Raad van de
Europese Unie

Brussel, 9 maart 2021
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

NOTA I/A-PUNT

van:	het secretariaat-generaal van de Raad
aan:	het Comité van permanente vertegenwoordigers/de Raad
Betreft:	Ontwerpconclusies van de Raad over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

1. Op 16 december 2020 hebben de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid hun gezamenlijke mededeling aan het Europees Parlement en de Raad "De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk" bekendgemaakt[1]. Doel van de nieuwe cyberbeveiligingsstrategie is Europa collectief beter bestand te maken tegen cyberdreigingen zodat alle burgers en bedrijven ten volle kunnen profiteren van betrouwbare diensten en digitale instrumenten.

[1] Document 14133/20.

2. De Commissie en de EDEO hebben toelichting gegeven bij de gezamenlijke mededeling tijdens de informele videoconferentie van de Horizontale Groep cybervraagstukken (HWPCI) van 17 december 2020 en 12 januari 2021. Tijdens de informele videoconferentie van de HWPCI van 17 december 2020 heeft het aantredende Portugese voorzitterschap zijn voornemen aangekondigd ontwerpconclusies van de Raad over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk op te stellen.

3. Het voorzitterschap heeft tijdens de informele videoconferentie van de HWPCI van 2 februari 2021 een eerste ontwerp van de conclusies van de Raad voorgesteld. Deze conclusies werden vervolgens besproken tijdens informele videoconferenties van de HWPCI die plaatsvonden op 9 februari 2021, 19 februari 2021, 1 maart 2021 en 9 maart 2021.

4. Aangezien de ontwerpconclusies ook een verwijzing naar het defensiebeleid van de EU bevatten (punt 30), heeft de Politiek-militaire Groep (PMG) het desbetreffende punt op 10 februari 2021 besproken.

5. Verschillende punten hebben betrekking op het gemeenschappelijk buitenlands en veiligheidsbeleid (punten 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32, en 33) en zijn derhalve voorgelegd aan het Politiek en Veiligheidscomité, dat deze punten op 4 maart 2021 heeft goedgekeurd.

6. Tijdens de informele videoconferentie van de HWPCI van 9 maart 2021 is in de groep overeenstemming bereikt over de ontwerpconclusies van de Raad in document 6722/21.

7. Het Comité van permanente vertegenwoordigers wordt derhalve verzocht de bijgaande ontwerpconclusies van de Raad aan de Raad voor te leggen en hem in overweging te geven ze als A-punt aan te nemen.

BIJLAGE

Ontwerpconclusies van de Raad over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

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[2],

- internetgovernance[3],

- 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[4],

- het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU[5],

- het belang van 5G voor de Europese economie en de noodzaak om de veiligheidsrisico's in verband met 5G te beperken[6],

- 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"[7],

- extra inspanningen ter versterking van de weerbaarheid en bestrijding van hybride dreigingen[8],

- de digitale toekomst van Europa vormgeven[9],

---

2 Document 12109/13.
3 Document 16200/14.
4 Document 14435/17 + COR 1.
5 Document 7737/19.
6 Document 14517/19.
7 Document 9596/19.
8 Document 14972/19.
9 Document 8711/20.

- digitale diplomatie[10],

- het versterken van de weerbaarheid en het bestrijden van hybride dreigingen, waaronder desinformatie, in de context van de COVID-19-pandemie[11],

- cyberdiplomatie[12],

- gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[13],

- een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("Instrumentarium voor cyberdiplomatie")[14],

- richtsnoeren voor het opbouwen van externe cybercapaciteit van de EU[15],

- een herstel dat de overgang naar een meer dynamische, veerkrachtige en concurrerende Europese industrie bevordert[16],

- de cyberbeveiliging van verbonden apparaten[17],

- het versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche[18],

- en resolutie van de Raad over versleuteling - Beveiliging dankzij versleuteling en beveiliging ondanks versleuteling[19],

---

10 Document 12804/20.
11 Document 14064/20.
12 Document 6122/15 + COR 1.
13 Document 10086/18.
14 Document 10474/17.
15 Document 10496/18.
16 Document 13004/20.
17 Document 13629/20.
18 Document 14540/16.
19 Document 13084/1/20 REV 1.

- en de verklaring van de lidstaten van 15 oktober 2020 over een "next generation cloud" voor bedrijven en de publieke sector in de EU,

HERINNEREND aan de conclusies van de Europese Raad over COVID-19, de eengemaakte markt, het industriebeleid, digitalisering en externe betrekkingen van 1-2 oktober 2020[20] en de conclusies over desinformatie en hybride dreigingen en over de nieuwe strategische agenda 2019-2024 van 20 juni 2019[21],

HERINNEREND aan de algemene strategie voor de Europese Unie op het gebied van buitenlands en veiligheidsbeleid – Gedeelde visie, gemeenschappelijke actie: een sterker Europa, van 28 juni 2016,

HERINNEREND aan de mededelingen van de Europese Commissie "De digitale toekomst van Europa vormgeven" van 19 december 2020[22] en "De EU-strategie voor de veiligheidsunie" van 24 juli 2020[23],

HERINNEREND AAN de gezamenlijke mededeling van de Europese Commissie en de hoge vertegenwoordiger over een nieuwe EU/VS-agenda voor wereldwijde verandering, van 2 december 2020[24],

1. BENADRUKT dat cyberbeveiliging van essentieel belang is voor de opbouw van een veerkrachtig, groen en digitaal Europa, en IS INGENOMEN met de gezamenlijke mededeling aan het Europees Parlement en de Raad "De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk", waarin het nieuwe kader wordt geschetst voor EU-actie op het gebied van "veerkracht, technologische soevereiniteit en leiderschap", om mensen, ondernemingen en instellingen in de EU te beschermen tegen cyberincidenten en -dreigingen, en waarmee het vertrouwen wordt aangewakkerd van personen en organisaties in het vermogen van de EU om veilige en betrouwbare netwerk- en informatiesystemen, infrastructuur en connectiviteit te bevorderen en om een mondiale, open, vrije, stabiele en veilige cyberspace die gestoeld is op mensenrechten, fundamentele vrijheden, democratische beginselen en de rechtsstaat te bevorderen en te beschermen.

---

20 Document EUCO 13/20.
21 Document EUCO 9/19.
22 Document COM(2020) 67 final, van 19.2.2020.
23 Document COM(2020) 605 final, van 24.7.2020.
24 Document JOIN(2020) 22 final, van 2.12.2020.

2. ERKENT dat de toenemende behoefte aan betrouwbare en veilige ICT-instrumenten door de COVID-19-pandemie in ons dagelijks leven brandend actueel is geworden. BENADRUKT dat cyberbeveiliging en het mondiale, open internet essentieel zijn voor de werking van openbare diensten en instellingen, zowel nationaal als op EU-niveau, en voor onze samenleving en de gehele economie.

3. BENADRUKT dat het zaak is de politieke en strategische besluitvormers beter bekend te maken met cybervraagstukken, door hun kennis en informatie over dat onderwerp te verschaffen, en ONDERSTREEPT dat het grote publiek hiervan bewuster moet worden gemaakt en dat cyberhygiëne moet worden bevorderd.

4. PLEIT voor de bevordering en bescherming van de kernwaarden van de EU: democratie, de rechtsstaat, mensenrechten en fundamentele vrijheden, met inbegrip van het recht op vrijheid van meningsuiting en informatie, het recht op vrijheid van vergadering en vereniging en het recht op privacy in cyberspace. VERWELKOMT in dit verband het aanhoudende streven tot bescherming van mensenrechtenverdedigers, maatschappelijke organisaties en academici die zich bezighouden met problemen omtrent cyberbeveiliging, dataprivacy, surveillance en onlinecensuur; dat streven houdt in dat verdere praktische richtsnoeren worden verstrekt, beste praktijken worden bevorderd en de EU-inspanningen ter voorkoming van mensenrechtenschendingen en misbruik van opkomende technologieën worden opgevoerd, met name door indien nodig diplomatieke maatregelen te nemen en de uitvoer van die technologieën te controleren. BENADRUKT in dit verband het belang van het EU-actieplan inzake mensenrechten en democratie 2020-2024 en de bijbehorende mensenrechtenrichtsnoeren inzake de vrijheid van meningsuiting online en offline.

5. BENADRUKT dat, om zelf te bepalen wat haar economische koers is en waar haar economische belangen liggen, de EU tot strategische autonomie met behoud van een open economie moet komen. Dit houdt onder meer in dat de EU beter in staat moet zijn autonome keuzes te maken op het gebied van cyberbeveiliging, teneinde haar digitale leiderschap en strategische capaciteiten te versterken. WIJST erop dat hiertoe strategische afhankelijkheden moeten worden vastgesteld en gereduceerd en dat de veerkracht in de gevoeligste industriële ecosystemen en op specifieke gebieden als energie moet worden vergroot. ONDERSTREEPT dat dit kan inhouden dat productie- en toeleveringsketens worden gediversifieerd, dat investeringen en productie in Europa worden gestimuleerd zo nodig naar Europa gehaald, dat er alternatieve oplossingen en circulaire modellen worden verkend, en dat brede industriële samenwerking tussen de lidstaten wordt gestimuleerd.

6. BENADRUKT dat er, gezien het tekort aan digitale en cyberbeveiligingsvaardigheden bij de beroepsbevolking, voldaan moet worden aan de vraag naar werknemers met dergelijke vaardigheden, met name door toptalenten te ontwikkelen, te behouden of aan te trekken, bijvoorbeeld via onderwijs en opleiding, om onze samenleving op een cyberveilige manier te kunnen digitaliseren. MOEDIGT vrouwen en meisjes aan om vaker te kiezen voor STEM-vakken (wetenschap, technologie, engineering en wiskunde), ICT-banen, en bij- en nascholingen in digitale vaardigheden, als middel om de digitale genderkloof te verkleinen.

7. HERINNERT eraan dat de gemeenschappelijke en alomvattende EU-aanpak voor cyberdiplomatie gericht is op conflictpreventie, het beperken van cyberbeveiligings-dreigingen en een grotere stabiliteit in de internationale betrekkingen. HERHAALT in dit verband dat hij zich inzet voor de vreedzame regeling van internationale geschillen in cyberspace en dat alle diplomatieke inspanningen van de EU als prioriteit beveiliging en stabiliteit in cyberspace moeten bevorderen door intensievere internationale samenwerking, en het risico op misvattingen, escalatie en conflicten als gevolg van ICT-incidenten moeten beperken, en STEUNT de verdere ontwikkeling en operationalisering van vertrouwen-wekkende maatregelen (CBM's) op regionaal en internationaal niveau. HERHAALT de bij consensus overeengekomen oproep van de Algemene Vergadering van de Verenigde Naties aan de VN-lidstaten om de aanbevelingen voor ICT-gebruik in de rapporten van de UNGGE te volgen en BEVESTIGT de toepassing van het internationaal recht, met name van het VN-Handvest in zijn geheel, in cyberspace.

8. BEVESTIGT dat de verdere ontwikkeling van normen en standaarden binnen de Unie van essentieel belang is om substantieel vorm te kunnen geven aan internationale normen en standaarden wat betreft opkomende technologieën en wat betreft de noodzakelijke technische en logische infrastructuur voor de algemene beschikbaarheid en integriteit van de publieke kern van het internet, zodat die in overeenstemming zijn met universele en EU-waarden en ontwikkeld worden via een multistakeholderbenadering. Op die manier kan het internet mondiaal, open, vrij, stabiel en veilig blijven, kunnen digitale technologieën gebruikt en ontwikkeld worden met respect voor de mensenrechten en kan er op een rechtmatige, veilige en ethische manier gebruik van worden gemaakt. NEEMT NOTA van de aanstaande normalisatiestrategie en VERBINDT ZICH ertoe proactief en gecoördineerd campagne te voeren voor EU-leiderschap en de EU-doelstellingen op internationaal niveau, onder meer in diverse internationale normalisatie-instellingen en door samen te werken met gelijkgestemde partners, het maatschappelijk middenveld, de academische wereld en de particuliere sector.

9. STEUNT ten zeerste het multistakeholdermodel voor internetgovernance en cyberbeveiliging en verbindt zich ertoe regelmatige en gestructureerde uitwisselingen met belanghebbenden – zoals de particuliere sector, de academische wereld en het maatschappelijk middenveld– in internationale fora te intensiveren, ook in het kader van de Paris call for Trust and Security in Cyberspace. STIMULEERT universele, betaalbare en gelijke toegang tot het internet om de digitale kloof te dichten, met bijzondere aandacht voor de empowerment van vrouwen en meisjes en personen in kwetsbare of gemarginaliseerde situaties, zowel bij beleidsontwikkeling als bij het internetgebruik.

10. BENADRUKT dat cyberbeveiliging de komende jaren moet worden geïntegreerd bij digitale investeringen en initiatieven en dat geleidelijk moet worden bijgedragen aan een gelijk speelveld op het gebied van cyberbeveiliging, en NEEMT NOTA van het plan van de Commissie om de overheidsuitgaven te verhogen en particuliere investeringen op het gebied van cyberbeveiliging aan te trekken. BENADRUKT het belang van kleine en middelgrote ondernemingen (kmo's) in het cyberbeveiligingsecosysteem en ONDERKENT de beschikbare financiële instrumenten waarmee een sterke focus op cyberbeveiliging binnen de digitale transformatie ondersteund kan worden tijdens de looptijd van het meerjarig financieel kader (MFK) 2021-2027 en in het kader van de herstel- en veerkrachtfaciliteit.

11. ZIET UIT naar de snelle uitvoering van de verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra, en hoopt dat het Europees kenniscentrum voor cyberbeveiliging in Boekarest snel kan worden opgestart en snel operationeel wordt. Mede door een snelle vaststelling van de agenda zullen de investeringen maximaal effect sorteren om het leiderschap en de strategische autonomie van de Unie op het gebied van cyberbeveiliging te versterken, om technologische capaciteiten en vaardigheden te ondersteunen, en om het mondiale concurrentievermogen van de Unie te vergroten met inbreng van het bedrijfsleven en academische gemeenschappen op het gebied van cyberbeveiliging, onder meer van kmo's en onderzoekscentra, die baat zullen hebben bij een meer systematische, inclusieve en strategische samenwerking, gelet op de cohesie van de Unie en al haar lidstaten.

12. IS, samen met de lidstaten en belanghebbenden, INGENOMEN met de lopende werkzaamheden van Enisa om Europese certificeringsregelingen op te stellen voor ICT-producten, -diensten en -processen die moeten bijdragen tot een hoger algemeen niveau van cyberbeveiliging binnen de digitale eengemaakte markt. ZIET in dit verband UIT naar het voortschrijdend werkprogramma van de Unie met het oog op de ontwikkeling van Europese certificeringsregelingen cyberbeveiliging in het kader van de cyberbeveiligingsverordening. ERKENT in dit verband de centrale rol van de EU om standaarden te ontwikkelen die het cyberbeveiligingslandschap vorm kunnen geven en die bijdragen tot eerlijke concurrentie binnen de EU en wereldwijd, waarbij markttoegang wordt bevorderd, veiligheidsrisico's worden aangepakt, en de toepasselijkheid van het wetgevingskader van de EU wordt gewaarborgd.

13. HERHAALT dat het belangrijk is na te gaan of er op lange termijn behoefte is aan horizontale wetgeving, onder meer tot nadere bepaling van de noodzakelijke voorwaarden voor marktintroductie, om alle relevante aspecten van cyberbeveiliging van verbonden apparaten, zoals beschikbaarheid, integriteit en vertrouwelijkheid, te regelen. VERWELKOMT in dit verband een bespreking over het werkingssfeer van dergelijke wetgeving en hoe die zich verhoudt tot het kader voor cyberbeveiligingscertificering zoals omschreven in de cyberbeveiligingsverordening, en die als doel heeft het beveiligingsniveau binnen de digitale eengemaakte markt te verhogen. BENADRUKT dat de vereisten inzake cyberbeveiliging moeten worden omschreven in overeenstemming met de desbetreffende Uniewetgeving, waaronder de cyberbeveiligingsverordening, het nieuwe wetgevingskader (NWK), de verordening Europese normalisatie en mogelijke toekomstige horizontale wetgeving, zulks om dubbelzinnige en gefragmenteerde wetgeving te voorkomen.

14. ONDERKENT het belang van een alomvattende en horizontale aanpak van cyberbeveiliging in de Unie, met volledige inachtneming van de bevoegdheden en behoeften van de lidstaten, evenals het belang van permanente ondersteuning voor technische bijstand en samenwerking om de capaciteit van de lidstaten op te bouwen. NEEMT, rekening houdend met het evoluerende landschap van cyberdreigingen, NOTA van het nieuwe voorstel voor een richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyber-beveiliging in de hele Unie, dat voortbouwt op de NIS-richtlijn, en herhaalt zijn steun voor sterkere en geharmoniseerde nationale cyberbeveiligingskaders en duurzame samenwerking tussen de lidstaten. BENADRUKT voorts dat afstemming en onderlinge samenhang van de sectorale wetgeving op dit gebied nodig zijn.

15. NEEMT NOTA van het voorstel van de Commissie om de lidstaten te ondersteunen bij het opzetten en versterken van operationele beveiligingscentra, teneinde een netwerk van dergelijke centra in de hele EU uit te bouwen, om signalen van mogelijke aanvallen op netwerken verder te monitoren en erop te anticiperen. WACHT in dit verband op de gedetailleerde plannen van de Commissie met betrekking tot het netwerk van operationele beveiligingscentra, met inachtneming van de bevoegdheden van de lidstaten. HERINNERT aan de door de EU gesteunde inspanningen van de lidstaten om sectorale, nationale en regionale Computer Security Incident Response Teams (CSIRT's) en nationale of Europese centra voor informatie-uitwisseling en -analyse (ISAC's) op te zetten als onderdeel van een doeltreffend netwerk van cyberbeveiligingspartnerschappen in de Unie. ZIET ernaar UIT na te gaan of dit netwerk te potentieel heeft voor het versterken van operationele beveiligings-centra, en of die centra complementair zijn en gecoördineerd worden met bestaande netwerken en actoren (met name het CSIRT-netwerk), teneinde een efficiënte, veilige en betrouwbare cultuur van informatie-uitwisseling te bevorderen. BENADRUKT dat dit proces zal voortbouwen op het werk dat is verricht rond initiatieven op het gebied van artificiële intelligentie en high-performance computing en door de Europese digitale-innovatiehubs.

16. NEEMT NOTA van de mogelijke ontwikkeling van een veilig connectiviteitssysteem, dat voortbouwt op de Europese kwantumcommunicatie-infrastructuur (EuroQCI) en het EU-initiatief voor satellietcommunicatie voor overheidsgebruik (GOVSATCOM), en ONDERKENT dat elke mogelijke toekomstige ontwikkeling gebaseerd moet zijn op een robuust cyberbeveiligingskader en rekening moet houden met de volledige elektronische-communicatie-infrastructuur, zoals netwerksystemen in de ruimte, over land of onder zee.

17. ZIET UIT naar besprekingen met de Commissie, Enisa, de twee exploitanten van DNS-rootservers in de EU en de multistakeholdergemeenschap om te beoordelen welke rol deze twee exploitanten spelen in het garanderen dat het internet wereldwijd toegankelijk blijft en niet versnipperd is. IS INGENOMEN met de verdere discussie over het voornemen van de Commissie om een alternatieve, Europese dienst te ontwikkelen om toegang te krijgen tot het mondiale internet (DNS4EU-initiatief), op basis van een transparant model dat in overeenstemming is met de meest recente normen en regels inzake beveiliging, gegevens-bescherming, privacy door ontwerp en privacy door standaardinstellingen, teneinde bij te dragen tot een grotere weerbaarheid en tevens de internationale connectiviteit voor alle lidstaten in stand te houden en te verbeteren.

18. ERKENT dat de Commissie en de lidstaten zich samen moeten inzetten om de toepassing van essentiële internetstandaarden, waaronder IPv6 en gevestigde standaarden voor internetbeveiliging te versnellen, gezien hun belangrijke rol bij het verhogen van het algemene niveau van beveiliging, weerbaarheid, openheid en interoperabiliteit van het mondiale internet en bij de versterking van het concurrentievermogen van de EU-industrie en met name van de exploitanten van internetinfrastructuur.

19. BENADRUKT het belang van een gecoördineerde aanpak en van de ontwikkeling en uitvoering van doeltreffende maatregelen op nationaal niveau ter versterking van de cyberbeveiliging van 5G-netwerken. STEUNT de volgende stappen die op het gebied van de cyberbeveiliging van 5G-netwerken gezet moeten worden, zoals uiteengezet in de bijlage bij de EU-strategie inzake cyberbeveiliging en die gebaseerd zijn op de resultaten van het verslag over het effect van de Aanbeveling van de Commissie betreffende de cyber-beveiliging van 5G-netwerken, bijvoorbeeld met betrekking tot het bepalen van een integrale langetermijnaanpak waarbij wordt gekeken naar de gehele 5G-waardeketen en het 5G-ecosysteem. VERZOEKT de lidstaten, de EU-instellingen en andere belanghebbenden, met het oog op een versterkte gecoördineerde aanpak van de beveiliging van 5G-netwerken, hun periodieke inventarisatie en de uitwisseling van informatie en beste praktijken binnen de specifieke werkstroom van de NIS-samenwerkingsgroep inzake 5G-cyberbeveiliging voort te zetten, en regelmatig verslag uit te brengen aan de Raad over de geboekte vooruitgang. WIJST erop dat hij vastbesloten is de maatregelen van de EU-toolbox voor 5G uit te voeren en snel te voltooien en zich te blijven inspannen om de beveiliging van 5G-netwerken en de ontwikkeling van toekomstige generaties netwerken te waarborgen, en benadrukt tevens dat de lidstaten verantwoordelijk zijn voor de bescherming van de nationale veiligheid. De nauwe samenwerking tussen de lidstaten, de Commissie en Enisa op het gebied van de beveiliging van 5G-netwerken kan als voorbeeld dienen voor andere cyberbeveiligings-vraagstukken, met inachtneming van de bevoegdheden van de lidstaten en de beginselen van subsidiariteit en evenredigheid.

20. ERKENT dat cyberbeveiliging verder moet worden ingebed in de EU-crisisrespons-mechanismen, die met oefeningen getest moeten worden, en ONDERSTREEPT dat de samenwerking en informatie-uitwisseling tussen de verschillende EU-cybergemeenschappen versterkt moet worden en de bestaande initiatieven, structuren en procedures (zoals de IPCR, het CSIRT-netwerk, de NIS-samenwerkingsgroep, het CyCLONe-netwerk, het Europees Centrum voor de bestrijding van cybercriminaliteit, het inlichtingen- en situatiecentrum van de Europese Unie (EU INTCEN) en andere relevante EU-organen) bij grootschalige en grensoverschrijdende cyberincidenten en -dreigingen aan elkaar gekoppeld moeten worden. VERWACHT, REKENING HOUDEND met de reeds geboekte vooruitgang op dit gebied, het voorstel van de Commissie inzake het proces, de mijlpalen en het tijdpad voor het opzetten van de gezamenlijke cybereenheid, teneinde toegevoegde waarde, duidelijke focus en stroomlijning van het EU-kader voor crisisbeheersing inzake cyberbeveiliging te kunnen bieden, onder meer door paraatheid, gedeeld situationeel bewustzijn, versterkte gecoördineerde respons en oefeningen, op een transparante en stapsgewijze manier, zonder dubbel werk of overlapping, en met inachtneming van de bevoegdheden van de lidstaten.

21. BENADRUKT dat de samenwerking en informatie-uitwisseling tussen cyberbeveiligings-actoren en de voor veiligheid en strafrecht bevoegde instanties, zoals rechtshandhavings- en gerechtelijke instanties, gestimuleerd moet worden, en wijst er ook op dat de capaciteit van deze instanties om cybercriminaliteit te onderzoeken en te vervolgen, moet worden uitgebreid en verbeterd, en dat internationale onderhandelingen en EU-regels inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal moeten worden bevorderd. Het is cruciaal dat de voor beveiliging en het strafrecht bevoegde instanties, ongeacht de stand der technologie op een gegeven tijdstip, via rechtmatige toegang hun bevoegdheden kunnen behouden om hun wettelijk voorgeschreven en toegestane taken uit te voeren. Dergelijke wetgeving waarin de handhavingsbevoegdheden worden geregeld, moet te allen tijde de eerlijke rechtsbedeling en andere waarborgen alsmede de grondrechten in acht nemen, met name het recht op eerbiediging van het privéleven en communicatie en het recht op bescherming van persoonsgegevens.

22. BEVESTIGT zijn steun voor de ontwikkeling, invoering en toepassing van krachtige versleuteling als noodzakelijk middel voor de bescherming van de grondrechten en voor de digitale beveiliging van personen, overheden, de bedrijfswereld en de samenleving, en ONDERKENT tegelijkertijd dat de op het gebied van beveiliging en het strafrecht bevoegde instanties, bijvoorbeeld rechtshandhavings- en gerechtelijke instanties, hun wettelijke bevoegdheden zowel online als offline moeten kunnen uitoefenen om onze samenlevingen en burgers te beschermen. De bevoegde autoriteiten moeten zich, met volledige inachtneming van de grondrechten en de toepasselijke gegevensbeschermingswetgeving, op rechtmatige en doelgerichte wijze toegang tot gegevens kunnen verschaffen en tegelijkertijd de cyberbeveiliging kunnen garanderen. BENADRUKT dat bij alle ondernomen acties deze belangen zorgvuldig moeten worden afgewogen tegen de beginselen van noodzakelijkheid, evenredigheid en subsidiariteit.

23. STEUNT en PROPAGEERT het Verdrag van Boedapest inzake cybercriminaliteit en de lopende werkzaamheden aan het tweede Aanvullend Protocol bij dat Verdrag. Blijft voorts deelnemen aan multilaterale uitwisselingen over cybercriminaliteit, onder meer inzake processen met betrekking tot de Raad van Europa, het Bureau van de Verenigde Naties voor drugs- en misdaadbestrijding (UNODC) en de Commissie Misdaadpreventie en Strafrecht (CCPCJ), teneinde te streven naar nauwere internationale samenwerking ter bestrijding van cybercriminaliteit, onder meer door uitwisseling van beste praktijken en technische kennis, en om capaciteitsopbouw te ondersteunen, met inachtneming, en ter bevordering en bescherming van de mensenrechten en de fundamentele vrijheden.

24. Herhaalt dat de nationale veiligheid de exclusieve verantwoordelijkheid van elke lidstaat blijft, maar ONDERKENT tevens het belang van strategische samenwerking inzake inlichtingen over cyberdreigingen en -activiteiten, en VERZOEKT de lidstaten via hun bevoegde instanties bij te dragen aan het werk van EU INTCEN als hub voor situationeel bewustzijn en dreigingsevaluaties voor Europese cybervraagstukken, en te onderzoeken of een werkgroep cyberinlichtingen van de lidstaten kan worden opgericht, teneinde de specifieke capaciteit van INTCEN op dit gebied te versterken, op basis van inlichtingen die vrijwillig door de lidstaten worden verstrekt, en onverminderd hun bevoegdheden.

25. BENADRUKT het belang van een robuust en consistent beveiligingskader om alle personeel, gegevens, communicatienetwerken en informatiesystemen evenals besluitvormingsprocessen in de EU te beschermen, op basis van alomvattende, consistente en homogene regels. Daartoe moet de EU weerbaarder worden gemaakt tegen cyber-dreigingen, moet er een betere Europese veiligheidscultuur komen, moet de beveiliging van gerubriceerde en niet-gerubriceerde EU-netwerken versterkt worden, en moet er tevens gezorgd worden voor goede governance en voldoende beschikbare middelen en capaciteiten, onder meer in het kader van de versterking van het mandaat van CERT-EU. IS in dit verband INGENOMEN met de lopende besprekingen over gemeenschappelijke regels inzake informatiebeveiliging, waarbij terdege rekening wordt gehouden met de beveiligings-voorschriften van de Raad voor de bescherming van gerubriceerde EU-informatie, en met de bepaling van gemeenschappelijke, bindende regels inzake cyberbeveiliging voor alle instellingen, organen en agentschappen van de EU.

26. VERBINDT ZICH ertoe om, VOORTBOUWEND op de cyberdiplomatie-inspanningen van de EU, de doeltreffendheid en de doelmatigheid van het Instrumentarium voor cyber-diplomatie te vergroten, en ZIET UIT naar diepgaandere besprekingen over de reikwijdte en het gebruik ervan waarbij wordt voortgebouwd op de lering die tot dusver is getrokken uit de toepassing van dit instrument. Deze besprekingen moeten ertoe bijdragen dat beveiliging op internationaal niveau wordt bevorderd, door dialoog en een gedeelde visie op cyber-beveiligingskwesties aan te moedigen, preventie, stabiliteit en samenwerking te versterken en vertrouwens- en capaciteitsopbouw te bevorderen alsook, waar nodig, beperkende maatregelen op te leggen, teneinde kwaadwillige cyberactiviteiten tegen de integriteit en veiligheid van de EU en haar lidstaten te voorkomen, te ontmoedigen, te bestrijden en erop te reageren, en aldus bij te dragen tot de internationale veiligheid en stabiliteit en de cyberhouding van de EU te consolideren, met volledige waarborging van de nationale bevoegdheden en prerogatieven. Er moet bijzondere aandacht worden besteed aan het voorkomen en tegengaan van cyberaanvallen met systemische effecten – onder andere cyberdiefstal van intellectuele eigendom – die onze toeleveringsketens, vitale infrastructuur, essentiële diensten, democratische instellingen en processen kunnen aantasten en onze economische zekerheid kunnen ondermijnen. De lidstaten en de EU-instellingen moeten ook verder nadenken over de onderlinge afstemming tussen het EU-kader voor crisisbeheersing inzake cyberbeveiliging, het Instrumentarium voor cyberdiplomatie en de bepalingen van artikel 42, lid 7, VEU en artikel 222, VWEU, met name door te werken op basis van scenario's om tot een gemeenschappelijk begrip te komen van de praktische regelingen voor de uitvoering van artikel 42, lid 7, VEU.

27. ERKENT dat de samenwerking met internationale organisaties en partnerlanden versterkt moet worden om het gemeenschappelijk inzicht in het cyberdreigingslandschap te bevorderen, dialogen en samenwerkingsmechanismen te ontwikkelen, in voorkomend geval gezamenlijke diplomatieke reacties te identificeren en de informatie-uitwisseling te verbeteren, onder meer via onderwijs, opleiding en oefeningen. BENADRUKT in het bijzonder dat een sterk trans-Atlantisch partnerschap op het gebied van cyberbeveiliging bijdraagt tot onze gemeenschappelijke veiligheid, stabiliteit en welvaart, en NEEMT NOTA van de bepalingen inzake samenwerking op het gebied van cyberbeveiliging in het kader van de handels- en samenwerkingsovereenkomst EU-VK. HERINNERT aan de belangrijkste resultaten van de samenwerking EU-NAVO op het gebied van cyber-beveiliging in het kader van de uitvoering van de gezamenlijke verklaringen van Warschau van 2016 en van Brussel van 2018, wijst nogmaals op het belang van een betere, wederzijds versterkende en voordelige samenwerking via onderwijs, opleiding, oefeningen en gecoördineerde respons op kwaadwillige cyberactiviteiten, met volledige inachtneming van de besluitvormingsautonomie en -procedures van beide organisaties, op basis van de beginselen van transparantie, wederkerigheid en inclusiviteit.

28. VERBINDT ZICH ertoe om – teneinde bij te dragen tot een mondiale, open, vrije, stabiele en veilige cyberspace, die een steeds belangrijker rol speelt bij het behoud van de welvaart, groei, veiligheid, het welzijn, de connectiviteit en integriteit van onze samenlevingen – betrokken te blijven bij normeringsprocessen in internationale organisaties, met name in de processen van de Eerste Commissie van de VN, door bij te dragen aan de erkenning van de toepassing van het internationaal recht in cyberspace en die processen tevens te bevorderen, en verbindt er zich eveneens toe de normen, regels en beginselen van verantwoordelijk staatsgedrag in cyberspace na te leven, onder meer door de spoedige oprichting van een actieprogramma ter bevordering van verantwoord gedrag van de staat in de cyberspace (PoA) als een constructief, inclusief en op consensus gebaseerde voortgangsbewaking van de huidige UNGGE- en openwerkgroepprocessen aan te moedigen.

29. HERINNERT eraan dat hij zeer gehecht is aan daadwerkelijk multilateralisme en een op regels gebaseerde wereldorde met een centrale rol voor de Verenigde Naties, en dat hij met betrekking tot besprekingen over cybervraagstukken en de voortzetting en uitbreiding van gestructureerde EU-cyberdialogen en -overleg met derde landen vastbesloten is om de samenwerking en coördinatie met internationale en regionale organisaties te versterken, te weten met het VN-systeem, de NAVO, de Raad van Europa, de OVSE, de OESO, de AU, de OAS, de Asean, het ARF, de GCC en de LAS. BENADRUKT dat hij de VN, en met name de Agenda 2030, inclusief de duurzameontwikkelingsdoelen, actief steunt en IS INGENOMEN met de routekaart voor digitale samenwerking van de secretaris-generaal van de VN en de agenda voor ontwapening van de secretaris-generaal van de VN, die verantwoordingsplicht en de naleving van normen in cyberspace stimuleren en bijdragen tot de preventie en het vreedzaam oplossen van conflicten die het gevolg zijn van kwaadwillige activiteiten in de cyberspace. IS INGENOMEN met het voorstel dat de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid een informeel EU-cyberdiplomatienetwerk zou oprichten, teneinde zowel op EU- als op lidstaatniveau te zorgen voor betrokkenheid en expertise op het gebied van internationale cybervraagstukken, om zo de gecoördineerde contacten te intensiveren.

30. ZIET UIT naar het komende voorstel voor een doorlichting van het beleidskader voor cyberdefensie (CDPF), en VERBINDT ZICH ertoe blijvende inspanningen te leveren om de cyberbeveiligings- en cyberdefensiedimensies te versterken, opdat deze volledig geïntegreerd worden in het bredere domein van veiligheid en defensie, met name in het kader van het werk omtrent het strategisch kompas. IS VAN OORDEEL dat de aanstaande "militaire visie en strategie over cyberspace als een domein van operaties" deze besprekingen vooruit zal helpen. IS INGENOMEN met het initiatief van het Europees Defensieagentschap (EDA) om samenwerking tussen militaire CERT's te stimuleren en STEUNT de geleverde inspanningen om civiel-militaire synergie alsook coördinatie op het gebied van cyberdefensie en cyberbeveiliging te versterken, onder meer voor ruimtegerelateerde aspecten en via de specifieke PESCO-projecten.

31. IS INGENOMEN met het voorstel om een externe agenda van de EU voor de opbouw van cybercapaciteit te ontwikkelen, met het voorstel om een EU-raad voor de opbouw van cybercapaciteit op te richten, en met de oprichting en uitvoering van EU CyberNet (het netwerk voor de opbouw van cybercapaciteit van de EU) om de cyberweerbaarheid en -capaciteiten wereldwijd te vergroten. VERWELKOMT in dit verband de samenwerking met de lidstaten en met partners uit de openbare en de particuliere sector, met name het Wereldwijde Forum inzake cyberexpertise (GFCE) en andere internationale organen, om te zorgen voor coördinatie en overlappingen te vermijden. MOEDIGT in het bijzonder samenwerking AAN met partners van de Westelijke Balkan en in de oostelijke en zuidelijke buurlanden van de EU.

32. VERBINDT ZICH ertoe, opdat alle landen de sociale, economische en politieke vruchten van het internet en het gebruik van technologieën kunnen plukken, en mede in aansluiting op de inspanningen onder het Europees actieplan voor democratie, de partnerlanden te helpen bij het aanpakken van de toenemende uitdaging van kwaadwillige cyberactiviteiten, met name die welke de ontwikkeling van hun economieën en samenlevingen alsook de integriteit en veiligheid van democratische systemen schaden.

33. SPOORT de Commissie en de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid AAN om, met het oog op de ontwikkeling, uitvoering en monitoring van voorstellen in de EU-cyberbeveiligingsstrategie, en rekening houdend met het meerjarige karakter van sommige initiatieven, een gedetailleerd uitvoeringsplan op te stellen met de prioriteiten en het tijdschema van de geplande acties. Zal TOEZIEN op de voortgang bij de uitvoering van deze conclusies door middel van een actieplan dat regelmatig zal worden geëvalueerd en geactualiseerd door de Raad, in nauwe samenwerking met de Europese Commissie en de hoge vertegenwoordiger.