Europäisches Parlament
2014-2019

Plenarsitzungsdokument

B8-0154/2019

6.3.2019

ENTSCHLIESSUNGSANTRAG

eingereicht im Anschluss an Erklärungen des Rates und der Kommission

gemäß Artikel 123 Absatz 2 der Geschäftsordnung

zu Sicherheitsbedrohungen im Zusammenhang mit der zunehmenden technologischen Präsenz Chinas in der EU und möglichen Maßnahmen zu ihrer Verringerung auf EU-Ebene
(2019/2575(RSP))

Caroline Nagtegaal
im Namen der ALDE-Fraktion

B8-0154/2019

Entschließung des Europäischen Parlaments zu Sicherheitsbedrohungen im Zusammenhang mit der zunehmenden technologischen Präsenz Chinas in der EU und möglichen Maßnahmen zu ihrer Verringerung auf EU-Ebene (2019/2575(RSP))

Das Europäische Parlament,

– unter Hinweis auf die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation[1],

– unter Hinweis auf die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[2],

– unter Hinweis auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 13. September 2017 über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“) (COM(2017)0477),

– unter Hinweis auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Aufstellung des Programms „Digitales Europa“ für den Zeitraum 2021–2027, COM(2018)0434,

– unter Hinweis auf den Vorschlag für eine Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren (COM(2018)0630),

– unter Hinweis auf die Erklärungen des Rates und der Kommission vom 13. Februar 2019 zu Sicherheitsbedrohungen im Zusammenhang mit der zunehmenden technologischen Präsenz Chinas in der EU und möglichen Maßnahmen zu ihrer Verringerung auf EU-Ebene,

– unter Hinweis auf seine legislative Entschließung vom 14. Februar 2019 zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Europäischen Union[3],

– unter Hinweis auf seine Entschließungen zu den Beziehungen zwischen der EU und China, insbesondere jene vom 12. September 2018 zum Stand der Beziehungen zwischen der EU und China[4],

[1] ABl. L 321 vom 17.12.2018, S. 36.
[2] ABl. L 194 vom 19.7.2016, S. 1.
[3] Angenommene Texte, P8_TA(2019)0121.
[4] Angenommene Texte, P8_TA(2018)0343.

– unter Hinweis auf die Mitteilung der Kommission vom 14. September 2016 mit dem Titel „5G für Europa: ein Aktionsplan“ (COM(2016)0588),

– unter Hinweis auf seine Entschließung vom 1. Juni 2017 zu dem Thema „Internetanbindung für Wachstum, Wettbewerbsfähigkeit und Zusammenhalt: Europäische Gigabit-Gesellschaft und 5G“[5],

– 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)[6],

– unter Hinweis auf die Verordnung (EU) Nr. 1316/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 zur Schaffung der Fazilität „Connecting Europe“, zur Änderung der Verordnung (EU) Nr. 913/2010 und zur Aufhebung der Verordnungen (EG) Nr. 680/2007 und (EG) Nr. 67/2010[7],

– gestützt auf Artikel 123 Absatz 2 seiner Geschäftsordnung,

A. in der Erwägung, dass die Konnektivität in der digitalen Wirtschaft dank der 5G-Infrastruktur auf eine völlig neue Ebene gehoben wird; in der Erwägung, dass die 5G-Infrastruktur ein wichtiger Baustein der Gigabit-Gesellschaft ist, insbesondere in den Bereichen Verkehr, Energie und Gesundheit sowie in den Bereichen Verteidigung und Sicherheit, und dass die 5G-Infrastruktur für die Zukunft der Technologien der mobilen Kommunikation maßgeblich ist;

B. in der Erwägung, dass Schwachstellen in den 5G-Netzen ausgenutzt werden könnten, um IT-Systeme zu gefährden, wodurch sowohl auf europäischer als auch auf nationaler Ebene erhebliche Schäden in den Volkswirtschaften verursacht werden könnten; in der Erwägung, dass ein auf die Analyse der Risiken gestützter Ansatz erforderlich ist;

C. in der Erwägung, dass die zunehmende Bedeutung von Technologieanbietern aus Drittländern auf dem Unionsmarkt für 5G zu heftigen Diskussionen in den Mitgliedstaaten geführt hat, insbesondere im Zusammenhang mit dem seit Juni 2017 geltenden Nachrichtendienstgesetz Chinas;

D. in der Erwägung, dass der Umfang und die Parameter dessen, was die Staatsorgane Chinas als „nachrichtendienstliche Tätigkeit“ bezeichnen, im Nachrichtendienstgesetz Chinas nicht klar definiert sind; in der Erwägung, dass den Staatsorganen mit dem Gesetz neue Rechtsgründe übertragen werden, Personen und Einrichtungen aus dem In- und Ausland, also auch Unionsbürger und die Unionsorgane, zu überwachen und gegen sie zu ermitteln, um die nationale Sicherheit Chinas zu schützen;

E. in der Erwägung, dass chinesische Telekommunikationsunternehmen staatliche Beihilfen erhalten, mit denen ihre Fähigkeit zur Umsetzung des Nachrichtendienstgesetzes weiter gestärkt werden könnte, was nicht nur zu

[5] ABl. L 307 vom 30.8.2018, S. 144.
[6] ABl. L 119 vom 4.5.2016, S. 1.
[7] ABl. L 348 vom 20.12.2013, S. 129.

Sicherheitsproblemen führt, sondern diesen Unternehmen auch unfaire wirtschaftliche Vorteile verschafft;

F. in der Erwägung, dass mit der Verordnung über die Überprüfung ausländischer Direktinvestitionen, die bis Ende 2020 in Kraft treten soll, die Fähigkeit der Mitgliedstaaten gestärkt wird, anhand von Kriterien der Sicherheit und der öffentlichen Ordnung ausländische Investitionen zu überprüfen, und ein Kooperationsmechanismus eingerichtet wird, auf dessen Grundlage die Kommission und die Mitgliedstaaten bei der Bewertung der von ausländischen Investitionen ausgehenden Sicherheitsrisiken – einschließlich der Risiken für die Cybersicherheit – zusammenarbeiten können;

G. in der Erwägung, dass die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) zum 9. Mai 2018 in nationales Recht umgesetzt werden musste; in der Erwägung, dass mit dieser Richtlinie angestrebt wird, die Sicherheit der wesentlichen Infrastruktur in der Union zu erhöhen und dafür Sorge zu tragen, dass schwerwiegende Cybersicherheitsvorfälle gemeldet werden; in der Erwägung, dass die Telekommunikationsunternehmen nach Maßgabe der Richtlinie über den europäischen Kodex für die elektronische Kommunikation verpflichtet sind, Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten zu ergreifen sowie die Behörden und in bestimmten Fällen auch die Nutzer über schwerwiegende Sicherheitsvorfälle zu unterrichten;

H. in der Erwägung, dass der europäische Kodex für die elektronische Kommunikation vorsieht, dass bis Ende 2020 in der Union 5G-Funkfrequenzen zur Verfügung stehen; in der Erwägung, dass die Mitgliedstaaten im Rahmen des 5G-Ausbaus unabhängige Versteigerungen von Frequenznutzungsrechten durchführen, wodurch Unternehmen aus Drittländern in mehreren Mitgliedstaaten und mithin in der gesamten Union eine marktbeherrschende Stellung erlangen könnten; in der Erwägung, dass China eine ehrgeizige Strategie für künstliche Intelligenz verfolgt, in der Daten eine entscheidende Ressource sind;

1. hält es nach wie vor für dringend geboten, in der EU Kapazitäten und Fähigkeiten für die digitale Infrastruktur aufzubauen und gleichzeitig die strategische Autonomie der EU zu stärken; weist erneut auf die Bedeutung der 5G-Netze hin und bekräftigt daher sein Engagement für den 5G-Aktionsplan;

2. stellt nochmals fest, dass die Einführung der 5G-Netze vorangebracht werden wird, wenn nach Maßgabe des europäischen Kodex für die elektronische Kommunikation sichergestellt wird, dass bis Ende 2020 in der EU die entsprechenden Funkfrequenzen zur Verfügung stehen; betont, dass die fehlende Koordinierung und Berechenbarkeit die größte Herausforderung für die Betreiber ist;

3. bekräftigt, dass die Union gemeinsame Maßnahmen ergreifen muss, um die aktuellen Bedenken in Bezug auf von der Regierung Chinas unterstützte Telekommunikationsanbieter auszuräumen und so die digitale Widerstandsfähigkeit zu steigern und die Maßnahmen zum Schutz des Binnenmarkts zukunftssicher zu gestalten; fordert, in der Zwischenzeit den Informationsaustausch unter den Mitgliedstaaten der Union zu intensivieren;

4. fordert, dass mögliche Sicherheitsrisiken im Zusammenhang mit der Nutzung von Technologien aus Drittländern geprüft und 5G als kritische Infrastruktur eingestuft wird, damit alle Unternehmen strengere Sicherheitsnormen einhalten müssen;

5. begrüßt in diesem Zusammenhang, dass die Mitgliedstaaten im Rahmen des in der Verordnung über die Überprüfung ausländischer Direktinvestitionen vorgesehenen Mechanismus für die Zusammenarbeit Informationen untereinander austauschen sollen, und erachtet dieses Element als besonders wichtig;

6. hebt hervor, dass durch die Verordnung über die Überprüfung ausländischer Direktinvestitionen die kritische Infrastruktur geschützt wird; weist darauf hin, dass Unternehmen, die eine Geschäftstätigkeit in der Union ausüben, in den Genuss der Vorteile des Binnenmarkts kommen, jedoch die Normen und den Rechtsrahmen der Union einhalten müssen;

7. nimmt mit Interesse zur Kenntnis, dass die Zahl der Mitgliedstaaten, die einen Überprüfungsmechanismus anwenden, gestiegen ist, seit die Kommission 2017 ihren Vorschlag für eine Verordnung über die Überprüfung ausländischer Direktinvestitionen vorlegte;

8. unterstützt die Kommission in ihren vielfältigen Schritten, die sie bereits unternommen hat, damit mehr Maßnahmen gegen Bedrohungen der Cybersicherheit getroffen werden können und angemessene Risikomanagementmaßnahmen wirklich strikt umgesetzt werden, darunter auch Sanktionen gegen Anbieter, die ihren Verpflichtungen nicht nachkommen;

9. befürwortet und unterstützt die Einigung über den Rechtsakt zur Cybersicherheit und die Stärkung des Mandats der Agentur der Europäischen Union für Cybersicherheit, wodurch die Mitgliedstaaten bei der Bewältigung von Bedrohungen und Angriffen im Zusammenhang mit der Cybersicherheit besser unterstützt werden sollen;

10. befürwortet und unterstützt die Vorschläge zu den Kompetenzzentren für Cybersicherheit und dem Netz nationaler Koordinierungszentren, die der Union dabei helfen sollen, die zum Schutz des digitalen Binnenmarkts benötigten technologischen und industriellen Kapazitäten im Bereich Cybersicherheit zu erhalten und auszubauen;

11. spricht sich in diesem Zusammenhang für das Programm „Digitales Europa“ aus, mit dem in der Union niedergelassenen, aber von Drittländern beherrschten Unternehmen Sicherheitsanforderungen auferlegt werden und diese Unternehmen unter die Aufsicht der Kommission gestellt werden, und zwar insbesondere im Hinblick auf Maßnahmen im Zusammenhang mit der Cybersicherheit;

12. weist erneut darauf hin, dass sich Cybersicherheit nur dann wirkungsvoll wahren lässt, wenn strenge Sicherheitsnormen gelten; fordert, dass Netze eingerichtet werden, die den Grundsätzen der Sicherheit durch Voreinstellungen und der Sicherheit durch Technik genügen; fordert die Mitgliedstaaten und die Kommission nachdrücklich auf, alle verfügbaren Mittel zu prüfen, um ein hohes Maß an Sicherheit herbeizuführen, nötigenfalls durch die Einführung eines Unionszertifikats für Cybersicherheit;

13. weist erneut darauf hin, dass der Wettbewerb in diesem innovationsgeprägten Wirtschaftszweig von entscheidender Bedeutung ist; stellt nochmals fest, dass durch Wettbewerb dafür gesorgt wird, dass Unternehmen wirklich konkurrenzfähig sind und über Ressourcen verfügen, mit denen sie die Marktnachfrage decken können;

14. fordert die Mitgliedstaaten auf, die NIS-Richtlinie vollständig umzusetzen, und fordert die Kommission auf, diese Phase genau zu überwachen, damit die Bestimmungen der Richtlinie ordnungsgemäß durchgesetzt werden und die Unionsbürger besser vor Sicherheitsbedrohungen, die von Drittländern ausgehen, geschützt sind;

15. fordert die Kommission auf, die oben genannten Forderungen bei den nächsten Erörterungen der Strategie für die Beziehungen zwischen der EU und China zu berücksichtigen, damit die EU wettbewerbsfähig bleibt und ihre digitale Infrastruktur gesichert wird;

16. beauftragt seinen Präsidenten, diese Entschließung der Kommission und dem Rat sowie der Regierung der Volksrepublik China sowie den Regierungen und Parlamenten der Mitgliedstaaten zu übermitteln.