Europa-Parlamentet
2019-2024

Mødedokument

A9-0426/2023

8.12.2023

***I
BETÆNKNING

om forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Udvalget om Industri, Forskning og Energi

Ordfører: Lina Gálvez Muñoz

Tegnforklaring

*	Høringsprocedure
***	Godkendelsesprocedure
***I	Almindelig lovgivningsprocedure (førstebehandling)
***II	Almindelig lovgivningsprocedure (andenbehandling)
***III	Almindelig lovgivningsprocedure (tredjebehandling)

(Proceduren afhænger af, hvilket retsgrundlag der er valgt i udkastet til retsakt)

Ændringsforslag til et udkast til retsakt

Ændringsforslag fra Parlamentet opstillet i to kolonner

Tekst, der udgår, er markeret med ***fede typer og kursiv*** i venstre kolonne.
Tekst, der udskiftes, er markeret med ***fede typer og kursiv*** i begge kolonner.
Ny tekst er markeret med ***fede typer og kursiv*** i højre kolonne.

Den første og den anden linje i informationsblokken til hvert ændringsforslag angiver den relevante passage i det pågældende udkast til retsakt. Hvis et ændringsforslag angår en eksisterende retsakt, som udkastet til retsakt har til formål at ændre, indeholder informationsblokken tillige en tredje og en fjerde linje, hvori det er anført, hvilken eksisterende retsakt og hvilken bestemmelse heri der er berørt.

Ændringsforslag fra Parlamentet i form af en konsolideret tekst

Ny tekst er markeret med ***fede typer og kursiv***. Tekst, som er bortfaldet, markeres med symbolet ▌ eller med overstregning. Ved udskiftninger markeres den nye tekst med ***fede typer og kursiv***, og den udskiftede tekst slettes eller overstreges.
Som en undtagelse bliver rent tekniske justeringer, der er foretaget af de berørte tjenestegrene med henblik på udarbejdelsen af den endelige tekst, ikke markeret.

INDHOLD

Side

DA

FORSLAG TIL EUROPA-PARLAMENTETS LOVGIVNINGSMÆSSIGE BESLUTNING

om forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Almindelig lovgivningsprocedure: førstebehandling)

Europa-Parlamentet,

– der henviser til Kommissionens forslag til Europa-Parlamentet og Rådet (COM(2023)0209),

– der henviser til artikel 294, stk. 2, artikel 173, stk. 3, og artikel 322, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde, på grundlag af hvilke Kommissionen har forelagt forslaget for Parlamentet (C9-0136/2023),

– der henviser til artikel 294, stk. 3, i traktaten om Den Europæiske Unions funktionsmåde,

– der henviser til udtalelse af 13. juli 2023 fra Det Europæiske Økonomiske og Sociale Udvalg[1],

– der henviser til forretningsordenens artikel 59,

– der henviser til udtalelser fra Udenrigsudvalget og Transport- og Turismeudvalget,

– der henviser til betænkning fra Udvalget om Industri, Forskning og Energi (A9-0426/2023),

1. vedtager nedenstående holdning ved førstebehandling;

2. godkender sin erklæring, der er vedføjet som bilag til denne beslutning;

3. anmoder om fornyet forelæggelse, hvis Kommissionen erstatter, i væsentlig grad ændrer eller agter i væsentlig grad at ændre sit forslag;

4. pålægger sin formand at sende Parlamentets holdning til Rådet, Kommissionen og de nationale parlamenter.

[1] EUT C 349 af 29.9.2023, s. 167.

Ændringsforslag 1

EUROPA-PARLAMENTETS ÆNDRINGSFORSLAG*

til Kommissionens forslag

2023/0109 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser *og om ændring af forordning (EU) 2021/694*

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR –

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 173, stk. 3, og artikel 322, stk. 1, litra a),

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Revisionsretten[2],

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[3],

under henvisning til udtalelse fra Regionsudvalget[4],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af økonomien ***og demokratiet, men har samtidig medført mulige sårbarheder,*** da offentlige forvaltninger, virksomheder og borgere mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden.

(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed ***på EU-plan og globalt plan, hvad angår fremgangsmåde og virkning***, herunder angreb mod forsyningskæden i form af cyberspionage, ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et

* Ændringer: Ny eller ændret tekst er markeret med fede typer og kursiv; udgået tekst er markeret med symbolet ▌.

[2] EUT C […] af […], s. […].
[3] EUT C […] af […], s. […].
[4] EUT C […] af […], s. […].

trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på ***økonomier, demokratier*** og kritisk infrastruktur ***i hele Unionen***, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige ***og*** kriminelle ▌ aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande. ***Der er derfor behov for et tæt og koordineret samarbejde mellem den offentlige og den private sektor, den akademiske verden og medierne. Desuden skal Unionens reaktion koordineres med internationale institutioner samt betroede og ligesindede internationale partnere. Betroede og ligesindede internationale partnere er lande, der deler Unionens værdier om demokrati, engagement i menneskerettigheder, effektiv multilateralisme og en regelbaseret verdensorden i overensstemmelse med internationale samarbejdsrammer og -aftaler. For at sikre samarbejde med betroede og ligesindede internationale partnere og beskyttelse mod systemiske rivaler bør enheder, der er etableret i tredjelande, som ikke er parter i GPA-aftalen, ikke have mulighed for at deltage i udbud i henhold til denne forordning.***

(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[5] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder***, navnlig mikrovirksomheder, små og mellemstore virksomheder (SMV'er), herunder startupvirksomheder*** og enheder, der driver kritisk infrastruktur***, herunder lokale og regionale myndigheder,*** over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester ***og opbygning af kapaciteter til at udvikle cybersikkerhedsfærdigheder***, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser.

(3a) Cyberangreb er ofte rettet mod lokale, regionale eller nationale offentlige tjenester og infrastrukturer. Lokale myndigheder er blandt de mest sårbare mål for cyberangreb på grund af deres mangel på finansielle og menneskelige ressourcer. Det er derfor særligt vigtigt, at ledere på lokalt plan gøres opmærksomme på behovet for at øge den digitale modstandsdygtighed, øge deres kapacitet til at mindske virkningerne af cyberangreb og udnytte de muligheder, der er fastsat i denne forordning.

[5] https://futureu.europa.eu/da/

(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[6], Kommissionens henstilling (EU) 2017/1584[7], Europa-Parlamentets og Rådets direktiv 2013/40/EU[8] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[9]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

(5) De voksende cybersikkerhedsrisici og det generelt komplekse trusselsbillede, hvor der er en klar risiko for, at cyberhændelser spreder sig fra én medlemsstat til andre og fra et tredjeland til Unionen, kræver styrket solidaritet på EU-niveau for bedre at kunne opdage, ▌reagere på ***og komme sig efter*** cybersikkerhedstrusler og -hændelser. Medlemsstaterne har også opfordret Kommissionen til at fremsætte et forslag om en ny beredskabsfond for cybersikkerhed i Rådets konklusioner om EU's cyberposition[10].

(6) I den fælles meddelelse om EU's politik for cyberforsvar[11], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til at opdage og reagere på hændelser ved at fremme etableringen af et EU-***netværk*** af sikkerhedsoperationscentre ("SOC'er"), støtte en gradvis opbygning af en cybersikkerhedsreserve på EU-plan med brug af tjenester fra betroede private udbydere og teste kritiske enheder for potentielle sårbarheder baseret på EU's risikovurderinger.

(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at ***forebygge og*** reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør et paneuropæisk ***netværk*** af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser ***og dermed styrke Unionens kapacitet til at opdage trusler og dele informationer***. Der bør etableres en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige

---

[6] 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 (EUT L 333 af 27.12.2022).

[7] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[8] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

[9] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

[10] Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, som blev godkendt af Rådet på samlingen den 23. maj 2022 (9364/22).

[11] Fælles meddelelse til Europa-Parlamentet og Rådet — EU's politik for cyberforsvar JOIN/2022/49 final.

eller omfattende cybersikkerhedshændelser og sikre en omgående efterfølgende genopretning. Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

(8) For at opfylde disse målsætninger er det også nødvendigt at ændre Europa-Parlamentets og Rådets forordning (EU) 2021/694[12] på visse områder. Denne forordning bør navnlig ændre forordning (EU) 2021/694 for så vidt angår tilføjelse af nye operationelle mål for det europæiske cyberskjold og beredskabsmekanismen ***for cybersikkerhed*** under specifikt mål nr. 3 i programmet for et digitalt Europa, hvis formål er at sikre det digitale indre markeds modstandsdygtighed, integritet og troværdighed, styrke kapaciteten til at overvåge cyberangreb og -trusler og reagere på dem og styrke det grænseoverskridende samarbejde om cybersikkerhed. De særlige betingelser, hvorunder der kan ydes finansiel støtte til disse aktioner, og de forvaltnings- og koordineringsmekanismer, der er nødvendige for at nå de fastsatte målsætninger, bør fastlægges. Andre ændringer af forordning (EU) 2021/694 bør omfatte beskrivelse af foreslåede foranstaltninger under de nye operationelle målsætninger og målbare indikatorer til overvågning af gennemførelsen heraf.

(9) Finansieringen af foranstaltninger under denne forordning bør fastsættes i forordning (EU) 2021/694, som fortsat bør være den relevante basisretsakt for disse foranstaltninger, der hører under specifik målsætning nr. 3 i programmet for et digitalt Europa. Der vil i de relevante arbejdsprogrammer blive fastsat særlige betingelser for deltagelse i de enkelte aktioner i overensstemmelse med den gældende bestemmelse i forordning (EU) 2021/694.

(9a) I lyset af den geopolitiske udvikling og det voksende cybertrusselsbillede (EPP 52) og for at sikre kontinuitet og videreudvikling efter 2027 af de foranstaltninger, der er fastsat i denne forordning, navnlig det europæiske cyberskjold og beredskabsmekanismen for cybersikkerhed, er det nødvendigt at sikre en særlig budgetpost i den flerårige finansielle ramme for perioden 2028-2034. Medlemsstaterne bør bestræbe sig på at støtte alle nødvendige foranstaltninger til at reducere cybertrusler og -hændelser i hele Unionen og styrke solidariteten.

(10) Horisontale finansielle regler, der er vedtaget af Europa-Parlamentet og Rådet på grundlag af artikel 322 i TEUF, finder anvendelse på denne forordning. Disse regler er fastsat i ***Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046[13]*** og fastlægger navnlig proceduren for opstilling og gennemførelse af Unionens budget og indeholder bestemmelser om kontrol af de finansielle aktørers ansvar. Regler vedtaget på grundlag af artikel 322 i TEUF omfatter også en generel ordning vedrørende

---

[12] Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240 (EUT L 166 af 11.5.2021, s. 1).

Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj)).

konditionalitet med henblik på beskyttelse af Unionens budget som fastsat i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2020/2092[14].

(11) Med henblik på forsvarlig økonomisk forvaltning bør særlige regler fastsættes for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i ***forordning (EU, Euratom) 2018/1046***, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler.

(11a) Beredskabsmekanismen for cybersikkerhed og EU's cybersikkerhedsreserve, der oprettes ved denne forordning, er nye initiativer og blev ikke forudset ved fastlæggelsen af den flerårige finansielle ramme for 2021-2027, og finansieringen af disse initiativer har til formål at begrænse nedskæringen af finansieringen til andre prioriteter i programmet for et digitalt Europa til det lavest mulige niveau. Den andel af de finansielle ressourcer, der er afsat til EU's cybersikkerhedsreserve, bør derfor reduceres og bør primært trækkes fra de uudnyttede margener under lofterne i den flerårige finansielle ramme eller mobiliseres gennem de særlige instrumenter under den ikketematiske flerårige finansielle ramme. Enhver øremærkning eller omfordeling af midler fra eksisterende programmer bør begrænses til et absolut minimum for at skærme eksisterende programmer, navnlig Erasmus+, mod negative virkninger og sikre, at disse programmer kan nå de mål, der er fastsat for dem.

(12) For mere effektivt at forebygge, vurdere, reagere på og ***komme sig efter*** cybertrusler og -hændelser er det nødvendigt at opbygge en mere omfattende viden om truslerne mod kritiske aktiver og infrastrukturer på Unionens område, herunder geografisk fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer. ***En proaktiv tilgang til at påvise, afbøde og forebygge potentielle cybertrusler nødvendiggør en øget evne hos avancerede detektionskapaciteter til at standse avancerede vedvarende trusler. Trusselsefterretninger er oplysninger, der indsamles, analyseres og fortolkes for at forstå potentielle trusler og risici. Gennem analyse og samkøring af store mængder data afslører de mønstre, tendenser og kompromitteringsindikatorer, der kan afsløre ondsindet aktivitet eller sårbarheder.*** Der bør etableres et ***netværk*** af SOC'er ("det europæiske cyberskjold") bestående af flere interoperable grænseoverskridende platforme, som hver samler en række nationale SOC'er. Infrastrukturen bør tjene nationale og europæiske cybersikkerhedsinteresser og -behov. Den nyeste teknologi til avancerede dataindsamlings- og analyseværktøjer bør udnyttes, cyberdetektions- og -forvaltningskapaciteten bør udnyttes, og et situationskendskab i realtid bør opbygges. ***En national SOC er en centraliseret kapacitet med ansvar for løbende at indsamle trusselsefterretninger og forbedre cybersikkerhedsstatussen for enheder under national jurisdiktion ved at forebygge, opdage og analysere cybersikkerhedstrusler.*** Infrastrukturen skal forbedre afsløring af cybersikkerhedstrusler og -hændelser og dermed supplere og støtte Unionens enheder og netværk med ansvar for krisestyring i

[14] ***Europa-Parlamentets og Rådets forordning (EU, Euratom) 2020/2092 af 16. december 2020 om en generel ordning med konditionalitet til beskyttelse af Unionens budget (EUT L 433 I af 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

Unionen, navnlig EU-netværket af forbindelsesorganisationer for cyberkriser ("EU-CyCLONe") som defineret i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[15].

(13) De enkelte medlemsstater bør ***for at deltage i cyberskjoldet hver især*** udpege et offentligt organ på nationalt plan, der har til opgave at koordinere aktiviteter til afsløring af cybertrusler i den pågældende medlemsstat. ***Medlemsstaterne opfordres til at inkorporere den nationale SOC-kapacitet i deres eksisterende cyberstruktur og -styring for ikke at skabe yderligere styringslag og til at bringe denne forordning i overensstemmelse med gældende retsakter, herunder direktiv (EU) 2022/2555.*** Disse nationale sikkerhedsoperationscentre (SOC'er) bør fungere som reference- og indgangspunkt på nationalt plan for ***private og offentlige enheders, navnlig deres nationale SOC'ers,*** deltagelse i det europæiske cyberskjold, og de bør sikre, at oplysninger om cybertrusler fra offentlige og private enheder deles og indsamles på nationalt plan på en effektiv og koordineret måde. ***Nationale SOC'er bør styrke samarbejdet og informationsudvekslingen mellem offentlige og private enheder for at nedbryde de aktuelle kommunikationssiloer. I den forbindelse kan de støtte oprettelsen af dataudvekslingsmodeller og bør lette og tilskynde til udveksling af oplysninger i et betroet og sikkert miljø. Et tæt og koordineret samarbejde mellem offentlige og private enheder er centralt, hvis Unionens modstandsdygtighed på cybersikkerhedsområdet skal styrkes.***

(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet***, herunder indsamling og deling af data og oplysninger om mulig hacking, nyopståede ondsindede trusler og angrebsværktøjer, som endnu ikke har været benyttet ved en cyberhændelse, samt analyseindsatser***, om cybersikkerhedstrusler, navnlig gennem deling af data fra forskellige offentlige eller private kilder samt gennem deling og fælles anvendelse af avancerede værktøjer og fælles udvikling af detektions-, analyse- og forebyggelseskapaciteter i et ***pålideligt og*** sikkert miljø ***med støtte fra ENISA i anliggender, der vedrører operationelt samarbejde mellem medlemsstaterne. De grænseoverskridende SOC'er bør lette og tilskynde til deling af oplysninger i et pålideligt og sikkert miljø*** og bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.

(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv (EU) 2022/2555. De grænseoverskridende SOC'er skal udgøre en ny kapacitet, der er ***inkorporeret i den eksisterende cybersikkerhedsinfrastruktur, navnlig*** CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og

[15] 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).

private enheder, ***navnlig deres SOC'er,*** værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til ***Unionens teknologiske suverænitet, dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed og til udviklingen af et væsentligt økosystem for cybersikkerhed, herunder i samarbejde med betroede og ligesindede internationale parter***. .

(16) De grænseoverskridende SOC'er bør fungere som et centralt knudepunkt, hvor relevante data og efterretninger om cybertrusler generelt sammenstilles, og de skal muliggøre udveksling af trusselsoplysninger blandt en lang række forskellige aktører (f.eks. IT-beredskabsenheder (CERT'er), CSIRT'er, informationsdelings- og analysecentre (ISAC'er) og operatører af kritisk infrastruktur ***med henblik på at gøre det lettere at nedbryde de aktuelt eksisterende kommunikationssiloer***. ***I den forbindelse kunne grænseoverskridende SOC'er også støtte oprettelsen af modeller for dataudveksling i hele Unionen.*** De oplysninger, der udveksles mellem deltagerne i et grænseoverskridende SOC, kan omfatte data fra netværk og sensorer, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, trusler og sårbarheder***, herunder indsamling og deling af data og oplysninger om mulig hacking, nyopståede ondsindede trusler og angrebsværktøjer, som endnu ikke har været benyttet i forbindelse med cyberhændelser, samt analyseindsatser.*** Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er.

(17) At de relevante myndigheder opbygger et fælles situationskendskab er en nødvendig forudsætning for EU-dækkende beredskab og koordinering vedrørende væsentlige og omfattende cybersikkerhedshændelser. Ved direktiv (EU) 2022/2555 oprettes EU–CyCLONe for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og for at sikre regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser omhandler alle de relevante aktørers rolle. I direktiv (EU) 2022/2555 påpeges også Kommissionens ansvar i forbindelse med EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU[16], samt for at udarbejde analytiske rapporter om ordningerne under den integrerede mekanisme for politisk kriserespons ("IPCR") i henhold til ***Rådets*** gennemførelsesafgørelse (EU) 2018/1993[17]. I situationer, hvor grænseoverskridende SOC'er indhenter oplysninger vedrørende en potentiel eller igangværende væsentlig cybersikkerhedshændelse, bør de derfor give relevante oplysninger til EU-CyCLONe, CSIRT-netværket og Kommissionen ***i overensstemmelse med direktiv (EU) 2022/2555***. Afhængigt af situationen kan de oplysninger, der skal udveksles, især omfatte tekniske oplysninger, oplysninger om angriberens eller den mulige angriberes kendetegn og motiver og ikke-tekniske oplysninger på overordnet niveau om en potentiel eller igangværende omfattende cybersikkerhedshændelse. I den sammenhæng bør der tages

---

[16] ***Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (***EUT L 347 af 20.12.2013, s. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

[17] ***Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons (***EUT L 320 af 17.12.2018, s. 28, ***ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

behørigt hensyn til, hvilke oplysninger der er nødvendige, og til den eventuelt følsomme karakter af de udvekslede oplysninger.

(18) Enheder, der deltager i det europæiske cyberskjold, bør sikre en høj grad af indbyrdes interoperabilitet, herunder, hvor det er relevant, for så vidt angår dataformater, taksonomi, datahåndterings- og dataanalyseværktøjer og sikre kommunikationskanaler, et minimumsniveau af sikkerhed i applikationslaget, oversigtstavle over situationskendskab samt indikatorer. Ved vedtagelse af en fælles taksonomi og udvikling af en skabelon til situationsrapporter til beskrivelse af den tekniske årsag til og virkningerne af cybersikkerhedshændelser bør der tages hensyn til det igangværende arbejde med underretning om hændelser i forbindelse med gennemførelsen af direktiv (EU) 2022/2555.

(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt ***og sikkert*** miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer ***samt kvalificeret personale***. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse.

(20) Gennem indsamling, deling og udveksling af data bør det europæiske cyberskjold kunne styrke Unionens teknologiske suverænitet, ***dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed og et væsentligt EU-økosystem for cybersikkerhed***. Sammenlægning af udvalgte data af høj kvalitet bør også kunne bidrage til udviklingen af avancerede teknologier inden for kunstig intelligens og dataanalyse. ***Kunstig intelligens er mest effektiv, når den kombineres med menneskelig analyse. Derfor er en kvalificeret arbejdsstyrke fortsat afgørende for at samle data af høj kvalitet.*** Processen bør fremmes ved at forbinde det europæiske cyberskjold med den paneuropæiske infrastruktur til højtydende databehandling, der er oprettet ved Rådets forordning (EU) 2021/1173[18].

(21) Selv om det europæiske cyberskjold er et civilt projekt, kan cyberforsvarssektoren udnytte et større civilt situationskendskab og en stærkere civil detektionskapacitet, der er udviklet med henblik på beskyttelse af kritisk infrastruktur. Grænseoverskridende SOC'er bør med støtte fra Kommissionen og Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") og i samarbejde med Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") gradvist udvikle særlige protokoller og standarder for ***adgangsbetingelser og beskyttelsesforanstaltninger*** for at muliggøre samarbejde med cyberforsvarssektoren, herunder kontrol- og sikkerhedsforhold***, under hensyntagen til institutionernes civile karakter og finansieringens bestemmelsessted, og derfor anvende de midler, der er til rådighed for forsvarssektoren***. Udviklingen af det europæiske cyberskjold bør ledsages af overvejelser om at muliggøre et fremtidigt samarbejde med de netværk og platforme, der har ansvar for informationsudveksling i cyberforsvarssektoren, i tæt samarbejde med den højtstående repræsentant ***og under fuld overholdelse af rettigheder og friheder***.

[18] Rådets forordning (EU) 2021/1173 af 13. juli 2021 om oprettelse af et fællesforetagende for europæisk højtydende databehandling og om ophævelse af forordning (EU) 2018/1488 (EUT L 256 af 19.7.2021, s. 3), ***ELI:*** ***https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=da***).

(22) Udveksling af oplysninger mellem deltagerne i det europæiske cyberskjold bør ske i overensstemmelse med eksisterende retlige krav og navnlig Unionens og den nationale databeskyttelseslovgivning samt Unionens konkurrenceregler vedrørende udveksling af oplysninger. Modtageren af oplysningerne bør, i det omfang behandlingen af personoplysninger er nødvendig, gennemføre tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og frihedsrettigheder og tilintetgøre data, så snart de ikke længere er nødvendige til det angivne formål, og underrette det organ, der stiller oplysningerne til rådighed, om, at oplysningerne er blevet destrueret.

(23) Med forbehold af artikel 346 i TEUF bør udvekslingen af oplysninger, der er fortrolige i henhold til EU-***ret*** eller national ***ret***, begrænses til det omfang, der er relevant og står i rimeligt forhold til formålet med denne udveksling. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser med fuld fortrolighed vedrørende handels- og forretningshemmeligheder.

(24) I betragtning af de stigende risici og antallet af cyberhændelser, der påvirker medlemsstaterne, er det nødvendigt at oprette et krisestøtteinstrument for at forbedre Unionens modstandsdygtighed over for væsentlige og omfattende cybersikkerhedshændelser og supplere medlemsstaternes foranstaltninger gennem finansiel nødhjælp til beredskab, indsats og øjeblikkelig genopretning af væsentlige tjenester. Dette instrument bør muliggøre hurtig ***og effektiv*** udsendelse af bistand under nærmere fastsatte omstændigheder og på klare betingelser og give mulighed for nøje overvågning og evaluering af, hvordan ressourcerne er blevet anvendt. Mens medlemsstaterne har det primære ansvar for forebyggelse, beredskab og indsats i tilfælde af cybersikkerhedshændelser og -kriser, skal ***beredskabsmekanismen for cybersikkerhed*** øge solidariteten mellem medlemsstaterne i overensstemmelse med artikel 3, stk. 3, i traktaten om Den Europæiske Union (TEU).

(25) ***Beredskabsmekanismen for cybersikkerhed*** bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed ("ENISA") i overensstemmelse med dets mandat, den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold[19] og hybride beredskabshold. Beredskabsmekanismen bør indgå i løsning af behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande.

(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[20], IPCR[21] og direktiv (EU)

[19] RÅDETS AFGØRELSE (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde (PESCO) og fastlæggelse af listen over deltagende medlemsstater.

[20] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

[21] Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, hvor det er relevant.

(27) Den bistand, der ydes i henhold til denne forordning, bør støtte og supplere de foranstaltninger, som medlemsstaterne træffer på nationalt plan. Med henblik herpå bør der sikres et tæt samarbejde og samråd mellem Kommissionen, ***ENISA*** og berørte medlemsstater. Når en medlemsstat anmoder om støtte i henhold til ***beredskabsmekanismen for cybersikkerhed***, bør den fremlægge relevante oplysninger, der begrunder behovet for støtte.

(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette én eller flere cyberkrisestyringsmyndigheder og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt og virkningsfuldt. I henhold til direktivet skal medlemsstaterne endvidere identificere kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise, og vedtage en national omfattende beredskabsplan for cybersikkerhedshændelser og -kriser, hvor målsætningerne og ordningerne vedrørende håndtering af væsentlige cybersikkerhedshændelser og -kriser er fastsat. Medlemsstaterne skal også oprette ét eller flere CSIRT'er, der har ansvar for håndtering af hændelser efter en veldefineret proces, der som minimum dækker de sektorer, delsektorer og typer af enheder, der er omfattet af nævnte direktivs anvendelsesområde, og sikre, at de har tilstrækkelige ressourcer til effektivt at udføre deres opgaver. Denne forordning berører ikke Kommissionens rolle med hensyn til at sikre, at medlemsstaterne overholder forpligtelserne i direktiv (EU) 2022/2555. ***Beredskabsmekanismen for cybersikkerhed*** bør yde bistand til foranstaltninger, der har til formål at styrke beredskabet og indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser, støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion.

(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med

Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[22]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

(30) Derudover bør ***beredskabsmekanismen for cybersikkerhed*** yde støtte til andre beredskabsforanstaltninger og støtte beredskabet i andre sektorer, der ikke er omfattet af den koordinerede afprøvning af enheder, der opererer i meget kritiske sektorer. Disse foranstaltninger kan omfatte forskellige typer af nationale beredskabsaktiviteter.

(31) ***Beredskabsmekanismen for cybersikkerhed*** bør yde støtte til indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser for at støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion. Den bør, hvor det er relevant, supplere EU-civilbeskyttelsesmekanismen for at sikre en samlet tilgang til indsatsen over for følgerne af cyberhændelser for borgerne.

(32) ***Beredskabsmekanismen for cybersikkerhed*** bør støtte bistand fra andre medlemsstater til en medlemsstat, der er berørt af en væsentlig eller omfattende cybersikkerhedshændelse, herunder af CSIRT-netværket, jf. artikel 15 i direktiv (EU) 2022/2555. Medlemsstater, der yder bistand, bør have mulighed for at indgive anmodning om dækning af omkostninger i forbindelse med udsendelse af eksperthold inden for rammerne af gensidig bistand. De støtteberettigede omkostninger kan omfatte udgifter til rejser, indkvartering og daglige udgifter for cybersikkerhedseksperter.

(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til støtte for indsatsen og foranstaltninger til omgående genopretning i tilfælde af væsentlige eller omfattende cybersikkerhedshændelser. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate***, og samtidig styrke Unions modstandsdygtighed, herunder deltagelse af europæiske udbydere af administrerede sikkerhedstjenester, som er SMV'er, og sikre, at der skabes et økosystem for cybersikkerhed, navnlig mikrovirksomheder og SMV'er, herunder startupvirksomheder, med investeringer i forskning og innovation (FoI) med henblik på at udvikle avancerede teknologier, eksempelvis teknologier vedrørende skyen og kunstig intelligens***. ***Betroede udbydere, herunder SMV'er, bør kunne samarbejde med hinanden for at opfylde ovenstående kriterier.*** Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i kritiske eller meget kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. ***Cybersikkerhedsreserven bør derfor tilskynde til investeringer i forskning og innovation for at sætte gang i udviklingen af disse teknologier. Hvis det er relevant, kan der gennemføres fælles øvelser med de betroede udbydere og potentielle brugere af cybersikkerhedsreserven for at sikre, at reserven fungerer effektivt, når der er behov herfor.*** Når medlemsstaterne anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som

[22] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011.

bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer***, kontorer*** og agenturer på lignende betingelser. ***Kommissionen bør sikre inddragelse af og omfattende udvekslinger med medlemsstaterne med henblik på at undgå overlapning med lignende initiativer, herunder inden for Den Nordatlantiske Traktats Organisation (NATO).***

(34) Med henblik på at udvælge private tjenesteudbydere, der skal levere tjenester i forbindelse med EU's cybersikkerhedsreserve, er det nødvendigt at fastsætte et sæt minimumskriterier, der bør indgå i udbuddet til udvælgelse af udbyderne, for at sikre, at behovene opfyldes hos medlemsstaternes myndigheder og enheder, der opererer i kritiske eller meget kritiske sektorer. ***Mindre udbydere, som er aktive på regionalt og lokalt plan, bør tilskyndes til at deltage.***

(35) For at støtte etableringen af EU's cybersikkerhedsreserve kan Kommissionen overveje at anmode ENISA om at udarbejde et forslag til en certificeringsordning for kandidater i henhold til forordning (EU) 2019/881 for administrerede sikkerhedstjenester på de områder, der er omfattet af ***beredskabsmekanismen for cybersikkerhed***. ***For at kunne udføre de yderligere opgaver, der følger af denne bestemmelse, bør ENISA modtage passende supplerende finansiering.***

(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en effektiv reaktion på væsentlige og omfattende cybersikkerhedshændelser bør EU-CyCLONe, CSIRT-netværket eller Kommissionen kunne anmode ENISA om at gennemgå og vurdere trusler, sårbarheder og afbødende foranstaltninger i forbindelse med en specifik væsentlig eller omfattende cybersikkerhedshændelse. Efter gennemførelsen af en gennemgang og vurdering af en hændelse bør ENISA udarbejde en rapport om hændelsen i samarbejde med relevante interessenter, herunder repræsentanter fra den private sektor, medlemsstaterne, Kommissionen og andre relevante EU-institutioner, -organer***, -kontorer*** og -agenturer. For så vidt angår den private sektor etablerer ENISA kanaler til udveksling af oplysninger med specialiserede udbydere, herunder udbydere af administrerede sikkerhedsløsninger og leverandører, med henblik på at bidrage til ENISA's opgave med at opnå et højt fælles cybersikkerhedsniveau i hele Unionen. På grundlag af samarbejdet med interessenter, herunder den private sektor, bør rapporten om gennemgang af specifikke hændelser have til formål at vurdere årsagerne til, virkningerne af og modvirkningen af en hændelse, efter at den er indtruffet. Der bør lægges særlig vægt på oplysninger og erfaringer, der indmeldes af udbydere af administrerede sikkerhedstjenester, som opfylder betingelserne om højeste faglige integritet, upartiskhed og den nødvendige tekniske ekspertise som krævet i denne forordning. Rapporten bør leveres og indgå i arbejdet i EU-CyCLONe, CSIRT-netværket og Kommissionen. Når hændelsen vedrører et tredjeland, videresender Kommissionen også rapporten til den højtstående repræsentant.

(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medrører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor kan tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve, hvis dette er fastsat i den respektive associeringsaftale til

programmet for et digitalt Europa. Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med programmet for et digitalt Europa.

(37a) Tredjelande kan få adgang til ressourcer og støtte i henhold til denne forordning ved at benytte støtten fra EU's cybersikkerhedsreserve til håndtering af hændelser. Udbydere af hændelsesberedskabstjenester fra tredjelande, herunder tredjelande, der er associeret med programmet for et digitalt Europa, eller andre internationale partnerlande, samt NATO-medlemmer kan være nødvendige for at levere specifikke tjenester i EU's cybersikkerhedsreserve. For at styrke Unionens teknologiske suverænitet, dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed og for at beskytte Unionens strategiske aktiver, interesser eller sikkerhed bør enheder, som er etableret i tredjelande, der ikke er parter i GPA, og som ikke har været genstand for screening som omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2019/452[23] og, om nødvendigt, for afbødende foranstaltninger, under hensyntagen til målene i nærværende forordning, ikke kunne deltage uanset forordning (EU, Euratom) 2018/1046. Denne forordnings eksterne dimension bør være i overensstemmelse med bestemmelserne i associeringsaftalen under programmet for et digitalt Europa. Deltagelse af tredjelande bør være underlagt offentlig kontrol med deltagelse af de lovgivende myndigheder for at sikre, at borgerne kan deltage i processen.

(38) For at sikre ensartede betingelser for gennemførelse af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge betingelserne for interoperabilitet mellem grænseoverskridende SOC'er fastlægge de proceduremæssige ordninger for udveksling af oplysninger vedrørende en mulig eller igangværende væsentlig cybersikkerhedshændelse mellem grænseoverskridende SOC'er og EU-enheder fastsætte de tekniske krav med henblik på at garantere sikkerheden i forbindelse med det europæiske cyberskjold præcisere, hvilke typer og hvor mange beredskabstjenester der er nødvendige i EU's cybersikkerhedsreserve og yderligere præcisere de detaljerede ordninger for tildeling af støttetjenesterne under EU's cybersikkerhedsreserve. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011*.

---

* ***Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

---

[23] Europa-Parlamentets og Rådets forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen (EUT L 79I af 21.3.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

(38a) Kvalificeret personale, der er i stand til pålideligt at levere de relevante cybersikkerhedstjenester i den højest mulige standard, er nødvendigt for en effektiv gennemførelse af det europæiske cyberskjold og cyberberedskabsmekanismen. Som erkendt i Kommissionens meddelelse af 18. april 2023 om akademiet for cyberfærdigheder er det derfor bekymrende, at Unionen står over for en talentkløft, der er kendetegnet ved mangel på kvalificerede fagfolk, og på samme tid et trusselsbillede i hastig udvikling. Det er vigtigt at overvinde denne talentkløft ved at styrke samarbejde og koordinering mellem de forskellige interessenter, herunder den private sektor, den akademiske verden, medlemsstaterne, Kommissionen og ENISA, for at opskalere og skabe synergier for investeringen i uddannelse og erhvervsuddannelse, udvikling af offentlig-private partnerskaber, støtte til forsknings- og innovationsinitiativer, udvikling og gensidig anerkendelse af fælles standarder og certificering af cybersikkerhedsfærdigheder, herunder gennem den europæiske ramme for cybersikkerhedsfærdigheder, i alle territorier. Dette bør også lette mobiliteten for fagfolk inden for cybersikkerhed i Unionen. Denne forordning bør sigte mod at fremme en mere mangfoldig arbejdsstyrke inden for cybersikkerhed. Alle foranstaltninger, der har til formål at øge cybersikkerhedsfærdighederne, kræver foranstaltninger for at undgå "hjerneflugt" og en risiko for arbejdskraftmobiliteten.

(38b) Der er behov for at styrke specialiserede, tværfaglige og generelle færdigheder og kompetencer i hele Unionen og navnlig fokusere på kvinder, da der fortsat er en kønsbestemt kløft inden for cybersikkerhed, hvor kvinder tegner sig for gennemsnitligt 20 % af arbejdsstyrken på verdensplan. Kvinder skal være til stede og deltage i udformningen af den digitale fremtid og dens forvaltning.

(38c) En styrkelse af forskning og innovation (FoI) inden for cybersikkerhed skal øge Unionens modstandsdygtighed og åbne strategiske autonomi. Det er ligeledes vigtigt at skabe synergier med FoI-programmer og med eksisterende instrumenter og institutioner og at styrke samarbejdet og koordineringen mellem de forskellige interessenter, herunder den private sektor, civilsamfundet, den akademiske verden, medlemsstaterne, Kommissionen og ENISA;

(38d) Denne forordning bør bidrage til forpligtelsen i den europæiske erklæring om digitale rettigheder og principper for det digitale årti med hensyn til at beskytte vores demokratiers, befolkningers, virksomheders og offentlige institutioner mod cybersikkerhedsrisici og cyberkriminalitet, herunder brud på datasikkerheden og identitetstyveri eller manipulation. Anvendelsen af denne forordning bør også bidrage til at forbedre gennemførelsen af anden lovgivning, f.eks. om kunstig intelligens, databeskyttelse og dataregulering med hensyn til cybersikkerhed og cyberrobusthed.

(38e) En styrkelse af cybersikkerhedskulturen, der omfatter sikkerhed, herunder i det digitale miljø, som et offentligt gode, vil være afgørende for en vellykket gennemførelse af denne forordning. Udvikling af foranstaltninger til at inddrage borgerne og øge deres bevidsthed bør derfor være et andet middel til at sikre beskyttelsen af vores demokratier og grundlæggende værdier.

(38f) For at supplere visse ikkevæsentlige elementer i denne forordning bør beføjelsen til at vedtage retsakter i overensstemmelse med artikel 290 i TEUF delegeres til Kommissionen med henblik på at præcisere betingelserne for interoperabilitet mellem de grænseoverskridende SOC'er, fastlægge de proceduremæssige ordninger for udveksling af oplysninger mellem de grænseoverskridende SOC'er på den ene side og

EU-CyCLONe, CSIRT-netværket og Kommissionen på den anden side, præcisere typer og antal af beredskabstjenester, der er nødvendige for EU's cybersikkerhedsreserve, og yderligere præcisere de nærmere ordninger for tildeling af støttetjenester under EU's cybersikkerhedsreserve. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning*. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

**** EUT L 123 af 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

(39) ***Målsætningerne*** for denne forordning***, nemlig at styrke Unionens kapacitet til at forebygge, afsløre, reagere på og komme sig efter cybertrusler og at etablere en generel ramme til at nedbryde kommunikationssiloer, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men*** kan ***snarere*** opfyldes på EU-plan. Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet og proportionalitetsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. ***I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne*** forordning ikke ud over, hvad der er nødvendigt for at nå dette mål —

VEDTAGET DENNE FORORDNING:

Kapitel I

GENERELLE FORMÅL, GENSTAND OG DEFINITIONER

Artikel 1

Genstand og formål

1. Ved denne forordning fastsættes foranstaltninger til styrkelse af Unionens kapacitet til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser, navnlig gennem følgende tiltag:

a) etablering af et paneuropæisk ***netværk af*** sikkerhedsoperationscentre ("et europæisk cyberskjold") for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser

b) oprettelse af en beredskabsmekanisme for cybersikkerhed som støtte til medlemsstaterne til at forberede sig og reagere på samt sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser

(c) oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige eller omfattende hændelser.

2. Formålet med denne forordning er at styrke solidariteten på EU-plan gennem følgende specifikke mål:

(a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og dermed gøre det muligt at ***støtte Unionens og medlemsstaternes industrielle kapacitet i cybersikkerhedssektoren og at*** styrke industriens***, navnlig mikrovirksomheders, SMV'ers, herunder startupvirksomheders,*** og servicesektorernes konkurrenceevne i hele den digitale økonomi, og ***at*** bidrage til Unionens teknologiske suverænitet ***og dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed i denne sektor og styrke cybersikkerhedsøkosystemet med henblik på at sikre stærke EU-kapaciteter, herunder i samarbejde med internationale partnere***

(b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa

(c) at øge Unionens modstandsdygtighed og bidrage til en effektiv indsats ved at gennemgå og vurdere væsentlige eller omfattende hændelser, herunder indhøstede erfaringer og henstillinger, hvor det er relevant

(ca) at udvikle arbejdsstyrkens færdigheder, knowhow og kompetencer på en koordineret måde med henblik på at sikre cybersikkerhed og skabe synergier med akademiet for cybersikkerhedsfærdigheder.

3. Denne forordning berører ikke medlemsstaternes primære ansvar for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

Artikel 2

Definitioner

I denne forordning forstås ved:

-1a) "Nationalt sikkerhedsoperationscenter" eller "nationalt SOC": en central national kapacitet, der løbende indsamler og analyserer efterretninger om cybertrusler og forbedrer cybersikkerhedsstatussen i overensstemmelse med artikel 4

1) **"grænseoverskridende sikkerhedsoperationscenter"** ***eller "*****grænseoverskridende SOC": e**n platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er ***i overensstemmelse med artikel 5***

2) **"offentligt organ"**: ***organer*** som defineret i artikel 2, stk. 1, nr. 4), i Europa-Parlamentets og Rådets direktiv 2014/24/EU[24];

3) **"værtskonsortium"**: et konsortium bestående af deltagende stater repræsenteret ved nationale SOC'er ***i overensstemmelse med artikel 5***

4) **"enhed"**: en enhed som defineret i artikel 6, nr. 38), i direktiv (EU) 2022/2555

4a) "kritisk enhed": en kritisk enhed som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets direktiv (EU) 2022/2557[25]

5) **"enheder, der opererer i kritiske eller meget kritiske sektorer"**: enheder ***i de sektorer***, der er opført i bilag I og II til direktiv (EU) 2022/2555

5a) "håndtering af hændelser": håndtering af hændelser som defineret i artikel 6, nr. 8), i direktiv (EU) 2022/2555

5b) "risiko": en risiko som defineret i artikel 6, nr. 9), i direktiv (EU) 2022/2555

6) "**cybertrussel**": en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

6a) "væsentlig cybertrussel": en væsentlig cybertrussel som defineret i artikel 6, nr. 11, i direktiv (EU) 2022/2555

7) **"væsentlig cybersikkerhedshændelse"**: en cybersikkerhedshændelse, der opfylder kriterierne i artikel 23, stk. 3, i direktiv (EU) 2022/2555

8) **"omfattende cybersikkerhedshændelse"**: en hændelse som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555

9) **"beredskab"**: en tilstand ved en væsentlig eller omfattende cybersikkerhedshændelse af parathed og kapacitet til at sikre en effektiv hurtig reaktion gennem forudgående risikovurderings- og overvågningsforanstaltninger

10) **"indsats"**: tiltag i forbindelse med, under eller efter en væsentlig eller omfattende cybersikkerhedshændelse for at håndtere dens umiddelbare og kortsigtede negative konsekvenser

10a) "udbyder af administrerede sikkerhedstjenester": en udbyder af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555

11) **"betroede udbydere *af administrerede sikkerhedstjenester*"**: betroede udbydere af administrerede sikkerhedstjenester, der er udvalgt ***til at indgå i EU's cybersikkerhedsreserve*** i overensstemmelse med artikel 16 i denne forordning.

---

[24] Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

[25] ***Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (EUT L 333 af 27.12.2022, s. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

Kapitel II

DET EUROPÆISKE CYBERSKJOLD

Artikel 3

Etablering af det europæiske cyberskjold

1. Der oprettes et sammenkoblet paneuropæisk ***netværk*** af sikkerhedsoperationscentre ("det europæiske cyberskjold") med henblik på at udvikle avancerede kapaciteter for Unionen til at opdage, analysere og behandle data om cybertrusler og ***forebygge*** hændelser i Unionen. Skjoldet består af nationale sikkerhedsoperationscentre ("nationale SOC'er") og grænseoverskridende sikkerhedsoperationscentre ("grænseoverskridende SOC'er").

Tiltag til gennemførelse af det europæiske cyberskjold støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

2. Det europæiske cyberskjold skal:

a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende SOC'er ***og, hvis det er relevant, udveksle oplysninger med CSIRT-netværket***

b) tilvejebringe anvendelige oplysninger af høj kvalitet og efterretninger om cybertrusler ved hjælp af de nyeste værktøjer, navnlig kunstig intelligens og dataanalyseteknologier

c) bidrage til bedre beskyttelse mod og reaktion på cybertrusler***, herunder ved at give konkrete anbefalinger til enheder***

d) bidrage til hurtigere opdagelse af cybertrusler og større situationskendskab i hele Unionen

e) levere tjenester og aktiviteter til cybersikkerhedssektoren i Unionen, herunder bidrage til udviklingen af værktøjer inden for avanceret kunstig intelligens og dataanalyse.

Det europæiske cyberskjold udvikles i samarbejde med den paneuropæiske højtydende databehandlingsinfrastruktur, der er etableret i henhold til forordning (EU) 2021/1173.

Artikel 4

Nationale sikkerhedsoperationscentre

1. For at ***kunne*** deltage i det europæiske cyberskjold skal hver medlemsstat udpege mindst ét nationalt SOC. Det nationale SOC skal være en ***centraliseret kapacitet i*** et offentligt organ. ***Når det er muligt, inkorporeres de nationale SOC'er i CSIRT'erne eller anden eksisterende cybersikkerhedsinfrastruktur og -forvaltning.***

Det skal have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private organisationer på nationalt plan, ***navnlig deres nationale SOC'er***, med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser ***og, hvis det er relevant, dele disse oplysninger med medlemmer af CSIRT-netværket i den pågældende medlemsstat*** og bidrage til et grænseoverskridende SOC. Det skal være udstyret med avancerede teknologier, der gør det muligt at ***forebygge***, finde, aggregere og analysere data, der er relevante for cybersikkerhedstrusler og -hændelser.

En national SOC eller CSIRT kan anmode om deres nationale kritiske enheders telemetri-, sensor- eller logningsdata fra udbydere af administrerede sikkerhedstjenester, der leverer en tjeneste til den kritiske enhed. Disse data deles i overensstemmelse med Unionens databeskyttelseslovgivning og udelukkende med det formål at støtte det nationale SOC eller CSIRT i at opdage og forebygge cybersikkerhedstrusler og -hændelser.

2. Efter en indkaldelse af interessetilkendegivelser kan Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) udvælge nationale SOC'er til at deltage i fælles indkøb af værktøjer og infrastrukturer sammen med ECCC. ECCC kan yde tilskud til de udvalgte nationale SOC'er til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af medlemsstaten. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og det nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

3. Et nationalt SOC, der er udvalgt i henhold til stk. 2, forpligter sig til at ansøge om at deltage i et grænseoverskridende SOC senest to år efter den dato, hvor værktøjerne og infrastrukturerne erhverves, eller hvor det modtager tilskudsfinansiering, alt efter hvad der indtræffer først. Hvis et national SOC ikke deltager i et grænseoverskridende SOC på det tidspunkt, er det ikke berettiget til yderligere EU-støtte i henhold til denne forordning.

Artikel 5

Grænseoverskridende sikkerhedsoperationscentre

1. Et værtskonsortium bestående af mindst tre medlemsstater, repræsenteret ved nationale SOC'er, der har forpligtet sig til at samarbejde om at koordinere deres cybersporings- og trusselsovervågningsaktiviteter, er berettiget til at deltage i foranstaltninger til oprettelse af et grænseoverskridende SOC. ***Et grænseoverskridende SOC skal være udformet med henblik på at opdage og analysere cybertrusler og støtte tilvejebringelsen af efterretninger af høj kvalitet,***

navnlig gennem udveksling af data fra forskellige kilder, såvel offentlige som private, samt gennem deling af avancerede værktøjer og fælles udvikling af cyberdetektions-, analyse-, forebyggelses- og beskyttelseskapaciteter i et betroet og sikkert miljø.

2. Efter en indkaldelse af interessetilkendegivelser ***kan*** et værtskonsortium ***blive udvalgt*** af ECCC til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til værtskonsortiet til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 75 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af værtskonsortiet. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og værtskonsortiet en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

2a. Uanset artikel 176 i forordning (EU, Euratom) 2018/1046 deltager enheder, der er etableret i tredjelande, som ikke er parter i GPA-aftalen, ikke i fælles indkøb af værktøjer og infrastrukturer.

3. Medlemmerne af værtskonsortiet indgår en skriftlig konsortieaftale, hvori de interne ordninger for gennemførelse af værts- og brugsaftalen fastlægges.

4. Et grænseoverskridende SOC repræsenteres i juridisk henseende af et nationalt SOC, der fungerer som koordinerende SOC, eller af værtskonsortiet, hvis det har status som juridisk person. Det koordinerende SOC er ansvarligt for overholdelse af kravene i værts- og brugsaftalen og af denne forordning.

Artikel 6

Samarbejde og informationsudveksling inden for og mellem grænseoverskridende SOC'er

1. Medlemmerne af et værtskonsortium udveksler indbyrdes relevante oplysninger inden for den grænseoverskridende SOC, herunder oplysninger om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, indikatorer for kompromittering, fjendtlige taktikker, trusselsspecifikke oplysninger, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til afsløring af cyberangreb, hvor en sådan informationsudveksling:

a) ***forbedrer udvekslingen af efterretninger om cybertrusler mellem nationale og grænseoverskridende SOC'er og industri-ISAC'er med henblik på at forebygge, opdage eller afbøde hændelser***

b) øger cybersikkerhedsniveauet, navnlig ved at øge kendskabet til cybertrusler, begrænse eller hindre muligheden for, at sådanne trusler spreder sig, støtte en række forsvarskapaciteter, afhjælpe og afsløre sårbarheder, støtte teknikker til opdagelse, begrænsning og forebyggelse af trusler, støtte afbødningsstrategier eller indsats- og

genopretningsfaserne eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

2. Den skriftlige konsortieaftale i henhold til artikel 5, stk. 3, skal indeholde:

a) en forpligtelse til at dele vigtige data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger

b) en forvaltningsramme, der tilskynder alle deltagere til at udveksle oplysninger

c) mål for bidrag til udvikling af værktøjer inden for avanceret kunstig intelligens og dataanalyse.

3. For at tilskynde til udveksling af oplysninger mellem grænseoverskridende SOC'er ***og med industri-ISAC'er*** skal disse sikre en høj grad af interoperabilitet indbyrdes ***og, hvis det er muligt, med industri-ISAC'er***. For at sikre interoperabilitet mellem de grænseoverskridende SOC'er ***og med industri-ISAC'er kan standarder og protokoller for informationsudveksling harmoniseres med internationale standarder og bedste praksis i branchen. Der skal også tilskyndes til fælles indkøb af cyberinfrastruktur, -tjenester og -værktøjer.*** Efter høring af ECCC ***og ENISA bemyndiges Kommissionen desuden til senest ... [seks måneder fra datoen for denne forordnings ikrafttræden] at vedtage delegerede retsakter i overensstemmelse med artikel 20a for at supplere denne forordning ved at fastsætte*** betingelserne for interoperabilitet ***i tæt samarbejde med de grænseoverskridende SOC'er og på grundlag af internationale standarder og bedste praksis i industrien.***

4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden ***og, hvis det er relevant, med ISAC'er i industrien***, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges ***under hensyntagen til allerede eksisterende relevante informationsudvekslingsmekanismer, som er fastlagt i direktiv (EU) 2022/2555. Hvis det er relevant, indgår grænseoverskridende SOC'er samarbejdsaftaler med ISAC'er i industrien. I forbindelse med en potentiel eller igangværende omfattende cybersikkerhedshændelse skal informationsudvekslingsmekanismerne opfylde de relevante bestemmelser i direktiv (EU) 2022/2555.***

Artikel 7

Samarbejde og informationsudveksling med *CSIRT-netværket*

1. Hvis grænseoverskridende SOC'er indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse ***med henblik på fælles situationskendskab***, forelægger ***den koordinerende SOC*** uden unødig forsinkelse de relevante oplysninger for ***sin CSIRT eller kompetente myndighed, som uden unødig forsinkelse rapporterer dette til*** EU-CyCLONe, CSIRT-netværket***,*** Kommissionen ***og ENISA i overensstemmelse med*** deres respektive krisestyringsroller ***og -procedurer*** i overensstemmelse med direktiv (EU) 2022/2555. ***Dette stykke pålægger ikke offentlige eller private enheder yderligere forpligtelser til at indberette en potentiel eller igangværende omfattende cybersikkerhedshændelse med henblik på at opfylde de forpligtelser, der er fastsat i direktiv (EU) 2022/2555.***

2. Kommissionen ***tillægges beføjelse til at vedtage*** retsakter ***i overensstemmelse med artikel 20a efter høring af CSIRT-netværket med henblik på at supplere denne forordning***

ved at fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i ***denne artikels*** stk. 1***, og i overensstemmelse med direktiv (EU) 2022/2555***.

Artikel 8

Sikkerhed

1. De medlemsstater, der deltager i det europæiske cyberskjold, sikrer et højt niveau af ***fortrolighed,*** datasikkerhed og fysisk sikkerhed i den infrastruktur, der udgør det europæiske cyberskjold, og sikrer, at infrastrukturen forvaltes og styres hensigtsmæssigt, så den beskyttes mod trusler og så sikkerheden i infrastrukturen og i systemerne, herunder data, der udveksles via infrastrukturen, garanteres.

2. Medlemsstater, der deltager i det europæiske cyberskjold, sikrer, at udvekslingen af oplysninger inden for det europæiske cyberskjold med enheder, der ikke er offentlige organer i medlemsstaterne, ikke har en negativ indvirkning på Unionens sikkerhedsinteresser.

3. Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter tekniske krav til medlemsstaternes opfyldelse af forpligtelserne i stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2. ***De skal være i overensstemmelse med direktiv (EU) 2022/2555 og (EU) 2022/2557.*** I ***sine gennemførelsesretsakter*** tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører.

Kapitel III

BEREDSKABSMEKANISME FOR CYBERSIKKERHED

Artikel 9

Etablering af beredskabsmekanismen *for cybersikkerhed*

1. Der etableres en beredskabsmekanisme for cybersikkerhed for at forbedre Unionens modstandsdygtighed over for større cybersikkerhedstrusler samt forberede Unionen på og solidarisk afbøde de kortsigtede virkninger af væsentlige og omfattende cybersikkerhedshændelser eller -kriser ("mekanismen").

2. Aktioner til gennemførelse af mekanismen støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

Artikel 10

Foranstaltningstyper

1. Under mekanismen støttes følgende typer foranstaltninger:

a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU

b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser, der leveres af betroede udbydere ***af administrerede sikkerhedstjenester***, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 12

c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555.

1a. Efter udløsningen af mekanismen foretager Kommissionen på årlig basis en vurdering af og offentliggør en rapport om både mekanismens positive og negative funktion, herunder om der er behov for yderligere samarbejde eller uddannelseskrav.

Artikel 11

Koordineret beredskabstest af enheder

1. Med henblik på at støtte den koordinerede beredskabstest af de enheder, der er omhandlet i artikel 10, stk. 1, litra a), i hele Unionen identificerer Kommissionen efter høring af NIS-samarbejdsgruppen og ENISA de berørte sektorer eller delsektorer blandt de sektorer af særlig kritisk betydning, der er anført i bilag I til direktiv (EU) 2022/2555, hvor enheder kan gøres til genstand for koordineret beredskabstest, under hensyntagen til eksisterende og planlagte koordinerede risikovurderinger og prøvning af modstandsdygtighed***, i overensstemmelse med de ordninger, der er fastsat for enheder af den type, der er omhandlet i bilag I om sektorer af særlig kritisk betydning til direktiv (EU) 2022/2555***.

2. NIS-samarbejdsgruppen udarbejder i samarbejde med Kommissionen, ENISA, den højtstående repræsentant ***og de enheder, der gøres til genstand for koordineret beredskabstest i medfør af stk. 1***, fælles risikoscenarier og metoder til gennemførelse af de koordinerede ***beredskabstest, hvilket udmunder i en samordnet arbejdsplan. De enheder, der gøres til genstand for koordineret beredskabstest, udarbejder og gennemfører en afhjælpningsplan til gennemførelse af de anbefalinger, som beredskabstestene giver anledning til.***

NIS-samarbejdsgruppen kan bidrage til prioritering af sektorer eller delsektorer med henblik på den koordinerede beredskabstest.

Artikel 12

Etablering af EU's cybersikkerhedsreserve

1. Der oprettes en EU-cybersikkerhedsreserve med henblik på at bistå de brugere, der er omhandlet i stk. 3, med at reagere på eller yde støtte til at reagere på væsentlige eller omfattende cybersikkerhedshændelser og omgående genopretning efter sådanne hændelser.

Hvis det er åbenbart, at de indkøbte tjenester ikke kan anvendes fuldt ud med henblik på at yde støtte til at reagere på væsentlige eller omfattende cybersikkerhedshændelser, kan disse tjenester undtagelsesvis omdannes til øvelser eller kurser til håndtering af hændelser og af den ordregivende myndighed efter anmodning stilles til rådighed for brugerne.

2. EU's cybersikkerhedsreserve består af hændelsesberedskabstjenester fra betroede udbydere ***af administrerede sikkerhedstjenester***, der er udvalgt i overensstemmelse med kriterierne i artikel 16. ***EU's cybersikkerhedsreserve*** omfatter tjenester omfattet af forhåndsforpligtelser. Tjenesterne kan indsættes i alle medlemsstater ***og skal styrke Unionens teknologiske suverænitet, dens åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed i cybersikkerhedssektoren, herunder ved at fremme innovation på det digitale indre marked i hele Unionen***.

3. Brugere af tjenester fra EU's cybersikkerhedsreserve omfatter:

a) medlemsstaternes cyberkrisestyringsmyndigheder og CSIRT'er som anført i henholdsvis artikel 9, stk. 1 og 2, og artikel 10 i direktiv (EU) 2022/2555

b) EU's institutioner, organer og agenturer ***som omhandlet i artikel 3, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) .../2023[26] og CERT-EU***.

4. Brugerne, som er nævnt i stk. 3, litra a), anvender tjenesterne fra EU's cybersikkerhedsreserve til at reagere på eller støtte indsatsen mod og den omgående genopretning efter væsentlige eller omfattende hændelser, der påvirker enheder, der opererer i kritiske eller meget kritiske sektorer.

5. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen fastlægger prioriteterne for og udviklingen af EU's cybersikkerhedsreserve ***i samarbejde med NIS 2-koordinationsgruppen og*** i overensstemmelse med kravene til de brugere, der er omhandlet i stk. 3, overvåger gennemførelsen og sikrer komplementaritet, sammenhæng, synergi og forbindelser med andre støtteaktioner i henhold til denne forordning samt andre EU-foranstaltninger og -programmer.

6. Kommissionen overdrager helt eller delvist driften og administrationen af EU's cybersikkerhedsreserve til ENISA ved hjælp af bidragsaftaler.

7. For at støtte Kommissionen i etableringen af EU's cybersikkerhedsreserve udarbejder ENISA en kortlægning af de nødvendige tjenester***, herunder de nødvendige færdigheder og den nødvendige kapacitet hos cybersikkerhedspersonalet,*** efter høring af medlemsstaterne og Kommissionen ***og, hvor det er relevant, af udbydere af administrerede sikkerhedstjenester og andre repræsentanter for cybersikkerhedsindustrien***. ENISA udarbejder efter høring af Kommissionen***, udbydere af administrerede sikkerhedstjenester og, hvor det er relevant, andre repræsentanter for cybersikkerhedsindustrien*** en lignende kortlægning for at identificere behovene i de tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve

---

[26] ***Forordning (EU) .../2023 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer (EUT C , , s. , , ELI: ...).***

i henhold til artikel 7. Kommissionen hører, hvor det er relevant, den højtstående repræsentant ***og informerer Rådet om tredjelandes behov***.

8. Kommissionen ***tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 20a med henblik på at supplere denne forordning ved at*** præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. ▌..

Artikel 13

Anmodninger om støtte fra EU's cybersikkerhedsreserve

1. De brugere, der er omhandlet i artikel 12, stk. 3, kan anmode om tjenester fra EU's cybersikkerhedsreserve til støtte for en reaktion på og en øjeblikkelig genopretning efter væsentlige eller omfattende cybersikkerhedshændelser.

2. For at modtage støtte fra EU's cybersikkerhedsreserve træffer de brugere, der er omhandlet i artikel 12, stk. 3, foranstaltninger til at afbøde virkningerne af den hændelse, der er årsag til anmodningen om støtte, herunder ydelse af direkte teknisk bistand og andre ressourcer som en del af reaktionen på hændelsen og den omgående genopretningsindsats.

3. Anmodninger om støtte fra de brugere, der er omhandlet i denne forordnings artikel 12, stk. 3, litra a), sendes til Kommissionen og ENISA via det centrale kontaktpunkt, der er udpeget eller oprettet af medlemsstaten i overensstemmelse med artikel 8, stk. 3, i direktiv (EU) 2022/2555.

4. Medlemsstaterne underretter CSIRT-netværket og, hvor det er relevant, EU-CyCLONe om deres anmodninger om støtte til reaktioner på hændelser og omgående genopretning i henhold til denne artikel.

5. Anmodninger om støtte til reaktioner på hændelser og omgående genopretning omfatter:

a) relevante oplysninger om den berørte enhed og mulige virkninger af hændelsen samt den planlagte anvendelse af den støtte, der anmodes om, herunder en angivelse af de anslåede behov

b) oplysninger om foranstaltninger, der er truffet for at afbøde den hændelse, der er årsag til anmodningen om støtte, jf. stk. 2

c) oplysninger om andre former for støtte, der er til rådighed for den berørte enhed, herunder indgåede kontrakter vedrørende reaktioner på hændelser og tjenester til omgående genopretning, samt forsikringsaftaler, der muligvis dækker hændelsestypen.

6. ENISA udarbejder i samarbejde med Kommissionen og NIS-samarbejdsgruppen en skabelon for at lette indgivelsen af anmodninger om støtte fra EU's cybersikkerhedsreserve.

7. Kommissionen ***tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 20a med henblik på at supplere denne forordning ved yderligere at*** præcisere de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve. ▌

Artikel 14

Gennemførelse af støtte fra EU's cybersikkerhedsreserve

1. Anmodninger om støtte fra EU's cybersikkerhedsreserve vurderes af Kommissionen med støtte fra ENISA eller som defineret i bidragsaftaler i henhold til artikel 12, stk. 6, og et svar sendes ***uden unødig forsinkelse og under alle omstændigheder inden for 24 timer*** til de brugere, der er omhandlet i artikel 12, stk. 3.

2. Hvis flere anmodninger indgives samtidig, skal der ved prioritering heraf tages hensyn til følgende kriterier, hvor det er relevant:

a) alvorligheden af cybersikkerhedshændelsen

b) typen af berørt enhed, idet der gives højere prioritet til hændelser, der påvirker væsentlige enheder som defineret i artikel 3, stk. 1, i direktiv (EU) 2022/2555

c) mulig indvirkning på den eller de berørte medlemsstater eller brugere

d) hændelsens ***omfang og*** mulige grænseoverskridende karakter og risikoen for afledte effekter for andre medlemsstater eller brugere

e) foranstaltninger truffet af brugeren for at medvirke til reaktionen herpå og den umiddelbare genopretningsindsats, jf. artikel 13, stk. 2, og artikel 13, stk. 5, litra b).

3. Tjenesterne under EU's cybersikkerhedsreserve leveres i overensstemmelse med særaftaler mellem tjenesteudbyderen og den bruger, som støtten under EU's cybersikkerhedsreserve ydes til. Aftalerne skal indeholde ansvarsbetingelser ***og andre bestemmelser, som aftalens parter skønner nødvendige for leveringen af den pågældende tjeneste***.

4. De i stk. 3 omhandlede aftaler baseres på skabeloner udarbejdet af ENISA efter høring af medlemsstaterne ***og, hvor det er relevant, andre brugere af EU's cybersikkerhedsreserve***.

5. Kommissionen og ENISA bærer intet kontraktligt ansvar for skader påført tredjepart som følge af de tjenester, der leveres inden for rammerne af gennemførelsen af EU's cybersikkerhedsreserve***, undtagen i tilfælde af grov uagtsomhed i evalueringen af tjenesteudbyderens anvendelse eller i tilfælde, hvor Kommissionen eller ENISA er brugere af EU's cybersikkerhedsreserve i henhold til artikel 14, stk. 3***.

6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen og ENISA***, CSIRT-netværket og, hvor det er relevant, EU-CyCLONe*** en sammenfattende rapport om den leverede tjeneste, de opnåede resultater og de indhøstede erfaringer. Når brugeren er fra et tredjeland, jf. artikel 17, videresendes rapporten til den højtstående repræsentant.
Rapporten skal overholde EU-retten og national ret vedrørende beskyttelse af følsomme eller klassificerede informationer.

7. Kommissionen aflægger regelmæssigt ***og mindst to gange om året*** rapport til NIS-samarbejdsgruppen om anvendelsen og resultaterne af støtten. ***Fortrolige oplysninger beskyttes i overensstemmelse med EU-retten og national ret vedrørende beskyttelse af følsomme eller klassificerede informationer.***

Artikel 15

Koordinering med krisestyringsmekanismer

1. I tilfælde, hvor væsentlige eller omfattende cybersikkerhedshændelser skyldes eller resulterer i katastrofer som defineret i afgørelse 1313/2013/EU[27], supplerer støtten til reaktioner på sådanne hændelser i henhold til denne forordning foranstaltninger i henhold til afgørelse 1313/2013/EU uden at berøre denne afgørelse.

2. I tilfælde af en omfattende, grænseoverskridende cybersikkerhedshændelse, hvor integrerede ordninger for politisk kriserespons (IPCR) udløses, skal støtten i henhold til denne forordning til at reagere på en sådan hændelse håndteres i overensstemmelse med de relevante protokoller og procedurer i henhold til IPCR.

3. I samråd med den højtstående repræsentant kan støtte under beredskabsmekanismen ***for cybersikkerhed*** supplere den bistand, der ydes inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik, herunder gennem cyberberedskabsholdene. Den kan også supplere eller bidrage til den bistand, som en medlemsstat yder til en anden medlemsstat inden for rammerne af artikel 42, stk. 7, i ***TEU***.

4. Støtte under beredskabsmekanismen ***for cybersikkerhed*** kan indgå i den fælles indsats mellem Unionen og medlemsstaterne i de situationer, der er omhandlet i artikel 222 i ***TEUF***.

Artikel 16

Betroede udbydere

1. I forbindelse med udbudsprocedurer med henblik på etablering af EU's cybersikkerhedsreserve handler den ordregivende myndighed i overensstemmelse med principperne i forordning (EU, Euratom) 2018/1046 og i overensstemmelse med følgende principper:

a) sikre, at EU's cybersikkerhedsreserve omfatter tjenester, der kan udrulles i alle medlemsstater, idet der navnlig tages hensyn til nationale krav til levering af sådanne tjenester, herunder certificering eller akkreditering

b) sikre beskyttelse af Unionens og dens medlemsstaters væsentlige sikkerhedsinteresser

c) sikre, at EU's cybersikkerhedsreserve skaber merværdi for EU ved at bidrage til de målsætninger, der er fastsat i artikel 3 i forordning (EU) 2021/694, herunder ved at fremme udviklingen af cybersikkerhedsfærdigheder i EU ***og opnåelsen af kønsbalance i sektoren og styrke Unionens teknologiske suverænitet, åbne strategiske autonomi, konkurrenceevne og modstandsdygtighed***.

2. Ved indkøb af tjenesteydelser til EU's cybersikkerhedsreserve medtager den ordregivende myndighed følgende udvælgelseskriterier i udbudsdokumenterne:

a) udbyderen skal påvise, at personalet har den højeste grad af faglig integritet, selvstændighed og ansvar samt den nødvendige tekniske kompetence til at udføre aktiviteterne inden for de specifikke områder, og udbyderen skal sikre, at ekspertisen samt de nødvendige tekniske ressourcer er permanent til rådighed uden afbrydelse

b) udbyderen og dennes datterselskaber og underleverandører skal have indført en ramme til beskyttelse af følsomme oplysninger vedrørende tjenesten, navnlig dokumentation,

[27] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

undersøgelser og rapporter, og arbejde i overensstemmelse med Unionens sikkerhedsregler om beskyttelse af EU's klassificerede informationer

c) udbyderen skal fremlægge tilstrækkelig dokumentation for en transparent ledelsesstruktur, hvor der ikke er sandsynlighed for, at upartiskheden og kvaliteten af tjenesterne kan anfægtes eller interessekonflikter opstå

d) udbyderen skal have en passende sikkerhedsgodkendelse, i det mindste for personale, der arbejder med udrulning af tjenesterne

e) udbyderens IT-systemer skal være sikret med et relevant sikkerhedsniveau

f) udbyderen skal være udstyret med den nødvendige ***opdaterede*** hardware og software til at understøtte den ønskede tjeneste ***og skal, såfremt det er relevant, overholde Europa-Parlamentets og Rådets forordning EU .../...[28] (2022/0272(COD))***

g) udbyderen skal kunne dokumentere erfaring med at levere lignende tjenester til relevante nationale myndigheder eller enheder, der opererer i kritiske eller meget kritiske sektorer

h) udbyderen skal være i stand til at levere tjenesten hurtigt i den eller de medlemsstater, hvor udbyderen kan levere tjenesten

i) udbyderen skal kunne levere tjenesten på det lokale sprog i den eller de medlemsstater, hvor udbyderen kan levere tjenesten***, eller på et af EU-institutionernes arbejdssprog***

j) når en ***europæisk cybersikkerhedscertificeringsordning*** for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning ***inden for en periode på to år, efter at ordningen er vedtaget***

ja) udbyderen skal kunne levere tjenesten uafhængigt og ikke som en del af en pakke for at sikre brugerens mulighed for at skifte til en anden tjenesteudbyder

jb) med henblik på artikel 12, stk. 1, skal udbyderen i forslaget til tilbud medtage muligheden for at omdanne ubrugte hændelsesberedskabstjenester til øvelser eller kurser

jc) udbyderen skal være etableret og have sine ledelsesstrukturer i Unionen, i et associeret land eller i et tredjeland, der indgår i aftalen om offentlige udbud (GPA) inden for rammerne af Verdenshandelsorganisationen.

jd) . udbyderen må ikke være underlagt kontrol af et ikkeassocieret tredjeland eller en enhed i et ikkeassocieret tredjeland, der ikke indgår i GPA-aftalen, eller alternativt skal en sådan enhed have været underlagt screening i den i forordning (EU) 2019/452 anvendte betydning og, om fornødent, afbødende foranstaltninger, under hensyntagen til målene, som er omhandlet i nærværende forordning.

Artikel 17

Støtte til tredjelande

---

[28] Europa-Parlamentets og Rådets forordning (EU) .../... af ... om (EUT L, …, ELI: …).

1. Tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom.

2. Støtte fra EU's cybersikkerhedsreserve er i overensstemmelse med denne forordning og opfylder eventuelle specifikke betingelser, der er fastsat i de associeringsaftaler, der er omhandlet i stk. 1.

3. Brugere fra associerede tredjelande, der er berettigede til levering af tjenester fra EU's cybersikkerhedsreserve, omfatter kompetente myndigheder såsom CSIRT'er og cyberkrisestyringsmyndigheder.

4. Tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve, udpeger en myndighed, der skal fungere som et centralt kontaktpunkt med henblik på denne forordning.

5. Forud for modtagelse af støtte fra EU's cybersikkerhedsreserve forelægger tredjelande Kommissionen og den højtstående repræsentant oplysninger om deres cyberrobusthed og risikostyringskapacitet, herunder som minimum oplysninger om nationale foranstaltninger, der er truffet for at forberede sig på væsentlige eller omfattende cybersikkerhedshændelser, samt oplysninger om ansvarlige nationale enheder, herunder CSIRT'er eller tilsvarende enheder, deres kapaciteter og de ressourcer, de har fået tildelt. Når bestemmelserne i artikel 13 og 14 i denne forordning henviser til medlemsstaterne, finder de anvendelse på tredjelande som fastsat i stk. 1.

6. Kommissionen ***underretter uden unødig forsinkelse Rådet og*** koordinerer behandlingen af de modtagne anmodninger med den højtstående repræsentant og gennemførelsen af den støtte, der ydes til tredjelande fra EU's cybersikkerhedsreserve.

Kapitel IV

MEKANISME TIL GENNEMGANG AF CYBERSIKKERHEDSHÆNDELSER

Artikel 18

Mekanisme til gennemgang af cybersikkerhedshændelser

1. Efter anmodning fra Kommissionen, EU-CyCLONe eller CSIRT-netværket gennemgår og vurderer ENISA trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. Efter afsluttet gennemgang og vurdering af en hændelse fremsender ENISA en rapport om hændelsen til CSIRT-netværket, EU-CyCLONe og Kommissionen som støtte til udførelsen af deres opgaver, navnlig opgaver i henhold til artikel 15 og 16 i direktiv (EU) 2022/2555. Hvis det er relevant, videresender Kommissionen rapporten med den højtstående repræsentant.

2. Ved udarbejdelse af den i stk. 1 omhandlede rapport om gennemgang af en hændelse samarbejder ENISA ***med og indsamler feedback fra*** alle relevante interessenter, herunder repræsentanter for medlemsstaterne, Kommissionen, andre relevante EU-institutioner, -organer***, -kontorer*** og -agenturer, udbydere af administrerede sikkerhedstjenester i ***nationale og grænseoverskridende SOC'er*** og brugere af cybersikkerhedstjenester***, hvilket suppleres med garantier og overvågning, der er tilstrækkelig til at sikre, at de indhøstede erfaringer og***

udpegede bedste praksisser støttes af aktørerne i branchen for cybersikkerhedstjenester. Hvor det er relevant, samarbejder ENISA også med enheder, der er berørt af væsentlige eller omfattende cybersikkerhedshændelser. Som støtte for gennemgangen kan ENISA også høre andre typer interessenter. De hørte repræsentanter skal oplyse om eventuelle interessekonflikter.

3. Rapporten omfatter en gennemgang og analyse af den specifikke væsentlige eller omfattende cybersikkerhedshændelse, herunder de vigtigste årsager, sårbarheder og indhøstede erfaringer. Fortrolige oplysninger beskyttes i overensstemmelse med EU-retten eller national ret vedrørende beskyttelse af følsomme eller klassificerede informationer. ***Den må ikke indeholde oplysninger om aktivt udnyttede sårbarheder, der ikke er blevet udbedret.***

3a. Den rapport, der er omhandlet i stk. 1 i denne artikel, skal indeholde erfaringerne fra de peerevalueringer, der gennemføres i henhold til artikel 19 i direktiv (EU) 2022/2555.

4. Rapporten skal, hvor det er relevant, indeholde anbefalinger***, herunder til alle relevante interessenter,*** til forbedring af Unionens cyberposition.

5. Hvis det er muligt, offentliggøres en udgave af rapporten. Denne udgave indeholder kun de oplysninger, der kan offentliggøres.

Kapitel V

AFSLUTTENDE BESTEMMELSER

Artikel 19

Ændringer af forordning (EU) 2021/694

I forordning (EU) 2021/694 foretages følgende ændringer:

1) Artikel 6 ændres således:

a) Stk. 1 ændres således:

i) Følgende indsættes som litra aa):

"aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af nationale og grænseoverskridende SOC-platforme, der bidrager til et øget situationskendskab i Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler".

ii) Følgende tilføjes som litra g):

"g) etablere og drive en beredskabsmekanisme ***for cybersikkerhed*** for at hjælpe medlemsstaterne med at forberede sig og reagere på væsentlige cybersikkerhedshændelser som supplement til nationale ressourcer og kapaciteter og andre former for støtte, der er til rådighed på EU-plan, herunder etablering af en EU-cybersikkerhedsreserve".

b) Stk. 2 affattes således:

"2. Foranstaltningerne under specifikt mål nr. 3 gennemføres primært gennem det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/887* med undtagelse af foranstaltninger til gennemførelse af EU's cybersikkerhedsreserve, som gennemføres af Kommissionen og ENISA."

_____

* Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1), ***ELI: https://eur-lex.europa.eu/eli/reg/2021/887/oj?locale=da).".***

2) Artikel 9 ændres således:

a) Stk. 2, litra b), c) og d), affattes således:

"b), 1 776 956 000 EUR til specifikt mål nr. 2 – Kunstig intelligens

c), ***1 620 566 000*** EUR til specifikt mål nr. 3 – Cybersikkerhed og tillid

d), ***500 347 000*** EUR til specifikt mål nr. 4 – Højtudviklede digitale færdigheder"

aa) Følgende nye stk. 2a indsættes:

" 2a). Det beløb, der er omhandlet i stk. 2, litra c), anvendes primært til at opfylde de operationelle mål, der er omhandlet i programmets artikel 6, stk. 1, litra a-f)."

ab) Følgende nye stk. 2b indsættes:

" 2b). Det beløb, der anvendes til etablering og gennemførelse af EU's cybersikkerhedsreserve, må ikke overstige 27 mio. EUR i løbet af den planlagte gyldighedsperiode for forordningen om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser."

b) Følgende tilføjes som stk. 8:

"8. Uanset artikel 12, stk. 4, i forordning (EU, Euratom) 2018/1046 overføres uudnyttede forpligtelses- og betalingsbevillinger ***vedrørende gennemførelsen af EU's cybersikkerhedsreserve*** til foranstaltninger, der forfølger de mål, der er fastsat i nærværende forordnings artikel 6, stk. 1, litra g), automatisk, og der kan indgås forpligtelser og betales frem til den 31. december i det følgende regnskabsår."

Kommissionen underretter Parlamentet og Rådet om bevillinger, der overføres i overensstemmelse med artikel 12, stk. 6, i forordning (EU, Euratom) 2018/1046.

3) Artikel 14, stk. 2, affattes således:

"2. Programmet kan yde finansiering i enhver af de former, der er fastsat i forordning ***(EU, Euratom) 2018/1046***, herunder navnlig gennem udbud som den primære form eller tilskud og priser.

Hvor det er nødvendigt at indkøbe innovative varer og tjenester for at opfylde målsætningen for en foranstaltning, må der kun ydes tilskud til støttemodtagere, der er ordregivende myndigheder eller ordregivende enheder som defineret i Europa-Parlamentets og Rådets direktiv 2014/24/EU [27] og 2014/25/EU [28].

Hvor levering af innovative varer eller tjenester, som endnu ikke er kommercielt tilgængelige i stor skala, er nødvendig for at opfylde målsætningen for en foranstaltning, kan den ordregivende myndighed eller den ordregivende enhed godkende tildelingen af flere kontrakter inden for samme udbudsprocedure.

Ud fra behørigt begrundede hensyn til den offentlige sikkerhed kan den ordregivende myndighed eller den ordregivende enhed kræve, at kontraktens opfyldelsessted skal være inden for Unionens område.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, der er oprettet ved artikel 12 i forordning (EU) 2023//**…**, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af tredjelande, der er associeret til programmet, jf. artikel 10. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til disse tredjelande. Uanset artikel 169, stk. 3, i forordning (EU) **…/…** er en anmodning fra et enkelt tredjeland tilstrækkelig til at give Kommissionen eller ENISA mandat til at handle.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, der etableres ved artikel 12 i forordning (EU) 2023/**…**, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af EU's institutioner, organer og agenturer. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til EU's institutioner, organer og agenturer. Uanset artikel 169, stk. 3, i forordning (EU)**…/…** er en anmodning fra en enkelt EU-institution, et enkelt EU-organ eller et enkelt EU-agentur tilstrækkelig til at give Kommissionen eller ENISA mandat til at handle.

Programmet kan også tilvejebringe finansiering i form af finansielle instrumenter inden for blandingsoperationer. ";

4) Følgende tilføjes som artikel 16a:

"***Artikel 16a***

For så vidt angår foranstaltninger til gennemførelse af det europæiske cyberskjold, der er oprettet ved artikel 3 i forordning (EU) 2023/XX, er reglerne fastsat i artikel 4 og 5 i forordning (EU) 2023/**…**. I tilfælde af konflikt mellem bestemmelserne i denne forordning

og artikel 4 og 5 i forordning (EU) 2023/**…** har sidstnævnte forrang og finder anvendelse på disse specifikke foranstaltninger***."***

5) Artikel 19 affattes således:

"Tilskud i henhold til programmet tildeles og forvaltes i overensstemmelse med afsnit VIII i ***forordning (EU, Euratom) 2018/1046*** og kan dække op til 100 % af de støtteberettigede omkostninger, uden at dette berører artikel 190 i ***forordning (EU, Euratom) 2018/1046***. Sådanne tilskud tildeles og forvaltes som nærmere angivet for hvert specifikt mål.

Støtte i form af tilskud kan ydes direkte af ECCC uden forslagsindkaldelse til de nationale SOC'er, der er omhandlet i artikel 4 i forordning ***(EU) .../...***, og værtskonsortiet, der er omhandlet i artikel 5 i forordning ***(EU) .../...***, i overensstemmelse med artikel 195, stk. 1, litra d) i ***forordning (EU, Euratom) 2018/1046***.

Støtte i form af tilskud til beredskabsmekanismen ***for cybersikkerhed***, jf. artikel 10 i forordning ***(EU) .../...***, kan tildeles direkte af ECCC til medlemsstaterne uden forslagsindkaldelse i overensstemmelse med artikel 195, stk. 1, litra d) i ***forordning (EU, Euratom) 2018/1046***.

For så vidt angår foranstaltninger omhandlet i artikel 10, stk. 1, litra c), i forordning ***(EU) .../...*** underretter ECCC Kommissionen og ENISA om medlemsstaternes anmodninger om direkte tilskud uden indkaldelse af forslag.

Med henblik på støtte til gensidig bistand til en reaktion på en væsentlig eller omfattende cybersikkerhedshændelse som defineret i artikel 10, litra c), i forordning ***(EU) .../...*** og i overensstemmelse med artikel 193, stk. 2, andet afsnit, litra a) i ***forordning (EU, Euratom) 2018/1046***, kan omkostningerne i behørigt begrundede tilfælde betragtes som støtteberettigede, selv om de blev afholdt, inden ansøgningen om tilskud blev indgivet."

6) Bilag I og II til forordning (EU) 2021/694 ændres som anført i bilaget til denne forordning.

Artikel 19a
Yderligere ressourcer til ENISA

ENISA modtager yderligere ressourcer til at udføre de yderligere opgaver, det er pålagt i henhold til denne forordning Denne yderligere støtte, herunder finansiering, må ikke sætte opfyldelsen af andre EU-programmers mål over styr, navnlig programmet for et digitalt Europa.

Artikel 20

Evaluering ***og revision***

1. Senest [***to*** år efter datoen for denne forordnings anvendelse] ***og derefter hvert andet år foretager*** Kommissionen ***en*** evaluering ***af, hvordan foranstaltningerne i denne forordning fungerer***, ***og forelægger en rapport for*** Europa-Parlamentet og Rådet.

2. Ved evalueringen vurderes navnlig følgende:

a) anvendelsen og merværdien af de grænseoverskridende SOC'er, og i hvilket omfang de bidrager til hurtigere opdagelse af og reaktion på cybertrusler og større situationskendskab; de nationale SOC'ers aktive deltagelse i det europæiske cyberskjold, herunder antallet af etablerede nationale SOC'er og grænseoverskridende SOC'er, og i hvilket omfang dette har bidraget til tilvejebringelse og udveksling af anvendelige oplysninger af høj kvalitet og efterretninger om cybertrusler; antallet af og omkostningerne ved cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er indkøbt i fællesskab; antallet af samarbejdsaftaler indgået mellem grænseoverskridende SOC'er og med ISAC'er i industrien; antallet af indberettede hændelser til CSIRT-netværket og deres indvirkning på CSIRT-netværkets arbejde

b) både den positive og negative funktion af beredskabsmekanismen for cybersikkerhed, herunder om der er behov for yderligere samarbejde eller uddannelseskrav

c) denne forordnings bidrag til at styrke Unionens modstandsdygtighed og åbne strategiske autonomi, forbedre de relevante industrisektorers, mikrovirksomheders og SMV'ers, herunder nystartede virksomheders, konkurrenceevne og udvikle cybersikkerhedsfærdigheder i EU

d) anvendelsen og merværdien af EU's cybersikkerhedsreserve, herunder antallet af betroede sikkerhedsudbydere, der er en del af EU's cybersikkerhedsreserve; antallet, typen og virkningen af samt omkostningerne ved de foranstaltninger, der er gennemført til støtte for reaktion på cybersikkerhedshændelser, samt deres brugere og udbydere; den tid, det gennemsnitligt tager for Kommissionen at erkende, at der foreligger en hændelse, for EU's cybersikkerhedsreserve at blive taget i brug og reagere og for brugeren at komme sig efter hændelser; hvorvidt anvendelsesområdet for cybersikkerhedsreserven om nødvendigt bør udvides til hændelsesberedskabstjenester eller fælles øvelser med de betroede udbydere af administrerede sikkerhedstjenester og potentielle brugere af EU's cybersikkerhedsreserve for at sikre, at EU's cybersikkerhedsreserve fungerer effektivt

e) denne forordnings bidrag til udvikling og forbedring af cybersikkerhedssektorens arbejdsstyrkes færdigheder og kompetencer, der er nødvendige for at styrke Unionens

kapacitet til at opdage, forebygge, reagere på og komme sig efter cybersikkerhedstrusler og -hændelser

f) denne forordnings bidrag til udbredelsen og udviklingen af de nyeste teknologier i Unionen.

3. På grundlag af de rapporter, der er omhandlet i stk. 1, forelægger Kommissionen i givet fald Europa-Parlamentet og Rådet et lovgivningsforslag om ændring af denne forordning.

Artikel 20a

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 6, stk. 3, artikel 7, stk. 2, artikel 12, stk. 8 og artikel 13, stk. 7, tillægges Kommissionen for en periode på ... år fra den … [datoen for den lovgivningsmæssige basisretsakts ikrafttræden eller enhver anden dato fastsat af medlovgiverne]. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af ...årsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 6, stk. 3, artikel 7, stk. 2, artikel 12, stk. 8, og artikel 13, stk. 7, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 6, stk. 3, artikel 7, stk. 2, artikel 12, stk. 8, eller artikel 13, stk. 7, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende

retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med [to måneder] på Europa-Parlamentets eller Rådets initiativ.

Artikel 21

Udvalgsprocedure

1. Kommissionen bistås af Koordinationsudvalget for Programmet for et Digitalt Europa, der er nedsat i medfør af forordning (EU) 2021/694. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.
2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

Artikel 22

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Strasbourg, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

BILAG

I forordning (EU) 2021/694 foretages følgende ændringer:

(1) I bilag I affattes afsnittet/kapitlet "Specifikt mål nr. 3 – Cybersikkerhed og tillid" således:

"Specifikt mål nr. 3 – Cybersikkerhed og tillid

Programmet skal fremme styrkelse, opbygning og erhvervelse af afgørende kapacitet til at sikre Unionens digitale økonomi, samfund og demokrati ved at styrke Unionens industrielle potentiale og konkurrenceevne inden for cybersikkerhed samt ved at forbedre både den private og den offentlige sektors kapacitet til at beskytte borgere og virksomheder mod cybertrusler, herunder ved at understøtte gennemførelsen af direktiv (EU) 2016/1148.

De indledende og, hvor det er relevant, efterfølgende tiltag under dette mål omfatter:

1. Investeringer i fællesskab med medlemsstaterne i højtudviklet cybersikkerhedsudstyr, -infrastruktur og -knowhow, som er afgørende for beskyttelsen af kritiske infrastrukturer og det digitale indre marked generelt. Sådanne fælles investeringer kan omfatte investeringer i kvantefaciliteter og dataressourcer til cybersikkerhed, situationskendskab vedrørende cyberspace, ***herunder nationale SOC'er og grænseoverskridende SOC'er, der udgør det europæiske cyberskjold***, samt andre værktøjer, som skal gøres tilgængelige for offentlige og private sektorer i hele Europa.

2. Opskalering af eksisterende teknologisk kapacitet og netværkssamarbejde mellem kompetencecentrene i medlemsstaterne, idet det sikres, at nævnte kapacitet opfylder den offentlige sektors og industriens behov, herunder gennem produkter og tjenester, som styrker cybersikkerhed og tillid inden for det digitale indre marked.

3. Sikring af en bred udrulning af effektive, avancerede cybersikkerheds- og tillidsløsninger i alle medlemsstater. En sådan udrulning omfatter styrkelse af produkters sikkerhed fra udformning til kommercialisering af dem.

4. Støtte til at slå bro over færdighedskløften inden for cybersikkerhed ***med særligt fokus på at opnå kønsbalance i sektoren ved*** f.eks. at ensrette programmerne for cybersikkerhedsfærdigheder, tilpasse dem til specifikke sektorbehov***, herunder et tværfagligt og generelt fokus,*** og lette adgangen til målrettet specialiseret uddannelse ***for alle borgere i alle områder, uden at dette berører deres mulighed for at drage fordel af de muligheder, som denne forordning giver.***

5. Fremme af solidaritet mellem medlemsstaterne i forbindelse med beredskab og indsats ved væsentlige cybersikkerhedshændelser gennem udrulning af cybersikkerhedstjenester på tværs af grænserne, herunder støtte til gensidig bistand mellem offentlige myndigheder og etablering af en reserve af betroede udbydere af ***administrerede sikkerhedstjenester*** på EU-plan."

(2) I bilag II affattes afsnittet/kapitlet "Specifikt mål nr. 3 – Cybersikkerhed og tillid" således:

"Specifikt mål nr. 3 – Cybersikkerhed og tillid

3.1. Antallet af cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er indkøbt i fællesskab ***som led i cybersikkerhedsskjoldet.***

3.2. Antal brugere og brugersamfund, som får adgang til europæiske cybersikkerhedsfaciliteter

3.3. ***Antallet, typen og virkningen af samt omkostningerne ved de*** foranstaltninger***, der er gennemført*** til støtte for beredskab og reaktion på cybersikkerhedshændelser inden for rammerne af beredskabsmekanismen ***for cybersikkerhed***. ***I hvilket omfang anbefalingerne fra beredskabstestningen er blevet iværksat og gennemført af brugeren, og den gennemsnitstid, det tager Kommissionen at anerkende, at der foreligger en hændelse, EU's cybersikkerhedsreserve at reagere og brugeren at komme på fode igen efter hændelser."***

BEGRUNDELSE

BAGGRUND

Cybersikkerhed er og bør være i kernen i vores demokratier. Trusler mod cybersikkerheden hænger sammen med en øget usikkerhed i befolkningen og hos virksomhederne samt en stigning i omfanget af desinformation, hvilket udfordrer de demokratiske principper, der sikrer respekt for menneskerettighederne. For at forhindre dette er et sikkert digitalt miljø, der er underlagt offentlig kontrol, afgørende for vores demokratier.

Cyberangreb i EU er stigende både med hensyn til fremgangsmåder og virkninger. Desuden har det russiske angreb på Ukraine skabt gennemgribende ændringer, selv før invasionen, og har åbnet en ny æra for **cyberprodukter** ifølge ENISA's rapport fra 2022 om trusselbilledet[1]. De prioriteter, der er identificeret som følge af denne cyberkonflikt, er behovet for at **opbygge kapacitet** i **multilaterale programmer** og projekter og behovet for hurtigt at **udvikle færdigheder**. For at blive mere modstandsdygtig er der et presserende behov for en fælles europæisk reaktion baseret på et stærkere samarbejde på europæisk plan, der rækker ud over det nationale plan.

En styrkelse af cybersikkerhedskulturen, der omfatter sikkerhed, herunder i det digitale miljø, som et offentligt gode, vil være afgørende for en vellykket gennemførelse af denne forordning.

Desuden er cyberangreb ofte rettet mod **lokale, regionale eller nationale offentlige tjenester** og infrastrukturer (f.eks. sundhedssektoren, der fortsat er et af de primære mål for cyberangreb[2]). Der er også dokumentation for, at **lokale myndigheder** er blandt de mest sårbare mål på grund af manglen på finansielle og menneskelige ressourcer, og at det er særlig vigtigt, at ledere på lokalt plan bliver bevidste om behovet for at øge den digitale modstandsdygtighed[3]. Angreb påvirker primært og direkte borgerne og bringer dermed vores demokratier i fare, herunder gennem desinformationskampagner. Den følelse af usikkerhed, som disse situationer kan skabe i befolkningen, kan føre til politiske valg, der forfølger en radikal forpligtelse til sikkerhed på bekostning af respekten for de grundlæggende rettigheder. Men det er det modsatte, der er nødvendigt: Sikkerhed er en hjørnesten i vores demokratier og er forenelig med og nødvendig for alle andre rettigheder.

Desuden oplever **virksomheder og SMV'er** i EU også cyberkriminalitet, og med den stigende brug af den digitale sfære til at drive virksomhed er der større bekymring med hensyn til cybersikkerhed. SMV'er er mindst forberedte, idet de har færre ressourcer til at beskytte sig selv, og de er også mindre bevidste om, at de kan blive udsat for sådanne angreb.

Det forventes, at denne slags angreb vil fortsætte og stige i fremtiden. Navnlig i situationer

---

[1] ENISA, "Threat Landscape 2022", oktober 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[2] ENISA, "Threat Landscape: Health Sector", juli 2023, https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[3] Det Europæiske Regionsudvalg: "Digital Resilience", 2023, https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

med politisk ustabilitet og mere specifikt i forbindelse med krig. Med den digitale omstilling, der hver dag skrider fremad, bliver digital modstandsdygtighed stadig vigtigere for vores dagligdag og for **EU's åbne strategiske autonomi.**

ORDFØRERENS FORSLAG

Ordføreren mener, at EU skal være bedre forberedt på fremtiden, og glæder sig over denne presserende retsakt med henblik på at samle ressourcer, information og viden for at sikre solidaritet mellem medlemsstaterne, øge den industrielle kapacitet i EU**, på en koordineret måde** udvikle **færdigheder og kapaciteter**, der sikrer cybersikkerhed, og for at blive mere modstandsdygtig over for fremtidige angreb og beskytte vores demokratier mod egennyttig udnyttelse af sikkerhedsbehov. Desuden er det vigtigt at beskytte integriteten af vores valgprocesser. Denne retsakt er et vigtigt tilsagn om at nå målet om **åben strategisk autonomi**.

Derfor har EU brug for en stærk og **koordineret styring** og et struktureret samarbejde med den private sektor for at fremme udviklingen af den europæiske cyberindustri. Ud over at samarbejde med ligesindede internationale partnere er der også behov for at samarbejde med andre lande, der ikke har de samme kapaciteter og kan have behov for bistand, når de udsættes for cyberangreb. EU's cybersolidaritetsinitiativ skal sikre en klar forvaltningsdefinition og må ikke overlappe med allerede eksisterende initiativer og lovgivning såsom NIS 2-direktivet.

Forslaget er i høj grad baseret på frivillig udveksling af oplysninger mellem medlemsstaterne. Ordføreren foreslår derfor at styrke garantierne for at opbygge tillid blandt medlemsstaterne, så de øger deres deltagelse og samarbejde, f.eks. med hensyn til fælles erhvervelse af infrastruktur og inddragelse af de lovgivende instanser, for at sikre borgernes tillid og **demokratiske garantier**.

For det andet foreslår ordføreren at **sikre budgettet** fra de kommende FFR'er til dette initiativ, også med tilsagn fra medlemsstaterne, for at sikre kontinuitet i de aktiviteter, der udvikles under EU's cybersolidaritetsinitiativ efter 2027.

For det tredje foreslår ordføreren at forbedre **forvaltningsstrukturen**, at få en klar definition af forvaltning og at knytte den sammen med eksisterende lovgivning.

Ordføreren foreslår også en bedre **koordinering** mellem medlemsstaternes forskellige enheder med ansvar for cybersikkerhed for at sikre et fælles cyberskjold. Desuden foreslås det at øge ENISA's bidrag til koordinering og interaktion mellem de forskellige aktører i medlemsstaterne.

Med hensyn til den **nye cybersikkerhedsreserve** mener ordføreren, at den har potentiale til at udvikle EU's industrielle kapacitet, herunder for SMV'er, gennem investeringer i forskning og innovation med henblik på at udvikle de mest avancerede teknologier, bl.a. cloudteknologier og kunstig intelligens. Ordføreren foreslår ligeledes at fastholde industriens deltagelse, styrke kriterierne for og tilliden til deres deltagelse (dvs. forbinde deres deltagelse med en national eller lokal virksomhed) ved at præcisere **betingelserne** for og definitionen af **teknologisk suverænitet** og sikre en balance mellem aktører fra ikke-EU-lande og EU-lande. Desuden foreslår ordføreren en **certificeringsordning** for **cyberberedskabsmekanismen**, der skal

anvendes i forbindelse med private udbydere med henblik på at opbygge et mangeårigt og pålideligt partnerskab.

Med hensyn til **mekanismen til gennemgang af hændelser** foreslår ordføreren at styrke ENISA's og den private sektors rolle i SOC'erne med de rette garantier og overvågning for at kontrollere, om de indhøstede erfaringer også støttes af aktørerne i industrien. Ordføreren foreslår at medtage erfaringerne fra de peerevalueringer, der foretages i henhold til NIS 2-direktivet og øge ENISA's finansiering med henblik på at sikre en effektiv anvendelse af lovgivningen og tilstrækkelig beskyttelse til at imødegå cybersikkerhedstrusler.

Derudover har dette forslag pr. definition en meget relevant **ekstern dimension**, eftersom tredjelande kan få adgang til ressourcer og støtte fra EU's cybersolidaritetsinitiativ gennem støtten til reaktioner på hændelser fra EU's cybersikkerhedsreserve, og der er stadig behov for aktører til cyberreserven fra den private sektor i tredjelande. Den eksterne dimension skal også være underlagt offentlig kontrol med deltagelse af de lovgivende myndigheder for at sikre, at borgerne kan deltage i processen. Cybersikkerhed bør betragtes som et offentligt gode.

En central søjle i dette forslag er desuden udviklingen af færdigheder og kompetencer, der bør gå videre end blot at investere i videnudvikling, men investere i adgang for alle borgere, så de kan uddanne sig i disse færdigheder. Ordføreren foreslår at styrke forbindelsen til **EU-akademiet for cyberfærdigheder**, som har til formål at lukke talentkløften inden for cybersikkerhed ved at samle private og offentlige initiativer og tilbyde uddannelse og certificering til borgerne. Den styrkede forbindelse kræver sikkerhedsforanstaltninger for at undgå hjerneflugt og må ikke være til skade for arbejdskraftens mobilitet.

Desuden foreslår ordføreren at investere i og medtage aktive foranstaltninger til udvikling af færdigheder i denne sektor i betragtning af, at 2023 er det europæiske år for færdigheder, samt at øge borgernes bevidsthed. Foranstaltningerne vil blive udformet således, at investeringer ikke skaber ubalancer mellem medlemsstaterne, da den nuværende høje efterspørgsel og de høje lønninger i denne sektor kan føre til en vis form for hjerneflugt i retning af de bedst betalte muligheder.

Af disse grunde foreslår ordføreren at styrke specialiserede, tværfaglige og generelle færdigheder og kompetencer i hele EU med særligt fokus på kvinder, da der fortsat er en kønsbestemt kløft inden for cybersikkerhed, idet den gennemsnitlige tilstedeværelse af kvinder på verdensplan ligger på 20 %.[4] Kvinder skal være til stede og være en del af udformningen af den digitale fremtid og dens forvaltning.

Ordføreren foreslår en styrkelse af trekanten mellem nationale kompetencecentre, Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) og ENISA med hensyn til udviklingen af færdigheder og kompetencer. Desuden foreslås det at øge **industriens** rolle med hensyn til at **udvikle færdigheder** og skabe partnerskaber med den **akademiske verden** og civilsamfundsaktører, idet der tages hensyn til regionale erfaringer, viden og specialisering

[4] Europa-Parlamentets beslutning af 10. juni 2021 om fremme af ligestilling mellem kønnene i uddannelse og karriereveje inden for naturvidenskab, teknologi, ingeniørvirksomhed og matematik (STEM) (2019/2164(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_DA.html

og alliancer fra tredjelande, og med ligesindede partnere for at øge udvekslingerne og sikre en global tilgang til støtte for borgere, virksomheder og institutioner.

Ordføreren foreslår også at øge samarbejdet om talentudvikling og måling af de menneskelige skader som følge af cyberangreb (f.eks. virkningen af et ransomwareangreb på sundhedssektoren).

Ordføreren foreslår foranstaltninger til at inddrage og øge borgernes bevidsthed uden alarmisme som et andet middel til at sikre beskyttelsen af vores demokratier og grundlæggende værdier. Det foreslås at styrke **cybersikkerhedskulturen**, der omfatter sikkerhed, herunder i det digitale miljø, som et offentligt gode. På denne måde vil vi være i stand til at garantere en model for digitalt demokrati – i modsætning til en, der fører til digitalt autoritære regimer – med gennemsigtighed, demokrati og den sikkerhed, som udviklingen af en foregribende lovgivning kan medføre.

Desuden mener ordføreren, at en styrkelse af **forskning og innovation** inden for cybersikkerhed vil øge EU's modstandsdygtighed og åbne strategiske autonomi. Ligeledes er hun fortaler for sikring af synergier med forsknings- og innovationsprogrammer og med eksisterende instrumenter og institutioner og styrkelse af videntrekanten for at slå bro over færdighedskløften i EU.

Denne lovgivning vil også øge EU's og medlemsstaternes modstandsdygtighed, ikke kun direkte via lovgivningen om cybersikkerhed og cyberrobusthed, men også i kraft af den indvirkning, den kan have på den eksponentielle udvikling af kunstig intelligens og den indvirkning, som reguleringen af data og databeskyttelse kan have på cybersikkerheden.

Desforuden vil lovgivningen bidrage til at opfylde forpligtelsen i den **europæiske erklæring om digitale rettigheder og principper for det digitale årti**, der er knyttet til beskyttelse af vores befolkningers, virksomheders og offentlige institutioners interesser mod cybersikkerhedsrisici og cyberkriminalitet, herunder brud på datasikkerheden og identitetstyveri eller manipulation.

På denne baggrund mener ordføreren, at dette forslag bør blive operationelt så hurtigt som muligt, herunder det europæiske cybersikkerhedsskjold og cyberberedskabsmekanismen, for at etablere en generel ramme og undgå siloer, da cyberspace ikke kender nogen grænser.

Bilag: ENHEDER ELLER PERSONER, SOM ORDFØREREN HAR MODTAGET INPUT FRA

I henhold til artikel 8 i bilag I til forretningsordenen erklærer ordføreren at have modtaget input fra følgende enheder eller personer som led i udarbejdelsen af betænkningen inden vedtagelsen i udvalget:

Organer og/eller personer
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Ovenstående liste er udelukkende udarbejdet på ordførerens ansvar.

27.10.2023

UDTALELSE FRA UDENRIGSUDVALGET

til Udvalget om Industri, Forskning og Energi

om forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
(COM(2023)0209) – C9-0136/2023 – 2023/0109(COD)

Ordfører for udtalelse: Dragoş Tudorache

Ændringsforslag 1

Forslag til forordning
Betragtning 1

Kommissionens forslag	*Ændringsforslag*
(1) Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af ***økonomien***, da offentlige forvaltninger, virksomheder og borgere mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden.	(1) Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af ***økonomiske og militære aktiviteter***, da offentlige forvaltninger, virksomheder og borgere ***samt aktører inden for militæret og forsvaret*** mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden.

Ændringsforslag 2

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage,	(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage,

ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. ***Truslen*** rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande.

ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. ***Alvoren af disse trusler blev endnu mere tydelig, da der igen blev krig på vores kontinent. Disse trusler*** rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der tager del i de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi ***og sikkerhed*** og sågar få sundhedsmæssige eller livstruende konsekvenser ***ved måske at underminere lokale eller nationale sikkerhedsrelaterede installationer***. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidigt eller spredes hurtigt til mange lande. ***Cybersikkerhed er vigtig for at beskytte vores europæiske værdier og sikrer, at vores demokratier fungerer, ved at beskytte vores valginfrastruktur og demokratiske procedurer mod enhver form for udenlandsk indblanding.***

Ændringsforslag 3

Forslag til forordning
Betragtning 2 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(2a) Cybersikkerhed er helt afgørende for at holde vores Union sikker og forhindre ondsindede aktører, både statslige og ikkestatslige, i at undergrave vores demokrati, økonomi og sikkerhed. Det er nødvendigt at forhindre et fragmenteret landskab, da en sådan situation ikke ville udgøre en passende tilgang, navnlig når vi står over for udfordringen med fremtidige omfattende cyberangreb rettet mod flere medlemsstater på samme tid eller mod tværnational kritisk infrastruktur. Derfor er der behov for et EU-organ, der skal fungere som en koordineringsplatform for alle eksisterende og fremtidige cybersikkerhedsinstrumenter, -fonde og -mekanismer.

Ændringsforslag 4

Forslag til forordning
Betragtning 3

Kommissionens forslag	*Ændringsforslag*
(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[16] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der driver kritisk infrastruktur, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug	(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[16] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der driver kritisk infrastruktur, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug

for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser.

for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser***, såvel som sin evne til at handle proaktivt og reagere effektivt på cybersikkerhedstrusler og -hændelser***.

[16] https://futureu.europa.eu/en/

[16] https://futureu.europa.eu/en/

Ændringsforslag 5

Forslag til forordning
Betragtning 4

Kommissionens forslag	*Ændringsforslag*
(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.	(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt ***og proaktivt***, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked. ***Endvidere godkendte og lancerede Unionen sit strategiske kompas for sikkerhed og forsvar i marts 2022, som bl.a. har fokus på at styrke***

cybersikkerheden og forbedre det internationale samarbejde med ligesindede allierede og demokratiske partnere, navnlig om dette spørgsmål. Derudover har cybersikkerhed været et centralt punkt i den nylige tredje fælles erklæring om samarbejdet mellem EU og NATO fra januar 2023. Navnlig anbefaledes det i EU-NATO-taskforcens endelige vurderingsrapport, at der gøres fuld brug af synergierne mellem EU og NATO[1], herunder udveksling af bedste praksis mellem civile og militære aktører om gennemførelsen af relevante cyberrelaterede politikker og lovgivning.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_da

---

[17] 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 (EUT L 333 af 27.12.2022).

[18] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[19] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

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

[17] 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 (EUT L 333 af 27.12.2022).

[18] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[19] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

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

cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

Ændringsforslag 6

Forslag til forordning
Betragtning 6

Kommissionens forslag	*Ændringsforslag*
(6) I den fælles meddelelse om EU's politik for cyberforsvar[22], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til at opdage og reagere på hændelser ved at fremme etableringen af en EU-infrastruktur for sikkerhedsoperationscentre ("SOC'er"), støtte en gradvis opbygning af en cybersikkerhedsreserve på EU-plan med brug af tjenester fra betroede private udbydere og teste kritiske enheder for potentielle sårbarheder baseret på EU's risikovurderinger.	(6) I den fælles meddelelse om EU's politik for cyberforsvar[22], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til at opdage og reagere på hændelser ved at fremme etableringen af en EU-infrastruktur for sikkerhedsoperationscentre ("SOC'er"), støtte en gradvis opbygning af en cybersikkerhedsreserve på EU-plan med brug af tjenester fra betroede private udbydere og teste kritiske enheder for potentielle sårbarheder baseret på EU's risikovurderinger. ***Derudover viser cybertrusselsbilledet, som er i hastig udvikling, og det hurtige tempo i teknologiudviklingen også behovet for styrket civil-militær koordinering og civil-militært samarbejde, hvilket Rådet understregede i dets konklusioner om EU's cyberforsvarspolitik[1].***
	[1] Rådets konklusioner om EU's cyberforsvarspolitik, godkendt af Rådet på samlingen den 22. maj 2023 (9618/23).
[22] Fælles meddelelse til Europa-Parlamentet og Rådet — EU's politik for cyberforsvar JOIN/2022/49 final	[22] Fælles meddelelse til Europa-Parlamentet og Rådet – EU's politik for cyberforsvar JOIN/2022/49.

Ændringsforslag 7

Forslag til forordning
Betragtning 6 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(6a) I betragtning af de stadig mere udviskede linjer mellem områderne for civile og militære anliggender og det forhold, at cyberværktøjer og -teknologier har dobbelt anvendelse, er der behov for en sammenhængende og holistisk tilgang til det digitale domæne. I tilfælde af en væsentlig cybersikkerhedshændelse og -krise, som involverer mere end én medlemsstat, bør der indføres passende krisestyring og -forvaltning. Sådanne strukturer bør tilrettelægge informationsudveksling, koordinering og samarbejde med Unionens eksterne sikkerhedsstrukturer og militære krisestyringsstrukturer og medlemsstaternes organer med ansvar for sikkerhed og forsvar (cyberforsvarssektoren). Dette bør også gælde operationer og missioner, der gennemføres af Unionen under den fælles sikkerheds- og forsvarspolitik for at sikre fred og stabilitet i og uden for dens nabolande.

Ændringsforslag 8

Forslag til forordning
Betragtning 7

Kommissionens forslag	*Ændringsforslag*
(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør en paneuropæisk infrastruktur af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Der bør etableres	(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør en paneuropæisk infrastruktur af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Der bør etableres

en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige eller omfattende cybersikkerhedshændelser og sikre en omgående efterfølgende genopretning. Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).	en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige eller omfattende cybersikkerhedshændelser***, herunder hændelser, der involverer mere end én medlemsstat,*** og sikre en omgående efterfølgende genopretning. ***Når det er muligt og nødvendigt, bør en beredskabsmekanisme for cybersikkerhed tilrettelægge informationsudveksling og samarbejde med medlemsstaternes forsvarsmyndigheder med støtte fra EU's institutioner, organer og agenturer (EU's cyberforsvarssektor).*** Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. ***Sådanne nye strukturer bør også støtte EU's FSFP-operationer og -missioner.*** Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

Ændringsforslag 9

Forslag til forordning
Betragtning 11

Kommissionens forslag	*Ændringsforslag*
(11) Med henblik på forsvarlig økonomisk forvaltning bør særlige regler fastsættes for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i finansforordningen, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler.	(11) Med henblik på forsvarlig økonomisk forvaltning bør der fastsættes særlige regler for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i finansforordningen, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler. ***Disse særlige regler vil også give mulighed for***

	mere langsigtet finansiel støtte til fælles indkøb af supersikre værktøjer og infrastruktur af næste generation for at forbedre den kollektive detektionskapacitet ved at anvende den sidste nye kunstige intelligens (AI) og dataanalyse.

Ændringsforslag 10

Forslag til forordning
Betragtning 13

Kommissionens forslag	*Ændringsforslag*
(13) De enkelte medlemsstater bør udpege et offentligt organ på nationalt plan, der har til opgave at koordinere aktiviteter til afsløring af cybertrusler i den pågældende medlemsstat. Disse nationale sikkerhedsoperationscentre (SOC'er) bør fungere som reference- og indgangspunkt på nationalt plan for deltagelse i det europæiske cyberskjold, og de bør sikre, at oplysninger om cybertrusler fra offentlige og private enheder deles og indsamles på nationalt plan på en effektiv og koordineret måde.	(13) De enkelte medlemsstater bør udpege et offentligt organ på nationalt plan, der har til opgave at koordinere aktiviteter til afsløring af cybertrusler i den pågældende medlemsstat. Disse nationale sikkerhedsoperationscentre (SOC'er) bør fungere som reference- og indgangspunkt på nationalt plan for deltagelse i det europæiske cyberskjold, og de bør sikre, at oplysninger om cybertrusler fra offentlige og private enheder deles og indsamles på nationalt plan på en effektiv og koordineret måde. ***Når det er muligt og nødvendigt, bør SOC'erne også gøre det muligt for forsvarsenheder at deltage ved at oprette en "forsvarssøjle" med hensyn til forvaltning og typen af udvekslede oplysninger, som beskrevet i den fælles meddelelse om EU's politik for cyberforsvar[1] og støttet af den højtstående repræsentant.*** ***[1] Fælles meddelelse til Europa-Parlamentet og Rådet – EU's politik for cyberforsvar JOIN/2022/0049.***

Ændringsforslag 11

Forslag til forordning
Betragtning 14

Kommissionens forslag	*Ændringsforslag*
(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet om cybersikkerhedstrusler, navnlig gennem deling af data fra forskellige offentlige eller private kilder samt gennem deling og fælles anvendelse af avancerede værktøjer og fælles udvikling af detektions-, analyse- og forebyggelseskapaciteter i et sikkert miljø. De bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.	(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, ***herunder en "forsvarssøjle",*** så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet om cybersikkerhedstrusler, navnlig gennem deling af data fra forskellige offentlige eller private ***og – når det er nødvendigt og muligt – militære*** kilder ***med tilstrækkelig vejledning i informationsudveksling*** samt gennem deling og fælles anvendelse af avancerede værktøjer og fælles udvikling af detektions-, analyse- og forebyggelseskapaciteter i et sikkert miljø. De bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.

Ændringsforslag 12

Forslag til forordning
Betragtning 15

Kommissionens forslag	*Ændringsforslag*
(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv	(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv

(EU) 2022/2555. De grænseoverskridende SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og ***teknologiske suverænitet***.	(EU) 2022/2555. De grænseoverskridende SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge sådanne data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og ***modstandsdygtighed***.

Ændringsforslag 13

Forslag til forordning
Betragtning 16

Kommissionens forslag	*Ændringsforslag*
(16) De grænseoverskridende SOC'er bør fungere som et centralt knudepunkt, hvor relevante data og efterretninger om cybertrusler generelt sammenstilles, og de skal muliggøre udveksling af trusselsoplysninger blandt en lang række forskellige aktører (f.eks. IT-beredskabsenheder (CERT'er), CSIRT'er, informationsdelings- og analysecentre (ISAC'er) og operatører af kritisk infrastruktur). De oplysninger, der udveksles mellem deltagerne i en grænseoverskridende SOC, kan omfatte data fra netværk og sensorer, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, trusler og sårbarheder. Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er.	(16) De grænseoverskridende SOC'er bør fungere som et centralt knudepunkt, hvor relevante data og efterretninger om cybertrusler generelt sammenstilles, og de skal muliggøre udveksling af trusselsoplysninger blandt en lang række forskellige aktører (f.eks. IT-beredskabsenheder (CERT'er), CSIRT'er, informationsdelings- og analysecentre (ISAC'er) og operatører af kritisk infrastruktur ***samt cyberforsvarssektoren***). De oplysninger, der udveksles mellem deltagerne i en grænseoverskridende SOC, kan omfatte data fra netværk og sensorer, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, trusler og sårbarheder. Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er ***og det operationelle netværk for milCERT'er (MICNET), når det er oprettet***.

Ændringsforslag 14

Forslag til forordning
Betragtning 17

Kommissionens forslag	*Ændringsforslag*
(17) At de relevante myndigheder opbygger et fælles situationskendskab er en nødvendig forudsætning for EU-dækkende beredskab og koordinering vedrørende væsentlige og omfattende cybersikkerhedshændelser. Ved direktiv (EU) 2022/2555 oprettes EU–CyCLONe for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og for at sikre regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser omhandler alle de relevante aktørers rolle. I direktiv (EU) 2022/2555 påpeges også Kommissionens ansvar i forbindelse med EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU, samt for at udarbejde analytiske rapporter om ordningerne under den integrerede mekanisme for politisk kriserespons ("IPCR") i henhold til gennemførelsesafgørelse (EU) 2018/1993. I situationer, hvor grænseoverskridende SOC'er indhenter oplysninger vedrørende en potentiel eller igangværende væsentlig cybersikkerhedshændelse, bør de derfor give relevante oplysninger til EU-CyCLONe, CSIRT-netværket og Kommissionen. Afhængigt af situationen kan de oplysninger, der skal udveksles, især omfatte tekniske oplysninger, oplysninger om angriberens eller den mulige angriberes kendetegn og motiver og ikke-tekniske oplysninger på overordnet niveau om en potentiel eller igangværende omfattende cybersikkerhedshændelse. I den sammenhæng bør der tages behørigt hensyn til, hvilke oplysninger der er nødvendige, og til den eventuelt følsomme karakter af de udvekslede oplysninger.	(17) At de relevante myndigheder opbygger et fælles situationskendskab er en nødvendig forudsætning for EU-dækkende beredskab og koordinering vedrørende væsentlige og omfattende cybersikkerhedshændelser. Ved direktiv (EU) 2022/2555 oprettes EU–CyCLONe for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og for at sikre regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser omhandler alle de relevante aktørers rolle. I direktiv (EU) 2022/2555 påpeges også Kommissionens ansvar i forbindelse med EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU, samt for at udarbejde analytiske rapporter om ordningerne under den integrerede mekanisme for politisk kriserespons ("IPCR") i henhold til gennemførelsesafgørelse (EU) 2018/1993. I situationer, hvor grænseoverskridende SOC'er indhenter oplysninger vedrørende en potentiel eller igangværende væsentlig cybersikkerhedshændelse, bør de derfor give relevante oplysninger til EU-CyCLONe, CSIRT-netværket***,*** ***cyberforsvarssektoren*** og Kommissionen. Afhængigt af situationen kan de oplysninger, der skal udveksles, især omfatte tekniske oplysninger, oplysninger om angriberens eller den mulige angriberes kendetegn og motiver og ikke-tekniske oplysninger på overordnet niveau om en potentiel eller igangværende omfattende cybersikkerhedshændelse. I den sammenhæng bør der tages behørigt hensyn til, hvilke oplysninger der er nødvendige, og til den eventuelt følsomme

karakter af de udvekslede oplysninger.

Ændringsforslag 15

Forslag til forordning
Betragtning 19

Kommissionens forslag	*Ændringsforslag*
(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse.	(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer***, hvor højrisikoleverandører af kritiske produkter med digitale elementer udelukkes***. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse. ***Der bør fastsættes bestemmelse om menneskeligt tilsyn i forbindelse med anvendelsen af AI, og der bør sikres et tilstrækkeligt niveau af AI-færdigheder, den nødvendige støtte og beføjelse til at udøve denne funktion.***

Ændringsforslag 16

Forslag til forordning
Betragtning 19 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(19a) I overensstemmelse med forordning [XX/XXXX (forordningen om cyberrobusthed)] bør enheder, der deltager i det europæiske cyberskjold, også dække de krav, der er fastsat i denne forordning, for alle produkter med digitale elementer. I betragtning af de øgede risici, der kommer af økonomiske afhængighedsforhold, er det nødvendigt

	at minimere eksponeringen for højrisikoleverandører af kritiske produkter gennem en fælles strategisk ramme for EU's økonomiske sikkerhed. Afhængighed af højrisikoleverandører af kritiske produkter med digitale elementer udgør en strategisk risiko, som bør adresseres på EU-plan, navnlig hvorvidt et land giver sig af med økonomisk spionage eller økonomisk tvang, og dets lovgivning kræver vilkårlig adgang til enhver form for virksomhedsoperationer eller -data, navnlig når de kritiske produkter er beregnet til brug i væsentlige enheder som omhandlet i direktiv (EU) 2022/2555.

Ændringsforslag 17

Forslag til forordning
Betragtning 20

Kommissionens forslag	*Ændringsforslag*
(20) Gennem indsamling, deling og udveksling af data bør det europæiske cyberskjold kunne styrke Unionens teknologiske suverænitet. Sammenlægning af udvalgte data af høj kvalitet bør også kunne bidrage til udviklingen af avancerede teknologier inden for kunstig intelligens og dataanalyse. Processen bør fremmes ved at forbinde det europæiske cyberskjold med den paneuropæiske infrastruktur til højtydende databehandling, der er oprettet ved Rådets forordning (EU) 2021/1173[25].	(20) Gennem indsamling, deling og udveksling af data bør det europæiske cyberskjold kunne styrke Unionens teknologiske suverænitet***, strategiske autonomi, konkurrenceevne og modstandsdygtighed***. Sammenlægning af udvalgte data af høj kvalitet bør også kunne bidrage til udviklingen af avancerede teknologier inden for kunstig intelligens og dataanalyse. Processen bør fremmes ved at forbinde det europæiske cyberskjold med den paneuropæiske infrastruktur til højtydende databehandling, der er oprettet ved Rådets forordning (EU) 2021/1173[25].
[25] Rådets forordning (EU) 2021/1173 af 13. juli 2021 om oprettelse af et fællesforetagende for europæisk højtydende databehandling og om ophævelse af forordning (EU) 2018/1488 (EUT L 256 af 19.7.2021, s. 3).	[25] Rådets forordning (EU) 2021/1173 af 13. juli 2021 om oprettelse af et fællesforetagende for europæisk højtydende databehandling og om ophævelse af forordning (EU) 2018/1488 (EUT L 256 af 19.7.2021, s. 3).

Ændringsforslag 18

Forslag til forordning
Betragtning 25

Kommissionens forslag	*Ændringsforslag*
(25) Cyberberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed ("ENISA") i overensstemmelse med dets mandat[26], den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold og hybride beredskabshold. Cyberberedskabsmekanismen bør indgå i løsning af behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande.	(25) Cyberberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed ("ENISA") i overensstemmelse med dets mandat, den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold***[1], det nye PESCO-projekt "Koordineringscenteret på cyber- og informationsområdet (CIDCC)" og den foreslåede efterfølger hertil, "EU-Koordinationscenteret for Cyberforsvar (EUCDCC)",*** og hybride beredskabshold. Cyberberedskabsmekanismen bør adressere behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande***, navnlig de EU-kandidatlande, der har bragt sig på linje med EU's fælles udenrigs- og sikkerhedspolitik og fælles sikkerheds- og forsvarspolitik, støtte dem med at opbygge deres cyberkapacitet og styrke det grænseoverskridende og regionale samarbejde blandt disse kandidatlande på cyberområdet***. ***[1] Rådets afgørelse (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde***

(PESCO) og fastlæggelse af listen over deltagende medlemsstater.

[26] RÅDETS AFGØRELSE (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde (PESCO) og fastlæggelse af listen over deltagende medlemsstater.

[26] Rådets afgørelse (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde (PESCO) og fastlæggelse af listen over deltagende medlemsstater.

Ændringsforslag 19

Forslag til forordning
Betragtning 26

Kommissionens forslag	*Ændringsforslag*
(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[27], IPCR[28],, og direktiv (EU) 2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, ***hvor det er relevant***.	(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[27], IPCR[28],, og direktiv (EU) 2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, ***navnlig med henblik på at styrke kapaciteten til at imødegå cybersikkerhedstrusler fra lande uden for Unionen, herunder restriktive foranstaltninger, der kan anvendes til at forhindre og reagere på ondsindede cyberaktiviteter***.

[27] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

[28] Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion

[27] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

[28] Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion

på væsentlige cybersikkerhedshændelser og -kriser.

på væsentlige cybersikkerhedshændelser og -kriser.

Ændringsforslag 20

Forslag til forordning
Betragtning 28

Kommissionens forslag	*Ændringsforslag*
(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt og virkningsfuldt. I henhold til direktivet skal medlemsstaterne endvidere identificere kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise, og vedtage en national omfattende beredskabsplan for cybersikkerhedshændelser og -kriser, hvor målsætningerne og ordningerne vedrørende håndtering af væsentlige cybersikkerhedshændelser og -kriser er fastsat. Medlemsstaterne skal også oprette et eller flere CSIRT'er, der har ansvar for håndtering af hændelser efter en veldefineret proces, der som minimum dækker de sektorer, delsektorer og typer af enheder, der er omfattet af nævnte direktivs anvendelsesområde, og sikre, at de har tilstrækkelige ressourcer til effektivt at udføre deres opgaver. Denne forordning berører ikke Kommissionens rolle med hensyn til at sikre, at medlemsstaterne overholder forpligtelserne i direktiv (EU) 2022/2555. Cyberberedskabsmekanismen bør yde bistand til foranstaltninger, der har til formål at styrke beredskabet og indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser, støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion.	(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt og virkningsfuldt. I henhold til direktivet skal medlemsstaterne endvidere identificere kapaciteter, aktiver og procedurer, der kan tages i brug i tilfælde af en krise, og vedtage en national omfattende beredskabsplan for cybersikkerhedshændelser og -kriser, hvor målsætningerne og ordningerne vedrørende håndtering af væsentlige cybersikkerhedshændelser og -kriser er fastsat. Medlemsstaterne skal også oprette en eller flere CSIRT'er, der har ansvar for håndtering af hændelser efter en veldefineret proces, der som minimum dækker de sektorer, delsektorer og typer af enheder, der er omfattet af nævnte direktivs anvendelsesområde, og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt. Denne forordning berører ikke Kommissionens rolle med hensyn til at sikre, at medlemsstaterne overholder forpligtelserne i direktiv (EU) 2022/2555. Cyberberedskabsmekanismen bør yde bistand til foranstaltninger, der har til formål at styrke beredskabet og indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser, støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion***, idet der gøres hensigtsmæssig brug af hele den vifte af defensive muligheder, som de civile og militære sektorer råder***

over.

Ændringsforslag 21

Forslag til forordning
Betragtning 29

Kommissionens forslag	*Ændringsforslag*
(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres	(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. ***Når det er hensigtsmæssigt, bør Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), navnlig gennem EU's Efterretnings- og Situationscenter (INTCEN) og dets analyseenhed for hybride trusler med støtte fra Den Europæiske Unions Militærstabs (EUMS') efterretningsdirektorat under den fælles efterretningsanalysekapacitet (SIAC), også tilknyttes for at levere ajourførte vurderinger og dermed bidrage til at indkredse de sektorer eller delsektorer, der*** bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer af særligt kritisk betydning"). De koordinerede afprøvningsøvelser bør være baseret på fælles risikoscenarier og -metoder. ***Disse øvelser bør også spille en vigtig rolle med hensyn til at forbedre samarbejdet mellem civile og militære enheder. I forbindelse med tilrettelæggelsen af øvelser bør Kommissionen, EU-Udenrigstjenesten og***

af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[29]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

ENISA derfor systematisk overveje at medtage deltagere fra andre cybersamfund som f.eks. Det Europæiske Forsvarsagentur (EDA) og andre relevante enheder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554***[1]***. Ved udvælgelsen af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

[1] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

---

[29] Europa-Parlamentets og Rådets

---

[29] Europa-Parlamentets og Rådets

forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011	forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

Ændringsforslag 22

Forslag til forordning
Betragtning 32

Kommissionens forslag	*Ændringsforslag*
(32) Cyberberedskabsmekanismen bør støtte bistand fra andre medlemsstater til en medlemsstat, der er berørt af en væsentlig eller omfattende cybersikkerhedshændelse, herunder af CSIRT-netværket, jf. artikel 15 i direktiv (EU) 2022/2555. Medlemsstater, der yder bistand, bør have mulighed for at indgive anmodning om dækning af omkostninger i forbindelse med udsendelse af eksperthold inden for rammerne af gensidig bistand. De støtteberettigede omkostninger kan omfatte udgifter til rejser, indkvartering og daglige udgifter for cybersikkerhedseksperter.	(32) Cyberberedskabsmekanismen bør støtte bistand fra andre medlemsstater til en medlemsstat, der er berørt af en væsentlig eller omfattende cybersikkerhedshændelse, herunder af CSIRT-netværket, jf. artikel 15 i direktiv (EU) 2022/2555. Medlemsstater, der yder bistand, bør have mulighed for at indgive anmodning om dækning af omkostninger i forbindelse med udsendelse af eksperthold inden for rammerne af gensidig bistand***, hvilket sikrer en effektiv koordinering mellem EU's relevante programmer og instrumenter, herunder den europæiske fredsfacilitet, FUSP og NDICI, når der ydes bistand til tredjelande, navnlig Ukraine og Moldova***. De støtteberettigede omkostninger kan omfatte udgifter til rejser, indkvartering og daglige udgifter for cybersikkerhedseksperter.

Ændringsforslag 23

Forslag til forordning
Betragtning 33

Kommissionens forslag	*Ændringsforslag*
(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til	(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til

støtte for indsatsen og foranstaltninger til omgående genopretning i tilfælde af væsentlige eller omfattende cybersikkerhedshændelser. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate. Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i kritiske eller meget kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. Når medlemsstaterne anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer og agenturer på lignende betingelser.	støtte for indsatsen og foranstaltninger til omgående genopretning i tilfælde af væsentlige eller omfattende cybersikkerhedshændelser. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate. Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i kritiske eller meget kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. Når medlemsstaterne anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer og agenturer***, herunder FSFP-missioner,*** på lignende betingelser.

Ændringsforslag 24

Forslag til forordning
Betragtning 34

Kommissionens forslag	*Ændringsforslag*
(34) Med henblik på at udvælge private tjenesteudbydere, der skal levere tjenester i forbindelse med EU's cybersikkerhedsreserve, er det nødvendigt at fastsætte et sæt minimumskriterier, der bør indgå i udbuddet til udvælgelse af udbyderne, for at sikre, at behovene opfyldes hos medlemsstaternes myndigheder og enheder, der opererer i kritiske eller meget kritiske sektorer.	(34) Med henblik på at udvælge private tjenesteudbydere, der skal levere tjenester i forbindelse med EU's cybersikkerhedsreserve, er det nødvendigt at fastsætte et sæt minimumskriterier, der bør indgå i udbuddet til udvælgelse af udbyderne, for at sikre, at behovene opfyldes hos medlemsstaternes myndigheder og enheder, der opererer i kritiske eller meget kritiske sektorer***, idet der også tages højde for de risici, der er forbundet med deltagelse af udbydere fra lande, der er vores strategiske konkurrenter, hvilket kan give anledning til økonomiske sikkerhedsrisici, såvel som for konsekvenserne for Unionens***

strategiske sikkerhed.

Ændringsforslag 25

Forslag til forordning
Betragtning 36

Kommissionens forslag	*Ændringsforslag*
(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en effektiv reaktion på væsentlige og omfattende cybersikkerhedshændelser bør EU-CyCLONe, CSIRT-netværket eller Kommissionen kunne anmode ENISA om at gennemgå og vurdere trusler, sårbarheder og afbødende foranstaltninger i forbindelse med en specifik væsentlig eller omfattende cybersikkerhedshændelse. Efter gennemførelsen af en gennemgang og vurdering af en hændelse bør ENISA udarbejde en rapport om hændelsen i samarbejde med relevante interessenter, herunder repræsentanter fra den private sektor, medlemsstaterne, Kommissionen og andre relevante EU-institutioner, -organer og -agenturer. For så vidt angår den private sektor etablerer ENISA kanaler til udveksling af oplysninger med specialiserede udbydere, herunder udbydere af administrerede sikkerhedsløsninger og leverandører, med henblik på at bidrage til ENISA's opgave med at opnå et højt fælles cybersikkerhedsniveau i hele Unionen. På grundlag af samarbejdet med interessenter, herunder den private sektor, bør rapporten om gennemgang af specifikke hændelser have til formål at vurdere årsagerne til, virkningerne af og modvirkningen af en hændelse, efter at den er indtruffet. Der bør lægges særlig vægt på oplysninger og erfaringer, der indmeldes af udbydere af administrerede sikkerhedstjenester, som opfylder betingelserne om højeste faglige integritet, upartiskhed og den nødvendige	(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en effektiv reaktion på væsentlige og omfattende cybersikkerhedshændelser bør EU-CyCLONe, CSIRT-netværket eller Kommissionen kunne anmode ENISA om at gennemgå og vurdere trusler, sårbarheder og afbødende foranstaltninger i forbindelse med en specifik væsentlig eller omfattende cybersikkerhedshændelse. ***Med henblik på udviklingen af et sikkert konnektivitetssystem, der bygger på den europæiske kvantekommunikationsinfrastruktur (EuroQCI) og Den Europæiske Unions statslige satellitkommunikation (GOVSATCOM), navnlig gennemførelsen af Galileo GNSS for forsvarsbrugere, bør enhver fremtidig mulig udvikling tage højde for fremkomsten af "hyperkrig", som forener kvantedatabehandlingens hastighed og sofistikerede karakter med højautonome militære systemer.*** Efter gennemførelsen af en gennemgang og vurdering af en hændelse bør ENISA udarbejde en rapport om hændelsen i samarbejde med relevante interessenter, herunder repræsentanter fra den private sektor, medlemsstaterne, Kommissionen og andre relevante EU-institutioner, -organer og -agenturer. For så vidt angår den private sektor etablerer ENISA kanaler til udveksling af oplysninger med specialiserede udbydere, herunder udbydere af administrerede sikkerhedsløsninger og leverandører, med henblik på at bidrage til ENISA's opgave

tekniske ekspertise som krævet i denne forordning. Rapporten bør leveres og indgå i arbejdet i EU-CyCLONe, CSIRT-netværket og Kommissionen. Når hændelsen vedrører et tredjeland, videresender Kommissionen også rapporten til den højtstående repræsentant.

med at opnå et højt fælles cybersikkerhedsniveau i hele Unionen. På grundlag af samarbejdet med interessenter, herunder den private sektor, bør rapporten om gennemgang af specifikke hændelser have til formål at vurdere årsagerne til, virkningerne af og modvirkningen af en hændelse, efter at den er indtruffet. Der bør lægges særlig vægt på oplysninger og erfaringer, der indmeldes af udbydere af administrerede sikkerhedstjenester, som opfylder betingelserne om højeste faglige integritet, upartiskhed og den nødvendige tekniske ekspertise som krævet i denne forordning. Rapporten bør leveres og indgå i arbejdet i EU-CyCLONe, CSIRT-netværket og Kommissionen. Når hændelsen vedrører et tredjeland, videresender Kommissionen også rapporten til den højtstående repræsentant***, EU-Udenrigstjenesten og en eventuel FSFP-mission i landet, som måtte være berørt af hændelsen, via deres hovedkvarterer***.

Ændringsforslag 26

Forslag til forordning
Betragtning 37

Kommissionens forslag	*Ændringsforslag*
(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medrører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor ***kan*** tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve***, hvis dette er fastsat i den respektive associeringsaftale til programmet for et***	(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medfører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes***, navnlig Ukraines og Moldovas,*** modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor ***bør*** tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve. ***Støtten bør også gælde de tredjelande, hvortil der er***

digitalt Europa. Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med programmet for et digitalt Europa.

udsendt en FSFP-mission med et specifikt mandat til at styrke modstandsdygtigheden over for hybride trusler, herunder cybertrusler, eller for hvilke der er vedtaget en bistandsforanstaltning inden for rammerne af den europæiske fredsfacilitet for at styrke landets cyberrobusthed. Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med programmet for et digitalt Europa.

Ændringsforslag 27

Forslag til forordning
Artikel 1 – stk. 1 – litra c

Kommissionens forslag	*Ændringsforslag*
c) oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige eller omfattende hændelser.	c) oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige eller omfattende hændelser ***eller trusler***.

Ændringsforslag 28

Forslag til forordning
Artikel 1 – stk. 2 – litra a

Kommissionens forslag	*Ændringsforslag*
a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og	a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og

dermed gøre det muligt at styrke industriens og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske ***suverænitet*** på cybersikkerhedsområdet	dermed gøre det muligt at styrke industriens og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske ***modstandsdygtighed*** på cybersikkerhedsområdet

Ændringsforslag 29

Forslag til forordning
Artikel 1 – stk. 2 – litra b

Kommissionens forslag	*Ændringsforslag*
b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa	b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa***, eller for de tredjelande, der er kandidater til tiltrædelse af Unionen, og som ikke handler i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i rammerne for FUSP i henhold til afsnit V i TEU. Medlemsstaterne bør overveje et aktivt cyberforsvarsprogram som en del af deres nationale cybersikkerhedsstrategi, der omfatter regelmæssige fælles øvelser mellem medlemsstaterne og på tværs af internationale organisationer. Et sådant program bør kunne tilvejebringe en synkroniseret realtidskapacitet til at afdække, analysere og afbøde trusler***

Ændringsforslag 30

Forslag til forordning
Artikel 1 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. at mindske systemiske cybersikkerhedsrisici som følge af afhængighed af kritisk udstyr fra lande, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU

Ændringsforslag 31

Forslag til forordning
Artikel 2 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	"cyberforsvarssektor": medlemsstaternes forsvarsmyndigheder med støtte fra EU's institutioner, organer og agenturer som fastsat i den fælles meddelelse om EU's politik for cyberforsvar[1]
	[1] Fælles meddelelse til Europa-Parlamentet og Rådet – EU's politik for cyberforsvar JOIN/2022/0049.

Ændringsforslag 32

Forslag til forordning
Artikel 3 – stk. 2 – afsnit 1 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ba) bidrage til at modernisere alle cyberforsvarssystemer, øge kvaliteten af cyberforsvarskapaciteter gennem udbredelse af AI-systemer og fremskynde udvekslingen af oplysninger mellem de nationale SOC'er og grænseoverskridende SOC'er

Ændringsforslag 33

Forslag til forordning
Artikel 3 – stk. 2 – afsnit 1 – litra d a (nyt)

Kommissionens forslag	*Ændringsforslag*
	da) gennemgå og evaluere kritisk cybersikkerhedsteknologi og -udstyr, der anvendes af SOC'er til at reagere på cybersikkerhedshændelser vedrørende systemiske risici som følge af kontrol over højrisikoudbydere udøvet af lande, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU.

Ændringsforslag 34

Forslag til forordning
Artikel 4 – nr. 1 – afsnit 1

Kommissionens forslag	*Ændringsforslag*
Det skal have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser og bidrage til et grænseoverskridende SOC. Det skal være udstyret med avancerede teknologier, der gør det muligt at finde, aggregere og analysere data, der er relevante for cybersikkerhedstrusler og -hændelser.	Det skal have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private ***– og om nødvendigt militære –*** organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser og bidrage til et grænseoverskridende SOC. Det skal være udstyret med avancerede teknologier, der gør det muligt at finde, aggregere og analysere data, der er relevante for cybersikkerhedstrusler og -hændelser.

Ændringsforslag 35

Forslag til forordning
Artikel 4 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Efter en indkaldelse af interessetilkendegivelser udvælges de	2. Efter en indkaldelse af interessetilkendegivelser udvælges de

nationale SOC'er af Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til de udvalgte nationale SOC'er til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af medlemsstaten. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og det nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.	nationale SOC'er af Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til de udvalgte nationale SOC'er til finansiering af driften af disse værktøjer og infrastrukturer ***under streng forudsætning af, at sådanne værktøjer og infrastrukturer leveres af betroede udbydere i overensstemmelse med artikel 16***. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af medlemsstaten. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og det nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

Ændringsforslag 36

Forslag til forordning
Artikel 5 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Efter en indkaldelse af interessetilkendegivelser udvælges et værtskonsortium af ECCC til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til værtskonsortiet til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 75 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af værtskonsortiet. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og værtskonsortiet en hosting- og brugsaftale, der regulerer brugen af værktøjerne og	2. Efter en indkaldelse af interessetilkendegivelser udvælges et værtskonsortium af ECCC til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til værtskonsortiet til finansiering af driften af disse værktøjer og infrastrukturer ***under streng forudsætning af, at sådanne værktøjer og infrastrukturer leveres af betroede udbydere i overensstemmelse med artikel 16***. Unionens finansielle bidrag dækker op til 75 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af værtskonsortiet. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og

infrastrukturerne.	infrastrukturer indgår ECCC og værtskonsortiet en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

Ændringsforslag 37

Forslag til forordning
Artikel 5 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. Alle infrastrukturer eller udbydere med oprindelse i et højrisikotredjeland udelukkes automatisk.

Ændringsforslag 38

Forslag til forordning
Artikel 6 – stk. 1 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ba) direkte understøtter en styrkelse af de deltagende medlemmers militære og forsvarsmæssige kapacitet eller forhindrer en direkte og overhængende trussel mod deres sikkerhed. Så længe udnyttelsen af sårbarheder i forsvarssektoren kan forvolde betydelige afbrydelser og betydelig skade, kræver forsvarsindustriens cybersikkerhed, at der træffes særlige foranstaltninger til at garantere sikkerheden i forsyningskæderne, navnlig hvad angår enheder længere nede i kæderne, som ikke har brug for adgang til klassificerede oplysninger, men som kan udgøre alvorlige trusler mod hele sektoren. Der bør lægges særlig vægt på den indvirkning, som et sikkerhedsbrud kan have, og på faren for eventuel manipulation af netværksdata, der kan gøre kritiske forsvarskomponenter ubrugelige eller endog deaktivere deres operativsystemer, så de kan kapres

Ændringsforslag 39

Forslag til forordning
Artikel 6 – stk. 1 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	bb) understøtter en styrkelse af de deltagende medlemmers forsvarskapacitet eller forhindrer en direkte og overhængende trussel mod deres sikkerhed, og derved garanterer sikkerheden i forsyningskæderne, navnlig hvad angår enheder længere nede i kæderne, som ikke har brug for adgang til klassificerede oplysninger, men som kan udgøre alvorlige trusler mod hele sektoren.

Ændringsforslag 40

Forslag til forordning
Artikel 7 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Hvis grænseoverskridende SOC'er indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse, forelægger de uden unødig forsinkelse de relevante oplysninger for EU-CyCLONe, CSIRT-netværket og Kommissionen i betragtning af deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.	1. Hvis grænseoverskridende SOC'er indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse, forelægger de uden unødig forsinkelse de relevante oplysninger for EU-CyCLONe, CSIRT-netværket og Kommissionen***, herunder den højtstående repræsentant og EU-Udenrigstjenesten, når den vedrører et tredjeland,*** i betragtning af deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.

Ændringsforslag 41

Forslag til forordning
Artikel 8 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. De medlemsstater, der deltager i det europæiske cyberskjold, sikrer et højt niveau af datasikkerhed og fysisk sikkerhed i den infrastruktur, der udgør det europæiske cyberskjold, og sikrer, at infrastrukturen forvaltes og styres hensigtsmæssigt, så den beskyttes mod trusler og så sikkerheden i infrastrukturen og i systemerne***, herunder data, der udveksles via infrastrukturen,*** garanteres.	1. De medlemsstater, der deltager i det europæiske cyberskjold, sikrer et højt niveau af datasikkerhed og fysisk sikkerhed i den infrastruktur, der udgør det europæiske cyberskjold, og sikrer, at infrastrukturen forvaltes og styres hensigtsmæssigt, så den beskyttes mod trusler, og så sikkerheden i infrastrukturen og i systemerne garanteres***, idet de mindsker risikoen for og fremmer EU's teknologiske forspring i kritiske sektorer, herunder foranstaltninger til at begrænse eller udelukke højrisikoleverandører og beskytte sikkerheden af data, der udveksles via infrastrukturen***.

Ændringsforslag 42

Forslag til forordning
Artikel 8 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Medlemsstater, der deltager i det europæiske cyberskjold, sikrer, at udvekslingen af oplysninger inden for det europæiske cyberskjold med enheder, der ikke er offentlige organer i medlemsstaterne, ikke har en negativ indvirkning på Unionens sikkerhedsinteresser.	2. Medlemsstater, der deltager i det europæiske cyberskjold, sikrer, at udvekslingen af oplysninger inden for det europæiske cyberskjold med enheder, der ikke er offentlige organer i medlemsstaterne, ikke har en negativ indvirkning på Unionens sikkerhedsinteresser***, og at enhver informationsudveksling med højrisikoleverandører er af begrænset omfang og ikke skader Unionens sikkerhed og strategiske interesser***.

Ændringsforslag 43

Forslag til forordning
Artikel 8 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Kommissionen kan vedtage	3. Kommissionen kan vedtage

gennemførelsesretsakter, der fastsætter tekniske krav til medlemsstaternes opfyldelse af forpligtelserne i stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2. I den forbindelse tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører.	gennemførelsesretsakter, der fastsætter tekniske krav til medlemsstaternes opfyldelse af forpligtelserne i stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2. I den forbindelse tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører ***og gør passende brug af hele den vifte af defensive muligheder, der er til rådighed for de civile og militære sektorer med henblik på EU's overordnede sikkerhed og forsvar, og underretter Europa-Parlamentet***.

Ændringsforslag 44

Forslag til forordning
Artikel 9 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Aktioner til gennemførelse af cyberberedskabsmekanismen støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.	2. Aktioner til gennemførelse af cyberberedskabsmekanismen støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3***, og støttes af den europæiske fredsfacilitet, når der leveres bistandsforanstaltninger til tredjelande, navnlig Ukraine og Moldova***.

Ændringsforslag 45

Forslag til forordning
Artikel 10 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU	a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer***, såsom offentlig infrastruktur, valginfrastruktur, transport,***

sundhedspleje, finans, telekommunikation, fødevareforsyning og -sikkerhed, i EU

Ændringsforslag 46

Forslag til forordning
Artikel 10 – stk. 1 – litra c

Kommissionens forslag	*Ændringsforslag*
c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555.	c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555 ***og inden for rammerne af artikel 42, stk. 7, i TEU og artikel 222 i TEUF***

Ændringsforslag 47

Forslag til forordning
Artikel 10 – stk. 1 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ca) udskiftning og udfasning af kritisk udstyr fra højrisikoleverandører, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU

Ændringsforslag 48

Forslag til forordning
Artikel 11 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. NIS-samarbejdsgruppen udarbejder i samarbejde med Kommissionen, ENISA ***og*** den højtstående repræsentant fælles risikoscenarier og metoder til gennemførelse af de koordinerede test.	2. NIS-samarbejdsgruppen udarbejder i samarbejde med Kommissionen, ENISA***,*** den højtstående repræsentant***, EU-Udenrigstjenesten og, hvor det er relevant, EDA*** fælles risikoscenarier og metoder til gennemførelse af de koordinerede

afprøvninger.

Ændringsforslag 49

Forslag til forordning
Artikel 12 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. EU's cybersikkerhedsreserve består af hændelsesberedskabstjenester fra betroede udbydere, der er udvalgt i overensstemmelse med kriterierne i artikel 16. Reserven omfatter tjenester omfattet af forhåndsforpligtelser. Tjenesterne kan indsættes i alle medlemsstater.	2. EU's cybersikkerhedsreserve består af hændelsesberedskabstjenester fra betroede udbydere, der er udvalgt i overensstemmelse med kriterierne i artikel 16. Reserven omfatter tjenester omfattet af forhåndsforpligtelser. Tjenesterne kan indsættes i alle medlemsstater ***og tredjelande, der opfylder de gældende krav i denne forordning***.

Ændringsforslag 50

Forslag til forordning
Artikel 12 – stk. 3 – litra b

Kommissionens forslag	*Ændringsforslag*
b) EU's institutioner, organer og agenturer.	b) EU's institutioner, organer og agenturer***, herunder FSFP-missioner***.

Ændringsforslag 51

Forslag til forordning
Artikel 12 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Brugerne, som er nævnt i stk. 3, litra a), anvender tjenesterne fra EU's cybersikkerhedsreserve til at reagere på eller støtte indsatsen mod og den omgående genopretning efter væsentlige eller omfattende hændelser, der påvirker enheder, der opererer i kritiske eller meget kritiske sektorer.	4. Brugerne, som er nævnt i stk. 3, litra a), anvender tjenesterne fra EU's cybersikkerhedsreserve til at reagere på eller støtte indsatsen mod og den omgående genopretning efter væsentlige eller omfattende hændelser, der påvirker enheder, der opererer i kritiske eller meget kritiske sektorer***, såsom offentlig infrastruktur, valginfrastruktur, transport, sundhedspleje, finans,***

	telekommunikation, fødevareforsyning og -sikkerhed.

Ændringsforslag 52

Forslag til forordning
Artikel 12 – stk. 5

Kommissionens forslag	*Ændringsforslag*
5. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen fastlægger prioriteterne for og udviklingen af EU's cybersikkerhedsreserve i overensstemmelse med kravene til de brugere, der er omhandlet i stk. 3, overvåger gennemførelsen og sikrer komplementaritet, sammenhæng, synergi og forbindelser med andre støtteaktioner i henhold til denne forordning samt andre EU-foranstaltninger og -programmer.	5. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen fastlægger prioriteterne for og udviklingen af EU's cybersikkerhedsreserve i overensstemmelse med kravene til de brugere, der er omhandlet i stk. 3, overvåger gennemførelsen og sikrer komplementaritet, sammenhæng, synergi og forbindelser med andre støtteaktioner i henhold til denne forordning samt andre EU-foranstaltninger og -programmer ***og -mål, navnlig det strategiske mål om at mindske afhængigheden af højrisikoleverandører, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU***.

Ændringsforslag 53

Forslag til forordning
Artikel 12 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7. For at støtte Kommissionen i etableringen af EU's cybersikkerhedsreserve udarbejder ENISA en kortlægning af de nødvendige tjenester efter høring af medlemsstaterne og Kommissionen. ENISA udarbejder efter høring af Kommissionen en lignende kortlægning for at identificere behovene i de tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve i henhold til	7. For at støtte Kommissionen i etableringen af EU's cybersikkerhedsreserve udarbejder ENISA en kortlægning af de nødvendige tjenester efter høring af medlemsstaterne og Kommissionen. ENISA udarbejder efter høring af Kommissionen en lignende kortlægning for at identificere behovene i de tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve i henhold til

artikel 17. Kommissionen hører, hvor det er relevant, den højtstående repræsentant.	artikel 17***, med støtte fra EU-Udenrigstjenesten***. Kommissionen hører, hvor det er relevant, den højtstående repræsentant.

Ændringsforslag 54

Forslag til forordning
Artikel 14 – stk. 2 – litra a a (nyt)

Kommissionens forslag	*Ændringsforslag*
	aa) hændelsens indvirkning på Unionens sikkerhed og forsvar

Ændringsforslag 55

Forslag til forordning
Artikel 15 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. I samråd med den højtstående repræsentant kan støtte under cyberberedskabsmekanismen supplere den bistand, der ydes inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik, herunder gennem cyberberedskabsholdene. Den kan også supplere eller bidrage til den bistand, som en medlemsstat yder til en anden medlemsstat inden for rammerne af artikel 42, stk. 7, i traktaten om Den Europæiske Union.	3. I samråd med den højtstående repræsentant kan støtte under cyberberedskabsmekanismen supplere den bistand, der ydes inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik, herunder gennem cyberberedskabsholdene ***(CRRT'erne), for bedre at støtte EU's medlemsstater, FSFP-missioner og -operationer og de tredjelande, der har lagt sig på linje med EU's fælles udenrigs- og sikkerhedspolitik og fælles sikkerheds- og forsvarspolitik, i deres bestræbelser på at opbygge cyberforsvarskapacitet, navnlig Ukraine og Moldova***. Den kan også supplere eller bidrage til den bistand, som en medlemsstat yder til en anden medlemsstat inden for rammerne af artikel 42, stk. 7, i traktaten om Den Europæiske Union.

Ændringsforslag 56

Forslag til forordning
Artikel 16 – stk. 2 – litra b a (nyt)

Kommissionens forslag	*Ændringsforslag*
	aa) udbyderen skal påvise, at dennes beslutnings- og forvaltningsstrukturer er fri for enhver utilbørlig påvirkning fra regeringer i stater, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU

Ændringsforslag 57

Forslag til forordning
Artikel 16 – stk. 2 – litra f

Kommissionens forslag	*Ændringsforslag*
f) udbyderen skal være udstyret med den nødvendige hardware og software til at understøtte den ønskede tjeneste	f) udbyderen skal være udstyret med den nødvendige hardware og software til at understøtte den ønskede tjeneste ***og skal opfylde kravene i artikel X i forordning XX/XXXX (forordningen om cyberrobusthed)***

Ændringsforslag 58

Forslag til forordning
Artikel 16 – stk. 2 – litra j a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ja) ingen udbyder med oprindelse i et højrisikotredjeland kan accepteres

Ændringsforslag 59

Forslag til forordning
Artikel 16 – stk. 2 – litra j b (nyt)

Kommissionens forslag	*Ændringsforslag*

	jb) udbyderen skal samarbejde tæt med relevante SMV'er, hvor det er muligt

Ændringsforslag 60

Forslag til forordning
Artikel 17 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom.	1. Tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis***:***
	a) de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom
	b) de tredjelande, hvortil der er udsendt en FSFP-mission med et specifikt mandat til at styrke modstandsdygtigheden over for hybride trusler, herunder cybertrusler, eller hvor der er indført en bistandsforanstaltning inden for rammerne af den europæiske fredsfacilitet for at styrke landets cyberrobusthed.

Ændringsforslag 61

Forslag til forordning
Artikel 17 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Støtte fra EU's cybersikkerhedsreserve er i overensstemmelse med denne forordning og opfylder eventuelle specifikke betingelser, der er fastsat i de associeringsaftaler, der er omhandlet i stk. 1.	2. Støtte fra EU's cybersikkerhedsreserve er i overensstemmelse med denne forordning og opfylder eventuelle specifikke betingelser, der er fastsat i de associeringsaftaler, der er omhandlet i stk. 1***, undtagen for de tredjelande, der er omfattet af bestemmelserne i stk. 1, litra***

b).

Ændringsforslag 62

Forslag til forordning
Artikel 18 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Efter anmodning fra Kommissionen, EU-CyCLONe eller CSIRT-netværket gennemgår og vurderer ENISA trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. Efter afsluttet gennemgang og vurdering af en hændelse fremsender ENISA en rapport om hændelsen til CSIRT-netværket, EU-CyCLONe og Kommissionen som støtte til udførelsen af deres opgaver, navnlig opgaver i henhold til artikel 15 og 16 i direktiv (EU) 2022/2555. Hvis det er relevant, videresender Kommissionen rapporten med den højtstående repræsentant.	1. Efter anmodning fra Kommissionen, EU-CyCLONe eller CSIRT-netværket gennemgår og vurderer ENISA trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. Efter afsluttet gennemgang og vurdering af en hændelse fremsender ENISA en rapport om hændelsen til CSIRT-netværket, EU-CyCLONe og Kommissionen som støtte til udførelsen af deres opgaver, navnlig opgaver i henhold til artikel 15 og 16 i direktiv (EU) 2022/2555. Hvis det er relevant, ***navnlig når hændelsen vedrører et tredjeland,*** videresender Kommissionen rapporten til den højtstående repræsentant ***og EU-Udenrigstjenesten***.

Ændringsforslag 63

Forslag til forordning
Artikel 18 – stk. 3 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	3a. Rapporten deles med Europa-Parlamentet i overensstemmelse med EU-retten eller national ret om beskyttelse af følsomme klassificerede oplysninger.

Ændringsforslag 64

Forslag til forordning
Artikel 19 – stk. 1 – nr. 1 – litra a – punkt 1

Forordning (EU) 2021/694.
Artikel 6 – stk. 1

Kommissionens forslag	*Ændringsforslag*
aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af nationale og grænseoverskridende SOC-platforme, der bidrager til et øget situationskendskab i Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler".	aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af nationale og grænseoverskridende SOC-platforme, der bidrager til et øget situationskendskab i Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler ***og mindske Unionens afhængighed af højrisikoleverandører af kritisk udstyr eller kritiske komponenter til cybersikkerhed, der ville handle i modstrid med Unionens og dens medlemsstaters sikkerheds- og forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU***".

Ændringsforslag 65

Forslag til forordning
Artikel 20 – stk. 1

Kommissionens forslag	*Ændringsforslag*
Senest [***fire*** år efter datoen for denne forordnings anvendelse] forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning.	Senest [***tre*** år efter datoen for denne forordnings anvendelse ***og hvert andet år derefter***] forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning.

PROCEDURE I RÅDGIVENDE UDVALG

Titel	Foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
Referencer	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Korresponderende udvalg Dato for vedtagelse	ITRE 1.6.2023
Udtalelse fra Dato for vedtagelse	AFET 1.6.2023
Ordfører for udtalelse Dato for valg	Dragoş Tudorache 16.6.2023
Behandling i udvalg	18.9.2023
Dato for vedtagelse	24.10.2023
Resultat af den endelige afstemning	+: 39 –: 4 0: 0
Til stede ved den endelige afstemning – medlemmer	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Til stede ved den endelige afstemning - stedfortrædere	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

ENDELIG AFSTEMNING VED NAVNEOPRÅB
I RÅDGIVENDE UDVALG

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller

25.10.2023

UDTALELSE FRA TRANSPORT- OG TURISMEUDVALGET

til Udvalget om Industri, Forskning og Energi

om forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Ordfører for udtalelse: Gheorghe Falcă

KORT BEGRUNDELSE

Organisationer, der er berørt af cyberangreb, herunder i transportsektoren, indberetter dem sjældent, navnlig virksomheder i den private sektor, da de ofte ser dem som "dårlig reklame". De fleste organisationer foretrækker at tage sig af dem internt, og det er ofte gerningsmændene, der offentliggør dem. I EU er den gode nyhed, at ikrafttrædelsen af direktiv 2022/2555 om netsikkerhed (kendt som "NIS2-direktivet"), som medlemsstaterne har indtil oktober 2024 til at gennemføre, harmoniserer forpligtelserne til indberetning af hændelser i medlemsstaterne. Det er derfor sandsynligt, at der i de kommende år vil opstå en bedre forståelse af problemets art og omfang.

Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) offentliggjorde en nylig rapport1, der indeholder oplysninger om cybersikkerhedstrusler i transportsektoren, hvor det understreger, at cyberkriminelle var ansvarlige for mere end halvdelen af de hændelser, der blev observeret i rapporteringsperioden 2022 (55 %), og at den vigtigste årsag til disse angreb var økonomisk gevinst. Det noterede sig også, at de fleste cyberangreb i transportsektoren er rettet mod IT-systemer, hvilket forårsager driftsforstyrrelser.

Med hensyn til beredskab og reaktion på cybersikkerhedshændelser er der i øjeblikket begrænset støtte på EU-niveau og begrænset solidaritet mellem medlemsstaterne. I Rådets konklusioner fra maj 2022 blev behovet fremhævet for at afhjælpe disse mangler ved at opfordre Kommissionen til at forelægge et forslag om en ny **beredskabsfond for cybersikkerhed**[2].

Med denne forordning gennemføres **EU's strategi for cybersikkerhed**, der blev vedtaget i december 2020, og som omfatter oprettelse af et **europæisk cyberskjold**, der styrker

[1] "Understanding Cyber Threats in Transport", ENISA, offentliggjort den 21. marts 2023.
[2] Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition af 23. maj 2022 (9364/22)

kapaciteten til at opdage og udveksle oplysninger om cybertrusler i Den Europæiske Union gennem en sammenslutning af nationale og grænseoverskridende sikkerhedsoperationscentre (SOC'er). Foranstaltningerne i denne forordning støttes med **finansiering under den strategiske målsætning "cybersikkerhed" i programmet for et digitalt Europa**.

Det samlede budget omfatter en forhøjelse på 100 mio. EUR, som i denne forordning foreslås omfordelt fra andre strategiske målsætninger for programmet for et digitalt Europa. Dermed bringes det nye samlede beløb, der er til rådighed til cybersikkerhedsforanstaltninger under programmet for et digitalt Europa, op på 842,8 mio. EUR.

En del af de supplerende 100 mio. EUR skal gå til at øge det budget, der forvaltes af Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC), med henblik på at gennemføre foranstaltninger vedrørende SOC'er og beredskab som led i deres arbejdsprogram(mer). Desuden vil den supplerende finansiering indgå som støtte til oprettelse af EU's cybersikkerhedsreserve. Den ekstra finansiering supplerer det budget, der allerede er afsat til lignende foranstaltninger i det primære arbejdsprogram for programmet for et digitalt Europa og arbejdsprogrammet for cybersikkerhed for perioden 2023-2027, hvilket bringer det samlede beløb op på 551 mio. for perioden 2023-2027, mens 115 mio. allerede var afsat i form af pilotprojekter i perioden 2021-2022. Når medlemsstaternes bidrag medregnes, kan det samlede budget blive på 1 109 mia. euro.

Ordførerens holdning

Ordføreren glæder sig over det nye forslag og mener, at det vil medføre betydelige fordele for de forskellige interessenter. Ordføreren understreger behovet for en dybere forståelse af cybersikkerhedsbehovene og -kravene i forbindelse med transport samt for at give kritiske transportenheder adgang til passende finansiering til beredskab, reaktion og løsning af hændelser.

Ordføreren støtter "værktøjskassen til cybersikkerhed på transportområdet", som har til formål at bidrage til større cyberbevidsthed og cyberhygiejne med særligt fokus på transportsektoren. Den er rettet mod transportorganisationer, uanset deres størrelse og aktivitetsområde, og der tages hensyn til kritisk transportinfrastruktur og militær mobilitet, navnlig i betragtning af krigen i Ukraine, navnlig, men ikke begrænset til:

- Luftfartsselskaber, lufthavnsdriftsorganer, centrale lufthavne, lufttrafikstyring og flyvekontrolcentre, Den Europæiske Unions Luftfartssikkerhedsagentur og Eurocontrol;
- Infrastrukturforvaltere, jernbanevirksomheder og det europæiske jernbanetrafikstyringssystem (ERTMS);
- Virksomheder, der udfører passager- og godstransport ad indre vandveje, sø- og kystfart, havneforvaltningsorganer, herunder deres havnefaciliteter, enheder, der driver arbejder og udstyr i havne, og operatører af skibstrafiktjenester;
- Vejmyndigheder med ansvar for trafikstyringskontrol, operatører af intelligente transportsystemer;
- Post- og kurérvirksomhed.

Ordføreren mener, at størrelsen af budgettet til driften af **Beredskabsfonden for Cybersikkerhed** (ERFC) vil være afgørende for dens succes. Den bør derfor være tilstrækkelig stor til styrke medlemsstaternes evne til at **forberede sig og reagere på** væsentlige eller omfattende cybersikkerhedshændelser **og sikre en genopretning**. Støtte til reaktioner på hændelser skal også stilles til rådighed for EU's institutioner, organer, kontorer og agenturer.

Det **europæiske cyberskjold** forbedrer medlemsstaternes kapacitet til at afsløre cybertrusler. **Cyberberedskabsmekanismen** supplerer medlemsstaternes foranstaltninger gennem nødhjælp til beredskab, indsats og øjeblikkelig genopretning/genetablering af væsentlige tjenesters funktion.

ÆNDRINGSFORSLAG

Transport- og Turismeudvalget opfordrer Udvalget om Industri, Forskning og Energi, som er korresponderende udvalg, til at tage hensyn til følgende:

Ændringsforslag 1

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage, ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande.	(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage, ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion ***samt kritisk IT-infrastruktur og fysisk infrastruktur***. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester***, at offentlig og privat transport*** og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi ***samt på mobiliteten inden for Unionen*** og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi

de forekommer samtidig eller spredes hurtigt til mange lande.

Ændringsforslag 2

Forslag til forordning
Betragtning 2 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(2a) Transportsektoren står over for en stadig mere alvorlig cybersikkerhedstrussel fra statsstøttede aktørers, cyberkriminelles og hacktivisters side rettet mod myndigheder, operatører, producenter, leverandører og tjenesteudbydere inden for luftfart, søtransport, jernbanetransport og vejtransport. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) har observeret en stigning på 25 % i det månedlige gennemsnitlige antal indberettede hændelser, der påvirkede transportsektoren i 2022, sammenlignet med niveauet i 2021. Størstedelen af angrebene på transportsektoren er rettet mod informationsteknologisystemer (IT-systemer), og der kan opstå driftsforstyrrelser som følge heraf[14a].
	[14b] ENISA (2023), ENISA's Trusselsbillede: Transportsektoren, s. 7 og 17

Ændringsforslag 3

Forslag til forordning
Betragtning 2 b (ny)

Kommissionens forslag	*Ændringsforslag*
	(2b) Ruslands uprovokerede invasion af Ukraine medførte en betydelig stigning i antallet af cybersikkerhedshændelser, herunder distributed denial of service-cyberangreb (DDoS-cyberangreb) rettet

mod transportsektoren i EU og områder tæt på EU, hovedsagelig lufthavne, jernbaner og transportmyndigheder[14b]. Denne stigning i antallet af angreb vil højst sandsynligt fortsætte.

[14b] ENISA (2023), ENISA's Trusselsbillede: Transportsektoren, s. 9.

Ændringsforslag 4

Forslag til forordning
Betragtning 2 c (ny)

Kommissionens forslag	*Ændringsforslag*
	(2c) Cyberangreb er rettet mod myndigheder og organer i alle transportdelsektorer og påvirker jernbanevirksomheder og infrastrukturforvaltere samt havneoperatører. For så vidt angår vejsektoren var cyberangrebene rettet mod originaludstyrsfabrikanter (OEM'er), leverandører og tjenesteudbydere sammen med operatører af offentlig transport. I luftfartssektoren var de vigtigste mål luftfartsselskaber og lufthavnsoperatører efterfulgt af tjenesteudbydere, operatører af overfladetransport og forsyningskæden[14c].

[14c] ENISA (2023), ENISA's Trusselsbillede: Transportsektoren, s. 17

Ændringsforslag 5

Forslag til forordning
Betragtning 3

Kommissionens forslag	*Ændringsforslag*
(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af	(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af

hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[16] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der driver kritisk infrastruktur, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser.

[16] https://futureu.europa.eu/da/

hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[16] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder***, transportoperatører*** og enheder, der driver kritisk infrastruktur, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser ***samt om tilstanden og udviklingen på arbejdsmarkedet for cybersikkerhed, da det spiller en afgørende rolle med hensyn til at tilvejebringe de nødvendige opdagelses- og beredskabstjenester***.

[16] https://futureu.europa.eu/da/

Ændringsforslag 6

Forslag til forordning
Betragtning 4

Kommissionens forslag	*Ændringsforslag*
(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og	(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og

Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20] ***samt forslaget til forordning om retningslinjer for udvikling af det transeuropæiske transportnet og forslaget til forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed)***. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

---

[17] 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 (EUT L 333 af 27.12.2022).

[18] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[19] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

[20] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi

[17] 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 (EUT L 333 af 27.12.2022).

[18] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[19] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

[20] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi

og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).	og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

Ændringsforslag 7

Forslag til forordning
Betragtning 4 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(4a) Transportoperatørerne glæder sig over Kommissionens værktøjskasse til cybersikkerhed på transportområdet[2a], som indeholder grundlæggende oplysninger om trusler, der kan påvirke transportorganisationer (spredning af malware, denial of service, uautoriseret adgang og tyveri og softwaremanipulation), og som indeholder en liste over god praksis for afbødning, men de bør imidlertid have passende uddannelse i cybersikkerhed og passende værktøjer til at forebygge cybertrusler. Unionens budget bør også dække den støtte såsom uddannelse, der ydes af ENISA, for at gøre det muligt for transportoperatører effektivt at gennemføre bedste praksis for afbødning, der indgår i værktøjskassen.
	1a ENISA's Trusselsbillede: transportsektoren/ENISA, marts 2023
	[2a] Europa-Kommissionen (2021). Værktøjskasse til cybersikkerhed inden for transport, tilgængelig på https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Ændringsforslag 8

Forslag til forordning
Betragtning 4 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(4a) En EU-dækkende koordineret tilgang til at styrke beredskabet og modstandsdygtigheden for kritisk infrastruktur såsom transportinfrastruktur er baseret på medlemsstaternes kapacitetsopbygning. Som det anerkendes i den nylige meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om "Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed"19a, kan EU's sikkerhed ikke garanteres uden EU's mest værdifulde aktiv: befolkningerne
	[19a] Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet med titlen "Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer")" COM(2023) 207 final.

Ændringsforslag 9

Forslag til forordning
Betragtning 12

Kommissionens forslag	*Ændringsforslag*
(12) For mere effektivt at forebygge, vurdere og reagere på cybertrusler og -hændelser er det nødvendigt at opbygge en mere omfattende viden om truslerne mod kritiske aktiver og infrastrukturer på Unionens område, herunder geografiske fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer. Der bør etableres en omfattende infrastruktur af SOC'er i EU ("det europæiske cyberskjold") bestående af flere interoperable grænseoverskridende platforme, som hver samler en række	(12) For mere effektivt at forebygge, vurdere og reagere på cybertrusler og -hændelser er det nødvendigt at opbygge en mere omfattende viden om truslerne mod kritiske aktiver og infrastrukturer på Unionens område, herunder geografiske fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer. ***Disse kritiske aktiver og infrastrukturer omfatter intelligente transportsystemer, der, samtidig med at de er væsentlige for automatiseret og multimodal mobilitet, fungerer på grundlag af afgørende***

nationale SOC'er. Infrastrukturen bør tjene nationale og europæiske cybersikkerhedsinteresser og -behov. Den nyeste teknologi til avancerede dataindsamlings- og analyseværktøjer bør udnyttes, cyberdetektions- og -forvaltningskapaciteten bør udnyttes, og et situationskendskab i realtid bør opbygges. Infrastrukturen skal forbedre afsløring af cybersikkerhedstrusler og -hændelser og dermed supplere og støtte Unionens enheder og netværk med ansvar for krisestyring i Unionen, navnlig EU-netværket af forbindelsesorganisationer for cyberkriser ("EU-CyCLONe") som defineret i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[24].

udvekslinger af følsomme data. Der bør etableres en omfattende infrastruktur af SOC'er i EU ("det europæiske cyberskjold") bestående af flere interoperable grænseoverskridende platforme, som hver samler en række nationale SOC'er. Infrastrukturen bør tjene nationale og europæiske cybersikkerhedsinteresser og -behov. Den nyeste teknologi til avancerede dataindsamlings- og analyseværktøjer bør udnyttes, cyberdetektions- og -forvaltningskapaciteten bør udnyttes, og et situationskendskab i realtid bør opbygges. Infrastrukturen skal forbedre afsløring af cybersikkerhedstrusler og -hændelser og dermed supplere og støtte Unionens enheder og netværk med ansvar for krisestyring i Unionen, navnlig EU-netværket af forbindelsesorganisationer for cyberkriser ("EU-CyCLONe") som defineret i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[24].

[24] 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).

[24] 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).

Ændringsforslag 10

Forslag til forordning
Betragtning 14 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(14a) Transportsektoren er i stigende grad ved at blive et af de mest lukrative erhverv for cyberkriminelle, idet kundedata betragtes som en meget værdifuld råvare, og transportforsyningskæden bliver mere og

mere et mål herfor. Derfor bør transportinfrastruktur, der er kendetegnet ved en grænseoverskridende karakter eller ved udveksling af data ved hjælp af trådløse teknologier, betragtes som et centralt mål for analyse og overvågning for både nationale og navnlig for grænseoverskridende SOC'er. For eksempel kræver det nylige forslag om revision af TEN-T-forordningen større solidaritet og samarbejde om udveksling af oplysninger om grænseoverskridende cybertrusler, som dette tværnationale netværk kan stå over for. Tilsvarende er intelligente transportsystemer (ITS) afgørende for at gøre transporten sikrere, mere effektiv og bæredygtig, men de gør transportsystemerne mere sårbare over for cyberangreb, der kan forårsage ulykker, trafikpropper eller økonomiske tab for både private og offentlige operatører. For at beskytte passagerernes sikkerhed, sikre beskyttelsen af brugernes og udbydernes data og for at undgå økonomiske skader er det vigtigt, at gennemførelsesprogrammet for det reviderede direktiv om intelligente transportsystemer indeholder bestemmelser og værktøjer til at styrke samarbejdet mellem medlemsstaterne om at opdage, forberede sig på og reagere på cybersikkerhedstrusler og -hændelser.

Ændringsforslag 11

Forslag til forordning
Betragtning 15

Kommissionens forslag	*Ændringsforslag*
(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv (EU) 2022/2555. De grænseoverskridende	(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv (EU) 2022/2555. De grænseoverskridende

SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og teknologiske suverænitet.	SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og teknologiske suverænitet. ***For at styrke Unionens autonomi på cyberområdet og med henvisning til artikel 47, stk. 4, i forslaget til forordning om retningslinjer for udvikling af det transeuropæiske transportnet (COM(2021)0812) er det i denne forbindelse også nødvendigt at forhindre adgang til data, der fører til cybertrusler, ved at håndhæve en robust lovgivningsmæssig ramme, der regulerer udenlandsk ejerskab og udenlandske investeringer i kritisk infrastruktur, f.eks. inden for transport.***

Ændringsforslag 12

Forslag til forordning
Betragtning 21

Kommissionens forslag	*Ændringsforslag*
(21) Selv om det europæiske cyberskjold er et civilt projekt, kan cyberforsvarssektoren udnytte et større civilt situationskendskab og en stærkere civil detektionskapacitet, der er udviklet med henblik på beskyttelse af kritisk infrastruktur. Grænseoverskridende SOC'er bør med støtte fra Kommissionen og Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") og i samarbejde med Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") gradvist udvikle særlige protokoller og standarder for at muliggøre samarbejde med cyberforsvarssektoren, herunder kontrol sikkerhedsforhold. Udviklingen af det europæiske cyberskjold bør ledsages af overvejelser om at muliggøre et fremtidigt	(21) Selv om det europæiske cyberskjold er et civilt projekt, kan cyberforsvarssektoren udnytte et større civilt situationskendskab og en stærkere civil detektionskapacitet, der er udviklet med henblik på beskyttelse af kritisk infrastruktur. Grænseoverskridende SOC'er bør med støtte fra Kommissionen og Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") og i samarbejde med Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") gradvist udvikle særlige protokoller og standarder for at muliggøre samarbejde med cyberforsvarssektoren, herunder kontrol sikkerhedsforhold. Udviklingen af det europæiske cyberskjold bør ledsages af overvejelser om at muliggøre et fremtidigt

samarbejde med de netværk og platforme, der har ansvar for informationsudveksling i cyberforsvarssektoren, i tæt samarbejde med den højtstående repræsentant.	samarbejde med de netværk og platforme, der har ansvar for informationsudveksling i cyberforsvarssektoren, i tæt samarbejde med den højtstående repræsentant. ***Det bør også muliggøre synergier med handlingsplanen for militær mobilitet 2.0. Et velfungerende militært mobilitetsnetværk skal være modstandsdygtigt, herunder i forbindelse med cybertrusler og andre hybride trusler, der kan påvirke kritiske knudepunkter i transportsystemet med dobbelt anvendelse. kan et cyberangreb på systemer, der anvendes i lufthavne, havne eller jernbaner, eller et cyberangreb på militære aktiver få store konsekvenser. Digitalisering af processer og procedurer, herunder med henblik på det nødvendige civile og militære samarbejde, vil derfor kræve en styrkelse af computerinformationssystemer (CIS'er) mod cybertrusler.***

Ændringsforslag 13

Forslag til forordning
Betragtning 21 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(21a) I tilfælde af en cybersikkerhedskrise er en effektiv udveksling af oplysninger afgørende for at sikre situationskendskab blandt de militære og civile transportsektorer. Denne udveksling af oplysninger bør også stimulere samarbejdet mellem relevante sektormyndigheder med ansvar for transport, kompetente cybersikkerhedsmyndigheder, SOC'er og CSIRT'er.

Ændringsforslag 14

Forslag til forordning
Betragtning 29

Kommissionens forslag	*Ændringsforslag*
(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital	(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). ***Der bør lægges særlig vægt på transportsektoren og dens delsektorer (luft-, jernbane-, vand- og vejtransport), da de omfatter kritisk infrastruktur, hvor cyberhændelser og -angreb i alvorlig grad kan undergrave passagerernes og operatørernes sikkerhed.*** De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde

operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[29]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[29]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

[29] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

[29] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

Ændringsforslag 15

Forslag til forordning
Betragtning 30 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(30a) Med henblik på sektorens kritiske karakter og konsekvenserne af cybertrusler for mobiliteten og som følge heraf for passagerers og fodgængeres liv bør transportsektoren prioriteres med hensyn til koordineret beredskabstest af enheder.

Ændringsforslag 16

Forslag til forordning
Betragtning 35 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(35a) I betragtning af ENISA's øgede

	opgaver og ansvarsområder på grundlag af dette forslag og forslaget om forordningen om cyberrobusthed er det nødvendigt at vedtage ENISA's ændringsbudget nr. 1/2022 for pilotgennemførelsen af en støtteforanstaltning for cybersikkerhed. I betragtning af Unionens interesser bør ENISA desuden tildeles yderligere finansielle og menneskelige ressourcer.

Ændringsforslag 17

Forslag til forordning
Betragtning 38 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(38a) Udviklingen af færdigheder og kompetencer bør derfor have en central placering på tværs af alle sektorer, ikke mindst dem, der er sårbare over for cybersikkerhedstrusler, såsom personale, der arbejder med massetransit eller kritiske infrastrukturer, herunder togkontrolsystemer og digitale transportplanlægningsværktøjer for alle transportformer. Indførelsen og videreudviklingen af cybersikkerhedskulturen er derfor afgørende for en vellykket gennemførelse af denne forordning for både borgernes bevidsthed og ekspertviden på tværs af alle sektorer for kritisk infrastruktur.

Ændringsforslag 18

Forslag til forordning
Artikel 1 – stk. 2 – litra a

Kommissionens forslag	*Ændringsforslag*
a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og dermed gøre det muligt at styrke industriens og servicesektorernes	a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og dermed gøre det muligt at styrke industriens***, transportinfrastrukturernes***

konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet

og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet

Ændringsforslag 19

Forslag til forordning
Artikel 1 – stk. 2 – litra b

Kommissionens forslag	*Ændringsforslag*
b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa	b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, ***med særlig vægt på kritisk IT-infrastruktur og fysisk infrastruktur,*** herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa

Ændringsforslag 20

Forslag til forordning
Artikel 1 – stk. 2 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	ca) at styrke Unionens beredskab, samarbejde og effektivitet med hensyn til at beskytte transportinfrastruktur og -tjenester i medlemsstaterne mod cybersikkerhedshændelser, sikre transportsektorens fortsatte funktion, forsyningskædernes integritet og mobilitet i hele Unionen.

Ændringsforslag 21

Forslag til forordning
Artikel 3 – stk. 2 – afsnit 1 – litra c

Kommissionens forslag	*Ændringsforslag*
c) bidrage til bedre beskyttelse mod og reaktion på cybertrusler	c) bidrage til bedre beskyttelse mod og reaktion på cybertrusler***, herunder for transportinfrastruktur, der er kendetegnet ved en grænseoverskridende karakter, såsom TEN-T, eller ved dataudveksling gennem trådløse teknologier såsom intelligente transportsystemer.***

Ændringsforslag 22

Forslag til forordning
Artikel 3 – stk. 2 – afsnit 2

Kommissionens forslag	*Ændringsforslag*
Det europæiske cyberskjold udvikles i samarbejde med den paneuropæiske højtydende databehandlingsinfrastruktur, der er etableret i henhold til forordning (EU) 2021/1173.	Det europæiske cyberskjold udvikles i samarbejde med den paneuropæiske højtydende databehandlingsinfrastruktur, der er etableret i henhold til forordning (EU) 2021/1173. ***Det skal muliggøre samarbejde via særlige protokoller og standarder med cyberforsvarssektoren for at sikre udviklingen af stærkere civilt situationskendskab og civil kapacitet til at opdage hændelser til beskyttelse af kritisk infrastruktur. I den forbindelse skal der også udvikles synergier med handlingsplanen for militær mobilitet 2.0, og der skal sikres en effektiv udveksling af oplysninger for at skabe situationskendskab blandt de militære og civile transportsektorer.***

Ændringsforslag 23

Forslag til forordning
Artikel 8 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. Kommissionen inddrager det europæiske cyberskjold, navnlig de grænseoverskridende SOC'er, i sin udtalelse til medlemsstaterne inden for rammerne af forslaget til forordning om

	det transeuropæiske transportnet (COM(2021)0812), når deltagelse af eller bidrag af enhver art fra en fysisk person fra et tredjeland eller en virksomhed i et tredjeland sandsynligvis vil påvirke cybersikkerheden i forbindelse med grænseoverskridende kritisk infrastruktur såsom TEN-T.

Ændringsforslag 24

Forslag til forordning
Artikel 10 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU	a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU***, med særlig vægt på transportinfrastrukturen og dens delsektorer, der er omfattet af bilag I til direktiv (EU) 2022/255***

Ændringsforslag 25

Forslag til forordning
Artikel 18 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Ved udarbejdelse af den i stk. 1 omhandlede rapport om gennemgang af en hændelse samarbejder ENISA med alle relevante interessenter, herunder repræsentanter for medlemsstaterne, Kommissionen, andre relevante EU-institutioner, -organer og -agenturer, udbydere af administrerede sikkerhedstjenester og brugere af cybersikkerhedstjenester. Hvor det er relevant, samarbejder ENISA også med enheder, der er berørt af væsentlige eller omfattende cybersikkerhedshændelser. Som støtte for gennemgangen kan ENISA også høre andre typer interessenter. De hørte repræsentanter skal oplyse om	2. Ved udarbejdelse af den i stk. 1 omhandlede rapport om gennemgang af en hændelse samarbejder ENISA med alle relevante interessenter, herunder repræsentanter for medlemsstaterne, Kommissionen, andre relevante EU-institutioner, -organer og -agenturer, udbydere af administrerede sikkerhedstjenester og brugere af cybersikkerhedstjenester. Hvor det er relevant, samarbejder ENISA også med enheder, der er berørt af væsentlige eller omfattende cybersikkerhedshændelser***, herunder transportoperatører***. Som støtte for gennemgangen kan ENISA også høre andre typer interessenter. De hørte

eventuelle interessekonflikter.	repræsentanter skal oplyse om eventuelle interessekonflikter.

Ændringsforslag 26

Forslag til forordning
Artikel 19 – stk. 1 – nr. 1 – litra b
Forordning (EU) 2021/694
Artikel 6 – stk. 2 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	2a. I betragtning af Unionens interesser i forbindelse med dens ansvar for udarbejdelse af forslag til certificeringsordninger i henhold til forordning (EU) 2019/881, dens ansvar for at gennemgå og vurdere cybertrusler, sårbarheder og afbødning, udarbejde en rapport om gennemgang af hændelser i forbindelse med mekanismen til evaluering af cybersikkerhedshændelser samt uddanne operatører af kritisk infrastruktur i bekæmpelse af cyberangreb og -hændelser, og i lyset af dens nyligt tildelte ansvarsområder inden for rammerne af forslaget om forordningen om cyberrobusthed tildeles ENISA de nødvendige ressourcer under EU-budgettet i overensstemmelse med gældende lovgivning.

Ændringsforslag 27

Forslag til forordning
Artikel 19 – stk. 1 – nr. 1 a (nyt)
Forordning (EU) 2021/694
Artikel 7 – stk. 1 – litra c a (nyt)

Kommissionens forslag	*Ændringsforslag*
	1a) Artikel 7 ændres således:
	a) Stk. 1 ændres således:
	1) Følgende indsættes som litra a a):
	ca) understøtte uddannelse af høj kvalitet til transportvirksomheder og ledere og

arbejdsstyrke inden for kritisk transportinfrastruktur, også med henblik på effektivt at dele og gennemføre afbødende praksisser over for cyberangreb eller -hændelser på kritisk infrastruktur såsom dem, der leveres af værktøjskassen til cybersikkerhed på transportområdet.

PROCEDURE I RÅDGIVENDE UDVALG

Titel	Foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser
Referencer	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Korresponderende udvalg Dato for meddelelse på plenarmødet	ITRE 1.6.2023
Udtalelse fra Dato for meddelelse på plenarmødet	TRAN 1.6.2023
Rådgivende ordfører Dato for valg	Gheorghe Falcă 7.7.2023
Dato for vedtagelse	25.10.2023
Resultat af den endelige afstemning	+: 38 –: 0 0: 0
Til stede ved den endelige afstemning – medlemmer	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Til stede ved den endelige afstemning - stedfortrædere	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

ENDELIG AFSTEMNING VED NAVNEOPRÅB
I RÅDGIVENDE UDVALG

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller

PROCEDURE I KORRESPONDERENDE UDVALG

Titel	Fastsættelse af foranstaltninger til ta styrke solidariteten og kapaciteten i Unionen til at opdage, forberede sig på og reagere på cybersikkerhedstusler og -hændelser			
Referencer	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Dato for forelæggelse for EP	19.4.2023			
Korresponderende udvalg Dato for meddelelse på plenarmødet	ITRE 1.6.2023			
Rådgivende udvalg Dato for meddelelse på plenarmødet	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Ingen udtalelse Dato for afgørelse	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Ordførere Dato for valg	Lina Gálvez Muñoz 2.5.2023			
Behandling i udvalg	19.9.2023			
Dato for vedtagelse	7.12.2023			
Resultat af den endelige afstemning	+: –: 0:	43 10 1		
Til stede ved den endelige afstemning – medlemmer	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Til stede ved den endelige afstemning – stedfortrædere	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Til stede ved den endelige afstemning – stedfortrædere (forretningsordenens art. 209, stk. 7)	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Dato for indgivelse	8.12.2023			

ENDELIG AFSTEMNING VED NAVNEOPRÅB I KORRESPONDERENDE UDVALG

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller