Raad van de
Europese Unie

**Brussel, 22 mei 2023**
**(OR. en)**

**9618/23**

| | |
|---|---|
| **COPS 269** | **JAI 656** |
| **POLMIL 123** | **RELEX 639** |
| **CYBER 130** | **JAIEX 22** |
| **HYBRID 31** | **TELECOM 154** |
| **EUMC 230** | **IPCR 38** |
| **CIVCOM 144** | **PROCIV 35** |
| **COPEN 162** | **COTER 101** |
| **COSI 103** | **DISINFO 34** |
| **DATAPROTECT 146** | **CSC 252** |
| **IND 256** | **CSDP/PSDC 402** |
| **RECH 191** | **CFSP/PESC 748** |

**RESULTAAT BESPREKINGEN**

| | |
|---|---|
| van: | het secretariaat-generaal van de Raad |
| aan: | de delegaties |
| nr. vorig doc.: | ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674 |
| Betreft: | Conclusies van de Raad over het cyberdefensiebeleid van de EU |

Hierbij gaan voor de delegaties de conclusies van de Raad over het cyberdefensiebeleid van de EU, die de Raad tijdens zijn zitting van 22 mei 2023 heeft goedgekeurd.

**Conclusies van de Raad over het cyberdefensiebeleid van de EU**

1. Op basis van het uit 2014 daterende, en in 2018 geactualiseerde, beleidskader voor cyberdefensie is de Raad ingenomen met de ambitieuze gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie, waaruit de bedoeling spreekt om verder te investeren in onze moderne en interoperabele strijdkrachten, geavanceerde technologieën en hoog ontwikkelde cyberdefensievermogens en partnerschappen te versterken teneinde gemeenschappelijke uitdagingen aan te gaan. Cyberspace is een terrein voor strategische concurrentie geworden, in tijden van toenemende afhankelijkheid van digitale technologieën. Het is dan ook van essentieel belang een open, vrije, stabiele en beveiligde cyberspace in stand te houden. De cyberoperaties die Ruslands iedere aanleiding of grond ontberende aanvalsoorlog tegen Oekraïne mogelijk hebben gemaakt en deze daarna hebben begeleid, hebben gevolgen voor de mondiale stabiliteit en veiligheid, vormen een belangrijk risico op escalatie en werken de reeds aanzienlijke toename van kwaadwillige cyberactiviteiten buiten de context van gewapende conflicten van de afgelopen jaren in de hand.

2. De oorlog in Oekraïne heeft een nieuwe strategische context geschapen, waaruit eens te meer blijkt dat de EU, haar lidstaten en hun partners de weerbaarheid van de EU tegen cyber-dreigingen verder moeten vergroten en wij onze gemeenschappelijke cyberbeveiliging en cyberdefensie tegen kwaadwillige gedragingen en agressie in cyberspace moeten versterken. De gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie geeft er blijk van dat wij vastbesloten zijn maatregelen op de onmiddellijke en de lange termijn aan te reiken om de handelingsvrijheid in cyberspace te garanderen en te reageren op dreigings-actoren die onder meer proberen in netwerk- en informatiesystemen van de EU en haar partners binnen te dringen of deze te verstoren of te vernietigen. Met deze gezamenlijke mededeling, die een aanvulling vormt op de EU-strategie inzake cyberbeveiliging en strookt met het strategisch kompas, wordt een grote stap gezet naar een EU-totaalaanpak inzake weerbaarheid, respons, conflictpreventie, samenwerking en stabiliteit in cyberspace. In dit verband onderstreept de Raad de noodzaak van passende en coherente antwoorden van de EU, haar lidstaten en hun partners, en ziet hij ook uit naar de herziening van de uitvoerings-richtsnoeren van het EU-instrumentarium voor cyberdiplomatie als nóg een belangrijke stap vooruit in de evolutie van de cybermentaliteit van de EU.

3. De Raad benadrukt dat recente cyberaanvallen op Europese kritieke infrastructuur, het snel evoluerende cyberdreigingslandschap en het snelle tempo van de technologische ontwikkeling ook de noodzaak aantonen van nauwere civiel-militaire coördinatie en samenwerking, waarbij duidelijk moet zijn dat er tussen de civiele en militaire gemeenschappen geen hiërarchie bestaat.

   Dankzij het EU-cyberdefensiebeleid kunnen de EU en haar lidstaten hun vermogen tot bescherming, opsporing, verdediging en ontmoediging versterken en daarbij adequaat gebruikmaken van het hele scala van defensieve opties waarover de civiele en militaire gemeenschappen beschikken voor de bredere beveiliging en defensie van de EU, conform het internationaal recht, met inbegrip van het recht inzake de mensenrechten en het internationaal humanitair recht.

4. Hoewel de nationale veiligheid, ook op cybergebied, uitsluitend de verantwoordelijkheid van elke lidstaat blijft, zoals vastgelegd in artikel 4, lid 2, VEU, benadrukt de Raad tegelijkertijd dat er zowel afzonderlijk als in samenwerking aanzienlijk moet worden geïnvesteerd in een grotere weerbaarheid en de inzet van het gehele spectrum bestrijkende cyberdefensie-vermogens en met gebruikmaking van EU-samenwerkingskaders en financiële stimulansen als hefboom. De Raad wijst erop dat de maatregelen van de lidstaten en de EU-instellingen, organen en instanties (EU-IOA's) verder moeten worden versterkt om de Unie, onze burgers, de EU-IOA's en GVDB-missies en -operaties in cyberspace te beschermen. Daarnaast wijst hij op het belang van de weerbaarheid van de EU in cyberspace door het ontwikkelen van cyberdefensievermogens en van de samenwerking met een betrouwbaar particulier ecosysteem.

I. **Samen werken aan een krachtigere cyberdefensie**

5. De Raad herhaalt dat een stapsgewijs, transparant en inclusief proces van essentieel belang is voor het vergroten van het vertrouwen, wat van cruciaal belang is voor de verdere ontwikkeling van een EU-kader voor crisisbeheersing op het gebied van de cyberveiligheid, die moet geschieden in overeenstemming met het in de Raad ontwikkelde stappenplan voor cybercrisisbeheersing. De Raad herhaalt dat wij ons vermogen tot bescherming, opsporing, verdediging en ontmoediging van cyberaanvallen moeten blijven versterken door middel van een verbeterd situationeel bewustzijn, capaciteitsopbouw, vermogensontwikkeling, opleiding, oefeningen en versterkte weerbaarheid, alsmede door krachtig en met alle passende middelen te reageren op cyberaanvallen tegen de EU, haar lidstaten en de EU-IOA's, de GVDB-missies en -operaties. Tegelijkertijd moedigt de Raad de hoge vertegenwoordiger en de Commissie aan de complexiteit op cybergebied te verminderen, onnodige overlapping te vermijden en samenwerking en synergieën met bestaande initiatieven tot stand te brengen. Er moet nauwer worden samengewerkt en gecoördineerd tussen de cyberdefensieactoren binnen de EU en de lidstaten, tussen de militaire en civiele cybergemeenschappen en tussen het publieke domein en een betrouwbaar particulier ecosysteem. In dit verband worden de lidstaten aangemoedigd de civiel-militaire nationale coördinatiemechanismen verder te verkennen en te versterken, gemeenschappelijke vrijwillige informatie-uitwisseling te faciliteren, geleerde lessen te delen, bij te dragen aan het ontwikkelen van interoperabele normen, risicobeoordelingen te verrichten en risicoscenario's op te stellen, evenals gezamenlijke oefeningen, met name op Europees niveau, met volledige inachtneming van het bepaalde in de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2).

6. De Raad erkent de inspanningen om de weerbaarheid van de Unie verder te vergroten door middel van NIS 2 en de richtlijn betreffende de weerbaarheid van kritieke entiteiten (CER), en herhaalt zijn aanbeveling voor een EU-brede gecoördineerde aanpak om de veerkracht van kritieke infrastructuur te versterken[1]. Hij roept op tot maatregelen om de weerbaarheid van kritieke entiteiten, infrastructuur, digitale producten en diensten verder te vergroten, maar merkt op dat de correcte uitvoering van NIS 2 de belangrijkste stap blijft. Hoewel dit voornamelijk een civiele verantwoordelijkheid is, versterkt het ook de cyberdefensie. In dit verband worden de EU-IOA's en de lidstaten aangemoedigd om steun te verlenen aan de verdere ontwikkeling en inzet van nieuwe en bestaande EU-coördinatiemechanismen, risicobeoordelingen, evaluaties en scenario's, gemeenschappelijke vrijwillige informatie-uitwisseling en oefeningen, en wel zo dat dit een meerwaarde oplevert, zonder onnodige overlapping met bestaande initiatieven.

7. Voor een verder versterken van het vertrouwen, consolideren van de samenwerking en faciliteren van tijdige uitwisseling van informatie over significante, grootschalige cyberincidenten die gevolgen hebben voor defensiesystemen, begroet de Raad het initiatief om de door elk voorzitterschap van de Raad van de EU te organiseren conferentie van EU-cybercommandanten verder te ontwikkelen, met de steun van het Europees Defensie-agentschap (EDA) en de deelname van de Europese Dienst voor extern optreden (EDEO). De Raad moedigt alle lidstaten aan om aan deze bijeenkomsten deel te nemen. Met het oog op een grotere weerbaarheid van de EU tegen grootschalige cyberveiligheidsincidenten verzoekt de Raad het Europees Netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) en de conferentie van EU-cybercommandanten mogelijke manieren te verkennen om samen te werken en profijt te hebben van een gezamenlijk militair en civiel perspectief.

[1] Voorstel voor een aanbeveling van de Raad betreffende een gecoördineerde aanpak van de Unie om de veerkracht van kritieke infrastructuur te versterken (COM(2022) 551 final).

8. Met het oog op een krachtigere en beter gecoördineerde respons op EU-niveau verwelkomt de Raad de oprichting van het operationeel netwerk van militaire computercrisisresponsteams van de EU (MICNET) voor een intensievere uitwisseling van technische informatie over cyberincidenten die gevolgen hebben voor defensiesystemen tussen de deelnemende lidstaten, en ziet hij uit naar het tijdstip van medio 2024, wanneer het MICNET de initiële operationele capaciteit zal bereiken. De Raad moedigt alle lidstaten aan deel te nemen aan het MICNET, om de effectiviteit van het netwerk te waarborgen. Voorts verzoekt de Raad de lidstaten voort te bouwen op de lessen die zijn getrokken uit het netwerk van Computer Security Incident Response Teams (CSIRT's) en moedigt hij het ten zeerste aan dat te gelegener tijd een doeltreffend mechanisme voor samenwerking en coördinatie tussen de twee netwerken wordt opgezet met volledige inachtneming van de governancemechanismen en gebruikersgroepen van elke entiteit.

9. Gezien de toename van kwaadwillige cyberactiviteiten van zowel overheids- als niet-overheidsactoren tegen GVDB-missies en -operaties van de EU, verzoekt de Raad de EU en haar lidstaten hun vermogens tot verdediging en beveiliging van GVDB-missies en -operaties te versterken. In dit verband is de Raad ingenomen met de doelstellingen voor verdere ontwikkeling van de bescherming van de militaire netwerken en structuren van de EU in overeenstemming met onder meer de militaire visie en strategie van de EU inzake cyberspace als domein van operaties[2].

[2] EEAS(2021) 706 REV 4.

10. De Raad herhaalt zijn conclusies van mei 2022[3] en de noodzaak te investeren in onze wederzijdse bijstand op grond van artikel 42, lid 7, VEU, alsmede de solidariteitsclausule van artikel 222 VWEU. De Raad acht het van groot belang dat de EU en de lidstaten, in overeenstemming met de desbetreffende beginselen van het internationaal recht, het gemeenschappelijke begrip van de uitvoering van artikel 42, lid 7, verder verdiepen, onder meer voor complexe scenario's waarbij sprake is van een cyberaanval. De Raad is ingenomen met de mogelijkheid dat de EU, op uitdrukkelijk verzoek van de betrokken lidstaat of lidstaten, ondersteuning verleent wanneer er een cyberaanval plaatsvindt, onverminderd het specifieke karakter van het veiligheids- en defensiebeleid van bepaalde lidstaten.

11. De Raad onderstreept de vooruitgang met het PESCO-project voor snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging (CRRT's), alsmede zijn bereidheid om enerzijds desgevraagd de behoeften van de lidstaten en de EU te faciliteren, ter ondersteuning van GVDB-missies en -operaties, en anderzijds EU-partners bij te staan. De Raad ziet uit naar de verdere ontwikkeling van de CRRT-capaciteit van de PESCO, de nationale cyberresponsteams en, in voorkomend geval, de aanvullende responscapaciteiten bij incidenten, zoals de in het strategisch kompas beoogde toekomstige snellereactieteams bij hybride dreigingen, onder meer via bevordering van hun coördinatie en samenwerking op EU-niveau.

[3] Conclusies van de Raad over de ontwikkeling van een cyberstrategie van de Europese Unie, 23 mei 2022 (doc. 9364/22).

12. De Raad is ingenomen met de werkzaamheden van het Coördinatiecentrum voor het cyberinformatiedomein (CIDCC), een PESCO-project dat tot doel heeft militaire capaciteit ter beschikking te stellen voor het verzamelen en analyseren van informatie die relevant is voor een gemeenschappelijk operationeel cyberbeeld. De Raad is voorts ingenomen met zowel het voorstel om de proof of concept, indien deze succesvol is als informatiecentrum, vanaf 2025 te integreren in een EU-coördinatiecentrum voor cyberdefensie (EUCDCC), en zo de coördinatie en het situationeel bewustzijn van met name commandanten van GVDB-missies en -operaties van de EU te verbeteren, alsmede met de versterking van de bredere EU-commando- en controlearchitectuur. De Raad verzoekt de hoge vertegenwoordiger een concept en een routekaart voor de oprichting van het EUCDCC voor te leggen, waarbij lering wordt getrokken uit soortgelijke internationale entiteiten, de benodigde middelen in kaart worden gebracht, onnodig dubbel werk wordt vermeden, en gestreefd wordt naar complementariteit met het bredere cyberbeveiligingskader van de EU.

13. De Raad wijst op het belang van strategische samenwerking op het vlak van inlichtingen over cyberdreigingen en -activiteiten, en verzoekt de lidstaten om via hun bevoegde autoriteiten te blijven bijdragen aan de activiteiten van het EU-Intcen, van het directoraat Inlichtingen van de EUMS en van de lidstaten in het kader van de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC). De Raad benadrukt voorts hoe belangrijk het is om onze cyberinlichtingencapaciteit te versterken en zo onze cyberweerbaarheid en -respons te vergroten en onze civiele en militaire GVDB-missies en -operaties, onze strijdkrachten en de capaciteit van de SIAC op cybergebied, doeltreffend te ondersteunen op basis van vrijwillige inlichtingenbijdragen van de lidstaten, zonder evenwel afbreuk te doen aan hun bevoegdheden.

14. De Raad neemt nota van het cybersituatie- en -analysecentrum van de Europese Commissie, dat tot doel heeft het situationeel bewustzijn van de Commissie te vergroten. De Raad acht het van groot belang dat er tussen dit centrum en andere EU-IOA's, met name Enisa en CERT-EU, wederzijds voordelige samenwerking tot stand wordt gebracht. De Raad onderstreept het belang van zowel nauwe samenwerking met de samenwerkingsnetwerken van de EU bij de ontwikkeling van situationeel bewustzijn, als de inachtneming van vertrouwelijkheid.
De Raad merkt op dat het gemeenschappelijk situationeel bewustzijn op EU-niveau moet worden versterkt en dat het EU-kader voor respons op cybercrises verder moet worden ontwikkeld, waarbij onnodig dubbel werk vermeden dient te worden.

15. De Raad brengt in herinnering dat onderwijs, opleiding en oefeningen op cybergebied essentieel zijn voor paraatheid en doeltreffendheid, en is ingenomen met de nationale activiteiten en die van de EU via de Europese Veiligheids- en defensieacademie (EVDA), het EDA, Enisa en lopende PESCO-projecten, zoals de onderlinge koppelingen van cybertest-voorzieningen (Cyber Ranges Federations - CRF) en de EU-cyberacademie en innovatiehub (CAIH). De Raad ziet met het oog op verdere intensivering van dit alles uit naar het EDA-kaderproject CyDef-X ter synchronisatie en ondersteuning van cyberdefensieoefeningen.
De Raad moedigt het EDA aan om, in nauwe samenwerking met de lidstaten en de EDEO, te bekijken hoe met CyDef-X oefeningen zoals CYBER PHALANX verder ondersteund kunnen worden, onder meer wat betreft wederzijdse bijstand uit hoofde van artikel 42, lid 7, VEU en de solidariteitsclausule uit hoofde van artikel 222 VWEU, en voorts om dat tevens met de Commissie en Enisa te doen wat betreft civiele oefeningen. Daarnaast ziet de Raad graag dat bestaande test- en oefenomgevingen voor cyberdefensie, zoals onderlinge koppelingen van cybertestvoorzieningen, gebruikt worden binnen CyDef-X en daar verder worden ontwikkeld.
De Raad acht het voor een flexibele en efficiënte besluitvorming bij cybercrises van belang dat er regelmatig theoretische simulatieoefeningen worden gehouden voor het besluitvormingsniveau van de lidstaten.

16. De Raad neemt nota van het voorstel voor een wet inzake cybersolidariteit en van het voornemen om het vermogen om cyberdreigingen en -incidenten in de EU op te sporen en aan te pakken, te vergroten. De Raad onderstreept dat voorstellen op dit vlak pas doeltreffend zijn als ze afgestemd worden op de crisisbeheersingskaders en -behoeften van de lidstaten.
De Raad onderstreept het belang van het testen van kritieke infrastructuur op potentiële kwetsbaarheden, voor zover dit nuttig wordt geacht, als een nationale bevoegdheid, met inachtneming van de risicobeoordelingen die de EU beschikbaar heeft.

17. De Raad neemt nota van het voorstel van de Commissie om een cybernoodmechanisme in te richten ter ondersteuning van de beschikbaarheid van cyberbeveiligingsdiensten van betrouwbare particuliere aanbieders om in geval van grootschalige cyberincidenten de lidstaten op verzoek bij te staan, daarbij onderstrepend dat de voor dit mechanisme essentiële Europese cyberbeveiligingssector met steun van het ECCC moet worden opgeschaald.
De Raad wijst op de sleutelrol van elke lidstaat bij de monitoring en beoordeling van zijn nationale behoeften.

## II. **Het defensie-ecosysteem van de EU beveiligen**

18. De Raad herhaalt zijn aanmoediging aan de lidstaten om hun eigen capaciteiten op het gebied van cyberdefensieoperaties verder te ontwikkelen, met inbegrip van, in voorkomend geval, proactieve defensieve maatregelen om zich tegen cyberaanvallen te beschermen en te verdedigen en deze op te sporen en tegen te gaan. Aangezien de NIS 2-richtlijn niet van toepassing is op overheidsinstanties die actief zijn op defensiegebied, verzoekt de Raad het EDA om, in voorkomend geval met steun van de Commissie en de EDEO, de lidstaten te helpen op basis van NIS2 niet-juridisch bindende vrijwillige aanbevelingen te ontwikkelen ter vergroting van de cyberbeveiliging in de defensiegemeenschap, alsmede verzoekt hij alle lidstaten daar actief aan deel te nemen. Bij deze aanbevelingen moet rekening worden gehouden met soortgelijke initiatieven binnen andere kaders.

19. Zoals ook in het strategisch kompas gesteld wordt, hangt het vermogen van de EU om op te treden af van de vraag of zij in staat is om op het vlak van cyberdefensievermogens en -toeleveringsketens haar strategische afhankelijkheden te verminderen en om geavanceerde cyberdefensietechnologieën te ontwikkelen en te beheersen. Onder meer moet daartoe in de hele EU de Europese technologische en industriële defensiebasis (EDTIB) worden versterkt en ook het vermogen om op basis van wederkerigheid ter wederzijds voordeel samen te werken met gelijkgestemde partners over de hele wereld. De Raad roept de cyberbeveiligings- en de cyberdefensie-industrie derhalve op nauw samen te werken voor de nodige synergie ter ontwikkeling en totstandbrenging van cyberdefensievermogens over het volledige spectrum. De Raad verzoekt de Commissie om, in voorkomend geval in nauwe samenwerking met het ECCC, via verdere investeringen en beleidsmaatregelen te blijven helpen bij de ontwikkeling van een sterke, flexibele, wereldwijd concurrerende en innovatieve Europese industriële en technologische basis voor cyberdefensie, met inbegrip van kleine en middelgrote ondernemingen (kmo's).

20. Aangezien het van groot belang is dat cyberdefensievermogens interoperabel en gemeenschappelijk van karakter zijn, ook als het gaat om de gezamenlijke ontwikkeling van cyberdefensievermogens van de volgende generatie, verzoekt de Raad het EDA en de Militaire Staf van de EU een reeks EU-interoperabiliteitseisen voor cyberdefensie te ontwikkelen, die voortbouwen op en verenigbaar zijn met bestaande beginselen, processen en normen zoals die met name zijn vastgesteld in het kader van de Noord-Atlantische Verdragsorganisatie (NAVO). Voorts verzoekt de Raad de lidstaten om in het Europees normalisatiecomité voor defensie na te gaan of er specifieke vrijwillige normen voor defensiesystemen nodig kunnen zijn en om dat te doen in nauwe samenwerking met alle relevante belanghebbenden, in voorkomend geval met inbegrip van Europese normalisatieorganisaties en de NAVO.

21. De Raad is ingenomen met de inspanningen van de Commissie om een plan voor te leggen ter bevordering van zowel het gebruik van bestaande normen voor civiele cyberveiligheid en cyberdefensietoepassingen als de ontwikkeling van nieuwe vrijwillige normen. De Raad benadrukt dat de normen inzake cyberbeveiliging en cyberdefensie waar nodig op elkaar moeten worden afgestemd. De Raad ziet het mogelijke nut van dergelijke vrijwillige normen voor de cyberbeveiligings- en cyberdefensie-industrie van de EU en dringt aan op nauwere samenwerking tussen civiele en defensienormalisatie-instellingen.

22. De Raad pleit voor een spoedige ontwikkeling van aanbevelingen op basis van een door de Commissie en de betrokken instellingen uitgevoerde inventarisatie van de bestaande instrumenten voor beveiligde communicatie op cybergebied. Die aanbevelingen moeten waar mogelijk worden afgestemd op bestaande initiatieven op het vlak van informatie-uitwisseling en tevens rekening houden met de uit de opkomende en disruptieve technologieën voortvloeiende risico's voor de huidige versleutelingsmethoden.

23. Voorts is de Raad ingenomen met de eerste stappen die op zijn verzoek door de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep zijn gezet op het vlak van risicobeoordeling en risicoscenario's voor, in eerste instantie, de energie- en de telecommunicatiesector. De Raad is zich ervan bewust dat er ook gerichte cyberbeveiligings-risicobeoordelingen voor communicatie-infrastructuur en -netwerken in de EU worden voorbereid. De Raad herhaalt dat het van het grootste belang is dat de lidstaten, maar ook de instellingen, organen en agentschappen van de EU, een gemeenschappelijke visie hebben op de mogelijke gevolgen van cyberincidenten. De Raad verzoekt de bovengenoemde actoren er derhalve voor te zorgen dat bij de vaststelling en prioritering van maatregelen en ondersteuning, op EU- en in voorkomend geval op nationaal niveau, rekening wordt gehouden met risico-evaluaties en -scenario's en daaropvolgende aanbevelingen. De Raad dringt er voorts op aan dat alle relevante actoren bij risicobeoordelingsprocessen en bij de ontwikkeling van cyberoefeningen rekening houden met de risicoscenario's.

III. **Investeren in cyberdefensievermogens**

24. De Raad moedigt de lidstaten aan meer te investeren in de opbouw, het in stand houden en de verdere ontwikkeling van interoperabele cyberdefensievermogens. De Raad steunt het opstellen van een reeks vrijwillige toezeggingen voor de verdere ontwikkeling van nationale cyberdefensievermogens, rekening houdend met soortgelijke inspanningen die worden geleverd in andere kaders.

25. De Raad roept de lidstaten en het EDA op om de herziening van het vermogens-ontwikkelingsplan aan te grijpen om een hoog ambitieniveau vast te stellen met betrekking tot de ontwikkeling van een gezamenlijke cyberdefensie op EU-niveau. De Raad moedigt de lidstaten verder aan voort te bouwen op de geactualiseerde reeks prioriteiten en hun PESCO-verbintenissen om hun betrokkenheid bij EU-samenwerkingsprojecten voor de ontwikkeling van cyberdefensievermogens te vergroten, en erkent daarbij dat samenwerkingsprojecten op EU-niveau ter ondersteuning van de ontwikkeling van nationale cyberdefensievermogens onmiddellijk voordeel opleveren.

26. De Raad is ingenomen met de gezamenlijke onderzoeksinspanningen op EU-niveau om de mogelijke toepassingen in defensiegerelateerde systemen van opkomende en disruptieve technologieën te onderzoeken, en merkt tevens op dat deze technologische ontwikkelingen snel in de bestaande en toekomstige vermogens moeten worden geïntegreerd. De Raad moedigt de lidstaten en de EU-industrie aan optimaal gebruik te maken van de gezamenlijke mogelijkheden voor onderzoek op EU-niveau, bijvoorbeeld in het kader van het EDA, lopende PESCO-projecten, zoals de EU-cyberacademie en innovatiehub (EU CAIH), het Europees Defensiefonds en, indien toepasselijk, Horizon Europa en het programma Digitaal Europa voor projecten voor tweeërlei gebruik. Voorts is de Raad ingenomen met het benutten van de specifieke kaders ter ondersteuning van defensie-innovatie door gebruik te maken van spin-ins uit het civiele domein, met name de EU-regeling voor defensie-innovatie en de hub voor Europese defensie-innovatie. Voorts moedigt de Raad het Europees Kenniscentrum voor cyberbeveiliging (ECCC) en het EDA aan een werkregeling op te stellen om informatie-uitwisseling tussen elkaars personeel over, respectievelijk, prioriteiten op het gebied van civiele technologie, technologie voor tweeërlei gebruik en defensietechnologie te faciliteren, teneinde synergieën tot stand te brengen en dubbel werk te voorkomen.

27. De Raad is ingenomen met het voornemen van de Commissie om, in samenwerking met het EDA en het ECCC, overeenkomstig hun respectieve mandaten, met de lidstaten en in overleg met relevante belanghebbenden, zoals de industrie, een technologieroutekaart voor kritieke cybertechnologieën op te stellen, die, door de kritieke cybertechnologieën te identificeren en technologische ontwikkelingen en strategische afhankelijkheden in kaart te brengen, manieren biedt om die afhankelijkheden te verminderen, ter ondersteuning van de strategische autonomie en technologische soevereiniteit van de EU, met behoud van een open economie. De Raad merkt op dat de technologieroutekaart als basis kan dienen voor het vaststellen van de strategische prioriteiten van de financieringsinstrumenten van de EU in overeenstemming met de respectieve daarvoor geldende voorwaarden. De Raad herinnert eraan dat de EU een ambitieus en assertief Europees industriebeleid moet voeren ten behoeve van een duurzaam, aantrekkelijk en concurrerend ondernemingsklimaat, dat ook Europese entiteiten op cybergebied in staat kan stellen op te schalen.

28. De Raad waardeert het voornemen om het aanzienlijke tekort aan cyberbeveiligings-vaardigheden aan te pakken door nieuwe, ook vrouwelijke, professionals aan te trekken, door bij- en omscholing en door het investeren in en het organiseren van opleidingen en oefeningen, teneinde een divers en inclusief personeelsbestand op cybergebied op te bouwen. De Raad erkent de uitdagingen waarmee de EU wordt geconfronteerd inzake menselijk kapitaal op het gebied van cyberbeveiliging en cyberdefensie, en is ingenomen met het initiatief voor een academie voor cyberbeveiligingsvaardigheden, dat ook ten goede kan komen aan het cyberdefensiepersoneelsbestand.

29. De Raad verzoekt de lidstaten informatie uit te wisselen over beste praktijken voor de opleiding van cyberbeveiligingsprofessionals, waarbij de synergieën tussen militaire, civiele en rechtshandhavingsinitiatieven worden benut, en roept de EVDA op om, met de steun en deskundigheid van het EDA en Enisa, na te gaan hoe de uitwisseling van beste praktijken en verdere synergieën tussen de militaire en civiele domeinen op het gebied van opleiding en de ontwikkeling van cyberspecifieke defensievaardigheden kan worden verbeterd.

30. De Raad onderstreept het belang van een gemeenschappelijk begrip van de samenstelling van het cyberbeveiligingspersoneelsbestand en van de bijbehorende vaardigheden om de lacunes op de cyberbeveiligingsarbeidsmarkt in kaart te brengen en aan te pakken, alsook de noodzaak om alle belanghebbenden, met inbegrip van de lidstaten en de industrie, daarbij te betrekken. De Raad erkent dat het vaststellen van indicatoren voor het monitoren van de cyberbeveiligingsarbeidsmarkt zou helpen om de behoeften op het gebied van cyberbeveiligingsvaardigheden te identificeren en de middelen passend toe te wijzen, en tegelijkertijd zou bijdragen tot het nakomen van de beleidsgerelateerde verplichtingen, met name die welke voortvloeien uit de NIS 2. De Raad is ingenomen met het voorstel voor een kader voor de certificering van cyberdefensievaardigheden en verzoekt de hoge vertegenwoordiger, in zijn hoedanigheid van hoofd van de EVDA, dat kader in samenwerking met de EDEO, de Commissie en de lidstaten te ontwikkelen door civiele initiatieven te benutten.

## IV. **Partnerschappen aangaan om gemeenschappelijke uitdagingen aan te pakken**

31. De Raad roept de hoge vertegenwoordiger en de Commissie op hun samenwerking te versterken en te bevorderen en wederzijds voordelige en op maat gesneden partnerschappen rond cyberdefensiebeleid te verkennen, onder meer op het gebied van capaciteitsopbouw voor cyberdefensie via de Europese Vredesfaciliteit (EPF). Daartoe moet cyberdefensie als onderwerp worden toegevoegd aan de cyberdialogen en -raadplegingen van de EU en het algemene veiligheids- en defensieoverleg met de partners. Voorts moeten de dialogen en de samenwerking met de particuliere sector worden versterkt. De Raad onderstreept dat internationale samenwerking op het gebied van cyberbeveiligingsnormen en -certificering een toegevoegde waarde voor de Europese industrie zou zijn. Hij is dan ook ingenomen met de toezegging van de Commissie om dit tot een essentieel onderdeel te maken van de cyberdialogen van de EU met derde landen en internationale organisaties.

32. De Raad benadrukt het belang van internationale samenwerking om de risico's op conflicten in cyberspace te voorkomen of te verminderen, met name door de verdere ontwikkeling en operationalisering van vertrouwenwekkende maatregelen (CBM's) op regionaal en internationaal niveau, onder meer op het niveau van de VN, en door het gebruik van bestaande cyber-CBM's, zoals bij de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE), verder aan te moedigen, ook in tijden van internationale spanningen.
De EU en haar lidstaten benadrukken dat het bestaande internationale recht van toepassing is op de cyberspace, en benadrukken het belang van voortdurende inspanningen om het VN-kader voor verantwoordelijk gedrag van staten te handhaven en te bevorderen en te werken aan de uitvoering ervan, onder meer door de vaststelling van het actieprogramma ter bevordering van verantwoordelijk gedrag van staten in de cyberspace.

33. Overeenkomstig de gezamenlijke verklaringen over de samenwerking tussen de EU en de NAVO verzoekt de Raad de hoge vertegenwoordiger, mede in zijn hoedanigheid van hoofd van het EDA, en de Commissie om het partnerschap op cybergebied met de NAVO verder te versterken, te verdiepen en uit te breiden met volledige inachtneming van de beginselen van inclusiviteit, wederkerigheid, wederzijdse openheid en transparantie en de beslissings-autonomie van beide organisaties. Rekening houdend met de noodzaak om te zorgen voor complementaire en gecoördineerde inspanningen met een zo groot mogelijke betrokkenheid van de lidstaten die geen deel uitmaken van de NAVO en om onnodige overlappingen te voorkomen, roept de Raad op om op de relevante niveaus verbanden tot stand te brengen tussen de EU en de NAVO op het gebied van opleiding, onderwijs, situationeel bewustzijn, oefeningen en O&O-platforms, en te zoeken naar mogelijke synergieën tussen de respectieve vrijwillige toezeggingen voor de ontwikkeling van de nationale cyberdefensievermogens en de crisisbeheersingskaders, de bescherming van kritieke infrastructuur en de intensivering van de uitwisselingen over situationeel bewustzijn, gecoördineerde reacties op kwaadwillige cyberactiviteiten en inspanningen voor capaciteitsopbouw in derde landen. Dit omvat de technische regeling tussen de responscapaciteit voor computerincidenten van de NAVO (NCIRC) en het computercrisisresponsteam van de EU (CERT-EU), alsmede een versterkte politieke dialoog over cyberdefensiekwesties op alle niveaus.

## V. **Conclusie**

34. Voortbouwend op de conclusies van de Raad over het cyberdefensiebeleid van de EU roept de Raad de hoge vertegenwoordiger en de Commissie op om uiterlijk in het tweede kwartaal van 2023 een uitvoeringsplan voor het beleid op te stellen ter goedkeuring door de lidstaten. De Raad verzoekt de lidstaten ook vrijwillig hun ambitie en acties met betrekking tot cyberdefensie kenbaar te maken in het kader van het cyberdefensiebeleid van de EU en ten volle gebruik te maken van niet-juridisch bindende vrijwillige aanbevelingen en toezeggingen om hun nationale en multinationale cyberdefensie-inspanningen op te voeren teneinde het effect op EU-niveau te maximaliseren. De hoge vertegenwoordiger, de Commissie en de lidstaten wordt verzocht om vanaf het tweede kwartaal van 2024 jaarlijks verslag uit te brengen en besprekingen te houden over de voortgang bij de uitvoering van de onderdelen van de gezamenlijke mededeling en het bijbehorende uitvoeringsplan.