Europäisches Parlament
2014-2019

ANGENOMMENE TEXTE

P8_TA(2017)0366

Bekämpfung der Cyberkriminalität

Entschließung des Europäischen Parlaments vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität (2017/2068(INI))

Das Europäische Parlament,

– gestützt auf die Artikel 2, 3 und 6 des Vertrags über die Europäische Union (EUV),

– gestützt auf die Artikel 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 und 88 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV),

– gestützt auf die Artikel 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 und 52 der Charta der Grundrechte der Europäischen Union,

– unter Hinweis auf das Übereinkommen der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989,

– unter Hinweis auf das Fakultativprotokoll zum Übereinkommen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie vom 25. Mai 2000,

– unter Hinweis auf die auf dem ersten Weltkongress gegen kommerzielle sexuelle Ausbeutung von Kindern angenommene Stockholmer Erklärung und Aktionsagenda, die auf dem zweiten Weltkongress gegen kommerzielle sexuelle Ausbeutung von Kindern angenommene Globale Verpflichtung von Yokohama und die auf der Vorbereitungskonferenz des zweiten Weltkongresses gegen kommerzielle sexuelle Ausbeutung von Kindern angenommene Verpflichtung von Budapest mit dem dazugehörigen Aktionsplan,

– unter Hinweis auf das Übereinkommen des Europarats vom 25. Oktober 2007 zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch,

– unter Hinweis auf seine Entschließung vom 20. November 2012 zum Kinderschutz in der digitalen Welt[1],

– unter Hinweis auf seine Entschließung vom 11. März 2015 zum sexuellen Missbrauch

[1] ABl. C 419 vom 16.12.2015, S. 33.

von Kindern im Internet[1],

– unter Hinweis auf den Rahmenbeschluss 2001/413/JAI des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[2],

– unter Hinweis auf das Budapester Übereinkommen über Computerkriminalität vom 23. November 2001[3] und dessen Zusatzprotokoll,

– unter Hinweis auf die Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Agentur der Europäischen Union für Netz- und Informationssicherheit[4],

– unter Hinweis auf die Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[5],

– unter Hinweis auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[6],

– unter Hinweis auf die Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI[7],

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

– unter Hinweis auf die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates[8],

– unter Hinweis auf die Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen[9] („EEA-Richtlinie“),

– unter Hinweis auf das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom

---

1 ABl. C 316 vom 30.8.2016, S. 109.
2 ABl. L 149 vom 2.6.2001, S. 1.
3 Europarat, Sammlung der Europaratsverträge, Nr. 185, 23.11.2001.
4 ABl. L 77 vom 13.3.2004, S. 1.
5 ABl. L 345 vom 23.12.2008, S. 75.
6 ABl. L 201 vom 31.7.2002, S. 37.
7 ABl. L 335 vom 17.12.2011, S. 1.
8 ABl. L 218 vom 14.8.2013, S. 8.
9 ABl. L 130 vom 1.5.2014, S. 1.

8. April 2014[1], mit dem die Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt wurde,

– unter Hinweis auf die Entschließung des Europäischen Parlaments vom 12. September 2013 mit dem Titel „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“[2],

– unter Hinweis auf die Mitteilung der Kommission vom 6. Mai 2015 mit dem Titel „Strategie für einen digitalen Binnenmarkt für Europa“ (COM(2015)0192),

– unter Hinweis auf die Mitteilung der Kommission vom 28. April 2015 mit dem Titel „Die Europäische Sicherheitsagenda“ (COM(2015)0185) und die nachfolgenden Fortschrittsberichte mit dem Titel „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“,

– unter Hinweis auf den Bericht der am 7. und 8. März 2016 in Amsterdam veranstalteten Konferenz zu dem Thema „Gerichtliche Zuständigkeit im virtuellen Raum“,

– unter Hinweis auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO)[3],

– unter Hinweis auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[4],

– unter Hinweis auf die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol)[5],

– unter Hinweis auf den Beschluss der Kommission vom 5. Juli 2016 über die Unterzeichnung einer vertraglichen Vereinbarung über eine öffentlich-private Partnerschaft für industrielle Forschung und Innovation auf dem Gebiet der Cybersicherheit zwischen der Europäischen Union, vertreten durch die Kommission, und dem Interessenverband (C(2016)4400),

– unter Hinweis auf die gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik und Vizepräsidentin der Kommission 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),

---

1 ECLI:EU:C:2014:238.
2 ABl. C 93 vom 9.3.2016, S. 112.
3 ABl. L 119 vom 4.5.2016, S. 1.
4 ABl. L 119 vom 4.5.2016, S. 89.
5 ABl. L 135 vom 24.5.2016, S. 53.

– unter Hinweis auf die Mitteilung der Kommission mit dem Titel „Europäische Strategie für ein besseres Internet für Kinder“ (COM(2012)0196) und den Bericht der Kommission vom 6. Juni 2016 mit dem Titel „Abschlussbewertung des Mehrjahresprogramms der EU zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien („Sicheres Internet“)“ (COM(2016)0364),

– unter Hinweis auf die gemeinsame Erklärung von Europol und der ENISA vom 20. Mai 2016 zur rechtmäßigen Strafverfolgung im Einklang mit den Datenschutzbestimmungen des 21. Jahrhunderts,

– unter Hinweis auf die Schlussfolgerungen des Rates vom 9. Juni 2016 zum Europäischen Justiziellen Netz für Cyberkriminalität,

– 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 Netzen und Informationssystemen in der Union[1],

– unter Hinweis auf die Stellungnahme der ENISA vom Dezember 2016 zu dem Thema „Leistungsfähige Verschlüsselung und Schutz der digitalen Identität“,

– unter Hinweis auf den Abschlussbericht der Arbeitsgruppe Cloud-Beweismittel des Europarates mit dem Titel „Zugang der Strafjustiz zu elektronischen Beweismitteln in der Cloud: Empfehlungen für die Beratungen der Arbeitsgruppe“ vom 16. September 2016,

– unter Hinweis auf die Tätigkeit der gemeinsamen Arbeitsgruppe gegen Cyberkriminalität (J-CAT),

– unter Hinweis auf die Europol-Berichte SOCTA (Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität) vom 28. Februar 2017 und IOCTA (Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet) vom 28. September 2016,

– unter Hinweis auf das Urteil des EuGH vom 21. Dezember 2016 in der Rechtssache C-203/15 (Tele2-Urteil)[2],

– unter Hinweis auf die Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates[3],

– gestützt auf Artikel 52 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres und die Stellungnahme des Ausschusses für die Rechte der Frau und die

---

1 ABl. L 194 vom 19.7.2016, S. 1.

2 Urteil des Gerichtshofs vom 21. Dezember 2016 in der Rechtssache C-203/15 Tele2 Sverige AB gegen Post- och telestyrelsen und Secretary of State for the Home Department gegen Tom Watson und andere, ECLI:EU:C:2016:970.

3 ABl. L 88 vom 31.3.2017, S. 6.

Gleichstellung der Geschlechter (A8-0272/2017),

A. in der Erwägung, dass durch Cyberkriminalität in zunehmendem Maße erheblicher sozialer und wirtschaftlicher Schaden verursacht wird und auf diese Weise die Grundrechte der Bürger beeinträchtigt wird, die Rechtsstaatlichkeit im Cyberraum bedroht ist und die Stabilität demokratischer Gesellschaften gefährdet ist;

B. in der Erwägung, dass Cyberkriminalität in den Mitgliedstaaten mehr und mehr zum Problem wird;

C. in der Erwägung, dass im IOCTA-Bericht 2016 aufgezeigt wird, dass die Cyberkriminalität an Intensität, Komplexität und Ausmaß zunimmt, dass die Zahl der gemeldeten Fälle von Cyberkriminalität in manchen Mitgliedstaaten größer ist als die Zahl herkömmlicher Straftaten, dass sich die Cyberkriminalität auf andere Deliktsbereiche wie Menschenhandel ausweitet, dass die Nutzung von Verschlüsselungs- und Anonymisierungsprogrammen zu kriminellen Zwecken zunimmt und dass es mehr Angriffe durch Erpressungssoftware als herkömmliche Bedrohungen durch Schadprogramme wie Trojaner gibt;

D. in der Erwägung, dass die Zahl der Angriffe auf Server der Kommission 2016 gegenüber 2015 um 20 % gestiegen ist;

E. in der Erwägung, dass die Anfälligkeit von Computern gegenüber Angriffen auf die einzigartigen Entwicklungsfortschritte der Informationstechnologie im Laufe der Jahre, das rasche Wachstum des Online-Geschäfts und auf die Untätigkeit staatlicher Einrichtungen zurückzuführen ist;

F. in der Erwägung, dass der Schwarzmarkt für computergestützte Erpressung, die Nutzung gemieteter Botnetze, Hackerangriffe und gestohlene digitale Güter immer größer wird;

G. in der Erwägung, dass der Schwerpunkt der Cyberangriffe nach wie vor auf Schadsoftware wie zum Beispiel Banken-Trojanern liegt, aber auch die Anzahl und Schwere der Angriffe auf industrielle Steuerungssysteme und Steuerungsnetze zunehmen, durch die kritische Infrastruktur und Wirtschaftsstrukturen zerstört und Gesellschaften destabilisiert werden sollen, wie im Fall des Angriffs mit der Erpressungssoftware „WannaCry“ im Mai 2017, was eine wachsende Bedrohung für die Sicherheit, Verteidigung und andere wichtige Bereiche darstellt; in der Erwägung, dass der Großteil der internationalen Datenanfragen im Bereich Strafverfolgung in Zusammenhang mit Finanzbetrug und Finanzkriminalität steht, dann folgen Gewaltverbrechen und schwere Straftaten;

H. in der Erwägung, dass die kontinuierlich zunehmende Vernetzung von Menschen, Orten und Dingen zwar viele Vorteile mit sich bringt, aber auch das Risiko der Cyberkriminalität erhöht; in der Erwägung, dass an das Internet der Dinge angeschlossene Geräte, etwa intelligente Netze, mit dem Internet verbundene Kühlschränke, Autos, medizinische Geräte oder Hilfsmittel, häufig nicht so gut geschützt sind wie herkömmliche, mit dem Internet verbundene Geräte und deshalb ein ideales Ziel für Cyberkriminelle abgeben, zumal die Regelungen für Sicherheitsaktualisierungen für an das Internet der Dinge angeschlossene Geräte häufig lückenhaft und manchmal schlicht nicht vorhanden sind; in der Erwägung, dass

gehackte Geräte des Internets der Dinge, die physische Stellglieder haben oder steuern können, unter Umständen eine konkrete Gefahr für das Leben von Menschen darstellen können;

I. in der Erwägung, dass ein wirksamer Datenschutz-Rechtsrahmen unbedingt erforderlich ist, um Vertrauen in die Online-Welt zu schaffen, wodurch Verbrauchern und Unternehmen gleichermaßen die Möglichkeit geboten wird, die Vorteile des digitalen Binnenmarkts uneingeschränkt auszuschöpfen und Cyberkriminalität zu bekämpfen;

J. in der Erwägung, dass die Unternehmen die Herausforderung, die vernetzte Welt sicherer zu machen, nicht allein bewältigen können und dass die Staaten zur Cybersicherheit beitragen sollten, indem sie Vorschriften erlassen und Anreize für ein weniger riskantes Verhalten der Nutzer setzen;

K. in der Erwägung, dass die Grenzen zwischen Cyberkriminalität, Cyberspionage, Cyberkrieg, Cybersabotage und Cyberterrorismus zunehmend verschwimmen; in der Erwägung, dass die Cyberkriminalität sowohl Einzelpersonen als auch öffentliche oder private Einrichtungen zum Ziel haben und eine große Bandbreite von Straftaten umfassen kann, etwa Verletzungen der Privatsphäre, sexueller Missbrauch von Kindern im Internet, Aufstachelung der Öffentlichkeit zu Gewalt und Hass, Sabotage, Spionage, Finanzkriminalität und Betrügereien wie Zahlungsbetrug, Diebstahl und Identitätsdiebstahl und rechtswidrige Eingriffe in Computersysteme;

L. in der Erwägung, dass groß angelegter Datenbetrug und Datendiebstahl im Welt-Risiko-Bericht 2017 des Weltwirtschaftsforums als eines der fünf globalen Risiken ausgewiesen ist, bei denen die Wahrscheinlichkeit, dass sie tatsächlich eintreten, am höchsten ist;

M. in der Erwägung, dass eine beträchtliche Anzahl der Fälle von Cyberkriminalität ungeahndet und ungestraft bleibt; in der Erwägung, dass nach wie vor zahlreiche Fälle nicht angezeigt werden, Cyberkriminelle infolge der langen Ermittlungszeiten mehrere Zugänge/Ausgänge oder Hintertüren entwickeln können, der Zugang zu elektronischen Beweismitteln schwierig ist, Probleme bei der Erlangung von Beweismitteln und ihrer Zulassung vor Gericht auftreten sowie komplexe Verfahren und rechtliche Herausforderungen in Zusammenhang mit dem grenzüberschreitenden Charakter von Cyberkriminalität bestehen;

N. in der Erwägung, dass der Rat in seinen Schlussfolgerungen vom Juni 2016 betonte, dass angesichts des grenzüberschreitenden Charakters der Cyberkriminalität und der gemeinsamen Bedrohungen für die Cybersicherheit, denen die EU gegenübersteht, eine verstärkte Zusammenarbeit und ein Informationsaustausch zwischen den Polizei- und Justizbehörden und den Experten auf dem Gebiet der Cyberkriminalität von entscheidender Bedeutung ist, wenn es darum geht, wirksame Ermittlungen im Cyberraum durchzuführen und elektronische Beweismittel zu erlangen;

O. in der Erwägung, dass mit der Nichtigerklärung der Richtlinie über die Vorratsdatenspeicherung durch den EuGH (Urteil vom 8. April 2014) und dem Verbot einer allgemeinen, undifferenzierten und nicht zielgerichteten Vorratsdatenspeicherung, das der EuGH in seiner Entscheidung in der Rechtssache Tele2 am 21. Dezember 2016 bestätigte, der Verarbeitung von Massen-Telekommunikationsdaten und dem Zugriff der zuständigen Behörden auf diese Daten enge Grenzen gesetzt wurden;

P. in der Erwägung, dass der EuGH[1] in seiner Entscheidung in der Rechtssache Maximilian Schrems klargestellt hat, dass Massenüberwachung gegen die Grundrechte verstößt;

Q. in der Erwägung, dass bei der Bekämpfung von Cyberkriminalität dieselben Verfahrensgarantien und inhaltlichen Garantien und dieselben Grundrechte – insbesondere mit Blick auf den Datenschutz und die Meinungsfreiheit – wie bei der Bekämpfung anderer Kriminalitätsformen gewahrt werden müssen;

R. in der Erwägung, dass Kinder das Internet in immer jüngerem Alter nutzen und in besonderem Maße Gefahr laufen, Opfer einer Kontaktaufnahme zu Missbrauchszwecken („Grooming“) und anderer Formen der sexuellen Ausbeutung im Internet (Cybermobbing, sexueller Missbrauch, sexuelle Nötigung und Erpressung) zu werden, und dass sie durch die widerrechtliche Aneignung personenbezogener Daten und durch gefährliche Kampagnen, mit denen verschiedene Formen der Selbstverletzung propagiert werden, wie beispielsweise bei dem Spiel „Blue Whale“, gefährdet sind und deshalb besonderen Schutz benötigen; in der Erwägung, dass Täter im Internet über Chaträume, E-Mails, Online-Spiele, Websites und soziale Netzwerke schneller ihre Opfer ausfindig machen und zu ihnen Kontakt aufnehmen können, und dass verborgene Peer-to-Peer-Netzwerke (P2P-Netzwerke) nach wie vor die zentralen Plattformen sind, über die einschlägige Täter Inhalte abrufen, die den sexuellen Missbrauch von Kindern zeigen, solche Inhalte speichern und austauschen und sich unerkannt an neue Opfer heranpirschen;

S. in der Erwägung, dass die zunehmende Tendenz zu sexueller Nötigung und Erpressung noch nicht hinreichend untersucht wurde und die Fälle nicht immer angezeigt werden, was in erster Linie darauf zurückzuführen ist, dass solche Straftaten bei den Opfern Scham- und Schuldgefühle hervorrufen;

T. in der Erwägung, dass die Online-Liveübertragung von Kindesmissbrauch als zunehmende Bedrohung betrachtet wird; in der Erwägung, dass die Online-Liveübertragung von Kindesmissbrauch am offensichtlichsten mit der kommerziellen Verbreitung von kinderpornografischem Material verknüpft ist;

U. in der Erwägung, dass die National Crime Agency im Vereinigten Königreich in einer aktuellen Studie herausgefunden hat, dass jüngere Menschen, die Hackerangriffe ausführen, weniger an Geld interessiert sind, sondern häufig in Computernetze eindringen, um Freunde zu beeindrucken oder den Staat herauszufordern;

V. in der Erwägung, dass die Sensibilisierung für die Risiken der Cyberkriminalität zwar gestiegen ist, doch die Schutzmaßnahmen einzelner Nutzer und öffentlicher Einrichtungen und Unternehmen nach wie vor völlig unzureichend sind, was in erster Linie auf mangelndes Wissen und fehlende Ressourcen zurückzuführen ist;

W. in der Erwägung, dass durch die Bekämpfung von Cyberkriminalität und illegalen Online-Aktivitäten die positiven Aspekte eines freien und offenen Cyberraums nicht in den Hintergrund geraten dürfen, die in neuen Möglichkeiten für die Weitergabe von Wissen und für die Förderung der politischen und sozialen Inklusion weltweit bestehen;

---

[1] ECLI:EU:C:2015:650.

Allgemeine Überlegungen

1. betont, dass die starke Zunahme des Einsatzes von Erpressungssoftware, Botnetzen und unbefugten Eingriffen in Computersysteme Auswirkungen auf die Sicherheit von Menschen, die Verfügbarkeit und Integrität personenbezogener Daten und den Schutz der Privatsphäre und der Grundfreiheiten hat und außerdem die Integrität von Einrichtungen der kritischen Infrastruktur wie der Energie- und Stromversorgung und von Teilen des Geld- und Kreditsystems wie Börsen beeinträchtigen kann; weist in diesem Zusammenhang erneut darauf hin, dass die Bekämpfung der Cyberkriminalität zu den Prioritäten der Europäischen Sicherheitsagenda vom 28. April 2015 zählt;

2. hält es für dringend geboten, gemeinsame Definitionen für Cyberkriminalität, Cyberkriegführung, Cybersicherheit, Cybermobbing und Cyberangriffe zu entwickeln, damit sichergestellt ist, dass die Organe der EU und die Mitgliedstaaten dieselbe Legaldefinition nutzen;

3. betont, dass bei der Bekämpfung der Cyberkriminalität zuallererst Einrichtungen der kritischen Infrastruktur und andere vernetzte Geräte geschützt und widerstandsfähiger gemacht werden sollten und nicht nur über repressive Maßnahmen nachgedacht werden sollte;

4. bekräftigt, dass rechtliche Schritte auf europäischer Ebene unternommen werden müssen, um die Definition der Straftatbestände, die Angriffe auf Informationssysteme sowie den sexuellen Missbrauch und die sexuelle Ausbeutung von Kindern im Internet betreffen, zu harmonisieren und die Mitgliedstaaten zu verpflichten, ein System zur Erfassung, Erstellung und Bereitstellung von statistischen Daten über solche Straftaten einzurichten, damit diese Formen der Kriminalität wirksamer bekämpft werden können;

5. fordert die Mitgliedstaaten nachdrücklich auf, die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie zügig und ordnungsgemäß umzusetzen und anzuwenden, sofern dies noch nicht geschehen ist; fordert die Kommission auf, die vollständige und tatsächliche Umsetzung der Richtlinie sorgsam zu überwachen und sicherzustellen, das Parlament und dessen zuständigen Ausschuss rasch über ihre Erkenntnisse zu informieren und gleichzeitig den Rahmenbeschluss des Rates 2004/68/JI zu ersetzen; betont, dass Eurojust und Europol mit genügend Ressourcen ausgestattet werden müssen, um die Opferidentifizierung zu verbessern und es diesen Organisationen zu ermöglichen, gegen organisierte Netze von Tätern des sexuellen Missbrauchs vorzugehen und kinderpornografisches Material im Internet und außerhalb des Internets schneller zu entdecken, zu prüfen und zu melden;

6. bedauert, dass 80 % der Unternehmen in Europa mindestens einmal von einem Cybervorfall betroffen waren und dass Cyberangriffe auf Unternehmen häufig unentdeckt bleiben oder nicht zur Anzeige gebracht werden; weist darauf hin, dass mehreren Studien zufolge die jährlichen Kosten von Cyberangriffen für die Weltwirtschaft erheblich sind; ist der Ansicht, dass die Pflicht zur Offenlegung von Sicherheitslücken und zum Austausch von Informationen über Risiken, die mit der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO) und mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

(Richtlinie über Netz- und Informationssicherheit – NIS-Richtlinie) eingeführt wurde, dazu beitragen dürfte, dieses Problem in den Griff zu bekommen, indem Unternehmen, insbesondere KMU, Unterstützung angeboten wird;

7. betont, dass die sich kontinuierlich wandelnden Cyberbedrohungen große rechtliche und technologische Herausforderungen für alle interessierten Akteure sind; ist der Auffassung, dass neue Technologien nicht als Bedrohung betrachtet werden sollten, und weist darauf hin, dass der Fortschritt der Technik auf dem Gebiet der Verschlüsselung zu einer Verbesserung der allgemeinen Sicherheit der Informationssysteme führen wird, etwa indem die Endnutzer in die Lage versetzt werden, ihre Daten und ihre Kommunikation besser zu schützen; weist jedoch darauf hin, dass immer noch erhebliche Lücken bei der Sicherung der Kommunikation bestehen und dass Verfahren wie die Mehrfachverschlüsselung nach dem Zwiebelschalenprinzip (Onion-Routing) und verborgene Netzwerke von böswilligen Nutzern, einschließlich Terroristen und Personen, die sexuelle Straftaten an Kindern begehen, sowie von Hackern, die von nicht befreundeten ausländischen Staaten finanziert werden, oder von extremistischen politischen oder religiösen Organisationen zu kriminellen Zwecken verwendet werden können, insbesondere zur Verschleierung ihrer kriminellen Aktivitäten oder ihrer Identitäten, wodurch die Ermittlungsbehörden vor enorme Herausforderungen gestellt werden;

8. bekundet seine große Besorgnis über den jüngsten weltweiten Angriff mit Erpressungssoftware, von dem offensichtlich Zehntausende Computer in annähernd 100 Ländern und zahlreiche Organisationen betroffen waren, darunter auch der National Health Service (NHS) des Vereinigten Königreichs, der das bekannteste Opfer dieses breit angelegten Angriffs mit Schadsoftware war; würdigt in diesem Zusammenhang die wichtige Tätigkeit der Initiative „No More Ransom“ (Keine Erpressung mehr), die mehr als 40 kostenfreie Entschlüsselungswerkzeuge anbietet, mit denen Opfer von Erpressungssoftware auf der ganzen Welt ihre Daten auf betroffenen Geräten entschlüsseln können;

9. betont, dass durch verborgene Netzwerke und das Onion-Routing in manchen Ländern auch freie Räume für Journalisten, politisch Engagierte und Menschenrechtsverfechter geschaffen werden und verhindert wird, dass repressive staatliche Stellen dieser Personen habhaft werden;

10. stellt fest, dass Netze von Kriminellen und Terroristen bislang nur in begrenztem Maße auf Werkzeuge und Dienstleistungen für Cyberkriminalität zugreifen können; hebt jedoch hervor, dass sich dies wahrscheinlich schon angesichts der immer engeren Verbindungen zwischen Terrorismus und organisierter Kriminalität und der großen Verfügbarkeit von Schusswaffen und sprengstofffähigem Material in verborgenen Netzwerken ändern dürfte;

11. verurteilt aufs Schärfste jedweden Eingriff in Systeme, der von einem fremden Staat oder dessen Agenten vorgenommen oder gesteuert wird, um demokratische Prozesse in einem anderen Land zu stören;

12. betont, dass grenzübergreifende Aufforderungen zum Domänendiebstahl, zum Entfernen von Inhalten und zum Zugriff auf Nutzerdaten schwierige Herausforderungen darstellen, auf die umgehend reagiert werden muss, da viel auf dem Spiel steht; betont in diesem Zusammenhang, dass die internationalen Rahmenregelungen im Bereich der

Menschenrechte, die sowohl für die Online-Welt als auch im wirklichen Leben gelten, als wichtiger Maßstab auf globaler Ebene dienen;

13. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass die Opfer von Cyberangriffen die in der Richtlinie 2012/29/EU verankerten Rechte in vollem Umfang in Anspruch nehmen können; fordert die Mitgliedstaaten außerdem auf, ihre Anstrengungen in Bezug auf die Identifizierung von Opfern und opferbezogene Dienste zu intensivieren, etwa indem sie die Europol-Arbeitsgruppe zur Identifizierung von Opfern auch künftig unterstützen; fordert die Mitgliedstaaten auf, in Zusammenarbeit mit Europol umgehend entsprechende Plattformen einzurichten, damit alle Internetnutzer wissen, wie sie gezielte Hilfe beantragen können, wenn sie von rechtswidrigen Online-Angriffen betroffen sind; fordert die Kommission auf, auf der Grundlage der Richtlinie 2012/29/EU eine Studie zu den Auswirkungen der grenzübergreifenden Cyberkriminalität auszuarbeiten;

14. betont, dass im Europol-Bericht 2014 über die Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität – unter Berücksichtigung der bestehenden Beschränkungen der Verfahren im Rahmen von Rechtshilfeabkommen – darauf hingewiesen wird, dass effizientere und wirksamere rechtliche Instrumente benötigt werden, und dass darin zudem eine weitergehende Harmonisierung der Rechtsvorschriften in der EU empfohlen wird, soweit hierfür Bedarf besteht;

15. hebt hervor, dass Cyberkriminalität das Funktionieren des digitalen Binnenmarkts gravierend beeinträchtigt, da sie das Vertrauen in die Anbieter digitaler Dienste schmälert, die Sicherheit grenzübergreifender Transaktionen schwächt und den Interessen der Nutzer digitaler Dienste erheblich schadet;

16. betont, dass Strategien und Maßnahmen im Bereich Cybersicherheit nur dann tragfähig und wirksam sein können, wenn die Cybersicherheit auf den in der Charta der Grundrechte der Europäischen Union verankerten Grundrechten und Grundfreiheiten und auf den Grundwerten der EU beruht;

17. erachtet es als berechtigterweise und dringend geboten, die Kommunikation zwischen Privatpersonen sowie zwischen Privatpersonen und öffentlichen und privaten Organisationen zu schützen, um der Cyberkriminalität vorzubeugen; betont, dass durch starke Verschlüsselung dazu beigetragen werden kann, dieser Anforderung zu entsprechen; betont außerdem, dass durch eine Einschränkung der Verwendung oder eine Schwächung der Leistung von Verschlüsselungswerkzeugen Schwachstellen, die zu kriminellen Zwecken ausgenutzt werden können, geschaffen werden und das Vertrauen in elektronische Dienste ausgehöhlt wird, was wiederum der Zivilgesellschaft und der Wirtschaft gleichermaßen schadet;

18. fordert einen Aktionsplan zum Schutz der Rechte von Kindern im Cyberraum, sowohl in den Netzen als auch im wirklichen Leben, und weist darauf hin, dass die Strafverfolgungsbehörden bei der Bekämpfung von Cyberkriminalität in erster Linie an Kindern begangene Straftaten ins Visier nehmen müssen; betont in diesem Zusammenhang, dass die Mitgliedstaaten die justizielle und polizeiliche Zusammenarbeit untereinander und mit Europol und dessen Europäischem Zentrum zur Bekämpfung der Cyberkriminalität intensivieren müssen, um der Cyberkriminalität und insbesondere der sexuellen Ausbeutung von Kindern im Internet vorzubeugen und sie zu bekämpfen;

19. fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, alle rechtlichen Hebel in Bewegung zu setzen, um gegen das Phänomen der Online-Gewalt gegen Frauen und Cybermobbing vorzugehen; fordert die EU und die Mitgliedstaaten insbesondere auf, mit vereinten Kräften einen rechtlichen Rahmen zur Verfolgung von Straftaten zu schaffen, mit dem Online-Unternehmen verpflichtet werden, herabsetzende, beleidigende und entwürdigende Inhalte zu löschen oder ihre Verbreitung zu unterlassen; fordert außerdem, für die psychologische Unterstützung von Frauen und Mädchen zu sorgen, die Opfer von Online-Gewalt oder Cybermobbing geworden sind;

20. betont, dass illegale Online-Inhalte auf der Grundlage eines ordentlichen Gerichtsverfahrens umgehend entfernt werden sollten; hebt hervor, dass mittels Informations- und Kommunikationstechnologie Internetdienstanbietern und Hostdienstanbietern die Aufgabe zukommt, illegale Online-Inhalte auf Ersuchen der zuständigen Strafverfolgungsbehörde schnell und tatsächlich zu entfernen;

Präventivmaßnahmen

21. fordert die Kommission auf, im Rahmen der Überprüfung der Cybersicherheitsstrategie der Europäischen Union auch künftig Schwachstellen europäischer Einrichtungen der kritischen Infrastruktur mit Blick auf die Netze und die Informationssicherheit zu ermitteln, Anreize für die Entwicklung nicht anfälliger Systeme zu setzen und die Lage der EU und der Mitgliedstaaten in Bezug auf die Bekämpfung der Cyberkriminalität zu beurteilen, um die Trends und Entwicklungen bezüglich der Straftaten im Cyberraum besser nachvollziehen zu können;

22. betont, dass die Widerstandsfähigkeit gegenüber Cyberangriffen von wesentlicher Bedeutung für die Verhütung der Cyberkriminalität ist und ihr deshalb höchste Priorität eingeräumt werden sollte; fordert die Mitgliedstaaten auf, vorausschauende Strategien und Maßnahmen zum Schutz von Netzen und Einrichtungen der kritischen Infrastruktur zu ergreifen, und fordert einen umfassenden europäischen Ansatz bei der Bekämpfung der Cyberkriminalität, der mit den Grundrechten, dem Datenschutz, der Cybersicherheit, dem Verbraucherschutz und dem elektronischen Handel im Einklang steht;

23. begrüßt in diesem Zusammenhang, dass EU-Mittel in Forschungsprojekte wie die öffentlich-private Partnerschaft (ÖPP) für Cybersicherheit investiert werden, mit der in der EU die Widerstandsfähigkeit gegenüber Cyberangriffen durch Innovation und Kapazitätsausbau gefördert werden soll; würdigt insbesondere die Bemühungen der ÖPP für Cybersicherheit um die Entwicklung geeigneter Maßnahmen für den Umgang mit Zero-Day-Sicherheitslücken;

24. betont in diesem Zusammenhang die Bedeutung von kostenfreier und quelloffener Software; fordert, dass mehr EU-Finanzmittel speziell für die auf kostenfreier und quelloffener Software beruhende Forschung im Bereich IT-Sicherheit zur Verfügung gestellt werden;

25. nimmt besorgt zur Kenntnis, dass es nicht genügend qualifizierte IT-Fachleute gibt, die im Bereich Cybersicherheit tätig sind; fordert die Mitgliedstaaten mit Nachdruck auf, in Bildung zu investieren;

26. ist der Ansicht, dass der Regulierung eine größere Bedeutung im Umgang mit den Risiken für die Cybersicherheit zukommen sollte, indem Produkt- und Softwarestandards mit Blick auf das Design und spätere Aktualisierungen verbessert und Mindeststandards zu vorgegebenen Nutzernamen und Kennwörtern eingeführt werden;

27. fordert die Mitgliedstaaten nachdrücklich auf, den Informationsaustausch im Rahmen von Eurojust, Europol und der ENISA und den Austausch bewährter Verfahren im Rahmen des Europäischen CSIRT-Netzwerks und der CERT-Notfallteams in Bezug auf die Herausforderungen, mit denen sie bei der Bekämpfung der Cyberkriminalität konfrontiert sind, und im Hinblick auf konkrete rechtliche und technische Lösungen zur Überwindung dieser Probleme auszubauen und die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen; fordert die Kommission in diesem Zusammenhang auf, die konkrete Zusammenarbeit zu fördern und den Austausch von Informationen zu erleichtern, damit – wie in der NIS-Richtlinie vorgesehen – potenzielle Risiken vorausgesehen und bewältigt werden können;

28. ist besorgt über die Feststellung von Europol, dass ein Großteil der erfolgreichen Angriffe auf Privatpersonen auf mangelnde digitale Hygiene und mangelnde Nutzersensibilisierung oder auf ungenügende Sorgfalt bei technischen Sicherheitsvorkehrungen wie der eingebauten Sicherheit zurückzuführen ist; betont, dass die ersten Opfer schlecht gesicherter Hard- und Software die Nutzer sind;

29. fordert die Kommission und die Mitgliedstaaten auf, unter Einbindung aller relevanten Akteure und Interessenträger eine Sensibilisierungskampagne ins Leben zu rufen, in deren Rahmen Kinder darüber aufgeklärt werden, welche Gefahren im Internet lauern und wie sie darauf reagieren können, und Eltern, Betreuer und Pädagogen hierbei und beim Schutz von Kindern vor den Gefahren im Internet unterstützt werden; fordert die Kommission und die Mitgliedstaaten zudem auf, die Mitgliedstaaten bei der Einrichtung von Programmen zur Vorbeugung von sexuellem Missbrauch im Internet zu unterstützen, Sensibilisierungskampagnen für verantwortungsvolles Verhalten in sozialen Medien zu fördern und die wichtigsten Suchmaschinen und sozialen Netzwerke dazu anzuhalten, vorausschauend Maßnahmen für den Schutz von Kindern im Internet zu ergreifen;

30. fordert die Kommission und die Mitgliedstaaten auf, Sensibilisierungs-, Informations- und Präventionskampagnen durchzuführen und bewährte Verfahren zu fördern, damit die Bürger, insbesondere Kinder und andere schutzbedürftige Nutzer, aber auch zentralstaatliche und kommunale Einrichtungen, bedeutende Betreiber und Akteure der Privatwirtschaft, insbesondere KMU, für die Risiken der Cyberkriminalität sensibilisiert werden und erfahren, wie sie sich im Internet und ihre Geräte schützen können; fordert die Kommission und die Mitgliedstaaten außerdem auf, für praktische Sicherheitsmaßnahmen zu werben, etwa Verschlüsselungstechnologien, sonstige Technologien zur Verbesserung der Sicherheit und Privatsphäre und Anonymisierungstools;

31. ist der Ansicht, dass die Sensibilisierungskampagnen mit Schulungsprogrammen für eine sachkundige Nutzung von IT-Instrumenten einhergehen sollten; legt den Mitgliedstaaten nahe, Themen wie Cybersicherheit und Risiken und Folgen der Angabe personenbezogener Daten im Internet in die Lehrpläne der Schulen aufzunehmen; hebt in diesem Zusammenhang die Bemühungen hervor, die im Rahmen der 2012

vorgestellten Europäischen Strategie für ein besseres Internet für Kinder unternommen wurden;

32. hält es mit Blick auf die Bekämpfung der Cyberkriminalität für dringend geboten, dass die Bemühungen um Bildung und Ausbildung im Bereich der Netz- und Informationssicherheit verstärkt werden, indem Schulungsangebote für Studierende der Computerwissenschaften zur Netz- und Informationssicherheit, zur Entwicklung sicherer Software und zum Schutz personenbezogener Daten und außerdem Grundlagenschulungen in Netz- und Informationssicherheit für Bedienstete der öffentlichen Verwaltung eingerichtet werden;

33. vertritt die Auffassung, dass eine Versicherung gegen Cyberangriffe durch Hacker eines der Instrumente sein könnte, mit denen sowohl Unternehmen, die für das Softwaredesign haftbar gemacht werden, als auch Nutzer, die zur ordnungsgemäßen Verwendung der Software angehalten werden, dazu bewegt werden könnten, Sicherheitsmaßnahmen zu ergreifen;

34. betont, dass Unternehmen anhand regelmäßiger Bewertungen Schwachstellen und Risiken ermitteln und ihre Produkte und Dienste dadurch schützen sollten, dass Schwachstellen sofort behoben werden, unter anderem durch Maßnahmen des Patch-Managements und durch Datenschutzaktualisierungen, und dass sie außerdem die Folgen von Angriffen mit Erpressungssoftware durch die Einrichtung robuster Sicherungssysteme begrenzen und Cyberangriffe fortlaufend melden sollten;

35. fordert die Mitgliedstaaten nachdrücklich auf, die IT-Notfallteams einzurichten, an die sich Unternehmen und Verbraucher wenden können, um bösartige E-Mails und Websites zu melden, wie in der NIS-Richtlinie vorgesehen, damit die Mitgliedstaaten regelmäßig Informationen über Sicherheitsvorfälle erhalten und Maßnahmen zur Bekämpfung und Minderung des Risikos ihrer eigenen Systeme ergreifen können; fordert die Mitgliedstaaten auf, die Einrichtung einer Datenbank zur Erfassung aller Arten von Cyberkriminalität und zur Überwachung der Entwicklung der diesbezüglichen Erscheinungsformen zu prüfen;

36. fordert die Mitgliedstaaten nachdrücklich auf, Investitionen zu tätigen, mit denen die Sicherheit ihrer kritischen Infrastruktur und der damit verbundenen Daten erhöht wird, damit sie Cyberangriffen standhalten können;

Stärkung der Verantwortung und Haftung der Diensteanbieter

37. vertritt die Ansicht, dass die verstärkte Zusammenarbeit zwischen den zuständigen Behörden und den Diensteanbietern ein entscheidender Faktor ist, um die gegenseitige Rechtshilfe und die Verfahren zur gegenseitigen Anerkennung in den in den EU-Rechtsvorschriften festgelegten Bereichen zu beschleunigen und zu vereinfachen; fordert die Anbieter elektronischer Kommunikationsdienste, die nicht in der Union niedergelassen sind, auf, auf schriftlichem Wege Vertreter in der Union zu benennen;

38. bekräftigt, dass im Zusammenhang mit der Verschärfung der Haftungsregelungen im Bereich des Internets der Dinge in erster Linie bei den Herstellern angesetzt werden muss, was eine bessere Qualität der Produkte und ein sichereres Umfeld beim externen Zugriff und eine dokumentierte Möglichkeit zu Aktualisierungen zur Folge haben wird;

39. ist der Ansicht, dass in Anbetracht der Innovationstrends und des immer weiter verbreiteten Zugangs zu Geräten des Internets der Dinge besonderes Augenmerk auf die Sicherheit aller – auch der einfachsten – Geräte gerichtet werden sollte; ist der Ansicht, dass es im Interesse der Hardwarehersteller und der Entwickler innovativer Software liegt, in Lösungen zur Verhinderung von Cyberkriminalität zu investieren und Informationen über Bedrohungen der Cybersicherheit auszutauschen; fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, das Konzept der eingebauten Sicherheit zu fördern, und fordert die Branche eindringlich auf, in all diese Geräte solche Lösungen einzubauen; fordert in diesem Zusammenhang die Privatwirtschaft auf, freiwillige Maßnahmen wie das „IoT Trust Label“ umzusetzen, die auf der Grundlage einschlägiger EU-Rechtsvorschriften wie der NIS-Richtlinie entwickelt wurden und international anerkannten Standards entsprechen, damit das Vertrauen in die Sicherheit von Software und Geräten gestärkt wird;

40. legt den Diensteanbietern nahe, dem Verhaltenskodex zur Bekämpfung illegaler Hetze im Internet beizutreten, und fordert die Kommission und die teilnehmenden Unternehmen auf, ihre Zusammenarbeit in diesem Bereich fortzusetzen;

41. weist erneut darauf hin, dass gemäß der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt[1] („Richtlinie über den elektronischen Geschäftsverkehr“) Vermittler nur dann von der Haftung für Inhalte ausgenommen sind, wenn sie hinsichtlich der übermittelten oder gehosteten Inhalte eine neutrale und passive Rolle einnehmen, sie aber verpflichtet sind, Inhalte unverzüglich zu entfernen oder zu sperren, sobald sie tatsächliche Kenntnis von einem Verstoß oder einer rechtswidrigen Tätigkeit oder Informationen erlangen;

42. erachtet es als unbedingt erforderlich, die Datenbanken der Strafverfolgungsbehörden vor Sicherheitsvorfällen und unberechtigten Zugriffen zu schützen, da dieser Schutz eine auch für Privatpersonen wichtige Angelegenheit ist; äußert seine Besorgnis über die extraterritoriale Reichweite der Strafverfolgungsbehörden, wenn diese Stellen im Rahmen strafrechtlicher Ermittlungen auf Daten zugreifen, und betont, dass in dieser Hinsicht strenge Vorschriften erlassen werden müssen;

43. vertritt die Auffassung, dass Probleme im Zusammenhang mit illegalen Online-Aktivitäten schnell und effizient gelöst werden müssen, auch mithilfe von Verfahren zur Entfernung, wenn der jeweilige Inhalt nicht oder nicht mehr für die Aufdeckung, Untersuchung und Verfolgung benötigt wird; weist erneut darauf hin, dass die Mitgliedstaaten die Maßnahmen ergreifen können, die notwendig und verhältnismäßig sind, um den Zugang zu solchen Inhalten aus dem Gebiet der Union zu sperren, wenn eine Entfernung nicht möglich ist; betont, dass solche Maßnahmen mit den bestehenden Legislativ- und Gerichtsverfahren und mit der Charta im Einklang stehen und darüber hinaus angemessenen Garantien unterliegen müssen, darunter die Möglichkeit, den Rechtsweg zu beschreiten;

44. hebt hervor, dass den Anbietern von digitalen Diensten der Informationsgesellschaft eine entscheidende Aufgabe zukommt, wenn es gilt, illegale Inhalte im Internet auf Ersuchen der zuständigen Strafverfolgungsbehörde schnell und tatsächlich zu entfernen,

---

[1] ABl. L 178 vom 17.7.2000, S. 1.

und begrüßt die Fortschritte, die in dieser Hinsicht, etwa durch den Beitrag des EU-Internetforums, erzielt worden sind; betont, dass es eines stärkeren Engagements und einer verbesserten Zusammenarbeit der zuständigen Behörden und der Anbieter von Diensten der Informationsgesellschaft bedarf, um zu erwirken, dass die Unternehmen derartige Inhalte schnell und tatsächlich entfernen, und um zu verhindern, dass die im Zuge staatlicher Maßnahmen erfolgte Sperrung rechtswidriger Inhalte umgangen wird; fordert die Mitgliedstaaten auf, dafür zu sorgen, dass Plattformen, die sich nicht an die Regeln halten, rechtlich zur Verantwortung gezogen werden; bekräftigt, dass Maßnahmen zur Entfernung rechtswidriger Online-Inhalte in allgemeinen Geschäftsbedingungen nur dann zulässig sein sollten, wenn die Nutzer gemäß den nationalen Verfahrensregeln die Möglichkeit haben, ihre Rechte vor einem Gericht geltend zu machen, nachdem sie von derartigen Maßnahmen Kenntnis erlangt haben;

45. betont, dass gemäß seiner Entschließung vom 19. Januar 2016 mit dem Titel „Auf dem Weg zu einer Akte zum digitalen Binnenmarkt“[1] die beschränkte Haftung der Vermittler von wesentlicher Bedeutung für die Wahrung der Offenheit des Internets und der Grundrechte und für Rechtssicherheit und Innovation ist; begrüßt die Absicht der Kommission, Leitlinien für Melde- und Entfernungsverfahren bereitzustellen, um die Online-Plattformen dabei zu unterstützen, ihrer Verantwortung und den Haftungsregeln der Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) nachzukommen, wodurch für mehr Rechtssicherheit gesorgt und das Vertrauen der Nutzer gestärkt wird; fordert die Kommission nachdrücklich auf, einen Rechtsetzungsvorschlag zu diesem Thema vorzulegen;

46. fordert, dass auf der Grundlage des durch die Richtlinie über den elektronischen Geschäftsverkehr und die Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums vorgegebenen Regelungsrahmens der Ansatz „Folge dem Geld“ zur Anwendung kommt, wie er in der Entschließung des Parlaments vom 9. Juni 2015 mit dem Titel „Ein EU-Aktionsplan für einen neuen Konsens über die Durchsetzung von Immaterialgüterrechten“ [2]dargelegt wird;

47. hält es für entscheidend, den Inhalte-Moderatoren in privaten und öffentlichen Einrichtungen, deren Aufgabe es ist, Online-Inhalte auf ihre Anstößigkeit oder Rechtswidrigkeit hin zu beurteilen, kontinuierliche und gezielte Schulungen und psychologische Unterstützung anzubieten, da von ihnen in diesem Bereich die erste Reaktion ausgehen sollte;

48. fordert die Diensteanbieter auf, für eindeutige Meldearten und für eine klar festgelegte Back-Office-Infrastruktur zu sorgen, mit der eine schnelle und angemessene Bearbeitung von Meldungen sichergestellt werden kann;

49. fordert die Diensteanbieter auf, ihre Maßnahmen zur Sensibilisierung für die Risiken des Internets zu intensivieren, insbesondere im Hinblick auf Kinder, und zwar durch die Entwicklung interaktiver Instrumente und die Ausarbeitung von Informationsmaterial;

Verstärkung der polizeilichen und justiziellen Zusammenarbeit

50. ist besorgt darüber, dass eine beträchtliche Anzahl der Fälle von Cyberkriminalität

---

1 Angenommene Texte, P8_TA(2016)0009.
2 ABl. C 407 vom 4.11.2016, S. 25.

ungestraft bleibt; bedauert, dass durch die Nutzung von Technologien wie der Netzwerkadressübersetzung auf Betreiber-Ebene (NAT CGN) seitens der Internetzugangsanbieter Ermittlungen stark beeinträchtigt werden, da es so technisch nicht mehr möglich ist, den Nutzer einer IP-Adresse genau zu identifizieren und mithin im Internet begangene Straftaten einer konkreten Person zuzuordnen; betont, dass der rechtmäßige Zugriff der Strafverfolgungsbehörden auf sachdienliche Informationen in den Fällen gewährt werden muss, in denen dieser Zugriff aus Gründen der Sicherheit und Gerechtigkeit notwendig und verhältnismäßig ist; betont, dass die Justiz- und Strafverfolgungsbehörden mit angemessenen Ressourcen ausgestattet werden müssen, damit sie rechtmäßige Ermittlungen durchführen können;

51. fordert die Mitgliedstaaten nachdrücklich auf, den Anbietern von Verschlüsselungsdiensten keine Verpflichtungen aufzuerlegen, die zu einer Schwächung oder Gefährdung der Sicherheit ihrer Netze oder Dienstleistungen führen würden, wie etwa das Einbauen oder die Ermöglichung von Hintertüren; betont, dass tragfähige Lösungen angeboten werden müssen, und zwar im Wege von Rechtsvorschriften und des kontinuierlichen technischen Fortschritts, soweit es für die Justiz und die Sicherheit zwingend geboten ist; fordert die Mitgliedstaaten auf, nach Rücksprache mit den Justizorganen und Eurojust zusammenzuarbeiten, um die Bedingungen für eine rechtmäßige Nutzung von Online-Ermittlungswerkzeugen anzugleichen;

52. betont, dass die rechtmäßige Überwachung ein äußerst wirksames Mittel darstellen kann, um gegen rechtswidrige Hackeraktivitäten vorzugehen, allerdings nur, sofern diese Maßnahme notwendig und verhältnismäßig ist, auf einem ordentlichen Gerichtsverfahren beruht und die Grundrechte, das EU-Datenschutzrecht und die diesbezügliche Rechtsprechung uneingeschränkt gewahrt werden; fordert alle Mitgliedstaaten auf, von den Möglichkeiten einer gezielten rechtmäßigen Überwachung verdächtiger Personen Gebrauch zu machen, klare Regeln für das Verfahren der vorherigen richterlichen Genehmigung rechtmäßiger Überwachungsmaßnahmen festzulegen – auch in Bezug auf Beschränkungen hinsichtlich der Nutzung und Dauer rechtmäßiger Hackerinstrumente –, einen Überwachungsmechanismus einzurichten und wirksame Rechtsbehelfe für die Betroffenen solcher Hackeraktivitäten zur Verfügung zu stellen;

53. fordert die Mitgliedstaaten auf, mit der IKT-Sicherheitsgemeinschaft zusammenzuarbeiten und sie darin zu bestärken, sich noch tatkräftiger am „White Hat Hacking“ und an der Meldung illegaler Inhalte, beispielsweise von Material über sexuellen Missbrauch von Kindern, zu beteiligen;

54. fordert Europol auf, ein System für die anonyme Übermittlung von Informationen aus verborgenen Netzwerken einzurichten, über das einzelne Personen rechtswidrige Inhalte wie die Darstellung von sexuellem Missbrauch von Kindern den Behörden melden können, und zwar unter Nutzung ähnlicher technischer Vorkehrungen wie sie viele Presseorganisationen verwenden, um den Austausch sensibler Informationen mit Journalisten in einer Weise zu erleichtern, die ein höheres Maß an Anonymität und Sicherheit bietet, als es bei gewöhnlichen E-Mails der Fall ist;

55. betont, dass die Risiken für die Privatsphäre von Internetnutzern reduziert werden müssen, die sich daraus ergeben, dass an die Öffentlichkeit gelangt ist, welche Programmschwachstellen die Strafverfolgungsbehörden im Rahmen ihrer rechtmäßigen

Ermittlungen systematisch ausnutzen (Rückgriff auf sogenannte Exploits) und welche Instrumente sie einsetzen;

56. betont, dass die Justiz- und Strafverfolgungsbehörden über eine angemessene Kapazitäts- und Finanzausstattung verfügen müssen, damit sie wirksam auf Cyberkriminalität reagieren können;

57. betont, dass durch den Flickenteppich separater, territorial definierter nationaler Gerichtsbarkeiten die Ermittlung des anwendbaren Rechts bei transnationalen Interaktionen erschwert und Rechtsunsicherheit geschaffen wird, was zur Folge hat, dass grenzüberschreitende Zusammenarbeit, die für die wirksame Bekämpfung von Cyberkriminalität erforderlich wäre, verhindert wird;

58. betont, dass – wie in der informellen Sitzung der Justiz- und Außenminister vom 26. Januar 2016 festgestellt – eine praktische Grundlage für einen gemeinsamen Ansatz der EU im Bereich der gerichtlichen Zuständigkeit im Cyberraum entwickelt werden muss;

59. betont in diesem Zusammenhang, dass gemeinsame Verfahrensnormen ausgearbeitet werden müssen, mit denen die territorialen Faktoren bestimmt werden können, die die Grundlage für die im Cyberraum anzuwendenden Rechtsvorschriften bilden, und dass Ermittlungsmaßnahmen festgelegt werden müssen, die ungeachtet geografischer Grenzen eingesetzt werden können;

60. stellt fest, dass ein derartiger gemeinsamer Ansatz auf EU-Ebene, in dessen Rahmen die Grundrechte und die Privatsphäre geachtet werden müssen, bei den Interessenträgern Vertrauen schaffen, die Verzögerungen bei der Behandlung grenzübergreifender Anfragen verringern, für Interoperabilität unter verschiedenartigen Akteuren sorgen und die Möglichkeit eröffnen dürfte, Anforderungen an ordnungsgemäße Verfahren in operative Rahmen aufzunehmen;

61. vertritt die Auffassung, dass langfristig auch auf internationaler Ebene gemeinsame verfahrensrechtliche Standards für die Strafverfolgungszuständigkeit im Cyberraum ausgearbeitet werden sollten; begrüßt in diesem Zusammenhang die Arbeit der Arbeitsgruppe Cloud-Beweismittel des Europarats;

Elektronische Beweismittel

62. hebt hervor, dass ein gemeinsamer europäischer Ansatz zur Strafgerichtsbarkeit im Cyberraum dringend geboten ist, da so der Grundsatz der Rechtsstaatlichkeit im Cyberraum besser durchgesetzt werden kann, die Erlangung von elektronischen Beweismitteln in Strafverfahren vereinfacht wird und dazu beigetragen wird, dass Fälle viel schneller abgeschlossen werden können, als es heute der Fall ist;

63. betont, dass Mittel und Wege für eine schnellere Sicherung und Erlangung von elektronischen Beweismitteln gefunden werden müssen, und hebt hervor, dass die enge Zusammenarbeit zwischen den Strafverfolgungsbehörden wichtig ist, auch durch den verstärkten Einsatz gemeinsamer Ermittlungsgruppen und die Zusammenarbeit mit Drittstaaten und mit auf der Grundlage der DSGVO (EU) 2016/679, der Richtlinie (EU) 2016/680 (Polizei-Richtlinie) und bestehender Rechtshilfeabkommen im Gebiet der Union tätigen Diensteanbietern; betont, dass es zentrale Anlaufstellen in allen

Mitgliedstaaten einzurichten und die Inanspruchnahme der bestehenden Anlaufstellen zu optimieren gilt, da hierdurch der Zugang zu elektronischen Beweismitteln und der Austausch von Informationen vereinfacht wird, die Zusammenarbeit mit den Diensteanbietern verbessert wird und die Rechtshilfeverfahren beschleunigt werden;

64. stellt fest, dass die derzeit fragmentierten rechtlichen Rahmenbedingungen ein Problem für Diensteanbieter sein können, die darum bemüht sind, den Ersuchen von Strafverfolgungsbehörden nachzukommen; fordert die Kommission auf, einen Vorschlag für einen EU-Rechtsrahmen für elektronische Beweismittel vorzulegen, der auch harmonisierte Vorschriften für die Einstufung eines Anbieters als inländischer oder ausländischer Anbieter enthält; fordert die Kommission außerdem auf, die Diensteanbieter dazu zu verpflichten, den von anderen Mitgliedstaaten übermittelten Ersuchen nachzukommen, die auf einem ordentlichen Gerichtsverfahren beruhen und mit der Europäischen Ermittlungsanordnung im Einklang stehen, und dabei dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen, damit negative Auswirkungen auf die Ausübung der Niederlassungs- und Dienstleistungsfreiheit abgewendet und angemessene Garantien gewahrt werden, und zwar mit dem Ziel, Rechtssicherheit zu schaffen und die Diensteanbieter besser in die Lage zu versetzen, den Ersuchen der Strafverfolgungsbehörden nachzukommen;

65. betont, dass ein Rechtsrahmen für elektronische Beweismittel ausreichende Garantien hinsichtlich der Achtung der Rechte und Freiheiten aller Betroffenen vorsehen muss; hebt hervor, dass darin auch vorgeschrieben werden sollte, dass Ersuchen um Herausgabe elektronischer Beweismittel zunächst an die Verantwortlichen oder an die Eigentümer der Daten gerichtet werden müssen, damit sichergestellt ist, dass ihre Rechte und die Rechte jener, auf die sich die Daten beziehen (beispielsweise ihr Recht, sich auf den Schutz der Vertraulichkeit zu berufen und Rechtsbehelfe im Fall eines unverhältnismäßigen oder anderweitig rechtswidrigen Zugriffs einzulegen), geachtet werden; weist außerdem darauf hin, dass ein Rechtsrahmen die Anbieter und alle anderen Parteien vor Gesuchen schützen muss, die Normenkollisionen verursachen oder auf andere Weise die Souveränität anderer Staaten verletzen könnten;

66. fordert die Mitgliedstaaten auf, die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen (EEA-Richtlinie) vollständig umzusetzen, damit elektronische Beweismittel in der EU tatsächlich gesichert und erlangt werden können; fordert die Mitgliedstaaten zudem auf, besondere Bestimmungen über den Cyberraum in ihr jeweiliges Strafgesetzbuch aufzunehmen, um so die Zulässigkeit elektronischer Beweismittel vor Gericht zu erleichtern und der Richterschaft klarere Leitlinien für die Bestrafung von Cyberkriminalität an die Hand zu geben;

67. begrüßt die laufenden Arbeiten der Kommission an einer Kooperationsplattform, die einen sicheren Kommunikationskanal für den digitalen Austausch von Europäischen Ermittlungsanordnungen zu elektronischen Beweismitteln umfassen und der Kommunikation zwischen den Justizbehörden der EU-Mitgliedstaaten dienen soll; fordert die Kommission auf, in Zusammenarbeit mit den Mitgliedstaaten, Eurojust und den Diensteanbietern die Formulare, Instrumente und Verfahren für die Beantragung der Sicherung und Erlangung elektronischer Beweismittel zu überprüfen und anzugleichen, um die Authentifizierung zu erleichtern, für schnelle Verfahren zu sorgen und die Transparenz und Rechenschaftspflicht im Zusammenhang mit den Verfahren zur Sicherung und Erlangung elektronischer Beweismittel zu verbessern; fordert die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der

Strafverfolgung (CEPOL) auf, Ausbildungsmodule für die konkrete Anwendung des geltenden Rechtsrahmens auf die Sicherung und Erlangung elektronischer Beweismittel zu konzipieren; betont in diesem Zusammenhang, dass sich die Vielfalt der Ansätze durch eine Vereinheitlichung der Maßnahmen der Diensteanbieter verringern lässt, insbesondere, was die Verfahren und die Bedingungen für die Gewährung des Zugriffs auf die angeforderten Daten anbelangt;

Aufbau von Kapazitäten auf EU-Ebene

68. weist darauf hin, dass die jüngsten Vorfälle die extreme Anfälligkeit der EU – insbesondere der Organe der EU, der nationalen Regierungen und Parlamente, großer Unternehmen aus der EU und der IT-Infrastrukturen und -Netzwerke in der EU – gegenüber technisch ausgereiften Angriffen mit komplexer Software und Schadsoftware verdeutlichen; fordert die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) auf, die Bedrohungslage fortlaufend zu bewerten, und fordert die Kommission auf, in die IT-Kapazitäten und in den Schutz und die Widerstandsfähigkeit der kritischen Infrastrukturen der EU-Institutionen zu investieren, um die Anfälligkeit der EU gegenüber schweren Cyberangriffen, die von großen kriminellen Vereinigungen, staatlich finanzierten Angreifern oder terroristischen Gruppen ausgehen, zu verringern;

69. würdigt den wichtigen Beitrag des bei Europol und Eurojust angesiedelten Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3) und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) zur Bekämpfung der Cyberkriminalität;

70. fordert Europol auf, die nationalen Strafverfolgungsbehörden bei der Einrichtung sicherer und geeigneter Übertragungskanäle zu unterstützen;

71. bedauert, dass es gegenwärtig keine EU-Standards für Schulungen und Zertifizierungen gibt; stellt fest, dass die künftigen Entwicklungen im Bereich Cyberkriminalität in zunehmendem Maße Fachwissen von Sachverständigen erforderlich machen; begrüßt, dass mit Initiativen wie der Europäischen Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG), dem Projekt zur Ausbildung der Ausbilder (TOT) und den Schulungen im Rahmen für den EU-Politikzyklus bereits darauf hingearbeitet wird, den Mangel an Fachwissen auf EU-Ebene zu beheben;

72. fordert die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) und das Europäische Netz für die Aus- und Fortbildung von Richtern und Staatsanwälten auf, ihre Aus- und Fortbildungsangebote zu Themen der Cyberkriminalität auf die zuständigen Strafverfolgungs- und Justizbehörden in der gesamten Europäischen Union auszuweiten;

73. betont, dass die Zahl der Cyberkriminalitätsdelikte, die an Eurojust weitergeleitet wurden, um 30 % zugenommen hat; fordert, dass genügend Mittel bereitgestellt und erforderlichenfalls mehr Stellen geschaffen werden, damit Eurojust das steigende Arbeitsvolumen im Bereich Cyberkriminalität bewältigen und die Unterstützung der nationalen Staatsanwaltschaften im Bereich Cyberkriminalität in grenzüberschreitenden Fällen ausbauen und stärken kann, unter anderem durch das unlängst gegründete Europäische Justizielle Netz gegen Cyberkriminalität;

74. fordert, dass das Mandat der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) überarbeitet wird und die nationalen Agenturen für Cybersicherheit gestärkt werden; fordert, dass der ENISA mehr Aufgaben, Personal und Ressourcen zugewiesen werden; betont, dass das neue Mandat auch stärkere Verbindungen zu Europol und Interessenträgern aus der Wirtschaft umfassen sollte, damit die Agentur die zuständigen Behörden bei der Bekämpfung der Cyberkriminalität besser unterstützen kann;

75. fordert die Agentur der Europäischen Union für Grundrechte (FRA) auf, ein detailliertes Handbuch für die Praxis zu verfassen, mit dem den Mitgliedstaaten Leitlinien für Überwachungs- und Überprüfungsmaßnahmen an die Hand gegeben werden;

Bessere Zusammenarbeit mit Drittstaaten

76. betont, dass die enge Zusammenarbeit mit Drittstaaten im globalen Kampf gegen Cyberkriminalität wichtig ist, unter anderem durch den Austausch bewährter Verfahren, gemeinsame Ermittlungen, den Aufbau von Kapazitäten und die gegenseitige Rechtshilfe;

77. fordert die Mitgliedstaaten, auf, das Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität („Budapester Übereinkommen“) und dessen Zusatzprotokolle zu ratifizieren und vollständig umzusetzen, sofern dies noch nicht geschehen ist, und es in Zusammenarbeit mit der Kommission in den entsprechenden internationalen Foren bekannt zu machen;

78. bekräftigt seine starken Bedenken hinsichtlich der Arbeiten im Rahmen des Ausschusses für das Übereinkommen über Computerkriminalität des Europarats in Bezug auf die Auslegung von Artikel 32 des Budapester Übereinkommens, in dem der grenzüberschreitende Zugriff auf gespeicherte Computerdaten („Beweise in der Cloud“) geregelt ist, und spricht sich gegen die Unterzeichnung eines Zusatzprotokolls oder von Leitlinien aus, mit denen der Anwendungsbereich dieser Bestimmung über die geltenden Regelungen im Rahmen dieses Übereinkommens hinaus ausgeweitet wird, da diese Bestimmung bereits eine wesentliche Ausnahme vom Territorialitätsgrundsatz darstellt, da sie zu einem ungehinderten Fernzugriff von Strafverfolgungsbehörden auf Server und Computersysteme in anderen Gerichtsbarkeiten führen könnten, ohne dass dazu auf Rechtshilfeabkommen und andere Instrumente der justiziellen Zusammenarbeit zurückgegriffen wird, die zur Sicherung der Grundrechte der Einzelnen, einschließlich des Rechts auf Datenschutz und auf ein faires Verfahren, eingerichtet wurden und von denen insbesondere das Übereinkommen des Europarats Nr. 108 zu erwähnen ist;

79. bedauert, dass es keine verbindlichen internationalen Rechtsvorschriften über Cyberkriminalität gibt, und fordert die Mitgliedstaaten und die Organe der EU nachdrücklich auf, auf den Abschluss eines entsprechenden Übereinkommens hinzuarbeiten;

80. fordert die Kommission auf, mögliche Initiativen vorzuschlagen, um Rechtshilfeabkommen effizienter zu gestalten und ihre Anwendung zu fördern und auf diese Weise der Übernahme extraterritorialen Rechts durch Drittländer entgegenzutreten;

81. fordert die Mitgliedstaaten auf, ausreichende Kapazitäten für die Bearbeitung von Rechtshilfeersuchen um Ermittlungen im Cyberraum zu schaffen und einschlägige Schulungsprogramme für das für die Bearbeitung derartiger Ersuchen zuständige Personal auszuarbeiten;

82. hebt hervor, dass durch Abkommen über die strategische und operationelle Zusammenarbeit zwischen Europol und Drittstaaten sowohl der Informationsaustausch gefördert als auch die praktische Zusammenarbeit vorangebracht wird;

83. nimmt zur Kenntnis, dass sich die meisten Ersuchen von Strafverfolgungsbehörden an die USA und an Kanada richten; ist besorgt darüber, dass die Freigabequote von großen amerikanischen Anbietern in Reaktion auf Ersuchen von Strafverfolgungsbehörden aus der EU bei weniger als 60 % liegt, und weist erneut darauf hin, dass gemäß Kapitel V der DSGVO Rechtshilfeabkommen und andere internationale Abkommen das vorrangige Mittel sind, um Zugang zu personenbezogenen Daten im Ausland zu erlangen;

84. fordert die Kommission auf, mit dem Ziel einer besseren Rechtshilfe konkrete Maßnahmen vorzulegen, um die Grundrechte der verdächtigten oder beschuldigten Person beim Austausch von Informationen zwischen den Strafverfolgungsbehörden aus der EU und Drittstaaten zu schützen, insbesondere Garantien in Bezug auf die zügige Erlangung einschlägiger Beweismittel, Nutzerinformationen, detaillierter Metadaten und Inhaltsdaten (sofern sie nicht verschlüsselt sind) von Strafverfolgungsbehörden bzw. Diensteanbietern, sofern ein entsprechender Gerichtsbeschluss vorliegt;

85. fordert die Kommission auf, in Zusammenarbeit mit den Mitgliedstaaten, assoziierten europäischen Einrichtungen und, falls geboten, Drittstaaten neue Wege zu prüfen, um durch eine beschleunigte und vereinheitlichte Nutzung der Verfahren für gegenseitige Rechtshilfe und, falls vorhanden, gegenseitige Anerkennung elektronischer Beweismittel, die in Drittstaaten gespeichert sind, im Einklang mit den Grundrechten und den Datenschutzbestimmungen der EU wirksam sichern und erlangen zu können;

86. weist auf die Bedeutung des Reaktionszentrums der NATO für Cybervorfälle (NATO Cyber Incidents Response Centre) hin;

87. fordert alle Mitgliedstaaten auf, sich am globalen Forum für Cyber-Fachwissen (Global Forum on Cyber Expertise, GFCE) zu beteiligen, um den Abschluss von Partnerschaften zum Aufbau von Kapazitäten zu erleichtern;

88. unterstützt die Hilfe der EU für die Länder der östlichen Nachbarschaft beim Aufbau von Kapazitäten, da viele Cyberangriffe ihren Ursprung in diesen Ländern haben;

°

° °

89. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission zu übermitteln.