Europa-Parlamentet
2019-2024

Udenrigsudvalget

2023/0109(COD)

27.10.2023

UDTALELSE

fra Udenrigsudvalget

til Udvalget om Industri, Forskning og Energi

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

Ordfører for udtalelse: Dragoş Tudorache

PA_Legam

Ændringsforslag 1

Forslag til forordning
Betragtning 1

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

Ændringsforslag 2

Forslag til forordning
Betragtning 2

Kommissionens forslag	*Ændringsforslag*
(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage, 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	(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. ***Alvoren af disse trusler blev endnu mere tydelig, da der igen blev krig på vores kontinent. Disse trusler*** rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der tager del i de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og

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.	udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi ***og sikkerhed*** og sågar få sundhedsmæssige eller livstruende konsekvenser ***ved måske at underminere lokale eller nationale sikkerhedsrelaterede installationer***. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidigt eller spredes hurtigt til mange lande. ***Cybersikkerhed er vigtig for at beskytte vores europæiske værdier og sikrer, at vores demokratier fungerer, ved at beskytte vores valginfrastruktur og demokratiske procedurer mod enhver form for udenlandsk indblanding.***

Ændringsforslag 3

Forslag til forordning
Betragtning 2 a (ny)

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

Ændringsforslag 4

Forslag til forordning
Betragtning 3

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

Ændringsforslag 5

Forslag til forordning
Betragtning 4

Kommissionens forslag	*Ændringsforslag*
(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.	(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[17], Kommissionens henstilling (EU) 2017/1584[18], Europa-Parlamentets og Rådets direktiv 2013/40/EU[19] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[20]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt ***og proaktivt***, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked. ***Endvidere godkendte og lancerede Unionen sit strategiske kompas for sikkerhed og forsvar i marts 2022, som bl.a. har fokus på at styrke cybersikkerheden og forbedre det internationale samarbejde med ligesindede allierede og demokratiske partnere, navnlig om dette spørgsmål. Derudover har cybersikkerhed været et centralt punkt i den nylige tredje fælles erklæring om samarbejdet mellem EU og NATO fra januar 2023. Navnlig anbefaledes det i EU-NATO-taskforcens endelige vurderingsrapport, at der gøres fuld brug af synergierne mellem EU og NATO[1], herunder udveksling af bedste praksis mellem civile og militære aktører om gennemførelsen af relevante cyberrelaterede politikker og lovgivning.*** ***[1] https://commission.europa.eu/document/3***

4209534-3c59-4b01-b4f0-b2c6ee2df736_da

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

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

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

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

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

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

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

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

Ændringsforslag 6

Forslag til forordning
Betragtning 6

Kommissionens forslag	*Ændringsforslag*
(6) I den fælles meddelelse om EU's politik for cyberforsvar[22], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til at	(6) I den fælles meddelelse om EU's politik for cyberforsvar[22], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til at

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

Ændringsforslag 7

Forslag til forordning
Betragtning 6 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(6a) I betragtning af de stadig mere udviskede linjer mellem områderne for civile og militære anliggender og det forhold, at cyberværktøjer og -teknologier har dobbelt anvendelse, er der behov for en sammenhængende og holistisk tilgang til det digitale domæne. I tilfælde af en væsentlig cybersikkerhedshændelse og -krise, som involverer mere end én medlemsstat, bør der indføres passende krisestyring og -forvaltning. Sådanne strukturer bør tilrettelægge informationsudveksling, koordinering og samarbejde med Unionens eksterne sikkerhedsstrukturer og militære

krisestyringsstrukturer og medlemsstaternes organer med ansvar for sikkerhed og forsvar (cyberforsvarssektoren). Dette bør også gælde operationer og missioner, der gennemføres af Unionen under den fælles sikkerheds- og forsvarspolitik for at sikre fred og stabilitet i og uden for dens nabolande.

Ændringsforslag 8

Forslag til forordning
Betragtning 7

Kommissionens forslag	*Ændringsforslag*
(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør en paneuropæisk infrastruktur af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Der bør etableres en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige eller omfattende cybersikkerhedshændelser og sikre en omgående efterfølgende genopretning. Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).	(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør en paneuropæisk infrastruktur af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Der bør etableres en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige eller omfattende cybersikkerhedshændelser***, herunder hændelser, der involverer mere end én medlemsstat,*** og sikre en omgående efterfølgende genopretning. ***Når det er muligt og nødvendigt, bør en beredskabsmekanisme for cybersikkerhed tilrettelægge informationsudveksling og samarbejde med medlemsstaternes forsvarsmyndigheder med støtte fra EU's institutioner, organer og agenturer (EU's cyberforsvarssektor).*** Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke

	væsentlige eller omfattende hændelser. ***Sådanne nye strukturer bør også støtte EU's FSFP-operationer og -missioner.*** Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

Ændringsforslag 9

Forslag til forordning
Betragtning 11

Kommissionens forslag	*Ændringsforslag*
(11) Med henblik på forsvarlig økonomisk forvaltning bør særlige regler fastsættes for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i finansforordningen, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler.	(11) Med henblik på forsvarlig økonomisk forvaltning bør der fastsættes særlige regler for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i finansforordningen, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler. ***Disse særlige regler vil også give mulighed for mere langsigtet finansiel støtte til fælles indkøb af supersikre værktøjer og infrastruktur af næste generation for at forbedre den kollektive detektionskapacitet ved at anvende den sidste nye kunstige intelligens (AI) og dataanalyse.***

Ændringsforslag 10

Forslag til forordning
Betragtning 13

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

Ændringsforslag 11

Forslag til forordning
Betragtning 14

Kommissionens forslag	*Ændringsforslag*
(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet om cybersikkerhedstrusler, navnlig gennem deling af data fra forskellige	(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, ***herunder en "forsvarssøjle",*** så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet om cybersikkerhedstrusler, navnlig

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.	gennem deling af data fra forskellige offentlige eller private ***og – når det er nødvendigt og muligt – militære*** kilder ***med tilstrækkelig vejledning i informationsudveksling*** samt gennem deling og fælles anvendelse af avancerede værktøjer og fælles udvikling af detektions-, analyse- og forebyggelseskapaciteter i et sikkert miljø. De bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.

Ændringsforslag 12

Forslag til forordning
Betragtning 15

Kommissionens forslag	*Ændringsforslag*
(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv (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 supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge sådanne data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og ***modstandsdygtighed***.

Ændringsforslag 13

Forslag til forordning
Betragtning 16

Kommissionens forslag	*Ændringsforslag*
(16) De grænseoverskridende SOC'er	(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.

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

Ændringsforslag 14

Forslag til forordning
Betragtning 17

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

Ændringsforslag 15

Forslag til forordning
Betragtning 19

Kommissionens forslag	*Ændringsforslag*
(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig	(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer***, hvor højrisikoleverandører af kritiske produkter med digitale elementer udelukkes***. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og

intelligens og dataanalyse.	relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse. ***Der bør fastsættes bestemmelse om menneskeligt tilsyn i forbindelse med anvendelsen af AI, og der bør sikres et tilstrækkeligt niveau af AI-færdigheder, den nødvendige støtte og beføjelse til at udøve denne funktion.***

Ændringsforslag 16

Forslag til forordning
Betragtning 19 a (ny)

Kommissionens forslag	*Ændringsforslag*
	(19a) I overensstemmelse med forordning [XX/XXXX (forordningen om cyberrobusthed)] bør enheder, der deltager i det europæiske cyberskjold, også dække de krav, der er fastsat i denne forordning, for alle produkter med digitale elementer. I betragtning af de øgede risici, der kommer af økonomiske afhængighedsforhold, er det nødvendigt at minimere eksponeringen for højrisikoleverandører af kritiske produkter gennem en fælles strategisk ramme for EU's økonomiske sikkerhed. Afhængighed af højrisikoleverandører af kritiske produkter med digitale elementer udgør en strategisk risiko, som bør adresseres på EU-plan, navnlig hvorvidt et land giver sig af med økonomisk spionage eller økonomisk tvang, og dets lovgivning kræver vilkårlig adgang til enhver form for virksomhedsoperationer eller -data, navnlig når de kritiske produkter er beregnet til brug i væsentlige enheder som omhandlet i direktiv (EU) 2022/2555.

Ændringsforslag 17

Forslag til forordning
Betragtning 20

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

Ændringsforslag 18

Forslag til forordning
Betragtning 25

Kommissionens forslag	*Ændringsforslag*
(25) Cyberberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed	(25) Cyberberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed

("ENISA") i overensstemmelse med dets mandat[26], den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold og hybride beredskabshold. Cyberberedskabsmekanismen bør indgå i løsning af behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande.

("ENISA") i overensstemmelse med dets mandat, den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold***[1], det nye PESCO-projekt "Koordineringscenteret på cyber- og informationsområdet (CIDCC)" og den foreslåede efterfølger hertil, "EU-Koordinationscenteret for Cyberforsvar (EUCDCC)",*** og hybride beredskabshold. Cyberberedskabsmekanismen bør adressere behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande***, navnlig de EU-kandidatlande, der har bragt sig på linje med EU's fælles udenrigs- og sikkerhedspolitik og fælles sikkerheds- og forsvarspolitik, støtte dem med at opbygge deres cyberkapacitet og styrke det grænseoverskridende og regionale samarbejde blandt disse kandidatlande på cyberområdet***.

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

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

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

Ændringsforslag 19

Forslag til forordning
Betragtning 26

Kommissionens forslag	*Ændringsforslag*
(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[27], IPCR[28],, og direktiv (EU) 2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, ***hvor det er relevant***.	(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[27], IPCR[28],, og direktiv (EU) 2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, ***navnlig med henblik på at styrke kapaciteten til at imødegå cybersikkerhedstrusler fra lande uden for Unionen, herunder restriktive foranstaltninger, der kan anvendes til at forhindre og reagere på ondsindede cyberaktiviteter***.
[27] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).	[27] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).
[28] Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.	[28] Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

Ændringsforslag 20

Forslag til forordning
Betragtning 28

Kommissionens forslag	*Ændringsforslag*
(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at	(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at

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

Ændringsforslag 21

Forslag til forordning
Betragtning 29

Kommissionens forslag	*Ændringsforslag*
(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning	(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning

og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[29]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk

og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. ***Når det er hensigtsmæssigt, bør Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), navnlig gennem EU's Efterretnings- og Situationscenter (INTCEN) og dets analyseenhed for hybride trusler med støtte fra Den Europæiske Unions Militærstabs (EUMS') efterretningsdirektorat under den fælles efterretningsanalysekapacitet (SIAC), også tilknyttes for at levere ajourførte vurderinger og dermed bidrage til at indkredse de sektorer eller delsektorer, der*** bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer af særligt kritisk betydning"). De koordinerede afprøvningsøvelser bør være baseret på fælles risikoscenarier og -metoder. ***Disse øvelser bør også spille en vigtig rolle med hensyn til at forbedre samarbejdet mellem civile og militære enheder. I forbindelse med tilrettelæggelsen af øvelser bør Kommissionen, EU-Udenrigstjenesten og ENISA derfor systematisk overveje at medtage deltagere fra andre cybersamfund som f.eks. Det Europæiske Forsvarsagentur (EDA) og andre relevante enheder.*** Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-

infrastrukturs modstandsdygtighed.

samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554***[1]***. Ved udvælgelsen af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

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

---

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

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

Ændringsforslag 22

Forslag til forordning
Betragtning 32

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

Ændringsforslag 23

Forslag til forordning
Betragtning 33

Kommissionens forslag	*Ændringsforslag*
(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til 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	(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til støtte for indsatsen og foranstaltninger til omgående genopretning i tilfælde af væsentlige eller omfattende cybersikkerhedshændelser. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate. Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i kritiske eller meget kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. Når medlemsstaterne

anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer og agenturer på lignende betingelser.

anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer og agenturer***, herunder FSFP-missioner,*** på lignende betingelser.

Ændringsforslag 24

Forslag til forordning
Betragtning 34

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

Ændringsforslag 25

Forslag til forordning
Betragtning 36

Kommissionens forslag	*Ændringsforslag*
(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en	(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en

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

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

forordning. Rapporten bør leveres og indgå i arbejdet i EU-CyCLONe, CSIRT-netværket og Kommissionen. Når hændelsen vedrører et tredjeland, videresender Kommissionen også rapporten til den højtstående repræsentant***, EU-Udenrigstjenesten og en eventuel FSFP-mission i landet, som måtte være berørt af hændelsen, via deres hovedkvarterer***.

Ændringsforslag 26

Forslag til forordning
Betragtning 37

Kommissionens forslag	*Ændringsforslag*
(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medrører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor ***kan*** tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve***, hvis dette er fastsat i den respektive associeringsaftale til programmet for et digitalt Europa***. Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med	(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medfører høj risiko for afsmittende virkninger, bidrager styrkelsen af nabolandenes***, navnlig Ukraines og Moldovas,*** modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor ***bør*** tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve. ***Støtten bør også gælde de tredjelande, hvortil der er udsendt en FSFP-mission med et specifikt mandat til at styrke modstandsdygtigheden over for hybride trusler, herunder cybertrusler, eller for hvilke der er vedtaget en bistandsforanstaltning inden for rammerne af den europæiske fredsfacilitet for at styrke landets cyberrobusthed.*** Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og

programmet for et digitalt Europa.	omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med programmet for et digitalt Europa.

Ændringsforslag 27

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

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

Ændringsforslag 28

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

Kommissionens forslag	*Ændringsforslag*
a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og 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 og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske ***modstandsdygtighed*** på cybersikkerhedsområdet

Ændringsforslag 29

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

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

Ændringsforslag 30

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

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

Ændringsforslag 31

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

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

Ændringsforslag 32

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

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

Ændringsforslag 33

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

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

	forsvarsinteresser som fastsat i FUSP-rammen i henhold til afsnit V i TEU.

Ændringsforslag 34

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

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

Ændringsforslag 35

Forslag til forordning
Artikel 4 – stk. 2

Kommissionens forslag	*Ændringsforslag*
2. Efter en indkaldelse af interessetilkendegivelser udvælges de 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	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 ***under streng forudsætning af, at sådanne værktøjer og infrastrukturer leveres af betroede udbydere i overensstemmelse med artikel 16***. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de

nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.	resterende omkostninger afholdes af medlemsstaten. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og det nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

Ændringsforslag 36

Forslag til forordning
Artikel 5 – stk. 2

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

Ændringsforslag 37

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

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

udelukkes automatisk.

Ændringsforslag 38

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

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

Ændringsforslag 39

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

Kommissionens forslag	*Ændringsforslag*
	bb) understøtter en styrkelse af de deltagende medlemmers forsvarskapacitet eller forhindrer en direkte og overhængende trussel mod deres sikkerhed, og derved garanterer sikkerheden i forsyningskæderne, navnlig hvad angår enheder længere nede i

	kæderne, som ikke har brug for adgang til klassificerede oplysninger, men som kan udgøre alvorlige trusler mod hele sektoren.

Ændringsforslag 40

Forslag til forordning
Artikel 7 – stk. 1

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

Ændringsforslag 41

Forslag til forordning
Artikel 8 – stk. 1

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

udveksles via infrastrukturen.

Ændringsforslag 42

Forslag til forordning
Artikel 8 – stk. 2

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

Ændringsforslag 43

Forslag til forordning
Artikel 8 – stk. 3

Kommissionens forslag	*Ændringsforslag*
3. Kommissionen kan vedtage 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. I den forbindelse tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører ***og gør passende brug af hele den vifte af defensive muligheder, der er til rådighed for de civile og militære sektorer med henblik på EU's overordnede sikkerhed og forsvar, og underretter Europa-Parlamentet***.

Ændringsforslag 44

Forslag til forordning
Artikel 9 – stk. 2

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

Ændringsforslag 45

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

Kommissionens forslag	*Ændringsforslag*
a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU	a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer***, såsom offentlig infrastruktur, valginfrastruktur, transport, sundhedspleje, finans, telekommunikation, fødevareforsyning og -sikkerhed,*** i EU

Ændringsforslag 46

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

Kommissionens forslag	*Ændringsforslag*
c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3,	c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3,

litra f), i direktiv (EU) 2022/2555.	litra f), i direktiv (EU) 2022/2555 ***og inden for rammerne af artikel 42, stk. 7, i TEU og artikel 222 i TEUF***

Ændringsforslag 47

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

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

Ændringsforslag 48

Forslag til forordning
Artikel 11 – stk. 2

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

Ændringsforslag 49

Forslag til forordning
Artikel 12 – stk. 2

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

Ændringsforslag 50

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

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

Ændringsforslag 51

Forslag til forordning
Artikel 12 – stk. 4

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

Ændringsforslag 52

Forslag til forordning
Artikel 12 – stk. 5

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

Ændringsforslag 53

Forslag til forordning
Artikel 12 – stk. 7

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

Ændringsforslag 54

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

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

Ændringsforslag 55

Forslag til forordning
Artikel 15 – stk. 3

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

Ændringsforslag 56

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

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

Ændringsforslag 57

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

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

Ændringsforslag 58

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

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

Ændringsforslag 59

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

Kommissionens forslag	*Ændringsforslag*
	jb) udbyderen skal samarbejde tæt med relevante SMV'er, hvor det er muligt

Ændringsforslag 60

Forslag til forordning
Artikel 17 – stk. 1

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

bestemmelser herom.

a) de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom

b) de tredjelande, hvortil der er udsendt en FSFP-mission med et specifikt mandat til at styrke modstandsdygtigheden over for hybride trusler, herunder cybertrusler, eller hvor der er indført en bistandsforanstaltning inden for rammerne af den europæiske fredsfacilitet for at styrke landets cyberrobusthed.

Ændringsforslag 61

Forslag til forordning
Artikel 17 – stk. 2

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

Ændringsforslag 62

Forslag til forordning
Artikel 18 – stk. 1

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

Ændringsforslag 63

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

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

Ændringsforslag 64

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

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

rammen i henhold til afsnit V i TEU".

Ændringsforslag 65

Forslag til forordning
Artikel 20 – stk. 1

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

PROCEDURE I RÅDGIVENDE UDVALG

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

ENDELIG AFSTEMNING VED NAVNEOPRÅB
I RÅDGIVENDE UDVALG

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

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

0	0

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