Yttrande av Europeiska ekonomiska och sociala kommittén om Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, och Förslag till Europaparlamentets och rådets direktiv om kritiska entiteters motståndskraft

[COM(2020) 823 final – 2020/0359(COD); COM(2020) 829 final – 2020/0365(COD)]

(2021/C 286/28)

Föredragande: **Maurizio MENSI**

Remiss	Europaparlamentet, 21.1.2021–11.2.2021
	Rådet, 26.1.2021–19.2.2021
Rättslig grund	Artikel 114 i fördraget om Europeiska unionens funktionssätt
Ansvarig sektion	Transporter, energi, infrastruktur och informationssamhället
Antagande av sektionen	14.4.2021
Antagande vid plenarsessionen	27.4.2021
Plenarsession nr	560
Resultat av omröstningen	
(för/emot/nedlagda röster)	243/0/5

1. **Slutsatser och rekommendationer**

1.1 EESK välkomnar kommissionens insatser för att göra offentliga och privata entiteter mer motståndskraftiga mot hot till följd av incidenter, cyberattacker och fysiska attacker, och håller med om att man måste stärka industrin och innovationskapaciteten i EU på ett inkluderande sätt, enligt en strategi som baseras på fyra pelare: dataskydd, grundläggande rättigheter, säkerhet och cybersäkerhet.

1.2 EESK noterar dock att relevansen och känsligheten hos de mål som eftersträvas med de båda förslagen gör att en förordning skulle ha varit att föredra framför ett direktiv. Det framgår för övrigt inte varför kommissionen inte har beaktat denna möjlighet ens bland de olika alternativ som övervägts.

1.3 EESK noterar att vissa bestämmelser i de båda förslagen till direktiv överlappar varandra eftersom de har ett nära samband och kompletterar varandra: i det ena fokuserar man främst på cybersäkerhet och i det andra på fysisk säkerhet. Kommittén uppmanar därför till att överväga möjligheten att slå samman de båda förslagen i en enda text i förenklings- och rationaliseringssyfte.

1.4 EESK ställer sig bakom förslaget om att avskaffa åtskillnaden mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster i det ursprungliga NIS-direktivet, men vad gäller dess tillämpningsområde efterlyser kommittén närmare och tydligare riktlinjer för fastställandet av de entiteter som omfattas av direktivet. I synnerhet bör kriterierna för åtskillnad mellan ”väsentliga” och ”viktiga” entiteter samt de krav som de ska uppfylla definieras mer exakt för att undvika att olika tillvägagångssätt på nationell nivå leder till hinder för konkurrensen och den fria rörligheten för varor och tjänster, vilket riskerar att påverka företagen och handeln negativt.

1.5 Mot bakgrund av komplexiteten i det system som beskrivs i de båda förslagen anser EESK att det är viktigt att kommissionen klargör det exakta tillämpningsområdet för dessa två regeluppsättningar, särskilt i de fall där olika bestämmelser reglerar samma fråga eller entitet.

1.6 EESK påpekar att tydlighet i varje regleringsbestämmelse utgör ett grundläggande mål, tillsammans med minskad byråkrati och fragmentering genom förenklade förfaranden, säkerhetskrav och incidentrapporteringsskyldigheter. Även i detta syfte skulle det kunna vara lämpligt, till fördel för både medborgare och företag, att slå samman de båda förslagen till direktiv i en enda text och därmed undvika en ibland komplicerad tolkning och tillämpning.

1.7 EESK erkänner den grundläggande roll, som framhålls i förslaget till direktiv, som spelas av de ”väsentliga” och ”viktiga” entiteternas ledningsorgan, vars medlemmar regelbundet måste genomgå särskild utbildning för att förvärva tillräcklig kunskap och kompetens för att kunna förstå och hantera de olika cybersäkerhetsriskerna och bedöma deras effekter. I detta avseende anser kommittén att man i förslaget bör ange minimiinnehållet i denna kunskap och kompetens för att ge vägledning på europeisk nivå om vilken utbildningskompetens som anses lämplig och för att undvika att innehållet i de olika utbildningarna skiljer sig åt mellan länderna.

1.8 EESK instämmer i den viktiga roll som Enisa spelar i den övergripande institutionella och operativa ramen för cybersäkerhet på europeisk nivå. I detta avseende anser kommittén att detta organ, utöver rapporten om cybersäkerhetsläget i unionen vartannat år, online bör offentliggöra regelbunden och aktuell information om cybersäkerhetsincidenter, vid sidan av sektorsspecifika tillkännagivanden, för att tillhandahålla ytterligare ett användbart informationsverktyg som gör att aktörer som berörs av NIS 2-direktivet bättre kan skydda sina företag.

1.9 EESK ställer sig bakom förslaget om att ge Enisa i uppgift att inrätta ett europeiskt sårbarhetsregister, och anser att rapporteringen av sårbarheterna och de allvarligaste incidenterna bör göras obligatorisk i stället för frivillig, så att det blir ett användbart instrument även för de upphandlande enheterna inom ramen för upphandlingsförfaranden på europeisk nivå, inklusive dem för 5G-produkter och 5G-teknik.

2. **Allmänna kommentarer**

2.1 Den 16 december 2020 presenterades EU:s nya strategi för cybersäkerhet tillsammans med två lagförslag: översynen av direktiv (EU) 2016/1148 ([1]) om säkerhet i nätverks- och informationssystem (NIS 2) och ett nytt direktiv om kritiska entiteters motståndskraft. Strategin, som är ett av huvudinslagen i meddelandet ”Att forma EU:s digitala framtid” ([2]), återhämtningsplanen för Europa och strategin för EU:s säkerhetsunion, syftar till att förstärka Europas kollektiva motståndskraft mot cyberhot och garantera att alla medborgare och företag kan ta del av tillförlitliga och säkra digitala tjänster och verktyg.

2.2 De befintliga åtgärderna på EU-nivå för att skydda kritiska tjänster och kritisk infrastruktur från cyberrisker och fysiska risker måste uppdateras. Risker som är kopplade till cybersäkerhet fortsätter att utvecklas i takt med att digitaliseringen och sammankopplingen ökar. Det gällande regelverket måste därför ses över i enlighet med EU:s säkerhetsstrategi för att överge dikotomin mellan online och offline och undvika en metod som baseras på strikt uppdelning.

2.3 De båda förslagen till direktiv avser ett brett spektrum av sektorer och tar upp såväl befintliga som framtida risker, både online och offline, kopplade till cyberattacker och brottsliga attacker, naturkatastrofer och andra incidenter, bland annat med utgångspunkt i lärdomarna av den rådande pandemin, som har visat hur samhällen och ekonomier som är alltmer beroende av digitala lösningar är sårbara och utsatta för växande cyberhot som snabbt förändras, särskilt för grupper som riskerar social utestängning, såsom personer med funktionsnedsättning. Detta har fått EU att föreslå åtgärder för att trygga en global och öppen cyberrymd som bygger på robusta säkerhetsgarantier, teknisk suveränitet och ledarskap genom att utveckla operativ kapacitet för att förebygga, avskräcka och reagera på möjliga hot genom ett mer omfattande samarbete, med respekt för medlemsstaternas befogenheter beträffande nationell säkerhet.

3. **Förslaget till översyn av direktivet om säkerhet i nätverks- och informationssystem**

3.1 NIS-direktivet (EU) 2016/1148, EU:s första ”övergripande” rättsliga instrument för cybersäkerhet, syftade till att öka motståndskraften mot cyberrisker i EU:s nätverks- och informationssystem. Trots de goda resultat som uppnåtts har NIS-direktivet visat sig ha vissa begränsningar, samtidigt som den digitala omvandlingen av samhället, som har påskyndats av covid-19-krisen, har medfört en större hotbild och en ökad sårbarhet i våra samhällen, som blir alltmer beroende av

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

varandra inför stora och oförutsedda risker. Nya utmaningar har uppstått, som kräver lämpliga och innovativa svar. Resultaten av det omfattande samrådet med berörda parter har visat på en otillräcklig cybersäkerhetsnivå hos europeiska företag, en inkonsekvent tillämpning av reglerna på olika områden från medlemsstaternas sida samt bristande kunskap om de främsta hoten och utmaningarna.

3.2 Förslaget till NIS 2-direktiv är nära kopplat till två andra initiativ: förslaget till förordning om digital operativ motståndskraft för finanssektorn (”Digital Operational Resilience Act”, DORA) och förslaget till direktiv om kritiska entiteters motståndskraft, som innebär att tillämpningsområdet för direktiv 2008/114/EG ([3]) om energi och transport utvidgas till att omfatta andra sektorer, med fokus på t.ex. hälso- och sjukvårdssektorn och aktörer som är verksamma inom forskning och utveckling av läkemedel. Direktivet om kritiska entiteters motståndskraft, vars tillämpningsområde omfattar samma sektorer som NIS 2-direktivet vad gäller väsentliga entiteter (bilaga I till NIS 2-direktivet), flyttar fokus från skyddet av fysiska tillgångar till motståndskraften hos de entiteter som förvaltar dem och övergår från att identifiera europeisk kritisk infrastruktur med en gränsöverskridande dimension till att identifiera kritisk infrastruktur på nationell nivå. NIS 2-direktivet överensstämmer med och kompletterar även andra gällande rättsliga instrument, såsom den europeiska kodexen för elektronisk kommunikation, den allmänna dataskyddsförordningen och eIDA-förordningen om elektronisk identifiering och betrodda tjänster.

3.3 I enlighet med programmet om lagstiftningens ändamålsenlighet och resultat (Refit) syftar förslaget till NIS 2-direktiv till att minska regelbördorna för de behöriga myndigheterna och efterlevnadskostnaderna för offentliga och privata aktörer och moderniserar den rättsliga referensramen. Dessutom skärper det säkerhetskraven för företag, tar upp frågan om säkerhet i leveranskedjorna, rationaliserar rapporteringsskyldigheterna, inför strängare tillsynsåtgärder för de nationella myndigheterna och syftar till att harmonisera sanktionssystemen i medlemsstaterna.

3.4 NIS 2-direktivet bidrar även till ökat informationsutbyte och samarbete vid hantering av cyberkriser på nationell och europeisk nivå. Åtskillnaden mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster i NIS-direktivet avskaffas. Dess tillämpningsområde omfattar medelstora och stora företag i de sektorer som har fastställts vara kritiska för ekonomin och samhället. Dessa offentliga eller privata entiteter delas in i två kategorier – ”väsentliga” och ”viktiga” – som omfattas av olika tillsynssystem. Medlemsstaterna har dock möjlighet att även beakta mindre entiteter med hög riskprofil.

3.5 Man planerar ett nytt nätverk av säkerhetscentrum på EU-nivå som utnyttjar artificiell intelligens och som kommer att utgöra en verklig ”cybersäkerhetssköld” som kan identifiera tecken på cyberattacker i tillräckligt god tid för att åtgärder ska kunna vidtas innan någon skada uppstår. Den artificiella intelligensens betydelse för cybersäkerheten betonas också i den rapport om artificiell intelligens som Förenta staternas kommission för nationell säkerhet (NSCAI) lade fram den 1 mars 2021. Medlemsstaterna och operatörerna av kritisk infrastruktur kommer därigenom att kunna få direkt tillgång till information om hot inom ramen för ett europeiskt säkerhetsnätverk i form av ”underrättelser om hot”.

3.6 Kommissionen tar även upp problemet med säkerhet i leveranskedjorna och förbindelserna med leverantörerna: Medlemsstaterna kan, i samarbete med kommissionen och Enisa, genomföra samordnade riskbedömningar av kritiska leveranskedjor, på grundval av den framgångsrika metoden för 5G-nätverk enligt rekommendationen av den 26 mars 2019 ([4]).

3.7 Genom förslaget stärks och rationaliseras säkerhets- och rapporteringsskyldigheterna för företag och inrättas en gemensam metod för riskhantering, med en minimiförteckning över grundläggande säkerhetsåtgärder som ska tillämpas. Mer detaljerade bestämmelser fastställs om processen för att rapportera incidenter, om rapporternas innehåll och om tidsfristerna. I detta avseende beskrivs i förslaget en tvåstegsprocess: Företagen har 24 timmar på sig att lämna in en första sammanfattande rapport, som ska följas av en detaljerad slutrapport inom en månad.

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

3.8 Medlemsstaterna ska utse nationella myndigheter med ansvar för krishantering, med särskilda planer och ett nytt nätverk för operativt samarbete: Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe). Samarbetsgruppens roll förstärks när det gäller att utarbeta strategiska beslut, och man kommer att inrätta ett register över sårbarheter som identifieras i EU, vilket ska förvaltas av Enisa. Informationsutbytet och samarbetet mellan medlemsstaternas myndigheter kommer också att öka, inklusive det operativa samarbetet vid hantering av cyberkriser.

3.9 Det införs strängare tillsynsåtgärder för de nationella myndigheterna och striktare tillämpningskrav, och man strävar efter att harmonisera sanktionssystemen i samtliga medlemsstater.

3.10 I detta avseende fastställs i förslaget till direktiv en förteckning över administrativa sanktioner vid brott mot riskhanterings- och rapporteringsskyldigheterna för cybersäkerhet. Det fastställs bestämmelser om ansvaret för fysiska personer som har representativa eller ledande poster i företag som omfattas av direktivet. I detta avseende förbättrar förslaget det sätt på vilket EU förebygger, hanterar och åtgärdar omfattande incidenter och kriser på cybersäkerhetsområdet, genom att fastställa tydliga ansvarsområden, en ordentlig planering och ökat samarbete på EU-nivå.

3.11 Medlemsstaterna kommer att gemensamt kunna övervaka tillämpningen av EU:s regler och hjälpa varandra vid gränsöverskridande problem. De kommer att kunna inrätta en mer strukturerad dialog med den privata sektorn, samordna informationen om sårbarheter i programvara och maskinvara som sålts på den inre marknaden samt på ett samordnat sätt bedöma säkerhetsrisker och hot kopplade till ny teknik, såsom var fallet med 5G.

4. **Förslaget till direktiv om kritiska entiteters motståndskraft**

4.1 År 2006 inrättade EU det europeiska programmet för skydd av kritisk infrastruktur (EPCIP), och 2008 antogs direktivet om europeisk kritisk infrastruktur, som gäller energi- och transportsektorerna. I både kommissionens strategi för EU:s säkerhetsunion 2020–2025 ([5]) och den nyligen antagna agendan för terrorismbekämpning betonas vikten av att säkerställa den kritiska infrastrukturens motståndskraft mot fysiska och digitala risker. Både 2019 års utvärdering av tillämpningen av direktivet om europeisk kritisk infrastruktur och resultaten av konsekvensbedömningen av det aktuella förslaget har dock visat att de gällande europeiska och nationella åtgärderna inte i tillräcklig utsträckning garanterar att operatörerna kan hantera de aktuella riskerna. Därför har rådet och parlamentet uppmanat kommissionen att se över den rådande metoden för att skydda kritisk infrastruktur.

4.2 I strategin för EU:s säkerhetsunion, som kommissionen antog den 24 juli 2020, erkändes den ökande sammankopplingen och det ökande ömsesidiga beroendet mellan fysisk och digital infrastruktur, och framhölls behovet av mer samstämmighet och enhetlighet mellan direktivet om europeisk kritisk infrastruktur och NIS-direktivet. I detta avseende utvidgar förslaget till direktiv om kritiska entiteters motståndskraft, vars tillämpningsområde är detsamma som NIS 2-direktivets vad gäller väsentliga entiteter, det ursprungliga tillämpningsområdet för direktiv 2008/114/EG, som enbart gäller energi och transport, till att omfatta följande sektorer: bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning och rymdsektorn. Det fastställs även tydliga ansvarsområden, en ordentlig planering och ökat samarbete. I detta avseende bör man skapa en referensram för alla risker och stödja medlemsstaterna i deras insatser för att se till att kritiska entiteter kan förebygga, stå emot och hantera konsekvenserna av incidenter, oavsett om riskerna beror på naturliga faror, olyckor, terrorism, inre hot eller hot mot folkhälsan såsom för närvarande.

4.3 Alla medlemsstater måste anta en nationell strategi för att säkerställa kritiska entiteters motståndskraft, genomföra regelbundna riskbedömningar och, på denna grund, identifiera kritiska entiteter. De kritiska entiteterna måste i sin tur genomföra riskbedömningar, vidta lämpliga tekniska och organisatoriska åtgärder för att öka motståndskraften och rapportera incidenter till de nationella myndigheterna. Entiteter som tillhandahåller tjänster till eller i minst en tredjedel av medlemsstaterna omfattas av särskild tillsyn, inklusive särskilda rådgivande uppdrag som anordnas av kommissionen.

4.4 I förslaget till direktiv om kritiska entiteters motståndskraft fastställs olika former av stöd till medlemsstaterna och de kritiska entiteterna, en översikt över riskerna på EU-nivå, bästa praxis och metoder samt utbildning och övningar för att testa de kritiska entiteternas motståndskraft. Systemet för gränsöverskridande samarbete omfattar även en särskild expertgrupp, gruppen för kritiska entiteters motståndskraft, som är ett forum för strategiskt samarbete och informationsutbyte mellan medlemsstaterna.

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

5. **Förslag till ändring av det aktuella lagförslaget**

5.1 EESK välkomnar kommissionens insatser för att göra offentliga och privata entiteter mer motståndskraftiga mot hot till följd av cyberattacker och fysiska attacker. Detta är särskilt viktigt och relevant framför allt mot bakgrund av den snabba digitala omvandling som covid-19-utbrottet har medfört. Kommittén håller också med om det som angavs i meddelandet ”Att forma EU:s digitala framtid”, nämligen att Europa måste utnyttja fördelarna med den digitala tidsåldern och stärka sin industri, med särskild hänsyn till små och medelstora företag, och sin innovationsförmåga på ett inkluderande sätt, enligt en strategi som baseras på fyra pelare – dataskydd, grundläggande rättigheter, säkerhet och cybersäkerhet – som avgörande förutsättningar för ett samhälle som bygger på datas makt.

5.2 Mot bakgrund av resultaten av den konsekvensbedömning och det samråd som föregick förslaget till NIS 2-direktiv och med beaktande av det flera gånger framhävda målet om att undvika fragmentering av de bestämmelser som antagits på nationell nivå (som även framfördes i meddelandet av den 4 oktober 2017 om genomförandet av NIS-direktivet ([6])) konstaterar dock EESK att det inte framgår varför kommissionen inte har föreslagit en förordning i stället för ett direktiv, inte ens bland de alternativ som övervägts.

5.3 EESK noterar att vissa bestämmelser i de båda förslagen till direktiv överlappar varandra eftersom de har ett nära samband och kompletterar varandra: i det ena fokuserar man främst på cybersäkerhet och i det andra på fysisk säkerhet. Kommittén konstaterar också att de kritiska entiteterna enligt direktivet om kritiska entiteters motståndskraft avser samma sektorer och sammanfaller med de ”väsentliga” entiteterna enligt NIS 2-direktivet ([7]). Dessutom omfattas alla kritiska entiteter enligt direktivet om kritiska entiteters motståndskraft av cybersäkerhetskraven i NIS 2-direktivet. I de båda förslagen anges även ett antal övergångsklausuler för att säkerställa sammankopplingen: bestämmelser för förstärkt samarbete mellan myndigheterna, informationsutbyte om övervakning, anmälan till NIS 2-myndigheterna om identifiering av kritiska entiteter enligt direktivet om kritiska entiteters motståndskraft samt regelbundna möten mellan respektive samarbetsgrupper minst en gång per år. De båda förslagen har dessutom samma rättsliga grund, artikel 114 i EUF-fördraget, som syftar till att få den inre marknaden att fungera genom att nationella bestämmelser tillnärmas, såsom den bland annat tolkats av EU-domstolen i domen i mål C58/08, Vodafone m.fl. Man bör därför överväga möjligheten att slå samman de båda förslagen i en enda text i förenklings- och rationaliseringssyfte.

5.4 EESK ställer sig bakom förslaget om att avskaffa åtskillnaden mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster i det ursprungliga NIS-direktivet, men vad gäller dess tillämpningsområde efterlyser kommittén närmare och tydligare riktlinjer för fastställandet av de entiteter som omfattas av direktivet. Utöver hänvisningarna i bilagorna I och II hänvisas i NIS 2-direktivet nämligen till en rad kriterier som inte är enhetliga och som kräver känsliga kvalitativa och kvantitativa bedömningar som kan genomföras på olika sätt på nationell nivå, med risk för att på nytt orsaka den fragmentering som man ville undvika genom detta lagförslag. Det är viktigt att undvika att olika tillvägagångssätt på nationell nivå leder till hinder för konkurrensen och den fria rörligheten för varor och tjänster, vilket riskerar att påverka företagen och handeln negativt.

5.5 Enligt NIS 2-direktivet omfattas kritiska aktörer inom de sektorer som anses vara ”väsentliga” i det aktuella förslaget också av allmänna skyldigheter att förbättra motståndskraften, med särskild tonvikt på risker som inte är cyberrelaterade enligt direktivet om kritiska entiteters motståndskraft. I det sistnämnda direktivet anges det dock uttryckligen att detsamma inte gäller de frågor som omfattas av NIS 2-direktivet. I direktivet om kritiska entiteters motståndskraft anges det nämligen att eftersom cybersäkerhet hanteras i tillräcklig grad genom NIS 2-direktivet bör de frågor som omfattas av det direktivet uteslutas från tillämpningsområdet för direktivet om kritiska entiteters motståndskraft, utan att det påverkar tillämpningen av den särskilda ordningen för entiteter inom sektorn för digital infrastruktur. I direktivet om kritiska entiteters motståndskraft konstateras även att entiteter som tillhör sektorn för digital infrastruktur huvudsakligen baseras på nätverks- och informationssystem och omfattas av NIS 2-direktivet, som även behandlar den fysiska säkerheten hos sådana system som en del av deras skyldigheter i fråga om hantering och rapportering av cybersäkerhetsrisker. Samtidigt utesluter inte direktivet om kritiska entiteters motståndskraft att vissa särskilda bestämmelser kan vara tillämpliga på dem.

5.6 Mot denna komplexa bakgrund anser EESK att det är mycket viktigt att kommissionen klargör det exakta tillämpningsområdet för dessa två regeluppsättningar, särskilt i de fall där olika bestämmelser reglerar samma fråga eller entitet.

5.7 Tydlighet i varje regleringsbestämmelse, än mer om den ingår i sådana omfattande och komplexa texter som de föreliggande, bör utgöra ett grundläggande mål, på alla nivåer, tillsammans med minskad byråkrati och fragmentering genom förenklade förfaranden, säkerhetskrav och incidentrapporteringsskyldigheter. Man bör också undvika att ökningen

([6]) COM(2017) 476 final.
([7]) Bilaga I (EUT L 194, 19.7.2016, s. 1).

av antalet organ som ansvarar för specifika uppgifter äventyrar ett tydligt fastställande av deras befogenheter, eftersom detta skulle undergräva de mål som eftersträvas. Även av detta skäl skulle det kunna vara lämpligt, till fördel för både medborgare och företag, att slå samman de båda förslagen till direktiv i en enda text och därmed undvika en ibland komplicerad tolkning och tillämpning.

5.8 I flera fall hänvisas i NIS 2-direktivet till bestämmelser i andra rättsliga instrument, såsom direktiv (EU) 2018/1972 ([8]) om inrättande av en europeisk kodex för elektronisk kommunikation, vars tillämpning styrs av specialitetsprincipen. Vissa bestämmelser i det direktivet upphävs uttryckligen (artiklarna 40 och 41), medan andra fortfarande ska tillämpas enligt ovannämnda princip, utan att något förtydligande lämnas i detta avseende. På denna punkt skulle EESK vilja att man skingrar alla tvivel för att undvika tolkningsproblem. När det gäller sanktionssystemet stöder EESK också kommissionens mål att harmonisera systemet i händelse av bristande efterlevnad i riskhanteringen, i samband med bättre informationsutbyte och samarbete på EU-nivå.

5.9 EESK erkänner den grundläggande roll, som framhålls i förslaget till direktiv, som spelas av de ”väsentliga” och ”viktiga” entiteternas ledningsorgan i cybersäkerhetsstrategin och riskhanteringen, eftersom de ska godkänna riskhanteringsåtgärder, övervaka deras genomförande och agera vid eventuell bristande efterlevnad. I detta avseende föreskrivs det att dessa organs medlemmar regelbundet måste genomgå särskild utbildning för att förvärva tillräcklig kunskap och kompetens för att kunna förstå och hantera de olika cybersäkerhetsriskerna och bedöma deras effekter. Kommittén anser dock att man i förslaget bör ange innehållet i denna kunskap och kompetens för att ge vägledning på europeisk nivå om vilken utbildningskompetens som anses lämplig för att uppfylla kraven i förslagen, i syfte att undvika att kraven och innehållet i utbildningarna skiljer sig åt mellan länderna.

5.10 EESK instämmer i den viktiga roll som Enisa spelar i den övergripande institutionella och operativa ramen för cybersäkerhet på europeisk nivå. I detta avseende anser kommittén att detta organ, utöver rapporten om cybersäkerhetsläget i unionen, online bör offentliggöra aktuell information om cybersäkerhetsincidenter och sektorsspecifika tillkännagivanden, för att tillhandahålla ett användbart informationsverktyg som gör att aktörer som berörs av NIS 2-direktivet bättre kan skydda sina företag.

5.11 EESK håller med om att tillgången till korrekt och aktuell information om sårbarheter som påverkar IKT-produkter och IKT-tjänster bidrar till en förbättrad hantering av cybersäkerhetsrisker. I detta avseende är källor till offentligt tillgänglig information om sårbarheter ett viktigt verktyg för behöriga nationella myndigheter, CSIRT-enheter, företag och användare. EESK ställer sig därför bakom förslaget om att ge Enisa i uppdrag att inrätta ett europeiskt sårbarhetsregister till vilket väsentliga och viktiga entiteter och deras leverantörer kan rapportera information som gör att användarna kan vidta lämpliga avhjälpande åtgärder. Kommittén anser också att denna rapportering av sårbarheterna och de allvarligaste incidenterna bör göras obligatorisk i stället för frivillig, så att registret blir ett användbart instrument även för de upphandlande enheterna inom ramen för olika upphandlingsförfaranden på europeisk nivå, inklusive dem för 5G-produkter och 5G-teknik. Ett sådant register skulle då innehålla information som skulle vara användbar vid utvärderingar av anbud, i syfte att kontrollera anbudens kvalitet samt de europeiska och utomeuropeiska uppdragstagarnas tillförlitlighet när det gäller säkerheten hos de produkter och tjänster som är föremål för anbudsinfordran, i enlighet med rekommendationen om it-säkerhet i 5G-nät av den 26 mars 2019. Man bör även se till att informationen i registret görs tillgänglig på ett sätt som innebär att alla typer av diskriminering undviks.

Bryssel den 27 april 2021.

Christa SCHWENG
Europeiska ekonomiska och sociala kommitténs ordförande

([8]) EUT L 321, 17.12.2018, s. 6.