Europa-Parlamentet
2019-2024

Udvalget om Industri, Forskning og Energi

2023/0109(COD)

22.9.2023

ÆNDRINGSFORSLAG
46 - 216

Udkast til betænkning
Lina Gálvez Muñoz
(PE752.795v01-00)

Foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser

Forslag til forordning
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Ændringsforslag 46
Evžen Tošenovský

Forslag til forordning
Afsnit 1

Kommissionens forslag	*Ændringsforslag*
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	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 ***(forordningen om cybersolidaritet)***

Or. en

Ændringsforslag 47
Ville Niinistö
for Verts/ALE-Gruppen

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 ***og sårbarheder*** i alle sektorer af økonomien, da offentlige forvaltninger, virksomheder og borgere mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden.

Or. en

Begrundelse

Behovet for denne lovtekst opstår som følge af, at der med grundlæggende afhængigheder også kommer sårbarheder.

Ændringsforslag 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu

Buşoi, Ioan-Rareş Bogdan

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. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på 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, 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. ***Derfor er et tæt og koordineret samarbejde mellem den offentlige sektor, den private sektor, medlemsstaterne, EU-institutionerne eller -agenturerne og den akademiske verden nødvendigt for at forbedre Unionens sikkerhedsstatus. Unionens reaktion bør ske i samarbejde med betroede og ligesindede internationale partnere og***

internationale institutioner og i overensstemmelse med internationale samarbejdsrammer og internationale aftaler.

Or. en

Ændringsforslag 49
Ville Niinistö
for Verts/ALE-Gruppen

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	(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 ***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.

til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande.

Or. en

Begrundelse

Den generelle inddragelse af hacktivisme sammen med kriminelle aktiviteter afspejler ikke forskelligartetheden i sådanne aktiviteter, herunder legitime protester og whistleblowing. Teksten vil have gavn af at undgå uklarheder og beskytte legitime aktiviteter.

Ændringsforslag 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

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 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.	(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 er der behov for at øge modstandsdygtigheden hos borgere, virksomheder***, herunder mikrovirksomheder, små og mellemstore virksomheder (SMV'er)*** og enheder, der driver kritisk infrastruktur***, herunder lokale eller regionale myndigheder***, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer***,*** tjenester ***og højt kvalificeret personale med de nødvendige færdigheder***, 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***, også gennem proaktiv indsamling af efterretninger***. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser. ***[1] https://futureu.europa.eu/da/***

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

Or. en

Ændringsforslag 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 5

Kommissionens forslag	*Ændringsforslag*
(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, forberede sig ***og*** reagere på 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 [21] .	(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, forberede sig***,*** 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 [21].
[21] Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, som blev godkendt af Rådet på samlingen den 23. maj 2022 (9364/22)	[21] Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, som blev godkendt af Rådet på samlingen den 23. maj 2022 (9364/22)

Or. en

Ændringsforslag 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 9 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(9a) I lyset af den geopolitiske udvikling og den stigende trussel på cyberområdet er kontinuiteten og videreudviklingen af de foranstaltninger, der er fastsat i denne forordning, især det europæiske cyberskjold og den europæiske beredskabsmekanisme, vigtig. Det er derfor nødvendigt at sikre en specifik budgetpost i den flerårige finansielle ramme for 2028-2034. Medlemsstaterne bør også forpligte sig til at støtte alle nødvendige foranstaltninger for at styrke solidariteten inden for Unionen og reducere cybertrusler og -hændelser i hele Unionen.

Or. en

Ændringsforslag 53
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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 geografiske fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer***, herunder ved at indsamle proaktive efterretninger***. Der bør etableres

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] .	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. ***En national SOC er en centraliseret kapacitet, der er ansvarlig for løbende at indsamle trusselsoplysninger og forbedre sikkerhedsstatussen for enheder under national jurisdiktion ved at forebygge, opdage og analysere cybersikkerhedstrusler.*** 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).***
	Or. en

Ændringsforslag 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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) ***For at kunne deltage i det europæiske cyberskjold bør*** de enkelte medlemsstater udpege et offentligt organ på nationalt plan, der har til opgave at koordinere aktiviteter til afsløring ***og informationsudveksling*** af cybertrusler i den pågældende medlemsstat. ***Medlemsstaterne opfordres på det kraftigste til at indarbejde den nationale kapacitet for SOC i deres allerede eksisterende cyberstruktur og -styring for ikke at skabe yderligere styringslag og til at tilpasse loven om cybersolidaritet til allerede eksisterende lovgivning, herunder direktiv (EU) 2022/2555.*** Disse nationale sikkerhedsoperationscentre (SOC'er) bør fungere som reference- og indgangspunkt på nationalt plan for ***private og offentlige enheders*** deltagelse***, navnlig deres SOC'er,*** 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 nuværende 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 for at styrke Unionens modstandsdygtighed på cybersikkerhedsområdet.***

Or. en

Ændringsforslag 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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, 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 ***proaktive*** 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 grænseoverskridende SOC'er bør lette og tilskynde til udveksling af oplysninger i et betroet og sikkert miljø. ENISA bør støtte grænseoverskridende SOC'er i spørgsmål vedrørende operationelt samarbejde.*** De bør stille ny supplerende kapacitet til rådighed, ***samtidig med at de indarbejdes i den allerede*** eksisterende ***cybersikkerhedsinfrastruktur, herunder*** SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.

Or. en

Ændringsforslag 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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.	(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 indarbejdet i den allerede eksisterende cybersikkerhedsinfrastruktur, navnlig*** CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder***, navnlig deres SOC'er***, 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 modstandsdygtighed***.

Or. en

Ændringsforslag 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra	(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***.	offentlige og private enheder, værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af ***et betydeligt cybersikkerhedsøkosystem med stærke EU-kapaciteter*** og ***samarbejde med ligesindede partnere***.

Or. en

Ændringsforslag 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***for at fremme opløsningen af de nuværende eksisterende kommunikationssiloer***. ***I den forbindelse kan grænseoverskridende SOC'er også støtte oprettelsen af dataudvekslingsmodeller i hele Unionen.*** De oplysninger, der udveksles mellem deltagerne i en grænseoverskridende SOC, kan omfatte data fra netværk og sensorer, trusselsefterretningsfeeds***, herunder indsamling af proaktive efterretninger***, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, trusler og sårbarheder. Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre

grænseoverskridende SOC'er.

Or. en

Ændringsforslag 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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). De oplysninger, der udveksles mellem deltagerne i en grænseoverskridende SOC, kan omfatte ***analyserede*** data fra netværk***,*** sensorer***,*** ***logning og telemetri***, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om ***taktikker, teknikker og procedurer,*** hændelser***,*** ***malwareprøver***, trusler og sårbarheder. Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er.

Or. en

Ændringsforslag 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 og Kommissionen ***i overensstemmelse med allerede eksisterende bestemmelser i henhold til 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 behørigt hensyn til, hvilke oplysninger der er

nødvendige, og til den eventuelt følsomme karakter af de udvekslede oplysninger.

Or. en

Ændringsforslag 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***samt højt 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.

Or. en

Ændringsforslag 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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] .	avancerede teknologier inden for kunstig intelligens og dataanalyse. ***Det skal dog bemærkes, at kunstig intelligens er den mest effektive, når den kombineres med menneskelig analyse. Derfor er højt kvalificeret personale fortsat afgørende for samling af data af høj kvalitet og indsamling af proaktive efterretninger om trusler.*** 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).

Or. en

Ændringsforslag 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***betydelige cybersikkerhedsøkosystem***. 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).***

Or. en

Ændringsforslag 64
Ville Niinistö
for Verts/ALE-Gruppen

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 samarbejde med de netværk og platforme, der har ansvar for informationsudveksling i cyberforsvarssektoren, i tæt samarbejde med den højtstående repræsentant.	(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 ***adgangsbetingelser og beskyttelsesprotokoller*** og standarder for at muliggøre samarbejde med cyberforsvarssektoren, herunder ***undersøgelse og*** sikkerhedsforhold***, under hensyntagen til institutternes 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.

Or. en

Begrundelse

For at undgå dobbeltarbejde og beskytte rettigheder og friheder skal samarbejdet mellem den civile side og forsvarssiden af cybersikkerhed være baseret på sikkerhedsforanstaltninger og undgå at ændre destinationen for den civile finansiering.

Ændringsforslag 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 24

Kommissionens forslag	*Ændringsforslag*
(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 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 cyberberedskabsmekanismen øge solidariteten mellem medlemsstaterne i overensstemmelse med artikel 3, stk. 3, i traktaten om Den Europæiske Union (TEU).	(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 cyberberedskabsmekanismen øge solidariteten mellem medlemsstaterne i overensstemmelse med artikel 3, stk. 3, i traktaten om Den Europæiske Union (TEU).

Or. en

Ændringsforslag 66
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 27

Kommissionens forslag	*Ændringsforslag*
(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 og berørte medlemsstater. Når en medlemsstat anmoder om støtte i henhold til cyberberedskabsmekanismen, bør den fremlægge relevante oplysninger, der begrunder behovet for støtte.	(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 cyberberedskabsmekanismen, bør den fremlægge relevante oplysninger, der begrunder behovet for støtte.

Or. en

Ændringsforslag 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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	(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 Unionens modstandsdygtighed og konkurrenceevne, herunder deltagelse af europæisk***

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.

administrerede sikkerhedstjenester, der er SMV'er. ***Pålidelige 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. ***Hvor det er muligt, bør tjenesterne baseres på de mest avancerede teknologier, herunder cloud og kunstig intelligens. Derfor bør cybersikkerhedsreserven tilskynde til investeringer i forskning og innovation for at sætte skub i udviklingen af disse teknologier. Hvor 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 det er nødvendigt.*** 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.

Or. en

Ændringsforslag 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***med en indledende finansiering på 10 mio. EUR i henhold til denne forordning indtil***

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.	***evalueringen. Den består*** 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. ***Kommissionen sikrer, at den ikke overlapper lignende initiativer inden for NATO.***

Or. en

Begrundelse

Kommissionen forudser en "gradvis oprettelse" af reserven, men dette afspejles ikke i resten af forslaget til forordning. Dette ændringsforslag foreslår derfor at reducere det oprindelige budget for reserven fra 36 mio. EUR til 10 mio. EUR indtil evalueringen af denne forordning. Dette vil returnere 26 mio. EUR til programmet for et digitalt Europa – særligt mål 4 om avancerede digitale færdigheder (af de 35 mio., der tages fra det). Udviklingen af en EU-cybersikkerhedsreserve ved siden af en eksisterende NATO-cybersikkerhedsreserve indebærer en høj risiko for dobbeltarbejde og bør ikke ske på bekostning af at investere mere i at udvikle og tiltrække cybersikkerhedstalenter i Europa.

Ændringsforslag 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 35

Kommissionens forslag	*Ændringsforslag*
(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 cyberberedskabsmekanismen.	(35) For at støtte etableringen af EU's cybersikkerhedsreserve ***bør*** Kommissionen 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 cyberberedskabsmekanismen.

Or. en

Ændringsforslag 70
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Forslag til forordning
Betragtning 35 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(35a) I lyset af de yderligere opgaver, der er fastsat i denne forordning samt i [forslaget til horisontale cybersikkerhedskrav til produkter med digitale elementer], bør ENISA tildeles de nødvendige menneskelige og finansielle ressourcer under Unionens budget.

Or. en

Ændringsforslag 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 37 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(37a) Udbydere af beredskabstjenester i forbindelse med hændelser fra tredjelande, herunder tredjelande, der er

associeret med programmet for et digitalt Europa eller NATO-medlemmer eller andre ligesindede internationale partnerlande, kan være nødvendige for at levere specifikke tjenester i EU's cybersikkerhedsreserve. For at styrke Unionens modstandsdygtighed og suverænitet og beskytte Unionens strategiske aktiver, interesser eller sikkerhed kan det være nødvendigt at begrænse eller udelukke deltagelse af juridiske enheder, der er etableret i eller kontrolleres af ikkeassocierede lande.

Or. en

Ændringsforslag 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 38 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(38a) Højt kvalificeret personale, der er i stand til pålideligt at levere de relevante cybersikkerhedstjenester af højeste standard, er afgørende for en effektiv gennemførelse af det europæiske cyberskjold og cyberberedskabsmekanismen. Det er derfor bekymrende, at Unionen står over for en talentkløft, der er kendetegnet ved mangel på kvalificerede fagfolk, samtidig med at den står over for et hurtigt udviklende trusselsbillede, som anerkendt i Kommissionens meddelelse af 18. april 2023 om akademiet for cyberfærdigheder. Det er vigtigt at overvinde denne talentkløft ved at styrke samarbejdet og koordineringen 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. Dette bør også fremme mobiliteten for cybersikkerhedsprofessionelle inden for Unionen. Denne forordning bør sigte mod at fremme en mere forskelligartet cybersikkerhedsarbejdsstyrke.

Or. en

Ændringsforslag 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 38 b (ny)

Kommissionens forslag	*Ændringsforslag*
	(38b) Medlemsstaternes kapacitetsopbygning er afgørende for en EU-dækkende koordineret tilgang til at styrke modstandsdygtigheden i Unionens sikkerhedsstatus. Som understreget i Kommissionens meddelelse af 18. april 2023 om akademiet for cyberfærdigheder kan Unionens sikkerhed ikke garanteres uden Unionens mest værdifulde aktiv: befolkningen. Den europæiske ramme for cybersikkerhedsfærdigheder kan bidrage til bedre at forstå sammensætningen af Unionens arbejdsstyrke, herunder de nuværende og krævede kompetencer inden for de deltagende enheder.

Or. en

Ændringsforslag 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu

Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Betragtning 39

Kommissionens forslag	*Ændringsforslag*
(39) Målsætningen for denne forordning kan bedre opfyldes på EU-plan end af medlemsstaterne hver især. Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet og proportionalitetsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. Denne forordning går ikke ud over, hvad der er nødvendigt for at opfylde denne målsætning.	(39) Målsætningen for denne forordning***, nemlig at nedbryde kommunikationssiloer og styrke Unionens kapacitet til forebyggelse, afsløring, reaktion og genopretning af cybertrusler,*** kan bedre opfyldes på EU-plan end af medlemsstaterne hver især. Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet og proportionalitetsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. Denne forordning går ikke ud over, hvad der er nødvendigt for at opfylde denne målsætning.

Or. en

Ændringsforslag 75
Nicola Danti

Forslag til forordning
Betragtning 39 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(39a) I lyset af de yderligere opgaver, der er fastsat i denne forordning samt i [forslaget til horisontale cybersikkerhedskrav til produkter med digitale elementer], bør ENISA tildeles de nødvendige menneskelige og finansielle ressourcer under Unionens budget.

Or. en

Ændringsforslag 76
Johan Nissinen

Forslag til forordning
Artikel 1 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
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:	1. Ved denne forordning fastsættes foranstaltninger til styrkelse af Unionens kapacitet til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser, ***samtidig med at den nationale sikkerhed, herunder på cyberområdet, forbliver den enkelte medlemsstats eneansvar, jf. artikel 4, stk. 2, i TEU,*** navnlig gennem følgende tiltag:

Or. en

Ændringsforslag 77
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
a) etablering af ***en paneuropæisk infrastruktur for*** sikkerhedsoperationscentre (***"et europæisk cyberskjold"***) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser	a) ***styrkelse af enheder, der håndterer IT-sikkerhedshændelser (CSIRT), jf. artikel 10 i direktiv (EU) 2022/2555, og af CSIRT-netværket, jf. artikel 15 i direktiv (EU) 2022/2555, og*** etablering af sikkerhedsoperationscentre (***SOC'er***) for at opbygge og styrke det ***nationale og*** fælles situationskendskab og den fælles kapacitet til at afsløre hændelser ***("et europæisk cyberskjold")***

Or. en

Ændringsforslag 78
Evžen Tošenovský

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.	***udgår***

Or. en

Ændringsforslag 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet	a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og dermed gøre det muligt at styrke industriens***, herunder SMV'ernes*** og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet

Or. en

Ændringsforslag 80
Johan Nissinen

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 konkurrenceposition i Unionen i hele den	a) at styrke Unionens ***frivillige*** 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	digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet

Or. en

Ændringsforslag 81
Johan Nissinen

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 ***det frivillige samarbejde*** 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

Or. en

Ændringsforslag 82
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
c) at øge Unionens modstandsdygtighed og bidrage til en effektiv reaktion ved at gennemgå og vurdere væsentlige eller omfattende hændelser, herunder ved at trække på indhøstede erfaringer og henstillinger, hvor det er relevant.	***udgår***

Or. en

Ændringsforslag 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
	ca) at udvikle og forbedre arbejdsstyrkens færdigheder og kompetencer inden for cybersikkerhedssektoren på en koordineret måde ved at samarbejde med akademiet for cyberfærdigheder om at tilbyde uddannelse og muligheder med det formål at lukke talentkløften inden for cybersikkerhedssektoren.

Or. en

Ændringsforslag 84
Johan Nissinen

Forslag til forordning
Artikel 1 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Denne forordning berører ikke medlemsstaternes primære ansvar for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.	3. Denne forordning berører ikke medlemsstaternes primære ansvar for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger ***og forhindrer unødvendig overlapning med eksisterende initiativer***.

Or. en

Ændringsforslag 85
Evžen Tošenovský

Forslag til forordning

Artikel 1 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Denne forordning berører ikke medlemsstaternes ***primære ansvar*** for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.	3. Denne forordning berører ikke medlemsstaternes ***enekompetence inden*** for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

Or. en

Ændringsforslag 86
Nicola Danti

Forslag til forordning
Artikel 1 – stk. 3 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	3a. Hvert år fremlægger Kommissionen ved forelæggelsen af budgetforslaget for det følgende år en detaljeret vurdering af ENISA's opgaver i henhold til denne forordning samt [forslaget til en forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer] og anden EU-lovgivning og beskriver de finansielle og menneskelige ressourcer, der er nødvendige for at udføre disse opgaver.

Or. en

Ændringsforslag 87
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 1

Kommissionens forslag	*Ændringsforslag*
(1) "grænseoverskridende sikkerhedsoperationscenter"	***udgår***

("grænseoverskridende SOC"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at forebygge cybertrusler og -hændelser og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø

Or. en

Ændringsforslag 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 2 – stk. 1 – nr. 1

Kommissionens forslag	*Ændringsforslag*
(1) "grænseoverskridende sikkerhedsoperationscenter" ("grænseoverskridende SOC"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at ***forebygge*** cybertrusler og ***-hændelser*** og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø	(1) "grænseoverskridende sikkerhedsoperationscenter" ("grænseoverskridende SOC"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at ***opdage og analysere*** cybertrusler og ***forebygge hændelser*** og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø

Or. en

Ændringsforslag 89
Johan Nissinen

Forslag til forordning
Artikel 2 – stk. 1 – nr. 1

Kommissionens forslag	*Ændringsforslag*
1) "grænseoverskridende sikkerhedsoperationscenter" ("grænseoverskridende SOC"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at forebygge cybertrusler og -hændelser og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø	1) "grænseoverskridende sikkerhedsoperationscenter" ("grænseoverskridende SOC"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at forebygge cybertrusler og -hændelser og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem ***frivillig*** udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø

Or. en

Ændringsforslag 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
	1a) "sikkerhedsoperationscenter" ("SOC"): en centraliseret kapacitet, der kan være intern eller outsourcet, og som er ansvarlig for løbende at overvåge og forbedre en enheds sikkerhedsstatus for at forebygge, opdage, analysere og reagere på cybersikkerhedstrusler

Or. en

Ændringsforslag 91
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
	1a) "sikkerhedsoperationscenter" ("SOC"): et center oprettet af private og offentlige enheder eller nationale myndigheder, der konstant overvåger og analyserer kommunikationsnetværk og computersystemer for at opdage indtrængen og uregelmæssigheder i realtid

Or. en

Ændringsforslag 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
	1b) "nationale sikkerhedsoperationscentre" ("national SOC"): en centraliseret kapacitet, der er ansvarlig for løbende at indsamle trusselsoplysninger og forbedre sikkerhedsstatussen for enheder under national jurisdiktion ved at forebygge, opdage og analysere cybersikkerhedstrusler for bedre at kunne reagere på cybersikkerhedstrusler. Denne kapacitet skal, hvis det er relevant, indarbejdes i allerede eksisterende nationale strukturer såsom CSIRT'er som oprettet i henhold til direktiv (EU) 2022/2555

Or. en

Ændringsforslag 93
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 2

Kommissionens forslag	*Ændringsforslag*
2) "***offentligt organ***": ***et offentligretligt organ*** som defineret i artikel ***2, stk. 1***, nr. ***4***), i ***Europa-Parlamentets og Rådets*** direktiv ***2014/24/EU*** [30]	2) "***offentlig forvaltningsenhed***": ***en offentlig forvaltningsenhed*** som defineret i artikel ***6***, nr. ***35***), i direktiv ***(EU) 2022/2555***

[30] 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).

Or. en

Ændringsforslag 94
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 3

Kommissionens forslag	*Ændringsforslag*
3) "værtskonsortium": et konsortium bestående af deltagende stater repræsenteret ved nationale SOC'er, der har indvilliget i at etablere og bidrage til erhvervelse af værktøjer og infrastruktur til og drift af et grænseoverskridende SOC	***udgår***

Or. en

Ændringsforslag 95
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 5 a (nyt)

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

Or. en

Ændringsforslag 96
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 5 b (nyt)

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

Or. en

Ændringsforslag 97
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 6 a (nyt)

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

Or. en

Ændringsforslag 98
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 9

Kommissionens forslag	*Ændringsforslag*

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	***udgår***

Or. en

Ændringsforslag 99
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 10

Kommissionens forslag	*Ændringsforslag*
10) tiltag i forbindelse med, under eller efter en væsentlig eller omfattende cybersikkerhedshændelse for at håndtere dens umiddelbare og kortsigtede negative konsekvenser "betroede udbydere":	***udgår***

Or. en

Ændringsforslag 100
Evžen Tošenovský

Forslag til forordning
Artikel 2 – stk. 1 – nr. 11

Kommissionens forslag	*Ændringsforslag*
11) udbydere af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555, der er udvalgt i overensstemmelse med artikel 16 i denne forordning.	11) ***"betroede udbydere af administrerede sikkerhedstjenester": betroede*** udbydere af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555, der er udvalgt ***til at indgå i EU's cybersikkerhedsreserve*** i overensstemmelse med artikel 16 i denne forordning.

Or. en

Ændringsforslag 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 3 – stk. 1 – afsnit 1

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

Or. en

Ændringsforslag 102
Johan Nissinen

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

Kommissionens forslag	*Ændringsforslag*
a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende SOC'er	a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem ***frivillig deling af oplysninger fra*** grænseoverskridende SOC'er

Or. en

Ændringsforslag 103
Evžen Tošenovský

Forslag til forordning

Artikel 3 – stk. 2 – afsnit 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende SOC'er	a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende SOC'er ***både på nationalt plan og på EU-plan***

Or. en

Ændringsforslag 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ved at give konkrete anbefalinger til enheder***

Or. en

Ændringsforslag 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
d) bidrage til hurtigere opdagelse af cybertrusler og større situationskendskab i hele Unionen	d) bidrage til hurtigere opdagelse af cybertrusler og større situationskendskab i hele Unionen***, herunder ved at indsamle proaktive efterretninger***

Or. en

Ændringsforslag 106

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Kommissionens forslag	*Ændringsforslag*
e) levere tjenester og aktiviteter til cybersikkerhedssektoren i Unionen, herunder bidrage til udviklingen af værktøjer inden for avanceret kunstig intelligens og dataanalyse.	e) *(Vedrører ikke den danske tekst)*

Or. en

Ændringsforslag 107
Evžen Tošenovský

Forslag til forordning
Artikel 4 – overskrift

Kommissionens forslag	*Ændringsforslag*
Nationale sikkerhedsoperationscentre	***Styrket samarbejde og informationsudveksling på nationalt plan***

Or. en

Ændringsforslag 108
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
For at ***deltage i*** det europæiske cyberskjold udpeger hver medlemsstat ***mindst ét nationalt SOC. Det nationale SOC skal være et offentligt organ***.	For at ***bidrage til*** det europæiske cyberskjold udpeger hver medlemsstat ***en af sine enheder, der håndterer IT-sikkerhedshændelser (CSIRT), jf. artikel 10 i direktiv (EU) 2022/2555, som et informationsudvekslings- og analysecenter (ISAC)***.

Or. en

Ændringsforslag 109
Evžen Tošenovský

Forslag til forordning
Artikel 4 – stk. 1 – afsnit 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	Private og offentlige organisationer eller nationale myndigheder, navnlig enheder, der opererer i kritiske eller meget kritiske sektorer, skal tilskyndes til at etablere og drive deres autonome eller delte SOC'er.

Or. en

Ændringsforslag 110
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 4 – stk. 1 – afsnit 2

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 organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler 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 eller den nationale CSIRT kan anmode om telemetri-, sensor- eller logningsdata, der vedrører sektorer af særlig kritisk betydning som defineret i direktiv (EU) 2022/2555 fra betroede udbydere eller udbydere af administrerede sikkerhedstjenester. Disse data kan kun deles for at understøtte den nationale SOC's eller CSIRT's opgaver og ansvar med at opdage og forebygge***

cybersikkerhedshændelser.

Or. en

Ændringsforslag 111
Evžen Tošenovský

Forslag til forordning
Artikel 4 – stk. 1 – afsnit 2

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 ***primært*** til ***SOC'er, der er oprettet af private og offentlige enheder eller nationale myndigheder, andre CSIRT'er i samme medlemsstat, koordinator for styring af omfattende cybersikkerhedshændelser og -kriser samt for*** andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser ***og, hvor det er relevant, dele disse oplysninger med andre medlemmer af CSIRT-netværket***. Det skal være udstyret med avancerede teknologier, der gør det muligt at finde, aggregere og analysere data, der er relevante for cybersikkerhedstrusler og -hændelser.

Or. en

Ændringsforslag 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 4 – stk. 1 – afsnit 2

Kommissionens forslag	*Ændringsforslag*
Det skal have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private organisationer på	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.	nationalt plan***, navnlig deres SOC'er,*** 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.

Or. en

Ændringsforslag 113
Evžen Tošenovský

Forslag til forordning
Artikel 4 – stk. 2

Kommissionens forslag	*Ændringsforslag*
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.	***udgår***

Or. en

Ændringsforslag 114

Ville Niinistö
for Verts/ALE-Gruppen

Forslag til forordning
Artikel 4 – stk. 2

Kommissionens forslag	*Ændringsforslag*
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.	2. Efter en indkaldelse af interessetilkendegivelser ***kan*** de nationale SOC'er ***blive udvalgt*** 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.

Or. en

Begrundelse

Den obligatoriske karakter af "skal", tømmer indholdet for begrebet indkaldelse af interessetilkendegivelser og udvælgelsesprocesser. SOC'erne kan naturligvis deltage og kan udvælges.

Ændringsforslag 115
Evžen Tošenovský

Forslag til forordning
Artikel 4 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Et nationalt SOC, der er udvalgt i henhold til stk. 2, forpligter sig til at	***udgår***

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.

Or. en

Ændringsforslag 116
Evžen Tošenovský

Forslag til forordning
Artikel 5 – overskrift

Kommissionens forslag	*Ændringsforslag*
Grænseoverskridende sikkerhedsoperationscentre	***Fælles indkøb af værktøjer og infrastrukturer***

Or. en

Ændringsforslag 117
Evžen Tošenovský

Forslag til forordning
Artikel 5 – stk. 1

Kommissionens forslag	*Ændringsforslag*
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.	***udgår***

Or. en

Ændringsforslag 118
Evžen Tošenovský

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 infrastrukturerne.	2. Efter en indkaldelse af interessetilkendegivelser ***kan CSIRT'erne og ISAC'erne blive udvalg*** af ECCC til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til ***CSIRT'erne og ISAC'erne*** 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 ***CSIRT'erne og ISAC'erne***. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og ***de deltagende CSIRT'er og ISAC'er*** en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne***, herunder deres anvendelse af andre CSIRT'er og SOC'er i den pågældende medlemsstat***.

Or. en

Ændringsforslag 119
Ville Niinistö
for Verts/ALE-Gruppen

Forslag til forordning
Artikel 5 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Efter en indkaldelse af	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 infrastrukturerne.	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.

Or. en

Begrundelse

Selv om denne forordning ikke indeholder eksplicitte kriterier, kan anden gældende lovgivning reducere sikkerheden for, at en ansøger/alle ansøgere får medhold.

Ændringsforslag 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Kommissionens forslag	*Ændringsforslag*
	2a. Indkøb fra og deltagelse af en privat enhed, der er etableret i et ligesindet tredjeland, bør være tilladt, hvis det ikke er i strid med Unionens og medlemsstaternes sikkerheds- og forsvarsinteresser som fastsat som led i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i TEU eller målene i denne forordning. Disse private enheder bør ikke kontrolleres af et ikkeassocieret tredjeland, eller de skal have været genstand for screening i henhold til Europa-Parlamentets og Rådets

forordning (EU) 2019/452.

Or. en

Ændringsforslag 121
Evžen Tošenovský

Forslag til forordning
Artikel 5 – stk. 3

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

Or. en

Ændringsforslag 122
Evžen Tošenovský

Forslag til forordning
Artikel 5 – stk. 4

Kommissionens forslag	*Ændringsforslag*
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.	***udgår***

Or. en

Ændringsforslag 123
Evžen Tošenovský

Forslag til forordning

Artikel 6 – overskrift

Kommissionens forslag	*Ændringsforslag*
Samarbejde og informationsudveksling ***inden for og mellem grænseoverskridende SOC'er***	***Styrket*** samarbejde og informationsudveksling ***på EU-plan***

Or. en

Ændringsforslag 124
Johan Nissinen

Forslag til forordning
Artikel 6 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
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:	1. Medlemmerne af et værtskonsortium ***kan*** indbyrdes ***udveksle*** 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:

Or. en

Ændringsforslag 125
Evžen Tošenovský

Forslag til forordning
Artikel 6 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
1. ***Medlemmerne af et værtskonsortium*** udveksler indbyrdes	1. ***CSIRT'er, ISAC'er og andre CSIRT'er*** udveksler indbyrdes relevante

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:	oplysninger inden for ***CSIRT-netværket***, 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:

Or. en

Ændringsforslag 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 6 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
a) ***har til formål at*** forebygge, opdage***, reagere på*** eller ***reetablere sig efter*** hændelser ***eller afbøde deres virkninger***	a) ***forbedrer udvekslingen af efterretninger om cybertrusler mellem SOC'er og industri-ISAC'er med henblik på at*** forebygge, opdage eller ***afbøde*** hændelser

Or. en

Ændringsforslag 127
Evžen Tošenovský

Forslag til forordning
Artikel 6 – stk. 2 – indledning

Kommissionens forslag	*Ændringsforslag*
2. ***Den skriftlige konsortieaftale i henhold til artikel 5, stk. 3, skal*** indeholde:	2. ***Informations- og efterretningsudvekslingsaftalen mellem CSIRT'er og ISAC'er eller, hvor det er relevant, andre CSIRT'er, kan*** indeholde:

Or. en

Ændringsforslag 128
Johan Nissinen

Forslag til forordning
Artikel 6 – stk. 2 – litra a

Kommissionens forslag	*Ændringsforslag*
a) en forpligtelse til at ***dele en betydelig mængde*** data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger	a) en forpligtelse til ***frivilligt*** at ***dele*** data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger

Or. en

Ændringsforslag 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 6 – stk. 2 – litra a

Kommissionens forslag	*Ændringsforslag*
a) en forpligtelse til at dele ***en betydelig mængde*** data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger	a) en forpligtelse til at dele ***væsentlige*** data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger

Or. en

Ændringsforslag 130
Evžen Tošenovský

Forslag til forordning
Artikel 6 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. For at tilskynde til udveksling af oplysninger mellem grænseoverskridende SOC'er skal disse sikre en høj grad af indbyrdes interoperabilitet. For at sikre interoperabilitet mellem de grænseoverskridende SOC'er kan	***udgår***

Kommissionen ved hjælp af gennemførelsesretsakter efter høring af ECCC fastsætte betingelserne for interoperabilitet. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Or. en

Ændringsforslag 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 6 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. For at tilskynde til udveksling af oplysninger ***mellem*** grænseoverskridende SOC'er skal disse sikre en høj grad af indbyrdes interoperabilitet. For at sikre interoperabilitet mellem de grænseoverskridende SOC'er ***kan*** Kommissionen ***ved hjælp af gennemførelsesretsakter efter høring af ECCC fastsætte*** betingelserne for interoperabilitet. Disse ***gennemførelsesretsakter*** vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.	3. For at tilskynde til udveksling af oplysninger ***blandt*** grænseoverskridende SOC'er ***og med industri-ISAC'er*** skal disse sikre en høj grad af indbyrdes interoperabilitet ***og, hvor det er muligt, med industri-ISAC'er***. For at sikre interoperabilitet mellem de grænseoverskridende SOC'er ***og med industri-ISAC'er bør standarder og protokoller for informationsudveksling harmoniseres med internationale standarder og bedste praksis i branchen. ECCC kan også anmode*** Kommissionen ***om ved delegerede retsakter at foreslå*** betingelserne for interoperabiliteten ***i tæt samarbejde med de regionale SOC'er og på grundlag af internationale standarder og bedste praksis i branchen***. Disse ***delegerede retsakter*** vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Or. en

Ændringsforslag 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 6 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. For at tilskynde til udveksling af oplysninger mellem grænseoverskridende SOC'er skal disse sikre en høj grad af indbyrdes interoperabilitet. ***For at*** sikre interoperabilitet mellem de grænseoverskridende SOC'er kan Kommissionen ved hjælp af gennemførelsesretsakter efter høring af ECCC fastsætte betingelserne for interoperabilitet. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.	3. For at tilskynde til udveksling af oplysninger mellem grænseoverskridende SOC'er skal disse sikre en høj grad af indbyrdes interoperabilitet. ***Fælles indkøb af cyberinfrastrukturer, -tjenester og -værktøjer kan*** sikre interoperabiliteten mellem de grænseoverskridende SOC'er***.*** ***For at præcisere betingelserne for interoperabilitet mellem de grænseoverskridende SOC'er*** kan Kommissionen ved hjælp af gennemførelsesretsakter efter høring af ECCC ***og ENISA*** fastsætte betingelserne for denne interoperabilitet. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Or. en

Ændringsforslag 133
Evžen Tošenovský

Forslag til forordning
Artikel 6 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges.	***udgår***

Or. en

Ændringsforslag 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu

Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 6 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges.	4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges ***under hensyntagen til allerede eksisterende relevante informationsudvekslingsmekanismer i henhold til direktiv (EU) 2022/2555. I forbindelse med en potentiel eller igangværende omfattende cybersikkerhedshændelse skal informationsudvekslingsmekanismerne overholde de relevante bestemmelser i direktiv (EU) 2022/2555.***

Or. en

Ændringsforslag 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 6 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges.	4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden ***og med industri-ISAC'er***, hvor principperne for informationsudveksling ***og interoperabilitet*** mellem de grænseoverskridende platforme fastlægges.

Or. en

Ændringsforslag 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 7 – overskrift

Kommissionens forslag	*Ændringsforslag*
Samarbejde og informationsudveksling med ***EU-enheder***	Samarbejde og informationsudveksling med ***CSIRT-netværket***

Or. en

Ændringsforslag 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***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 og Kommissionen i betragtning af deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.

Or. en

Begrundelse

Foreslå at overholde NIS 2-proceduren ved omfattende hændelser.

Ændringsforslag 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***og ENISA*** i ***overensstemmelse med*** deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.

Or. en

Ændringsforslag 139
Evžen Tošenovský

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 ***CSIRT'er og ISAC'er*** indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse, forelægger de uden unødig forsinkelse de relevante oplysninger for EU-CyCLONe ***og*** CSIRT-netværket i betragtning af deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.

Or. en

Ændringsforslag 140
Evžen Tošenovský

Forslag til forordning
Artikel 7 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Kommissionen kan ved hjælp af	***udgår***

gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Or. en

Ændringsforslag 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 7 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.	2. Kommissionen kan ***efter høring af de grænseoverskridende platforme og CSIRT-netværket*** ved hjælp af gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2***, og i overensstemmelse med direktiv (EU) 2022/2555***.

Or. en

Begrundelse

Foreslå at overholde NIS 2-proceduren ved omfattende hændelser og derfor først konsultere CSIRT-netværket.

Ændringsforslag 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 7 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.	2. Kommissionen kan ***efter høring af ENISA*** ved hjælp af gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Or. en

Ændringsforslag 143
Johan Nissinen

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 ***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.

Or. en

Ændringsforslag 144
Evžen Tošenovský

Forslag til forordning
Artikel 8 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter	***udgår***

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.

Or. en

Ændringsforslag 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 8 – stk. 3

Kommissionens forslag	*Ændringsforslag*
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.	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***, og med direktiv (EU) 2022/2555 og direktiv (EU) 2022/2557***. I den forbindelse tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører.

Or. en

Ændringsforslag 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 8 – stk. 3

Kommissionens forslag	*Ændringsforslag*
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.	3. Kommissionen kan ***efter høring af ENISA*** 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.

Or. en

Ændringsforslag 147
Johan Nissinen

Forslag til forordning
Artikel 9 – stk. 1

Kommissionens forslag	*Ændringsforslag*
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").	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") ***efter udtrykkelig anmodning fra den eller de pågældende medlemsstater***.

Or. en

Ændringsforslag 148
Evžen Tošenovský

Forslag til forordning
Artikel 9 – stk. 1

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

Or. en

Ændringsforslag 149
Johan Nissinen

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

Kommissionens forslag	*Ændringsforslag*
b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser, der leveres af betroede udbydere, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 12	b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser, der leveres af betroede udbydere, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 12***, efter udtrykkelig anmodning fra den eller de pågældende medlemsstater***

Or. en

Ændringsforslag 150
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig	b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig

genopretning efter væsentlige og omfattende cybersikkerhedshændelser, der leveres af betroede udbydere, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 12	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

Or. en

Ændringsforslag 151
Ville Niinistö
for Verts/ALE-Gruppen

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

Kommissionens forslag	*Ændringsforslag*
	1a. Efter udløsningen af cyberberedskabsmekanismen rapporterer Kommissionen hvert år vurderingen af mekanismens både positive og negative funktion, herunder om der er behov for yderligere samarbejde eller uddannelseskrav.

Or. en

Ændringsforslag 152
Evžen Tošenovský

Forslag til forordning
Artikel 11 – stk. 1

Kommissionens forslag	*Ændringsforslag*
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	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 på EU-plan.	genstand for koordineret beredskabstest, under hensyntagen til eksisterende og planlagte ***frivillige*** koordinerede risikovurderinger og prøvning af modstandsdygtighed på EU-plan.

Or. en

Ændringsforslag 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 og den højtstående repræsentant fælles risikoscenarier og metoder til gennemførelse af de koordinerede ***beredskabstest. Dette vil informere om identifikationen af berørte sektorer eller delsektorer, hvorfra enheder kan være genstand for den koordinerede beredskabstest som beskrevet i stk. 1***.

Or. en

Ændringsforslag 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***og de enheder, der kan være genstand for beredskabstesten,*** fælles risikoscenarier og metoder til gennemførelse af de koordinerede test.

Or. en

Ændringsforslag 155
Johan Nissinen

Forslag til forordning
Artikel 12 – stk. 1

Kommissionens forslag	*Ændringsforslag*
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.	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 ***efter udtrykkelig anmodning fra den eller de pågældende medlemsstater, og uden at det berører den særlige karakter af visse medlemsstaters sikkerheds- og forsvarspolitik***.

Or. en

Ændringsforslag 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, styrke Unionens modstandsdygtighed og suverænitet og forbedre Unionens konkurrenceevne***. ***Navnene på de udvalgte betroede***

udbydere og deres tjenester behandles fortroligt.

Or. en

Ændringsforslag 157
Johan Nissinen

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. ***EU's cybersikkerhedsreserve begrænser ikke behovet for at give landene mulighed for at overvåge og vurdere deres egne behov.***

Or. en

Ændringsforslag 158
Evžen Tošenovský

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 ***af administrerede sikkerhedstjenester***, der er udvalgt i overensstemmelse med kriterierne i artikel 16. Reserven omfatter tjenester omfattet af forhåndsforpligtelser. Tjenesterne kan ***efter anmodning*** indsættes i alle medlemsstater.

Or. en

Ændringsforslag 159
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
b) ***EU's institutioner, organer og agenturer***.	b) ***tredjelande omhandlet i artikel 17 i denne forordning***.

Or. en

Ændringsforslag 160
Evžen Tošenovský

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), ***kan efter anmodning anvende*** 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.

Or. en

Ændringsforslag 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	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.

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.

Or. en

Ændringsforslag 162
Evžen Tošenovský

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 ***i samarbejde med ENISA*** 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.

Or. en

Ændringsforslag 163
Evžen Tošenovský

Forslag til forordning
Artikel 12 – stk. 6

Kommissionens forslag	*Ændringsforslag*

6. Kommissionen kan helt eller delvist overdrage driften og administrationen af EU's cybersikkerhedsreserve til ENISA ved hjælp af bidragsaftaler.	***udgår***

Or. en

Ændringsforslag 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 12 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Kommissionen ***kan*** helt eller delvist ***overdrage*** driften og administrationen af EU's cybersikkerhedsreserve til ENISA ved hjælp af bidragsaftaler.	6. Kommissionen ***overdrager*** helt eller delvist driften og administrationen af EU's cybersikkerhedsreserve til ENISA ved hjælp af bidragsaftaler.

Or. en

Ændringsforslag 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 artikel 17. Kommissionen hører, hvor det	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. ENISA udarbejder efter høring af Kommissionen ***og i partnerskab med den private sektor*** en lignende kortlægning for

er relevant, den højtstående repræsentant.	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.

Or. en

Ændringsforslag 166
Evžen Tošenovský

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 artikel 17. Kommissionen hører, hvor det er relevant, den højtstående repræsentant.	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 ***og informerer Rådet om tredjelandes behov.***

Or. en

Ændringsforslag 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	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.	efter høring af medlemsstaterne***,*** Kommissionen***, udbydere af administrerede sikkerhedstjenester og repræsentanter for branchen***. 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.

Or. en

Ændringsforslag 168
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 12 – stk. 8

Kommissionens forslag	*Ændringsforslag*
8. Kommissionen kan ***i gennemførelsesretsakter*** præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.	8. Kommissionen kan ***vedtage en delegeret retsakt i overensstemmelse med artikel 20a i denne forordning for at*** præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.

Or. en

Ændringsforslag 169
Evžen Tošenovský

Forslag til forordning
Artikel 13 – stk. 5 – litra a

Kommissionens forslag	*Ændringsforslag*
a) ***relevante oplysninger om den berørte*** enhed og mulige virkninger af	a) ***type berørt*** enhed og mulige virkninger af hændelsen samt den planlagte

hændelsen samt den planlagte anvendelse af den støtte, der anmodes om, herunder en angivelse af de anslåede behov	anvendelse af den støtte, der anmodes om, herunder en angivelse af de anslåede behov

Or. en

Ændringsforslag 170
Evžen Tošenovský

Forslag til forordning
Artikel 13 – stk. 5 – litra b

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

Or. en

Ændringsforslag 171
Evžen Tošenovský

Forslag til forordning
Artikel 13 – stk. 5 – litra c

Kommissionens forslag	*Ændringsforslag*
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.***	c) oplysninger om andre former for støtte, der er til rådighed for den berørte enhed

Or. en

Ændringsforslag 172
Evžen Tošenovský

Forslag til forordning

Artikel 13 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7. Kommissionen kan i gennemførelsesretsakter yderligere præcisere de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.	***udgår***

Or. en

Ændringsforslag 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 13 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7. Kommissionen kan ***i gennemførelsesretsakter*** yderligere præcisere de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.	7. Kommissionen kan ***vedtage delegerede retsakter i overensstemmelse med artikel 20a i denne forordning for*** yderligere ***at*** præcisere de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.

Or. en

Ændringsforslag 174
Evžen Tošenovský

Forslag til forordning
Artikel 14 – stk. 1

Kommissionens forslag	*Ændringsforslag*
1. Anmodninger om støtte fra EU's	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 ***straks*** til de brugere, der er omhandlet i artikel 12, stk. 3.	cybersikkerhedsreserve vurderes af Kommissionen med støtte fra ENISA, og ***dens afgørelse*** sendes ***uden unødig forsinkelse og under alle omstændigheder inden for 24 timer*** til de brugere, der er omhandlet i artikel 12, stk. 3.

Or. en

Ændringsforslag 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 14 – stk. 2 – litra d

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

Or. en

Ændringsforslag 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 14 – stk. 3

Kommissionens forslag	*Ændringsforslag*
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.	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 af aftalens parter skønnes nødvendige for leveringen af den pågældende tjenesteydelse***.

Or. en

Ændringsforslag 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 14 – stk. 3

Kommissionens forslag	*Ændringsforslag*
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.	3. Tjenesterne under EU's cybersikkerhedsreserve leveres ***efter godkendelse fra brugeren og*** i overensstemmelse med særaftaler mellem tjenesteudbyderen og den bruger, som støtten under EU's cybersikkerhedsreserve ydes til. Aftalerne skal indeholde ansvarsbetingelser. Aftalerne skal indeholde ansvarsbetingelser.

Or. en

Ændringsforslag 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 14 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. De i stk. 3 omhandlede aftaler ***kan*** baseres på skabeloner udarbejdet af ENISA efter høring af medlemsstaterne.	4. De i stk. 3 omhandlede aftaler baseres på skabeloner udarbejdet af ENISA efter høring af medlemsstaterne ***og andre brugere af reserven***.

Or. en

Ændringsforslag 179
Evžen Tošenovský

Forslag til forordning
Artikel 14 – stk. 5

Kommissionens forslag	*Ændringsforslag*

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.	***udgår***

Or. en

Ændringsforslag 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 14 – stk. 5

Kommissionens forslag	*Ændringsforslag*
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.	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 uagtsomhed i evalueringen af tjenesteudbyderens anvendelse eller i tilfælde, hvor Kommissionen eller ENISA er brugere og findes ansvarlig for skader***.

Or. en

Ændringsforslag 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 14 – stk. 5

Kommissionens forslag	*Ændringsforslag*
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.	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, hvor Kommissionen eller ENISA er brugere af reserven i henhold til artikel 14, stk. 3.

Or. en

Ændringsforslag 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 14 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen og ENISA 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.	6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen og ENISA 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 eller national ret vedrørende beskyttelse af følsomme eller klassificerede informationer.***

Or. en

Ændringsforslag 183
Evžen Tošenovský

Forslag til forordning
Artikel 14 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen ***og*** ENISA 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.	6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen***,*** 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.

Or. en

Ændringsforslag 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 14 – stk. 7

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

Or. en

Ændringsforslag 185
Evžen Tošenovský

Forslag til forordning
Artikel 14 – stk. 7

Kommissionens forslag	*Ændringsforslag*
7. Kommissionen aflægger ***regelmæssigt*** rapport til NIS-samarbejdsgruppen om anvendelsen og resultaterne af støtten.	7. Kommissionen aflægger ***mindst to gange om året*** rapport til NIS-samarbejdsgruppen om anvendelsen og resultaterne af støtten.

Or. en

Ændringsforslag 186
Evžen Tošenovský

Forslag til forordning

Artikel 15 – overskrift

Kommissionens forslag	*Ændringsforslag*
Koordinering med krisestyringsmekanismer	Koordinering ***af cyberberedskabsmekanismen*** med krisestyringsmekanismer

Or. en

Ændringsforslag 187
Evžen Tošenovský

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.

Or. en

Ændringsforslag 188
Evžen Tošenovský

Forslag til forordning
Artikel 16 – overskrift

Kommissionens forslag	*Ændringsforslag*
Betroede udbydere	Betroede udbydere ***af administrerede sikkerhedstjenester***

Or. en

Ændringsforslag 189
Johan Nissinen

Forslag til forordning
Artikel 16 – stk. 1 – indledning

Kommissionens forslag	*Ændringsforslag*
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:	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***, uden at dette berører medlemsstaternes primære ansvar for national sikkerhed,*** og i overensstemmelse med følgende principper:

Or. en

Ændringsforslag 190
Evžen Tošenovský

Forslag til forordning
Artikel 16 – stk. 1 – litra a

Kommissionens forslag	*Ændringsforslag*
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	a) sikre, at EU's cybersikkerhedsreserve omfatter tjenester, der kan udrulles i alle medlemsstater ***og tredjelande i overensstemmelse med artikel 17 i denne forordning***, idet der navnlig tages hensyn til nationale krav til levering af sådanne tjenester, herunder certificering eller akkreditering

Or. en

Ændringsforslag 191

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 16 – stk. 1 – litra c

Kommissionens forslag	*Ændringsforslag*
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.	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***, styrke Unionens modstandsdygtighed og suverænitet og forbedre Unionens konkurrenceevne***.

Or. en

Ændringsforslag 192
Evžen Tošenovský

Forslag til forordning
Artikel 16 – stk. 1 – litra c

Kommissionens forslag	*Ændringsforslag*
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.	c) sikre, at EU's cybersikkerhedsreserve ***bidrager*** til de målsætninger, der er fastsat i artikel 3 i forordning (EU) 2021/694, herunder ved at fremme udviklingen af cybersikkerhedsfærdigheder i EU.

Or. en

Ændringsforslag 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***opdaterede*** hardware og software til at understøtte den ønskede tjeneste ***og skal overholde kravene i forordning XX/XXX (forordningen om cyberrobusthed), hvor det er relevant***

Or. en

Ændringsforslag 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
	fa) udbyderen skal påvise, at dens beslutnings- og forvaltningsstrukturer er fri for enhver utilbørlig indflydelse fra regeringer i stater, der er klassificeret som systemiske rivaler til Unionen

Or. en

Ændringsforslag 195
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
h) udbyderen skal være i stand til at levere tjenesten hurtigt i den eller de medlemsstater, hvor udbyderen kan levere tjenesten	h) udbyderen skal være i stand til at levere tjenesten hurtigt i den eller de medlemsstater ***eller tredjelande***, hvor udbyderen kan levere tjenesten

Or. en

Ændringsforslag 196
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
i) udbyderen skal kunne levere tjenesten på det lokale sprog 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 ***eller tredjelande***, hvor udbyderen kan levere tjenesten***, eller på et af EU-institutionernes arbejdssprog***

Or. en

Ændringsforslag 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Kommissionens forslag	*Ændringsforslag*
j) når en EU-certificeringsordning for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning.	j) når en EU-certificeringsordning 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***.

Or. en

Ændringsforslag 198
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
j) når en ***EU-certificeringsordning*** for administrerede sikkerhedstjenester i	j) når en ***europæisk cybersikkerhedscertificeringsordning*** for

henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning.	administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning.

Or. en

Ændringsforslag 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Kommissionens forslag	*Ændringsforslag*
j) når en EU-certificeringsordning for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning.	j) når en EU-certificeringsordning for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning ***inden for to år***.

Or. en

Begrundelse

Kommissionens forslag går ud på, at en certificeringsordning skal erstatte de tekniske krav, som er opstillet i denne forordning. Denne ændring giver virksomheder, navnlig SMV'er, mere tid til at overgå til denne ordning, hvilket fremmer mere lige vilkår i hele Unionen. Indtil da skal de overholde de tekniske krav i denne forordning.

Ændringsforslag 200
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Kommissionens forslag	*Ændringsforslag*
	ja) udbyderen skal kunne adskille deres tjenester fra den bredere kontrakt, så brugeren kan skifte til en anden tjenesteudbyder.

Or. en

Ændringsforslag 201
Evžen Tošenovský

Forslag til forordning
Artikel 17 – stk. 6

Kommissionens forslag	*Ændringsforslag*
6. Kommissionen koordinerer behandlingen af de modtagne anmodninger med den højtstående repræsentant og gennemførelsen af den støtte, der ydes til tredjelande fra EU's cybersikkerhedsreserve.	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.

Or. en

Ændringsforslag 202
Evžen Tošenovský

Forslag til forordning
Artikel 18

Kommissionens forslag	*Ændringsforslag*
Artikel 18	***udgår***
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 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 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.

4. Rapporten skal, hvor det er relevant, indeholde anbefalinger til forbedring af Unionens cyberposition.

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

Or. en

Ændringsforslag 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 eventuelle interessekonflikter.	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 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 eventuelle interessekonflikter.

Or. en

Ændringsforslag 204
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Forslag til forordning
Artikel 18 – stk. 3

Kommissionens forslag	*Ændringsforslag*
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.	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.***

Or. en

Ændringsforslag 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 18 – stk. 4

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

Or. en

Ændringsforslag 206
Johan Nissinen

Forslag til forordning
Artikel 18 – stk. 4

Kommissionens forslag	*Ændringsforslag*
4. Rapporten skal, hvor det er relevant, indeholde anbefalinger til forbedring af Unionens cyberposition.	4. Rapporten skal, hvor det er relevant, indeholde ***frivillige*** anbefalinger***, der ikke er juridisk bindende,*** til forbedring af Unionens cyberposition.

Or. en

Ændringsforslag 207
Evžen Tošenovský

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

Kommissionens forslag	*Ændringsforslag*
aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af ***nationale*** og ***grænseoverskridende SOC-platforme***, der	aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af ***CSIRT'er, ISAC'er*** og ***SOC'er***, der bidrager til et øget situationskendskab i

bidrager til et øget situationskendskab i Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler".	Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler".

Or. en

Ændringsforslag 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 19 – stk. 1 – nr. 3
Forordning (EU) 2021/694.
Artikel 14, stk. 2

Kommissionens forslag	*Ændringsforslag*
Programmet kan yde finansiering i enhver af de former, der er fastsat i finansforordningen, herunder navnlig gennem udbud som den primære form eller tilskud og priser.	Programmet kan yde finansiering i enhver af de former, der er fastsat i finansforordningen, herunder navnlig gennem udbud som den primære form eller tilskud og priser. ***ENISA modtager yderligere ressourcer til at udføre sine yderligere opgaver, der er fastsat i forordning XX/XXX (forordningen om cyberrobusthed). Denne yderligere finansiering må ikke bringe opfyldelsen af programmets mål i fare.***

Or. en

Ændringsforslag 209
Evžen Tošenovský

Forslag til forordning
Artikel 19 – stk. 1 – nr. 5
Forordning (EU) 2021/694.
Artikel 19

Kommissionens forslag	*Ændringsforslag*
Støtte i form af tilskud kan ydes direkte af ECCC uden forslagsindkaldelse til ***de nationale SOC'er***, der er omhandlet i	Støtte i form af tilskud kan ydes direkte af ECCC uden forslagsindkaldelse til ***CSIRT'er og ISAC'er***, der er omhandlet i

artikel 4 i forordning XXXX***, og værtskonsortiet***, der er omhandlet i artikel 5 i forordning XXXX, i overensstemmelse med finansforordningens artikel 195, stk. 1, litra d).	artikel 4 i forordning XXXX, der er omhandlet i artikel 5 i forordning XXXX, i overensstemmelse med finansforordningens artikel 195, stk. 1, litra d).

Or. en

Ændringsforslag 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 20 – overskrift

Kommissionens forslag	*Ændringsforslag*
Evaluering	Evaluering ***og revision***

Or. en

Ændringsforslag 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 [***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*** Europa-Parlamentet og Rådet en rapport. ***Ved evalueringen vurderes navnlig følgende:*** ***a) medlemsstaternes deltagelse i det europæiske cyberskjold, herunder antallet af nationale SOC'er og grænseoverskridende SOC'er, der er oprettet som led i forordningen, og***

effektiviteten af informationsudvekslingen

b) denne forordnings bidrag til at styrke Unionens modstandsdygtighed og suverænitet, forbedre de relevante industrisektorers konkurrenceevne, herunder SMV'er, og udvikle cybersikkerhedsfærdigheder i EU

c) brugen af cybersikkerhedsreserven, herunder om omfanget af reserven bør udvides til hændelsesberedskabstjenester eller fælles øvelser med de betroede udbydere og potentielle brugere af cybersikkerhedsreserven for at sikre, at reserven fungerer effektivt, når det er nødvendigt

d) denne forordnings bidrag til udvikling og forbedring af arbejdsstyrkens færdigheder og kompetencer inden for cybersikkerhedssektoren, der er nødvendige for at styrke Unionens kapacitet til at opdage, forebygge, reagere på og komme sig efter cybersikkerhedstrusler og -hændelser

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

På grundlag af denne rapport forelægger Kommissionen i givet fald Europa-Parlamentet og Rådet et lovgivningsforslag om ændring af denne forordning.

Or. en

Ændringsforslag 212
Evžen Tošenovský

Forslag til forordning
Artikel 20 – stk. 1

Kommissionens forslag	*Ændringsforslag*
Senest [fire år efter datoen for denne forordnings anvendelse] forelægger Kommissionen Europa-Parlamentet og	Senest [fire år efter datoen for denne forordnings anvendelse] forelægger Kommissionen Europa-Parlamentet og

Rådet en rapport om evaluering og revision af denne forordning.	Rådet en rapport om evaluering og revision af denne forordning. ***Rapporten ledsages om nødvendigt af et lovgivningsforslag.***

Or. en

Ændringsforslag 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Forslag til forordning
Artikel 20 – stk. 1 a (nyt)

Kommissionens forslag	*Ændringsforslag*
	Hvert år fremlægger Kommissionen ved forelæggelsen af budgetforslaget for det følgende år en detaljeret vurdering af ENISA's opgaver i henhold til denne forordning samt [forslaget til en forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer] og anden EU-lovgivning og beskriver de finansielle og menneskelige ressourcer, der er nødvendige for at udføre disse opgaver.

Or. en

Ændringsforslag 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Forslag til forordning
Artikel 20 a (ny)

Kommissionens forslag	*Ændringsforslag*
	Artikel 20a
	Udøvelse af 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 12, stk. 8, og artikel

13, stk. 7, tillægges Kommissionen for en periode på fem år fra ... [datoen for den lovgivningsmæssige basisretsakts ikrafttræden eller en anden dato fastsat af medlovgiverne]. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. 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 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 samtidig Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til 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 eller

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

Or. en

Ændringsforslag 215
Evžen Tošenovský

Forslag til forordning
Bilag I – stk. 1 – punkt 1
Forordning (EU) 2021/694.
I bilag I affattes afsnittet/kapitlet "Specifikt mål nr. 3 — Cybersikkerhed og tillid" således:

Kommissionens forslag	*Ændringsforslag*
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.	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 ***CSIRT'er*** og SOC'er, der udgør det europæiske cyberskjold, samt andre værktøjer, som skal gøres tilgængelige for offentlige og private sektorer i hele Europa.

Or. en

Ændringsforslag 216
Evžen Tošenovský

Forslag til forordning
Bilag I – stk. 1 – punkt 1
Forordning (EU) 2021/694.
I bilag I affattes afsnittet/kapitlet "Specifikt mål nr. 3 — Cybersikkerhed og tillid" således:

Kommissionens forslag	*Ændringsforslag*
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 ***cybersikkerhedsudbydere*** på EU-plan."	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."

Or. en