Raad van de
Europese Unie

Brussel, 20 maart 2019
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	19 maart 2019
aan:	de delegaties
nr. vorig doc.:	6866/19
Betreft:	Conclusies van de Raad over het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU

Voor de delegaties gaan in de bijlage de conclusies van de Raad over het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU, die door de Raad Algemene Zaken van 19 maart 2019 zijn aangenomen.

BIJLAGE

Conclusies van de Raad over het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU

De Raad van de Europese Unie,

1. HERINNEREND AAN zijn conclusies over "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU"[1];

2. HERINNEREND AAN zijn ontwerpconclusies over een gecoördineerde EU-respons op grootschalige cyberincidenten en -crises[2];

3. HERINNEREND AAN zijn conclusies over het opbouwen van externe cybercapaciteit[3];

4. HERHALEND dat een hoge beveiliging van netwerk- en informatiesystemen kan worden bereikt door de capaciteit en de vermogens inzake cyberbeveiliging van de lidstaten en de EU-instellingen, -organen en -instanties te verbeteren, en door vervolgens hun cyberweerbaarheid te versterken;

5. VERHEUGD OVER de vooruitgang die de lidstaten hebben geboekt bij het versterken van de Computer Security Incident Response Teams (CSIRT's);

6. ZIJN WAARDERING UITSPREKEND VOOR de oprichting van het CSIRT-netwerk door de lidstaten met de actieve steun van de Commissie en Enisa, alsmede voor de versterkte samenwerking op strategisch niveau door middel van de NIS-samenwerkingsgroep, bestaande uit de lidstaten, de Commissie en Enisa;

---

1 Doc. 14435/17 (Conclusies van de Raad over de gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" van 20 november 2017)

2 Doc. 10086/18 (Conclusies over een gecoördineerde EU-respons op grootschalige cyberincidenten en -crises van 26 juni 2018)

3 Doc. 10496/18 (Conclusies van de Raad over richtsnoeren voor het opbouwen van externe cybercapaciteit van de EU van 26 juni 2018)

7. De belangrijke rol BENADRUKKEND van de NIS-samenwerkingsgroep in het bieden van de nodige sturing om de aanpak bij de omzetting van de NIS-richtlijn[4] zoveel mogelijk onderling af te stemmen in de hele EU, en in het aanpakken van relevante kwesties inzake cyberbeveiliging;

8. ONDERKENNEND dat de Commissie reeds steun biedt aan de lidstaten voor de capaciteits-opbouw van de CSIRT's via de Connecting Europe Facility;

9. ONDERKENNEND dat via het Fonds voor interne veiligheid en Cepol ondersteuning wordt geboden aan rechtshandhavingsinstanties voor capaciteitsopbouw in de strijd tegen cybercriminaliteit ;

10. INGENOMEN MET de actualisering van het EU-beleidskader voor cyberdefensie om verdere steun te bieden aan de ontwikkeling van de cyberdefensievermogens van de lidstaten;

11. ZIJN WAARDERING UITSPREKEND VOOR de vooruitgang die is geboekt bij de uitvoering van de NIS-richtlijn door de lidstaten;

12. CONSTATEREND dat cyberbeveiliging een complex, onderling afhankelijk en voortdurend veranderend domein is waarvoor het politieke en juridische kader moet worden aangepast in het licht van nieuwe technologische ontwikkelingen en opkomende technologieën, zoals kunstmatige intelligentie, blockchain en quantumcomputing;

---

[4] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

13. BENADRUKKEND dat onderwijs- en opleidingsprogramma's in verband met cyberbeveiliging en op eindgebruikers gerichte voorlichtings- en bewustmakingscampagnes over veiligheidsdreigingen van cruciaal belang zijn om de cyberveiligheidsrisico's te verminderen;

14. ONDERSTREPEND dat cyberoefeningen effectieve hulpmiddelen zijn voor de evaluatie en de verdere verbetering van de paraatheid van de EU en haar lidstaten voor de bestrijding van grootschalige cyberincidenten en -crises;

15. HERHALEND dat de cyberruimte geen grenzen heeft, hetgeen betekent dat grens- en sectoroverschrijdende perspectieven en samenwerking vaste beginselen zijn bij activiteiten en initiatieven in verband met de opbouw van cybercapaciteit;

16. Het belang BENADRUKKEND van samenwerking tussen de publieke sector, de private sector en de academische wereld, met name door middel van samenwerkingsprojecten;

17. Het belang BENADRUKKEND van civiel-militaire samenwerking, waarbij gemeenschappelijke doelen op cybergebied nagestreefd worden om tot een coherente en doeltreffende respons op cyberdreigingen te komen;

18. NEEMT NOTA VAN de vooruitgang die is geboekt door een groep van lidstaten bij het ontwikkelen van snellereactieteams bij cyberincidenten ter verdieping van de vrijwillige samenwerking op cybergebied via wederzijdse bijstand;

19. IS VERHEUGD OVER de lopende besprekingen in de Raad over het Commissievoorstel voor een verordening van het Europees Parlement en de Raad tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra;

20. PLEIT VOOR een actieve deelname aan de lopende werkzaamheden van de NIS-samenwerkingsgroep, met name met betrekking tot opbouw van cybercapaciteit;

21. MOEDIGT de lopende werkzaamheden AAN van de NIS-samenwerkingsgroep over een gecoördineerde EU-respons op grootschalige cyberincidenten en -crises;

22. VERZOEKT de lidstaten om voort te bouwen op hun nationale strategieën inzake cyberbeveiliging en om cyberbeveiliging te mainstreamen, rekening houdend met sectorspecifieke vereisten;

23. VERZOEKT de lidstaten om te zorgen voor voortdurend toezicht op en evaluatie/beoordeling van het effect van maatregelen om de cyberweerbaarheid en cyberbeveiliging te versterken en de cybervermogens en -capaciteiten op nationaal niveau te vergroten;

24. VERZOEKT de lidstaten om cyberbeveiliging en digitale geletterdheid te integreren in onderwijsprogramma's op alle onderwijsniveaus (basis-, middelbaar en hoger onderwijs, een leven lang leren) in voorkomend geval gebaseerd op bestaande en toekomstige beroepsprofielen;

25. VERZOEKT de lidstaten om initiatieven voor bewustmaking inzake cyberbeveiliging en inzake cyberhygiëne voor het publiek en de eindgebruikers uit te voeren, gericht op werknemers in de publieke sector;

26. SPOORT de lidstaten ERTOE AAN op nationaal niveau oefeningen op het gebied van cyberbeveiliging te houden en zulke oefeningen ook op EU-niveau te houden en/of eraan deel te nemen teneinde te testen en te trainen voor strategische en technologische aspecten, en effectief en op praktisch niveau de nodige vaardigheden te ontwikkelen;

27. VERZOEKT de lidstaten om de technische en operationele vermogens op het gebied van cyberbeveiliging van hun CSIRT's verder te ontwikkelen met het oog op incidentpreventie, schadebeperking en reactie op incidenten;

28. DRINGT ER bij de Commissie en Enisa OP AAN verder steun te verlenen voor het ontwikkelen van de capaciteit en het vermogen van het netwerk van CSIRT's door lidstaten teneinde beter samen te werken, informatie over incidenten uit te wisselen en efficiënt te reageren op grootschalige grensoverschrijdende incidenten;

29. VERZOEKT de lidstaten de rechtshandhavingsinstanties verder te helpen bij het ontwikkelen van specifieke competenties, in ruggespraak met de bevoegde Europese autoriteiten, met het oog op een effectieve bestrijding op EU-niveau van cybercriminaliteit;

30. VERZOEKT de lidstaten meer te investeren in cybercapaciteitsopbouw;

31. DRINGT ER bij de Commissie en Enisa OP AAN programma's ter bewustmaking van cyberbeveiliging uit te voeren en opleiding te verstrekken, specifiek gericht op aan werknemers van de EU-instellingen, -organen en -instanties;

32. DRINGT ER bij de EU en haar lidstaten OP AAN op vrijwillige basis informatie en beste praktijken uit te wisselen, om bij te dragen tot het in kaart brengen en aanpakken van de belangrijkste behoeften inzake cybercapaciteitsopbouw op nationaal en EU-niveau;

33. VERZOEKT de EU en haar lidstaten steun te verlenen voor onderzoek naar cyberbeveiliging, en cyberbeveiliging te bevorderen als thema op andere studiegebieden, en zodoende de verschillende takken van onderzoek en ontwikkeling op het gebied van cyberbeveiliging samen te brengen in een geïntegreerd geheel, en onderzoek van topkwaliteit naar cyberbeveiliging te bevorderen;

34. VERZOEKT de EU en haar lidstaten om onderzoek op het gebied van cyberbeveiliging te doen dat beantwoordt aan de behoeften van de samenleving en de onderzoeksresultaten in de markt integreert;

35. DRINGT ER bij de EU en haar lidstaten OP AAN cyberbeveiliging in voorkomend geval in aanmerking te nemen bij ICT-aanbestedingen.