Raad van de
Europese Unie

Brussel, 20 november 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	20 november 2017
aan:	de delegaties
nr. vorig doc.:	13943/17 + COR 1
Nr. Comdoc.:	12210/17, 12211/17
Betreft:	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 - Conclusies van de Raad (20 november 2017)

Voor de delegaties gaan hierbij de 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", die de Raad Algemene Zaken op 20 november 2017 heeft aangenomen.

BIJLAGE

Ontwerpconclusies 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"

De Raad van de Europese Unie,

1. ZICH BEWUST VAN het belang van cyberbeveiliging voor de welvaart, groei en veiligheid van de EU en de integriteit van onze vrije en democratische samenlevingen en de daaraan ten grondslag liggende processen in het digitale tijdperk, omdat die zowel de rechtsstaat als de mensenrechten en de fundamentele vrijheden van eenieder beschermt;

2. WIJZEND OP de noodzaak van een samenhangende aanpak van cyberbeveiliging op nationaal, EU- en mondiaal niveau, aangezien cyberdreigingen onze democratie, welvaart, stabiliteit en veiligheid in gevaar kunnen brengen;

3. EROP WIJZEND dat een hoog niveau van cyberweerbaarheid in de EU tevens van groot belang is voor het kweken van vertrouwen in de digitale eengemaakte markt en de verdere ontwikkeling van een digitaal Europa;

4. BEVESTIGEND dat de EU zich zal blijven inzetten voor een open, mondiale, vrije, vreedzame en veilige cyberruimte, waarin de mensenrechten en fundamentele vrijheden – met name de vrijheid van meningsuiting, de toegang tot informatie, gegevensbescherming, privacy en veiligheid – en de kernwaarden en -beginselen van de EU zowel binnen de EU als wereldwijd volledig worden toegepast en geëerbiedigd, en BEKLEMTONEND dat het cruciaal is om een juist evenwicht te waarborgen tussen de mensenrechten en de fundamentele vrijheden enerzijds, en de randvoorwaarden van het interneveiligheidsbeleid van de EU anderzijds[1];

5. ZICH ERVAN BEWUST dat het internationale recht, met inbegrip van het volledige VN-Handvest, het internationale humanitaire recht en het recht inzake de mensenrechten van toepassing zijn in de cyberruimte en aldus het belang ONDERSTREPEND van het voortzetten van de inspanningen die de eerbiediging van het internationale recht in de cyberruimte moeten garanderen;

---

[1] Doc. 12650/17.

6. INDACHTIG zijn conclusies over de EU-strategie inzake cyberbeveiliging[2], internet-governance[3], versterking van het Europese cyberweerbaarheidssysteem[4], cyberdiplomatie[5], een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten[6], verbetering van de strafrechtspleging in de cyberruimte[7], veiligheid en defensie in het kader van de integrale EU-strategie[8], het gezamenlijk kader voor de bestrijding van hybride bedreigingen[9], en de tussentijdse evaluatie van de vernieuwde interneveiligheidsstrategie voor de Europese Unie 2015-2020[10];

7. ERKENNENDE dat het kader van het Verdrag inzake cybercriminaliteit van de Raad van Europa (Verdrag van Boedapest) een solide basis vormt voor het gebruik, door een heterogene groep landen, van één doeltreffende wettelijke norm voor verschillende nationale wetgevingen en voor internationale samenwerking ter bestrijding van cybercriminaliteit;

8. ONDERKENNEND dat er hernieuwde aandacht moet komen voor de uitvoering van het EU-beleidskader voor cyberdefensie van 2014, dat geactualiseerd moet worden zodat cyberbeveiliging en -defensie beter geïntegreerd kunnen worden in het gemeenschappelijk veiligheids- en defensie-beleid (GVDB) en de bredere veiligheids- en defensieagenda;

9. ZICH ERVAN BEWUST dat een mondiaal concurrerende Europese industrie een belangrijk element is voor de verwezenlijking van een hoog niveau van cyberbeveiliging, zowel op nationaal niveau als in de hele EU;

10. ERAAN HERINNEREND dat nationale veiligheid volgens artikel 4, lid 2, VEU de uitsluitende verantwoordelijkheid van elke lidstaat blijft.

---

2 Doc. 12109/13 en 6225/13 (gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace (COM JOIN(2013) 1 final).

3 Doc. 16200/14 en 6460/14 (mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Internetbeleid en -governance - De rol van Europa bij het vormgeven van de toekomst van internetgovernance (COM(2014) 72 final)).

4 Doc. 14540/16 en 11013/16 (mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Versterken van het Europese cyberbeveiligings-systeem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche (COM(2016) 410 final)).

5 Doc. 6122/15.

6 Doc. 9916/17.

7 Doc. 10007/16.

8 Doc. 9178/17.

9 Doc. 7688/16 (Gezamenlijke mededeling aan het Europees Parlement en de Raad: Gezamenlijk kader voor de bestrijding van hybride bedreigingen: een reactie van de Europese Unie).

10 Doc. 12650/17.

VERKLAART HET VOLGENDE:

11. IS INGENOMEN met de gezamenlijke mededeling aan het Europees Parlement en de Raad "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU", waarin een ambitieuze doelstelling wordt gepresenteerd, namelijk het verbeteren van de cyberbeveiliging in de EU. De mededeling is tevens bevorderlijk voor de strategische autonomie van de EU waarnaar wordt verwezen in de conclusies over de integrale strategie voor het buitenlands en veiligheids-beleid van de Europese Unie[11] doordat ze streeft naar het opbouwen van een digitaal Europa dat veiliger is, vertrouwen kweekt, zich bewust is van zijn sterke kanten, concurrerend is, openstaat voor de wereld en de gedeelde waarden van de EU met betrekking tot een open, vrij, vreedzaam en veilig mondiaal internet eerbiedigt, en zo een hoger niveau van weerbaarheid bewerkstelligt voor het voorkomen, ontmoedigen en opsporen van en reageren op cyberdreigingen, en het gezamenlijk reageren op cyberdreigingen in de hele EU; en

12. VERZOEKT de lidstaten en de instellingen, instanties en organen van de EU om, onder eerbiediging van elkaars bevoegdheden en de beginselen subsidiariteit en evenredigheid, samen te werken om de in deze conclusies vervatte strategische doelstellingen te verwezenlijken, en

13. ONDERSTREEPT dat de EU, de lidstaten en de particuliere sector, met inachtneming van de beschikbare middelen, voor voldoende financiering moeten zorgen om zowel ondersteuning te bieden aan de verbetering van de cyberweerbaarheid als aan onderzoeks- en ontwikkelings-inspanningen in de EU op het gebied van cyberbeveiliging, om samenwerking te intensiveren voor het voorkomen, ontmoedigen en opsporen van en reageren op cyberdreigingen, en het gezamenlijk reageren op grootschalige cyberincidenten en kwaadwillige cyberaanvallen in de EU;

---

[11] Doc. 13202/16.

Hoofdstuk I

ZORGEN VOOR EEN DOELTREFFENDE CYBERWEERBAARHEID VAN DE EU EN VERTROUWEN IN DE DIGITALE EENGEMAAKTE MARKT

14. ONDERSTREEPT dat elke lidstaat in de eerste plaats de verantwoordelijkheid draagt om zijn eigen cyberbeveiliging te versterken en te reageren op cyberincidenten en -crises, terwijl de EU een grote meerwaarde kan bieden bij het ondersteunen van de samenwerking tussen de lidstaten. BENADRUKT in dit verband dat alle lidstaten aan de voor cyberbeveiliging bevoegde nationale autoriteiten de nodige middelen ter beschikking moeten stellen voor het voorkomen en opsporen van en reageren op cyberincidenten en -crises in de hele EU;

15. ONDERSTREEPT de noodzaak om waar mogelijk gebruik te maken van bestaande mechanismen, structuren en organisaties op EU-niveau;

16. PRIJST:

- de vooruitgang die de lidstaten hebben geboekt bij de omzetting van de NIS-richtlijn en BEKLEMTOONT de noodzaak van een volledige en doeltreffende uitvoering uiterlijk in mei 2018, zoals in de genoemde richtlijn is aangegeven[12];
- de werkzaamheden in het kader van de NIS-samenwerkingsgroep ter versterking van de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten;
- de werkzaamheden binnen het CSIRT-netwerk, in het bijzonder ter versterking van de operationele samenwerking tussen lidstaten, het opbouwen van geloof en vertrouwen in het uitwisselen van informatie bij het omgaan met grootschalige incidenten op het gebied van cyberbeveiliging en in het aanreiken van elementen voor een gedeeld situationeel bewustzijn op Europees niveau, op basis van nationale conclusies van de lidstaten;
- de werkzaamheden in het kader van de contractuele publiek-private samenwerking voor cyberbeveiliging (cPPP).

[12] Dit doet geen afbreuk aan de bevoegdheid van de lidstaten voor de omzetting van de NIS-richtlijn, in het bijzonder met betrekking tot de aanbieders van essentiële diensten.

17. IS INGENOMEN MET de bevestiging in de gezamenlijke mededeling dat sterke en betrouwbare encryptie uiterst belangrijk is voor het naar behoren waarborgen van de mensenrechten en de fundamentele vrijheden in de EU en voor het publieke vertrouwen in de digitale eengemaakte markt, er evenwel rekening mee houdend dat de rechtshandhavingsautoriteiten toegang moeten hebben tot gegevens die nodig zijn voor hun onderzoek, en met de bevestiging dat veilige digitale identificatie en communicatie beide van wezenlijk belang zijn voor een doeltreffende cyber-beveiliging in de EU;

18. IS VERHEUGD OVER het in de gezamenlijke mededeling aangehaalde plan om naar een hoger ambitieniveau over te schakelen in het geregeld verrichten van de pan-Europese oefeningen inzake cyberbeveiliging, voortbouwend op de ervaringen met de "Cyber Europe"-oefeningen, waarbij de respons op verschillende niveaus wordt gecombineerd, aangezien dit een belangrijk element zal zijn in het verbeteren van de paraatheid van de lidstaten en de EU-instellingen om op grootschalige cyberincidenten te reageren;

19. ROEPT de EU en haar lidstaten op geregeld strategische oefeningen op het gebied van cyberbeveiliging te houden in verschillende Raadsformaties, voortbouwend op de ervaring die is opgedaan tijdens EU CYBRID 2017, en

20. Onverminderd het resultaat van het wetgevingsproces:

- IS INGENOMEN MET het voorstel voor een sterk en permanent mandaat voor Enisa, met als voornaamste doelstelling de ondersteuning en ontwikkeling van een nauwere samenwerking tussen de lidstaten, teneinde hun capaciteit te vergroten en het vertrouwen in een digitaal Europa te versterken;

- HERBEVESTIGT dat het toekomstige Enisa moet bouwen op de ervaring en deskundigheid binnen de lidstaten en de EU en de consequente ontwikkeling en tenuitvoerlegging van bestaande en toekomstige beleidsmaatregelen en regelgeving van de EU op het vlak van cyberbeveiliging moet ondersteunen, waarbij ervoor wordt gezorgd dat alle bevoegdheden van Enisa zo worden ontwikkeld dat ze die van de lidstaten aanvullen;

- HERHAALT de doelstelling om het vertrouwen in een digitaal Europa te doen groeien door het geloof en het vertrouwen in digitale oplossingen en innovaties te versterken, waaronder het internet der dingen, e-handel en e-overheid, in het bijzonder in de vorm van een Europees kader van wereldniveau voor cyberbeveiligingscertificering[13]. Dit is een belangrijke voorwaarde om het vertrouwen in en de veiligheid van digitale producten en diensten te vergroten, waarbij kritieke infrastructuren en gegevens van de overheid, van burgers en van ondernemingen worden beschermd, en het is essentieel om te evolueren naar een "beveiliging door ontwerp"-aanpak voor producten, diensten en processen in de digitale eengemaakte markt;

- BEKLEMTOONT dat wetgevingswerkzaamheden ter versterking van de cyber-beveiligingscertificering op EU-niveau zullen moeten tegemoetkomen aan de behoeften van de markt en de gebruikers, voortbouwen op de ervaringen met reeds bestaande certificeringscapaciteiten en -processen in de EU (bijvoorbeeld het SOG-IS-kader) en een kader zouden moeten bieden dat zich snel kan aanpassen aan de laatste stand van toekomstige digitale ontwikkelingen;

- BENADRUKT dat bij het versterken van de cyberbeveiligingscertificering in de EU het hele spectrum van beveiligingsvereisten moet worden bestreken, tot en met de strengste, wanneer bestendigheid tegen de vermogens van aanvallers moet worden aangetoond. Belangrijke succesfactoren zouden zijn: zorgen voor een betrouwbaar, transparant en onafhankelijk proces voor beveiligingscertificering, met het oog op de bevordering van de beschikbaarheid van betrouwbare en beveiligde toestellen, software en diensten binnen de eengemaakte markt en daarbuiten; de respectieve deskundigheid van de Europese industrie, regeringen en evaluatiespecialisten erkennen via Europese en mondiale normen[14]; de rol van de lidstaten in het certificeringsproces respecteren, in het bijzonder wat betreft evaluatie op hogere beveiligingsniveaus, en vooral met betrekking tot de inschatting van essentiële beveiligingsbehoeften en -vaardigheden. Een dergelijk certificeringskader moet er tevens voor zorgen dat een EU-brede certificeringsregeling evenredig is met het zekerheidsniveau dat nodig is voor het gebruik van de betrokken ICT-producten, -diensten en/of -systemen, en grensoverschrijdende handel mogelijk maken voor ondernemingen van elke omvang, met het oog op de ontwikkeling en verkoop van nieuwe producten, zowel binnen de EU als op markten buiten de EU.

---

13 Via mondiale normen die worden ontwikkeld in de geest van de Praktijkrichtlijn van de WTO inzake technische handelsbelemmeringen.

14 Via Europese en mondiale normen die worden ontwikkeld in de geest van de Praktijkrichtlijn van de WTO inzake technische handelsbelemmeringen.

21. IS INGENOMEN MET het voornemen een netwerk van kenniscentra voor cyberbeveiliging op te zetten ter stimulering van de ontwikkeling en de uitrol van cyberbeveiligingstechnologieën en de EU-industrie op mondiaal niveau een bijkomende innovatiestimulans te geven bij de ontwikkeling van baanbrekende en toekomstgerichte technologieën, zoals kunstmatige intelligentie, quantumcomputing, blockchain en beveiligde digitale identiteiten;

22. BENADRUKT dat het netwerk van kenniscentra voor cyberbeveiliging inclusief moet zijn ten aanzien van alle lidstaten en hun bestaande excellentie- en kenniscentra, en dat er bijzondere aandacht dient te worden besteed aan complementariteit, en NEEMT, dit indachtig, NOTA VAN het geplande Europees onderzoeks- en kenniscentrum voor cyberbeveiliging, waarvan de belangrijkste rol zal bestaan in het focussen op complementariteit en het vermijden van overlappingen binnen het netwerk van kenniscentra voor cyberbeveiliging en met andere EU-instanties;

23. BEKLEMTOONT dat het netwerk van kenniscentra voor cyberbeveiliging een scala aan problemen zou moeten behartigen, gaande van het onderzoek tot de industrie, en dat het daarom onder meer de doelstelling van Europese strategische autonomie zou moeten helpen verwezenlijken;

24. HERHAALT, met het oog op het voorgestelde netwerk van kenniscentra voor cyberbeveiliging, dat de EU via haar lidstaten een Europese capaciteit moet ontwikkelen voor het beoordelen van de sterkte van de cryptografie die wordt gebruikt in producten en diensten die beschikbaar zijn voor burgers, ondernemingen en overheden binnen de digitale eengemaakte markt, in het besef dat beleidsmaatregelen inzake cryptografie een belangrijk aspect van de nationale veiligheid vormen en derhalve binnen de bevoegdheid van de lidstaten vallen;

25. VERZOEKT alle betrokken partijen meer te investeren in cyberbeveiligingstoepassingen van nieuwe technologieën, teneinde bij te dragen tot het verzekeren van cyberbeveiliging in alle sectoren van de Europese economie;

26. BENADRUKT het belang van geloofwaardige, betrouwbare en gecoördineerde verlening van cyberbeveiligingsdiensten voor de EU-instellingen en ROEPT de Commissie en andere EU-instellingen OP CERT-EU verder te ontwikkelen overeenkomstig deze doelstellingen en tevens te zorgen voor passende middelen daartoe;

27. IS VERHEUGD OVER de oproep tot erkenning van de belangrijke rol van derden die onderzoek doen naar beveiliging, bij het opsporen van kwetsbaarheden in bestaande producten en diensten en VRAAGT de lidstaten beste praktijken te delen voor de gecoördineerde bekendmaking van kwetsbaarheden;

28. BENADRUKT ieders verantwoordelijkheid inzake cyberbeveiliging en VERZOEKT de EU en haar lidstaten digitale vaardigheden en mediageletterdheid te bevorderen, zodat gebruikers worden geholpen om hun digitale informatie online te beschermen en bewuster worden gemaakt van de risico's die het op internet plaatsen van persoonsgegevens met zich meebrengt;

29. IS VERHEUGD dat in de gezamenlijke mededeling de nadruk wordt gelegd op onderwijs, cyberhygiëne en bewustzijn in de lidstaten en in de EU;

30. VERZOEKT DE COMMISSIE snel een effectbeoordeling te verstrekken en uiterlijk medio 2018 de relevante rechtsinstrumenten voor te stellen met betrekking tot de uitvoering van het initiatief tot instelling van een netwerk van kenniscentra voor cyberbeveiliging en een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging;

31. VERZOEKT de lidstaten:

- prioriteit te verlenen aan informatiecampagnes rond cyberbewustzijn, en cyber-beveiliging te stimuleren als onderdeel van universitaire leerplannen en leerplannen voor onderwijs en beroepsopleiding . De aandacht dient in het bijzonder uit te gaan naar de opleiding van jongeren en het stimuleren van digitale vaardigheden, teneinde toekomstbestendige professionals te vormen die klaar zijn voor de uitdagingen op het gebied van veiligheid, economie en diensten;

- meer inspanningen te doen om gespecialiseerde programma's op hoog niveau inzake cyberbeveiliging te openen, teneinde het huidige tekort aan professionals op het gebied van cyberbeveiliging in de EU weg te werken;

- een doeltreffend samenwerkingsnetwerk te creëren van onderwijscontactpunten in het kader van Enisa. Het doel van dit netwerk van onderwijscontactpunten is een betere coördinatie en uitwisseling van beste praktijken tussen de lidstaten inzake onderwijs en bewustmaking over cyberbeveiliging, alsmede opleiding, oefeningen en capaciteits-opbouw;

- te overwegen de regels van de NIS-richtlijn ook toe te passen op overheidsdiensten die deelnemen aan kritieke maatschappelijke of economische activiteiten, indien die niet reeds gedekt zijn door de nationale wetgeving en waar passend, en ook in overheids-diensten opleiding in verband met cyberbeveiliging aan te bieden, gezien de rol die zij spelen in onze samenleving en economie.

HOOFDSTUK II

OPBOUW VAN EU-CAPACITEIT VOOR HET VOORKOMEN, ONTMOEDIGEN EN OPSPOREN VAN EN REAGEREN OP KWAADWILLIGE CYBERACTIVITEITEN

32. BEKLEMTOONT dat een cyberincident of -crisis van bijzonder ernstige aard voldoende reden kan zijn om een beroep te doen op de solidariteitsclausule van de EU[15] en/of de clausule inzake wederzijdse bijstand[16];

33. IS INGENOMEN MET de goedkeuring van het "kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten" dat bijdraagt tot conflictpreventie, samenwerking en stabiliteit in de cyberruimte door binnen het GBVB maatregelen te nemen, waaronder beperkende maatregelen, die kunnen worden gebruikt ter voorkoming van en om te reageren op kwaadwillige cyberactiviteiten, en ROEPT de EDEO en de lidstaten OP regelmatig oefeningen te verrichten met betrekking tot dat kader;

---

15 Artikel 222 VWEU.
16 Artikel 42, lid 7, VEU.

34. BENADRUKT de noodzaak van een efficiënte EU-respons op grootschalige cyberincidenten en -crises, met inachtneming van de bevoegdheden van de lidstaten, en de behoefte aan opneming van cyberbeveiliging in de bestaande crisisbeheersingsmechanismen op EU-niveau[17]. ROEPT daartoe OP tot een regelmatige EU-respons op grootschalige cyberincidenten - gaande van diplomatiek-strategische reacties tot technische reacties - op basis van de relevante kaders en procedures[18], die zo nodig moeten worden verfijnd;

35. WIJST OP het belang van goed geïntegreerde mechanismen voor reactie en uitwisseling van informatie tussen verschillende gemeenschappen die cruciaal zijn voor het waarborgen van cyberbeveiliging in Europa, en tussen betrokken EU-organen en autoriteiten van de lidstaten. Dergelijke mechanismen moeten worden getest en gecontroleerd als onderdeel van Europabrede cyberbeveiligingsoefeningen, en geformaliseerd via respectieve overeenkomsten, indien nodig;

36. WIJST OP de mogelijkheid van het bestuderen van een eventueel Commissievoorstel voor de oprichting van een cyberbeveiligingsnoodfonds, naast de bestaande inspanningen van de lidstaten en met inachtneming van de beschikbare middelen (met name binnen het meerjarig financieel kader van de EU), om lidstaten te helpen bij het reageren op grootschalige cyberincidenten en het verzachten van de impact ervan, op voorwaarde dat die lidstaten voorafgaand aan het incident een voorzichtig cyberbeveiligingssysteem hebben ingesteld, daaronder begrepen de volledige uitvoering van de NIS-richtlijn en goed ontwikkelde risicobeheersings- en toezichtskaders op nationaal niveau;

37. ERKENT de groeiende connecties tussen cyberbeveiliging en defensie, en ROEPT OP tot intensivering van de samenwerking op het gebied van cyberdefensie, mede door het stimuleren van samenwerking tussen civiele en militaire gemeenschappen die zich bezighouden met de respons op incidenten, en tot verdere versterking van de cyberbeveiliging van GVDB-missies en -operaties;

---

17 C/2017/6100 final.
18 Doc. 9916/17 en C/2017/6100 final.

38. BENADRUKT de noodzaak om zo mogelijk ten volle profijt te trekken van de voorgestelde defensie-initiatieven teneinde de ontwikkeling van adequate cyberbeveiligingsvermogens in Europa te versnellen, ONDERKENT de mogelijkheden van de eventuele ontwikkeling van cyberdefensie-projecten via de PESCO, indien noodzakelijk geacht door de aan de PESCO deelnemende lidstaten, en ERKENT de rol van de Europese industriële en technologische defensiebasis (EDTIB) en van de ruimere civiele cyberbeveiligingssector bij het verschaffen van middelen voor de lidstaten om hun cybergerelateerde veiligheids- en defensiebelangen te vrijwaren;

39. NEEMT KENNIS VAN het voorstel van de Commissie om eind 2018 een opleidings- en onderwijsplatform voor cyberbeveiliging op te richten, en BENADRUKT dat het platform de opleidings- en onderwijskansen in de lidstaten moet opvoeren en moet zorgen voor complementariteit met andere initiatieven en inspanningen van de EU, met name met de EVDA en het EDA;

40. VERZOEKT de EU en haar lidstaten om in te spelen op de dreiging van ICT-gestuurde diefstal van intellectuele eigendom, waaronder bedrijfsgeheimen of andere vertrouwelijke bedrijfsinformatie, met de bedoeling concurrentievoordelen aan bedrijven en commerciële sectoren te verschaffen;

41. ERKENT de noodzaak om criminaliteit in de cyberruimte aan te pakken, met inbegrip van die in het darkweb, seksuele uitbuiting van kinderen online, en fraude met en vervalsing van niet-contante betaalmiddelen, met name door ernaar te streven een beter beeld van de inlichtingen te verkrijgen, gezamenlijke onderzoeken te voeren en operationele steun uit te wisselen;

42. VERWELKOMT de werkzaamheden die de EU en haar lidstaten verrichten om problemen aan te pakken die worden opgeworpen door systemen met behulp waarvan criminelen en terroristen met elkaar kunnen communiceren, en waartoe de bevoegde autoriteiten geen toegang hebben, en BENADRUKT dat in dit verband niet mag worden vergeten dat sterke en betrouwbare encryptie van groot belang is voor cyberbeveiliging en voor het vertrouwen in de digitale eengemaakte markt alsook voor het waarborgen van de eerbiediging van de mensenrechten en de fundamentele vrijheden;

43. ONDERSTREEPT dat het van belang is dat rechtshandhavingsinstanties worden toegerust met instrumenten voor het opsporen, onderzoeken en vervolgen van cybercriminaliteit, opdat misdrijven in de cyberruimte niet onopgemerkt of onbestraft blijven, en HEEFT WAARDERING voor de bijdrage van het Europees justitieel netwerk cybercriminaliteit in de strijd tegen criminaliteit via de samenwerking tussen justitiële autoriteiten;

44. WIJST OP het belang van een gecoördineerd EU-standpunt voor de daadwerkelijke totstandkoming van Europese en mondiale internetgovernancebeslissingen binnen de gemeenschap van multistakeholders, zoals het verzekeren van snel toegankelijke en accurate Whois-databanken van domeinnamen en IP-adressen, zodat de rechtshandhavingsvermogens en het openbaar belang zijn gewaarborgd;

45. BENADRUKT het belang van de toepassing van het internetprotocol IPv6, dat cruciaal is voor de grootschalige ontwikkeling van het internet der dingen en voor de verbetering van de toewijzing van misdaden in de cyberruimte;

46. MOEDIGT de lopende werkzaamheden op de volgende gebieden AAN: grensoverschrijdende toegang tot elektronisch bewijsmateriaal, het bewaren van gegevens en de uitdagingen voor strafrechtelijke procedures die worden opgeworpen door systemen met behulp waarvan criminelen en terroristen met elkaar kunnen communiceren, en waartoe de bevoegde autoriteiten geen toegang hebben, rekening houdend met de noodzaak van eerbiediging van de mensenrechten en de fundamentele vrijheden en gegevensbescherming;

47. ROEPT de Commissie OP:

- uiterlijk in december 2017 met een voortgangsverslag te komen over de uitvoering van de praktische maatregelen ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal;

- begin 2018 een wetgevingsvoorstel in te dienen ter verbetering van de grens-overschrijdende toegang tot elektronisch bewijsmateriaal;

48. VERZOEKT Europol, Enisa en Eurojust:

- voort te gaan met de versterking van hun samenwerking in de strijd tegen cybercriminaliteit, zowel onderling als met andere belanghebbenden, waaronder de CSIRT-gemeenschap, Interpol, de particuliere sector en de academische wereld, en te zorgen voor synergieën en complementariteit, in overeenstemming met hun respectieve mandaten en bevoegdheden.

- samen met de lidstaten bij te dragen aan een gecoördineerde aanpak voor de respons van EU-rechtshandhavingsinstanties op grootschalige cyberincidenten en -crises, ter aanvulling van de procedures die in de relevante kaders worden uiteengezet[19];

49. VERZOEKT de EU en haar lidstaten om door te gaan met:

- het wegnemen van de belemmeringen voor strafrechtelijk onderzoek en voor doeltreffende strafrechtspleging in de cyberruimte, evenals het versterken van de internationale samenwerking en coördinatie in de strijd tegen criminaliteit in de cyberruimte;

- et aanpakken van de uitdagingen in verband met anonimiserende technologieën, indachtig het feit dat sterke en betrouwbare encryptie van groot belang is voor cyberbeveiliging en voor het vertrouwen in de digitale eengemaakte markt;

- het vorm geven aan internetgovernancebeslissingen, die van invloed zijn op de vermogens van rechtshandhavingsinstanties in de strijd tegen criminaliteit in de cyberruimte.

[19] Doc. 9916/17 en C/2017/6100 final.

Hoofdstuk III

VERSTERKING VAN DE INTERNATIONALE SAMENWERKING VOOR EEN OPEN, VRIJE, VREEDZAME EN VEILIGE MONDIALE CYBERRUIMTE

50. ERKENT dat het waarborgen van cyberbeveiliging een mondiaal probleem is, dat doeltreffende wereldwijde samenwerking tussen alle actoren vereist, en ERKENT dat er bijzondere aandacht moet worden geschonken aan de eerbiediging van de democratische waarden en de beginselen van een open, vrije, vreedzame en veilige mondiale cyberruimte, en, tegen die achtergrond,

51. DOET EEN BEROEP op de EU en haar lidstaten om te werken aan de totstandbrenging van een strategisch kader voor conflictpreventie, samenwerking en stabiliteit in de cyberruimte dat gebaseerd is op de toepassing van het bestaande internationaal recht, met name het VN-Handvest in zijn geheel, de ontwikkeling en uitvoering van universele normen van verantwoordelijk gedrag van staten en regionale vertrouwenwekkende maatregelen tussen de lidstaten;

52. ERKENT de rol van de Verenigde Naties bij de verdere ontwikkeling van normen voor verantwoordelijk gedrag van staten in de cyberruimte, en herinnert eraan dat de besprekingen van de groep van regeringsdeskundigen van de Verenigde Naties in de loop der jaren hebben geleid tot een reeks normen en aanbevelingen[20], die door de Algemene Vergadering herhaaldelijk zijn bekrachtigd, en die staten als basis moeten nemen voor een verantwoordelijk gedrag van staten in de cyberruimte;

53. ERKENT dat deze normen van verantwoordelijk gedrag van staten inhouden dat staten hun grondgebied niet doelbewust mogen laten gebruiken voor internationale onrechtmatige daden, moeten beantwoorden aan passende verzoeken om bijstand van een andere staat waarvan de kritieke infrastructuur wordt geraakt door kwaadwillige ICT-acties vanaf hun grondgebied, en passende maatregelen moeten nemen ter bescherming van hun kritieke infrastructuur tegen ICT-dreigingen;

54. ERKENT de gedeelde cyberdreigingen en risico's waarmee de EU, de NAVO en hun respectieve lidstaten worden geconfronteerd, en HERHAALT het belang van voortzetting van de samenwerking tussen de EU en de NAVO op het gebied van cyberbeveiliging en defensie, met volledige inachtneming van de beginselen wederkerigheid, inclusiviteit en besluitvormings-autonomie van de EU, en overeenkomstig zijn conclusies van 6 december 2016 over de uitvoering van de gemeenschappelijke verklaring van de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie, en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie[20];

55. DOET EEN BEROEP op de EU en haar lidstaten om steun te verlenen en te ijveren voor de ontwikkeling van regionale vertrouwenwekkende maatregelen, die een essentieel element zijn voor het versterken van de samenwerking en de transparantie en het beperken van het risico op conflicten. De uitvoering van vertrouwenwekkende maatregelen inzake cyberbeveiliging in het kader van de OVSE en andere regionale organisaties zal de voorspelbaarheid van het gedrag van staten vergroten en verder bijdragen tot het stabiliseren van de cyberruimte;

56. BEVESTIGT dat de EU zal blijven vasthouden aan haar kernwaarden inzake bescherming van mensenrechten en fundamentele vrijheden, voortbouwend op de mensenrechtenrichtsnoeren van de EU over vrijheid online. De EU onderstreept tevens hoe belangrijk het is alle belanghebbenden, waaronder de academische wereld, het maatschappelijk middenveld en de particuliere sector, te betrekken bij de internetgovernance;

57. VERZOEKT de EU en haar lidstaten zich in te zetten voor de opbouw van cybercapaciteit in derde landen, waarbij de buurlanden van de EU en ontwikkelingslanden die gekenmerkt worden door snelgroeiende connectiviteit, voorrang moeten krijgen. Doel is het aanpakken van cyber-criminaliteit en het opbouwen van cyberweerbaarheid, in overeenstemming met de kernwaarden van de EU. Om de EU op dit gebied vooruit te helpen, moeten er een EU-netwerk voor de opbouw van cybercapaciteit en EU-richtsnoeren voor de opbouw van cybercapaciteit worden ontwikkeld, die complementair moeten zijn aan de bestaande mechanismen en structuren;

---

[20] Doc. 15283/16.

58. BENADRUKT dat er vooruitgang is geboekt bij de samenwerking tussen de EU en de NAVO op het vlak van cyberdefensie en veiligheid, bij de ontwikkeling ervan in opleiding, onderwijs en concepten, waarbij onnodige doublures worden voorkomen, en bij het bevorderen van inter-operabiliteit door middel van de vereisten en standaarden inzake cyberdefensie, en DRINGT AAN op verdere samenwerking op het vlak van cyberdefensie-oefeningen (personeel) en de uitwisseling van goede praktijken op het gebied van crisisbeheersing, waarbij onnodige doublures worden voorkomen, met volledige inachtneming van het EU-beleidskader inzake oefeningen en de beginselen inclusiviteit, wederkerigheid en besluitvormingsautonomie van de EU;

59. ERKENT dat het Verdrag van de Raad van Europa inzake cybercriminaliteit, het Verdrag van Boedapest, een doeltreffende juridische standaard biedt die als uitgangspunt kan dienen voor de nationale wetgeving inzake cybercriminaliteit. VERZOEKT alle landen passende nationale rechtskaders te ontwerpen en de samenwerking binnen dit bestaande internationale kader, het Verdrag van Boedapest, voort te zetten;

60. HERINNERT AAN de verwezenlijkingen in de bilaterale cyberdialogen van de EU en dringt aan op verdere inspanningen om de samenwerking met derde landen op het gebied van cyber-beveiliging te faciliteren;

61. HERINNERT ERAAN dat de EU over een robuust en juridisch bindend mechanisme voor uitvoercontrole beschikt, gebaseerd op besluiten en beste praktijken die zijn ontwikkeld in het kader van internationale non-proliferatieregelingen, NEEMT NOTA van het lopende debat in de Raad over de beste manieren voor verdere verbetering van de werking van deze controles, en VERZOEKT de lidstaten in de betrokken internationale uitvoercontroleregelingen (bv. Wassenaar Arrangement), essentiële cyberbeveiligingstoepassingen van nieuwe technologieën aan de orde te blijven stellen om aldus te zorgen voor doeltreffende controle van kritieke cyberbeveiligingstechnologieën van de toekomst.

62. Bij wijze van follow-up van de conclusies van de Europese Raad van 19 oktober 2017[21] zullen deze conclusies worden uitgevoerd door middel van een actieplan, dat naar verwacht vóór eind 2017 door de Raad zal worden aangenomen. Het actieplan is een levend document, dat regelmatig zal worden herzien en geactualiseerd door de Raad.

---

[21] Doc. EUCO 14/17.