Raad van de
Europese Unie

Brussel, 23 mei 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	23 mei 2022
aan:	de delegaties
Betreft:	Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie - Conclusies van de Raad die de Raad tijdens zijn zitting van 23 mei 2022 heeft goedgekeurd

Voor de delegaties gaan hierbij de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie, die de Raad tijdens zijn zitting van 23 mei 2022 heeft goedgekeurd.

BIJLAGE

Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie

DE RAAD VAN DE EUROPESE UNIE,

HERINNEREND aan zijn conclusies over:

– de gezamenlijke mededeling van 25 juni 2013 aan het Europees Parlement en de Raad over de Strategie inzake cyberbeveiliging van de Europese Unie: "Een open, veilige en beveiligde cyberspace"[1],

– het EU-beleidskader voor cyberdefensie[2],

– internetgovernance[3],

– cyberdiplomatie[4],

– het versterken van het Europese cyberbeveiligingssysteem en het bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche[5],

– de gezamenlijke mededeling van 20 november 2017 aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU"[6],

– een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("Instrumentarium voor cyberdiplomatie")[7],

– de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[8],

– richtsnoeren voor het opbouwen van externe cybercapaciteit van de EU[9],

---

1 Doc. 12109/13.
2 Doc. 15585/14.
3 Doc. 16200/14.
4 Doc. 6122/15 + COR 1.
5 Doc. 14540/16.
6 Doc. 14435/17 + COR 1.
7 Doc. 10474/17.
8 Doc. 10086/18.
9 Doc. 10496/18.

– Uitvoeringsbesluit (EU) 2018/1993 van de Raad van 11 december 2018 inzake de geïntegreerde EU- regeling politieke crisisrespons[10],

– het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU[11],

– het belang van 5G voor de Europese economie en de noodzaak om de veiligheidsrisico's in verband met 5G te beperken[12],

– de toekomst van een sterk gedigitaliseerd Europa na 2020: "Versterking van het digitale en economische concurrentievermogen in de hele Unie en van de digitale cohesie"[13],

– extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen[14],

– de digitale toekomst van Europa vormgeven[15],

– de cyberbeveiliging van verbonden apparaten[16],

– de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[17],

– veiligheid en defensie[18],

– het potentieel verkennen van het initiatief voor een gezamenlijke cybereenheid ter aanvulling op de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[19],

– een strategisch kompas voor veiligheid en defensie - Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid[20],

---

10 PB L 320 van 17.12.2018, blz. 28.
11 Doc. 7737/19.
12 Doc. 14517/19.
13 Doc. 9596/19.
14 Doc. 14972/19.
15 Doc. 8711/20.
16 Doc. 13629/20.
17 Doc. 7290/21.
18 Doc. 8396/21.
19 Doc. 13048/21.
20 Doc. 7371/22.

1. BENADRUKT dat kwaadwillig gedrag in de cyberspace van zowel staten als andere actoren de afgelopen jaren is toegenomen, onder meer door een grote en voortdurende toename van kwaadwillige activiteiten tegen de kritieke infrastructuur, toeleveringsketens en intellectuele eigendom van de EU en haar lidstaten, het toegenomen risico van overloopeffecten, alsook door een toename van ransomwareaanvallen op onze bedrijven, organisaties en burgers. MERKT OP dat sommige landen met de terugkeer van de machtspolitiek steeds meer proberen de op regels gebaseerde internationale orde in de cyberspace op de proef te stellen en te ondermijnen door van de cyberspace, net als van de volle zee, de lucht en de ruimte, steeds vaker een betwist domein te maken. ERKENT dat grootschalige cyberaanvallen of pogingen om netwerk- en informatiesystemen binnen te dringen, te verstoren of te vernietigen met systemische gevolgen steeds vaker voorkomen, onze economische veiligheid kunnen ondermijnen en onze democratische instellingen en processen kunnen aantasten, en aantonen dat sommige actoren bereid zijn de internationale veiligheid en stabiliteit in gevaar te brengen. ONDERSTREEPT dat de militaire agressie van Rusland tegen Oekraïne heeft aangetoond dat offensieve cyberactiviteiten integraal deel kunnen uitmaken van hybride strategieën die een combinatie zijn van intimidatie, destabilisatie en economische ontwrichting.

2. HERHAALT dat de kracht van onze Unie in het licht van de huidige geopolitieke verschuivingen ligt in eenheid, solidariteit en vastberadenheid, en dat de uitvoering van het strategisch kompas de strategische autonomie van de EU en haar vermogen om met partners samen te werken om haar waarden en belangen te beschermen, onder meer op cybergebied, zal versterken. BENADRUKT dat een sterkere en slagvaardigere EU op het gebied van veiligheid en defensie een positieve bijdrage zal leveren aan de mondiale en trans-Atlantische veiligheid en complementair is aan de NAVO, die het fundament blijft van de collectieve defensie van haar leden. BEVESTIGT andermaal dat de EU voornemens is de op regels gebaseerde internationale orde, waarvan de kern gevormd wordt door de Verenigde Naties, intensiever te ondersteunen.

3. HERHAALT, conform de Raadsconclusies over de EU-cyberbeveiligingsstrategie en het strategisch kompas, de noodzaak om de cyberafweer van de Unie te ontwikkelen door ons vermogen om cyberaanvallen te voorkomen te vergroten door middel van capaciteitsopbouw, vermogensontwikkeling, opleiding, oefeningen, grotere weerbaarheid en een krachtige reactie op cyberaanvallen tegen de EU en haar lidstaten met gebruikmaking van alle beschikbare EU-instrumenten. Dit houdt onder meer in dat de EU verder moet aantonen dat zij vastbesloten is om onmiddellijk en op lange termijn te reageren op dreigingsactoren die onze veilige en open toegang tot cyberspace willen ontzeggen en onze strategische belangen, waaronder de veiligheid van onze partners, willen aantasten. BENADRUKT in dat verband dat met de cyberstrategie wordt beoogd de verschillende initiatieven te bundelen van de EU-acties ten behoeve van vrede en stabiliteit in de cyberspace en van een open, vrije, wereldwijde, stabiele en veilige cyberspace, en tegelijkertijd de acties op korte, middellange en lange termijn ter voorkoming, ontmoediging, afschrikking en bestrijding van cyberdreigingen en -aanvallen en ter benutting van cybercapaciteiten beter te coördineren. BENADRUKT dat deze elementen moeten worden opgenomen in de cyberstrategie van de EU, volgens de vijf functies van de EU op cybergebied: onze cyberweerbaarheid en beschermingscapaciteiten versterken; solidair en alomvattend crisisbeheer versterken; onze visie op de cyberspace bevorderen; de samenwerking met partnerlanden en internationale organisaties verbeteren; voorkomen van, zich wapenen tegen en reageren op cyberaanvallen.

I. ONZE CYBERWEERBAARHEID EN BESCHERMINGSCAPACITEITEN VERSTERKEN

4. HERHAALT dat het algemene niveau van cyberbeveiliging in de EU moet worden verhoogd, ZIET UIT naar de snelle vaststelling van de ontwerprichtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (NIS), de ontwerpverordening betreffende digitale operationele veerkracht voor de financiële sector (DORA) en de ontwerprichtlijn betreffende de veerkracht van kritieke entiteiten (CER), en NEEMT NOTA van het voorstel voor een verordening tot vaststelling van maatregelen voor een hoog niveau van cyberbeveiliging bij de instellingen, organen en instanties van de Unie, teneinde een Europese Unie te bevorderen die haar burgers, openbare diensten en bedrijven in cyberspace beschermt. MOEDIGT de Commissie AAN de goedkeuring van belangrijke voorstellen ter beveiliging van digitale infrastructuur, technologieën, producten en diensten af te ronden om een duidelijk signaal te geven over de ambities van de EU op dit gebied en bedrijven in dat verband te kunnen ondersteunen. VERZOEKT de Commissie gemeenschappelijke EU-cyberbeveiligingsvereisten voor verbonden apparaten en bijbehorende processen en diensten voor te stellen via de cyberweerbaarheidswet, die de Commissie vóór eind 2022 moet voorstellen, rekening houdend met de noodzaak van een horizontale en holistische aanpak die de hele levenscyclus van digitale producten bestrijkt, alsook met bestaande regelgeving, met name op het gebied van cyberbeveiliging.

5. VERZOEKT de betrokken autoriteiten, zoals het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en de samenwerkingsgroep voor netwerk- en informatiebeveiliging (NIB), samen met de Europese Commissie, op basis van een risicobeoordeling aanbevelingen te doen aan de lidstaten en de Europese Commissie om de weerbaarheid van communicatie-netwerken en -infrastructuren binnen de Europese Unie te versterken, met inbegrip van de verdere uitvoering van de EU-toolbox voor 5G.

6. ROEPT de EU en haar lidstaten OP meer inspanningen te leveren om het algemene cyberbeveiligingsniveau te verhogen, bijvoorbeeld door de opkomst van betrouwbare aanbieders van cyberbeveiligingsdiensten te vergemakkelijken, en BENADRUKT dat het aanmoedigen van de ontwikkeling van dergelijke aanbieders een prioriteit moet zijn voor het industriebeleid van de EU op het gebied van cyberbeveiliging. VERZOEKT de Commissie om, teneinde cyberaanvallen met potentiële systemische effecten beter te weerstaan en te bestrijden en lessen te trekken uit de aanpak van de kwetsbaarheden van Solarwinds, Microsoft Exchange en Apache Log4J, opties voor te stellen om de ontwikkeling van betrouwbare cyberbeveiligingsdiensten aan te moedigen, de cyberbeveiliging van de ICT-toeleveringsketen te versterken, de potentiële gevolgen van zwakke plekken van software voor de EU en haar lidstaten aan te pakken, onder meer met het oog op de komende wet inzake cyberweerbaarheid, en de capaciteiten voor het opsporen en delen van cyberdreigingen in en tussen de lidstaten te verbeteren.

7. HERHAALT dat investeren in innovatie en beter gebruik van civiele technologie van cruciaal belang is om onze technologische soevereiniteit te versterken, ook op cybergebied, ROEPT de Commissie OP het Europees Kenniscentrum voor cyberbeveiliging snel operationeel te maken om een sterk Europees cyberonderzoeks-, industrieel en technologisch ecosysteem te ontwikkelen, en ONDERSTREEPT dat onderzoek en innovatie moeten worden gestimuleerd, meer moet worden geïnvesteerd op civiel en defensiegebied om de technologische en industriële defensiebasis van de EU (EDTIB) te versterken, en de cybercapaciteiten van de EU en haar lidstaten, met inbegrip van strategische ondersteuningscapaciteiten, moeten worden ontwikkeld. BENADRUKT het belang van het intensief gebruiken van nieuwe technologieën, met name kwantumcomputing, artificiële intelligentie en big data, om comparatieve voordelen te behalen, ook wat betreft cyberresponsoperaties en informatiesuperioriteit.

8. ERKENNENDE dat het verbeteren van onze cyberbeveiliging een manier is om onze inspanningen op het land, in de lucht, op zee en in de ruimte doeltreffender en veiliger te maken, BENADRUKT het belang van het integreren van cyberbeveiligingsoverwegingen in alle beleidsmaatregelen van de EU, met inbegrip van sectorale wetgeving ter aanvulling van de NIS 2-richtlijn, en VERZOEKT de Commissie mogelijkheden te verkennen om de cyberbeveiliging in de hele toeleveringsketen van de technologische en industriële defensiebasis van de EU (EDTIB) te verbeteren.

9. ERKENT dat het waarborgen van toereikende financiële en personele middelen voor cyberbeveiliging en maatregelen die gericht zijn op het creëren van een gunstig klimaat voor het concurrentievermogen van de particuliere sector van essentieel belang zijn om de cyberstrategie van de EU te ontwikkelen en dat de EU moet zorgen voor stabiele en langetermijnfinanciering van cyberbeveiliging, met inbegrip van de kosten van hoog-gekwalificeerd personeel, aan de hand van een horizontaal mechanisme met meerdere financieringsbronnen. VERZOEKT de Commissie derhalve vóór eind 2022 de opties na te gaan voor een dergelijk mechanisme, dat in de bevoegde Raadsinstanties zal worden besproken.

10. BENADRUKT dat we onze inspanningen moeten opvoeren en meer moeten samenwerken in de strijd tegen internationale cybercriminaliteit, met name ransomware, door middel van het Empact (Europees multidisciplinair platform tegen criminaliteitsdreiging), door middel van uitwisselingen tussen de cyberbeveiligings-, de rechtshandhavings- en de diplomatieke sector, en door een versterking van de rechtshandhavingscapaciteit bij het onderzoeken en vervolgen van cybercriminaliteit. HERHAALT zijn toezegging om het publiek te informeren over cyberdreigingen en over de maatregelen die daartoe op nationaal en EU-niveau worden genomen, door het maatschappelijk middenveld, de particuliere sector en de academische wereld hierbij te betrekken, om het bewustzijn te vergroten en een geschikt niveau van cyberbescherming en cyberhygiëne aan te moedigen. BENADRUKT dat de aandacht moet uitgaan naar de vaardigheden en capaciteiten van de burgers van de EU en van de lidstaten op het gebied van cyberbeveiliging en dat gebruikers actief moeten worden betrokken bij hun eigen bescherming.

II. **SOLIDAIR EN ALOMVATTEND CRISISBEHEER VERSTERKEN**

11. BENADRUKT, op basis van de jaarlijkse cyberoefeningen, andere oefeningen met een cyberdimensie en de CyCLES 2022-oefening van de EU, dat het van belang is een programma van regelmatige intracommunautaire cyberoefeningen op verschillende niveaus op te zetten, teneinde de interne en externe respons van de EU op grootschalige cyberincidenten te testen en te ontwikkelen, met medewerking van de Raad, de EDEO, de Commissie en belanghebbenden zoals Enisa en de particuliere sector, en dat dit programma zal worden afgestemd op en zal bijdragen tot het algemene oefeningenbeleid van de EU. BENADRUKT het belang van de verdere ontwikkeling van de Cyber Europe- en BlueOLEx-oefeningen, waarbij de respons op verschillende niveaus wordt gecombineerd. ERKENT dat de bestaande oefeningen moeten worden geëvalueerd en geconsolideerd en dat de mogelijkheid van verdere oefeningen op specifieke onderdelen van het cyberdomein moet worden onderzocht, met name een militaire CERT-oefening en een oefening die gericht is op crisissamenwerking tussen de instellingen, organen en agentschappen van de EU. ONDERKENT dat de cyberstrategie van de Unie ons vermogen om cyberaanvallen te voorkomen, zal versterken door middel van diverse acties, waaronder opleiding, en VERZOEKT de lidstaten derhalve de civiel-militaire samenwerking op het gebied van cyberopleiding en gezamenlijke oefeningen te versterken.

12. BENADRUKT dat de operationele samenwerking en het gedeeld omgevingsbewustzijn tussen de lidstaten verder moeten worden getest en versterkt, onder meer via bestaande netwerken zoals het CSIRT-netwerk en het netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), teneinde de paraatheid van de EU voor grootschalige cyberincidenten te vergroten. ONDERSTREEPT het belang van de ontwikkeling van een gemeenschappelijke taal onder de lidstaten en met de instellingen, organen en agentschappen van de EU voor besprekingen op politiek niveau, ter ondersteuning van een geconsolideerde beoordeling van de ernst en de gevolgen van relevante cyberincidenten, alsook van mogelijke evolutiescenario's en de daaruit voortvloeiende behoeften. BENADRUKT in dat verband dat de complementariteit van de gedeelde situatiebeoordelingsverslagen moet worden verbeterd, met inbegrip van de EU-CyCLONe-verslagen over de impact en ernst van grootschalige cyberincidenten in de EU-lidstaten en de dreigingsevaluaties van het EU-Intcen in het kader van het EU-instrumentarium voor cyberdiplomatie. VERZOEKT de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep, in coördinatie met de betrokken civiele en militaire organen en agentschappen en de bestaande netwerken, waaronder het EU-CyCLONe, uiterlijk eind 2022 een risicobeoordeling uit te voeren en risicoscenario's op te stellen voor cyberbeveiliging in een situatie van dreiging of een mogelijke aanval tegen lidstaten of partnerlanden, en deze aan de bevoegde Raadsinstanties voor te leggen. BENADRUKT de noodzaak van geschikte en gecoördineerde publieke communicatie over de reactie van de EU op grootschalige cyberincidenten.

13. BENADRUKT dat, in geval van een grootschalig cyberincident, de coördinatie moet worden versterkt en, in voorkomend geval, moet worden voortgebouwd op de vorderingen en werkzaamheden van de snellereactieteams bij cyberincidenten van de PESCO, en op het werk van het CSIRT-netwerk en EU-CyCLONe, de vrijwillige bundeling tussen de lidstaten van onze responscapaciteit bij incidenten. ERKENT dat samenwerking met de particuliere sector de publieke capaciteit zou kunnen versterken, in het bijzonder gelet op het tekort aan vaardigheden in de EU, en dat het identificeren en coördineren van deze particuliere partners een verschil zou kunnen maken bij grootschalige incidenten. VERZOEKT de Commissie, om volledig voorbereid te zijn op grootschalige cyberincidenten, tegen het einde van het derde kwartaal 2022 een voorstel over een nieuw cyberbeveiligingsnoodfonds in te dienen.

14. HERHAALT, in overeenstemming met het strategisch kompas, de noodzaak om te blijven investeren in onze wederzijdse bijstand op grond van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie, en in solidariteit op grond van artikel 222 van het Verdrag betreffende de werking van de Europese Unie, met name door frequente oefeningen. BENADRUKT in dit verband dat de bilaterale civiele en/of militaire steun verder moet worden verstrekt en gecoördineerd, onder meer door na te gaan of de EU op uitdrukkelijk verzoek van de lidstaten steun kan verlenen, en dat geschikte responsmaatregelen, waaronder een communicatiestrategie, moeten worden vastgesteld in het kader van de uitvoering van artikel 42, lid 7. NEEMT ER NOTA VAN dat dit ook een betere coördinatie met bestaande EU-mechanismen voor crisisbeheersing en het Uniemechanisme voor civiele bescherming moet inhouden.

15. ONDERSTREEPT dat een versterkte cyberstrategie van de EU een sterker beveiligde communicatie vereist. HERHAALT daartoe de richting die hieraan in het strategisch kompas is gegeven en VERZOEKT de Commissie en andere betrokken instellingen, organen en agentschappen om uiterlijk eind 2022 de bestaande instrumenten voor beveiligde communicatie op cybergebied in kaart te brengen, zodat deze in de betrokken Raadsorganen en met de betrokken samenwerkingsgroepen, zoals het CSIRT-netwerk en EU CyCLONe, kunnen worden besproken.

III. ONZE VISIE OP DE CYBERSPACE BEVORDEREN

16. HERINNERT eraan dat de gemeenschappelijke totaalaanpak van de EU voor cyberdiplomatie gericht is op conflictpreventie, het beperken van cyberbeveiligingsdreigingen en een grotere stabiliteit in de internationale betrekkingen. BEVESTIGT in dit verband de toezegging van de EU om internationale geschillen in de cyberspace met vreedzame middelen te beslechten en het internationaal recht, met inbegrip van het internationaal recht inzake de mensenrechten en het internationaal humanitair recht, toe te passen op acties van staten in de cyberspace. ONDERSTREEPT de toezegging van de EU en haar lidstaten om te handelen in overeenstemming met de vrijwillige, door alle VN-lidstaten overeengekomen niet-bindende normen voor verantwoordelijk gedrag van staten in de cyberspace. BENADRUKT dat een open, vrije, mondiale, stabiele en veilige cyberspace waar mensenrechten, fundamentele vrijheden en de rechtsstaat onverkort gelden, belangrijk is voor het sociale welzijn, de economische groei, de welvaart en de integriteit van onze vrije en democratische samenlevingen, en BEVESTIGT dat de EU en haar lidstaten hebben toegezegd deze waarden en beginselen te blijven bevorderen. BENADRUKT dat het voor de ontwikkeling van kanalen voor constructieve, eerlijke en open dialogen met belangrijke belanghebbenden in de cyberspace belangrijk is om cyberaangelegenheden, met inbegrip van het EU-instrumentarium voor cyberdiplomatie, integraal op te nemen in de toetredings-onderhandelingen van de Unie en de strategische en politieke dialogen van de EU met internationale partners en concurrenten, en VERZOEKT tegelijkertijd de hoge vertegenwoordiger de bestaande bilaterale cyberdialogen te evalueren en, indien nodig, voor te stellen een soortgelijke samenwerking met andere landen of betrokken internationale organisaties op te zetten.

17. HERINNERT eraan dat samenwerking met meerdere belanghebbenden belangrijk is, aangezien ook andere belanghebbenden verantwoordelijk zijn voor cyberbeveiliging en de betreffende aanbevelingen en besluiten die in internationale en regionale fora worden aangenomen, moeten uitvoeren. VERZOEKT de EU en haar lidstaten onze cyberspace- en internetmodellen te bevorderen via hun betrekkingen met meerdere belanghebbenden en door middel van initiatieven zoals de Oproep van Parijs voor vertrouwen en veiligheid in de cyberspace en de Verklaring over de toekomst van het internet, en daarbij de gedeelde voordelen van een stabiele cyberspace te benadrukken en wereldwijd meer bekendheid te geven aan de gevaren van een staatsgebonden, autoritaire visie op het internet, en VERZOEKT de EU en haar lidstaten de samenwerking met de gemeenschap van belanghebbenden te versterken, onder meer door gebruik te maken van relevante projecten zoals het EU-cyberdiplomatie-initiatief van het EU-instrument van het buitenlands beleid.

18. ZEGT TOE betrokken te blijven bij relevante internationale organisaties, met name in de processen van de Eerste en de Derde Commissie van de VN, en BENADRUKT dat het bestaande internationale recht zonder voorbehoud van toepassing is in, en met betrekking tot, de cyberspace. BENADRUKT het belang van voortgezette inspanningen om het VN-kader voor verantwoordelijk gedrag van staten te handhaven en te bevorderen, en ONDERSTREEPT dat de EU en haar lidstaten actief zullen werken aan een betere uitvoering ervan, onder meer door de vaststelling van het actieprogramma ter bevordering van verantwoordelijk gedrag van staten in de cyberspace. BENADRUKT dat de EU en haar lidstaten actief zullen deelnemen aan de onderhandelingen over een toekomstig VN-verdrag dat moet dienen als een doeltreffend instrument voor rechtshandhavings- en gerechtelijke autoriteiten in de wereldwijde strijd tegen cybercriminaliteit, waarbij zij ten volle rekening zullen houden met het bestaande kader van internationale en regionale instrumenten op dit gebied, met name het Verdrag van Boedapest inzake cybercriminaliteit. BENADRUKT dat het belangrijk is de ontwikkeling en operationalisering van vertrouwenwekkende maatregelen op regionaal en internationaal niveau verder te ondersteunen en het gebruik van bestaande vertrouwenwekkende cybermaatregelen in de OVSE, ook in tijden van internationale spanningen, verder aan te moedigen.

19. HERINNERT eraan dat een proactieve, op mensenrechten gebaseerde aanpak voor het waarborgen van internationale normen op het gebied van opkomende technologieën en de kernarchitectuur van het internet in overeenstemming met democratische waarden en beginselen van essentieel belang is om een wereldwijd, niet-gefragmenteerd en open internet te blijven waarborgen, en STEUNT het beginsel dat technologieën worden gebruikt en ontwikkeld met eerbiediging van de mensenrechten en de persoonlijke levenssfeer en dat zij op een rechtmatige, veilige en ethische manier worden aangewend. MOEDIGT de hoge vertegenwoordiger en de Commissie AAN een strategische visie te ontwikkelen betreffende digitale technische aangelegenheden die gevolgen hebben voor het buitenlands beleid en kunnen hebben voor de stabiliteit van de cyberspace en het internet in het bijzonder, onder meer in de betrokken gespecialiseerde internationale organisaties zoals de Internationale Unie voor Telecommunicatie.

IV. DE SAMENWERKING MET PARTNERLANDEN EN INTERNATIONALE ORGANISATIES VERBETEREN

20. BENADRUKT dat de EU-strategie voor cybercapaciteitsopbouw beter moet worden afgestemd op de VN-normen voor verantwoordelijk gedrag van staten in de cyberspace, onder meer door op maat gesneden samenwerkings- en capaciteitsopbouwprogramma's te ontwikkelen om derde landen te helpen bij de uitvoering, en door ons daarbij te blijven inspannen en zelfs meer in te spannen voor een bredere uitvoering van het VN-actie-programma ter bevordering van verantwoordelijk gedrag van staten in de cyberspace. BENADRUKT dat het belangrijk is de cybercapaciteitsopbouw volledig te integreren in het veiligheidsaanbod van de EU, met passende coördinatie van de inspanningen tussen de lidstaten en de instellingen, organen en agentschappen van de EU, en IS met name INGENOMEN met de samenwerking tussen de lidstaten en met publieke en private partners, met name via EU-CyberNet (het netwerk voor de opbouw van cybercapaciteit van de EU) en het Wereldwijde Forum inzake cyberexpertise, om de inspanningen te coördineren en dubbel werk te voorkomen.

VERZOEKT de hoge vertegenwoordiger en de Commissie om uiterlijk in het derde kwartaal van 2022 een raad voor de opbouw van cybercapaciteit op te richten en regelmatig van gedachten te wisselen in de Horizontale Groep cybervraagstukken. VERZOEKT de Commissie en de hoge vertegenwoordiger verder gebruik te maken van het instrument voor nabuurschapsbeleid, ontwikkeling en internationale samenwerking, het instrument voor

pretoetredingssteun (IPA III) en andere financiële instrumenten, zoals de Europese Vredesfaciliteit en het Global Gateway-initiatief, om de veerkracht van onze partners en hun capaciteit om cyberdreigingen in kaart te brengen en aan te pakken en om cybermisdrijven te onderzoeken en te vervolgen, te helpen versterken en om de ontwikkeling van samenwerkingsprojecten, ook in de context van crises, te ondersteunen, en MOEDIGT met name de samenwerking met partners in de Westelijke Balkan en met de landen van het oostelijk en zuidelijk nabuurschap van de EU AAN, alsook de inzet van deskundigen van de EU en de lidstaten om, met inachtneming van de bestaande wettelijke mandaten, steun te bieden in cybercrises.

21. BENADRUKT dat er meer inspanningen moeten worden geleverd om een gestructureerde en open EU-outreachbenadering te ontwikkelen voor een beter wereldwijd gemeenschappelijk begrip van de toepassing van het internationaal recht in de cyberspace, het VN-kader voor verantwoordelijk gedrag van staten in de cyberspace, met inbegrip van het initiatief voor een actieprogramma ter bevordering van verantwoordelijk gedrag van staten in de cyberspace, en betreffende het standpunt van de EU en haar lidstaten in de lopende onderhandelingen over een VN-verdrag inzake cybercriminaliteit, en VERZOEKT de hoge vertegenwoordiger om in het kader van deze inspanningen uiterlijk eind 2022 een outreachplan aan de Raad voor te leggen. MOEDIGT de hoge vertegenwoordiger en de diensten van de Commissie AAN ten volle en systematisch gebruik te maken van hun 145 delegaties en, onder de auspiciën van het op te richten EU-cyberdiplomatienetwerk, een regelmatige, vruchtbare samenwerking tussen deze delegaties en de ambassades van de lidstaten in derde landen tot stand te brengen. ROEPT de hoge vertegenwoordiger OP om uiterlijk in het derde kwartaal van 2022 het EU-cyberdiplomatienetwerk op te richten, dat zal bijdragen aan de uitwisseling van informatie, gezamenlijke opleidingsactiviteiten voor personeel van de EU en de lidstaten, coherente capaciteitsopbouwinspanningen en een betere uitvoering van het VN-kader voor verantwoordelijk gedrag van staten en van vertrouwenwekkende maatregelen tussen staten.

22. BENADRUKT zijn engagement om verder samen te werken met internationale organisaties en partnerlanden om het gemeenschappelijk inzicht in het cyberdreigingslandschap te bevorderen, samenwerkingsmechanismen te ontwikkelen en proactief gezamenlijke diplomatieke reacties in kaart te brengen. HERINNERT aan de belangrijkste verwezenlijkingen van de samenwerking tussen de EU en de NAVO op het gebied van cyberbeveiliging in het kader van de uitvoering van de gezamenlijke verklaringen van Warschau (2016) en Brussel (2018), en BENADRUKT, met volledige inachtneming van de beslissingsautonomie en -procedures van beide organisaties en op basis van de beginselen van transparantie, wederkerigheid en inclusiviteit, dat de samenwerking met de NAVO op cybergebied moet worden versterkt door middel van oefeningen, informatiedeling en uitwisselingen tussen deskundigen, onder meer inzake capaciteitsontwikkeling, capaciteitsopbouw voor partners, en missies en operaties, alsook inzake de toepasselijkheid van het internationaal recht en de VN-normen inzake verantwoordelijk gedrag van staten in de cyberspace, en mogelijke gecoördineerde reacties op kwaadwillige cyberactiviteiten.

V. VOORKOMEN VAN, ZICH WAPENEN TEGEN EN REAGEREN OP CYBERAANVALLEN

23. ERKENT dat de cyberspace een arena voor geopolitieke concurrentie is geworden en HERHAALT daarom dat de EU snel en krachtig moet kunnen reageren op cyberaanvallen, zoals door de staat gesteunde kwaadwillige cyberactiviteiten die gericht zijn op de EU en haar lidstaten, en dat zij daarom het EU-instrumentarium voor cyberdiplomatie moet versterken en volledig gebruik moet maken van alle instrumenten daarin, waaronder de beschikbare politieke, economische, diplomatieke, wettelijke en strategische communicatiemiddelen om kwaadwillige cyberactiviteiten te voorkomen, te ontmoedigen en erop te reageren. ONDERSTREEPT dat vijandige actoren zich ervan bewust moeten zijn dat cyberaanvallen tegen de lidstaten en EU-instellingen in een vroeg stadium zullen worden opgespoord, snel zullen worden geïdentificeerd en met alle nodige instrumenten en beleidsmaatregelen zullen worden afgeslagen. VERZOEKT de lidstaten en de hoge vertegenwoordiger om, met steun van de Commissie, uiterlijk aan het einde van het eerste kwartaal van 2023 met een herziene versie van de uitvoeringsrichtsnoeren van het EU-instrumentarium voor cyberdiplomatie te komen en hiervoor met name extra responsmaatregelen te bestuderen en voort te bouwen op de elementen van de cyberstrategie en de lessen die kunnen worden getrokken uit de uitvoering van het EU-instrumentarium voor cyberdiplomatie en uit de EU CyCLES-oefening.

24. ONDERSTREEPT dat in de betrokken organen en comités van de Raad regelmatig van gedachten moet worden gewisseld over het cyberdreigingslandschap, dat regelmatig met de privésector moet worden overlegd, dat moet worden voortgebouwd op de beoordeling van de gevolgen en de ernst van recente incidenten, zodat het EU-instrumentarium voor cyberdiplomatie meer bekendheid krijgt en de paraatheid voor verdere toepassing ervan wordt vergroot, en dat bijkomende instrumenten ter ondersteuning van de uitvoering ervan moeten worden ontwikkeld. Neemt ER NOTA VAN dat nationale veiligheid weliswaar de exclusieve bevoegdheid van elke lidstaat blijft, maar dat de uitwisseling van inlichtingen en informatie en de samenwerking tussen de lidstaten onderling en met EU-Intcen moeten worden versterkt, zodat inlichtingen, onder meer over het attributievraagstuk, aan het begin van het besluitvormingsproces kunnen worden uitgewisseld en zo een snelle, doeltreffende en onderbouwde respons op kwaadwillige cyberactiviteiten die gericht zijn op de EU en haar partners, mogelijk maken. HERHAALT dat het belangrijk is de capaciteit van EU-Intcen op cybergebied te versterken, op basis van inlichtingen die de lidstaten vrijwillig verstrekken en onverminderd hun bevoegdheden, en het voorstel voor de mogelijke oprichting van een werkgroep cyberinlichtingen van de lidstaten te onderzoeken.

25. ERKENT dat van de EU-verklaringen en de beperkende maatregelen in het kader van het EU-instrumentarium voor cyberdiplomatie het krachtige signaal is uitgegaan dat kwaadwillige cyberactiviteiten die voor de EU, haar lidstaten en partners een externe bedreiging vormen, onaanvaardbaar zijn, en dat deze verklaringen en maatregelen aldus bijdragen aan het voorkomen, ontmoedigen en aanpakken van kwaadwillige cyberactiviteiten, en HERHAALT zijn voornemen deze maatregelen te gebruiken om te herinneren aan de verplichtingen die uit hoofde van het internationaal recht, met inbegrip van het gehele VN-Handvest, op de cyberspace van toepassing zijn, alsook zijn voornemen het VN-kader voor verantwoordelijk gedrag van staten in de cyberspace te bevorderen, waaronder de zorgvuldigheidsverplichting voor alle staten om hun grondgebied niet bewust te lenen voor internationale kwaadwillige acties waarbij van ICT wordt gebruikgemaakt, met het oog op de verdere ontwikkeling en bevordering van een gemeenschappelijk EU-standpunt over de toepassing van het internationaal recht in de cyberspace. STELT VAST dat passende en snelle signalen de risico's van escalatie beperken en aanvallers die het op Europese belangen gemunt hebben, kunnen ontmoedigen, en VERZOEKT de hoge vertegenwoordiger een samenhangende communicatiestrategie over het gebruik van het EU-instrumentarium voor cyberdiplomatie te ontwikkelen en aan de lidstaten voor te leggen.

26. MOEDIGT de ontwikkeling AAN van geleidelijke, gerichte en duurzame benaderingen van en reacties op kwaadwillige cyberactiviteiten, waarbij wordt gebruikgemaakt van het brede scala aan instrumenten van het EU-instrumentarium voor cyberdiplomatie, met inbegrip van de EU-cybersanctieregeling, en aanvullende maatregelen worden overwogen. BENADRUKT dat de mogelijkheid moet worden vergroot om, per geval, alle beschikbare interne en externe instrumenten in te zetten om cyberaanvallen te voorkomen, te ontmoedigen en erop te reageren, en dat deze snel, doeltreffend, geleidelijk, gericht, op duurzame wijze en op basis van strategische langetermijnbetrokkenheid moeten worden uitgevoerd. VERZOEKT de hoge vertegenwoordiger om, in samenwerking met de Commissie, mogelijke gezamenlijke reacties van de EU op cyberaanvallen in het hele spectrum, met inbegrip van sanctiemogelijkheden, in kaart te brengen, teneinde voorbereid te zijn om indien nodig snel en doeltreffend op te treden, en deze reacties uiterlijk aan het einde van het eerste kwartaal van 2023 aan de Raad voor te leggen.

27. STELT VAST dat cyberdefensie in de eerste plaats een nationale bevoegdheid is en MOEDIGT de lidstaten AAN hun capaciteiten op het gebied van cyberdefensieoperaties verder te ontwikkelen en proactieve maatregelen te nemen om zich te beschermen en te wapenen tegen cyberaanvallen en deze op te sporen en te ontmoedigen, en eventueel andere lidstaten en de EU hierbij te ondersteunen. Elke lidstaat wordt aangemoedigd om, indien nodig, zijn vermogen om steun en bijstand te verlenen en te ontvangen, op te voeren. BENADRUKT dat de verdere ontwikkeling van deze vermogens een van de belangrijkste doelstellingen van het komende cyberdefensiebeleid van de EU moet zijn. STELT VAST dat in het cyberdefensiebeleid van de EU meer aandacht moet worden besteed aan de rol die de betrokken EU-instellingen en -organen overeenkomstig hun respectieve mandaten kunnen spelen bij het versterken van de samenwerking tussen de relevante cyberdefensieactoren van de EU en van de lidstaten en het ontwikkelen van hun capaciteiten. VERZOEKT de hoge vertegenwoordiger en de Commissie om, ter aanvulling van de ontwikkeling van een EU-cyberstrategie, in 2022 met een ambitieus voorstel voor een cyberdefensiebeleid van de EU te komen, op basis waarvan de Raad de EU-cyberstrategie verder zal kunnen ontwikkelen.

28. BENADRUKT DAT de interoperabiliteit en de informatiedeling moeten worden vergroot door samenwerking tussen militaire computercrisisteams (mil CERT). VERZOEKT de lidstaten om, voortbouwend op de werkzaamheden van het EDA, een "mil CERT"-netwerk op te zetten voor een betere samenwerking en informatie-uitwisseling, hetgeen ook de coördinatie met andere cybergemeenschappen zou helpen bevorderen, alsook een netwerk van militaire cybercommandanten om de strategische samenwerking tussen de cybercommando's van de EU-lidstaten of andere soortgelijke autoriteiten te versterken. Het opzetten van deze netwerken zou, samen met PESCO-cyberprojecten, bijdragen tot een versterkte cyberdefensie op EU-niveau. BENADRUKT dat samenwerking tussen het voorgestelde "mil CERT"-netwerk en het reeds bestaande civiele CSIRT's-netwerk belangrijk is om de informatiedeling en het situatiebewustzijn te verbeteren.

29. HERHAALT, op basis van de militaire visie en strategie van de EU inzake cyberspace als een domein van operaties en nota nemend van de lopende ontwikkeling van het militaire concept inzake cyberdefensie voor door de EU geleide militaire operaties en missies, dat de cyberdimensie moet worden geïntegreerd in de planning en uitvoering van GBVB-missies en -operaties, onder meer door het verbeteren van de cybercapaciteiten ervan, en BENADRUKT dat dit zal bijdragen tot een groter situatiebewustzijn op EU-niveau wat betreft cyberbeveiliging.

30. STELT tot slot VAST dat de cyberstrategie een stap zal zijn in de richting van de vaststelling van een EU-doctrine voor actie in de cyberspace, die gebaseerd zal zijn op een grotere veerkracht, ruimere capaciteiten en betere responsmogelijkheden, alsook van een gedeeld standpunt over de toepassing van het internationaal recht in de cyberspace. De Raad ZAL in 2023 DE BALANS OPMAKEN van de vorderingen met de uitvoering van deze conclusies, teneinde de cyberstrategie van de EU verder te ontwikkelen.