Rådet for
Den Europæiske Union

Bruxelles, den 6. december 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Vedr.:	Rådets konklusioner om ENISA

Vedlagt følger til delegationerne Rådets konklusioner om ENISA som godkendt af Rådet på samlingen den 6. december 2024.

BILAG

Udkast til Rådets konklusioner om ENISA

RÅDET FOR DEN EUROPÆISKE UNION:

1. FREMHÆVER, at de udfordringer, der følger af det globale cyberspace, aldrig har været så komplekse, forskelligartede og alvorlige som nu på grund af nye avancerede cybertrusler, det konstant skiftende sikkerhedsmiljø og de aktuelle geopolitiske spændinger. EU og dets medlemsstater bør derfor arbejde videre på at øge modstandsdygtigheden, så de konkret kan identificere og håndtere nuværende og nye trusler og udfordringer, UNDERSTREGER, at arbejdet hen imod øget cyberrobusthed bør fortsættes efter en tilgang, som inddrager hele samfundet, UNDERSTREGER, at EU og medlemsstaterne i de kommende år bør fokusere på en effektiv gennemførelse af lovgivningsmæssige og ikkelovgivningsmæssige initiativer, der understøtter og bidrager til alle de foranstaltninger, der hidtil er blevet truffet i denne henseende;

2. MINDER OM, at den nationale sikkerhed fortsat er den enkelte medlemsstats eneansvar, og ANERKENDER, at EU og medlemsstaterne i de seneste år har haft et udstrakt samarbejde om at etablere den nødvendige institutionelle struktur og de nødvendige samarbejdsformer på både nationalt plan og EU-plan på cyberområdet, SER MED TILFREDSHED PÅ de forskellige lovgivningsmæssige og ikkelovgivningsmæssige initiativer, som på dette område har givet EU og medlemsstaterne en stærk og robust ramme, der øger Unionens overordnede cyberrobusthed. Denne ramme har udviklet sig til at dække flere aspekter af cyberområdet: sikkerhed, diplomati, retshåndhævelse og forsvar, NOTERER SIG, at et stort antal aktører, herunder medlemsstaternes cybersikkerhedsmyndigheder, NIS-samarbejdsgruppen (NIS CG), CSIRT-netværket, Den Europæiske Unions Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), netværket af nationale koordinationscentre (NCC), Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG), Kommissionen, Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC), CERT-EU, Det Europæiske Forsvarsagentur (EDA) og Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3), er en del af EU's cybersikkerhedsøkosystem og hver især udfører deres del af gennemførelsen af den EU-dækkende ramme for cybersikkerhed;

3. ANERKENDER, at ENISA i løbet af de seneste to årtier har vist sig at være en uvurderlig enhed i det europæiske cybersikkerhedsøkosystem og spiller en afgørende rolle med hensyn til aktivt at støtte medlemsstaterne og EU's institutioner, organer, kontorer og agenturer i deres gennemførelse og udvikling af cybersikkerhedspolitikker, deres kapacitetsopbygning og beredskab, deres samarbejde og deres fremme af cybersikkerhedsbevidsthed og -certificering;

GENERELLE HENSTILLINGER

4. OPFORDRER Kommissionen TIL at benytte **evalueringen af forordningen om cybersikkerhed** til at undersøge, hvordan den kan bidrage til at forenkle det komplekse cyberøkosystem og dermed øge effektiviteten og en effektiv anvendelse af ressourcer, OPFORDRER derfor Kommissionen TIL at sikre, at ENISA's mandat til at støtte medlemsstaterne og EU's institutioner, organer, kontorer og agenturer er fokuseret og klart defineret med konkrete strategiske mål og prioriterede opgaver ud over en mere præcis fordeling af opgaver og kompetencer med hensyn til andre aktører, OPFORDRER i den forbindelse Kommissionen TIL at undersøge og yderligere styrke ENISA's rolle med hensyn til at støtte operationelt samarbejde på EU-plan og blandt medlemsstaterne med henblik på at øge cyberrobustheden under hensyntagen til medlemsstaternes kompetencer på dette område, OPFORDRER desuden Kommissionen TIL at styrke ENISA's rådgivende rolle med hensyn til at give ekspert- og evidensbaserede vejledninger og henstillinger angående gennemførelsen af nuværende og fremtidige lovgivningsmæssige og ikkelovgivningsmæssige EU-initiativer, samtidig med at der sikres en sammenhængende EU-cybersikkerhedsramme;

5. TILSKYNDER i samme ånd Kommissionen TIL at overveje at strømline ENISA's rolle med hensyn til opgaver, der ikke er centrale for dets mission, UNDERSTREGER, at ENISA's **ansvarsområder er blevet udvidet betydeligt** gennem nylige lovgivningsinitiativer, herunder NIS 2-direktivet, forordningen om cyberrobusthed og forordningen om cybersolidaritet. NOTERER SIG, at ENISA har modtaget yderligere ressourcer som følge af nogle af disse initiativer, men FREMHÆVER, at udvidelsen af ENISA's ansvarsområder og cybertruslers og -udfordringers stigende kompleksitet har givet det langt flere opgaver, hvilket bør afspejles i **tilstrækkelige ressourcer** – menneskelige, finansielle og tekniske – så agenturet fuldt ud kan udføre alle de opgaver, der henhører under dets kompetence, uden at foregribe forhandlingerne om den flerårige finansielle ramme, OPFORDRER med henblik herpå Kommissionen TIL at prioritere foranstaltninger og opgaver, der støtter medlemsstaternes styrkelse af deres cyberrobusthed, deres operationelle samarbejde og udviklingen og gennemførelsen af EU-retten i forbindelse med udarbejdelsen af forslaget til Unionens almindelige budget;

ENISAS STØTTE TIL UDVIKLING OG GENNEMFØRELSE AF POLITIKKER

6. MINDER OM, at ENISA i henhold til den nuværende retlige ramme for cybersikkerhed har flere centrale støtte- og rådgivningsopgaver i hele EU, SER i denne forbindelse MED TILFREDSHED PÅ ENISA's rolle med hensyn til at yde **bistand til medlemsstaterne** med henblik på effektiv gennemførelse af lovgivningsmæssige og ikkelovgivningsmæssige initiativer, OPFORDRER ENISA TIL i tæt samarbejde med NIS-samarbejdsgruppen og Kommissionen fortsat at dele generelle erfaringer og analyser af de nuværende retlige rammer for cybersikkerhed, TILSKYNDER ENISA TIL at dele og aktivt fremme teknisk vejledning og bedste praksis på en regelmæssig og struktureret måde, der bistår medlemsstaterne med at gennemføre cybersikkerhedspolitik og -lovgivning;

7. ANERKENDER ENISA's afgørende rolle i udviklingen af **europæiske cybersikkerhedscertificeringsordninger**, der understøtter tilliden til IKT-produkter, -tjenester og -processer samt de administrerede sikkerhedstjenester i lyset af den kommende målrettede ændring af forordningen om cybersikkerhed, UNDERSTREGER, at medlemsstaterne og industrien er berørt af den langvarige proces med udvælgelse, udarbejdelse og vedtagelse af cybersikkerhedscertificeringsordninger, OPFORDRER derfor INDTRÆNGENDE Kommissionen TIL at benytte evalueringen af forordningen om cybersikkerhed til at finde en mere lempelig, risikobaseret og mere gennemsigtig og hurtigere tilgang til udviklingen af EU's cybersikkerhedscertificeringsordninger og UNDERSTREGER samtidig medlemsstaternes vigtige rolle i processen, FREMHÆVER desuden betydningen af udtrykkeligt at tildele ansvaret for vedligeholdelsen af hver certificeringsordning, MINDER endvidere OM, at ENISA rettidigt bør høre alle relevante interessenter ved hjælp af en formel, åben, gennemsigtig og inklusiv proces i forbindelse med udarbejdelsen af forslag til ordninger, og at Kommissionen bør høre alle relevante interessenter på en åben, gennemsigtig og inklusiv måde, når den vurderer effektiviteten og anvendelsen af vedtagne ordninger, TILSKYNDER ENISA TIL yderligere at styrke samarbejdet med databeskyttelsesmiljøet, navnlig Det Europæiske Databeskyttelsesråd, hvor det er relevant, og de nationale kompetente myndigheder, navnlig med henblik på at fremme synergier i forbindelse med udviklingen af fremtidige europæiske cybersikkerhedscertificeringsordninger;

8. OPFORDRER ENISA TIL i samarbejde med Kommissionen at fortsætte udvekslingen med medlemsstaterne om de praktiske aspekter, forenkling og strømlining af rapporteringsproceduren for at undgå, at der opstår unødvendig administrativ byrde som følge af en kompleks rapporteringsramme, MINDER endvidere OM sin opfordring til Kommissionen om med støtte fra ENISA og andre relevante EU-enheder at udarbejde en kortlægning af de relevante rapporteringsforpligtelser, der er fastsat i de respektive EU-retsakter om cyberspørgsmål og digitale spørgsmål, MINDER OM, at udveksling af oplysninger mellem ENISA og medlemsstaterne er baseret på et tillidsforhold, hvor sikkerhed og fortrolighed er garanteret i overensstemmelse med forordningen om cybersikkerhed og relevante regler og protokoller, og bør begrænses til, hvad der er relevant og står i et rimeligt forhold til formålet med udvekslingen, UNDERSTREGER behovet for, at data og oplysninger behandles med fornøden omhu;

9. FREMHÆVER, at ENISA er ansvarligt for at oprette og vedligeholde **den fælles rapporteringsplatform i henhold til forordningen om cyberrobusthed**, som vil have en konkret operationel merværdi, navnlig for aktivt udnyttede sårbarheder og alvorlige hændelser, der påvirker sikkerheden af produkter med digitale elementer. I betragtning af denne horisontale lovgivnings brede anvendelsesområde bør den fælles rapporteringsplatform være et effektivt og sikkert redskab til at lette udvekslingen af oplysninger mellem nationale CSIRT'er og ENISA, OPFORDRER derfor INDTRÆNGENDE ENISA TIL at fremskynde oprettelsen af platformen som en central prioritet og afsætte tilstrækkelige menneskelige ressourcer til at sikre, at den er klar inden for den frist, der er fastsat i forordningen om cyberrobusthed;

10. ANERKENDER ENISA's rolle i forbindelse med oprettelsen af et **europæisk sårbarhedsregister**, som skal skabe større gennemsigtighed med hensyn til offentliggørelse af sårbarheder og samtidig sikre en passende håndtering af følsomme oplysninger, OPFORDRER INDTRÆNGENDE ENISA TIL i betragtning af udløbet af gennemførelsesperioden for NIS 2-direktivet at øge det nødvendige arbejde for at sikre, at dette register fungerer gnidningsløst, OPFORDRER sideløbende hermed NIS-samarbejdsgruppen TIL med bistand fra ENISA yderligere at offentliggøre vejledninger, politikker og procedurer vedrørende offentliggørelse af sårbarheder;

11. ANERKENDER fordelene ved ENISA's **støtteforanstaltning for cybersikkerhed**, der fungerer som en pulje af cybersikkerhedstjenester, der er til rådighed for medlemsstaterne som supplement til deres bestræbelser, samt ENISA's erfaringer med gennemførelse deraf, FREMHÆVER i den forbindelse, at ENISA bør spille en central rolle i forvaltningen og driften af EU's cybersikkerhedsreserve, OPFORDRER ENISA TIL at påbegynde kortlægningen af de nødvendige tjenester og deres tilgængelighed, så snart forordningen om cybersolidaritet er trådt i kraft, så EU's cybersikkerhedsreserve i videst muligt omfang bliver nyttig og skræddersyet til brugernes behov i alle medlemsstater, OPFORDRER TIL, at ENISA efter overdragelsen af opgaven inddrager medlemsstaterne, navnlig ved at indsamle input om de krævede kriterier og informere om kommende udbud, tidligt i processen med at oprette EU's cybersikkerhedsreserve, OPFORDRER TIL, at ENISA efter overdragelsen af opgaven sikrer, at udvælgelsesprocessen for betroede udbydere af administrerede sikkerhedstjenester er gennemsigtig, åben og retfærdig, så udbydere fra alle medlemsstater uanset størrelse kan deltage, MINDER desuden OM, at ENISA er forpligtet til at udstede interoperabilitetsretningslinjer for de grænseoverskridende cyberknudepunkter uden unødig forsinkelse;

12. UNDERSTREGER, at **overvågning af tendenser inden for fremspirende teknologier** på et område i hastig udvikling såsom cybersikkerhed er afgørende for at opretholde og yderligere styrke vores cyberposition, ANERKENDER ENISA's hidtidige arbejde med at gøre offentligheden opmærksom på de risici og muligheder, der er forbundet med teknologier såsom kunstig intelligens og kvantecomputing, og dermed fremme en bedre forståelse af de aktuelle udfordringer, TILSKYNDER TIL, at ENISA bidrager yderligere til disse opgaver, aktivt arbejder for gennemførelsen af dets anbefalinger og rådgiver og samarbejder med ECCC, hvor det er relevant;

ENISA'S STØTTE TIL MEDLEMSSTATERNE FOR AT ØGE CYBERROBUSTHEDEN OG DET OPERATIONELLE SAMARBEJDE

13. UNDERSTREGER, at ENISA udfylder en vigtig rolle som **sekretariat for de to cybersamarbejdsnetværk på EU-plan drevet af medlemsstaterne, CSIRT-netværket og EU-CyCLONe**. FREMHÆVER ENISA's værdifulde deltagelse i NIS-samarbejdsgruppen, navnlig gennem dets aktive deltagelse og tekniske bidrag på de forskellige arbejdsområder, OPFORDRER ENISA TIL fortsat at støtte disse netværks funktion og samarbejde i fremtiden, da de udgør grundlæggende kanaler for medlemsstaternes samarbejde på forskellige niveauer;

14. GENTAGER behovet for at styrke den **fælles situationsbevidsthed** på EU-plan, som bidrager til EU's cyberposition i forhold til at opdage, forebygge og reagere på cybersikkerhedshændelser, UNDERSTREGER i den forbindelse betydningen af ENISA's fremsynsaktiviteter, regelmæssige rapporter og trusselsvurderinger, som alle er med til at forbedre situationsbevidstheden, TILSKYNDER TIL et tæt samarbejde mellem ENISA og medlemsstaterne om at bidrage til udviklingen af situationsbevidsthed på EU-plan, ANERKENDER i den forbindelse ENISA's vigtige rolle sammen med CERT-EU og Europol med hensyn til at støtte Rådet med statusbriefinger inden for rammerne af den cyberdiplomatiske værktøjskasse, der supplerer den situationsbevidsthed, som den fælles efterretningsanalysekapacitet (SIAC) giver, og UNDERSTREGER behovet for at opbygge et samlet trusselsbillede fra forskellige kilder, herunder den private sektor, TILSKYNDER i den forbindelse TIL videreudvikling af ENISA's samarbejde med EU-Udenrigstjenesten og navnlig med INTCEN med fuld respekt for deres respektive mandater;

15. FREMHÆVER, at Kommissionens cybersituations- og analysecenter varetager en intern funktion i Kommissionen og støttes af dets samarbejde med ENISA og CERT-EU. OPFORDRER Kommissionen TIL at tage resultaterne af evalueringen af forordningen om cybersikkerhed og drøftelserne om evalueringen af cyberplanen i betragtning med henblik på at strømline opgaverne for Kommissionens cybersituations- og analysecenter og ENISA's relaterede opgaver, så der skabes størst muligt potentiale for synergier og mindre kompleksitet i EU's cyberøkosystem, OPFORDRER Kommissionen til at undgå unødvendigt dobbeltarbejde og samtidig sikre ENISA's centrale rolle med hensyn til at bidrage til at udvikle en fælles situationsbevidsthed på EU-plan til støtte for medlemsstaterne under behørig hensyntagen til deres nationale kompetencer;

16. PÅPEGER, at udvikling af en fælles situationsbevidsthed er en forudsætning for rettidig og effektiv krisestyring i Unionen som helhed, UNDERSTREGER, at en række centrale aktører på EU-plan er involveret i **reaktionen på omfattende cybersikkerhedshændelser**, og at det effektive samarbejde mellem medlemsstaterne i tilfælde af sådanne hændelser hovedsageligt understøttes af CSIRT-netværket og EU-CyCLONe. ENISA spiller en vigtig rolle i cyberkrisestyringen som sekretariat for CSIRT-netværket og EU-CyCLONe, OPFORDRER Kommissionen TIL at anvende evalueringen af cyberplanen til korrekt at afspejle de yderligere opgaver og ansvarsområder med hensyn til at bidrage til at udvikle en samarbejdsorienteret reaktion på omfattende grænseoverskridende cyberhændelser eller -kriser samt den rolle, som ENISA har fået tildelt som sekretariat for CSIRT-netværket og EU-CyCLONe og af den seneste lovgivning om cybersikkerhed;

17. UNDERSTREGER betydningen af at tilrettelægge regelmæssige **cybersikkerhedsøvelser**, som i høj grad øger EU's beredskab til at reagere på hændelser og kriser, ANERKENDER, at ENISA har indsamlet værdifulde og omfattende erfaringer på dette område til støtte for medlemsstaterne, ANERKENDER ENISA's vigtige rolle i planlægnings-, forberedelses-, gennemførelses- og evalueringsfasen af cybersikkerhedsøvelser og FREMHÆVER, at det fortsat bør være en af de centrale aktører på EU-plan, idet det bemærkes, at sådanne øvelser bør gennemføres på grundlag af strukturerede rammer og fælles terminologier, OPFORDRER ENISA, CSIRT-netværket og EU-CyCLONe TIL at bruge eksisterende regelmæssige øvelser mest effektivt for at teste og forbedre EU's krisereaktionsramme og sikre maksimal udnyttelse af de indhøstede erfaringer;

ENISA'S SAMARBEJDE MED ANDRE AKTØRER I CYBERØKOSYSTEMET

18. GENTAGER, at **samarbejde mellem alle aktører på medlemsstats- og EU-plan** er afgørende på grund af den horisontale karakter af cybersikkerhed, og UNDERSTREGER derfor, at øget overordnet cyberrobusthed på europæisk plan også kræver et fælles arbejde mellem ENISA og andre relevante enheder på cyberområdet;

19. UNDERSTREGER, at EU's institutioner, organer og agenturers evne til at forblive cybersikre er af betydning for den overordnede cyberrobusthed på EU-plan, hvor CERT-EU's rolle er uvurderlig, SER i den forbindelse MED TILFREDSHED PÅ det etablerede strukturerede samarbejde mellem CERT-EU og ENISA og OPFORDRER dem TIL at fortsætte deres tætte samarbejde i fremtiden;

20. Med den opnåede finansielle autonomi vil ECCC bidrage væsentligt til udviklingen af et stærkt europæisk forskningsmæssigt, industrielt og teknologisk cyberøkosystem, der omfatter færdigheder til udvikling af arbejdsstyrken i overensstemmelse med sit mandat, TILSKYNDER ENISA og ECCC TIL at fortsætte deres tætte samarbejde, navnlig i forbindelse med forsknings- og innovationsbehov og -prioriteter samt cyberfærdigheder, for at øge konkurrenceevnen i Unionens cybersikkerhedsindustri, OPFORDRER Kommissionen TIL at undersøge, hvordan synergierne i ENISA's og ECCC's arbejdsmetoder kan optimeres yderligere, og hvordan aktiviteterne kan strømlines bedre i overensstemmelse med deres respektive mandater;

21. UNDERSTREGER, at regelmæssige opdateringer om trusselsbilledet bidrager til bedre at kunne identificere, hvilke foranstaltninger og værktøjer der er nødvendige for effektivt at bekæmpe cyberkriminalitet, FREMHÆVER merværdien af rapporterne fra EU's fælles cybervurdering (J-CAR), som er resultatet af det fælles samarbejde mellem ENISA, Europols EC3 og CERT-EU, og som allerede har givet værdifuldt input til håndteringen af de forskellige udfordringer, herunder bekæmpelse af cyberkriminalitet, OPFORDRER ENISA og Europol til fortsat at samarbejde på en struktureret måde i fremtiden;

22. PÅPEGER, at cyberforsvar udgør en vigtig og konstant voksende del af håndteringen af trusler fra cyberspace, FREMHÆVER behovet for, at ENISA samarbejder med EU-Udenrigstjenesten og Kommissionen i de tilfælde, hvor ENISA spiller en rolle med hensyn til at støtte gennemførelsen af EU's cyberforsvarspolitik i tæt samarbejde med EDA, ECCC og cyberforsvarsmiljøet, FREMHÆVER ENISA's rolle som et civilt agentur, UNDERSTREGER betydningen af at uddybe og strømline det civil-militære samarbejde på cyberområdet i EU, herunder en klar fordeling af roller og ansvarsområder mellem de to parter og mellem EU og NATO med fuld respekt for principperne om inklusion, gensidighed, gensidig åbenhed og gennemsigtighed samt begge organisationers beslutningsautonomi, TILSKYNDER ENISA TIL at fortsætte samarbejdsordningen med NATO's kommunikations- og informationsagentur;

23. TILSKYNDER EU TIL fortsat at fremme vores fælles værdier og fælles bestræbelser i globale fora for at sikre et frit, globalt, åbent og sikkert cyberspace, UNDERSTREGER, at cybertruslers og -hændelsers grænseoverskridende karakter kræver et stærkt og effektivt samarbejde, ikke kun på EU-plan, men også **med internationale organisationer og partnere**, BEMÆRKER, at ENISA's internationale engagement bør fokusere på strategiske partnere og EU-kandidatlande i overensstemmelse med EU's fælles udenrigs- og sikkerhedspolitik, UNDERSTREGER, at ENISA i sit internationale engagement bør handle i overensstemmelse med sit mandat og de respektive bestemmelser i forordningen om cybersikkerhed, ANERKENDER nødvendigheden af i overensstemmelse med de relevante procedurer at præcisere ENISA's internationale engagement og navnlig sikre, at dets bestyrelse underrettes behørigt og rettidigt om de dermed forbundne aktiviteter, TILSKYNDER ENISA TIL at deltage i relevante internationale rammer for cybersikkerhedssamarbejde, herunder organisationer som NATO og OSCE;

24. GENTAGER, at EU og dets medlemsstater ofte har fremhævet mangler i **cybersikkerhedsfærdigheder**, MINDER OM, at Kommissionen og ENISA har indført en bred og overordnet ramme for at yde vejledning til alle interessenter såsom den europæiske ramme for cybersikkerhedsfærdigheder, meddelelsen om akademiet for cybersikkerhedsfærdigheder og den årligt organiserede europæiske konference om cyberfærdigheder, og OPFORDRER Kommissionen og ENISA TIL at bygge videre på disse initiativer, navnlig med hensyn til de igangværende drøftelser om et konsortium for en europæiske digital infrastruktur (EDIC), OPFORDRER med henblik herpå Kommissionen TIL at samarbejde med de medlemsstater, der er interesserede i at oprette et EDIC, ANERKENDER, at både ENISA og ECCC har mandat til at fremme færdigheder i hele Unionen, OPFORDRER ENISA TIL at prioritere støtte til medlemsstaternes færdigheds- og uddannelsesindsats, øge bevidstheden i den brede befolkning og samarbejde med ECCC, hvor det er relevant;

25. ANERKENDER, at ENISA har udviklet et **samarbejde med den private sektor** i de seneste år, MINDER OM, at fordi den private sektor løbende overvåger cybertrusselsbilledet, kan de oplysninger, der indsamles af industrien, bidrage til at forbedre den fælles situationsbevidsthed, OPFORDRER derfor ENISA TIL i tæt samarbejde med medlemsstaterne og på tværs af EU-enheder at styrke samarbejdet med den private sektor;

26. OPFORDRER Kommissionen og ENISA TIL at overveje, hvordan samarbejdet mellem ENISA og de europæiske **standardisering**sorganer kan styrkes, UNDERSTREGER, at ENISA bør øge sin ekspertise inden for europæisk cybersikkerhedsstandardisering ved bl.a. at følge op på og deltage i standardiseringsaktiviteter;

27. OPFORDRER INDTRÆNGENDE Kommissionen og ENISA TIL at undersøge, hvordan EU's ramme for cybersikkerhed kan fungere optimalt under hensyntagen til henstillingerne og forslagene i disse konklusioner. Løbende samarbejde, prioritering af opgaver og ressourcer samt forenkling af det komplekse cybertrusselsbillede vil være centrale elementer til at håndtere de nuværende og fremtidige udfordringer.