Raad van de Europese Unie

Brussel, 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

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
Betreft:	Conclusies van de Raad over Enisa

De delegaties vinden in de bijlage de conclusies van de Raad over Enisa, zoals goedgekeurd door de Raad tijdens zijn zitting van 6 december 2024.

BIJLAGE

Ontwerpconclusies van de Raad over Enisa

DE RAAD VAN DE EUROPESE UNIE

1. WIJST EROP dat de uitdagingen die voortkomen uit de wereldwijde cyberspace nog nooit zo complex, divers en ernstig als nu zijn geweest, als gevolg van de geavanceerdheid van nieuwe cyberdreigingen, de voortdurend veranderende veiligheidsomgeving en de huidige geopolitieke spanningen. Daarom moeten de EU en haar lidstaten hun inspanningen voortzetten om weerbaarder te worden teneinde huidige en opkomende dreigingen en uitdagingen doeltreffend in kaart te brengen en aan te pakken. BENADRUKT dat de inspanningen om een hoger niveau van cyberweerbaarheid te bereiken, moeten worden voortgezet met een samenlevingsbrede aanpak. BEKLEMTOONT dat de EU en haar lidstaten zich in de komende jaren moeten richten op de doeltreffende uitvoering van wetgevings- en niet wetgevingsinitiatieven die alle maatregelen die tot dusver zijn genomen ondersteunen en eraan bijdragen.

2. HERINNERT ERAAN dat nationale veiligheid de exclusieve verantwoordelijkheid van elke lidstaat blijft en ONDERKENT dat de EU en haar lidstaten de afgelopen jaren geweldig hebben samengewerkt aan de totstandbrenging van de noodzakelijke institutionele structuren en samenwerkingsvormen op cybergebied, zowel op nationaal als op Unieniveau. IS INGENOMEN MET de verschillende wetgevings- en niet-wetgevingsinitiatieven die de EU en haar lidstaten een sterk en robuust kader hebben verschaft op dit gebied, waardoor de algehele cyberweerbaarheid van de Unie is vergroot. Dit kader heeft zich zodanig ontwikkeld dat het verschillende aspecten van het cyberdomein beslaat: veiligheid, diplomatie, rechtshandhaving en defensie. MERKT OP dat een groot aantal actoren, waaronder de cyberbeveiligingsautoriteiten van de lidstaten, de NIS-samenwerkingsgroep (NIS CG), het CSIRT-netwerk, het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), het Netwerk van nationale coördinatiecentra (NNC's), de Europese Groep voor cyberbeveiligingscertificering (EGC), de Commissie, de Europese Dienst voor extern optreden (EDEO), het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees Kenniscentrum voor cyberbeveiliging (ECCC), CERT-EU, het Europees Defensieagentschap (EDA) en het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol deel uitmaken van het cyberbeveiligingsecosysteem van de EU en elk een rol spelen bij de uitvoering van het EU-brede cyberbeveiligingskader.

3. ERKENT dat Enisa zich de afgelopen twee decennia heeft bewezen als een entiteit van onschatbare waarde in het Europese cyberbeveiligingsecosysteem, door een onmisbare rol te spelen met actieve ondersteuning van de lidstaten en de EU-instellingen, -organen en -instanties (EU-IOA's) bij de uitvoering en ontwikkeling van hun cyberbeveiligingsbeleid, hun capaciteitsopbouw en paraatheid, hun onderlinge samenwerking en hun bevordering van bewustwording en certificering op het gebied van cyberbeveiliging.

ALGEMENE BELEIDSAANBEVELINGEN

4. VERZOEKT de Commissie om **de evaluatie van de cyberbeveiligingsverordening** te benutten als een kans om na te gaan hoe deze kan bijdragen tot de vereenvoudiging van het complexe cyberbeveiligingsecosysteem en zo de doeltreffendheid en het efficiënte gebruik van middelen kan verbeteren. ROEPT de Commissie derhalve OP ervoor te zorgen dat het mandaat van Enisa om de lidstaten en de instellingen, organen en instanties van de EU (EU-IOA's) te ondersteunen, toegespitst en duidelijk omschreven is, met concrete strategische doelstellingen en prioritaire taken, naast een preciezere verdeling van taken en bevoegdheden ten opzichte van andere actoren. VERZOEKT de Commissie in dit verband de rol van Enisa bij de ondersteuning van de operationele samenwerking op EU-niveau en tussen de lidstaten bij het vergroten van de cyberweerbaarheid te onderzoeken en verder te versterken, waarbij rekening wordt gehouden met de bevoegdheden van de lidstaten op dit gebied. ROEPT de Commissie daarnaast OP tot versterking van de adviserende rol van Enisa bij het verstrekken van deskundige en empirisch onderbouwde richtsnoeren en aanbevelingen met betrekking tot de uitvoering van de huidige en toekomstige wetgevings- en niet-wetgevingsinitiatieven van de EU, en tegelijkertijd te zorgen voor een samenhangend EU-kader voor cyberbeveiliging.

5. MOEDIGT de Commissie in dezelfde geest AAN te overwegen de rol van Enisa met betrekking tot taken die niet tot de kern van zijn opdracht behoren, te vereenvoudigen. ONDERSTREEPT dat de **verantwoordelijkheden** van Enisa **aanzienlijk zijn uitgebreid** door recente wetgevingsinitiatieven, waaronder NIS 2, de verordening cyberweerbaarheid en de verordening cyber-solidariteit. WIJST EROP dat Enisa aanvullende middelen heeft ontvangen als gevolg van sommige van deze initiatieven, en BENADRUKT dat de verbreding van de verantwoordelijkheden van Enisa en de toenemende complexiteit van de cyberdreigingen en -uitdagingen hebben geleid tot een aanzienlijke toename van taken, wat tot uiting moet komen in **toereikende** – personele, financiële en technische – **middelen** om het Agentschap ten volle in staat te stellen alle onder zijn bevoegdheid vallende taken uit te voeren, zonder vooruit te lopen op de onderhandelingen over het meerjarig financieel kader. ROEPT de Commissie OP, gelet op het vorige, om bij het opstellen van het ontwerp van algemene begroting van de Unie prioriteit te geven aan acties en taken te prioriteren die in verband staan met het ondersteunen van de lidstaten bij het versterken van hun cyberweerbaarheid, hun operationele samenwerking en de ontwikkeling en uitvoering van het Unierecht.

ONDERSTEUNING DOOR ENISA VAN BELEIDSONTWIKKELING EN -UITVOERING

6. HERINNERT ERAAN dat Enisa op grond van het huidige rechtskader voor cyberbeveiliging in de hele EU verschillende belangrijke ondersteunende en adviserende verantwoordelijkheden heeft. IS in dit verband INGENOMEN MET Enisa's rol bij het verlenen van **ondersteuning aan de lidstaten** bij de doeltreffende uitvoering van wetgevings- en niet-wetgevingsinitiatieven. ROEPT Enisa OP om, in nauwe samenwerking met de NIS-samenwerkingsgroep en de Commissie, algemene inzichten en analyses te blijven verstrekken over het actuele juridische kader op het gebied van cyberbeveiliging. MOEDIGT Enisa AAN om technische richtsnoeren en beste praktijken te delen en actief onder de aandacht te brengen op regelmatige en gestructureerde wijze, en zo de lidstaten bij te staan bij de uitvoering van beleid en wetgeving op het gebied van cyberbeveiliging.

7. ERKENT de cruciale rol van Enisa bij de ontwikkeling van **Europese regelingen voor de certificering van cyberbeveiliging** die het vertrouwen onderstutten in ICT-producten, -diensten en -processen, en daarnaast in de beheerde-beveiligingsdiensten, in het licht van de komende gerichte wijziging van de verordening cyberbeveiliging. BEKLEMTOONT dat de lidstaten en het bedrijfsleven bezorgd zijn over het langdurige proces van selectie, uitwerking en vaststelling van regelingen voor de certificering van cyberbeveiliging. SPOORT de Commissie derhalve AAN de evaluatie van de cyberbeveiligingsverordening aan te grijpen om manieren te vinden voor een eenvoudiger, op risico's gebaseerde en tevens transparantere en snellere aanpak voor het ontwikkelen van EU-regelingen voor de certificering van cyberbeveiliging, en BEKLEMTOONT daarbij de belangrijke rol van de lidstaten in het proces. BENADRUKT bovendien dat het van belang is de verantwoordelijkheid voor de instandhouding van elke certificeringsregeling uitdrukkelijk toe te wijzen. HERINNERT ER voorts AAN dat Enisa bij de voorbereiding van potentiële regelingen tijdig alle relevante belanghebbenden moet raadplegen via een formeel, open, transparant en inclusief proces, en dat de Commissie op een open, transparante en inclusieve manier overleg moet plegen bij het beoordelen van de efficiëntie en bruikbaarheid van vastgestelde regelingen. MOEDIGT Enisa AAN de samenwerking met de gegevensbeschermingsgemeenschap verder te versterken, met name met het Europees Comité voor gegevensbescherming, waar nodig, en met de nationale bevoegde autoriteiten, met bijzondere aandacht voor het bevorderen van synergieën in de context van de ontwikkeling van toekomstige Europese regelingen voor cyberbeveiligingscertificering.

8. ROEPT Enisa OP om in samenwerking met de Commissie met de lidstaten van gedachten te blijven wisselen over de praktische aspecten, vereenvoudiging en stroomlijning van de rapportageprocedure om de onnodige administratieve lasten te voorkomen die zouden kunnen voortvloeien uit een complex rapportagekader. HERINNERT voorts AAN zijn verzoek aan de Commissie om, met de steun van Enisa en andere relevante EU-entiteiten, een overzicht op te stellen van de relevante rapportageverplichtingen die zijn vastgesteld in de respectieve wetgevingshandelingen van de EU op het gebied van cyber- en digitale aangelegenheden. HERINNERT ERAAN dat de uitwisseling van informatie tussen Enisa en de lidstaten is gebaseerd op een vertrouwensrelatie, waarbij de veiligheid en vertrouwelijkheid worden gewaarborgd overeenkomstig de cyberbeveiligingsverordening en de desbetreffende regels en protocollen, en beperkt moet blijven tot hetgeen relevant is voor en in verhouding staat tot het doel van de uitwisseling. BENADRUKT dat gegevens en informatie met de nodige zorgvuldigheid moeten worden behandeld.

9. BENADRUKT dat Enisa verantwoordelijk is voor het oprichten en onderhouden van **het centrale meldingsplatform in het kader van de verordening cyberweerbaarheid**, dat een concrete operationele meerwaarde zal hebben, met name voor actieve uitgebuite kwetsbaarheden en ernstige incidenten die gevolgen hebben voor de beveiliging van producten met digitale elementen. Gezien het brede toepassingsgebied van deze horizontale wetgeving moet het centrale meldingsplatform een doeltreffend en veilig instrument zijn om de uitwisseling van informatie tussen nationale CSIRT's en Enisa te vergemakkelijken. DRINGT ER derhalve bij Enisa OP AAN om, naast de toewijzing van voldoende personele middelen, de oprichting van het platform als topprioriteit te versnellen om ervoor te zorgen dat het binnen de in de verordening cyberweerbaarheid vastgestelde termijn gereed is.

10. ERKENT de rol van Enisa bij het opzetten van een **Europese kwetsbaarheidsdatabase**, die moet leiden tot meer transparantie met betrekking tot de openbaarmaking van kwetsbaarheden, waarbij gevoelige gegevens op een passende manier worden behandeld. DRINGT ER bij Enisa OP AAN, met het oog op het einde van de omzettingstermijn van de NIS 2-richtlijn, alles in het werk te stellen om de vlotte werking van deze database te waarborgen. VERZOEKT tegelijkertijd de NIS-samenwerkingsgroep, bijgestaan door Enisa, door te gaan met het publiceren van richtsnoeren, beleidsmaatregelen en procedures inzake de openbaarmaking van kwetsbaarheden.

11. ERKENT de voordelen van de **ondersteuningsactie voor cyberbeveiliging** van Enisa, die fungeert als een pool van cyberbeveiligingsdiensten die de lidstaten ter beschikking staan om hun inspanningen aan te vullen, alsook de ervaring die Enisa met de uitvoering ervan heeft opgedaan. BENADRUKT in dit verband dat Enisa een centrale rol moet spelen bij de exploitatie en het beheer van de EU-cyberbeveiligingsreserve. VERZOEKT Enisa onmiddellijk na de inwerkingtreding van de verordening cybersolidariteit te beginnen met het in kaart brengen van de benodigde diensten en de beschikbaarheid ervan, teneinde de EU-cyberbeveiligingsreserve zo nuttig mogelijk te maken en zo goed mogelijk af te stemmen op de behoeften van de gebruikers in alle lidstaten. VERZOEKT Enisa, zodra het daarmee is belast, de lidstaten te betrekken, met name door in een vroeg stadium van het proces van de instelling van de EU-cyberbeveiligingsreserve input te verzamelen over de vereiste criteria en informatie te verstrekken over komende aanbestedingen. VERZOEKT Enisa, zodra het daarmee is belast, ervoor te zorgen dat de selectieprocedure voor betrouwbare aanbieders van beheerde-beveiligingsdiensten transparant, open en eerlijk is en dat aanbieders uit alle lidstaten eraan kunnen deelnemen, ongeacht hun omvang. HERINNERT er bovendien AAN dat Enisa de interoperabiliteitsrichtsnoeren voor de landsgrensoverschrijdende cyberhubs onverwijld moet uitvaardigen.

12. ONDERSTREEPT dat **het monitoren van trends met betrekking tot opkomende technologieën** in een snel evoluerend domein zoals het cyberdomein van cruciaal belang is om onze cyberstrategie in stand te houden en verder te versterken. ERKENT het werk dat Enisa heeft verricht om de aandacht van het publiek te vestigen op de risico's en mogelijkheden van technologieën zoals artificiële intelligentie en kwantumcomputing, hetgeen leidt tot een beter inzicht in de huidige uitdagingen. MOEDIGT Enisa AAN verder bij te dragen aan deze taken, actief te pleiten voor de uitvoering van zijn aanbevelingen, en in voorkomend geval advies te verlenen en samen te werken met het ECCC.

STEUN VAN ENISA AAN DE LIDSTATEN OM DE CYBERWEERBAARHEID EN OPERATIONELE SAMENWERKING TE VERBETEREN

13. BENADRUKT dat Enisa een belangrijke rol vervult **als secretariaat van de twee door de lidstaten gestuurde cybersamenwerkingsnetwerken op EU-niveau, het CSIRT-netwerk en EU-CyCLONe**. BENADRUKT de waardevolle deelname van Enisa aan de NIS-samenwerkingsgroep, met name door zijn actieve betrokkenheid en technische bijdragen aan de verschillende werkstromen. MOEDIGT Enisa AAN de werking en samenwerking van deze netwerken in de toekomst te blijven ondersteunen, aangezien zij fundamentele kanalen bieden voor de lidstaten om op verschillende niveaus samen te werken.

14. HERHAALT dat het **gemeenschappelijk situationeel bewustzijn** op EU-niveau moet worden verbeterd, wat bijdraagt aan de cyberstrategie van de EU, met betrekking tot de opsporing, preventie en respons op cyberbeveiligingsincidenten. BENADRUKT in dit verband het belang van de prognoseactiviteiten, regelmatige verslagen en dreigingsevaluaties van Enisa, die allemaal bijdragen tot een beter situationeel bewustzijn. MOEDIGT Enisa AAN nauw samen te werken met de lidstaten om bij te dragen aan de ontwikkeling van het situationeel bewustzijn op EU-niveau. ERKENT in dit verband de belangrijke rol van Enisa, samen met CERT-EU en Europol, bij het ondersteunen van de Raad door middel van situatiebriefings in het kader van het instrumentarium voor cyberdiplomatie die het situationeel bewustzijn dat wordt geboden door de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC) aanvullen, en BENADRUKT dat er een alomvattend dreigingsbeeld moet worden gevormd op basis van verschillende bronnen, waaronder bronnen uit de particuliere sector. MOEDIGT in dit verband de verdere ontwikkeling aan van de samenwerking van Enisa met de EDEO, en met name met het EU-Intcen, met volledige inachtneming van hun respectieve mandaten.

15. BENADRUKT dat het cybersituatie- en -analysecentrum van de Commissie een interne functie binnen de Commissie vervult en wordt gesteund door zijn samenwerking met Enisa en CERT-EU. VERZOEKT de Commissie, teneinde het maximale potentieel voor synergieën te scheppen en de complexiteit binnen het cyberecosysteem van de EU te verminderen, rekening te houden met de resultaten van de evaluatie van de cyberbeveiligingsverordening en met de besprekingen over de evaluatie van de cyberblauwdruk, zodat de taken van het cybersituatie- en -analysecentrum van de Commissie en de daarmee verband houdende taken van Enisa kunnen worden gestroomlijnd. MOEDIGT de Commissie AAN onnodige overlapping van taken te voorkomen en tegelijkertijd de centrale rol van Enisa bij het bijdragen aan de ontwikkeling van een gemeenschappelijk situationeel bewustzijn op het niveau van de Unie te waarborgen ter ondersteuning van de lidstaten, met inachtneming van hun nationale bevoegdheden.

16. BENADRUKT dat de ontwikkeling van een gemeenschappelijk situationeel bewustzijn een voorwaarde is voor een tijdige en doeltreffende crisisbeheersing van de Unie als geheel. ONDERSTREEPT dat, op EU-niveau, een verscheidenheid aan belangrijke actoren betrokken is bij **de respons op grootschalige cyberbeveiligingsincidenten**, en dat, indien dergelijke incidenten zich voordoen, de doeltreffende samenwerking tussen de lidstaten voornamelijk wordt geschraagd door het CSIRT-netwerk en EU-CyCLONe. Enisa speelt een belangrijke rol bij cybercrisisbeheersing als secretariaat van het CSIRT-netwerk en EU-CyCLONe. VERZOEKT de Commissie de evaluatie van de cyberblauwdruk te benutten om een precies beeld te geven van de extra taken en verantwoordelijkheden voor de bijdrage aan de ontwikkeling van een gezamenlijke respons op grootschalige grensoverschrijdende cyberincidenten of -crises, alsook de rol die Enisa als secretariaat van het CSIRT-netwerk en EU-CyCLONe en door de recente wetgeving inzake cyberbeveiliging heeft gekregen.

17. ONDERSTREEPT het belang van het organiseren van regelmatige **oefeningen op het gebied van cyberbeveiliging**, die de paraatheid van de EU bij het reageren op incidenten en crises aanzienlijk vergroten. ERKENT dat Enisa waardevolle en uitgebreide ervaring heeft opgedaan op dit gebied bij de ondersteuning van de lidstaten. ERKENT de belangrijke rol van Enisa in de plannings-, voorbereidings-, uitvoerings- en evaluatiefasen van cyberbeveiligingsoefeningen, en BENADRUKT dat het een van de centrale actoren op EU-niveau moet blijven, ermee rekening houdend dat de uitvoering van dergelijke oefeningen gebaseerd moet zijn op gestructureerde kaders en gemeenschappelijke terminologie. VERZOEKT Enisa, het CSIRT-netwerk en EU-CyCLONe zo efficiënt mogelijk gebruik te maken van de bestaande regelmatige oefeningen om het EU-crisisresponskader te testen en te verbeteren, en ervoor te zorgen dat de geleerde lessen maximaal worden toegepast.

SAMENWERKING VAN ENISA MET ANDERE ACTOREN IN HET CYBERECOSYSTEEM

18. HERHAALT dat **de samenwerking tussen alle actoren op het niveau van de lidstaten en de Unie** vanwege de horizontale aard van cyberbeveiliging van vitaal belang is, en ONDERSTREEPT daarom dat het vergroten van de algehele cyberweerbaarheid op Europees niveau ook gezamenlijke werkzaamheden vereist van Enisa en andere betrokken entiteiten op cybergebied.

19. ONDERSTREEPT dat het vermogen van de EU-IOA's om cyberveilig te blijven van belang is voor de algehele cyberweerbaarheid op EU-niveau, waarbij de rol van CERT-EU van onschatbare waarde is. IS in dit verband INGENOMEN met de gevestigde gestructureerde samenwerking tussen CERT-EU en Enisa en MOEDIGT hen AAN hun nauwe samenwerking in de toekomst voort te zetten.

20. Met de bereikte financiële autonomie zal het ECCC aanzienlijk bijdragen tot de ontwikkeling van een sterk Europees ecosysteem voor onderzoek, industrie en technologie op cybergebied, dat vaardigheden voor personeelsontwikkeling omvat, overeenkomstig zijn mandaat. MOEDIGT Enisa en het ECCC AAN hun nauwe samenwerking voort te zetten, met name met betrekking tot de behoeften en prioriteiten op het gebied van onderzoek en innovatie, alsook met betrekking tot cybervaardigheden, om het concurrentievermogen van de cyberbeveiligingssector van de Unie te vergroten. VERZOEKT de Commissie na te gaan hoe synergieën in de werking van Enisa en het ECCC verder kunnen worden geoptimaliseerd en hoe de activiteiten beter kunnen worden gestroomlijnd overeenkomstig hun respectieve mandaten.

21. ONDERSTREEPT dat regelmatige updates over het dreigingslandschap helpen om beter in kaart te brengen welke maatregelen en instrumenten nodig zijn om cybercriminaliteit doeltreffend te bestrijden. WIJST OP de toegevoegde waarde van de verslagen over de gezamenlijke cyberevaluatie (J-CAR) van de EU, die het resultaat zijn van de gezamenlijke samenwerking tussen Enisa, het EC3 van Europol en CERT-EU, en die reeds waardevolle input hebben opgeleverd voor het aanpakken van de verschillende uitdagingen, waaronder de bestrijding van cybercriminaliteit. VERZOEKT Enisa en Europol in de toekomst op gestructureerde wijze te blijven samenwerken.

22. BENADRUKT dat cyberdefensie een belangrijk onderdeel vormt van de aanpak van dreigingen die voortvloeien uit cyberspace en dat dit onderdeel constant in ontwikkeling is. WIJST OP de noodzaak voor Enisa om samen te werken met het EDEO en de Commissie in de gevallen waarin Enisa een rol speelt bij de ondersteuning van de uitvoering van het EU-beleid inzake cyberdefensie, in nauwe samenwerking met het EDA, het ECCC en de cyberdefensiegemeenschap. BENADRUKT de rol van Enisa als civiel agentschap. ONDERSTREEPT dat het belangrijk is de civiel-militaire samenwerking op cybergebied binnen de EU te verdiepen en te stroomlijnen, onder andere door de taken en verantwoordelijkheden tussen de twee gemeenschappen en de EU en de NAVO duidelijk te onderscheiden, met volledige inachtneming van de beginselen van inclusiviteit, wederkerigheid, wederzijdse openheid en transparantie, alsook van de beslissingsautonomie van beide organisaties. MOEDIGT Enisa AAN werkafspraken te blijven maken met het Agentschap voor communicatie en informatie van de NAVO.

23. MOEDIGT de EU AAN onze gemeenschappelijke waarden en gezamenlijke inspanningen in mondiale fora te blijven bevorderen om een vrije, mondiale, open en veilige cyberspace te waarborgen. BENADRUKT dat het grensoverschrijdende karakter van cyberdreigingen en -incidenten een sterke en doeltreffende samenwerking vereist, niet alleen op EU-niveau, maar ook **met internationale organisaties en partners**. MERKT OP dat de internationale betrokkenheid van Enisa zich moet toespitsen op strategische partners en kandidaat-lidstaten van de EU, in overeenstemming met het gemeenschappelijk buitenlands en veiligheidsbeleid van de EU. BENADRUKT dat Enisa bij zijn internationale betrokkenheid moet handelen in overeenstemming met zijn mandaat en de respectieve bepalingen van de cyberbeveiligingsverordening. ERKENT dat de internationale betrokkenheid van Enisa overeenkomstig de desbetreffende procedures moet worden verduidelijkt, met name door ervoor te zorgen dat zijn raad van bestuur naar behoren en tijdig wordt geïnformeerd over de desbetreffende activiteiten. MOEDIGT de deelname van Enisa aan de desbetreffende internationale samenwerkingskaders op het gebied van cyberbeveiliging AAN, met inbegrip van organisaties zoals de NAVO en de OVSE.

24. HERHAALT dat de EU en haar lidstaten vaak hebben gewezen op lacunes in **vaardigheden op het gebied van cyberbeveiliging**. HERINNERT ERAAN dat de Commissie en Enisa een breed en overkoepelend kader hebben ingevoerd om richtsnoeren te verstrekken aan alle belanghebbenden, zoals het Europees kader voor vaardigheden op het gebied van cyberbeveiliging, de mededeling over de academie voor cyberbeveiligingsvaardigheden en de jaarlijks georganiseerde Europese conferentie over cybervaardigheden, en MOEDIGT de Commissie en Enisa AAN voort te bouwen op deze initiatieven, waarbij bijzondere aandacht moet uitgaan naar de lopende discussie over het Europees consortium voor digitale infrastructuur (EDIC). VERZOEKT de Commissie daartoe in contact te treden met de lidstaten die een EDIC willen opzetten. ERKENT dat zowel Enisa als het ECCC verantwoordelijk zijn voor het bevorderen van vaardigheden in de hele Unie. VERZOEKT Enisa prioriteit te geven aan het ondersteunen van de inspanningen van de lidstaten op het gebied van vaardigheden en onderwijs, het versterken van het algemeen bewustzijn van het publiek, en waar nodig samen te werken met het ECCC.

25. ERKENT dat Enisa de afgelopen jaren een **samenwerking met de particuliere sector** tot stand heeft gebracht. HERINNERT eraan dat de door de sector verzamelde informatie kan bijdragen tot een beter gemeenschappelijk situationeel bewustzijn, aangezien de particuliere sector het cyberdreigingslandschap voortdurend monitort. MOEDIGT Enisa derhalve AAN om, in nauwe samenwerking met de lidstaten en over alle EU-entiteiten heen, de samenwerking met de particuliere sector te versterken.

26. ROEPT de Commissie en Enisa OP na te gaan hoe de samenwerking tussen Enisa en de Europese **normalisatie**-instellingen kan worden verbeterd. BENADRUKT dat Enisa zijn deskundigheid inzake Europese normalisatie op het gebied van cyberbeveiliging moet vergroten door onder meer normalisatieactiviteiten op te volgen en aan dergelijke activiteiten deel te nemen.

27. DRINGT ER bij de Commissie en Enisa OP AAN na te gaan hoe de werking van het EU-kader voor cyberbeveiliging verder kan worden geoptimaliseerd, rekening houdend met de aanbevelingen en voorstellen die in deze conclusies zijn gedaan. Doorlopende samenwerking, prioritering van taken en middelen alsook het vereenvoudigen van het complexe cyberlandschap zullen essentiële elementen zijn om de huidige en toekomstige uitdagingen het hoofd te bieden.