Europäisches Parlament
2014-2019

Plenarsitzungsdokument

B8-0153/2019

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))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
im Namen der EFDD-Fraktion

B8-0153/2019

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 Mitteilungen der Kommission vom 14. September 2016 mit den Titeln „Konnektivität für einen wettbewerbsfähigen digitalen Binnenmarkt – Hin zu einer europäischen Gigabit-Gesellschaft“ (COM(2016)0587) und „5G für Europa: ein Aktionsplan“ (COM(2016)0588),

– unter Hinweis auf den geänderten Vorschlag vom 29. Januar 2016 für eine Verordnung des Europäischen Parlaments und des Rates über den Zugang von Waren und Dienstleistungen aus Drittländern zum EU-Binnenmarkt für öffentliche Aufträge und über die Verfahren zur Unterstützung von Verhandlungen über den Zugang von Waren und Dienstleistungen aus der Union zu den Märkten für öffentliche Aufträge von Drittländern (COM(2016)0034),

– 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] (NIS-Richtlinie),

– 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 die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation[2],

– unter Hinweis auf den Vorschlag vom 12. September 2018 für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren (COM(2018)0630),

– unter Hinweis auf das WTO-Streitbeilegungsverfahren vom 1. Juni 2018 über bestimmte Maßnahmen, die China im Zusammenhang mit dem Transfer ausländischer Technologie nach China auferlegt hat (WT/DS549/6),

[1] ABl. L 194 vom 19.7.2016, S. 1.
[2] ABl. L 321 vom 17.12.2018, S. 36.

– unter Hinweis auf seinen am 14. Februar 2019 in erster Lesung festgelegten Standpunkt zu dem 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 die laufenden Verhandlungen zwischen der EU und China über ein umfassendes Investitionsabkommen,

– gestützt auf Artikel 123 Absatz 2 seiner Geschäftsordnung,

A. in der Erwägung, dass die jüngsten Fortschritte im IKT-Bereich, einschließlich der fünften Generation der Telekommunikation (5G), neue Wege für die Erzeugung, Verbreitung und Realisierung von Waren und Dienstleistungen und für die Interaktion unter den Geräten, den Bürgern, den öffentlichen Verwaltungen und anderen sozioökonomischen Akteuren geebnet haben und somit über das Potenzial verfügen, die Wirtschaft in der EU anzukurbeln;

B. in der Erwägung, dass die Cybersicherheit in den Bereichen IKT, Schutz sensibler Informationen, Achtung der individuellen Rechte und Schutz vor externen Cyber-Bedrohungen eine Voraussetzung dafür ist, dass die technologische Souveränität der EU-Bürger sichergestellt und letztlich Wohlstand in der EU geschaffen und die Demokratie in der EU unterstützt wird;

C. in der Erwägung, dass Forschung und Erprobung im Bereich 5G kaum mit dem internationalen Druck Schritt halten, 5G-Netze einzuführen und zu vermarkten, während jedoch in einer Reihe wissenschaftlicher Studien Bedenken und Unsicherheiten hinsichtlich der Sicherheit und der Gefahrenabwehr in den 5G-Netzen geäußert wurden, insbesondere in Bezug auf die Risiken der elektromagnetischen Verschmutzung für die menschliche Gesundheit und die Umwelt;

D. in der Erwägung, dass die Sicherstellung der Cybersicherheit in 5G-Netzen aufgrund des virtualisierten und dezentralen Charakters des 5G-Standards und seiner fragmentierten und stark spezialisierten Wertschöpfungskette von der Produktion bis hin zu Auslieferung, Installation, Konfiguration, Betrieb, Wartung und Softwareaktualisierungen eine neue und komplexe Herausforderung darstellt; in der Erwägung, dass die EU die Cybersicherheitslücke in ihrer kritischen Infrastruktur unter anderem in den Bereichen Telekommunikation, Energie, Verkehr, Gesundheit, Verteidigung und Sicherheit schließen muss;

E. in der Erwägung, dass Sicherheit und Gefahrenabwehr in den 5G-Netzen eine Aufgabe darstellen, die nicht von einzelnen Herstellern oder Netzbetreibern erfüllt werden kann, sondern ein wirksames koordiniertes Vorgehen aller zuständigen nationalen und internationalen Behörden erfordert;

F. in der Erwägung, dass die EU das Potenzial hat, bei der Entwicklung von Cybersicherheitstechnologien eine führende Rolle einzunehmen, indem sie EU-Unternehmen in diesem Bereich unterstützt und alle Veränderungen in der Wertschöpfungskette fördert, die die Abhängigkeit der EU von Technologie aus Drittländern verringern könnten;

[3] Angenommene Texte, P8_TA(2019)0121.

G. in der Erwägung, dass die EU ein Maßnahmenpaket zur Sicherstellung der Cybersicherheit entwickelt hat, einschließlich der NIS-Richtlinie und des Rechtsakts zur Cybersicherheit, die rasch umgesetzt und kontinuierlich überwacht werden sollten, um dafür zu sorgen, dass sie durch die erforderlichen Aktualisierungen und Überprüfungen ihre Wirksamkeit nicht verlieren;

H. in der Erwägung, dass auf dem 5G-Markt der EU eine zunehmende Präsenz von Technologieanbietern aus China und anderen Drittländern zu verzeichnen ist, insbesondere von staatseigenen Unternehmen oder Unternehmen, denen es an Transparenz mangelt;

I. in der Erwägung, dass die Gegenseitigkeit eine der wirksamsten Methoden ist, um Fortschritte auf dem Weg hin zu weltweit gleichen Wettbewerbsbedingungen zu erzielen;

J. in der Erwägung, dass sich Unternehmen aus Drittländern mit der derzeitigen Lücke in den EU-Datenschutzstandards zwischen der Datenschutz-Grundverordnung und den unterschiedlichen Anforderungen nach nationalem Recht auseinandersetzen müssen;

K. in der Erwägung, dass die EU und China seit 2013 über ein umfassendes Investitionsabkommen verhandeln; in der Erwägung, dass das vorgeschlagene Abkommen dazu beitragen würde, Probleme beim Marktzugang zu lösen, einen Rahmen für den Investitionsschutz zu schaffen und grundlegende Arbeits- und Umweltstandards festzulegen;

L. in der Erwägung, dass es zwar keine eindeutigen Beweise, wohl aber Hinweise auf Sicherheitsmängel in Geräten von Anbietern aus Drittländern, darunter auch China, gibt, die das Recht auf Schutz der Privatsphäre und den Schutz sicherheitskritischer Informationen in der EU gefährden könnten;

1. betont, dass der Ausbau und die Vermarktung von 5G-Netzen im Einklang mit dem Vorsorgeprinzip erfolgen sollten, wobei alle sozialen und wirtschaftlichen Akteure potenzielle Auswirkungen auf Sicherheit und Gefahrenabwehr voraussehen und angemessene Vorsichtsmaßnahmen treffen, einschließlich der unverzüglichen Offenlegung von Faktoren, die die öffentliche Gesundheit oder die Umwelt gefährden könnten;

2. betont, dass die sozialen und wirtschaftlichen Auswirkungen des 5G-Standards und der Technologien, die durch ihn ermöglicht werden, vom Internet der Dinge bis hin zur künstlichen Intelligenz, eingehend bewertet werden sollten und dass Maßnahmen ergriffen werden sollten, um den Übergang zur europäischen Gigabit-Gesellschaft in fairer und gleicher Weise für alle und auf der Grundlage ethischer Verantwortung zu vollziehen;

3. fordert die Kommission und die Mitgliedstaaten auf, ein innovationsfreundliches Umfeld für EU-Anbieter zu schaffen, damit sie neue Produkte, Dienstleistungen und Technologien entwickeln können, und die Unternehmer in der EU bei der Einführung und Vermarktung sicherer und gefahrloser 5G-Netze zu unterstützen und gleichzeitig dafür zu sorgen, dass das Potenzial dieser Netze allen Unternehmen in der digitalen Wirtschaft der EU, einschließlich kleiner und mittlerer Unternehmen, zugänglich ist;

4. weist darauf hin, dass die Cybersicherheit eine der größten Herausforderungen ist, denen die EU derzeit gegenübersteht, und dass durch ein Versagen in diesem Bereich die Privatsphäre und die Grundrechte der Verbraucher und Erzeuger in der EU verletzt werden könnten, das Vertrauen der Bürger in IKT-Produkte und -Dienstleistungen ernsthaft untergraben und letztlich schwerer wirtschaftlicher Schaden verursacht werden könnte; fordert, dass Netze eingerichtet werden, die den Grundsätzen der Sicherheit durch Voreinstellungen und der Sicherheit durch Technik genügen;

5. fordert die Kommission und die Mitgliedstaaten auf, bei der Umsetzung der Cybersicherheitsstrategie der EU eng zusammenzuarbeiten und die Maßnahmen der EU und der Mitgliedstaaten miteinander zu kombinieren, um das Risiko von Sicherheitslücken und Datenschutzverletzungen entlang der gesamten Wertschöpfungskette zu minimieren; ist der Ansicht, dass sich diese Maßnahmen auf die EU-Cybersicherheitszertifizierung, die Konfigurationsanforderungen, die Betriebsverfahren und die Betriebspraxis sowie die Förderung der Cyberhygiene und der Bildung im digitalen Bereich erstrecken könnten;

6. ist der Ansicht, dass die Cybersicherheitsagentur der EU (die Agentur der Europäischen Union für Netz- und Informationssicherheit – ENISA) bei der Analyse möglicher Bedrohungen durch Anbieter aus Drittländern, einschließlich Chinas, und bei der Koordinierung eines gemeinsamen Ansatzes der Mitgliedstaaten zur Abwehr von Bedrohungen und Angriffen auf die Cybersicherheit eine entscheidende Rolle spielen muss;

7. fordert die Kommission und die Mitgliedstaaten auf, das Paket zur Kreislaufwirtschaft zügig umzusetzen und die Bewirtschaftung von Rohstoffen während ihrer gesamten Lebensdauer sowie das Recycling von Rohstoffen zu fördern, um den Zugang der EU zu kritischen Rohstoffen zu verbessern, die für Hochtechnologieprodukte und neue Innovationen von grundlegender Bedeutung sind;

8. ist der Ansicht, dass es dringend geboten ist, die potenziellen Bedrohungen der technologischen Sicherheit zu bewältigen, die durch die derzeitige Durchdringung des EU-Marktes mit Anbietern aus Drittländern, einschließlich Chinas, entstehen, indem die Mitgliedstaaten einen gemeinsamen Ansatz in Bezug auf die Sicherheit und den Datenschutz verfolgen;

9. fordert die Kommission und die Mitgliedstaaten auf, die Sicherheit derjenigen IKT-Systeme zu analysieren und zu überwachen, in denen Technologien aus Drittländern stark präsent sind, auch durch die Durchführung von Stresstests;

10. betont, dass Anbieter aus Drittländern nicht aufgrund ihres Herkunftslands diskriminiert werden sollten, sondern dass die Transparenz dieser Unternehmen, ihre Cybersicherheitsstandards und die Existenz von Gegenseitigkeitsbedingungen für EU-Unternehmen im Ursprungsland berücksichtigt werden sollten, wenn es gilt, für gleiche Wettbewerbsbedingungen zu sorgen;

11. betont, dass chinesische oder andere Anbieter und Betreiber aus Drittländern unter keinen Umständen die nach EU-Recht garantierten individuellen Rechte gefährden dürfen, selbst wenn nach nationalem Recht in ihrem Ursprungsland unterschiedliche Anforderungen bestehen;

12. fordert den Rat auf, die Wiederaufnahme von Gesprächen über den neuen überarbeiteten Vorschlag der Kommission für das Verfahren, mit dem der Zugang von Erzeugnissen aus Drittländern zum Beschaffungsmarkt der EU eingeschränkt wird, wenn ein gegenseitiger Marktzugang nicht möglich ist, wohlwollend in Betracht zu ziehen,

13. erinnert daran, dass es wichtig ist, die Verhandlungen mit Drittländern über die Zusammenarbeit in Regulierungsfragen im Bereich der digitalen Technologien weiter zu intensivieren und für ein stärkeres Engagement dieser Länder in den internationalen Normungsorganisationen zu sorgen;

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