælde af grænseoverskridende problemer. De skal etablere en mere struktureret dialog med den private sektor, koordinere offentliggørelsen af konstaterede sårbarheder i software og hardware, som markedsføres på det indre marked, og koordinere vurderingen af de sikkerhedsrisici og trusler, der er forbundet med de nye teknologier, sådan som det var tilfældet med 5G.

4. **Forslaget til direktiv om kritiske enheders modstandsdygtighed**

4.1. I 2006 indførte EU det europæiske program for beskyttelse af kritisk infrastruktur (EPCIP), og i 2008 vedtog EU direktivet om europæisk kritisk infrastruktur, som gælder for energi- og transportsektoren. Både strategien for EU's sikkerhedsunion 2020-2025 ([5]), som Kommissionen har vedtaget, og den nyligt vedtagne dagsorden om terrorbekæmpelse understreger vigtigheden af at sikre kritisk infrastrukturs modstandsdygtighed over for fysiske og digitale risici. Både den vurdering af gennemførelsen af direktivet om europæisk kritisk infrastruktur, der blev udført i 2019, og konsekvensanalysen af det nu foreliggende forslag viser imidlertid, at de gældende europæiske og nationale foranstaltninger ikke i tilstrækkelig grad sikrer, at operatørerne er i stand til at håndtere de aktuelle risici. Derfor opfordrer Rådet og Europa-Parlamentet Kommissionen til at genoverveje den nuværende tilgang til beskyttelsen af kritisk infrastruktur.

4.2. I strategien for EU's sikkerhedsunion, som Kommissionen vedtog den 24. juli 2020, anerkendte man den stadig større indbyrdes forbundethed og afhængighed mellem de fysiske og digitale infrastrukturer, og behovet for mere sammenhæng og ensartethed mellem direktivet om europæisk kritisk infrastruktur og NIS-direktivet blev understreget. Derfor udvides med forslaget til direktiv om kritiske enheders modstandsdygtighed — hvis objektive referenceområde er det samme som i NIS 2 om væsentlige enheder — det oprindelige anvendelsesområde for direktiv 2008/114/EF, der var begrænset til energi og transport, til at omfatte følgende områder: bankvæsen, finansmarkedsinfrastruktur, sundhed, drikkevand, spildevand, digital infrastruktur, offentlig forvaltning og rummet. Forslaget indeholder tillige bestemmelser om en klar ansvarsfordeling, hensigtsmæssig planlægning og større samarbejde. Der er med henblik derpå behov for at skabe en referenceramme for alle risici og støtte medlemsstaterne i deres bestræbelser på at sikre, at kritiske enheder er i stand til at forebygge, modstå og absorbere konsekvenserne af hændelser, uanset om risiciene stammer fra naturkatastrofer, ulykker, terrorisme, interne trusler eller folkesundhedskriser som den nuværende.

4.3. Alle medlemsstater skal vedtage en national strategi for at sikre kritiske enheders modstandsdygtighed, foretage regelmæssige risikovurderinger og på dette grundlag identificere de kritiske enheder. De kritiske enheder skal til gengæld foretage risikovurderinger, træffe passende tekniske og organisatoriske foranstaltninger for at øge modstandsdygtigheden og underrette de nationale myndigheder om hændelser. Enheder, som leverer tjenester til mindst en tredjedel af medlemsstaterne eller i mindst en tredjedel af dem, er underlagt et særligt tilsyn, som omfatter særlige rådgivende missioner rettet mod disse og tilrettelagt af Kommissionen.

4.4. Forslaget til direktiv om kritiske enheders modstandsdygtighed omfatter forskellige former for støtte til medlemsstaterne og de kritiske enheder, en oversigt over risiciene på EU-plan, bedste praksis og metoder samt uddannelsesaktiviteter og øvelser for at afprøve kritiske enheders modstandsdygtighed. Systemet for grænseoverskridende samarbejde skal desuden omfatte en ad hoc-ekspertgruppe, gruppen for kritiske enheders modstandsdygtighed, et forum for det strategiske samarbejde og udveksling af oplysninger mellem medlemsstaterne.

([5]) COM(2020) 605 final.

5. **Ændringsforslag til det omhandlede lovgivningsforslag**

5.1. EØSU værdsætter Kommissionens indsats for at øge offentlige og private enheders modstandsdygtighed over for trusler fra cyberangreb og fysiske angreb. Især i lyset af den hurtige digitalisering, som covid-19-krisen har sat i gang, har dette fået en særlig betydning og relevans. EØSU er ligeledes enig i, at det, som det anføres i meddelelsen »Europas digitale fremtid i støbeskeen«, er nødvendigt, at Europa høster fordelene ved den digitale tidsalder og styrker sin industri, herunder især de små og mellemstore virksomheder, og innovationskapacitet på en inklusiv måde efter en strategi, der bygger på fire søjler, nemlig databeskyttelse, grundlæggende rettigheder, sikkerhed og cybersikkerhed, som er vigtige forudsætninger for et databaseret samfund.

5.2. EØSU bemærker imidlertid, at det ikke fremgår, hvorfor Kommissionen ikke foreslår vedtagelse af en forordning i stedet for et direktiv, og heller ikke hvorfor det slet ikke er blevet overvejet. Dette skal ses i lyset af resultaterne af den konsekvensanalyse og den høring, der gik forud for NIS 2-forslaget, og det ofte understregede mål om at undgå en fragmentering af de vedtagne regler på nationalt plan, sådan som der også gives udtryk for i meddelelsen af 4. oktober 2017 om NIS-direktivets gennemførelse ([6]).

5.3. EØSU bemærker, at nogle af bestemmelserne i de to forslag til direktiver overlapper hinanden. De hænger tæt sammen og supplerer hinanden, idet det ene forslag hovedsagelig omhandler cybersikkerhedsaspekter og det andet fysisk sikkerhed. Udvalget gør endvidere opmærksom på, at de kritiske enheder i direktivet om kritiske enheders modstandsdygtighed findes i samme sektorer som og er sammenfaldende med de »væsentlige« enheder i NIS 2 ([7]). Dertil kommer, at alle de kritiske enheder, der er omfattet af direktivet om kritiske enheders modstandsdygtighed, er underlagt de forpligtelser vedrørende cybersikkerhed, der er fastlagt i NIS 2. De to forslag indeholder desuden en række brobyggende bestemmelser, som binder dem sammen, nemlig bestemmelser om et styrket samarbejde mellem myndighederne, udveksling af oplysninger om tilsynsaktiviteterne, underretning af NIS 2-myndighederne om identifikation af kritiske enheder i henhold til direktivet om kritiske enheders modstandsdygtighed og regelmæssige møder i de respektive samarbejdsgrupper mindst én gang om året. De to forslag har også samme retsgrundlag, nemlig artikel 114 i TEUF, der handler om indbyrdes tilnærmelse af medlemsstaternes love af hensyn til det indre markeds funktion, sådan som det f.eks. blev fortolket af EU-Domstolen i dommen i sag C-58/08, Vodafone m.fl. EØSU opfordrer derfor til, at man overvejer at samle de to forslag i ét dokument med henblik på forenkling og strømlining.

5.4. EØSU bifalder, at man går bort fra den skelnen mellem operatører af væsentlige tjenester og udbydere af digitale tjenester, der fandtes i det oprindelige NIS direktiv, men mener dog, at det vil være hensigtsmæssigt, at det defineres mere klart og præcist, hvilke enheder der falder ind under direktivets anvendelsesområde. Ud over de henvisninger, der er medtaget i bilag I og II, indeholder NIS 2 nemlig en række uensartede kriterier, som indebærer vanskelige kvalitative og kvantitative vurderinger, som kan blive gennemført på forskellig vis i medlemsstaterne. Dette skaber risiko for en gentagelse af den fragmenterede situation, som man ønskede at undgå med den pågældende lovgivning. Det er således vigtigt at undgå, at forskellige nationale tilgange resulterer i hindringer for konkurrencen og den frie bevægelighed, hvilket risikerer at gå ud over virksomhederne og skade handelen.

5.5. I henhold til NIS 2 er kritiske operatører i sektorer, der betragtes som »væsentlige« i det pågældende forslag, også underlagt generelle forpligtelser til at øge modstandsdygtigheden, idet der lægges særlig vægt på ikkecyberrelaterede risici i henhold til direktivet om kritiske enheders modstandsdygtighed. Det fremgår dog udtrykkeligt af direktivet, at det ikke gælder for de områder, som NIS 2 vedrører. Det fastlægges således i direktivet om kritiske enheders modstandsdygtighed, at cybersikkerhed behandles tilstrækkeligt i NIS 2-direktivet, hvorfor de områder, der reguleres af NIS 2, bør være udelukket fra anvendelsesområdet for direktivet om kritiske enheders modstandsdygtighed, uden at dette berører den særlige ordning for enheder i den digitale infrastruktursektor. I henhold til direktivet om kritiske enheders modstandsdygtighed gælder det desuden, at enheder i den digitale infrastruktursektor i det væsentlige er baseret på net- og informationssystemer og falder ind under anvendelsesområdet for NIS 2-direktivet, som også omhandler den fysiske sikkerhed for sådanne systemer som en del af deres forpligtelser med hensyn til risikostyring og rapportering vedrørende cybersikkerhed. Samtidig fremgår det af direktivet om kritiske enheders modstandsdygtighed, at det ikke er udelukket, at der kan gælde særlige bestemmelser for dem.

5.6. Inden for disse komplekse rammer anser EØSU det således for absolut nødvendigt, at Kommissionen omhyggeligt præciserer anvendelsesområdet for de to retsakter, ikke mindst når bestemmelserne regulerer det samme spørgsmål eller den samme enhed.

5.7. Klare lovgivningsbestemmelser, især i omfattende og detaljerede retsakter som de omhandlede, bør altid være et ufravigeligt mål på ethvert niveau ligesom mindskelse af bureaukrati og fragmentering gennem forenkling af procedurerne, sikkerhedskravene og pligten til underretning om hændelser. Det er ligeledes vigtigt at undgå, at en flerdobling af organer

([6]) COM(2017) 476 final.
([7]) Bilag 1: EUT L 194 af 19.7.2016, s. 1.

med særlige opgaver vanskeliggør en klar identifikation af kompetencer, da dette vil forpurre opnåelsen af de ønskede mål. Også derfor kunne det være hensigtsmæssigt, at man — til gavn for borgerne og virksomhederne — samler de to direktivforslag i ét dokument, så man undgår eventuelle fortolknings- og anvendelsesproblemer.

5.8. I flere tilfælde henvises der i NIS 2 til bestemmelser i andre retsakter, f.eks. direktiv (EU) 2018/1972 ([8]) om oprettelse af en europæisk kodeks for elektronisk kommunikation, hvis anvendelse er underlagt specialitetskriteriet. Nogle af bestemmelserne i nævnte direktiv er udtrykkeligt blevet ophævet (artikel 40 og 41), mens andre skal anvendes i henhold til førnævnte princip, uden at der gives nogen præcisering i den forbindelse. På dette punkt ønsker EØSU, at enhver usikkerhed fjernes, så der ikke opstår fortolkningsproblemer. Hvad angår sanktionsordningen er EØSU i øvrigt enig i Kommissionens mål om at harmonisere reglerne i tilfælde af manglende overholdelse i forbindelse med risikostyringen som led i bedre informationsdeling og samarbejde på EU-niveau.

5.9. EØSU anerkender den afgørende rolle, som ledelsesorganerne for »væsentlige« og »vigtige« enheder spiller, sådan som det understreges i forslaget til direktiv, da det er dem, der skal godkende risikostyringsforanstaltningerne, føre tilsyn med deres gennemførelse og gribe ind ved eventuel manglende overholdelse. Med henblik derpå skal medlemmerne af disse organer regelmæssigt følge specifikke uddannelseskurser for at opnå tilstrækkelig viden og færdigheder til at forstå og håndtere de forskellige cybersikkerhedsrisici og vurdere deres indvirkning på driften. Det bør dog i forslaget præciseres, hvilken viden og hvilke færdigheder der er tale om, således at der på EU-niveau er en rettesnor for, hvilke uddannelseskvalifikationer der anses for passende til at opfylde forpligtelserne i forslaget, og man undgår, at kravene til og indholdet af uddannelseskurserne er forskelligt fra land til land.

5.10. EØSU er enig i, at ENISA institutionelt og operationelt har stor betydning for cybersikkerheden på EU-niveau. EØSU mener derfor, at ENISA i tillæg til den rapport om cybersikkerhedssituationen i Unionen, der skal offentliggøres, også bør offentliggøre opdaterede oplysninger online om cybersikkerhedshændelser og sektorspecifikke meddelelser, som de interessenter, der er omfattet af NIS 2, kan anvende som et nyttigt informationsredskab til at beskytte deres egne virksomheder bedre.

5.11. EØSU er enig i, at adgang til korrekte og rettidige oplysninger om sårbarheder, der påvirker IKT-produkter og -tjenester, bidrager til en forbedret risikostyring i forbindelse med cybersikkerhed. I denne henseende udgør kilder til offentligt tilgængelige oplysninger om sårbarheder et vigtigt redskab for de nationale kompetente myndigheder, CSIRT'er, virksomheder og brugere. EØSU bifalder derfor forslaget om at give ENISA til opgave at udvikle et europæisk sårbarhedsregister, som væsentlige og vigtige enheder samt deres leverandører kan give oplysninger til, så det bliver muligt for brugerne at træffe passende afbødende foranstaltninger. EØSU er desuden af den opfattelse, at en sådan rapportering af sårbarheder og af de vigtigste hændelser bør være obligatorisk i stedet for frivillig, så registret også bliver et nyttigt instrument for de ordregivende myndigheder i forbindelse med udbudsprocedurer på EU-niveau, bl.a. for produkter og teknologier til 5G. Dette register ville i så fald indeholde nyttige oplysninger til vurderingen af buddenes kvalitet og de europæiske og ikkeeuropæiske kontrahenters pålidelighed med hensyn til sikkerheden af de varer og tjenesteydelser, der er genstand for udbuddet, i tråd med henstillingen af 26. marts 2019 om cybersikkerhed i 5G-net. Det bør også sikres, at oplysningerne i registret gøres tilgængelige på en måde, der forhindrer enhver form for forskelsbehandling.

Bruxelles, den 27. april 2021.

Christa SCHWENG
Formand
for Det Europæiske Økonomiske og Sociale Udvalg

([8]) EUT L 321 af 17.12.2018, s. 36.