Woensdag 13 juni 2018

P8_TA(2018)0258

Cyberdefensie

Resolutie van het Europees Parlement van 13 juni 2018 over cyberdefensie (2018/2004(INI))

(2020/C 28/06)

Het Europees Parlement,

— gezien het Verdrag betreffende de Europese Unie (VEU) en het Verdrag betreffende de werking van de Europese Unie (VWEU),

— gezien het document "Gedeelde visie, gemeenschappelijke actie: een sterker Europa – Een algemene strategie voor de Europese Unie op het gebied van het buitenlands en veiligheidsbeleid", dat op 28 juni 2016 door de vicevoorzitter van de Commissie/hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (VV/HV) werd gepresenteerd,

— gezien de conclusies van de Europese Raad van 20 december 2013, 26 juni 2015, 15 december 2016, 9 maart 2017, 22 juni 2017, 20 november 2017 en 15 december 2017,

— gezien de mededeling van de Commissie van 7 juni 2017 getiteld "Discussienota over de toekomst van de Europese defensie" (COM(2017)0315),

— gezien de mededeling van de Commissie van 7 juni 2017 getiteld "Oprichting van het Europees Defensiefonds" (COM(2017)0295),

— gezien de mededeling van de Commissie van 30 november 2016 over het Europees defensieactieplan (COM(2016)0950),

— gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 7 februari 2013 aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace(JOIN(2013)0001),

— gezien het werkdocument van de diensten van de Commissie van 13 september 2017 getiteld "Assessment of the EU 2013 Cybersecurity Strategy" ("Beoordeling van de EU-strategie voor 2013 inzake cyberbeveiliging") (SWD(2017)0295),

— gezien het EU-beleidskader voor cyberdefensie van 18 november 2014,

— gezien de conclusies van de Raad van 10 februari 2015 over cyberdiplomatie,

— gezien de conclusies van de Raad van 19 juni 2017 over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (het "instrumentarium voor cyberdiplomatie"),

— gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 13 september 2017 aan het Europees Parlement en de Raad getiteld "Weerbaarheid, afschrikking en defensie: Bouwen aan sterke cyberbeveiliging voor de EU" (JOIN(2017)0450),

Woensdag 13 juni 2018

— gezien het "Handboek van Tallinn 2.0 over het internationale recht toepasselijk op cyberoperaties" ([1]),

— gezien 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 ([2]),

— gezien de werkzaamheden van de Global Commission on the Stability of Cyberspace (de wereldcommissie voor stabiliteit in cyberspace),

— gezien de mededeling van de Commissie van 28 april 2015 over de Europese veiligheidsagenda (COM(2015)0185),

— gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 6 april 2016 aan het Europees Parlement en de Raad over het "Gezamenlijk kader voor de bestrijding van hybride bedreigingen: Een reactie van de Europese Unie" (JOIN(2016)0018),

— gezien zijn resolutie van 3 oktober 2017 over de strijd tegen cybercriminaliteit ([3]),

— gezien de gezamenlijke verklaring van de voorzitters van de Europese Raad en de Commissie, en van de secretaris-generaal van de NAVO van 8 juli 2016, alsook de gemeenschappelijke reeksen voorstellen voor de toepassing van de gemeenschappelijke verklaring als bekrachtigd door de NAVO-Raad en de EU-Raad op 6 december 2016 en 5 december 2017, en de voortgangsverslagen van 14 juni en 5 december 2017 over de tenuitvoerlegging daarvan,

— gezien zijn resolutie van 22 november 2012 over cyberveiligheid en -defensie ([4]),

— gezien zijn resolutie van 22 november 2016 over de Europese defensie-unie ([5]),

— gezien het voorstel van de Commissie van 13 september 2017 voor een verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening") (COM(2017)0477),

— gezien zijn resolutie van 13 december 2017 over het jaarverslag over de uitvoering van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) ([6]),

— gezien zijn resolutie van 13 december 2017 over het jaarverslag over de uitvoering van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) ([7]),

— gezien artikel 52 van zijn Reglement,

— gezien het verslag van de Commissie buitenlandse zaken (A8-0189/2018),

A. overwegende dat hybride en cyberproblemen, -dreigingen en -aanvallen een ernstige bedreiging vormen voor de veiligheid, de defensie, de stabiliteit en het concurrentievermogen van de EU, haar lidstaten en haar burgers; overwegende dat cyberdefensie zowel militaire als civiele aspecten omvat;

([1]) Cambridge University Press, februari 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524
([2]) PB L 194 van 19.7.2016, blz. 1.
([3]) Aangenomen teksten, P8_TA(2017)0366.
([4]) PB C 419 van 16.12.2015, blz. 145.
([5]) Aangenomen teksten, P8_TA(2016)0435.
([6]) Aangenomen teksten, P8_TA(2017)0493.
([7]) Aangenomen teksten, P8_TA(2017)0492.

B. overwegende dat de EU en de lidstaten worden geconfronteerd met een ongekende dreiging in de vorm van politiek gemotiveerde en door overheden gesponsorde cyberaanvallen, alsmede van cybercriminaliteit en -terrorisme;

C. overwegende dat cyberspace algemeen door strijdkrachten wordt erkend als het vijfde operationele domein en dat dit ruimte biedt voor de ontwikkeling van het cyberdefensievermogen; overwegende dat er momenteel wordt gedebatteerd over het al dan niet erkennen van cyberspace als het vijfde domein van oorlogvoering;

D. overwegende dat in de clausule betreffende wederzijdse defensie van artikel 42, lid 7, VEU is bepaald dat de lidstaten verplicht zijn elkaar met alle middelen waarover zij beschikken hulp en bijstand te verlenen indien een lidstaat op zijn grondgebied gewapenderhand wordt aangevallen; overwegende dat dit het specifieke karakter van het veiligheids- en defensiebeleid van bepaalde lidstaten onverlet laat; overwegende dat de solidariteitsclausule van artikel 222 VWEU een aanvulling vormt op de clausule betreffende wederzijdse defensie, aangezien hierin is bepaald dat lidstaten gezamenlijk moeten optreden indien een lidstaat getroffen wordt door een terroristische aanval, een natuurramp of een door de mens veroorzaakte ramp; overwegende dat de solidariteitsclausule het gebruik van zowel civiele als militaire middelen omvat;

E. overwegende dat de EU, hoewel cyberdefensie een kerncompetentie van de lidstaten is en blijft, een beslissende rol speelt bij het bieden van een platform voor Europese samenwerking en bij het waarborgen van de nauwe coördinatie van de inspanningen op dit gebied op internationaal niveau en binnen de trans-Atlantische veiligheidsarchitectuur, vanaf het begin, om de lacunes en inefficiëntie die veelal bij traditionele defensie-inspanningen komen kijken, te vermijden; overwegende dat het versterken van onze samenwerking en coördinatie niet volstaat; overwegende dat er voor doeltreffende preventie moet worden gezorgd door de EU beter in staat te stellen om aanvallen te identificeren, af te weren en te beletten; overwegende dat er voor de verwezenlijking van doeltreffende cyberbeveiliging voor de EU een geloofwaardig vermogen voor het afweren en beletten van aanvallen vereist is, en dat er tegelijkertijd voor moet worden gezorgd dat de landen die het minst zijn voorbereid, geen makkelijke doelwitten worden voor cyberaanvallen, en overwegende dat solide cyberdefensie een onmisbaar onderdeel moet vormen van het GVDB en van de ontwikkeling van de Europese defensie-unie; overwegende dat we momenteel te maken hebben met een permanent gebrek aan hoogopgeleide cyberveiligheidsdeskundigen; overwegende dat de nauwe coördinatie van de bescherming van de strijdkrachten tegen cyberaanvallen essentieel is voor de ontwikkeling van een doeltreffend GVDB;

F. overwegende dat de EU-lidstaten vaak het slachtoffer zijn van cyberaanvallen op civiele of militaire doelwitten door vijandige en gevaarlijke (niet-)overheidsactoren; overwegende dat de huidige kwetsbaarheid voornamelijk te wijten is aan de fragmentatie van Europese defensiestrategieën en -vermogens, wat buitenlandse inlichtingendiensten de kans geeft om herhaaldelijk te profiteren van zwakke punten in de beveiliging van IT-systemen en -netwerken die van essentieel belang zijn voor de Europese veiligheid; overwegende dat de overheden van de lidstaten vaak hebben verzaakt de betrokken belanghebbenden tijdig van deze kwetsbaarheden in hun producten en diensten in kennis te stellen om hun de gelegenheid te geven deze te verhelpen; overwegende dat dringende versterking en uitbreiding van de offensieve en defensieve capaciteiten van Europa op civiel en militair niveau vereist is om het hoofd te bieden aan dergelijke aanvallen en de mogelijke grensoverschrijdende gevolgen op economisch en maatschappelijk gebied te voorkomen;

G. overwegende dat het onderscheid tussen civiele en militaire inmenging in cyberspace vervaagt;

H. overwegende dat veel cyberincidenten plaatsvinden vanwege een gebrek aan weerbaarheid en betrouwbaarheid van de private en publieke netwerkinfrastructuur, slecht beschermde of beveiligde databanken en andere gebreken in de vitale informatie-infrastructuur; overwegende dat slechts een paar lidstaten het beschermen van hun afzonderlijke netwerken en informatiesystemen en de daarin opgenomen gegevens tot hun zorgplicht en verantwoordelijkheden rekenen, wat het algemene gebrek aan investeringen in opleiding en geavanceerde beveiligingstechnologieën, alsmede aan de ontwikkeling van relevante richtsnoeren verklaart;

I. overwegende dat het recht op privacy en het recht op gegevensbescherming zijn vastgelegd in het Handvest van de grondrechten van de Europese Unie en in artikel 16 VWEU, en worden geregeld bij de algemene verordening gegevensbescherming (AVG) van de EU, die op 25 mei 2018 in werking is getreden;

J. overwegende dat een actief en doeltreffend cyberbeleid vijanden moet kunnen afschrikken en mogelijkheden moet omvatten om te anticiperen op aanvallen en het aanvalsvermogen van vijanden te verminderen;

Woensdag 13 juni 2018

K. overwegende dat verscheidene terroristische groeperingen en organisaties cyberspace gebruiken als een goedkoop middel voor werving en radicalisering en voor het verspreiden van terroristische propaganda; overwegende dat terroristische groeperingen, niet-overheidsactoren en grensoverschrijdende misdaadnetwerken cyberoperaties inzetten om anoniem geld te verkrijgen, inlichtingen te verzamelen en cyberwapens te ontwikkelen met het oog op cyberterreurcampagnes, om vitale infrastructuur te verstoren, te beschadigen of te vernietigen, om financiële systemen aan te vallen en om andere onwettige activiteiten te verrichten met alle gevolgen van dien voor de veiligheid van de Europese burgers;

L. overwegende dat de cyberdefensie en -afschrikking van de Europese krijgsmacht en de bescherming van vitale infrastructuur tegen cyberaanvallen cruciale kwesties zijn geworden in debatten over de modernisering van defensie, de gemeenschappelijke inspanningen van Europa op het gebied van defensie, de toekomstige ontwikkeling van de krijgsmacht en haar operaties, en de versterking van de strategische autonomie van de Europese Unie;

M. overwegende dat verscheidene lidstaten aanzienlijke investeringen hebben gedaan in goed uitgeruste cybercommando's om deze nieuwe problemen aan de orde te stellen, maar dat er nog veel werk moet worden verzet aangezien het steeds moeilijker wordt om cyberaanvallen op het niveau van de lidstaten tegen te gaan; overwegende dat de cybercommando's van de afzonderlijke lidstaten verschillen met betrekking tot hun offensieve of defensieve mandaat; overwegende dat andere cyberdefensiestructuren sterk uiteenlopen per lidstaat en nog altijd aanzienlijk versnipperd zijn; overwegende dat cyberdefensie en -afschrikking op operationeel gebied geen nationale of organisatorische grenzen kennen en daarom het best in samenwerkingsverband op Europees niveau en in overleg met onze partners en bondgenoten kunnen worden benaderd; overwegende dat militaire en civiele cyberbeveiliging nauw met elkaar verband houden en dat er daarom meer samenwerking tussen militaire en civiele deskundigen nodig is; overwegende dat particuliere ondernemingen veel ervaring hebben op dit gebied, hetgeen fundamentele beheers- en veiligheidsvragen doet rijzen over het vermogen van overheden om hun burgers te beschermen;

N. overwegende dat er dringend behoefte is aan versterking van het cyberdefensievermogen van de EU, omdat er niet tijdig is ingespeeld op het veranderende cyberbeveiligingslandschap; overwegende dat een snelle reactie en goede voorbereiding essentieel zijn voor het waarborgen van de veiligheid op dit gebied;

O. overwegende dat permanente gestructureerde samenwerking (PESCO) en het Europees Defensiefonds (EDF) beide nieuwe initiatieven zijn met een toepassingsgebied dat ruimte biedt voor de bevordering van een vruchtbare omgeving voor kmo's en start-ups, alsmede voor samenwerkingsprojecten op het gebied van cyberdefensie, en dat beide initiatieven zullen bijdragen aan de vormgeving van het institutioneel en regelgevingskader;

P. overwegende dat de lidstaten die aan PESCO deelnemen, zich ertoe hebben verbonden te waarborgen dat de samenwerkingsinspanningen op het gebied van cyberdefensie, zoals informatie-uitwisseling, opleiding en operationele ondersteuning, voortdurend worden uitgebreid;

Q. overwegende dat twee van de zeventien projecten die in het kader van PESCO zijn uitgekozen, betrekking hebben op cyberdefensie;

R. overwegende dat het EDF, aan de hand van investeringen in digitale en cybertechnologieën, ter ondersteuning van het mondiale innovatie- en concurrentievermogen van de Europese defensie-industrie moet dienen en dat het tevens kansen moet creëren voor kmo's en start-ups om een steentje bij te dragen en de ontwikkeling van slimme oplossingen te bevorderen;

S. overwegende dat het Europees Defensieagentschap (EDA) een aantal projecten heeft opgezet om aan de behoeften van de lidstaten met betrekking tot de ontwikkeling van hun cyberdefensievermogen tegemoet te komen, waaronder onderwijs- en opleidingsprojecten als het Cyber Defence Training & Exercises Coordination Platform (CD TEXP), Demand Pooling for Cyber Defence Training and Exercise (DePoCyTE) voor opleidingen van particulieren, en het Cyber Ranges-project met betrekking tot cybertestomgevingen;

T. overwegende dat er momenteel andere EU-projecten lopen op het gebied van situationeel bewustzijn, malwaredetectie en informatie-uitwisseling (het Malware Information Sharing Platform (MISP) en het Multi-Agent System For Advanced persistent threat Detection (MASFAD));

U. overwegende dat er een beduidende en toenemende behoefte is aan capaciteitsopbouw en opleidingen op het gebied van cyberdefensie en dat hieraan het best in samenwerkingsverband op EU- en NAVO-niveau tegemoet kan worden gekomen;

V. overwegende dat GVDB-missies en -operaties, net als andere moderne organisatorische inspanningen, sterk afhankelijk zijn van goed werkende IT-systemen; overwegende dat bij GVDB-missies en -operaties op verschillende niveaus cyberdreigingen kunnen komen kijken, variërend van het tactische (GVDB-missies en -operaties) en operationele niveau (EU-netwerken), tot het bredere niveau van de wereldwijde IT-infrastructuur;

W. overwegende dat commando- en besturingssystemen, informatie-uitwisseling en logistiek met name op tactisch en operationeel niveau sterk afhankelijk zijn van (niet-)gerubriceerde IT-infrastructuur; overwegende dat deze systemen aantrekkelijke doelwitten vormen voor actoren die kwaadwillige bedoelingen hebben en missies willen saboteren; overwegende dat cyberaanvallen ernstige gevolgen kunnen hebben voor de infrastructuur van de EU; overwegende dat met name cyberaanvallen op de energie-infrastructuur van de EU ernstige gevolgen zouden hebben en dat deze infrastructuur hier daarom tegen moet worden beschermd;

X. overwegende dat het duidelijk is dat in alle fasen van de planning van GVDB-missies en -operaties goed rekening moet worden gehouden met cyberdefensie en dat voortdurend toezicht hierbij onontbeerlijk is, en dat het defensievermogen toereikend moet zijn om cyberdefensie volledig in de planning van missies op te kunnen nemen en doorlopend de essentiële ondersteuning te kunnen bieden;

Y. overwegende dat de Europese Veiligheids- en defensieacademie (EVDA) de enige Europese instantie is die opleidingen aanbiedt voor GVDB-structuren, -missies en operaties; overwegende dat de academie in de toekomst naar verwachting een grotere rol zal gaan spelen in het bundelen van Europese opleidingen op het gebied van cyberdefensie;

Z. overwegende dat cyberspace in de verklaring van de NAVO-top van 2016 in Warschau wordt erkend als operationeel domein waarbinnen de NAVO zich even doeltreffend moet kunnen verdedigen als in de lucht, te land en op zee;

AA. overwegende dat de EU en de NAVO aan de hand van onderzoek voor tweeërlei gebruik en van door het EDA en de NAVO gecoördineerde projecten hebben bijgedragen aan de bevordering van het cyberdefensievermogen van de lidstaten en aan de vergroting van de weerbaarheid op cybergebied van de lidstaten, met steun van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa);

AB. overwegende dat de NAVO operaties op het gebied van cyberbeveiliging in 2014 heeft aangemerkt als onderdeel van haar collectieve defensie, en cyberspace in 2016, naast land, lucht en zee, heeft erkend als operationeel domein; overwegende dat de EU en de NAVO elkaar als partners aanvullen bij het versterken van hun weerbaarheid en defensievermogen op cybergebied; overwegende dat de samenwerking tussen de partijen het intensiefst is op het vlak van cyberbeveiliging en -defensie, en dat beide op dit gebied unieke capaciteiten hebben; overwegende dat de EU en de NAVO in hun gezamenlijke verklaring van 8 juli 2016 hebben ingestemd met een brede agenda voor samenwerking; overwegende dat vier van de 42 voorstellen voor nauwere samenwerking betrekking hebben op cyberbeveiliging en -defensie, terwijl verdere voorstellen meer in het algemeen gericht zijn op het aanpakken van hybride dreigingen; overwegende dat er op 5 december 2017 een aanvullend voorstel over cyberbeveiliging en -defensie is gepresenteerd;

AC. overwegende dat de groep van regeringsdeskundigen van de Verenigde Naties (UN GGE) haar laatste overlegronde heeft afgerond; overwegende dat de verslagen van 2013 en 2015, ondanks het feit dat de groep tijdens de overlegronde van 2017 geen overeenstemming heeft kunnen bereiken, van toepassing zijn en tevens dat het bestaand internationaal recht, en met name het Handvest van de Verenigde Naties, daarmee van toepassing is op en van wezenlijk belang is voor de handhaving van vrede en stabiliteit, en de bevordering van een open, veilige, vredige en toegankelijke ICT-omgeving;

AD. overwegende dat het onlangs ingevoerde kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (het zogenaamde "instrumentarium voor cyberdiplomatie"), dat gericht is op de ontwikkeling van het vermogen van de EU en haar lidstaten om het gedrag van potentiële agressors te kunnen beïnvloeden, een set van evenredige (restrictieve) maatregelen omvat die binnen het GBVB kunnen worden toegepast;

AE. overwegende dat verscheidene overheidsactoren, waaronder Rusland, China en Noord-Korea, maar ook door overheden geïnspireerde, ingehuurde of gesponsorde niet-overheidsactoren (met inbegrip van georganiseerde criminele groepen), veiligheidsdiensten en particuliere bedrijven, betrokken zijn geweest bij kwaadwillige cyberactiviteiten ter verwezenlijking van politieke, economische of veiligheidsdoelstellingen, bijvoorbeeld door middel van cyberaanvallen op vitale infrastructuur, cyberspionage en massa-observatie van EU-burgers, hulp bij desinformatiecampagnes en beperking van de internettoegang en de werking van IT-systemen door het verspreiden van malware (Wannacry, NotPetya enz.); overwegende dat dergelijke aanvallen in strijd zijn met het internationaal recht, de mensenrechten en de grondrechten van de EU en een gevaar vormen voor de democratie, de veiligheid, de openbare orde en de strategische autonomie van de EU, en dat ze derhalve tot een gezamenlijk diplomatisch EU-optreden (met inbegrip van restrictieve maatregelen in het kader van het EU-instrumentarium voor cyberdiplomatie zoals, in het geval van privébedrijven, geldboetes en beperking van de toegang tot de interne markt) zouden moeten leiden;

AF. overwegende dat er in het verleden verscheidene malen dergelijke grootschalige aanvallen zijn uitgevoerd op de ICT-infrastructuur van, bijvoorbeeld, Estland in 2007 en van Georgië in 2008, en dat er momenteel vrijwel dagelijks aanvallen worden uitgevoerd op de infrastructuur van Oekraïne; overwegende dat offensief cybervermogen momenteel ook op ongekende schaal wordt ingezet tegen EU- en NAVO-lidstaten;

AG. overwegende dat cyberbeveiligingstechnologieën, die zowel op civiel als militair gebied van groot belang zijn, zogenaamde technologieën voor tweeërlei gebruik zijn die tal van mogelijkheden bieden voor de ontwikkeling van synergieën tussen civiele en militaire actoren op een aantal terreinen, waaronder programma's voor encryptie, beveiliging en risicobeheer, en inbraakdetectie- en preventiesystemen;

AH. overwegende dat de ontwikkeling van cybertechnologieën de komende jaren een invloed zal hebben op nieuwe gebieden als kunstmatige intelligentie, het internet der dingen, robotica en mobiele apparaten, en dat dit ook op het gebied van defensie veiligheidsimplicaties met zich mee kan brengen;

AI. overwegende dat de door verscheidene lidstaten opgerichte cybercommando's een aanzienlijke bijdrage kunnen leveren aan de bescherming van vitale civiele infrastructuur en dat kennis over cyberdefensie op civiel gebied vaak even nuttig is;

Ontwikkeling van het defensie- en afschrikkingsvermogen op cybergebied

1. benadrukt dat een gemeenschappelijk cyberdefensiebeleid en een aanzienlijk cyberdefensievermogen tot de kernelementen van de ontwikkelingen op het gebied van de Europese defensie-unie moeten behoren;

2. is ingenomen met het initiatief van de Commissie voor een cyberbeveiligingspakket ter bevordering van de weerbaarheid, afschrikking en defensie op cybergebied in de EU;

3. herinnert eraan dat cyberdefensie zowel militaire als civiele aspecten heeft en daarom gebaat is bij een geïntegreerde beleidsaanpak en nauwe samenwerking tussen militaire en civiele belanghebbenden;

4. pleit voor een coherente ontwikkeling van het cybervermogen in alle EU-instellingen en -organen, alsook in de lidstaten, en voor de nodige politieke en praktische oplossingen om de overgebleven politieke, wettelijke en organisatorische belemmeringen voor de samenwerking op het gebied van cyberdefensie uit de weg te ruimen; acht een regelmatige en intensievere uitwisseling en samenwerking op EU- en nationaal niveau op het gebied van cyberdefensie tussen de betrokken publieke belanghebbenden van cruciaal belang;

5. wijst er in het kader van de opkomende Europese defensie-unie nadrukkelijk op dat het cyberdefensievermogen van de lidstaten voorop moet staan en vanaf de beginfase zo goed mogelijk in het beleid moet worden opgenomen om te zorgen voor een maximale doeltreffendheid; verzoekt de lidstaten daarom met klem om hun nationale cyberdefensie in nauwe samenwerking en op basis van een duidelijk stappenplan te ontwikkelen, teneinde coördinatie door de Commissie, de Europese Dienst voor extern optreden (EDEO) en het EDA te vereenvoudigen voor een betere onderlinge aansluiting van de cyberdefensiestructuren van de lidstaten door dringend de beschikbare kortetermijnmaatregelen te nemen en de uitwisseling van deskundigheid te stimuleren; is van mening dat er een veilig Europees netwerk voor cruciale informatie en vitale infrastructuur moet worden ontwikkeld; bevestigt dat het met het oog op doeltreffende cyberdefensie en -afschrikking van wezenlijk belang is om de aanstichter te kunnen aanwijzen, en dat voor doeltreffende preventie aanzienlijke verdere technologische deskundigheid moet worden vergaard; dringt er bij de lidstaten op aan om de financiële en personele middelen te verruimen, met name voor deskundigen op het gebied van forensisch computeronderzoek, om bij cyberaanvallen gemakkelijker de aanstichter aan te kunnen wijzen; benadrukt dat een dergelijke samenwerking ook ten uitvoer moet worden gelegd middels de versterking van het Enisa;

6. realiseert zich dat het beschikken over het eigen cyberdefensievermogen door veel lidstaten als kern van het nationaal veiligheidsbeleid en als wezenlijk onderdeel van de nationale soevereiniteit wordt beschouwd; beklemtoont echter dat er voor alomvattende en doeltreffende acties op het gebied van cyberdefensie ter waarborging van de strategische autonomie van de EU in cyberspace vanwege de grensoverschrijdende aard van cyberspace een toepassingsgebied en deskundigheid vereist zijn die buiten het bereik van de afzonderlijke lidstaten vallen, wat inhoudt dat er intensiever en op gecoördineerde wijze door de lidstaten moet worden opgetreden op EU-niveau; merkt in dit verband op dat de EU en haar lidstaten met betrekking tot de uitwerking van dergelijke acties onder tijdsdruk staan en direct in actie moeten komen; merkt op dat de EU, dankzij EU-initiatieven als de digitale eengemaakte markt, in een goede positie verkeert om het voortouw te nemen bij de ontwikkeling van Europese cyberdefensiestrategieën; herinnert eraan dat de ontwikkeling van cyberdefensie op Europees niveau het vermogen van de EU om zich te beschermen en zelfstandig op te treden moet versterken; is in dit verband ingenomen met het voorstel voor een permanent mandaat voor en versterking van de rol van het Enisa;

7. verzoekt de lidstaten in dit verband met klem het uit PESCO en het Europees Defensiefonds voortvloeiende kader zo goed mogelijk toe te passen om voorstellen voor samenwerkingsprojecten op te stellen;

8. neemt kennis van de vele inspanningen van de EU en haar lidstaten op het gebied van cyberdefensie; neemt in het bijzonder kennis van de projecten van het EDA in verband met cybertestomgevingen, de strategische onderzoeksagenda voor cyberdefensie, en de samenstelling van pakketten voor bewustmaking met betrekking tot cybersituaties voor hoofdkwartieren;

9. is ingenomen met de cyberprojecten die in het kader van PESCO worden uitgevoerd, namelijk het platform voor informatie-uitwisseling over cyberdreigingen en -incidenten, de cybercrisisteams en wederzijdse bijstand op het gebied van cyberbeveiliging; benadrukt dat beide projecten gericht zijn op een defensief cyberbeleid dat gebaseerd is op de uitwisseling van informatie over cyberdreigingen via een netwerkplatform van de lidstaten en de samenstelling van cybercrisisteams met behulp waarvan de lidstaten elkaar kunnen helpen om de weerbaarheid op cybergebied te vergroten en cyberdreigingen collectief op te sporen, te herkennen en te ondervangen; vraagt de Commissie en de lidstaten voort te bouwen op de PESCO-projecten voor nationale cybercrisisteams en wederzijdse bijstand op het gebied van cyberbeveiliging, door een Europees cybercrisisteam op te richten om collectieve cyberdreigingen te detecteren en af te slaan en acties te coördineren ter ondersteuning van de inspanningen van de deelnemende lidstaten;

10. merkt op dat kennis van technologieën, apparatuur, diensten en gegevens en de bewerking daarvan bepalend is voor het vermogen van Europa om cyberdefensieprojecten te ontwikkelen en dat hiertoe een beroep moet worden gedaan op een groep betrouwbare actoren uit het bedrijfsleven;

11. herinnert eraan dat de geleverde inspanningen ter versterking van de homogeniteit van de commandosystemen onder meer tot doel hebben ervoor te zorgen dat de beschikbare commandostructuren interoperabel zijn met die van derde landen die bij de NAVO zijn aangesloten, alsmede met die van gelegenheidspartners, zodat ervoor kan worden gezorgd dat de uitwisseling vlot verloopt teneinde het besluitvormingsproces te versnellen en dat de leidende positie op gebied van informatie over cyberrisico's wordt gehandhaafd;

12. pleit voor nieuwe mogelijkheden (bijvoorbeeld een meerjarige ontwikkeling van het cyberdefensievermogen) ter aanvulling van de projecten van de NAVO op het gebied van slimme defensie, de zogenaamde "Smart Defense"-projecten, het platform voor de uitwisseling van informatie over malware (MISP) en multinationale scholing en opleidingen over cyberdefensie (MN CD E&T);

13. is zich bewust van de ontwikkelingen op het gebieden als nanotechnologie, kunstmatige intelligentie, big data, elektronisch afval en geavanceerde robotica; dringt er bij de lidstaten en de EU op aan bijzondere aandacht te schenken aan de mogelijke uitbuiting van deze gebieden door vijandige overheidsactoren en de georganiseerde misdaad; pleit voor de ontwikkeling van opleidingen en het vermogen om bescherming te bieden tegen de opkomst van geavanceerde misdrijven als complexe identiteitsfraude en namaak van goederen;

14. benadrukt dat de terminologie in verband met de veiligheid in cyberspace moet worden verduidelijkt, en dat er behoefte is aan een alomvattende geïntegreerde aanpak en gemeenschappelijke inspanningen om cyber- en hybride dreigingen te bestrijden, en wijkplaatsen voor extremisten en criminelen op het internet op te sporen en op te doeken, door de uitwisseling van informatie tussen de EU en EU-agentschappen als Europol, Eurojust, het EDA en het Enisa te versterken en te intensiveren;

15. benadrukt de toenemende rol van kunstmatige intelligentie bij cyberagressie en -defensie; verzoekt de EU en de lidstaten met klem hier zowel bij het onderzoek naar en de praktische uitwerking van hun cyberdefensievermogen bijzondere aandacht aan te schenken;

16. wijst er nadrukkelijk op dat er met het oog op de inzet van al dan niet bewapende onbemande luchtvaartuigen, aanvullende maatregelen moeten worden getroffen om mogelijke cyberkwetsbaarheden te verminderen;

Cyberdefensie tijdens GVDB-missies en -operaties

17. beklemtoont dat cyberdefensie bij GVDB-missies en -operaties beschouwd moet worden als een operationele taak, en dat zij in alle planningsprocessen moet worden opgenomen om te waarborgen dat in alle fasen van het planningsproces rekening wordt gehouden met cyberveiligheid en zo cyberkwetsbaarheden te verminderen;

18. bevestigt dat voor het plannen van succesvolle GVDB-missies en -operaties zowel in de operationele hoofdkwartieren als binnen de missie zelf aanzienlijke deskundigheid op het gebied van cyberdefensie alsook een veilige IT-infrastructuur en veilige netwerken vereist zijn om een grondige dreigingsanalyse uit te kunnen voeren en adequate bescherming te kunnen bieden in het veld; verzoekt de EDEO en de lidstaten die fungeren als hoofdkwartieren voor GVDB-operaties de tijdens EU-missies en -operaties geboden deskundigheid op het gebied van cyberdefensie te bevorderen; merkt op dat er grenzen zijn met betrekking tot de mate waarin GVDB-missies op cyberaanvallen kunnen worden voorbereid;

19. benadrukt dat de planning van GVDB-missies en -operaties steeds vergezeld moet gaan van een grondige analyse van het cyberdreigingslandschap; merkt op dat de door het Enisa opgestelde dreigingsclassificatie een passend model voor een dergelijke analyse vormt; pleit voor de totstandbrenging van een vermogen voor het analyseren van de cyberweerbaarheid voor GVDB-hoofdkwartieren;

20. bevestigt met name hoe belangrijk het is om de digitale voetafdruk en het aanvalsoppervlak van GVDB-missies en -operaties tot een minimum te beperken; verzoekt de betrokken planners met klem dit vanaf de beginfase van het planningsproces in aanmerking te nemen;

21. is zich ervan bewust dat de analyse door het EDA met betrekking tot opleidingsbehoeften belangrijke tekortkomingen op het gebied van cyberdefensievaardigheden en -competenties bij besluitvormers binnen en buiten de EU aan het licht heeft gebracht, en is ingenomen met de EDA-initiatieven inzake opleidingen voor belangrijke besluitvormers in de lidstaten ter ondersteuning van GVDB-missies en -operaties;

Onderwijs en opleiding op het gebied van cyberdefensie

22. merkt op dat het stroomlijnen van het opleidings- en scholingslandschap van de EU-cyberdefensie de dreigingen in hoge mate zou inperken en roept de EU en de lidstaten op hun samenwerking op het gebied van opleiding, scholing en oefeningen te intensiveren;

23. is groot voorstander van het militair Erasmus-programma en andere gemeenschappelijke opleidings- en uitwisselingsinitiatieven die gericht zijn op het bevorderen van de interoperabiliteit van de strijdkrachten van de lidstaten en van de ontwikkeling van een gemeenschappelijke strategische cultuur door frequentere uitwisseling van jonge militaire medewerkers, gezien het feit dat een dergelijke interoperabiliteit tussen alle lidstaten en NAVO-bondgenoten van essentieel belang is; is echter van mening dat de uitwisseling voor opleidings- en onderwijsdoeleinden op het vlak van cyberdefensie zich niet tot dit initiatief moet beperken, maar militair personeel van alle leeftijden en rangen moet beslaan, evenals studenten uit alle academische instellingen die opleidingsprogramma's op het gebied van cyberveiligheid bieden;

24. benadrukt dat er meer deskundigen nodig zijn op het gebied van cyberdefensie; verzoekt de lidstaten de samenwerking tussen civiele academische instellingen en militaire academies te vergemakkelijken om dit tekort te overbruggen en te voorzien in meer mogelijkheden voor onderwijs en opleiding op het gebied van cyberdefensie, en pleit tevens voor het inzetten van meer middelen voor gespecialiseerde opleidingen op het gebied van cyberoperaties, met inbegrip van opleidingen op het gebied van kunstmatige intelligentie; verzoekt militaire academies onderwijs op het gebied van cyberdefensie in hun curricula op te nemen om zo de pool van cyberdeskundigen uit te breiden ten behoeve van GVDB-missies;

25. verzoekt alle lidstaten om bedrijven, scholen en burgers proactief te informeren en te adviseren over cyberveiligheid en de grootste digitale dreigingen, en bij hen het bewustzijn hiervan te vergroten; is in dit opzicht verheugd over de ontwikkeling van cyberrichtsnoeren die burgers en organisaties kunnen helpen een betere cyberveiligheidsstrategie te ontwikkelen, en over de hele linie kennis over cyberveiligheid en weerbaarheid in de cyberspace kunnen bevorderen;

26. constateert dat de lidstaten zich gezien de behoefte aan meer gespecialiseerd personeel niet alleen moeten richten op het werven van militair personeel, maar ook op het behouden van de benodigde deskundigen;

27. is ingenomen met de tenuitvoerlegging van het eerste van de vier in het kader van de EDA-agenda voor bundelen en delen gestarte cyberdefensieprojecten door de elf lidstaten (België, Duitsland, Estland, Finland, Griekenland, Ierland, Letland, Nederland, Oostenrijk, Portugal en Zweden) die deelnemen aan het "Cyber Ranges Federation"-project; roept de andere lidstaten op zich bij dit initiatief aan te sluiten; verzoekt de lidstaten de wederzijdse beschikbaarheid van virtuele cybertestomgevingen en opleidingen op het gebied van cyberdefensie te bevorderen; merkt in dit verband op dat ook de rol en deskundigheid van het Enisa in overweging moeten worden genomen;

28. is van mening dat dergelijke initiatieven Uniebreed kunnen bijdragen aan de verbetering van de kwaliteit van onderwijs op het gebied van cyberdefensie, met name door het opzetten van uitgebreide technische platformen en het samenstellen van groepen van EU-deskundigen; is van mening dat de Europese krijgsmacht ervoor kan zorgen dat deze initiatieven meer in trek raken door veelomvattende opleidingen op het gebied van cyberdefensie te bieden en cyberdeskundigen aan te trekken en te behouden; benadrukt dat het van essentieel belang is zwakke plekken in computersystemen te identificeren in zowel de lidstaten als de EU-instellingen; realiseert zich dat het merendeel van deze zwakke plekken in cyberveiligheidssystemen het gevolg is van menselijk falen en pleit derhalve voor periodieke opleidingen voor zowel militair als civiel personeel in dienst van de EU-instellingen;

29. verzoekt het EDA het coördinatieplatform voor opleiding en oefening op het gebied van cyberdefensie (CD TEXP) zo spoedig mogelijk op te zetten ter ondersteuning van het "Cyber Ranges Federation"-project, met speciale aandacht voor versterkte samenwerking ten aanzien van geharmoniseerde voorschriften, het stimuleren van onderzoek op het gebied van cyberdefensie en technologische innovatie, en het gezamenlijk helpen van derde landen bij hun capaciteitsopbouw met betrekking tot hun weerbaarheid in cyberspace; verzoekt de Commissie en de lidstaten deze initiatieven aan te vullen met een Europees Kenniscentrum voor cyberdefensie om de meest veelbelovende nieuwe medewerkers van vakkundige opleidingen te kunnen voorzien ter ondersteuning van de opleidingen op het gebied van cyberdefensie in de deelnemende lidstaten;

30. is ingenomen met de ontwikkeling van het platform voor onderwijs, opleiding, evaluatie en oefening op het gebied van cyberdefensie binnen de EVDA om de mogelijkheden op het gebied van opleiding en onderwijs in de lidstaten uit te kunnen breiden;

31. dringt aan op een betere uitwisseling van kennis over het situationeel bewustzijn door middel van simulatieoefeningen op cybergebied en het coördineren van de afzonderlijke inspanningen ter ontwikkeling van het cyberdefensievermogen teneinde de interoperabiliteit te bevorderen, toekomstige aanvallen beter te kunnen voorkomen en hier beter op te kunnen reageren; pleit ervoor om dergelijke projecten uit te voeren in samenwerking met NAVO-bondgenoten en andere partners die ruime ervaring hebben bij het afslaan van cyberaanvallen ter bevordering van de operationele paraatheid en de ontwikkeling van gemeenschappelijke procedures en normen om zo verschillende cyberdreigingen grondig aan te kunnen pakken; is in dit opzicht ingenomen met de deelname van de EU aan cyberoefeningen zoals "CODE" (Cyber Offence and Defence Exercise);

32. herinnert eraan dat een weerbare cyberspace een feilloze cyberhygiëne vereist; verzoekt alle publieke en particuliere belanghebbenden voor al hun medewerkers regelmatig opleidingen op het gebied van cyberhygiëne te organiseren;

33. pleit voor de intensivering van de uitwisseling van deskundigheid en geleerde lessen tussen strijdkrachten, politiediensten en andere overheidsdiensten van de lidstaten die zich actief bezighouden met de bestrijding van cyberdreigingen;

Samenwerking tussen de EU en de NAVO op het gebied van cyberdefensie

34. herhaalt dat de EU en de NAVO op basis van hun gemeenschappelijke waarden en strategische belangen een bijzondere verantwoordelijkheid en daarnaast ook het vermogen hebben om de toenemende cyberveiligheids- en cyberdefensieproblemen doelmatiger en in hechte samenwerking aan te pakken door te zoeken naar mogelijke complementariteit en daarbij dubbel werk te vermijden en elkaars afzonderlijke verantwoordelijkheden te eerbiedigen;

Woensdag 13 juni 2018

35. verzoekt de Raad met andere betrokken EU-instellingen en -structuren samen te werken om zo snel mogelijk manieren te vinden om ondersteuning te bieden op communautair niveau en om het cyberdomein op geharmoniseerde wijze en in nauwe samenwerking met de NAVO in de militaire doctrine van de lidstaten op te nemen;

36. pleit voor de tenuitvoerlegging van de reeds toegezegde maatregelen; pleit voor nieuwe initiatieven voor verdere samenwerking tussen de EU en de NAVO, waarbij tevens de mogelijkheden voor samenwerking met het Kenniscentrum voor cyberdefensie van de NAVO (CCD COE), alsmede met de Academie voor communicatie en informatie van de NAVO (NCI) in overweging moeten worden genomen, met als doel opleidingen op het gebied van het cyberdefensievermogen met betrekking tot IT- en cybersystemen, wat betreft software en hardware, te bevorderen; merkt op dat hiertoe ook een dialoog met de NAVO moet worden gevoerd over de mogelijke deelname van de EU aan het Kenniscentrum om zo de complementariteit en samenwerking te bevorderen; is ingenomen met de recente oprichting van het Europees Kenniscentrum voor de bestrijding van hybride dreigingen; spoort alle betrokken instellingen en bondgenoten aan regelmatig hun werkzaamheden te bespreken teneinde overlappingen te voorkomen en een gecoördineerde aanpak ten aanzien van cyberdefensie te bevorderen; is van mening dat het van cruciaal belang is om, op basis van wederzijds vertrouwen, de uitwisseling van informatie over cyberdreigingen tussen de EU-lidstaten en met de NAVO te bevorderen;

37. is ervan overtuigd dat meer samenwerking tussen de EU en de NAVO op het gebied van cyberdefensie belangrijk en nuttig is voor het voorkomen, identificeren en beletten van cyberaanvallen; verzoekt beide partijen derhalve hun operationele samenwerking en coördinatie te bevorderen en hun gezamenlijke inspanningen ter ontwikkeling van het cyberdefensievermogen te intensiveren, met name in de vorm van gezamenlijke oefeningen en opleidingen voor civiele en militaire werknemers in de cyberdefensiesector, en via de deelname van lidstaten aan NAVO-projecten op het gebied van slimme defensie; acht het van cruciaal belang dat de EU en de NAVO de uitwisseling van informatie intensiveren zodat cyberaanvallen formeel aan bepaalde partijen kunnen worden toegeschreven en restrictieve maatregelen kunnen worden vastgesteld tegen deze partijen; spoort beide partijen aan om nauwer samen te werken, onder meer waar het de cybergerelateerde aspecten van crisisbeheersing betreft;

38. is ingenomen met de uitwisseling van ideeën met als doel de vereisten en normen op het gebied van cyberdefensie op te nemen in de planning en uitvoering van missies en operaties ter bevordering van de interoperabiliteit, en spreekt de hoop uit dat deze aanpak wordt gevolgd door een hechtere operationele samenwerking om de cyberdefensie tijdens deze missies te waarborgen, alsook de afstemming van operationele strategieën;

39. is ingenomen met de regeling tussen het computercrisisteam van de EU (EU Computer Emergency Response Team, CERT-EU) en dat van de NAVO (NATO Computer Incident Response Capability, NCIRC), waarmee wordt beoogd de uitwisseling van informatie, logistieke steun, gedeelde dreigingsanalyses, personeelswerving en beste praktijken te vergemakkelijken zodat dreigingen in real time kunnen worden aangepakt; benadrukt dat het van belang is om informatie-uitwisseling tussen het CERT-EU en NCIRC te stimuleren en het wederzijdse vertrouwen te bevorderen; is van mening dat de informatie waar het CERT-EU over beschikt van nut kan zijn voor onderzoek op het gebied van cyberbeveiliging en voor de NAVO en dat deze informatie derhalve moet worden gedeeld, mits volledig aan de EU-wetgeving inzake gegevensbescherming wordt voldaan;

40. is ingenomen met de samenwerking tussen de twee instanties met betrekking tot oefeningen op het gebied van cyberdefensie; neemt kennis van de deelname van EU-vertegenwoordigers aan de jaarlijkse "Cyber Coalition"-oefening; neemt daarnaast kennis van de vooruitgang die via de deelname van de EU aan de parallelle en gecoördineerde oefeningen (PACE) van 2017, als onderdeel van de crisisbeheersingsoefening van 2017 van de NAVO, is geboekt, en is in het bijzonder ingenomen met het daaraan toegevoegde cyberdefensie-onderdeel; verzoekt beide instanties met klem deze inspanningen te intensiveren;

41. verzoekt de EU en de NAVO met klem periodieke oefeningen op strategisch niveau te organiseren en de politieke leiders van beide instellingen daaraan te laten deelnemen; is in dit verband ingenomen met de Estische "EU CYBRID 2017"-oefening, waarbij voor het eerst aan een EU-oefening werd deelgenomen door de secretaris-generaal van de NAVO;

42. verzoekt beide instellingen met klem om bij de volgende toetsing van de tenuitvoerlegging van de gezamenlijke verklaring bestaande maatregelen concreet en doeltreffend uit te voeren en met ambitieuzere voorstellen te komen; verzoekt beide instellingen met klem om alle reeds bestaande maatregelen daadwerkelijk in de praktijk ten uitvoer te leggen en om bij de volgende toetsing van de tenuitvoerlegging van de gezamenlijke verklaring met ambitieuzere voorstellen te komen;

43. is verheugd over het in 2014 opgerichte NATO Industry Cyber Partnership (NICP) en verzoekt de EU een bijdrage te leveren aan de inspanningen in het kader van het NICP teneinde de gezamenlijke inspanningen van de NAVO en de EU te koppelen aan de inspanningen van vooraanstaande partijen uit de industrie die gespecialiseerd zijn in cybertechnologieën, om zo de cyberveiligheid te bevorderen door middel van een blijvende samenwerking die specifiek gericht is op: opleidingen, oefeningen en onderwijs voor vertegenwoordigers van de NAVO, de EU en de industrie, de deelname van de EU en de industrie aan NAVO-projecten op het gebied van slimme defensie, de uitwisseling van informatie en beste praktijken tussen de NAVO, de EU en de industrie met het oog op paraatheid en herstel, het leveren van inspanningen gericht op de gezamenlijke ontwikkeling van het cyberdefensievermogen, en in voorkomend geval het waarborgen van een gezamenlijke aanpak van cyberincidenten;

44. neemt kennis van de lopende werkzaamheden inzake het voorstel voor een verordening tot herziening van de Enisa-verordening ((EU) nr. 526/2013) en tot vaststelling van een Europees kader voor ICT-beveiligingscertificering en -etikettering; verzoekt het Enisa een overeenkomst met de NAVO aan te gaan ter bevordering van de praktische samenwerking tussen de partijen, met inbegrip van de uitwisseling van informatie en deelname aan oefeningen op het gebied van cyberdefensie;

Internationale normen met betrekking tot cyberspace

45. pleit voor de sectoroverschrijdende opname van cybercapaciteit in het externe optreden en het GBVB van de EU en haar lidstaten, en voor nauwere samenwerking tussen de lidstaten, de EU-instellingen, de NAVO, de Verenigde Naties, de Verenigde Staten en andere strategische partners, met name wat regels, normen en handhavingsmaatregelen op het gebied van cyberspace betreft;

46. betreurt het dat de VN-groep van regeringsdeskundigen (UN GGE) 2016-2017 na maanden van onderhandelingen niet tot een nieuw consensusverslag heeft kunnen komen; herinnert eraan dat het bestaande internationaal recht, en met name het Handvest van de Verenigde Naties, waarin bedreiging met of het gebruik van geweld tegen de politieke onafhankelijkheid van een staat, met inbegrip van dwingende cyberoperaties die tot doel hebben de technische infrastructuur te verstoren die nodig is voor het uitvoeren van officiële participatieve procedures, waaronder verkiezingen, in een andere staat, verboden wordt, van toepassing is en in cyberspace moet worden gehandhaafd, zoals ook in het verslag van 2013 is vastgesteld; merkt op dat het verslag van de UN GGE van 2015 een reeks normen voor verantwoordelijk staatsgedrag bevat, met inbegrip van het verbod voor landen om bewust bij te dragen aan cyberactiviteiten die krachtens internationale bepalingen in strijd zijn met de verplichtingen van de desbetreffende landen, of deze zelf uit te voeren; doet een beroep op de EU om een leidende rol op zich te nemen in het lopende en toekomstige debat over en bij de tenuitvoerlegging van internationale normen met betrekking tot cyberspace;

47. merkt op dat het Handboek van Tallinn 2.0 een basis biedt voor discussie over en analyse van de manier waarop het bestaande internationaal recht in cyberspace kan worden toegepast; roept de lidstaten op de door de deskundigen in het Handboek van Tallinn vastgelegde bevindingen te analyseren en toe te passen, en verdere vrijwillige normen voor internationaal gedrag vast te stellen; merkt in het bijzonder op dat het offensief gebruik van het cybervermogen gegrond moet zijn op het internationaal recht;

48. bevestigt zijn volledige toewijding aan een open, vrije, stabiele en veilige cyberspace, onder eerbiediging van de kernwaarden van democratie, mensenrechten en de rechtsstaat, en waarbij internationale geschillen op vreedzame wijze worden beslecht op basis van het Handvest van de Verenigde Naties en de internationale rechtsbeginselen; verzoekt de lidstaten de verdere tenuitvoerlegging van de gemeenschappelijke en alomvattende EU-aanpak voor cyberdiplomatie en bestaande cybernormen te bevorderen, en samen met de NAVO op EU-niveau criteria en definities vast te stellen om duidelijk te maken wat een cyberaanval precies inhoudt zodat de EU sneller tot een gezamenlijk standpunt kan komen in het geval van een volgens het internationaal recht onrechtmatige handeling in de vorm van een cyberaanval; ondersteunt nadrukkelijk de tenuitvoerlegging van de in het verslag van de UN GGE van 2015 vastgelegde vrijwillige, vrijblijvende normen voor verantwoordelijk staatsgedrag in cyberspace, met eerbiediging van de privacy en grondrechten van de burgers, en pleit tevens voor vaststelling van regionale maatregelen ter bevordering van het vertrouwen; ondersteunt in dit kader de werkzaamheden van de Global Commission on the Stability for Cyberspace (wereldcommissie voor stabiliteit in cyberspace), die gericht zijn op de opstelling van voorstellen voor normen en beleidsmaatregelen ter bevordering van de internationale veiligheid en stabiliteit, alsook van verantwoordelijk gedrag van (niet-)overheidsactoren in cyberspace; steunt het voorstel waarin wordt gesteld dat zowel overheids- als niet-overheidsactoren geen activiteiten mogen uitvoeren of bewust mogen toestaan wanneer deze activiteiten tot doel hebben de algemene beschikbaarheid of integriteit van de openbare kernfuncties van het internet, en daarmee de stabiliteit van cyberspace, doelbewust en ernstig aan te tasten;

49. erkent dat het grootste deel van de technologische infrastructuur eigendom is van of beheerd wordt door de particuliere sector en dat nauwe samenwerking en overleg met, alsook de inclusie van, de particuliere sector en groepen uit het maatschappelijk middenveld door middel van een dialoog tussen de diverse belanghebbenden daarom van essentieel belang zijn voor het waarborgen van een open, vrije, stabiele en veilige cyberspace;

50. realiseert zich dat bilaterale overeenkomsten tussen landen vanwege handhavingsproblemen niet altijd de gewenste resultaten opleveren; is derhalve van mening dat er coalities moeten worden gevormd binnen groepen van gelijkgestemde landen die bereid zijn om met elkaar in overleg te treden, om op doeltreffende wijze de inspanningen van de diverse belanghebbenden op dit gebied aan te vullen; benadrukt het belang van de rol van lokale overheden bij het proces van technologische innovatie en bij het delen van gegevens om de bestrijding van criminaliteit en terroristische activiteiten te versterken;

51. is verheugd over de vaststelling door de Raad van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten, het zogeheten EU-instrumentarium voor cyberdiplomatie; steunt de mogelijkheid dat de EU restrictieve maatregelen neemt tegen tegenstanders die cyberaanvallen tegen de lidstaten uitvoeren, met inbegrip van het opleggen van sancties;

52. pleit daarnaast voor een duidelijke, proactieve strategie voor cyberveiligheid en -defensie en voor de algemene versterking van het vermogen en de instrumenten van de EU met betrekking tot cyberdiplomatie als sectoroverschrijdende taak in het buitenlands beleid van de EU, zodat de normen en waarden van de EU op doeltreffende wijze kunnen worden bevorderd en wereldwijd overeenstemming kan worden bereikt over regels, normen en handhavingsmaatregelen met betrekking tot cyberspace; merkt op dat het bevorderen van de cyberweerbaarheid in derde landen een bijdrage levert aan de internationale vrede en veiligheid, en uiteindelijk ook aan de veiligheid van de Europese burgers;

53. is van mening dat cyberaanvallen als NotPetya en WannaCry vanuit overheden worden aangestuurd of plaatsvinden met medeweten en goedkeuring van overheden; merkt op dat deze cyberaanvallen, die blijvende economische schade veroorzaken en een levensgevaarlijke dreiging vormen, een duidelijke schending zijn van het internationaal recht en de rechtsnormen; is van mening dat de cyberaanvallen NotPetya en WannaCry schendingen van het internationaal recht betreffen waar respectievelijk de Russische Federatie en Noord-Korea voor verantwoordelijk zijn, en dat hier een evenredige en passende respons vanuit de EU en de NAVO op moet volgen;

54. pleit ervoor dat het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol een centraal punt voor wetshandhavingsafdelingen en overheidsorganen wordt, dat zich specifiek bezighoudt met cybercriminaliteit en met name verantwoordelijk is voor de beveiliging van zowel de .eu-domeinen als de vitale infrastructuur van de EU-netwerken tijdens een aanval; benadrukt dat een dergelijk centraal punt ook gemachtigd moet zijn om informatie uit te wisselen en lidstaten van steun te voorzien;

55. benadrukt het belang van de ontwikkeling van normen met betrekking tot privacy en beveiliging, encryptie, haatuitingen, desinformatie en terroristische dreigingen;

56. beveelt alle EU-lidstaten aan de verplichting aan te gaan om andere lidstaten die slachtoffer worden van een cyberaanval bij te staan en in nauwe samenwerking met de NAVO toe te zien op de waarborging van verantwoordingsplicht op het gebied van cyberveiligheid op nationaal niveau;

Civiel-militaire samenwerking

57. roept alle belanghebbenden op om de vorming van partnerschappen voor uitwisseling van kennis te stimuleren, de juiste bedrijfsmodellen toe te passen en vertrouwen te scheppen tussen bedrijven, defensie en civiele eindgebruikers, alsmede om de omzetting van academische kennis in praktische oplossingen te bevorderen, teneinde synergieën en overbruggingsoplossingen te vormen tussen de civiele en militaire markt voor cyberbeveiliging – in wezen een Europese eengemaakte markt voor cyberbeveiliging en producten op dit gebied – op basis van transparante procedures en met eerbiediging van het EU- en internationaal recht met het oog op de instandhouding en versterking van de strategische autonomie van de EU; wijst op de sleutelrol die particuliere cyberbeveiligingsbedrijven spelen bij het vroegtijdig waarschuwen voor cyberaanvallen en het aanwijzen van de partijen die verantwoordelijk zijn voor deze aanvallen;

58. benadrukt met klem het belang van onderzoek en ontwikkeling, met name in het licht van de strenge eisen met betrekking tot veiligheid in de defensiemarkt; verzoekt de EU en de lidstaten met klem om meer praktische ondersteuning te bieden aan de Europese cyberveiligheidssector en andere betrokken economische actoren en om de bureaucratische lasten te verminderen, met name voor kmo's en start-ups (belangrijke bronnen van innovatieve oplossingen op het gebied van cyberdefensie), en om nauwere samenwerking met instanties voor universiteitsonderzoek en andere belangrijke spelers te bewerkstelligen, teneinde de afhankelijkheid van externe bronnen voor cyberdefensieproducten te minimaliseren en een strategische voorzieningsketen binnen de EU op te zetten; merkt in dit verband op dat het Europees Defensiefonds en andere instrumenten in het kader van het meerjarig financieel kader (MFK) een waardevolle bijdrage kunnen leveren;

59. spoort de Commissie aan cyberdefensie-elementen te integreren in een netwerk van Europese onderzoeks- en kenniscentra voor cyberbeveiliging, mede teneinde in voldoende middelen te voorzien voor het tweeledige gebruik van cybercapaciteit en cybertechnologieën binnen het volgende MFK;

60. merkt op dat de bescherming van essentiële publieke en andere civiele infrastructuur, en met name informatiesystemen en de bijbehorende gegevens, een cruciale defensietaak is voor de lidstaten, en in het bijzonder voor de instanties die belast zijn met de beveiliging van informatiesystemen, en dat deze defensietaak onder de bevoegdheden van nationale cybercommando's of dergelijke instanties moet vallen; benadrukt dat hiervoor wederzijds vertrouwen en zo nauw mogelijke samenwerking tussen militaire actoren, agentschappen voor cyberdefensie, andere relevante autoriteiten en de betrokken sectoren nodig zijn, wat enkel kan worden bereikt door de taken, rollen en verantwoordelijkheden van civiele en militaire actoren duidelijk te definiëren, en verzoekt alle belanghebbenden met klem dit bij hun planningsprocessen in aanmerking te nemen; pleit voor meer grensoverschrijdende samenwerking inzake wetshandhaving gericht op de bestrijding van kwaadwillige cyberactiviteiten, met volledige inachtneming van de EU-wetgeving inzake gegevensbescherming;

61. verzoekt alle lidstaten om hun nationale strategieën inzake cyberveiligheid toe te spitsen op de bescherming van hun informatiesystemen en daarmee samenhangende gegevens en om de bescherming van deze cruciale infrastructuur te beschouwen als onderdeel van hun zorgplicht; dringt er bij de lidstaten op aan om strategieën, richtsnoeren en instrumenten aan te nemen en toe te passen die redelijke beschermingsniveaus bieden tegen redelijkerwijs identificeerbare dreigingen, waarbij de kosten en lasten van deze bescherming evenredig dienen te zijn aan de vermoedelijke schade voor de betrokken partijen; verzoekt de lidstaten om de nodige stappen te zetten teneinde rechtspersonen onder hun bevoegdheid te verplichten de aan hen toevertrouwde persoonsgegevens te beschermen;

62. is zich ervan bewust dat het vanwege de ontwikkelingen op het gebied van cyberdreigingen mogelijk verstandig is nauwer en op gestructureerdere wijze samen te werken met de politiediensten, met name op cruciale terreinen als de opsporing van dreigingen onder de noemer van de cyberjihad, cyberterrorisme, radicalisering via het internet en de financiering van extremistische of radicale organisaties;

63. dringt aan op nauwe samenwerking tussen de EU-agentschappen, zoals het EDA, het Enisa en het Europees Centrum voor de bestrijding van cybercriminaliteit, in de vorm van een sectoroverschrijdende benadering ter bevordering van synergieën en ter voorkoming van overlappingen;

64. verzoekt de Commissie een stappenplan voor een gecoördineerde aanpak van de Europese cyberdefensie te ontwikkelen en het EU-beleidskader voor cyberdefensie verder bij te werken om ervoor te zorgen dat dit beleidsmechanisme geschikt blijft voor het beoogde doel: de verwezenlijking van de doelstellingen van de EU op het gebied van cyberdefensie, dit alles in nauwe samenwerking met de lidstaten, het EDA, het Parlement en de EDEO; merkt op dat dit onderdeel moet zijn van een bredere strategische benadering ten aanzien van het GVDB;

65. pleit voor de ontwikkeling van het cyberdefensievermogen via onwikkelingssamenwerking en onderwijs en bewustwordingstrainingen over cyberveiligheid, waarbij rekening moet worden gehouden met het feit dat er in de komende jaren, voornamelijk in ontwikkelingslanden, miljoenen nieuwe internetgebruikers bij zullen komen en het dan ook zaak is de weerbaarheid van deze landen en gemeenschappen tegen hybride dreigingen en cyberdreigingen te verhogen;

66. pleit voor de totstandbrenging van internationale samenwerking en multilaterale initiatieven voor het creëren van sterke kaders voor cyberdefensie en cyberbeveiliging ter bestrijding van de "gijzeling" van staten in de vorm van corruptie, financiële fraude, witwaspraktijken en de financiering van terrorisme, alsook om de problemen als gevolg van cyberterrorisme, het gebruik van cryptovaluta en andere betaalmethoden aan te pakken;

67. wijst erop dat cyberaanvallen als NotPetya zich razendsnel verspreiden en zo willekeurig schade kunnen aanrichten indien de mondiale weerbaarheid tegen dergelijke aanvallen niet wordt versterkt; is van mening dat opleidingen en onderwijs op het gebied van cyberdefensie deel moeten uitmaken van het externe optreden van de EU, en dat het bevorderen van de cyberweerbaarheid in derde landen een bijdrage levert aan de internationale vrede en veiligheid, en uiteindelijk ook aan de veiligheid van de Europese burgers;

Institutionele versterking

68. roept de lidstaten op zich in te zetten voor een ambitieuzere samenwerking met betrekking tot cyberveiligheid in het kader van PESCO; pleit ervoor dat de lidstaten een nieuw PESCO-samenwerkingsprogramma op het gebied van cyberveiligheid te ontwikkelen ter ondersteuning van de snelle en doeltreffende planning van en bevelvoering en controle over huidige en toekomstige EU-operaties en -missies; wijst erop dat dit een beter gecoördineerde operationele capaciteit in cyberspace zou opleveren en mogelijk tot de ontwikkeling van een gemeenschappelijk cyberdefensiecommando zou leiden, mocht de Europese Raad hiertoe besluiten;

69. verzoekt nogmaals de lidstaten en de VV/HV een EU-witboek over veiligheid en defensie uit te brengen; verzoekt de lidstaten en de VV/HV cyberdefensie en -afschrikking als hoofdthema's voor dit witboek te gebruiken, waarbij zowel de bescherming van het cyberdomein als bedoeld in artikel 43 VEU aan bod komt, als de gemeenschappelijke defensie als bedoeld in artikel 42, lid 7, VEU;

70. wijst erop dat het nieuwe PESCO-samenwerkingsprogramma op het gebied van cyberveiligheid op basis van een rouleersysteem moet worden geleid door hooggeplaatste militaire en civiele medewerkers vanuit elke lidstaat, en verantwoording moet afleggen aan zowel de ministers van Defensie van de EU-landen die deelnemen aan PESCO als aan de VV/HV, teneinde vertrouwen te creëren bij de lidstaten en EU-instellingen en -agentschappen wanneer informatie en inlichtingen worden uitgewisseld;

71. pleit nogmaals voor de totstandbrenging van een EU-defensieraad bestaande uit de huidige ministeriële stuurgroep van het EDA en de ministers van defensie van de EU-landen die deelnemen aan PESCO ter bevordering van het stellen van prioriteiten, de inzet van middelen, en doeltreffende samenwerking en integratie tussen de lidstaten;

72. herinnert eraan dat het Europees Defensiefonds in het volgende MFK moet worden voortgezet of zelfs moet worden geïntensiveerd, en dat er voldoende middelen voor cyberdefensie moeten worden gereserveerd;

73. pleit ervoor dat er meer middelen worden ingezet voor het moderniseren en stroomlijnen van cyberveiligheid en de uitwisseling van informatie tussen de EDEO/het Inlichtingen- en situatiecentrum van de Europese Unie (EU-Intcen), de Raad en de Commissie;

Publiek-private partnerschappen

74. erkent dat particuliere ondernemingen een sleutelrol spelen bij het voorkomen, identificeren en beperken van en het reageren op cyberveiligheidsincidenten, niet alleen als aanbieders van technologieën, maar ook als aanbieders van diensten buiten de IT-sector;

75. erkent dat de particuliere sector een sleutelrol speelt bij het voorkomen, identificeren en beperken van en het reageren op cyberveiligheidsincidenten, alsook bij het stimuleren van innovaties op het gebied van cyberdefensie, en pleit dan ook voor betere samenwerking met de particuliere sector om zo tot gezamenlijke inzichten te komen met betrekking tot de EU- en NAVO-vereisten en het vinden van gemeenschappelijke oplossingen te vergemakkelijken;

76. verzoekt de EU een grondige evaluatie uit te voeren van de binnen de instellingen gebruikte software, IT- en communicatieapparatuur, en infrastructuur, om zo mogelijk gevaarlijke programma's en apparatuur te elimineren en het gebruik van programma's waarvan bekend is dat ze kwaadaardig zijn, zoals Kaspersky Lab, te verbieden;

o

o o

77. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Europese Raad, de Raad, de Commissie, de vicevoorzitter van de Commissie / hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, de EU-agentschappen op het gebied van defensie en cyberbeveiliging, de secretaris-generaal van de NAVO, en de nationale parlementen van de lidstaten.