Europäisches Parlament
2014-2019

Plenarsitzungsdokument

A8-0189/2018

25.5.2018

BERICHT

über die Cyberabwehr
(2018/2004(INI))

Ausschuss für auswärtige Angelegenheiten

Berichterstatter: Urmas Paet

INHALT

Seite

ENTWURF EINER ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

zur Cyberabwehr
(2018/2004(INI))

Das Europäische Parlament,

– unter Hinweis auf den Vertrag über die Europäische Union (EUV) und den Vertrag über die Arbeitsweise der Europäischen Union (AEUV),

– unter Hinweis auf das am 28. Juni 2016 von der Vizepräsidentin der Kommission und Hohen Vertreterin der Union für Außen- und Sicherheitspolitik (VP/HR) vorgelegte Dokument mit dem Titel „Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa – Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union“,

– unter Hinweis auf die Schlussfolgerungen des Europäischen Rates vom 20. Dezember 2013, 26. Juni 2015, 15. Dezember 2016, 9. März 2017, 22. Juni 2017, 20. November 2017 und 15. Dezember 2017,

– unter Hinweis auf die Mitteilung der Kommission vom 7. Juni 2017 mit dem Titel „Reflexionspapier über die Zukunft der europäischen Verteidigung “ (COM(2017)0315),

– unter Hinweis auf die Mitteilung der Kommission vom 7. Juni 2017 mit dem Titel „Einrichtung des Europäischen Verteidigungsfonds“ (COM(2017)0295),

– unter Hinweis auf die Mitteilung der Kommission vom 30. November 2016 über den Europäischen Verteidigungs-Aktionsplan (COM(2016)0950),

– unter Hinweis auf die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 7. Februar 2013 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“ (JOIN(2013)0001),

– unter Hinweis auf die Arbeitsunterlage der Kommissionsdienststellen vom 13. September 2017 mit dem Titel „Assessment of the EU 2013 Cybersecurity Strategy“ (Bewertung der Cybersicherheitsstrategie der EU aus dem Jahr 2013) (SWD(2017)0295),

– unter Hinweis auf den EU-Politikrahmen vom 18. November 2014 für die Cyberabwehr,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 10. Februar 2015 zur Cyberdiplomatie,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 19. Juni 2017 zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“),

– unter Hinweis auf die gemeinsame Mitteilung an das Europäische Parlament und den Rat mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ (JOIN(2017)0450),

– unter Hinweis auf das „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations“[1],

– unter Hinweis auf die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union,

– unter Hinweis auf die Arbeit der Global Commission on the Stability for Cyberspace,

– unter Hinweis auf die Mitteilung der Kommission vom 28. April 2015 mit dem Titel „Die Europäische Sicherheitsagenda“ (COM(2015)0185),

– unter Hinweis auf die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 6. April 2016 an das Europäische Parlament und den Rat mit dem Titel „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union“ (JOIN(2016)0018),

– unter Hinweis auf seine Entschließung vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität[2],

– unter Hinweis auf die gemeinsame Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des NATO-Generalsekretärs vom 8. Juli 2016, auf die gemeinsamen Pakete von Vorschlägen zur Umsetzung der gemeinsamen Erklärung, die vom Rat der EU und vom NATO-Rat am 6. Dezember 2016 und 5. Dezember 2017 gebilligt wurden, sowie auf die Sachstandsberichte vom 14. Juni und 5. Dezember 2017 über die Umsetzung der Pakete,

– unter Hinweis auf seine Entschließung vom 22. November 2012 zu Cybersicherheit und Verteidigung[3],

– unter Hinweis auf seine Entschließung vom 22. November 2016 zur europäischen Verteidigungsunion[4],

– unter Hinweis auf den Vorschlag der Kommission vom 13. September 2017 für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“),

[1] Cambridge University Press, Februar 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
[2] Angenommene Texte, P8_TA(2017)0366.
[3] ABl. C 419 vom 16.12.2015, S. 145.
[4] Angenommene Texte, P8_TA(2016)0435.

– unter Hinweis auf seine Entschließung vom 13. Dezember 2017 zur Umsetzung der Gemeinsamen Außen- und Sicherheitspolitik (GASP)[1],

– unter Hinweis auf seine Entschließung vom 13. Dezember 2017 zur Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP)[2],

– gestützt auf Artikel 52 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für auswärtige Angelegenheiten (A8-0189/2018),

A. in der Erwägung, dass Herausforderungen, Bedrohungen und Angriffe im Cyberraum sowie solche hybrider Natur eine große Bedrohung für die Sicherheit, die Verteidigung, die Stabilität und die Wettbewerbsfähigkeit der EU, ihrer Mitgliedstaaten und ihrer Bürger darstellen; in der Erwägung, dass die Cyberabwehr ganz eindeutig militärischer wie auch ziviler Natur ist;

B. in der Erwägung, dass die EU und ihre Mitgliedstaaten einer beispiellosen Bedrohung in Form von politisch motivierten, staatlich geförderten Cyberangriffen sowie Cyberkriminalität und Cyberterrorismus ausgesetzt sind;

C. in der Erwägung, dass der Cyberraum vom Militär weitgehend als fünfter operativer Bereich anerkannt wird, was die Entwicklung von Kapazitäten im Bereich der Cyberabwehr ermöglicht; in der Erwägung, dass diskutiert wird, ob der Cyberraum als fünfte Dimension der Kriegsführung anerkannt werden soll;

D. in der Erwägung, dass die Beistandsklausel (Artikel 42 Absatz 7 EUV) vorsieht, dass im Falle eines bewaffneten Angriffs auf das Hoheitsgebiet eines Mitgliedstaats die anderen Mitgliedstaaten ihm alle in ihrer Macht stehende Hilfe und Unterstützung schulden; in der Erwägung, dass dies den besonderen Charakter der Sicherheits- und Verteidigungspolitik bestimmter Mitgliedstaaten unberührt lässt; in der Erwägung, dass die Beistandsklausel durch die Solidaritätsklausel (Artikel 222 AEUV) ergänzt wird, laut der die EU-Länder verpflichtet sind, gemeinsam zu handeln, wenn ein Mitgliedstaat von einem Terroranschlag, einer Naturkatastrophe oder einer vom Menschen verursachten Katastrophe betroffen ist; in der Erwägung, dass die Solidaritätsklausel den Einsatz sowohl ziviler als auch militärischer Mittel vorsieht;

E. in der Erwägung, dass die Cyberabwehr zwar nach wie vor einer der wichtigsten Zuständigkeitsbereiche der Mitgliedstaaten ist, die EU aber eine wichtige Rolle spielt, wenn eine Plattform für die europäische Zusammenarbeit geboten und sichergestellt werden soll, dass diese neuen Anstrengungen auf internationaler Ebene und im Rahmen der transatlantischen Sicherheitsarchitektur von Beginn an eng aufeinander abgestimmt werden, damit die Lücken und Ineffizienzen, die viele herkömmliche Verteidigungsbereiche kennzeichnen, gar nicht erst entstehen; in der Erwägung, dass wir mehr tun müssen, als nur unsere Zusammenarbeit und die Koordinierung zu verbessern; in der Erwägung, dass wir für eine wirksame Prävention sorgen müssen, indem die Fähigkeiten der EU in den Bereichen Aufdeckung, Abwehr und Abschreckung verbessert werden; in der Erwägung, dass es einer glaubwürdigen

[1] Angenommene Texte, P8_TA(2017)0493.
[2] Angenommene Texte, P8_TA(2017)0492.

Cyberabwehr und digitalen Abschreckung bedarf, um für die EU eine wirksame Cybersicherheit zu erreichen und gleichzeitig sicherzustellen, dass die am wenigsten vorbereiteten Staaten nicht zu leichten Zielen für Cyberangriffe werden, und in der Erwägung, dass eine solide Cyberabwehr ein notwendiger Bestandteil der GSVP und der Entwicklung der Europäischen Verteidigungsunion sein sollte; in der Erwägung, dass es im Bereich der Cyberabwehr beständig an hochqualifizierten Fachkräften mangelt; in der Erwägung, dass eine enge Abstimmung beim Schutz der Streitkräfte vor Cyberanschlägen ein notwendiger Bestandteil der Entwicklung einer wirksamen GSVP ist;

F. in der Erwägung, dass sich die EU-Mitgliedstaaten häufig Cyberangriffen ausgesetzt sehen, die von feindlich gesinnten und gefährlichen staatlichen und nichtstaatlichen Akteuren ausgehen und gegen zivile oder militärische Ziele gerichtet sind; in der Erwägung, dass die gegenwärtige Gefährdung in erster Linie auf die Zersplitterung der europäischen Strategien und Fähigkeiten im Bereich der Verteidigung zurückzuführen ist, die es ausländischen Nachrichtendiensten ermöglicht, sich die Sicherheitslücken in den IT-Systemen und -Netzen, die für die europäische Sicherheit essenziell sind, immer wieder zunutze zu machen; in der Erwägung, dass die Regierungen der Mitgliedstaaten die betroffenen Interessenträger in der Vergangenheit häufig nicht rechtzeitig informiert haben, um ihnen die Behebung der Schwachstellen in ihren Produkten und Diensten zu ermöglichen; in der Erwägung, dass die Angriffe dringende Verstärkungen und die Entwicklung offensiver und defensiver europäischer Fähigkeiten auf ziviler und militärischer Ebene erforderlich machen, um mögliche grenzüberschreitende wirtschaftliche und soziale Auswirkungen, die durch Cybervorfälle verursacht werden können, abzuwenden;

G. in der Erwägung, dass die Grenzen zwischen zivilen und militärischen Störungen im Cyberraum verschwimmen;

H. in der Erwägung, dass viele Cybervorfälle erst durch die mangelnde Widerstandsfähigkeit und Robustheit der privaten und öffentlichen Netzinfrastruktur, den mangelhaften Schutz und die unzureichende Sicherung von Datenbanken und durch andere Mängel in der kritischen Informationsinfrastruktur ermöglicht werden; in der Erwägung, dass nur wenige Mitgliedstaaten im Rahmen ihrer Sorgfaltspflicht Verantwortung für den Schutz ihrer jeweiligen Netze und Informationssysteme und der damit verbundenen Daten übernehmen, was den allgemeinen Mangel an Investitionen in Schulungen und moderne Sicherheitstechnologie und die mangelnde Entwicklung geeigneter Leitlinien erklärt;

I. in der Erwägung, dass die Rechte auf Privatsphäre und Datenschutz in der EU-Grundrechtecharta und in Artikel 16 AEUV verankert und in der am 25. Mai 2018 in Kraft getretenen Datenschutz-Grundverordnung der EU geregelt sind;

J. in der Erwägung, dass eine aktive und effiziente Cyberpolitik in der Lage sein muss, Feinde abzuschrecken sowie ihre Kapazitäten zu zerschlagen und ihrer Fähigkeit, Angriffe durchzuführen, vorzugreifen und sie zu schwächen;

K. in der Erwägung, dass der Cyberraum von verschiedenen terroristischen Vereinigungen und Organisationen als kostengünstiges Instrument zum Zwecke der Anwerbung neuer Mitglieder, der Radikalisierung und der Verbreitung terroristischer Propaganda genutzt wird; in der Erwägung, dass terroristische Vereinigungen, nichtstaatliche Akteure und

grenzüberschreitend agierende kriminelle Netze sich Cyber-Operationen bedienen, um anonym Gelder zu beschaffen, Erkenntnisse zu gewinnen und Cyber-Ableger aufzubauen, um über das Internet Terrorkampagnen zu führen, kritische Infrastruktur zum Erliegen zu bringen, zu beschädigen oder zu zerstören, Finanzsysteme anzugreifen und andere illegale Aktivitäten, die sich auf die Sicherheit der europäischen Bürger auswirken, zu verfolgen;

L. in der Erwägung, dass die Cyberabschreckung und die Cyberabwehr in Bezug auf die europäischen Streitkräfte und die kritische Infrastruktur in den Debatten über die Modernisierung der Verteidigung, die gemeinsame Verteidigung Europas, die künftige Entwicklung von Streitkräften und ihrer Einsätze sowie die strategische Autonomie der Europäischen Union zu kritischen Fragen geworden sind;

M. in der Erwägung, dass etliche Mitgliedstaaten Investitionen in beträchtlicher Höhe getätigt haben, um zur Bewältigung dieser neuen Herausforderungen und zur Verbesserung ihrer Widerstandsfähigkeit gegen Cyberangriffe personell gut ausgestattete Cyberkommandos einzurichten, dass aber noch viel mehr getan werden muss, weil es immer schwieriger wird, Cyberangriffe auf der Ebene der Mitgliedstaaten abzuwehren; in der Erwägung, dass sich die Cyberkommandos der einzelnen Mitgliedstaaten unterscheiden, was ihre offensiven bzw. defensiven Aufträge angeht; in der Erwägung, dass sich auch andere Cyberabwehrstrukturen von einem Mitgliedstaat zum anderen stark unterscheiden und häufig nach wie vor zersplittert sind; in der Erwägung, dass die Cyberabwehr und die Cyberabschreckung am besten durch Zusammenarbeit auf europäischer Ebene und in Zusammenarbeit mit unseren Partnern und Verbündeten bewältigt werden können, weil ihr Wirkungsraum weder Staats- noch Organisationsgrenzen kennt; in der Erwägung, dass die militärische und die zivile Cybersicherheit eng miteinander verbunden sind und es daher einer verstärkten Bündelung der Kräfte ziviler und militärischer Fachleute bedarf; in der Erwägung, dass Privatunternehmen auf diesem Gebiet über beträchtlichen Sachverstand verfügen, was grundlegende Fragen hinsichtlich Kontrolle und Sicherheit und bezüglich der Fähigkeit von Staaten, ihre Bürger zu schützen, aufwirft;

N. in der Erwägung, dass die Cyberabwehrfähigkeiten der EU dringend ausgebaut werden müssen, weil nicht rechtzeitig auf die Veränderungen der Cybersicherheitslandschaft reagiert wurde; in der Erwägung, dass eine rasche Reaktion und eine angemessene Vorsorge zentrale Elemente sind, um die Sicherheit in diesem Bereich zu wahren;

O. in der Erwägung, dass es sich bei der Ständigen Strukturierten Zusammenarbeit (SSZ) wie auch beim Europäischen Verteidigungsfonds um neue Initiativen handelt, die über die erforderlichen Möglichkeiten verfügen, ein Umfeld zu fördern, das Chancen für KMU und Jungunternehmen bieten kann, sowie Kooperationsprojekte im Bereich der Cyberabwehr zu unterstützen, und in der Erwägung, dass beide zur Ausgestaltung des regulatorischen und institutionellen Rahmens beitragen werden;

P. in der Erwägung, dass sich die an der SSZ beteiligenden Mitgliedstaaten verpflichtet haben, dafür zu sorgen, dass die Kooperationsbemühungen im Bereich der Cyberabwehr etwa auf dem Gebiet des Informationsaustauschs, der Ausbildung und der operativen Unterstützung weiter ausgebaut werden;

Q. in der Erwägung, dass es bei zweien der 17 für die SSZ ausgewählten Projekte um die Cyberabwehr geht;

R. in der Erwägung, dass durch den Europäischen Verteidigungsfonds die weltweite Wettbewerbsfähigkeit und der Innovationsgeist der europäischen Verteidigungsindustrie gefördert werden müssen, indem in digitale Technologien und Cybertechnologien investiert wird, und dass die Entwicklung intelligenter Lösungen vorangetrieben werden muss, indem KMU und Jungunternehmen Gelegenheiten der Beteiligung daran geboten werden;

S. in der Erwägung, dass die EDA eine Reihe von Projekten auf den Weg gebracht hat, mit denen dem Bedarf der Mitgliedstaaten, ihre Fähigkeiten im Bereich der Cyberabwehr auszubauen, unter anderem durch Aus- und Fortbildungsprojekte entsprochen werden soll, und dass zu diesen Projekten beispielsweise die Koordinierungsplattform für Schulungen und Übungen im Bereich der Cyberabwehr (CD TEXP), die Bedarfsbündelung hinsichtlich Schulungen und Übungen im Bereich der Cyberabwehr mit Unterstützung durch den Privatsektor (DePoCyTE) und das Cyber-Ranges-Projekt gehören;

T. in der Erwägung, dass es weitere laufende EU-Projekte in den Bereichen Lagebewusstsein, Erkennung von Schadprogrammen und Informationsaustausch gibt (die Malware Information Sharing Platform (MISP) und das Multi-Agent System For Advanced persistent threat Detection (MASFAD));

U. in der Erwägung, dass im Bereich der Cyberabwehr ein großer und ständig wachsender Bedarf im Bereich des Kapazitätsaufbaus und der Ausbildung besteht, der am effizientesten durch Zusammenarbeit auf Ebene der EU und der NATO gedeckt werden kann;

V. in der Erwägung, dass die Missionen und Operationen im Rahmen der GSVP wie alle modernen organisatorischen Unternehmungen stark von funktionierenden IT-Systemen abhängen; in der Erwägung, dass gegen GSVP-Missionen und -Operationen gerichtete Cyberbedrohungen auf verschiedenen Ebenen bestehen können – von der taktischen Ebene (GSVP-Missionen und -Operationen) über die operative Ebene (EU-Netze) bis hin zu der breiteren Ebene weltweiter IT-Infrastruktur;

W. in der Erwägung, dass die Führungs- und Kontrollsysteme, der Informationsaustausch und die Logistik insbesondere auf taktischer und operativer Ebene auf gesicherter und auf frei zugänglicher IT-Infrastruktur beruhen; in der Erwägung, dass diese Systeme für Personen mit unlauteren Absichten, die es auf Missionen abgesehen haben, attraktive Ziele darstellen; in der Erwägung, dass Cyberangriffe empfindliche Auswirkungen auf EU-Infrastruktur haben können; in der Erwägung, dass Cyberangriffe insbesondere für die Energieinfrastruktur der EU schwerwiegende Folgen hätten und daher verhindert werden müssen;

X. in der Erwägung, dass die Cyberabwehr in allen Phasen des Planungsprozesses für GSVP-Missionen und -Operationen selbstverständlich gebührend berücksichtigt werden sollte, dass sie einer ständigen Überwachung bedarf und dass angemessene Kapazitäten zur Verfügung stehen müssen, um sie zu einem festen Bestandteil der Missionsplanung zu machen und ununterbrochen die notwendige wichtige Unterstützung zu leisten;

Y. in der Erwägung, dass das Netzwerk des Europäischen Sicherheits- und Verteidigungskollegs (ESVK) der einzige europäische Ausbildungsanbieter für die Strukturen, Missionen und Operationen im Rahmen der GSVP ist; in der Erwägung, dass die Rolle, die es bei der Bündelung der europäischen Ausbildungskapazitäten im Cyberbereich spielt, nach aktuellen Plänen deutlich ausgebaut werden soll;

Z. in der Erwägung, dass der Cyberraum in der beim NATO-Gipfel 2016 in Warschau abgegebenen Erklärung als operativer Bereich anerkannt wurde, in dem sich die NATO genauso wirksam verteidigen muss wie in der Luft, zu Land und auf See;

AA. in der Erwägung, dass die EU und die NATO durch von der EDA und der NATO koordinierte Projekte im Bereich der Dual-Use-Forschung und durch Verbesserung der Widerstandsfähigkeit der Mitgliedstaaten gegen Cyberangriffe mittels von der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) geleisteter Unterstützung dazu beigetragen haben, die Fähigkeiten der Mitgliedstaaten im Bereich der Cyberabwehr zu verbessern;

AB. in der Erwägung, dass die NATO Operationen im Bereich der Cybersicherheit im Jahr 2014 als Bestandteil ihrer kollektiven Verteidigung etabliert hat und im Jahr 2016 den Cyberraum neben Land, Luft und See als weiteren operativen Bereich anerkannt hat; in der Erwägung, dass sich die EU und die NATO beim Aufbau ihrer Widerstandsfähigkeit gegen Cyberangriffe und ihrer Fähigkeiten im Bereich der Cyberabwehr partnerschaftlich ergänzen; in der Erwägung, dass die Cybersicherheit und die Cyberabwehr bereits eine der stärksten Säulen der Zusammenarbeit zwischen beiden Organisationen sind und ein wichtiges Gebiet darstellen, auf dem beide einzigartige Fähigkeiten haben; in der Erwägung, dass die EU und die NATO in der gemeinsamen Erklärung der EU und der NATO vom 8. Juli 2016 einer umfassenden Kooperationsagenda zugestimmt haben; in der Erwägung, dass vier von 42 Vorschlägen für eine engere Zusammenarbeit die Cybersicherheit und die Cyberabwehr betreffen und dass weitere Vorschläge auf die Bekämpfung hybrider Bedrohungen im weiteren Sinne abzielen; in der Erwägung, dass dies am 5. Dezember 2017 durch einen weiteren Vorschlag zum Thema Cybersicherheit und Cyberabwehr ergänzt wurde;

AC. in der Erwägung, dass die von den Vereinten Nationen eingesetzte Gruppe von Regierungssachverständigen für die Informationssicherheit (UNGGE) ihre letzte Verhandlungsrunde abgeschlossen hat; in der Erwägung, dass sie 2017 zwar nicht in der Lage war, einen Konsensbericht zu erstellen, die Berichte aus den Jahren 2015 und 2013 aber Gültigkeit unter anderem dahingehend haben, dass darin anerkannt wird, dass das bestehende Völkerrecht und insbesondere die Charta der Vereinten Nationen anwendbar und für die Wahrung von Frieden und Stabilität und für die Förderung eines offenen, sicheren, friedlichen und zugänglichen IKT-Umfelds essenziell sind;

AD. in der Erwägung, dass der unlängst auf den Weg gebrachte Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (die „Cyber Diplomacy Toolbox“ der EU), der auf die Entwicklung der Fähigkeiten der EU und der Mitgliedstaaten zur Beeinflussung des Verhaltens potenzieller Angreifer abzielt, den Einsatz angemessener und auch restriktiver Maßnahmen im Rahmen der GASP vorsieht;

AE. in der Erwägung, dass verschiedene staatliche Akteure – unter anderem Russland, China und Nordkorea –, aber auch von Staaten angestiftete, beauftragte oder geförderte nichtstaatliche Akteure (einschließlich organisierter krimineller Vereinigungen), Sicherheitsbehörden und Privatunternehmen immer wieder an böswilligen Cyberaktivitäten beteiligt sind, mit denen politische, wirtschaftliche oder sicherheitsrelevante Ziele verfolgt werden, wobei zu diesen Aktivitäten unter anderem Angriffe auf kritische Infrastruktur, Cyberspionage und Massenüberwachung von EU-Bürgern, die Unterstützung von Desinformationskampagnen und die Verbreitung von Schadprogrammen (Wannacry, NotPetya usw.), durch die der Zugang zum Internet und die Betriebsfähigkeit von IT-Systemen beschränkt werden, zählen; in der Erwägung, dass durch derartige Aktivitäten das Völkerrecht, die Menschenrechte und die Grundrechte der EU missachtet und verletzt und gleichzeitig die Demokratie, die Sicherheit, die öffentliche Ordnung und die strategische Autonomie der EU gefährdet werden und dass diese Aktivitäten daher eine gemeinsame Reaktion der EU wie etwa den Einsatz des Rahmens für eine gemeinsame diplomatische Reaktion der EU, einschließlich der Nutzung der in der „Cyber Diplomacy Toolbox“ vorgesehenen restriktiven Maßnahmen wie etwa im Falle von Privatunternehmen die Verhängung von Bußgeldern oder die Beschränkung des Zugangs zum Binnenmarkt nach sich ziehen sollten;

AF. in der Erwägung, dass es in der Vergangenheit bereits etliche Male derartige groß angelegte Angriffe auf IKT-Infrastruktur gegeben hat, darunter 2007 in Estland, 2008 in Georgien und gegenwärtig fast täglich in der Ukraine; in der Erwägung, dass offensiv ausgerichtete Cyberfähigkeiten in bislang ungekanntem Maße derzeit auch gegen die Mitgliedstaaten der EU und der NATO eingesetzt werden;

AG. in der Erwägung, dass Cybersicherheitstechnologien, die für den militärischen wie auch den zivilen Bereich von Bedeutung sind (sogenannte „Dual-Use-Technologien“), zahlreiche Möglichkeiten bieten, in etlichen Bereichen wie etwa bei Verschlüsselungs-, Sicherheits- und Schwachstellenmanagementtools und Systemen zum Erkennen und Verhindern von unberechtigtem Eindringen Synergieeffekte zwischen zivilen und militärischen Akteuren zu schaffen;

AH. in der Erwägung, dass sich die Entwicklung von Cybertechnologien in den kommenden Jahren auch auf neue Gebiete wie künstliche Intelligenz, das Internet der Dinge, Robotertechnik und mobile Geräte erstrecken wird und dass all diese Bereiche auch Folgen für die Sicherheit auf dem Gebiet der Verteidigung haben könnten;

AI. in der Erwägung, dass die von verschiedenen Mitgliedstaaten eingerichteten Cyberkommandos einen wesentlichen Beitrag zum Schutz grundlegender ziviler Infrastruktur leisten können, und in der Erwägung, dass Wissen im Bereich der Cyberabwehr im zivilen Bereich häufig gleichermaßen nützlich ist;

Entwicklung von Fähigkeiten im Bereich der Cyberabwehr und der Cyberabschreckung

1. betont, dass eine gemeinsame Politik und solide Kapazitäten im Bereich der Cyberabwehr eines der Kernstücke der Entwicklung der Europäischen Verteidigungsunion bilden sollten;

2. begrüßt, dass die Kommission ein Cybersicherheitspaket auf den Weg gebracht hat, um die Widerstandsfähigkeit der EU gegen Cyberangriffe und die entsprechende Abschreckung und Abwehr voranzubringen;

3. erinnert daran, dass die Cyberabwehr militärischen und zivilen Charakter hat und dass daher eine integrierte politische Vorgehensweise und eine enge Zusammenarbeit zwischen militärischen und zivilen Interessenträgern erforderlich ist;

4. fordert, dass über sämtliche Organe und Einrichtungen der EU hinweg sowie in den Mitgliedstaaten in kohärenter Weise Cyberkapazitäten entwickelt werden und dass politische und praktische Lösungen hervorgebracht werden, die erforderlich sind, um die verbleibenden politischen, rechtlichen und organisatorischen Hindernisse, die einer Zusammenarbeit im Bereich der Cyberabwehr im Wege stehen, zu beseitigen; hält es daher für äußerst wichtig, dass sich die betreffenden öffentlichen Interessenträger auf Ebene der EU und der Einzelstaaten im Bereich der Cyberabwehr regelmäßig und vermehrt austauschen und regelmäßig und intensiver zusammenarbeiten;

5. betont nachdrücklich, dass die Fähigkeiten der Mitgliedstaaten im Bereich der Cyberabwehr im Rahmen der im Entstehen begriffenen Europäischen Verteidigungsunion eine führende Rolle spielen und von Beginn an so weit wie möglich verzahnt werden sollten, um größtmögliche Effizienz zu erzielen; fordert die Mitgliedstaaten daher nachdrücklich auf, bei der Entwicklung ihrer jeweiligen Cyberabwehr unter Verfolgung eines klaren Fahrplans eng zusammenzuarbeiten, um so einen von der Kommission, dem Europäischen Auswärtigen Dienst (EAD) und der EDA koordinierten Prozess voranzubringen, durch den die Cyberabwehrstrukturen unter den Mitgliedstaaten besser aufeinander abgestimmt und verfügbare kurzfristige Maßnahmen akut umgesetzt werden sollen und der Austausch von Fachwissen gefördert werden soll; vertritt die Auffassung, dass wir ein sicheres europäisches Netz für kritische Informationen und Infrastruktur entwickeln sollten; weist darauf hin, dass solide Fähigkeiten im Bereich der Attribution wesentlicher Bestandteil einer wirksamen Cyberabwehr und Cyberabschreckung sind und dass eine wirksame Prävention die Entwicklung bedeutenden weiteren technologischen Fachwissens erfordern würde; fordert die Mitgliedstaaten nachdrücklich auf, mehr finanzielle und personelle Ressourcen und insbesondere Fachleute für Cyberforensik einzusetzen, um die Attribution von Cyberangriffen zu verbessern; betont, dass diese Zusammenarbeit auch durch den Ausbau der ENISA realisiert werden sollte;

6. nimmt zur Kenntnis, dass viele Mitgliedstaaten der Auffassung sind, dass der Besitz eigener Fähigkeiten im Bereich der Cyberabwehr für ihre nationale Sicherheitsstrategie von zentraler Bedeutung ist und einen wesentlichen Teil ihrer nationalen Souveränität ausmacht; betont jedoch, dass der Umfang an Kapazitäten und Wissen, der für wirklich umfassende und schlagkräftige Streitkräfte erforderlich ist, die das Ziel der strategischen Autonomie der EU im Cyberraum sicherstellen, wegen der Abwesenheit von Grenzen im Cyberraum von keinem Mitgliedstaat alleine geleistet werden kann und daher eine verstärkte und koordinierte Reaktion seitens aller Mitgliedstaaten auf EU-Ebene erforderlich ist; stellt in diesem Zusammenhang fest, dass die EU und ihre Mitgliedstaaten beim Aufbau von Streitkräften dieser Art unter Zeitdruck stehen und unverzüglich handeln müssen; nimmt zur Kenntnis, dass sich die EU wegen EU-Initiativen wie dem digitalen Binnenmarkt in einer guten Ausgangsposition befindet, um bei der Entwicklung europäischer Strategien zur Cyberabwehr eine führende Rolle

einzunehmen; weist erneut darauf hin, dass bei der Entwicklung der Cyberabwehr auf EU-Ebene besonderes Augenmerk auf die Fähigkeit der EU gelegt werden muss, sich selbst zu schützen; begrüßt in diesem Zusammenhang den Vorschlag für ein dauerhaftes Mandat und eine gefestigte Rolle der ENISA;

7. fordert die Mitgliedstaaten in diesem Zusammenhang nachdrücklich auf, den von der SSZ und dem Europäischen Verteidigungsfonds gebotenen Rahmen bestmöglich zu nutzen, um Kooperationsprojekte vorzuschlagen;

8. nimmt die von der EU und ihren Mitgliedstaaten auf dem Gebiet der Cyberabwehr geleistete harte Arbeit zur Kenntnis; nimmt insbesondere die Projekte der EDA im Bereich Cyber Ranges, die strategische Forschungsagenda für die Cyberabwehr und die Entwicklung einsetzbarer Cyber-Lagebewusstseinspakete für Hauptquartiere zur Kenntnis;

9. begrüßt die beiden Cyberprojekte, die im Rahmen der SSZ auf den Weg gebracht werden sollen, nämlich die Plattform für den Austausch von Informationen über die Reaktion auf Cyberbedrohungen und -vorfälle und die Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit; betont, dass diese beiden Projekte auf eine defensive Cyberpolitik ausgerichtet sind, die auf dem Austausch von Informationen über Cyberbedrohungen über eine vernetzte Plattform der Mitgliedstaaten und der Einrichtung von Teams für die rasche Reaktion auf Cybervorfälle fußt, wodurch es den Mitgliedstaaten ermöglicht wird, einander dabei zu helfen, eine hohe Widerstandsfähigkeit gegen Cyberangriffe sicherzustellen, und Cyberbedrohungen gemeinsam aufzudecken, zu erkennen und zu entschärfen; fordert die Kommission und die Mitgliedstaaten auf, auf der Grundlage der SSZ-Projekte für nationale Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit ein europäisches Team für die rasche Reaktion auf Cybervorfälle einzurichten, das zur Unterstützung der Bemühungen der teilnehmenden Mitgliedstaaten mit der Koordinierung sowie der Erkennung und Bekämpfung gemeinsamer Cyberbedrohungen betraut ist;

10. stellt fest, dass die Fähigkeit der EU, Projekte im Bereich der Cyberabwehr zu entwickeln, davon abhängt, dass Technologien, Ausrüstung, Dienste, Daten und Datenverarbeitung beherrscht werden und dass auf vertrauenswürdige Akteure aus der Branche zurückgegriffen werden kann;

11. weist erneut darauf hin, dass ein Ziel der Anstrengungen, die zur Verbesserung der Homogenität von Kommandosystemen unternommen werden, darin besteht, für die Interoperabilität der verfügbaren Kommandoinstrumente, mit denen der NATO-Länder, die nicht gleichzeitig Mitgliedstaaten der EU sind, sowie mit denen gelegentlicher Partner zu sorgen und einen reibungslosen Austausch von Informationen sicherzustellen, um den Entscheidungsprozess zu beschleunigen und vor dem Hintergrund des Cyberrisikos die Kontrolle über die Informationen zu wahren;

12. empfiehlt, Möglichkeiten zu sondieren, die Projekte im Rahmen der „Intelligenten Verteidigung“ der NATO (etwa das Projekt zur Kapazitätsentwicklung für die multinationale Cyberabwehr, die Plattform für den Austausch von Informationen über Schadprogramme (MISP) und die multinationale Aus- und Fortbildung im Bereich der Cyberabwehr (MNCDE&T)) zu ergänzen;

13. weist auf die Entwicklungen hin, die in Bereichen wie der Nanotechnologie, der künstlichen Intelligenz, Big Data, Elektronikschrott und Hochleistungsrobotik gegenwärtig stattfinden; fordert die Mitgliedstaaten und die EU nachdrücklich auf, der möglichen Ausnutzung dieser Bereiche durch feindlich gesinnte staatliche Akteure und organisierte kriminelle Vereinigungen besondere Aufmerksamkeit zu widmen; fordert, dass Schulungsmaßnahmen und Fähigkeiten, die dem Schutz vor der Entstehung ausgeklügelter krimineller Machenschaften wie etwa komplexem Identitätsbetrug und Warenfälschungen dienen, ausgebaut werden;

14. betont, dass es auf dem Gebiet der Sicherheit im Cyberraum größerer terminologischer Klarheit sowie einer umfassenden und integrierten Herangehensweise und gemeinsamer Anstrengungen bedarf, um Cyberbedrohungen und hybride Bedrohungen zu bekämpfen und extremistische und kriminelle sichere Häfen im Internet zu erkennen und zu eliminieren, indem der Informationsaustausch zwischen der EU und EU-Agenturen wie Europol, Eurojust, der EDA und der ENISA verstärkt und intensiviert wird;

15. hebt die zunehmend wichtige Funktion hervor, die der künstlichen Intelligenz sowohl bei Cyberangriffen als auch bei deren Abwehr zukommt; fordert die EU und ihre Mitgliedstaaten nachdrücklich auf, diesem Bereich im Rahmen der Forschung wie auch bei der praktischen Entwicklung ihrer Fähigkeiten im Bereich der Cyberabwehr besondere Aufmerksamkeit zu widmen;

16. betont nachdrücklich, dass beim Einsatz unbemannter Luftfahrzeuge unabhängig davon, ob sie bewaffnet sind oder nicht, zusätzliche Maßnahmen ergriffen werden sollten, um ihre mögliche Gefährdung durch Cyberangriffe zu verringern;

Cyberabwehr im Rahmen von GSVP-Missionen und -Operationen

17. betont, dass die Cyberabwehr für GSVP-Missionen und -Operationen als operative Aufgabe betrachtet und in alle GSVP-Planungsprozesse eingebunden werden sollte, wobei sichergestellt werden sollte, dass die Cybersicherheit im gesamten Planungsprozess eine ständige Erwägung bleibt, damit die Angriffsflächen für Cyberangriffe verringert werden;

18. nimmt zur Kenntnis, dass es bei der Planung einer erfolgreichen GSVP-Mission oder -Operation eines beträchtlichen Sachverstands im Bereich der Cyberabwehr sowie sicherer IT-Infrastruktur und -Netze sowohl in den operativen Hauptquartieren als auch im Rahmen der Missionen selbst bedarf, um eine genaue Bewertung der Bedrohungslage vornehmen und im Einsatz angemessenen Schutz gewähren zu können; fordert den EAD und die Mitgliedstaaten mit Hauptquartieren für GSVP-Operationen auf, den für EU-Missionen und -Operationen bereitgestellten Sachverstand im Bereich der Cyberabwehr zu stärken; stellt fest, dass eine Vorbereitung von GSVP-Missionen auf den Schutz vor Cyberangriffen nur begrenzt möglich ist;

19. betont, dass jede Planung von GSVP-Missionen und -Operationen mit einer eingehenden Bewertung der Bedrohungslage im Cyberraum einhergehen muss; stellt fest, dass die von der ENISA erstellte Klassifizierung eine geeignete Vorlage für eine Bewertung dieser Art bietet; empfiehlt, dass für die GSVP-Hauptquartiere Kapazitäten zur Bewertung der Widerstandsfähigkeit gegen Cyberangriffe geschaffen werden;

20. weist insbesondere darauf hin, wie wichtig es ist, die Fußabdrücke und Angriffsflächen von GSVP-Missionen und -Operationen im Netz auf das erforderliche Mindestmaß zu beschränken; fordert die an den Planungen beteiligten Personen nachdrücklich auf, dies im Planungsprozess von Anfang an zu berücksichtigen;

21. nimmt die Untersuchung der EDA zum Fortbildungsbedarf zur Kenntnis, bei der sich im Bereich der Cyberabwehr enorme Lücken bei den Fertigkeiten und Kompetenzen der Entscheidungsträger nicht nur in den Mitgliedstaaten gezeigt haben, und begrüßt die Initiativen, die die EDA zur Fortbildung ranghoher Entscheidungsträger in den Mitgliedstaaten zur Unterstützung der Planung von GSVP-Missionen und -Operationen ergriffen hat;

Aus- und Fortbildungsmaßnahmen im Bereich der Cyberabwehr

22. stellt fest, dass durch ein EU-weit vereinheitlichtes Angebot an Aus- und Fortbildungsmaßnahmen im Bereich der Cyberabwehr Bedrohungen deutlich abgeschwächt werden könnten, und fordert die EU und die Mitgliedstaaten auf, ihre Zusammenarbeit im Bereich Aus- und Fortbildungs- sowie Übungsmaßnahmen zu verstärken;

23. unterstützt nachdrücklich das militärische Erasmus-Programm und andere gemeinsame Initiativen in den Bereichen Schulung und Austausch, die darauf abzielen, die Interoperabilität der Streitkräfte der Mitgliedstaaten und den Aufbau einer gemeinsamen Strategiekultur durch einen verstärkten Austausch von jungen Militärangehörigen zu erhöhen, wobei nicht außer Acht gelassen werden darf, dass eine solche Interoperabilität zwischen allen Mitgliedstaaten und NATO-Bündnispartnern erforderlich ist; vertritt die Ansicht, dass der Austausch zu Aus- und Fortbildungszwecken im Bereich der Cyberabwehr über diese Initiative hinausgehen und sich auf Militärangehörige aller Altersgruppen und Ränge sowie Studierende aller akademischen Einrichtungen, die Ausbildungsprogramme zur Cybersicherheit anbieten, erstrecken sollte;

24. betont, dass im Bereich der Cyberabwehr mehr Fachkräfte benötigt werden; fordert die Mitgliedstaaten auf, die Zusammenarbeit zwischen zivilen akademischen Einrichtungen und Militärakademien zu erleichtern, um diese Lücke zu schließen und so mehr Möglichkeiten auf dem Gebiet der Aus- und Fortbildungsmaßnahmen im Bereich der Cyberabwehr zu schaffen, und mehr Ressourcen für Spezialschulungen im Bereich der Cyberoperationen einschließlich Schulungen zur künstlichen Intelligenz bereitzustellen; fordert die Militärakademien auf, die Schulung im Bereich der Cyberabwehr in ihre Lehrpläne aufzunehmen und so dazu beizutragen, den Pool von Talenten im Bereich der Computer- und Netzsicherheit, die für GSVP-Missionen benötigt werden, zu vergrößern;

25. fordert alle Mitgliedstaaten auf, Unternehmen, Schulen und Bürger hinreichend und aktiv über die Cybersicherheit und die größten digitalen Bedrohungen aufzuklären bzw. das Bewusstsein dafür zu schärfen und dazu zu beraten; begrüßt in diesem Zusammenhang Leitfäden zur Computer- und Netzsicherheit, mit deren Hilfe den Bürgern und Organisationen bessere Strategien im Bereich der Cybersicherheit nahegebracht werden, das entsprechende Wissen vertieft und die Widerstandsfähigkeit in diesem Bereich durchgehend verbessert werden kann;

26. stellt fest, dass die Mitgliedstaaten angesichts des Umstands, dass mehr Fachkräfte benötigt werden, nicht ausschließlich auf die Rekrutierung kompetenter Angehöriger der Streitkräfte, sondern auch auf die Bindung des benötigten Fachpersonals setzen sollten;

27. begrüßt, dass elf Mitgliedstaaten des Projekts „Cyber Ranges Federation“ (Belgien, Deutschland, Estland, Finnland, Griechenland, Irland, Lettland, die Niederlande, Österreich, Portugal und Schweden) das erste von vier Cyberabwehrprojekten, die im Rahmen der Agenda der EDA zur Bündelung und gemeinsamen Nutzung auf den Weg gebracht wurden, umgesetzt haben; fordert die übrigen Mitgliedstaaten auf, sich dieser Initiative anzuschließen; fordert die Mitgliedstaaten auf, einander vermehrt Schulungsangebote im Bereich der virtuellen Cyberabwehr anzubieten und Cyber Ranges zur Verfügung zu stellen; weist in diesem Zusammenhang darauf hin, dass auch der Rolle der ENISA und ihrer Fachkompetenz Rechnung getragen werden sollte;

28. vertritt die Auffassung, dass derartige Initiativen dazu beitragen, die Ausbildungsqualität im Bereich der Cyberabwehr auf EU-Ebene insbesondere durch die Schaffung breit angelegter technischer Plattformen und die Etablierung einer Gemeinschaft von EU-Sachverständigen zu verbessern; vertritt die Ansicht, dass die europäischen Streitkräfte ihre Attraktivität erhöhen und Talente im Bereich der Computer- und Netzsicherheit anwerben und binden können, wenn sie umfassende Schulungsangebote im Bereich der Cyberabwehr anbieten; betont, dass Schwachstellen in den Computersystemen der Mitgliedstaaten und der Organe der EU aufgedeckt werden müssen; weist darauf hin, dass menschliches Versagen zu den häufigsten Schwachstellen in Cybersicherheitssystemen zählt, und fordert daher, dass sowohl das Militär- als auch das Zivilpersonal, das für die Organe der EU tätig ist, auf diesem Gebiet regelmäßig geschult wird;

29. fordert die EDA auf, die Koordinierungsplattform für die Ausbildung und Übungen im Bereich der Cyberabwehr (CD TEXP) zur Unterstützung der „Cyber Ranges Federation“ baldmöglichst in Betrieb zu nehmen, wobei der Schwerpunkt auf einer verstärkten Zusammenarbeit zur Vereinheitlichung der Anforderungen, auf der Förderung der Forschung im Bereich der Cyberabwehr und der technologischen Innovationen und auf der gemeinsamen Unterstützung von Drittstaaten beim Aufbau ihrer Kapazitäten mit Blick auf die Widerstandsfähigkeit im Bereich der Cyberabwehr liegen sollte; fordert die Kommission und die Mitgliedstaaten auf, diese Initiativen durch ein spezielles europäisches Kompetenzzentrum für die Fortbildung im Bereich Cyberabwehr zu ergänzen, das eine Spezialisierung der aussichtsreichsten Rekruten bietet und die teilnehmenden Mitgliedstaaten bei der Fortbildung im Bereich der Cyberabwehr unterstützt;

30. begrüßt die Entwicklung der Plattform zur Aus- und Fortbildung, Evaluierung und Übung im Bereich der Cyberabwehr im Rahmen des ESVK, durch die sich die Qualität der Aus- und Fortbildungsangebote in den Mitgliedstaaten verbessern sollte;

31. fordert einen verstärkten Austausch von Lagebewusstsein, indem Simulationsübungen zur Cybersicherheit angeboten und die entsprechenden Anstrengungen zum Aufbau von Fähigkeiten koordiniert werden, die auf eine höhere Interoperabilität sowie eine bessere Prävention gegen und eine bessere Reaktion auf künftige Angriffe ausgerichtet sind; fordert, dass Projekte dieser Art mit den NATO-Bündnispartnern, den Streitkräften der

EU-Mitgliedstaaten und anderen Partnern, die über weitreichende Erfahrungen in der Abwehr von Cyberangriffen verfügen, durchgeführt werden, um die operative Einsatzbereitschaft zu stärken und gemeinsame Verfahren und Standards auszuarbeiten, damit auf die verschiedenen Cyberbedrohungen umfassend reagiert werden kann; begrüßt in diesem Zusammenhang die Beteiligung der EU an Cyberübungen wie etwa der Übung zu Cyberangriffen und -abwehr (Cyber Offence and Defence Exercise, CODE);

32. weist erneut darauf hin, dass ein widerstandsfähiger Cyberraum eine lückenlose Cyberhygiene voraussetzt; fordert alle öffentlichen und privaten Interessenträger auf, für alle Mitarbeiter regelmäßig Fortbildungen zum Thema Cyberhygiene durchzuführen;

33. empfiehlt, dass die Streitkräfte, die Polizeikräfte und andere aktiv an der Bekämpfung von Cyberbedrohungen beteiligte staatliche Stellen der Mitgliedstaaten verstärkt Fachwissen und Erfahrungen austauschen;

Zusammenarbeit der EU und der NATO im Bereich der Cyberabwehr

34. weist erneut darauf hin, dass der EU und der NATO aufgrund ihrer gemeinsamen Werte und strategischen Interessen besondere Verantwortung zukommt und sie in der Lage sind, den wachsenden Herausforderungen im Bereich der Cybersicherheit und -abwehr mit mehr Effizienz und in enger Zusammenarbeit zu begegnen, und zwar durch Ermittlung möglicher Komplementaritäten, durch Vermeidung von Doppelarbeit und unter Anerkennung der Aufgaben der jeweils anderen Seite;

35. fordert den Rat auf, mit anderen einschlägigen Organen und Strukturen der EU zusammenzuarbeiten, damit auf Unionsebene möglichst bald Unterstützung für die einheitliche Einbindung von Cyberfragen in die Militärdoktrin der Mitgliedstaaten in enger Zusammenarbeit mit der NATO geboten werden kann;

36. fordert, dass bereits beschlossene Maßnahmen in die Praxis umgesetzt werden; fordert, dass neue Initiativen sondiert werden, mit denen die Zusammenarbeit zwischen der EU und der NATO weiter vorangetrieben werden kann, wobei auch die Möglichkeiten einer Zusammenarbeit innerhalb des Kompetenzzentrums der NATO für kooperativen Schutz vor Computerangriffen (CCD COE) und der Kommunikations- und Informationsakademie der NATO berücksichtigt werden sollten, deren Ziel es ist, die Fortbildungskapazitäten im Bereich der Cyberabwehr in IT- und Cybersystemen sowohl die Software als auch die Hardware betreffend zu verstärken; weist darauf hin, dass dies auch einen Dialog mit der NATO über die mögliche partnerschaftliche Beteiligung der EU am CCD COE umfasst, durch den die Komplementarität verstärkt und die Zusammenarbeit ausgeweitet werden soll; begrüßt das neu entstandene Europäische Zentrum zur Bewältigung hybrider Bedrohungen; fordert alle einschlägigen Institutionen und Bündnispartner auf, ihre Tätigkeiten regelmäßig zu besprechen, um Überschneidungen zu vermeiden und im Bereich der Cyberabwehr eine koordinierte Vorgehensweise voranzutreiben; hält es für äußerst wichtig, auf der Grundlage des gegenseitigen Vertrauens den Austausch von Informationen zu Cyberbedrohungen unter den Mitgliedstaaten und mit der NATO zu fördern;

37. ist überzeugt, dass eine verstärkte Zusammenarbeit zwischen der EU und der NATO im Bereich der Cyberabwehr wichtig und nützlich ist, um Cyberangriffe zu verhindern und aufzudecken und Angreifer abzuschrecken; fordert daher beide Organisationen auf, ihre operative Zusammenarbeit und Koordinierung zu verstärken und ihre gemeinsamen Bemühungen zum Aufbau von Kapazitäten insbesondere in Form gemeinsamer Übungen und Fortbildungen für mit der Cyberabwehr befasstes ziviles und militärisches Personal und durch die Teilnahme der Mitgliedstaaten an NATO-Projekten im Rahmen der „Intelligenten Verteidigung“ auszubauen; vertritt die Ansicht, dass es für die EU und die NATO von wesentlicher Bedeutung ist, verstärkt nachrichtendienstliche Informationen auszutauschen, damit Cyberangriffe offiziell zugeordnet und anschließend restriktive Sanktionen gegen die Verantwortlichen verhängt werden können; fordert beide Organisationen nachdrücklich auf, auch bei den Cyberaspekten des Krisenmanagements enger zusammenzuarbeiten;

38. begrüßt, dass Konzepte ausgetauscht wurden, um Anforderungen und Normen für die Cyberabwehr in die Planung und Durchführung von Missionen und Operationen zu integrieren und dadurch die Interoperabilität zu fördern, und bringt die Hoffnung zum Ausdruck, dass darauf eine weitere operative Zusammenarbeit folgt, mit der der Aspekt der Cyberabwehr der jeweiligen Missionen und die Abstimmung der operativen Vorgehensweisen gesichert wird;

39. begrüßt die zwischen dem IT-Notfallteam der EU (CERT-EU) und der Computer Incident Response Capability der NATO (NCIRC) getroffene Vereinbarung, durch die der Austausch von Informationen, logistische Unterstützung, die gemeinsame Bewertung von Bedrohungen, die Gewinnung von Personal und der Austausch bewährter Verfahren erleichtert werden sollen, damit auf Bedrohungen in Echtzeit reagiert werden kann; betont, wie wichtig es ist, den Informationsaustausch zwischen dem CERT-EU und dem NCIRC zu verstärken und auf ein höheres Maß an Vertrauen hinzuarbeiten; geht davon aus, dass im Besitz des CERT-EU befindliche Informationen zu Forschungszwecken im Bereich der Cyberabwehr und zugunsten der NATO verwendet werden könnten und dass diese Informationen daher unter umfassender Wahrung der Datenschutzvorschriften der EU ausgetauscht werden sollten;

40. begrüßt die Zusammenarbeit zwischen den beiden Organisationen im Rahmen von Cyberabwehrübungen; weist auf die Teilnahme von EU-Vertretern an der jährlichen Übung „Cyber Coalition“ hin; erkennt den Fortschritt an, den die Beteiligung der EU über parallele und koordinierte Übungen (PACE) 17 an der NATO-Krisenmanagementübung 17 bedeutet, und begrüßt insbesondere, dass es bei der Übung auch um die Cyberabwehr ging; fordert beide Organisationen nachdrücklich auf, diese Bemühungen zu intensivieren;

41. fordert die EU und die NATO nachdrücklich auf, regelmäßig strategische Übungen unter Beteiligung der höchsten politischen Führungsebene beider Organisationen zu veranstalten; begrüßt in diesem Zusammenhang die Übung EU CYBRID 2017 in Estland als erste EU-Übung, an der auch der NATO-Generalsekretär teilnahm;

42. weist darauf hin, dass großer Spielraum für ein noch ehrgeizigeres und konkreteres Kooperationsprogramm im Bereich der Cyberabwehr vorhanden ist, das im Rahmen konkreter Operationen über die konzeptionelle Ebene der Zusammenarbeit hinausgeht; fordert beide Organisationen nachdrücklich auf, alle bereits bestehenden Pläne wirksam in die Praxis umzusetzen und ehrgeizigere Vorschläge für die nächste Überprüfung der Umsetzung der gemeinsamen Erklärung vorzulegen;

43. begrüßt die 2014 eingerichtete Branchenpartnerschaft der NATO zu Cyberfragen (NICP) und fordert, dass sich die EU an den Kooperationsbemühungen im Rahmen der NICP beteiligt, damit die Zusammenarbeit zwischen der NATO und der EU mit den Kooperationsabsichten von Branchenführern aus dem Bereich der Cybertechnologie verknüpft wird, um die Cybersicherheit über eine dauerhafte Zusammenarbeit zu stärken, wobei Folgendes den Schwerpunkt bilden sollte: Fortbildung, Übungen und Ausbildung für Vertreter der NATO, der EU und der Branche, die Einbindung der EU und der Branche in NATO-Projekte im Rahmen der „Intelligenten Verteidigung“, der wechselseitige Austausch von Informationen und bewährten Verfahren zwischen der NATO, der EU und der Branche mit Blick auf Vorsorge- und Wiederherstellungsmaßnahmen, der gemeinsame Aufbau von Kapazitäten zur Cyberabwehr und die Sicherstellung gemeinsamer Reaktionen auf Cybervorfälle, soweit zweckmäßig;

44. weist darauf hin, dass derzeit an einem Vorschlag für eine Verordnung gearbeitet wird, mit dem die Verordnung (EU) Nr. 526/2013 über die ENISA überarbeitet und ein Rahmen für die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und eine entsprechende Kennzeichnung geschaffen werden soll; fordert die ENISA auf, mit der NATO ein Übereinkommen über eine stärkere Zusammenarbeit in der Praxis zu unterzeichnen, das den Informationsaustausch und die Teilnahme an Übungen zur Cyberabwehr einschließt;

Für den Cyberraum geltende internationale Normen

45. fordert, dass die Fähigkeiten im Bereich der Cyberabwehr im Rahmen der GASP und des auswärtigen Handelns der EU und ihrer Mitgliedstaaten als Querschnittsaufgabe einen festen Platz einnehmen sollten, und fordert im Bereich der Cyberabwehr eine engere Abstimmung zwischen den Mitgliedstaaten, den EU-Organen, der NATO, den Vereinten Nationen, den Vereinigten Staaten und anderen strategischen Partnern, insbesondere was die Bestimmungen, Normen und Durchsetzungsmaßnahmen im Cyberraum anbelangt;

46. bedauert, dass es der von den Vereinten Nationen für den Zeitraum 2016–2017 eingesetzten Gruppe von Regierungssachverständigen (UNGGE) auch nach mehrmonatigen Verhandlungen nicht gelungen ist, einen neuen Konsensbericht zu erstellen; erinnert daran, dass dem Bericht aus dem Jahr 2013 zufolge das bestehende Völkerrecht und insbesondere die Charta der Vereinten Nationen – laut der die gegen die politische Unabhängigkeit eines Staates gerichtete Androhung oder Anwendung von Gewalt zu unterlassen ist, wobei hierzu auch als Druckmittel konzipierte Cyberoperationen zählen, mit denen die technische Infrastruktur, die in einem anderen Staat für auf Partizipation ausgerichtete amtliche Verfahren wie etwa Wahlen essenziell ist, zum Erliegen gebracht werden soll – gilt und auch im Cyberraum durchgesetzt werden sollte; weist darauf hin, dass der Bericht der UNGGE aus dem Jahr 2015 eine

Reihe von Normen für verantwortungsvolles staatliches Verhalten enthält, darunter das Verbot für Staaten, Cyberaktivitäten durchzuführen oder wissentlich zu unterstützen, die ihren völkerrechtlichen Verpflichtungen zuwiderlaufen; fordert die EU auf, in den laufenden und künftigen Debatten über internationale Normen im Cyberraum und bei deren Umsetzung eine Führungsrolle zu übernehmen;

47. stellt fest, dass das „Tallinn Manual 2.0“ als Grundlage für eine Debatte und als Analyse dahingehend, wie geltendes Völkerrecht auf den Cyberraum angewendet werden kann, von Bedeutung ist; fordert die Mitgliedstaaten auf, mit der Auswertung und Anwendung der Feststellungen der Sachverständigen aus dem Tallinn Manual zu beginnen und sich auf weitere freiwillige Normen für das internationale Verhalten zu verständigen; stellt insbesondere fest, dass sich jedweder offensiv ausgerichtete Einsatz von Cyberfähigkeiten auf das Völkerrecht stützen muss;

48. bekräftigt sein uneingeschränktes Bekenntnis zu einem offenen, freien, stabilen und sicheren Cyberraum, in dem die Grundwerte der Demokratie, der Menschenrechte und der Rechtsstaatlichkeit geachtet und völkerrechtliche Streitigkeiten auf der Grundlage der Charta der Vereinten Nationen und der Grundsätze des Völkerrechts mit friedlichen Mitteln beigelegt werden; fordert die Mitgliedstaaten auf, die weitere Umsetzung des gemeinsamen, umfassenden Ansatzes der EU für die Cyberdiplomatie und bestehender Normen für den Cyberraum voranzutreiben und zusammen mit der NATO auf EU-Ebene geltende Kriterien und Definitionen zu erarbeiten, um festzulegen, was einen Cyberangriff darstellt, damit die EU nach einer völkerrechtswidrigen Handlung in Form eines Cyberangriffs schneller zu einem gemeinsamen Standpunkt gelangen kann; unterstützt nachdrücklich die Umsetzung der in dem Bericht der UNGGE aus dem Jahr 2015 festgehaltenen freiwilligen, nicht bindenden Normen für ein verantwortungsvolles Verhalten der Staaten im Cyberraum, das die Wahrung der Privatsphäre und der Grundrechte der Bürger sowie die Schaffung regionaler vertrauensbildender Maßnahmen einschließt; unterstützt in diesem Zusammenhang die Arbeit der Global Commission on the Stability of Cyberspace, die mit Blick auf die Verbesserung der internationalen Sicherheit und Stabilität Vorschläge für Normen und politische Strategien ausarbeitet und eine Richtschnur für verantwortungsvolles staatliches und nichtstaatliches Verhalten im Cyberraum bieten will; unterstützt den Vorschlag, dass staatliche und nichtstaatliche Akteure keine Handlungen vornehmen oder wissentlich unterstützen sollten, mit denen die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des Internets und damit die Stabilität des Cyberraums vorsätzlich und in beträchtlichem Maße beschädigt wird;

49. nimmt zur Kenntnis, dass sich der Großteil der technologischen Infrastruktur im Besitz der Privatwirtschaft befindet oder durch diese betrieben wird und dass der engen Zusammenarbeit, Beratungen und der Einbeziehung der Privatwirtschaft und zivilgesellschaftlicher Gruppen in Form eines mehrseitigen Dialogs daher eine wesentliche Bedeutung zukommt, wenn es darum geht, einen offenen, freien, stabilen und sicheren Cyberraum zu schaffen;

50. nimmt zur Kenntnis, dass durch bilaterale Vereinbarungen zwischen einzelnen Staaten aufgrund von Schwierigkeiten bei der Durchsetzung nicht immer die erhofften Ergebnisse erzielt werden; ist daher der Ansicht, dass die Bildung von Bündnissen innerhalb von Gruppen gleichgesinnter, konsensbereiter Staaten eine wirksame Möglichkeit darstellt, die Bemühungen der unterschiedlichen Interessenträger zu

ergänzen; unterstreicht die wichtige Rolle, die den lokalen Behörden bei der technologischen Innovation und dem Austausch von Daten mit Blick auf die Verbesserung der Verbrechens- und Terrorismusbekämpfung zukommt;

51. begrüßt, dass der Rat den Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswilliger Cyberaktivitäten – die sogenannte „Cyber Diplomacy Toolbox“ der EU – angenommen hat; unterstützt die Möglichkeit für die EU, restriktive Maßnahmen einschließlich der Verhängung von Sanktionen gegen Feinde einzusetzen, die EU-Mitgliedstaaten im Cyberraum angreifen;

52. fordert darüber hinaus, dass ein klares, vorausschauendes Konzept für die Cybersicherheit und die Cyberabwehr entworfen wird und dass die Cyberdiplomatie der EU als außenpolitische Querschnittsaufgabe der EU wie auch die damit verbundenen Kapazitäten und Instrumente allgemein gestärkt werden, um die Normen und Werte der EU wirksam zu festigen und den Weg für einen weltweiten Konsens bezüglich der Regeln, Normen und Durchsetzungsmaßnahmen für den Cyberraum zu ebnen; stellt fest, dass mit dem Aufbau der Widerstandsfähigkeit gegen Cyberangriffe in Drittländern ein Beitrag zum Weltfrieden und zur internationalen Sicherheit geleistet wird, wobei dies letztlich auch der Sicherheit der Unionsbürger zuträglich ist;

53. vertritt die Auffassung, dass Cyberangriffe wie NotPetya und WannaCry entweder staatlich gelenkt sind oder mit dem Wissen eines Staates und dessen Zustimmung durchgeführt werden; stellt fest, dass diese Cyberangriffe, die schwerwiegende und nachhaltige wirtschaftliche Schäden verursachen und lebensbedrohlich sind, einen eindeutigen Verstoß gegen das Völkerrecht und Rechtsnormen darstellen; ist daher der Ansicht, dass NotPetya und WannaCry Verstöße der Russischen Föderation bzw. Nordkoreas gegen das Völkerrecht darstellen und dass die beiden Länder mit angemessenen und geeigneten Reaktionen der EU und der NATO konfrontiert werden sollten;

54. fordert, dass das Europol-Zentrum zur Bekämpfung der Cyberkriminalität zu einer Anlaufstelle für Strafverfolgungsabteilungen und Regierungsstellen wird, die im Bereich der Bekämpfung der Cyberkriminalität tätig sind, wobei die vorrangige Aufgabe des Zentrums darin bestehen sollte, bei einem Angriff die Verteidigung der auf .eu lautenden Domains und der kritischen Infrastruktur der EU-Netze zu steuern; hebt hervor, dass eine solche Anlaufstelle ebenfalls den Auftrag erhalten sollte, Informationen auszutauschen und den Mitgliedstaaten Unterstützung anzubieten;

55. betont, dass der Ausarbeitung von Normen in den Bereichen Privatsphäre und Sicherheit, Verschlüsselung, Hetze, Desinformation und terroristische Bedrohungen große Bedeutung zukommt;

56. empfiehlt, dass sich jeder Mitgliedstaat verpflichtet, jedem anderen Mitgliedstaat im Fall eines Cyberangriffs beizustehen und in enger Zusammenarbeit mit der NATO die nationale Rechenschaftspflicht in Cyberangelegenheiten sicherzustellen;

Zivil-militärische Zusammenarbeit

57. fordert alle Interessenträger auf, Partnerschaften für den Wissenstransfer zu stärken, geeignete Geschäftsmodelle einzuführen und das Vertrauen zwischen Unternehmen und Endnutzern aus dem Wehr- und dem Zivilbereich zu vertiefen sowie die Umsetzung akademischen Wissens in praktische Lösungen zu verbessern, um auf der Grundlage transparenter Verfahren und unter Einhaltung von Rechtsvorschriften der EU und des Völkerrechts Synergieeffekte zu schaffen und Lösungen zwischen dem zivilen und dem militärischen Markt zu portieren, d. h. im Wesentlichen einen Einheitsmarkt für Cybersicherheit und Cybersicherheitsprodukte zu schaffen, um auf diesem Wege die strategische Autonomie der EU zu erhalten und auszubauen; stellt fest, dass den im Bereich der Cybersicherheit tätigen Privatunternehmen eine Schlüsselrolle bei der Frühwarnung und der Attribution von Cyberangriffen zukommt;

58. betont nachdrücklich, dass Forschung und Entwicklung insbesondere in Anbetracht der hohen Sicherheitsanforderungen im Verteidigungsmarkt eine wichtige Rolle spielen; fordert die EU und die Mitgliedstaaten nachdrücklich auf, der europäischen Cybersicherheitsindustrie und anderen einschlägigen Wirtschaftsakteuren verstärkt praktische Unterstützung zukommen zu lassen, den bürokratischen Aufwand insbesondere für KMU und Jungunternehmen (die wichtigsten Entwickler innovativer Lösungen im Bereich der Cyberabwehr) zu verringern und eine engere Zusammenarbeit mit universitären Forschungseinrichtungen und großen Akteuren zu fördern, um im Bereich der Cybersicherheit die Abhängigkeit von Fremdprodukten zu reduzieren und eine strategische Lieferkette innerhalb der EU aufzubauen und so die strategische Autonomie zu verbessern; weist in diesem Zusammenhang auf den wertvollen Beitrag hin, der vom Europäischen Verteidigungsfonds und von anderen Instrumenten im Rahmen des mehrjährigen Finanzrahmens (MFR) geleistet werden kann;

59. legt der Kommission nahe, Elemente der Cyberabwehr in ein Netz europäischer Kompetenz- und Forschungszentren auf dem Gebiet der Cybersicherheit zu integrieren, auch mit Blick darauf, dass im nächsten mehrjährigen Finanzrahmen ausreichend Mittel für Cyberfähigkeiten und -technologien mit doppeltem Verwendungszweck bereitgestellt werden;

60. weist darauf hin, dass der Schutz öffentlicher und anderer kritischer ziviler Infrastrukturanlagen und insbesondere von Informationssystemen und der damit verbundenen Daten eine wesentliche Verteidigungsaufgabe für die Mitgliedstaaten und insbesondere für die mit der Sicherheit der Informationssysteme betrauten Behörden ist und dass er in den Aufgabenbereich entweder der nationalen Cyberabwehrstrukturen oder der besagten Behörden fallen sollte; betont, dass dies ein gewisses Maß an Vertrauen und eine möglichst enge Zusammenarbeit zwischen militärischen Akteuren, für die Cyberabwehr zuständigen Behörden, anderen einschlägigen Behörden und den betreffenden Wirtschaftszweigen voraussetzt, wobei dies nur gelingen kann, wenn die Pflichten, Aufgaben und Zuständigkeiten der zivilen und militärischen Akteure eindeutig festgelegt werden, und fordert alle Interessenträger nachdrücklich auf, dies in ihren Planungsprozessen zu berücksichtigen; fordert eine stärkere grenzüberschreitende Zusammenarbeit bei der Strafverfolgung böswilliger Cyberaktivitäten, wobei die Datenschutzvorschriften der EU uneingeschränkt einzuhalten sind;

61. fordert alle Mitgliedstaaten auf, ihre nationalen Strategien für die Cybersicherheit auf den Schutz der Informationssysteme und der damit verbundenen Daten auszurichten und den Schutz dieser kritischen Infrastruktur als Teil ihrer jeweiligen Sorgfaltspflicht zu betrachten; fordert die Mitgliedstaaten nachdrücklich auf, Strategien, Leitlinien und Instrumente zu beschließen und umzusetzen, die einen angemessenen Schutz vor Bedrohungen, die ohne übermäßigen Aufwand erkennbar sind, bieten, wobei die mit dem Schutz verbundenen Kosten und Belastungen im Verhältnis zu dem Schaden stehen müssen, der den betroffenen Parteien aller Voraussicht nach entsteht; fordert die Mitgliedstaaten auf, geeignete Maßnahmen zu ergreifen, um juristische Personen auf ihrem Hoheitsgebiet zum Schutz der ihnen anvertrauten personenbezogenen Daten zu verpflichten;

62. weist darauf hin, dass angesichts der im ständigen Wandel befindlichen Cyberbedrohungen vor allem in einigen kritischen Bereichen wie der Verfolgung von Bedrohungen in den Bereichen Cyber-Dschihad, Cyber-Terrorismus, Radikalisierung über das Internet und Finanzierung extremistischer oder radikaler Organisationen eine tiefergreifende und strukturiertere Zusammenarbeit mit Polizeikräften ratsam sein könnte;

63. setzt sich dafür ein, dass die Agenturen der EU – etwa die EDA, die ENISA und das Europäische Zentrum zur Bekämpfung der Cyberkriminalität – bereichsübergreifend zusammenarbeiten, um Synergieeffekte zu begünstigen und Überschneidungen zu vermeiden;

64. fordert die Kommission auf, einen Fahrplan für ein abgestimmtes Konzept für die europäische Cyberabwehr und die Aktualisierung des EU-Politikrahmens für die Cyberabwehr auszuarbeiten, damit er als einschlägiger politischer Mechanismus für die Umsetzung der Ziele der EU im Bereich der Cyberabwehr auch weiterhin seinem Zweck genügt, wobei eine enge Zusammenarbeit mit den Mitgliedstaaten, der EDA, dem Parlament und dem EAD erforderlich ist; stellt fest, dass dieses Vorgehen Teil eines umfassenderen Strategiekonzepts für die GSVP sein muss;

65. fordert, dass im Rahmen der Entwicklungszusammenarbeit Kapazitäten im Bereich der Cybersicherheit aufgebaut werden und eine kontinuierliche Aus- und Fortbildung zur Sensibilisierung für Cyberfragen angestrebt wird, weil in den kommenden Jahren vor allem in Entwicklungsländern Millionen neue Internetnutzer online gehen werden; weist darauf hin, dass dadurch die Widerstandsfähigkeit von Ländern und Gesellschaften gegenüber Cyberbedrohungen und hybriden Bedrohungen gestärkt wird;

66. fordert eine internationale Zusammenarbeit und multilaterale Initiativen, die darauf ausgerichtet sind, einen stringenten Rahmen für die Cyberabwehr und die Cybersicherheit aufzubauen, um einer Vereinnahmung von Staaten durch Korruption, Finanzbetrug, Geldwäsche und Terrorismusfinanzierung entgegenzuwirken, und die Herausforderungen zu bewältigen, die durch Cyberterrorismus und durch Kryptowährungen und andere alternative Zahlungsmethoden entstehen;

67. stellt fest, dass sich Cyberangriffe wie NotPetya rasch ausbreiten und dabei unterschiedslos Schaden anrichten, wenn weltweit keine allgemeine Widerstandsfähigkeit besteht; ist der Ansicht, dass die Aus- und Fortbildung in Sachen Cyberabwehr Teil des auswärtigen Handeln der EU sein sollte und dass mit dem Aufbau der Widerstandsfähigkeit gegen Cyberangriffe in Drittländern ein Beitrag zum Weltfrieden und zur internationalen Sicherheit geleistet wird, wobei dies letztlich auch der Sicherheit der Unionsbürger zuträglich ist;

Institutionelle Stärkung

68. fordert die Mitgliedstaaten auf, im Rahmen der SSZ eine ambitioniertere Zusammenarbeit in Cyberangelegenheiten zu verfolgen; schlägt vor, dass die Mitgliedstaaten ein neues SSZ-Programm zur Zusammenarbeit in Cyberangelegenheiten auf den Weg bringen, um die rasche und wirksame Planung, Führung und Kontrolle aktueller und künftiger EU-Operationen und -Missionen zu unterstützen; stellt fest, dass dies zu einer besseren Koordinierung operativer Fähigkeiten, die den Cyberraum betreffen, führen sollte und den Aufbau eines gemeinsamen Cyberabwehrkommandos nach sich ziehen könnte, wenn der Europäische Rat einen entsprechenden Beschluss fasst;

69. wiederholt seine an die Mitgliedstaaten und die VP/HR gerichtete Forderung, ein Weißbuch der EU zu Sicherheit und Verteidigung vorzulegen; fordert die Mitgliedstaaten und die VP/HR auf, die Cyberabwehr und die Cyberabschreckung zu einem Eckpfeiler des Weißbuches zu machen, das den Schutz des Cyberraums für Operationen nach Artikel 43 EUV und die gemeinsame Verteidigung nach Artikel 42 Absatz 7 EUV abdecken sollte;

70. stellt fest, dass das neue SSZ-Programm zur Zusammenarbeit in Cyberangelegenheiten nach einem Rotationsverfahren von hochrangigen Militärangehörigen und hochrangigem Zivilpersonal aus jedem Mitgliedstaat geleitet werden und gegenüber den Verteidigungsministern der EU in der SSZ-Zusammensetzung und gegenüber der VP/HR rechenschaftspflichtig sein sollte, damit beim Austausch von Informationen und nachrichtendienstlichen Erkenntnissen das Vertrauen unter den Mitgliedstaaten und den Organen und Agenturen der EU gefördert wird;

71. wiederholt seine Forderung nach der Einsetzung eines EU-Rates für Verteidigung, der auf dem bestehenden ministeriellen Lenkungsausschuss der EDA und dem SSZ-Format der EU-Verteidigungsminister aufbaut, damit für eine Priorisierung und die erforderliche Bereitstellung von Ressourcen sowie eine wirksame Zusammenarbeit und Verzahnung unter den Mitgliedstaaten gesorgt wird;

72. weist erneut darauf hin, dass der Europäische Verteidigungsfonds beibehalten bzw. im nächsten MFR ausgebaut werden muss, wobei ausreichend Mitteln für die Cyberabwehr zweckgebunden werden müssen;

73. fordert zusätzliche Mittel, um die Cybersicherheit und den Austausch nachrichtendienstlicher Erkenntnisse zwischen dem EAD bzw. dem Zentrum der Europäischen Union für Informationsgewinnung und -analyse (INTCEN), dem Rat und der Kommission zu modernisieren und zu optimieren;

Öffentlich-private Partnerschaften

74. stellt fest, dass privaten Unternehmen bei der Prävention, der Aufdeckung, der Eindämmung und der Reaktion in Zusammenhang mit Cybervorfällen nicht nur deshalb große Bedeutung zukommt, weil sie Technologie bereitstellen, sondern auch, weil sie über IT-Dienste hinaus auch andere Dienstleistungen erbringen;

75. stellt fest, dass die Privatwirtschaft bei der Prävention, der Aufdeckung, der Eindämmung und der Reaktion in Zusammenhang mit Cybervorfällen eine wichtige Aufgabe übernimmt und Impulsgeber für Innovationen im Bereich der Cyberabwehr ist, und fordert daher eine verstärkte Zusammenarbeit mit der Privatwirtschaft, um das gemeinsame Verständnis der Anforderungen der EU und der NATO und Hilfe bei der Suche nach gemeinsamen Lösungen sicherzustellen;

76. fordert die EU auf, die Software, die IT- und Kommunikationsgeräte sowie die entsprechenden Infrastrukturen, die in den Organen eingesetzt werden, einer umfassenden Überprüfung zu unterziehen, um die Verwendung potenziell gefährlicher Programme und Geräte auszuschließen und die Verwendung als böswillig eingestufter Programme und Geräte wie Kaspersky Lab zu verbieten;

77. beauftragt seinen Präsidenten, diese Entschließung dem Europäischen Rat, dem Rat, der Kommission, der VP/HR, den EU-Agenturen in den Bereichen Verteidigung und Cybersicherheit, dem NATO-Generalsekretär und den nationalen Parlamenten der Mitgliedstaaten zu übermitteln.

MINDERHEITENANSICHT

zu dem Entwurf eines Berichts über die Verteidigung
(2018/2004(INI))

Ausschuss für auswärtige Angelegenheiten, Berichterstatter: Urmas Paet

Minderheitenansicht, eingereicht von Javier Couso Permuy (GUE/NGL)

Mit dem Bericht wird die Linie der EU weiterverfolgt, die Fähigkeiten der EU im Bereich der Cyberabwehr zu stärken. Dabei handelt es sich um ein weiteres Beispiel für die militaristische und aggressive Politik der EU. Es geht darum, die militärischen Fähigkeiten der EU im Bereich Sicherheit und Verteidigung auszubauen und zu verstärken und dabei auch die Aufstockung der Finanzmittel für diesen Bereich zu rechtfertigen, und zwar stets in Zusammenarbeit mit der NATO.

Wir lehnen den Bericht ab, weil darin

– ein Binnenmarkt für Cybersicherheit unterstützt wird, um Synergieeffekte zu schaffen und Lösungen zwischen dem zivilen und dem militärischen Markt zu portieren,

– die Mitgliedstaaten nachdrücklich aufgefordert werden, den sich durch die Ständige Strukturierte Zusammenarbeit (SSZ) und den Europäischen Verteidigungsfonds bietenden Rahmen zu nutzen, um Kooperationsprojekte auf dem Gebiet der Cyberabwehr vorzuschlagen,

– die Zusammenarbeit der EU und der NATO im Bereich der Verteidigung unterstützt wird,

– das Sicherheitsdenken und die restriktive Politik der EU unterstützt werden, die den Rechten und Freiheiten der Bürger der EU-Mitgliedstaaten zuwiderlaufen;

– die Verwendung einiger Instrumente aus dem mehrjährigen Finanzrahmen (MFR) für die Cyberabwehr verteidigt wird.

Wir fordern,

– dass die NATO aufgelöst wird,

– dass aus dem EU-Haushalt keine Militärausgaben finanziert werden und Artikel 41 Absatz 2 EUV eng ausgelegt wird,

– dass die militaristischen Maßnahmen der EU, nämlich die SSZ, der Europäische Verteidigungsfonds und das Europäische Programm zur industriellen Entwicklung im Verteidigungsbereich, eingestellt werden,

– dass öffentliche Mittel zur Förderung hochwertiger Arbeitsplätze, der Reindustrialisierung und von KMU eingesetzt werden,

– dass die bürgerlichen Rechte und Freiheiten aller Bürger der EU-Mitgliedstaaten strikt verteidigt und geschützt werden,

– dass die Aufsicht durch die Vereinten Nationen, die Charta der Vereinten Nationen und das Völkerrecht bei allen Maßnahmen genau eingehalten werden.

ANGABEN ZUR ANNAHME IM FEDERFÜHRENDEN AUSSCHUSS

Datum der Annahme	16.5.2018
Ergebnis der Schlussabstimmung	+: 45 –: 8 0: 8
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Lars Adaktusson, Michèle Alliot-Marie, Francisco Assis, Petras Auštrevičius, Goffredo Maria Bettini, Elmar Brok, Klaus Buchner, Fabio Massimo Castaldo, Lorenzo Cesa, Aymeric Chauprade, Javier Couso Permuy, Andi Cristea, Arnaud Danjean, Eugen Freund, Sandra Kalniete, Manolis Kefalogiannis, Tunne Kelam, Wajid Khan, Eduard Kukan, Ilhan Kyuchyuk, Arne Lietz, Barbara Lochbihler, Sabine Lösing, Tamás Meszerics, Francisco José Millán Mon, Clare Moody, Javier Nart, Pier Antonio Panzeri, Demetris Papadakis, Ioan Mircea Paşcu, Alojz Peterle, Tonino Picula, Kati Piri, Julia Pitera, Cristian Dan Preda, Jozo Radoš, Michel Reimon, Sofia Sakorafa, Jean-Luc Schaffhauser, Alyn Smith, Dobromir Sośnierz, Jaromír Štětina, Dubravka Šuica, Charles Tannock, László Tőkés, Ivo Vajgl, Geoffrey Van Orden, Boris Zala
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	David Coburn, Marek Jurek, Norica Nicolai, Urmas Paet, Soraya Post, José Ignacio Salafranca Sánchez-Neyra, Bodil Valero, Marie-Christine Vergiat, Janusz Zemke, Željana Zovko
Zum Zeitpunkt der Schlussabstimmung anwesende Stellv. (Art. 200 Abs. 2)	Renate Weber, Francis Zammit Dimech, Joachim Zeller

NAMENTLICHE SCHLUSSABSTIMMUNG IM FEDERFÜHRENDEN AUSSCHUSS

45	+
ALDE	Petras Auštrevičius, Ilhan Kyuchyuk, Javier Nart, Norica Nicolai, Urmas Paet, Jozo Radoš, Ivo Vajgl, Renate Weber
EFDD	Fabio Massimo Castaldo, Aymeric Chauprade
PPE	Lars Adaktusson, Michèle Alliot-Marie, Elmar Brok, Lorenzo Cesa, Arnaud Danjean, Sandra Kalniete, Manolis Kefalogiannis, Tunne Kelam, Eduard Kukan, Francisco José Millán Mon, Alojz Peterle, Julia Pitera, Cristian Dan Preda, José Ignacio Salafranca Sánchez-Neyra, Jaromír Štětina, Dubravka Šuica, László Tőkés, Francis Zammit Dimech, Joachim Zeller, Željana Zovko
S&D	Francisco Assis, Goffredo Maria Bettini, Andi Cristea, Eugen Freund, Wajid Khan, Arne Lietz, Clare Moody, Pier Antonio Panzeri, Demetris Papadakis, Ioan Mircea Paşcu, Tonino Picula, Kati Piri, Soraya Post, Boris Zala, Janusz Zemke

8	-
ECR	Geoffrey Van Orden
EFDD	David Coburn
ENF	Jean-Luc Schaffhauser
GUE/NGL	Javier Couso Permuy, Sabine Lösing, Sofia Sakorafa, Marie-Christine Vergiat
NI	Dobromir Sośnierz

8	0
ECR	Marek Jurek, Charles Tannock
VERTS/ALE	Klaus Buchner, Barbara Lochbihler, Tamás Meszerics, Michel Reimon, Alyn Smith, Bodil Valero

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung