**Europäisches Parlament**
2014-2019

*Plenarsitzungsdokument*

**B8-0154/2019 }**
**B8-0155/2019 }**
**B8-0159/2019 }**
**B8-0160/2019 } RC1**

8.3.2019

# GEMEINSAMER ENTSCHLIESSUNGSANTRAG

eingereicht gemäß Artikel 123 Absätze 2 und 4 der Geschäftsordnung

anstelle der folgenden Entschließungsanträge:
B8-0154/2019 (ALDE)
B8-0155/2019 (PPE)
B8-0159/2019 (S&D)
B8-0160/2019 (Verts/ALE)

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))

**Luděk Niedermayer**
im Namen der PPE-Fraktion
**Dan Nica**
im Namen der S&D-Fraktion
**Caroline Nagtegaal**
im Namen der ALDE-Fraktion
**Reinhard Bütikofer**
im Namen der Verts/ALE-Fraktion

**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*,

– gestützt 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 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[3],

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

– unter Hinweis auf den Vorschlag der Kommission vom 12. September 2018 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 Annahme des neuen Nachrichtendienstgesetzes durch den Nationalen Volkskongress Chinas am 28. Juni 2017,

– 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 Maßnahmen, die zu ihrer Verringerung auf der Ebene der EU getroffen werden können,

– unter Hinweis auf die Annahme der staatlichen Sicherheitsreformen im Telekommunikationsbereich durch die australische Regierung, die am 18. September 2018 in Kraft getreten sind,

– 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

[1] ABl. L 321 vom 17.12.2018, S. 36.
[2] ABl. L 194 vom 19.7.2016, S. 1.
[3] ABl. L 218 vom 14.8.2013, S. 8.

Europäischen Union[4],

– unter Hinweis auf seine früheren Entschließungen zu den Beziehungen zwischen der EU und China, insbesondere seine Entschließung vom 12. September 2018[5],

– 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“[6],

– 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)[7],

– 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[8],

– unter Hinweis auf den Vorschlag der Kommission vom 6. Juni 2018 für eine Verordnung des Europäischen Parlaments und des Rates zur Aufstellung des Programms „Digitales Europa“ für den Zeitraum 2021–2027 (COM(2018)0434),

– gestützt auf Artikel 123 Absätze 2 und 4 seiner Geschäftsordnung,

A. in der Erwägung, dass die EU ihre Agenda im Bereich Cybersicherheit vorantreiben muss, damit sie ihr Potenzial ausschöpfen, damit eine Führungsrolle bei der Cybersicherheit übernehmen und dies zum Vorteil ihrer Industrie nutzen kann;

B. in der Erwägung, dass Schwachstellen in den 5G-Netzen ausgenutzt werden könnten, um IT-Systeme zu gefährden, wodurch auf EU-Ebene und auf nationaler Ebene erhebliche Schäden in den Volkswirtschaften verursacht werden könnten; in der Erwägung, dass ein auf die Analyse der Risiken gestützter Ansatz in der gesamten Wertschöpfungskette erforderlich ist, um die Risiken so gering wie möglich zu halten;

C. in der Erwägung, dass das 5G-Netz das Rückgrat unserer digitalen Infrastruktur sein wird, dass es die Möglichkeiten erweitern wird, verschiedene Geräte an Netze anzuschließen (z. B. Internet der Dinge) und dass es neue Vorteile und Möglichkeiten für die Gesellschaft und die Unternehmen in vielen Bereichen bieten wird, einschließlich kritischer Wirtschaftsbereiche wie Verkehr, Energie, Gesundheit, Finanzen, Telekommunikation, Verteidigung, Raumfahrt und Sicherheit;

[4] Angenommene Texte, P8_TA(2019)0121.
[5] Angenommene Texte, P8_TA(2018)0343.
[6] ABl. L 307 vom 30.8.2018, S. 144.
[7] ABl. L 119 vom 4.5.2016, S. 1.
[8] ABl. L 348 vom 20.12.2013, S. 129.

D. in der Erwägung, dass die Schaffung geeigneter Mechanismen zur Reaktion auf Herausforderungen im Sicherheitsbereich der EU die Möglichkeit geben würde, aktiv Schritte zu unternehmen, um Standards für 5G aufzustellen;

E. in der Erwägung, dass Bedenken hinsichtlich Anbietern von Ausrüstungen aus Drittländern geäußert wurden, die wegen der Gesetze ihres Herkunftslandes ein Sicherheitsrisiko für die EU darstellen könnten, insbesondere nachdem die chinesischen Staatssicherheitsgesetze in Kraft getreten sind, die Verpflichtungen für alle Bürger, Unternehmen und sonstige Einrichtungen vorsehen, zum Schutz der Staatssicherheit mit dem Staat zusammenzuarbeiten, wobei der Begriff „Staatsicherheit“ sehr weit gefasst ist; in der Erwägung, dass es keine Garantie gibt, dass diese Verpflichtungen nicht auch außerhalb Chinas angewendet werden, und in der Erwägung, dass sich die Reaktionen auf die chinesischen Gesetze von Land zu Land unterscheiden und von der Durchführung von Sicherheitseinschätzungen bis hin zu völligen Verboten reichen;

F. in der Erwägung, dass die tschechische nationale Behörde für Cybersicherheit im Dezember 2018 eine Warnung vor Sicherheitsbedrohungen herausgegeben hat, die von der Technologie der chinesischen Firmen Huawei und ZTE ausgehen; in der Erwägung, dass die tschechischen Steuerbehörden Huawei daraufhin im Januar 2019 von einer Ausschreibung zum Bau eines Steuerportals ausgeschlossen haben;

G. in der Erwägung, dass eine gründliche Untersuchung notwendig ist, um zu ermitteln, ob die betreffenden Geräte oder andere Geräte oder Anbieter wegen Funktionen wie etwa Hintertüren zu Systemen ein Sicherheitsrisiko darstellen;

H. in der Erwägung, dass Lösungen auf EU-Ebene koordiniert und bearbeitet werden sollten, damit keine unterschiedlichen Sicherheitsniveaus und keine potentiellen Lücken bei der Cybersicherheit entstehen, wobei auch eine Koordinierung auf globaler Ebene erforderlich ist, um eine entschiedene Reaktion zu ermöglichen;

I. in der Erwägung, dass mit den Vorteilen des Binnenmarkts die Verpflichtung einhergeht, die EU-Standards und den Rechtsrahmen der Union einzuhalten, und in der Erwägung, dass die Anbieter nicht aufgrund ihres Herkunftslandes unterschiedlich behandelt werden sollten;

J. 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, ausländische Investitionen unter dem Gesichtspunkt der Sicherheit und der öffentlichen Ordnung zu überprüfen, ein Kooperationsmechanismus eingerichtet wird, auf dessen Grundlage die Kommission und die Mitgliedstaaten bei der Bewertung der von sensiblen ausländischen Investitionen ausgehenden Sicherheitsrisiken – einschließlich der Risiken für die Cybersicherheit – zusammenarbeiten können, und auch Projekte und Programme erfasst werden, die von EU-Interesse sind, wie etwa die transeuropäischen Telekommunikationsnetze und Horizont 2020;

1. ist der Ansicht, dass die Union die Führung bei der Cybersicherheit durch ein gemeinsames Konzept übernehmen muss, das sich auf die wirksame und effiziente Nutzung des Sachverstands in der EU, den Mitgliedstaaten und der Industrie stützt, da ein Flickenteppich unterschiedlicher nationaler Entscheidungen dem digitalen

Binnenmarkt schaden würde;

2. ist zutiefst besorgt angesichts der in jüngster Zeit erhobenen Vorwürfe, dass 5G-Geräte, die von chinesischen Unternehmen entwickelt werden, eingebaute Hintertüren enthalten könnten, die es den Herstellern und den Behörden ermöglichen, unbefugt auf private und personenbezogene Daten sowie auf die Telekommunikation in der EU zuzugreifen;

3. ist gleichermaßen besorgt darüber, dass sich bei der Einführung von 5G-Netzen in den kommenden Jahren potenziell größere Schwachstellen in den von diesen Herstellern entwickelten 5G-Geräten auftun könnten, wenn sie installiert würden;

4. betont, dass die Auswirkungen auf die Sicherheit der Netze und der technischen Ausrüstung weltweit ähnlich sind, und fordert, dass die EU Lehren aus den verfügbaren Erfahrungen zieht, um bei der Cybersicherheit für höchste Standards sorgen zu können; fordert die Kommission auf, eine Strategie zu entwickeln, die der EU zu einer Führungsrolle bei der Technologie für Cybersicherheit verhilft und darauf ausgerichtet ist, die Abhängigkeit der EU von ausländischer Technologie im Bereich der Cybersicherheit zu verringern; ist der Ansicht, dass angemessene Maßnahmen ergriffen werden müssen, wenn nicht garantiert werden kann, dass die Sicherheitsanforderungen erfüllt werden;

5. fordert die Mitgliedstaaten auf, die Kommission von etwaigen nationalen Maßnahmen, die sie anzunehmen gedenken, zu unterrichten, um die Reaktion der Union zu koordinieren und damit die höchsten Standards für Cybersicherheit in der gesamten Union sicherzustellen, und betont erneut, wie wichtig es ist, dass keine unverhältnismäßigen einseitigen Maßnahmen ergriffen werden, die zu einer Fragmentierung des Binnenmarktes führen würden;

6. bekräftigt, dass alle Stellen, die in der EU Ausrüstung oder Dienstleistungen zur Verfügung stellen, unabhängig von ihrem Ursprungsland, die Pflichten im Bereich der Grundrechte und das Recht der EU und der Mitgliedstaaten einhalten müssen, wozu auch der Rechtsrahmen für Privatsphäre, Datenschutz und Cybersicherheit gehört;

7. fordert die Kommission auf zu prüfen, wie solide der Rechtsrahmen der Union ist, um Bedenken aufgrund der etwaigen Präsenz anfälliger technischer Ausrüstung in strategischen Sektoren und der Backbone-Infrastruktur Rechnung zu tragen; fordert die Kommission nachdrücklich auf, Initiativen, wenn erforderlich einschließlich Gesetzgebungsvorschlägen, vorzulegen, um die ermittelten Mängel rechtzeitig zu beheben, zumal sich die Union in einem ständigen Prozess der Ermittlung und Bewältigung von Herausforderungen im Bereich Cybersicherheit und der Stärkung der Abwehrfähigkeit der EU in diesem Bereich befindet;

8. fordert diejenigen Mitgliedstaaten, die das noch nicht getan haben, nachdrücklich auf, die Richtlinie zur Netz- und Informationssicherheit unverzüglich vollständig umzusetzen, und fordert die Kommission auf, diese Umsetzung genau zu überwachen um sicherzustellen, dass die Bestimmungen ordnungsgemäß umgesetzt und durchgesetzt und die europäischen Bürger vor externen und internen Sicherheitsbedrohungen besser geschützt werden;

9. fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, dafür zu sorgen,

dass die durch die Richtlinie über Netz- und Informationssysteme eingeführten Meldemechanismen ordnungsgemäß angewandt werden; weist darauf hin, dass die Kommission und die Mitgliedstaaten etwaige die Sicherheit betreffende Zwischenfälle oder unangemessene Reaktionen von Anbietern eingehend weiterverfolgen sollten, um ermittelte Sicherheitslücken zu schließen;

10. fordert die Kommission auf zu prüfen, ob der Anwendungsbereich der Richtlinie über Netz- und Informationssysteme auf andere kritische Bereiche und Dienstleistungen ausgeweitet werden muss, die nicht von branchenspezifischen Rechtsvorschriften erfasst sind;

11. begrüßt und unterstützt die Einigung über den Rechtsakt zur Cybersicherheit und die Stärkung des Mandats der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), wodurch die Mitgliedstaaten bei der Bewältigung von Bedrohungen und Angriffen im Zusammenhang mit der Cybersicherheit besser unterstützt werden sollen;

12. fordert die Kommission nachdrücklich auf, der ENISA den Auftrag zu erteilen, die Arbeit an einem Zertifizierungssystem für 5G-Ausrüstung zu einer Priorität zu machen, um sicherzustellen, dass beim Aufbau von 5G-Systemen in der Union die höchsten Sicherheitsstandards eingehalten werden und diese Systeme gegen Hintertüren oder größere Schwachstellen geschützt sind, die die Sicherheit der Telekommunikationsnetze der Union und der dazugehörigen Dienstleistungen gefährden würden; empfiehlt, häufig verwendeten Verfahren und Produkten sowie häufig verwendeter Software, die wegen des schieren Umfangs ihrer Nutzung beträchtliche Auswirkungen auf das tägliche Leben der Bürger und die Wirtschaft haben, besondere Aufmerksamkeit zu schenken;

13. begrüßt ausdrücklich 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; erinnert jedoch daran, dass die Zertifizierung die zuständigen Behörden und Betreiber nicht von der Kontrolle der Lieferkette ausschließen sollte, damit für die Integrität und Sicherheit ihrer Ausrüstung, die in kritischen Umgebungen und Telekommunikationsnetzen betrieben wird, gesorgt ist;

14. weist erneut darauf hin, dass die Cybersicherheit hohe Sicherheitsstandards erfordert; 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 Möglichkeiten zu ermitteln, wie für ein hohes Maß an Sicherheit gesorgt werden kann;

15. fordert die Kommission und die Mitgliedstaaten auf, in Zusammenarbeit mit der ENISA Leitlinien bereitzustellen, wie bei der Beschaffung von 5G-Ausrüstung Cyberbedrohungen und Schwachstellen beseitigt werden können, beispielsweise durch die Diversifizierung der Ausrüstung unter Nutzung verschiedener Anbieter oder die Einführung mehrstufiger Beschaffungsverfahren;

16. bekräftigt seinen Standpunkt zu dem Programm „Digitales Europa“, 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;

17. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass öffentliche Einrichtungen und private Unternehmen, die daran beteiligt sind, das reibungslose Funktionieren kritischer Infrastrukturnetze, wie etwa Telekommunikation, Energie, Gesundheit und Sozialsysteme, sicherzustellen, einschlägige Bewertungen in Form von Risikobewertungen vornehmen, wobei diejenigen Sicherheitsbedrohungen zu berücksichtigen sind, die in einem besonderen Zusammenhang mit technischen Merkmalen des jeweiligen Systems oder mit der Abhängigkeit von externen Anbietern von Hard- und Softwaretechnologien stehen;

18. erinnert daran, dass die geltenden Vorschriften im Bereich Telekommunikation die Mitgliedstaaten dazu verpflichten, dafür zu sorgen, dass die Telekommunikationsbetreiber die Anforderungen hinsichtlich der Integrität und Verfügbarkeit öffentlicher elektronischer Kommunikationsnetze – soweit erforderlich einschließlich der Übermittlungsverschlüsselung – erfüllen; hebt hervor, dass die Mitgliedstaaten im Rahmen des Europäischen Kodex für die elektronische Kommunikation über weitreichende Befugnisse verfügen, um Erzeugnisse auf dem EU-Markt zu untersuchen und im Falle ihrer Nichtkonformität ein breites Spektrum an Abhilfemaßnahmen anzuwenden;

19. fordert die Kommission und die Mitgliedstaaten auf, die Sicherheit zu einem obligatorischen Aspekt bei allen öffentlichen Ausschreibungen für relevante Infrastrukturen sowohl auf EU-Ebene als auch auf nationaler Ebene zu machen;

20. erinnert die Mitgliedstaaten an ihre Verpflichtung gemäß dem EU-Rechtsrahmen, insbesondere der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme, Sanktionen gegen juristische Personen zu verhängen, die Straftaten wie Angriffe auf solche Systeme begangen haben; betont, dass sich die Mitgliedstaaten auch der Möglichkeit bedienen sollten, andere Sanktionen gegen diese juristischen Personen zu verhängen, wie etwa das vorübergehende oder ständige Verbot der Ausübung gewerblicher Tätigkeiten;

21. fordert die Mitgliedstaaten, Cybersicherheitsagenturen und Telekommunikationsbetreiber sowie die Hersteller und Anbieter von kritischen Infrastrukturdiensten auf, der Kommission und der ENISA sämtliche Nachweise für Hintertüren oder andere größere Schwachstellen zu melden, die die Integrität und Sicherheit der Telekommunikationsnetze beeinträchtigen oder gegen das Unionsrecht und die Grundrechte verstoßen könnten; erwartet, dass die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte bei Anzeichen für Verletzungen des Schutzes personenbezogener Daten durch externe Anbieter gründliche Ermittlungen durchführen und angemessene Bußgelder und Sanktionen im Einklang mit dem EU-Datenschutzrecht verhängen;

22. begrüßt, dass eine Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen (ADI) aus Gründen der Sicherheit und der öffentlichen Ordnung in Kraft treten wird, und hebt hervor, dass mit dieser Verordnung erstmals eine Liste der Bereiche und Faktoren, darunter Kommunikation und

Cybersicherheit, festgelegt wird, die für die Sicherheit und die öffentliche Ordnung auf EU-Ebene relevant sind;

23. fordert den Rat auf, seine Arbeit an der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung) zu beschleunigen;

24. betont erneut, dass die EU die Cybersicherheit in der gesamten Wertschöpfungskette – von der Forschung bis zur Entwicklung und dem Einsatz von Schlüsseltechnologien – unterstützen, einschlägige Informationen verbreiten sowie Cyberhygiene und Ausbildungspläne unter anderem zur Cybersicherheit fördern muss, und ist der Auffassung, dass das Programm „Digitales Europa“ zusammen mit weiteren Maßnahmen hierfür ein wirksames Hilfsmittel sein wird;

25. fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, die erforderlichen Schritte, einschließlich solider Investitionsprogramme, zu unternehmen, um ein Umfeld in der EU zu schaffen, das Innovationen begünstigt und allen Unternehmen der digitalen Wirtschaft der EU zugänglich ist, einschließlich kleiner und mittlerer Unternehmen (KMU); fordert außerdem nachdrücklich, dass ein solches Umfeld europäischen Anbietern die Entwicklung neuer Produkte, Dienstleistungen und Technologien ermöglicht, durch die sie wettbewerbsfähig würden;

26. fordert die Kommission und die Mitgliedstaaten nachdrücklich auf, die genannten Forderungen im Rahmen der bevorstehenden Beratungen über die künftige Strategie für die Beziehungen zwischen der EU und China zu berücksichtigen, da sie die Voraussetzungen dafür sind, dass die EU wettbewerbsfähig bleibt und für die Sicherheit ihrer digitalen Infrastruktur gesorgt wird;

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