Rat der
Europäischen Union

Brüssel, den 20. November 2017
(OR. en)

14435/17

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

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	20. November 2017
Empfänger:	Delegationen
Nr. Vordok.:	13943/17 + COR 1
Nr. Komm.dok.:	12210/17, 12211/17
Betr.:	Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" – Schlussfolgerungen des Rates (20. November 2017)

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen", die der Rat (Allgemeine Angelegenheiten) am 20. November 2017 angenommen hat.

ANLAGE

Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"

Der Rat der Europäischen Union –

1. IN DER ERKENNTNIS, dass Cybersicherheit von großer Bedeutung für den Wohlstand, das Wachstum und die Sicherheit in der EU und für die Integrität unserer freien und demokratischen Gesellschaften und der ihnen zugrunde liegenden Prozesse im digitalen Zeitalter ist, da sie sowohl die Rechtsstaatlichkeit als auch die Menschenrechte und Grundfreiheiten aller Menschen schützt;

2. UNTER BETONUNG DESSEN, dass Cybersicherheit ein kohärentes Vorgehen auf nationaler Ebene, EU-Ebene und weltweit erfordert, da Cyberbedrohungen Auswirkungen auf unsere Demokratie, unseren Wohlstand, unsere Stabilität und unsere Sicherheit haben können;

3. UNTER HINWEIS DARAUF, dass ein hohes Maß an Abwehrfähigkeit im Bereich der Cybersicherheit in der gesamten EU auch wichtig ist, um Vertrauen in den digitalen Binnenmarkt und die Weiterentwicklung des digitalen Europas zu schaffen;

4. UNTER ERNEUTEM HINWEIS DARAUF, dass die EU stets einen offenen, globalen, freien, friedlichen und sicheren Cyberraum fördern wird, in dem die Menschenrechte und Grundfreiheiten, insbesondere das Recht auf freie Meinungsäußerung, der Zugang zu Informationen, der Datenschutz, der Schutz der Privatsphäre und die Sicherheit sowie die grundlegenden Werte und Prinzipien der EU sowohl innerhalb der EU als auch weltweit uneingeschränkt angewandt und eingehalten werden, und UNTER BETONUNG DESSEN, dass unbedingt für ein ausgewogenes Verhältnis zwischen Menschenrechten und Grundfreiheiten einerseits und den Anforderungen der Politik der inneren Sicherheit der EU andererseits zu sorgen ist[1];

5. IN ANERKENNUNG DESSEN, dass das Völkerrecht – einschließlich der Charta der Vereinten Nationen in allen ihren Teilen –, das humanitäre Völkerrecht und die Menschenrechte im Cyberraum gelten, und daher UNTER BETONUNG der Notwendigkeit, weitere Anstrengungen zu unternehmen, um die Einhaltung des Völkerrechts im Cyberraum sicherzustellen;

---

[1] Dok. 12650/17.

6. UNTER HINWEIS AUF seine Schlussfolgerungen zur Cybersicherheitsstrategie der EU[2], zur Internet-Governance[3], zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit[4], zur Cyberdiplomatie[5] und über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten[6], zur Verbesserung der Strafjustiz im Cyberspace[7]; zu Sicherheit und Verteidigung im Kontext der Globalen Strategie der EU[8], zum Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen[9] und zur Halbzeitüberprüfung der erneuerten Strategie der inneren Sicherheit der Europäischen Union (2015-2020)[10];

7. IN ANERKENNUNG DESSEN, dass der durch das Übereinkommen des Europarates über Computerkriminalität (Übereinkommen von Budapest) gebildete Rahmen eine solide Grundlage für eine heterogene Gruppe von Ländern bietet, um einen wirksamen rechtlichen Standard für die verschiedenen nationalen Rechtsvorschriften und für die internationale Zusammenarbeit bei der Bewältigung der Cyberkriminalität anzuwenden;

8. IN DER ERKENNTNIS, dass die Umsetzung des 2014 eingeführten EU-Rahmens für die Cyberabwehrstrategie wieder in den Mittelpunkt gerückt und dieser Rahmen aktualisiert werden muss, um Cyber-Sicherheit und -Abwehr stärker in die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) und die weiter gefasste Sicherheits- und Verteidigungsagenda zu integrieren;

9. IN ANERKENNUNG DESSEN, dass eine weltweit wettbewerbsfähige europäische Industrie ein wichtiges Element ist, um ein hohes Maß an Cybersicherheit auf nationaler und EU-Ebene zu erreichen;

10. UNTER HINWEIS DARAUF, dass gemäß Artikel 4 Absatz 2 EUV die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt –

---

2 Dok. 12109/13 und Dok. 6225/13 (Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum (COM JOIN(2013) 1 final)).

3 Dok. 16200/14 und Dok. 6460/14 (Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: "Internet-Politik und Internet-Governance – Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance" (COM(2014) 72 final)).

4 Dok. 14540/16 und Dok. 11013/16 (Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: "Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche" (COM(2016) 410 final)).

5 Dok. 6122/15.

6 Dok. 9916/17.

7 Dok. 10007/16.

8 Dok. 9178/17.

9 Dok. 7688/16 (Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Gemeinsamer Rahmeneine Antwort der Europäischen Union"). für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union").

10 Dok. 12650/17.

STELLT HIERMIT FOLGENDES FEST: ER

11. BEGRÜSST die Gemeinsame Mitteilung an das Europäische Parlament und den Rat mit dem Titel "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen", da sie ein ehrgeiziges Ziel für die Verbesserung der Cybersicherheit in der EU vorgibt. Sie trägt auch zur strategischen Autonomie der EU bei, wie in den Schlussfolgerungen des Rates zur Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union[11] erwähnt wird, indem sie das Ziel verfolgt, ein digitales Europa aufzubauen, in dem die Sicherheit, das Vertrauen, das Bewusstsein für seine Stärken, die Wettbewerbsfähigkeit und die Offenheit gegenüber der Welt sowie die Achtung der gemeinsamen Werte der EU im Zusammenhang mit einem offenen, freien, friedlichen und sicheren globalen Internet gestärkt werden und das daher eine größere Abwehrfähigkeit erreichen kann, um Cyberbedrohungen zu verhindern, zu bekämpfen, zu erkennen und darauf zu reagieren und um gemeinsam auf Cyberbedrohungen in der ganzen EU reagieren zu können;

12. ERSUCHT die Mitgliedstaaten und die Organe, Agenturen und Einrichtungen der EU, unter Wahrung der jeweiligen Zuständigkeitsbereiche sowie des Subsidiaritätsprinzips- und des Verhältnismäßigkeitsgrundsatzes entsprechend den in diesen Schlussfolgerungen niedergelegten strategischen Zielen zusammenzuarbeiten;

13. BETONT, dass die EU, ihre Mitgliedstaaten und die Privatwirtschaft ausreichende Finanzmittel bereitstellen müssen, wobei den verfügbaren Ressourcen zur Unterstützung des Aufbaus der Abwehrfähigkeit gegen Cyberangriffe und der Anstrengungen im Bereich Forschung und Entwicklung auf dem Gebiet der Cybersicherheit in der gesamten EU Rechnung zu tragen ist; zudem müssen sie ihre Zusammenarbeit intensivieren, um Cyberbedrohungen zu verhindern, zu bekämpfen, zu erkennen und darauf zu reagieren und um gemeinsam auf Cybersicherheitsvorfälle großen Ausmaßes und böswillige Cyberaktivitäten in der ganzen EU reagieren zu können;

---

[11] Dok. 13202/16.

Kapitel I

GEWÄHRLEISTUNG EINER WIRKSAMEN ABWEHRFÄHIGKEIT IM BEREICH DER CYBERSICHERHEIT UND DES VERTRAUENS IN DEN DIGITALEN BINNENMARKT

14. BETONT, dass jeder Mitgliedstaat die Hauptverantwortung dafür trägt, seine eigene Cybersicherheit zu verbessern und auf Cybersicherheitsvorfälle und -krisen reagieren zu können, während die EU einen großen zusätzlichen Nutzen bieten kann, indem sie die Zusammenarbeit zwischen den Mitgliedstaaten fördert. BETONT in diesem Zusammenhang, dass alle Mitgliedstaaten den für Cybersicherheit zuständigen nationalen Behörden die erforderlichen Ressourcen zur Verfügung stellen müssen, um Prävention, Erkennung und Reaktion in Bezug auf Cybersicherheitsvorfälle und -krisen in der EU zu gewährleisten;

15. BETONT, dass – sofern möglich – die vorhandenen Mechanismen, Strukturen und Einrichtungen auf der Ebene der EU zu nutzen sind;

16. WÜRDIGT

- die Fortschritte, die die Mitgliedstaaten bei der Umsetzung der NIS-Richtlinie erzielt haben, und BETONT, dass eine vollständige und wirksame Umsetzung bis Mai 2018, wie in der Richtlinie vorgesehen, erreicht werden muss[12];
- die Arbeit, die die NIS-Kooperationsgruppe im Hinblick auf die Verbesserung der strategischen Zusammenarbeit und des Informationsaustausches zwischen den Mitgliedstaaten geleistet hat;
- die Arbeit des CSIRT-Netzes insbesondere im Hinblick auf die Stärkung der operativen Zusammenarbeit der Mitgliedstaaten, auf die Schaffung von Vertrauen in den Informationsaustausch bei großen Cybersicherheitsvorfällen und – auf der Grundlage nationaler Schlussfolgerungen der Mitgliedstaaten – auf die Bereitstellung von Anhaltspunkten für eine gemeinsame Lageeinschätzung auf EU-Ebene;
- die Arbeit im Rahmen der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit (cPPP);

[12] Unbeschadet der Zuständigkeit der Mitgliedstaaten für die Umsetzung der NIS-Richtlinie, vor allem im Hinblick auf die Betreiber wesentlicher Dienste.

17. BEGRÜSST, dass in der Gemeinsamen Mitteilung bekräftigt wurde, dass eine leistungsstarke und vertrauenswürdige Verschlüsselung sehr wichtig ist, damit die Menschenrechte und Grundfreiheiten in der EU gebührend gewahrt werden und die Öffentlichkeit Vertrauen in den digitalen Binnenmarkt hat, während zu berücksichtigen ist, dass die Strafverfolgungsbehörden Zugriff auf die für ihre Ermittlungen erforderlichen Daten haben müssen, und dass bekräftigt wurde, dass sichere digitale Identifizierung und Kommunikation für eine wirksame Cybersicherheit in der EU von zentraler Bedeutung sind;

18. BEGRÜSST das in der Gemeinsamen Mitteilung genannte Vorhaben, hinsichtlich der Durchführung regelmäßiger europaweiter Übungen zur Cybersicherheit, bei denen auf den Erfahrungen der Cyber-Europe-Übungen aufgebaut und die Reaktion auf verschiedenen Ebenen kombiniert wird, ehrgeiziger vorzugehen, da dies ein wichtiger Faktor für die Stärkung der Vorsorge der Mitgliedstaaten und der EU-Institutionen für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes sein wird;

19. RUFT die EU und ihre Mitgliedstaaten auf, regelmäßig strategische Cybersicherheitsübungen in verschiedenen Ratsformationen durchzuführen und dabei auf den Erfahrungen aufzubauen, die bei der Übung EU CYBRID 2017 gemacht wurden, und

20. – unbeschadet des Ergebnisses des Rechtssetzungsprozesses –

- BEGRÜSST den Vorschlag für ein starkes und dauerhaftes Mandat der ENISA mit dem vorrangigen Ziel, eine engere Zusammenarbeit zwischen den Mitgliedstaaten zu unterstützen und zu entwickeln, ihre Kapazitäten auszubauen und das Vertrauen in ein digitales Europa zu stärken;

- BEKRÄFTIGT, dass sich die künftige ENISA auf die Erfahrungen und das Fachwissen in den Mitgliedstaaten und bei der EU stützen und die kohärente Entwicklung und Durchführung der vorhandenen und künftigen Maßnahmen und Regelungen der EU für Cybersicherheit unterstützen sollte, wobei dafür zu sorgen ist, dass alle Zuständigkeiten der ENISA so gestaltet werden sollten, dass sie die Zuständigkeiten der Mitgliedstaaten ergänzen;

- BEKRÄFTIGT das Ziel, das Vertrauen in ein digitales Europa zu stärken, indem das Vertrauen in digitale Lösungen und Innovationen, einschließlich des Internets der Dinge, des elektronischen Geschäftsverkehrs und der elektronischen Verwaltung, gestärkt werden, und zwar insbesondere durch einen europäischen Cybersicherheitszertifizierungsrahmen von Weltniveau13. Dies ist eine Grundvoraussetzung für die Verbesserung des Vertrauens in digitale Produkte und Dienstleistungen und der Sicherheit dieser Produkte und Dienstleistungen und für den Schutz kritischer Infrastrukturen sowie der Daten von Staaten, Bürgern und Unternehmen und ist hilfreich für die Einführung eines Ansatzes der konzeptionsintegrierten Sicherheit für Produkte, Dienste und Verfahren im digitalen Binnenmarkt;
- BETONT, dass die Rechtsetzungsarbeit zur Stärkung der Zertifizierung der Cybersicherheit auf EU-Ebene dem Bedarf des Marktes und der Nutzer gerecht werden muss, auf den Erfahrungen der in der EU vorhandenen Zertifizierungskapazitäten und -verfahren (beispielsweise der Rahmen der Gruppe Hoher Beamter für Informationssicherheit (SOG-IS-Rahmen)) aufbauen muss und einen Rahmen bieten müsste, mit dem eine rasche Anpassung an den neuesten Stand künftiger digitaler Entwicklungen erfolgen kann;
- BETONT, dass mit der Verbesserung der Zertifizierung der Cybersicherheit in der EU das gesamte Spektrum der Sicherheitsanforderungen bis hin zu den höchsten Anforderungen, bei denen die Abwehrkraft gegen die Fähigkeiten der Angreifer nachgewiesen werden muss, erfasst werden sollte. Zentrale Faktoren für den Erfolg wären ein zuverlässiger, transparenter und unabhängiger Prozess für die Sicherheitszertifizierung zur Förderung der Verfügbarkeit vertrauenswürdiger und gesicherter Geräte, Software und Dienste im Binnenmarkt und darüber hinaus, ferner die Anerkennung des jeweiligen Fachwissens der Wirtschaft, der Staaten und der Evaluierungsspezialisten Europas durch europäische und weltweite Normen[14] und schließlich die Achtung der Rolle der Mitgliedstaaten im Zertifizierungsprozess insbesondere hinsichtlich der Evaluierung auf höheren Sicherheitsebenen und vor allem hinsichtlich wesentlicher Sicherheitserfordernisse und einer Sicherheitskompetenzbewertung. Mit einem derartigen Zertifizierungsrahmen sollte außerdem gewährleistet werden, dass ein EU-weites Zertifizierungssystem der für die Nutzung von IKT-Produkten, -Diensten und/oder -Systemen erforderlichen Gewährleistungsstufe angemessen ist und Unternehmen jeder Größe grenzüberschreitenden Handel ermöglicht, damit neue Produkte entwickelt und auf den EU-Märkten und außerhalb der EU-Märkte abgesetzt werden.

---

13 Durch globale Standards, die im Geiste des TBT-Verhaltenskodexes der WTO entwickelt werden.

14 Durch europäische und globale Standards, die im Geiste des TBT-Verhaltenskodexes der WTO entwickelt werden.

21. BEGRÜSST die Absicht, ein Netz von Cybersicherheitskompetenzzentren aufzubauen, damit die Entwicklung und der Einsatz von Cybersicherheitstechnologien gefördert wird und zusätzliche Anreize gegeben werden, die der Innovation der Unternehmen der EU auf globaler Ebene bei der Entwicklung von Technologien der nächsten Generation und bahnbrechenden Technologien – wie künstliche Intelligenz, Quanteninformatik, Blockchain-Technologien und sichere digitale Identitäten – zugute kommen;

22. BETONT, dass das Netz von Cybersicherheitskompetenzzentren allen Mitgliedstaaten und deren bestehenden Exzellenz- und Kompetenzzentren gegenüber inklusiv sein und besonders auf Komplementarität achten muss, und – in Anbetracht dessen – WEIST HIN auf das geplante Europäische Cybersicherheits- und Forschungszentrum, das in erster Linie Komplementarität gewährleisten und Überschneidungen mit dem Netz von Cybersicherheitskompetenzzentren und mit sonstigen Einrichtungen der EU vermeiden sollte;

23. BETONT, dass das Netz von Cybersicherheitskompetenzzentren ein von der Forschung bis zur Wirtschaft reichendes Spektrum von Fragen behandeln und daher unter anderem dazu beitragen sollte, dass das Ziel der strategischen Autonomie Europas erreicht wird;

24. BEKRÄFTIGT im Hinblick auf das geplante Netz von Cybersicherheitskompetenzzentren, dass die EU über ihre Mitgliedstaaten eine europäische Fähigkeit für die Evaluierung der Leistungsfähigkeit der Kryptographie entwickeln muss, wie sie in Produkten und Diensten für Bürger, Unternehmen und Staaten im digitalen Binnenmarkt verwendet wird, wobei anerkannt wird, dass Kryptographiemaßnahmen ein zentraler Aspekt der nationalen Sicherheit sind und daher in der Zuständigkeit der Mitgliedstaaten liegen;

25. ERSUCHT alle einschlägigen Akteure, die Investitionen in Cybersicherheitsanwendungen neuer Technologien zu erhöhen, um zur Cybersicherheit in allen Sektoren der europäischen Wirtschaft beizutragen;

26. BETONT, wie wichtig die glaubwürdige, vertrauenswürdige und koordinierte Bereitstellung von Cybersicherheitsdiensten für die Organe der EU ist und RUFT die Kommission und die übrigen Organe der EU AUF, CERT-EU gemäß diesen Zielen weiterzuentwickeln und dafür auch für angemessene Ressourcen zu sorgen;

27. BEGRÜSST die Forderung, die wichtige Rolle dritter Sicherheitsexperten bei der Aufdeckung von Schwachstellen in bestehenden Produkten und Diensten zu würdigen und FORDERT die Mitgliedstaaten AUF, bewährte Verfahren für die koordinierte Offenlegung von Schwachstellen auszutauschen;

28. BETONT die Verantwortung eines jeden für Cybersicherheit und ERSUCHT die EU und ihre Mitgliedstaaten, digitale Kompetenzen und Medienkompetenz zu fördern, damit Nutzer dabei unterstützt werden, ihre digitalen Informationen online zu schützen, und damit für die Risiken, die bestehen, wenn personenbezogene Daten ins Internet gestellt werden, eine Sensibilisierung bewirkt wird;

29. BEGRÜSST, dass in der Gemeinsamen Mitteilung Bildung, Cyber-Hygiene und Aufklärung in den Mitgliedstaaten und der EU einen hohen Stellenwert haben;

30. RUFT DIE KOMMISSION AUF, rasch eine Folgenabschätzung vorzunehmen und bis Mitte 2018 die entsprechenden Rechtsinstrumente für die Durchführung der Initiative zum Aufbau eines Netzes von Cybersicherheitskompetenzzentren und eines Europäischen Cybersicherheits- und Forschungszentrum vorzuschlagen;

31. ERSUCHT die Mitgliedstaaten,

- vorrangig die Thematik der Cyberbedrohungen in Informationskampagnen einzubeziehen und das Thema Cybersicherheit als Teil der Lehrpläne von Hochschulen und Bildungs- und Berufsausbildungseinrichtungen zu fördern. Ein besonderer Schwerpunkt sollte auf der Jugendbildung und auf der Förderung digitaler Kompetenzen liegen, damit zukunftsfähige Fachleute herangebildet werden, die für die Herausforderungen in den Bereichen Sicherheit, Wirtschaft und Dienste gewappnet sind;

- die Bemühungen um die Auflegung von fachspezifischen Cybersicherheitsprogrammen auf hohem Niveau zu verstärken, damit der gegenwärtig bestehende Mangel an Cybersicherheitsfachleuten in der EU beseitigt wird;
- ein wirksames Kooperationsnetz von Bildungskontaktstellen (PoCs) unter der Schirmherrschaft der ENISA einzurichten. Das PoCs-Netz sollte darauf abzielen, die Koordinierung und den Austausch bewährter Vorgehensweisen zwischen den Mitgliedstaaten in Bezug auf Ausbildung und Aufklärung zu Cybersicherheit sowie Ausbildung, Übung und Kapazitätsaufbau zu verbessern;
- in Erwägung zu ziehen, die Bestimmungen der NIS-Richtlinie auch auf öffentliche Verwaltungen, die an kritischen gesellschaftlichen oder wirtschaftlichen Tätigkeiten beteiligt sind, anzuwenden, wenn diese nicht bereits von den nationalen Rechtsvorschriften erfasst sind und dies als zweckmäßig erachtet wird, und in Anbetracht der Rolle, die öffentliche Verwaltungen in unserer Gesellschaft und in der Wirtschaft spielen, Aus- und Fortbildung zur Cybersicherheit auch in öffentlichen Verwaltungen anzubieten.

Kapitel II

AUFBAU DER FÄHIGKEIT DER EU ZUR PRÄVENTION, ABSCHRECKUNG UND AUFDECKUNG BÖSWILLIGER CYBERAKTIVITÄTEN UND ZU ENTSPRECHENDEN REAKTIONEN

32. BETONT, dass besonders schwere Cybersicherheitsvorfälle oder -krisen für die Mitgliedstaaten einen hinreichenden Grund darstellen könnten, die "Solidaritätsklausel" der EU[15] und/oder die Beistandsklausel[16] geltend zu machen;

33. BEGRÜSST die Annahme des "Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten", der durch die Festlegung von GASP-Maßnahmen einschließlich restriktiver Maßnahmen, die zur Prävention bösartiger Cyberaktivitäten und zur Reaktion darauf genutzt werden können, zur Konfliktverhütung, Zusammenarbeit und Stabilität im Cyberraum beiträgt, und FORDERT den EAD und die Mitgliedstaaten zu regelmäßigen Übungen in Bezug auf diesen Rahmen AUF;

---

15 Artikel 222 AEUV.
16 Artikel 42 Absatz 7 EUV.

34. BETONT, dass schwerwiegende Cybersicherheitsvorfälle und -krisen einer effizienten Reaktion auf EU-Ebene bedürfen, bei der die Zuständigkeiten der Mitgliedstaaten gewahrt werden müssen, und dass die Cybersicherheit in die bestehenden Krisenbewältigungsmechanismen auf EU-Ebene einbezogen werden muss[17]; FORDERT zu diesem Zweck, die Reaktion auf EU-Ebene auf schwerwiegende Cybersicherheitsvorfälle – von den diplomatisch-strategischen bis hin zu den technischen Reaktionen – ausgehend von den jeweiligen Rahmen und Verfahren, die erforderlichenfalls weiterentwickelt werden, regelmäßig zu üben[18];

35. UNTERSTREICHT, wie wichtig gut integrierte Mechanismen für Reaktionen und Informationsaustausch zwischen den einzelnen Gemeinschaften sind, die für die Gewährleistung der Cybersicherheit in Europa von ausschlaggebender Bedeutung sind, auch zwischen den zuständigen EU-Einrichtungen und den zuständigen Behörden der Mitgliedstaaten. Diese Mechanismen müssen im Rahmen der Cybersicherheitsübungen auf EU-Ebene getestet und geprüft und erforderlichenfalls durch entsprechende Vereinbarungen formalisiert werden;

36. WEIST auf die Möglichkeit HIN, gegebenenfalls einen Vorschlag der Kommission zu prüfen, mit dem ein Cybersicherheits-Notfallfond zusätzlich zu den bestehenden Maßnahmen der Mitgliedstaaten und im Rahmen der vorhandenen Mittel (insbesondere des Mehrjährigen Finanzrahmens der EU) eingerichtet wird, um die Mitgliedstaaten bei der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und der Minderung ihrer Folgen zu unterstützen, sofern der betreffende Mitgliedstaat vor dem Vorfall ein umsichtiges Cybersicherheitssystem errichtet hat, das die vollständige Umsetzung der NIS-Richtlinie, ein ausgereiftes Risikomanagementsystem und nationale Aufsichtsregelungen beinhaltet;

37. ERKENNT die immer engere Verknüpfung zwischen Cybersicherheit und Cyberabwehr AN und RUFT dazu AUF, die Zusammenarbeit bei der Cyberabwehr u. a. durch die Förderung der Zusammenarbeit zwischen den zivilen und militärischen Gemeinschaften, die für die Reaktion auf Vorfälle zuständig sind, zu verstärken und die Cybersicherheit von GSVP-Missionen und -Operationen weiter auszubauen;

---

17 C(2017)6100 final.
18 9916/17 und C/2017/6100 final.

38. BETONT, dass die vorgeschlagenen Verteidigungsinitiativen möglicherweise voll und ganz genutzt werden müssen, um die Entwicklung geeigneter digitaler Fähigkeiten in Europa zu beschleunigen, und ERKENNT AN, welche Chancen mit einer eventuellen Entwicklung von Cyberabwehrprojekten im Rahmen der Ständigen Strukturierten Zusammenarbeit (PESCO) verbunden sind, wenn die an der PESCO beteiligten Mitgliedstaaten diese als erforderlich erachten, und WÜRDIGT die Rolle der technologischen und industriellen Basis der europäischen Verteidigung (EDTIB) und der zivilen Cybersicherheitsbranche im weiteren Sinne, die die Mitgliedstaaten in die Lage versetzen, ihre Interessen in Bezug auf Cybersicherheit und Cyberabwehr zu schützen;

39. NIMMT den Vorschlag der Kommission ZUR KENNTNIS, bis Ende 2018 eine Plattform für Schulung und Ausbildung in Cyberabwehr zu schaffen, und BETONT, dass die Plattform die Schulungs- und Ausbildungsmöglichkeiten in den Mitgliedstaaten aufwerten und die Komplementarität mit anderen EU-Maßnahmen und -Initiativen, insbesondere mit dem ESVK und der EDA sicherstellen sollte;

40. FORDERT die EU und ihre Mitgliedstaaten AUF, auf die Gefahr des IKT-gestützten Diebstahls geistigen Eigentums, einschließlich von Geschäftsgeheimnissen und anderen vertraulichen Geschäftsinformationen zu reagieren, bei dem es darum geht, Unternehmen oder Wirtschaftszweigen Wettbewerbsvorteile zu verschaffen;

41. ERKENNT AN, dass gegen Internetstraftaten, insbesondere im Darknet, sexuellen Missbrauch von Kindern im Internet sowie Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vorgegangen werden muss, wobei insbesondere eine bessere Erkenntnislage, die Durchführung gemeinsamer Ermittlungen und gegenseitige operative Unterstützung angestrebt werden;

42. BEGRÜSST die Arbeit der EU und ihrer Mitgliedstaaten bei der Bewältigung der Herausforderungen durch Systeme, die Kriminellen und Terroristen die Kommunikation ohne Zugriffsmöglichkeiten für die zuständigen Behörden ermöglichen, und BETONT, dass bei dieser Arbeit nicht außer Acht gelassen werden darf, dass eine starke und zuverlässige Verschlüsselung von großer Bedeutung für die Cybersicherheit, das Vertrauen in den digitalen Binnenmarkt und die Gewährleistung der Achtung der Menschenrechte und Grundfreiheiten ist;

43. HEBT HERVOR, wie wichtig es ist, die Strafverfolgungsbehörden mit Instrumenten auszustatten, die die Aufdeckung, Untersuchung und Verfolgung von Cyberstraftaten ermöglichen, so dass im Cyberraum begangene Verbrechen nicht unbemerkt oder ungestraft bleiben, und BEGRÜSST den Beitrag des Europäischen Justiziellen Netzes gegen Cyberkriminalität zur Verbrechensbekämpfung durch die Zusammenarbeit der Justizbehörden;

44. BETONT, wie wichtig ein koordinierter Standpunkt der EU ist, um die Entscheidungen über die europäische und globale Internet-Governance innerhalb der Multi-Stakeholder-Gemeinschaft wirksam mitzugestalten, wo es beispielsweise darum geht, schnell zugängliche und genaue WHOIS-Datenbanken von IP-Adressen und Domain-Namen zu gewährleisten, sodass die Fähigkeiten im Bereich der Rechtsdurchsetzung und das öffentliche Interesse gewahrt werden;

45. HEBT HERVOR, wie wichtig die Übernahme des Internet-Protokolls IPv6 ist, das für die Entwicklung des Internets der Dinge in großem Maßstab sowie für die Verbesserung der Zuordnung von Straftaten im Cyberraum von wesentlicher Bedeutung ist;

46. BEFÜRWORTET die derzeitigen Arbeiten am grenzüberschreitenden Zugang zu elektronischen Beweismitteln, die sich mit der Vorratsdatenspeicherung befassen, und an der Bewältigung der Schwierigkeiten für Strafverfahren aufgrund von Systemen, die Kriminellen und Terroristen die Kommunikation ohne Zugriffsmöglichkeiten für die zuständigen Behörden ermöglichen, wobei zu berücksichtigen ist, dass die Menschenrechte und Grundfreiheiten sowie der Datenschutz gewahrt bleiben müssen;

47. FORDERT die Kommission AUF,

- bis Dezember 2017 einen Sachstandsbericht über die Umsetzung der praktischen Maßnahmen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln vorzulegen;

- Anfang 2018 einen Legislativvorschlag zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln vorzulegen;

48. ERSUCHT Europol, die ENISA und Eurojust,

- ihre Zusammenarbeit bei der Bekämpfung der Cyberkriminalität sowohl untereinander als auch mit anderen einschlägigen Akteuren einschließlich der CSIRT-Gemeinschaft, Interpol, dem Privatsektor und den Hochschulen weiter zu intensivieren und im Einklang mit ihren jeweiligen Aufgaben und Zuständigkeiten Synergien und Komplementarität sicherzustellen;

- gemeinsam mit den Mitgliedstaaten einen Beitrag zu einem koordinierten Konzept für eine Reaktion der Strafverfolgungsbehörden der EU auf schwer wiegende Cybersicherheitsvorfälle und -krisen zu leisten und die in den diesbezüglichen Rahmen vorgesehenen Verfahren zu ergänzen[19];

49. ERSUCHT die EU und ihre Mitgliedstaaten, weiter daran zu arbeiten,

- Hindernisse für Ermittlungen zu Straftaten und für eine wirksame Strafjustiz im Cyberraum zu beseitigen und die internationale Zusammenarbeit und Koordinierung bei der Bekämpfung der Cyberkriminalität zu verstärken;

- die Probleme aufgrund von Anonymisierungstechnologien zu bewältigen, wobei nicht außer Acht gelassen werden darf, dass eine starke und zuverlässige Verschlüsselung von großer Bedeutung für die Cybersicherheit und das Vertrauen in den digitalen Binnenmarkt ist;

- Entscheidungen über die Internet-Governance mitzugestalten, die sich auf die Fähigkeit der Strafverfolgungsbehörden zur Bekämpfung der Cyberkriminalität auswirken.

[19] 9916/17 und C/2017/6100 final.

Kapitel III

STÄRKUNG DER INTERNATIONALEN ZUSAMMENARBEIT FÜR EINEN OFFENEN, FREIEN, FRIEDLICHEN UND SICHEREN GLOBALEN CYBERRAUM

50. ERKENNT AN, dass die Gewährleistung der Cybersicherheit eine globale Herausforderung darstellt, die einer wirksamen globalen Zusammenarbeit aller Akteure bedarf, und ERKENNT AN, dass die Erhaltung der demokratischen Werte und der Grundsätze eines offenen, freien, friedlichen und sicheren globalen Cyberraums besonders im Mittelpunkt stehen muss, und in Anbetracht dessen,

51. RUFT die EU und ihre Mitgliedstaaten AUF, sich für die Schaffung eines strategischen Rahmens für die Konfliktverhütung, die Zusammenarbeit und die Stabilität im Cyberraum, der sich auf die Anwendung des geltenden Völkerrechts und insbesondere der gesamten Charta der Vereinten Nationen stützt, für die Entwicklung und Umsetzung universeller Normen für ein verantwortungsvolles Verhalten der Staaten und für regionale vertrauensbildende Maßnahmen zwischen Staaten einzusetzen;

52. ERKENNT die Rolle der Vereinten Nationen bei der Weiterentwicklung von Normen für ein verantwortungsvolles Verhalten der Staaten im Cyberraum AN und WEIST darauf HIN, dass in den Beratungen der Gruppe von Regierungssachverständigen der Vereinten Nationen im Laufe der Jahre einvernehmliche Normen und Empfehlungen ausgearbeitet wurden, die die Generalversammlung wiederholt gebilligt hat und die die Staaten als Grundlage für ihr verantwortungsvolles Verhalten im Cyberspace heranziehen sollten;

53. ERKENNT AN, dass Staaten diesen Normen für das verantwortungsvolle Verhalten der Staaten zufolge eine Nutzung ihres Hoheitsgebiets für völkerrechtswidrige Handlungen nicht wissentlich zulassen sollten, auf angemessene Hilfeersuchen eines anderen Staates reagieren sollten, dessen kritische Infrastrukturen böswilligen Cyberaktivitäten von ihrem Hoheitsgebiet aus ausgesetzt sind, und geeignete Maßnahmen zum Schutz ihrer kritischen Infrastrukturen vor Bedrohungen aus dem Cyberraum ergreifen sollten;

54. IST SICH der gemeinsamen Cyberbedrohungen und -risiken BEWUSST, denen die EU, die NATO und ihre jeweiligen Mitgliedstaaten gegenüberstehen, und BEKRÄFTIGT, wie wichtig es ist, die Zusammenarbeit zwischen EU und NATO im Bereich Cybersicherheit und Cyberabwehr unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der EU und im Einklang mit seinen Schlussfolgerungen vom 6. Dezember 2016 zur Umsetzung der Gemeinsamen Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des Generalsekretärs der Nordatlantikvertrags-Organisation[20] fortzusetzen;

55. FORDERT die EU und ihre Mitgliedstaaten AUF, die Ausarbeitung regionaler vertrauensbildender Maßnahmen zu unterstützen und zu ermutigen, die von wesentlicher Bedeutung dafür sind, die Zusammenarbeit und Transparenz zu erhöhen und die Gefahr von Konflikten zu verringern. Durch die Durchführung vertrauensbildender Maßnahmen zur Cybersicherheit in der OSZE und anderen regionalen Kontexten wird staatliches Verhalten berechenbarer und ein weiterer Beitrag zur Stabilisierung des Cyberraums geleistet;

56. BESTÄTIGT, dass die EU durch den Schutz der Menschenrechte und Grundfreiheiten weiterhin an ihren Grundwerten festhalten und sich dabei auf die EU-Menschenrechtsleitlinien zum Thema Online-Freiheit stützen wird. Des Weiteren betont die EU, wie wichtig es ist, alle Interessenträger, einschließlich der Wissenschaft, der Zivilgesellschaft und des Privatsektors, in die Internet-Governance einzubeziehen;

57. FORDERT die EU und ihre Mitgliedstaaten AUF, den Aufbau von Cyberkapazitäten in Drittländern zur Bekämpfung der Cyberkriminalität und zum Aufbau von Abwehrfähigkeit gegenüber Cyberangriffen im Einklang mit den Grundwerten der EU zu fördern, wobei den Nachbarländern der EU und den Entwicklungsländern mit schnell wachsender Internetanbindung besonderer Vorrang eingeräumt wird. Um die Bemühungen der EU in diesem Bereich zu fördern, sollten ein EU-Netz für den Aufbau von Cyberkapazitäten geschaffen und EU-Leitlinien für den Aufbau von Cyberkapazitäten ausgearbeitet werden, die die bestehenden Mechanismen und Strukturen ergänzen;

---

[20] Dok. 15283/16.

58. HEBT die Fortschritte HERVOR, die bei der Zusammenarbeit zwischen der EU und der NATO bei der Cyberabwehr und der Cybersicherheit sowie der Entwicklung von Schulung, Ausbildung und Konzepten erzielt wurden, wobei unnötige Doppelarbeit bei sich überschneidenden Anforderungen vermieden und die Interoperabilität durch Anforderungen und Standards im Bereich der Cyberabwehr gefördert wurde, und RUFT dazu AUF, unter uneingeschränkter Achtung des EU-Übungsrahmens und der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der EU die Zusammenarbeit bei Cyberabwehrübungen (auf Personalebene) fortzusetzen und bewährte Verfahren für die Krisenbewältigung auszutauschen, wobei unnötige Doppelarbeit bei sich überschneidenden Anforderungen zu vermeiden ist;

59. STELLT FEST, dass das Übereinkommen des Europarats über Computerkriminalität (das Budapester Übereinkommen) eine wirksame Rechtsnorm für die Gestaltung innerstaatlicher Rechtsvorschriften über Cyberkriminalität bietet; FORDERT alle Länder AUF, entsprechende nationale Rechtsrahmen zu konzipieren und die Zusammenarbeit innerhalb dieses internationalen Rahmens, den das Budapester Übereinkommen bietet, fortzusetzen;

60. WEIST auf die Erfolge bei den bilateralen Dialogen der EU über den Cyberraum HIN und fordert weitere Anstrengungen, um im Bereich der Cybersicherheit eine Zusammenarbeit mit Drittländern zustande zu bringen;

61. WEIST darauf HIN, dass die EU über einen soliden und rechtsverbindlichen Ausfuhrkontrollmechanismus verfügt, der sich auf die Entscheidungen und bewährten Vorgehensweisen stützt, die im Rahmen der internationalen Nichtverbreitungsregelungen ausgearbeitet wurden, NIMMT die derzeitigen Beratungen im Rat ZUR KENNTNIS, bei denen festgestellt werden soll, wie die Funktionsweise dieser Kontrollen weiter verbessert werden kann, und ERSUCHT die Mitgliedstaaten, im Rahmen der einschlägigen internationalen Ausfuhrkontrollregelungen (z. B. des Wassenaar-Arrangements) die kritischen Cybersicherheitsanwendungen neuartiger Technologien weiter zur Sprache zu bringen, um eine effektive Kontrolle der kritischen Cybersicherheitstechnologien von morgen sicherzustellen.

62. Als Folgemaßnahme zu den Schlussfolgerungen des Europäischen Rates vom 19. Oktober 2017[21] werden die vorliegenden Schlussfolgerungen durch einen Aktionsplan umgesetzt, den der Rat noch vor Jahresende 2017 annehmen sollte. Der Aktionsplan ist ein fortzuschreibendes Dokument und wird vom Rat regelmäßig überprüft und aktualisiert.

---

[21] EUCO 14/17.