Raad van de
Europese Unie

Brussel, 8 oktober 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

NOTA I/A-PUNT

van:	het secretariaat-generaal van de Raad
aan:	het Comité van permanente vertegenwoordigers (2e deel)/de Raad
Betreft:	Conclusies van de Raad – Het potentieel verkennen van het initiatief voor een gezamenlijke cybereenheid ter aanvulling op de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises - Goedkeuring

1. De Commissie heeft op 23 juni 2021 een aanbeveling uitgebracht over de opbouw van een gezamenlijke cybereenheid[1] tegen het toenemende aantal ernstige cyberincidenten waar overheidsdiensten, bedrijven en burgers in de hele Europese Unie het slachtoffer van zijn.

2. De Commissie heeft de aanbeveling op 28 juni 2021 gepresenteerd in de Horizontale Groep cybervraagstukken (HWPCI). Op 7 en 14 juli 2021 heeft de HWPCI zich onder Sloveens voorzitterschap over de Commissieaanbeveling gebogen om te inventariseren hoe de lidstaten deze bezien.

[1] C(2021)4520 final (11155/21 en 11155/21 ADD1).

3. Het voorzitterschap heeft tijdens de informele videoconferentie van de leden van de HWPCI van 23 juli 2021 een eerste ontwerp van Raadsconclusies uitgebracht over "Het potentieel verkennen van het initiatief voor een gezamenlijke cybereenheid ter aanvulling op de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[2]. De HWPCI heeft zich op 8 en 29 september 2021 nader over deze ontwerpconclusies gebogen.

4. De HWPCI heeft op 6 oktober 2021 overeenstemming over bijgaande ontwerpconclusies van de Raad bereikt.

5. Het Comité van permanente vertegenwoordigers wordt derhalve verzocht deze ontwerp-conclusies van de Raad voor te leggen aan de Raad en deze in overweging te geven ze als A-punt aan te nemen.

---

[2] 10975/21.

BIJLAGE

Ontwerpconclusies van de Raad – Het potentieel verkennen van het initiatief voor een gezamenlijke cybereenheid ter aanvulling op de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises

DE RAAD VAN DE EUROPESE UNIE,

HERINNEREND aan zijn conclusies over:

– de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[3],

– de gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[4],

– cyberdiplomatie[5],

– een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("Instrumentarium voor cyberdiplomatie")[6],

– veiligheid en defensie[7],

– het EU-beleidskader voor cyberdefensie,[8]

– de digitale toekomst van Europa vormgeven[9],

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

---

3 7290/21.
4 10086/18.
5 6122/15 + COR 1.
6 10474/17.
7 8396/21.
8 15585/14.
9 8711/20.

– de gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU[10],

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

1. WIJST OP het grote belang van cyberbeveiliging voor de opbouw van een weerbaar, digitaal en groen Europa. ONDERSTREEPT dat cyberbeveiliging onontbeerlijk is voor de welvaart en de veiligheid van de EU en haar lidstaten, burgers, bedrijven en instellingen, alsmede voor de instandhouding van de integriteit van onze vrije en democratische samenlevingen.

2. IS ZICH BEWUST van het grensoverschrijdende en sectoroverschrijdende karakter van veel cyberdreigingen, alsmede van de risico's en mogelijke gevolgen van alle impactvollere, verfijndere, doelgerichtere, complexere, aanhoudende en/of wijdverbreide kwaadwillige cybercampagnes[12]. De COVID-19-pandemie heeft nog eens extra aangetoond hoezeer onze samenlevingen kwetsbaar zijn, en ook hoezeer onze economie, democratie, essentiële diensten en kritieke infrastructuur - vooral ook in de gezondheidszorg - vatbaar voor schadelijke cyberincidenten op grote schaal zijn. Voorts heeft de pandemie connectiviteit belangrijker gemaakt en de afhankelijkheid van de samenleving van deugdelijke, betrouwbare en veilige netwerk- en informatiesystemen vergroot. Al met al is duidelijk geworden dat we een wereldwijd, open, vrij, stabiel en veilig internet nodig hebben, dat we moeten kunnen vertrouwen op ICT-producten, -processen en -diensten en de beveiliging daarvan, en dat bijvoorbeeld toeleveringsketens daartoe veerkrachtig moeten zijn.

---

10 14435/17 + COR 1.
11 7737/19.
12 ENISA Threat Landscape 2020.

3. WIJST ANDERMAAL op het belang van cyberweerbaarheid en verdere uitbouw van het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging[13] ten behoeve van een efficiënte en tijdige respons op EU-niveau op grootschalige cyberincidenten en -crises, alsmede op het belang van verdere integratie van dat kader in bestaande horizontale en sectorale EU-crisisresponsmechanismen. ONDERSTREEPT de rol van de Raad en de geïntegreerde regeling politieke crisisrespons bij het verzorgen van tijdige crisiscoördinatie en -respons op het politieke niveau van de Unie, ongeacht of zo'n crisis met verstrekkende gevolgen of politieke betekenis nu binnen of buiten de Unie is ontstaan. ACHT het van groot belang dat dergelijke kaders en mechanismen regelmatig getest worden middels oefeningen.

4. BRENGT IN HERINNERING dat activiteiten op EU-niveau wat betreft grootschalige cyberincidenten en -crises gevoerd worden in overeenstemming met de beginselen van subsidiariteit, evenredigheid, complementariteit, voorkoming van dubbel werk, en vertrouwelijkheid. HERHAALT dat in de eerste plaats de lidstaten zelf verantwoordelijk zijn voor de respons op de grootschalige cyberincidenten en -crises die hen treffen. ACHT het van groot belang dat overeenkomstig artikel 4, lid 2, van het Verdrag betreffende de Europese Unie, de bevoegdheden van de lidstaten en hun exclusieve verantwoordelijkheid voor nationale veiligheid op onder meer het gebied van cyberbeveiliging geëerbiedigd worden.

5. ACHT het tevens van groot belang dat ook de bevoegdheden en mandaten van de instellingen, organen en agentschappen van de EU geëerbiedigd worden. Op grond van het Unierecht is er tevens een essentiële rol weggelegd voor de hoge vertegenwoordiger, de Commissie en andere EU-instellingen, -organen en -agentschappen, onder meer gezien de mogelijke impact van grootschalige cyberincidenten en -crises op de eengemaakte markt en op het functioneren van de instellingen, organen en agentschappen van de EU zelf.

[13] 10086/18.

6. ONDERSTREEPT dat onnodig dubbel werk moet worden vermeden en dat bij de verdere ontwikkeling van het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging gestreefd moet worden naar complementariteit en toegevoegde waarde, alsmede dat het geheel moet worden afgestemd op bestaande mechanismen, initiatieven, netwerken, processen en procedures op nationaal en Europees niveau. BENADRUKT dat bestaande processen en structuren gestroomlijnd moeten worden om de complexiteit te verminderen en om in het belang van de cohesie in de Unie de toegankelijkheid en het reactievermogen ten aanzien van degenen die om hulp en solidariteit vragen, te verbeteren.

7. ERKENT de toepasselijkheid van het internationaal recht, waaronder het volledige Handvest van de Verenigde Naties, het internationaal humanitair recht en het mensenrechtenrecht, in de cyberruimte, en SPOORT AAN tot naleving van de vrijwillige, door alle VN-lidstaten onderschreven, niet-bindende normen, regels en beginselen van verantwoordelijk gedrag van staten in de cyberruimte.

8. Is INGENOMEN met de vooruitgang van de afgelopen jaren binnen de Raad, met name in de Horizontale Groep cybervraagstukken (HWPCI) en andere werkgroepen van de Raad ter zake, en met de vooruitgang bij het opzetten van andersoortige samenwerkings- en informatie-uitwisselingsinitiatieven, netwerken en mechanismen tussen de lidstaten, en dan met name de NIS-samenwerkingsgroep en het bij Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 opgerichte CSIRT-netwerk, het netwerk van verbindingsorganisaties voor cybercrises (CyCLONe), alsmede de desbetreffende cyberdefensiegerelateerde projecten in het kader van de permanente gestructureerde samenwerking (PESCO)[14], de Taskforce voor gezamenlijke actie op het gebied van cybercriminaliteit (J-CAT), het Europees justitieel netwerk cybercriminaliteit (EJCN), de vrijwillige bijdragen van de lidstaten aan het EU-Intcen, alsmede met de coördinatie en samenwerking binnen de context van het instrumentarium voor cyberdiplomatie.

---

[14] Met name de door Litouwen gecoördineerde "snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging", het door Duitsland gecoördineerde "coördinatiecentrum voor het cyber- en informatiedomein", en het door Griekenland gecoördineerde "platform voor het delen van informatie over cyberdreigingen en respons op incidenten".

9. HERINNERT AAN de bestaande kaders voor samenwerking tussen EU-instellingen, -organen en -agentschappen, zoals de gestructureerde samenwerking tussen Enisa en CERT-EU, alsmede aan het memorandum van overeenstemming tussen Enisa, het Europees Defensieagentschap (EDA), het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol (EC3) en CERT-EU. BENADRUKT dat het belangrijk is regelmatig informatie te blijven uitwisselen met de Raad over verdere ontwikkelingen in deze samenwerkingskaders.

10. ONDERSTREEPT hoe belangrijk het is dat de samenwerking en informatie-uitwisseling tussen de verschillende cybergemeenschappen in de EU en haar lidstaten op alle noodzakelijke niveaus – technisch, operationeel en strategisch/politiek – worden versterkt en dat bestaande mechanismen, netwerken, structuren, processen en procedures voor crisisbeheersing worden gekoppeld waar dit de aanpak van grootschalige cyberincidenten en -crises ondersteunt en verbetert.

11. ONDERKENT de vooruitgang die een groep lidstaten heeft geboekt bij de oprichting van een gezamenlijk operationeel cybervermogen "snellereactieteams bij cyberincidenten" in het kader van de PESCO, dat tot doel heeft de vrijwillige samenwerking op cybergebied te verdiepen door middel van wederzijdse bijstand, onder meer in reactie op grootschalige cyberincidenten en -crises.

12. ONDERKENT de ervaring en de 24/7-responscapaciteit van de rechtshandhavings-gemeenschap op het gebied van operationele samenwerking en veilige informatie-uitwisseling in de strijd tegen grote grensoverschrijdende cyberaanvallen door middel van het protocol crisisrespons van de EU-rechtshandhavingsinstanties.

13. WAARDEERT de voortgezette uitvoering van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("instrumentarium voor cyberdiplomatie"). HERINNERT ERAAN dat het elke lidstaat vrij staat per geval zijn eigen soevereine beslissing over het toeschrijven van een kwaadwillige cyberactiviteit te nemen. HERINNERT ERAAN dat de maatregelen die worden genomen in het kader van een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten gebaseerd moeten zijn op een gedeeld situationeel bewustzijn waarover de lidstaten overeenstemming hebben bereikt. EU-Intcen speelt een belangrijke rol als centrum voor het creëren van situationeel bewustzijn en voor de dreigingsevaluatie inzake cyberkwesties voor de EU, op basis van vrijwillige inlichtingenbijdragen van de lidstaten en zonder afbreuk te doen aan hun bevoegdheden.

14. HERHAALT het belang van wederzijdse bijstand en solidariteit, overeenkomstig artikel 42, lid 7, van het Verdrag betreffende de Europese Unie en artikel 222 van het Verdrag betreffende de werking van de Europese Unie, en ROEPT OP tot verdere oefeningen met een cyberdimensie. HERINNERT ERAAN dat moet worden nagedacht over de koppeling tussen het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging, het instrumentarium voor cyberdiplomatie en de bepalingen van bovengenoemde artikelen in geval van grootschalige cyberincidenten of -crises. HERINNERT ER voorts AAN dat de verplichtingen voor de lidstaten op grond van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie geen afbreuk doen aan het specifieke karakter van het veiligheids- en defensiebeleid van bepaalde lidstaten. HERINNERT ER tevens AAN dat de NAVO het fundament blijft van de collectieve defensie van de staten die er lid van zijn.

15. ONDERKENT de samenwerking tussen de EU en de NAVO op het gebied van cyber-veiligheid en -defensie, met inbegrip van informatie-uitwisseling tussen CERT-EU en de responscapaciteit voor computerincidenten van de NAVO (NCIRC), met volledige inachtneming van de beginselen van transparantie, wederkerigheid en inclusiviteit, alsook van de besluitvormingsautonomie van beide organisaties.

16. ONDERKENT het belang van samenwerking, waar passend, met de particuliere sector op het gebied van informatie-uitwisselingsoefeningen en het verstrekken van relevante expertise, alsook van betrouwbare oplossingen en diensten, onder meer bij het ondersteunen van de respons op incidenten en het versterken van het situationeel bewustzijn tussen verschillende cybergemeenschappen.

17. BENADRUKT het belang van veilige communicatiekanalen voor de uitwisseling van gerubriceerde en gevoelige informatie. WIJST OP de noodzaak van verdere vooruitgang.

In dit verband en rekening houdend met het bovenstaande,

18. NEEMT NOTA VAN de aanbeveling van de Commissie betreffende de opbouw van een gezamenlijke cybereenheid, als een initiatief dat in overweging moet worden genomen bij de verdere ontwikkeling van het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging[15].

19. VERZOEKT de EU en haar lidstaten zich te blijven inzetten voor een uitgebreider en doeltreffender EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging, voortbouwend op bestaande mechanismen en de reeds geboekte vooruitgang, en rekening te houden met het potentieel van het initiatief voor een gezamenlijke cybereenheid om deze mechanismen stapsgewijs aan te vullen. BENADRUKT dat een incrementeel, transparant en inclusief proces van essentieel belang is voor het vergroten van het vertrouwen en derhalve van cruciaal belang is voor de verdere ontwikkeling van een EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging. Bij dit proces moet rekening worden gehouden met de bestaande rollen, bevoegdheden en mandaten van de lidstaten en de EU-instellingen, -organen en -agentschappen, alsook met de in deze conclusies vermelde beginselen, waaronder evenredigheid, subsidiariteit, inclusiviteit, complementariteit, voorkoming van dubbel werk en vertrouwelijkheid van informatie. BENADRUKT tegelijkertijd dat eventuele deelname aan of bijdragen van lidstaten aan een mogelijke gezamenlijke cybereenheid van vrijwillige aard zijn.

---

[15] C(2021)4520 final (11155/21 en 11155/21 ADD1).

20. ONDERSTREEPT dat passende werkmethoden en governance moeten worden vastgesteld, zodat alle lidstaten kunnen worden betrokken bij en deelnemen aan de beraadslagingen, de ontwikkeling en de doeltreffende besluitvormingsprocessen inzake het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging, met inbegrip van het mogelijke initiatief voor een gezamenlijke cybereenheid. DRINGT EROP AAN dat de prerogatieven van de Raad uit hoofde van de Verdragen en het beginsel van loyale samenwerking worden geëerbiedigd.

21. WIJST OP het belang van het in kaart brengen en betrekken van alle relevante cybergemeenschappen binnen de EU en haar lidstaten, rekening houdend met hun verschillende rollen en verantwoordelijkheden in verschillende soorten grootschalige cyberincidenten en -crises. ONDERSTREEPT de belangrijke rol van de Raad, met name via de Horizontale Groep cybervraagstukken, in de beleidsvorming en de coördinatie voor de verdere ontwikkeling van het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging. VERZOEKT derhalve de lidstaten, de Commissie, de Europese Dienst voor extern optreden (EDEO), EU-Intcen, CERT-EU, Enisa, Europol (EC3), Eurojust (EJCN), het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (ECCC), en ook vertegenwoordigers van het CSIRT-netwerk, CyCLONe, de NIS-samenwerkingsgroep, het EDA en relevante PESCO-projecten, alsook andere mogelijke belanghebbenden, zich bij dit proces aan te sluiten. Een mogelijke werkgroep, zoals voorgesteld in de aanbeveling van de Commissie, zou als tijdelijk forum waarin vertegenwoordigers van alle relevante cybergemeenschappen in de lidstaten en binnen de EU bijeenkomen, verder kunnen worden onderzocht, waarbij wordt gezorgd voor een adequate vertegenwoordiging van alle lidstaten en politieke aansturing door de Raad. Die werkgroep dient regelmatig verslag uit te brengen over haar activiteiten en mogelijke suggesties voor bespreking, goedkeuring en verdere sturing aan de Raad voor te leggen. Daarnaast kunnen binnen en tussen gemeenschappen andere vormen van dialoog tot stand worden gebracht, onder meer via workshops, seminars, gezamenlijke opleidingen en oefeningen.

22. ONDERSTREEPT de rol van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (ECCC) en het netwerk van nationale coördinatiecentra met betrekking tot de potentiële gezamenlijke cybereenheid, met name gezien de rol ervan om de technologische capaciteiten, technologische oplossingen, capaciteiten en vaardigheden van de Unie op het gebied van cyberbeveiliging aanzienlijk te vergroten.

23. VERZOEKT de EU en haar lidstaten zich in te zetten voor de verdere ontwikkeling van het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging, onder meer door het potentieel van een initiatief voor een gezamenlijke cybereenheid te verkennen, door het proces vast te stellen en te definiëren, met inbegrip van mijlpalen en een tijdschema, en door de doelstellingen en mogelijke taken en verantwoordelijkheden te verduidelijken. BENADRUKT dat prioriteit moet worden gegeven aan het consolideren van bestaande netwerken en interacties binnen elke gemeenschap, alsook aan het opstellen van een grondig overzicht van mogelijke lacunes en behoeften op het gebied van informatie-uitwisseling binnen en tussen cybergemeenschappen en ook binnen en tussen Europese instellingen, organen en agentschappen, en dat vervolgens overeenstemming moet worden bereikt over mogelijke primaire doelstellingen en prioriteiten van een mogelijke gezamenlijke cybereenheid. ONDERSTREEPT, zonder vooruit te lopen op het resultaat, dat de aandacht moet worden toegespitst op het in kaart brengen van de behoeften op het gebied van informatie-uitwisseling, teneinde een gemeenschappelijk situationeel bewustzijn onder alle betrokken gemeenschappen te creëren. Bij het vaststellen van lacunes en behoeften op het gebied van informatie-uitwisseling, met inbegrip van het mogelijke gebruik van virtuele platforms, moet de nodige aandacht blijven uitgaan naar veilige communicatiekanalen voor de uitwisseling van gerubriceerde en gevoelige informatie, waarbij WORDT GEWEZEN OP het belang van het gebruik van reeds bestaande infrastructuur. De invoering van een geleidelijke aanpak is bedoeld om vertrouwen op te bouwen en de basis te leggen voor mogelijke verdere stappen met het oog op het verbeteren van de paraatheid en de operationele samenwerking. ONDERKENT dat verschillende doelstellingen verschillende oplossingen en de betrokkenheid van verschillende groepen vertegenwoordigers van relevante cyber-gemeenschappen binnen de EU en haar lidstaten kunnen rechtvaardigen.

24. VRAAGT dat tijdens het gehele proces verder wordt nagedacht over een rechtsgrondslag voor de mogelijke gezamenlijke cybereenheid, met inbegrip van een beoordeling van de taken en rollen ten opzichte van de taken en rollen die aan Enisa zijn toegewezen in het kader van de aanbeveling op basis van artikel 7 van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019. DRINGT AAN OP verdere reflectie over afzonderlijke elementen van de aanbeveling inzake de gezamenlijke cybereenheid, onder meer wat betreft het idee van de snellereactieteams voor cyberbeveiliging van de EU, en het responsplan voor incidenten en crises inzake cyberbeveiliging van de EU. BENADRUKT dat een mogelijke gezamenlijke cybereenheid de competenties, mandaten en wettelijke bevoegdheden van haar mogelijke toekomstige deelnemers moet eerbiedigen.

25. VERZOEKT de EU en haar lidstaten na te denken over het potentieel van een initiatief voor een gezamenlijke cybereenheid, ook vanuit het perspectief van de instellingen, organen en agentschappen van de EU, als aanvulling op de lopende inspanningen op het niveau van de lidstaten. IS INGENOMEN MET het voornemen van de Commissie om de weerbaarheid van de bevoegde EU-instellingen, -organen en -agentschappen te versterken door middel van haar komende voorstel voor een verordening betreffende gemeenschappelijke bindende voorschriften inzake cyberbeveiliging voor EU-instellingen, -organen en -agentschappen.

26. HERHAALT tot slot zijn toezegging om de cyberweerbaarheid te vergroten en het EU-kader voor crisisbeheersing op het gebied van cyberbeveiliging verder te ontwikkelen, en ZAL REGELMATIG TOEZIEN OP de vorderingen en verdere richtsnoeren verstrekken ter aanvulling van dit EU-kader.