Raad van de
Europese Unie

Brussel, 10 december 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
Betreft:	Extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen - Conclusies van de Raad (10 december 2019)

Voor de delegaties gaan hierbij de conclusies van de Raad over extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen, die de Raad tijdens zijn 3739e zitting op 10 december 2019 heeft aangenomen.

BIJLAGE

Conclusies van de Raad over extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen

1. De Raad herinnert aan de desbetreffende conclusies van de Europese Raad[1] en de Raad[2], en verklaart zich te blijven inzetten voor de versterking van de weerbaarheid van de Unie en haar lidstaten tegen de vele facetten omvattende en steeds veranderende hybride bedreigingen en ter verbetering van de samenwerking met het oog op het opsporen, voorkomen en bestrijden ervan.

2. De Raad erkent de vooruitgang die is geboekt bij de uitvoering van het gezamenlijk kader voor de bestrijding van hybride bedreigingen (2016) en de gezamenlijke mededeling over het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen (2018), alsmede van het actieplan tegen desinformatie (2018), overeenkomstig de desbetreffende conclusies van de Raad.

3. De verantwoordelijkheid voor de bestrijding van hybride bedreigingen ligt in eerste instantie bij de lidstaten. De inspanningen op EU-niveau zijn complementair van aard en laten de verantwoordelijkheid van de lidstaten op het gebied van de nationale veiligheid onverlet. Voor de aanpak van hybride bedreigingen, met een meer strategische, gecoördineerde en coherente werkwijze in alle relevante beleidssectoren is een alomvattende veiligheidsaanpak nodig waarbij de hele overheid en de hele samenleving betrokken zijn. Het is belangrijk dat een overheidsbrede aanpak wordt gevolgd en ook op EU-niveau wordt toegepast.

4. In deze conclusies bepaalt de Raad prioriteiten met betrekking tot de bescherming van onze samenlevingen, burgers en vrijheden en de veiligheid van onze Unie tegen hybride bedreigingen in de context van de uitvoering van de nieuwe strategische agenda voor 2019-2024, door het bevorderen van een alomvattende benadering van veiligheid met betere coördinatie, middelen en technologische capaciteiten, waarbij wordt voortgebouwd op het belangrijke werk dat reeds in verschillende beleidssectoren is verricht, onder meer in het kader van de EU-samenwerking op het gebied van veiligheid en defensie.

---

1 Met name de conclusies van de Europese Raad van juni 2019, maart 2019, december 2018, oktober 2018, juni 2018, maart 2018, juni 2015 en maart 2015.

2 Met name ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16

5. De inspanningen om onze democratische instellingen tegen hybride bedreigingen te beschermen, moeten altijd de grondrechten in acht nemen, waaronder de bescherming van persoonsgegevens, de vrijheid van meningsuiting en informatie en de vrijheid van vereniging, zoals vastgelegd in het Handvest van de grondrechten.

6. De EU en haar lidstaten moeten vermogens voor het opsporen, het analyseren van de bronnen van en het reageren op hybride activiteiten blijven ontwikkelen, opleiden en uitvoeren, en moeten het vergroten van de weerbaarheid van de lidstaten en van de instellingen, organen en instanties van de EU tegen hybride bedreigingen op lange termijn ondersteunen, daarbij ten volle gebruik makend van bestaande instrumenten die daartoe geschikt zijn. De Raad benadrukt dat het operationele protocol van de EU voor de bestrijding van hybride bedreigingen moet worden geactualiseerd op basis van de lering die uit eerdere ervaringen is getrokken.

7. De Raad onderstreept dat het noodzakelijk blijft om samen te werken met internationale organisaties zoals de VN, de OVSE en de Raad van Europa en met structuren als de G7, teneinde de op regels gebaseerde wereldorde te verdedigen, ook in de context van de bestrijding van hybride bedreigingen, onder meer door middel van vertrouwenwekkende en andere relevante maatregelen.

8. De Raad benadrukt dat de EU zich ertoe verbindt de nauwe en wederzijds versterkende samenwerking met en de steun aan alle betrokken partnerlanden, met name de buurlanden van de EU, betreffende de versterking van de weerbaarheid en de bestrijding van hybride bedreigingen, voort te zetten.

9. De Raad roept op tot voortdurende en volgehouden inspanningen om verdere vooruitgang te boeken bij de uitvoering van alle acties in verband met de bestrijding van hybride bedreigingen in het kader van het gemeenschappelijk pakket voorstellen voor de uitvoering van de gezamenlijke verklaringen over de samenwerking tussen de EU en de NAVO, onder meer op het gebied van situationeel bewustzijn, strategische communicatie, crisispreventie en -respons, en de versterking van de weerbaarheid. In dit verband herhaalt de Raad dat de politieke dialoog over de bestrijding van hybride bedreigingen verder moet worden versterkt en dat regelmatige parallelle en gecoördineerde oefeningen (PACE) moeten plaatsvinden, met deelname van alle EU-lidstaten en NAVO-bondgenoten, en dringt hij aan op een tijdige afronding van het nieuwe PACE-plan. De Raad benadrukt dat rekening moet worden gehouden met de getrokken lessen en het belang van ongehinderde uitwisseling van informatie op een inclusieve en niet-discriminerende wijze.

Voorts wijst de Raad op de waardevolle bijdragen van het Europees Kenniscentrum voor de bestrijding van hybride dreigingen in Helsinki en moedigt hij zijn samenwerking met de relevante kenniscentra van de NAVO aan. Hij is tevens ingenomen met de regelmatige en gestructureerde personeelscontacten, met inbegrip van de samenwerking tussen de Fusiecel voor analyse van hybride dreigingen van het Inlichtingen- en situatiecentrum van de EU (EU-Intcen) en de Hybrid Analysis Branch van de NAVO.

10. De Raad erkent de inspanningen van de lidstaten, in samenwerking met de Commissie en de Europese Dienst voor extern optreden (EDEO), bij de uitvoering van de in actie 1 van het gezamenlijk kader voor de bestrijding van hybride bedreigingen (2016) geplande analyse van de hybride risico's en dringt aan op voortzetting van de werkzaamheden en een mogelijke herziening van de analyse van de hybride risico's, teneinde de kwetsbare punten beter aan te pakken.

Op samenhangende wijze werken aan versterking van de weerbaarheid en bestrijding van hybride bedreigingen

11. Bij de ontwikkeling en het gebruik van nieuwe en opkomende technologieën, met inbegrip van technieken voor kunstmatige intelligentie en het verzamelen van gegevens, moet, met het oog op de vermindering van algemene risico's, terdege rekening worden gehouden met nieuwe mogelijkheden om de weerbaarheid te vergroten en met de potentiële zwakke punten en cascade-effecten in de context van de bestrijding van hybride bedreigingen, ook in het proces voor strategische planning van het kaderprogramma voor onderzoek en innovatie.

12. De Raad merkt op dat kwaadwillige cyberactiviteiten deel kunnen uitmaken van hybride bedreigingen en onderstreept in dit verband de relevantie van het EU-instrumentarium voor cyberdiplomatie.

13. Het verband tussen hybride bedreigingen en economische zekerheid is een relevant element dat in aanmerking moet worden genomen en dat in de eerste plaats onder de verantwoordelijkheid van de lidstaten blijft vallen.

14. Nieuwe instrumenten zoals het mechanisme in het kader van de verordening betreffende de screening van buitenlandse directe investeringen in de EU moeten doeltreffend worden ingezet om de weerbaarheid te vergroten en hybride bedreigingen tegen te gaan door middelen te verstrekken om buitenlandse directe investeringen die gevolgen kunnen hebben voor de veiligheid of de openbare orde op te sporen en aan te pakken.

15. De Raad verzoekt de Commissie om weerbaarheid tegen hybride bedreigingen op te nemen in het effectbeoordelingsproces voor relevante toekomstige wetgevingsvoorstellen, waaronder toekomstige kaderprogramma's voor onderzoek en innovatie.

16. De Raad onderstreept het belang van regelmatige oefeningen en op scenario's gebaseerde besprekingen over de bestrijding van hybride bedreigingen op ministerieel niveau en andere niveaus, alsook van het opnemen van hybride elementen in andere relevante EU-opleidings- en oefenactiviteiten op alle niveaus, met de steun van de lidstaten en de relevante organen, met name het Europees Kenniscentrum voor de bestrijding van hybride dreigingen, naargelang het geval.

17. Om de samenhang van de volgende stappen van de EU-samenwerking ter versterking van de weerbaarheid en de bestrijding van hybride bedreigingen te waarborgen, verzoekt de Raad de Commissie en de hoge vertegenwoordiger om, met het oog op mogelijke nieuwe initiatieven, een overzicht op te stellen waarin op alomvattende wijze de tot dusver genomen maatregelen en de in verband daarmee aangenomen documenten zijn opgenomen.

Het verband tussen interne en externe veiligheid

18. Rechtshandhaving, civiele bescherming en andere relevante autoriteiten moeten hun paraatheid ter voorkoming en bestrijding van hybride bedreigingen verder blijven ontwikkelen. De samenwerking tussen de betrokken nationale instanties en de instellingen, organen en agentschappen van de EU op het raakvlak van de interne en de externe veiligheid, conform hun respectieve mandaten, moet voortdurend worden verbeterd en geïntegreerd, terwijl tegelijkertijd de synergieën worden versterkt en dubbel werk wordt vermeden, onder meer door middel van horizontale werkmethoden, vrijwillige informatie-uitwisseling en opleiding en oefeningen die alle sectoren omvatten. Daartoe moeten de ondersteunende rollen en bijdragen van de relevante EU-mechanismen en EU-agentschappen — binnen hun respectieve mandaten en met inachtneming van de bestaande budgettaire beperkingen — verder worden geëvalueerd.

19. Het gebruik van de relevante EU-mechanismen en -instrumenten ter ondersteuning van de reacties van de lidstaten op sectoroverschrijdende en grensoverschrijdende bedreigingen, met inbegrip van de geïntegreerde regeling politieke crisisrespons (IPCR), het Uniemechanisme voor civiele bescherming (UCPM) en het Coördinatiecentrum voor respons in noodsituaties (ERCC), moet door de instellingen en organen van de EU samen met de lidstaten verder worden uitgewerkt.

20. De Raad erkent dat de lidstaten zich kunnen beroepen op de solidariteitsclausule (artikel 222 VWEU) bij het aanpakken van een ernstige crisis ten gevolge van hybride activiteiten.

Situationeel bewustzijn en inlichtingenanalyse

21. De EU-samenwerking bij het versterken van de weerbaarheid en de bestrijding van hybride bedreigingen moet worden gestuurd door een regelmatig bijgewerkte dreigingsanalyse en een breed situationeel bewustzijn. Deze moeten door het EU-Intcen en de Fusiecel voor analyse van hybride dreigingen verder worden uitgewerkt om het vermogen van de EU en haar lidstaten om hybride activiteiten op te sporen, te voorkomen, te verstoren en te bestrijden, te vergroten, met inachtneming van de bevoegdheden van de lidstaten. De Raad is van oordeel dat de werkzaamheden van de EU-Fusiecel voor analyse van hybride dreigingen verder moeten worden geïntensiveerd, rekening houdend met een passend niveau van hulpmiddelen, waaronder professionele deskundigheid.

22. De Raad herinnert aan zijn conclusies over bestrijding van hybride bedreigingen van 19 april 2016, waarin werd opgeroepen EU-instrumenten in te zetten om hybride bedreigingen voor de Unie en haar lidstaten en partners te voorkomen en te bestrijden. De Raad onderstreept dat de bestaande functies voor situationeel bewustzijn van de EU en van de lidstaten verder moeten worden ontwikkeld, rekening houdend met de bronnen van bedreigingen, en dat beter gebruik moet worden gemaakt van de inlichtingenanalyse van het EU-Intcen en de Fusiecel voor analyse van hybride dreigingen, met name in de EU-beleids- en -crisisbeheersingsprocessen betreffende de bestrijding van hybride bedreigingen.

23. De Raad erkent de relevante bijdrage die GVDB-missies en -operaties, waar van toepassing en naargelang het geval, kunnen leveren bij het identificeren en analyseren van indicatoren van mogelijke hybride acties van derden, met inbegrip van desinformatie die bedoeld is om het optreden van de EU en haar lidstaten in diskrediet te brengen en te belemmeren, en erkent de waarde van het verder onderzoeken van de mogelijkheid om deze bijdrage te ontwikkelen.

Bescherming van kritieke infrastructuur

24. De bescherming van nationale en Europese kritieke infrastructuren, alsook van de functies en diensten die cruciaal zijn voor de goede werking van de staat, de economie en de samenleving, is een hoofdprioriteit, ook in de context van het versterken van de weerbaarheid tegen hybride bedreigingen, waarvoor een globale benadering van de overheid en de samenleving nodig is. Bij deze werkzaamheden moet rekening worden gehouden met de sterke onderlinge afhankelijkheid tussen verschillende kritieke functies en diensten, waaronder financiële diensten, de sleutelrol van de particuliere sector, de veranderende veiligheidsomgeving en opkomende risico's, zowel op fysiek als op cybergebied.

25. Voorts moeten, naast EU- en nationale wettelijke, regulerings- en toezichtsvereisten met betrekking tot de operationele weerbaarheid en de bedrijfscontinuïteit, regelingen met eigenaren in de particuliere sector en exploitanten van infrastructuur en diensten worden bevorderd om de continuïteit van en de toegang tot kritieke diensten te waarborgen, ook als er sprake is van overmacht, door te zorgen voor een aanvaardbaar niveau van paraatheid om alle relevante dreigingen het hoofd te bieden, alsook voor flexibiliteit om op weinig waarschijnlijke rampen met ernstige gevolgen te reageren, en deze in te dammen en ervan te herstellen.

26. De Raad benadrukt dat, hoewel de verantwoordelijkheid voor de bescherming van kritieke infrastructuur in de eerste plaats onder de bevoegdheid van de lidstaten valt, de hoge mate van grensoverschrijdende en sectoroverschrijdende onderlinge afhankelijkheid gecoördineerde of, waar nodig, geharmoniseerde inspanningen op EU-niveau vereist, ook met het oog op de ononderbroken werking van de interne markt.

27. Naar aanleiding van de evaluatie van juli 2019 betreffende de tenuitvoerlegging van Richtlijn 2008/114/EG inzake de identificatie van Europese kritieke infrastructuren en de aanmerking van infrastructuren als Europese kritieke infrastructuren (ECI), verzoekt de Raad de Commissie om met de lidstaten te overleggen over een mogelijk voorstel voor een herziening van de richtlijn in een vroeg stadium van de nieuwe wetgevingscyclus, met inbegrip van mogelijke aanvullende maatregelen om de bescherming en de weerbaarheid van kritieke infrastructuur in de EU te verbeteren, rekening houdend met de sterke onderlinge afhankelijkheid tussen kritieke functies en diensten.

28. De Raad verzoekt de Commissie om met de lidstaten te blijven samenwerken en, in voorkomend geval, niet-bindende samenwerkingsregelingen te ontwikkelen tussen de lidstaten die onderling verbonden kritische infrastructuren delen.

29. De Raad erkent het belang van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn) voor de ontwikkeling van een risicobeheers- en beveiligingscultuur door de exploitanten in kritieke sectoren, alsmede voor de nationale vermogens en strategieën die een hoog niveau van beveiliging van netwerk- en informatiesystemen op hun grondgebied waarborgen, ook in de context van hybride bedreigingen. De Raad verzoekt de lidstaten, de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) hun samenwerking te blijven ontwikkelen op basis van de aanbeveling van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (blauwdruk) op alle relevante niveaus.

Bestrijding van desinformatie en zorgen voor vrije en eerlijke verkiezingen

30. De Raad is ingenomen met het verslag over de uitvoering van het actieplan tegen desinformatie en erkent dat de voortzetting van de uitvoering van het actieplan de kern blijft van de inspanningen van de EU. De Raad onderstreept dat het actieplan regelmatig moet worden geëvalueerd en, indien nodig, moet worden geactualiseerd om te zorgen voor een doeltreffende langetermijnaanpak.

31. De Raad benadrukt dat de werkzaamheden van de afdeling strategische communicatie van de EDEO, en met name van de drie taskforces (Oost, Westelijke Balkan, Zuid), moeten worden ondersteund met voldoende middelen om langetermijnplanning, uitvoering en evaluatie mogelijk te maken. In het kader van hun taken moeten alle drie de taskforces in staat zijn om de desinformatie-activiteiten van buitenlandse overheidsactoren en externe niet-overheidsactoren voortdurend op te sporen, te analyseren en te bestrijden. De taskforces moeten ook blijven bijdragen tot doeltreffende en op feiten gebaseerde positieve communicatie en de bevordering van de beginselen, waarden en beleidsmaatregelen van de Unie in de oostelijke en zuidelijke buurlanden van de EU en de Westelijke Balkan, en tot de versterking van het algemene medialandschap en het maatschappelijk middenveld in hun desbetreffende regio's. De Raad verzoekt de EDEO de behoeften en de mogelijkheden te beoordelen voor het versterken van zijn strategische communicatieactiviteiten in andere geografische gebieden, zoals Afrika ten zuiden van de Sahara, met gelijktijdig behoud van de nodige capaciteit voor de uitvoering van de bestaande strategische communicatietaken.

32. De Raad erkent dat een alomvattende aanpak op alle niveaus nodig is voor het aanpakken van de problemen van desinformatie, waaronder inmenging ter ondermijning van vrije en eerlijke Europese verkiezingen, waarbij optimaal gebruik wordt gemaakt van alle beschikbare instrumenten online en offline. Dit moet monitoring en analyse van desinformatie en manipulatieve inmenging, handhaving van de Europese regels inzake gegevensbescherming, toepassing van de waarborgen voor verkiezingen, inspanningen ter bevordering van pluralistische media, professionele journalistiek en mediageletterdheid en bewustmaking van de burgers omvatten. De Raad beveelt de consolidatie aan van een actief onafhankelijk Europees netwerk van factcheckers en -onderzoekers tegen desinformatie. De Raad erkent het belang en de rol van het maatschappelijk middenveld, de academische wereld en de particuliere sector bij het aanpakken van desinformatie en het opbouwen van weerbaarheid.

33. De Raad erkent het potentieel van het systeem voor snelle waarschuwingen (RAS) voor de bestrijding van desinformatie, met name wat betreft inmenging in verkiezingen. Hij dringt er bij de Commissie en de EDEO op aan om, samen met de lidstaten, het systeem voor snelle waarschuwingen verder te ontwikkelen tot een breed platform voor de lidstaten en de EU-instellingen ter verbetering van de samenwerking, de coördinatie en de uitwisseling van informatie, zoals onderzoeks- en analytische inzichten, beste praktijken en communicatieproducten, om de aanpak van desinformatiecampagnes in het kader van een reeks Europese en nationale inspanningen te ondersteunen.

34. De Raad erkent het nut van de maatregelen en aanbevelingen die de Commissie op 12 september 2018 in haar verkiezingspakket voor het waarborgen van de Europese verkiezingen heeft gepresenteerd. De Raad moedigt de Commissie en de lidstaten aan de mogelijkheden te onderzoeken om de activiteiten van de Europese samenwerkingsnetwerken voor verkiezingen voort te zetten ter ondersteuning van de uitwisseling van informatie en beste praktijken. De Raad is ingenomen met de inspanningen van de Commissie om met alle relevante belanghebbenden samen te werken en een breed scala aan maatregelen te ondersteunen, zoals de oefening over de cyberbeveiliging van de Europese verkiezingen (EU ELEx19), rekening houdend met de nationale bevoegdheden op dit gebied.

35. De Raad is er zich van bewust dat de samenwerking met socialemediaplatforms moet worden voortgezet om te komen tot hogere normen inzake verantwoordelijkheid, transparantie en verantwoordingsplicht bij het aanpakken van desinformatie. Daarnaast moet ten behoeve van academisch onderzoek ongehinderde toegang tot geanonimiseerde gegevens van aanbieders op socialemediaplatforms worden verleend om empirisch onderbouwd beleid te vergemakkelijken. De Raad verzoekt de Commissie om initiatieven te presenteren betreffende de verdere aanpak van desinformatie op onlineplatforms. Deze initiatieven moeten gebaseerd zijn op een evaluatie van de uitvoering van de praktijkcode betreffende desinformatie, waarbij rekening moet worden gehouden met de analytische werkzaamheden en verslagen van de academische wereld en organisaties van het maatschappelijk middenveld, het monitoringverslag over de code door de Europese groep van regelgevende instanties voor audiovisuele mediadiensten, en de lessen die zijn getrokken uit de verkiezingen voor het Europees Parlement in mei 2019. In dit verband verzoekt de Raad de Commissie zich te beraden op manieren, met inbegrip van mogelijke handhavingsmechanismen voor onlineplatforms, om de uitvoering van de praktijkcode verder te verbeteren, met name door een onafhankelijke evaluatie van de uitvoering door de ondertekenaars van hun verbintenissen op te nemen.

Veiligheid van de instellingen, organen en agentschappen van de EU

36. De veiligheid van het personeel en de instellingen, organen en agentschappen van de EU tegen hybride bedreigingen en andere kwaadwillige activiteiten is een belang dat de EU en haar lidstaten delen. De Raad roept de instellingen, organen en agentschappen van de EU, ondersteund door de lidstaten, op te zorgen voor het vermogen van de Unie om haar integriteit te beschermen en de beveiliging te verbeteren van de EU-informatie- en communicatienetwerken en -besluitvormingsprocessen tegen alle soorten kwaadwillige activiteiten, op basis van een uitgebreide dreigingsanalyse. Daartoe moeten instellingen, organen en agentschappen, ondersteund door de lidstaten, een uitgebreide reeks maatregelen uitwerken en toepassen om hun veiligheid te waarborgen, overeenkomstig het mandaat van de Europese Raad van juni 2019. De Raad onderstreept het belang van het waarborgen van de interoperabiliteit van de IT-infrastructuur van de EU voor de uitwisseling van gerubriceerde gegevens tussen EU-instellingen, -organen, -agentschappen en de lidstaten.