Parlament Europejski
2014-2019

Dokument z posiedzenia

B8-0154/2019

6.3.2019

PROJEKT REZOLUCJI

złożony w następstwie oświadczeń Rady i Komisji

zgodnie z art. 123 ust. 2 Regulaminu

w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia
(2019/2575(RSP))

Caroline Nagtegaal
w imieniu grupy ALDE

B8-0154/2019

Rezolucja Parlamentu Europejskiego w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP))

Parlament Europejski,

– uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej[1],

– uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2],

– uwzględniając wniosek z dnia 13 września 2017 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") (COM(2017)0477),

– uwzględniając wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" na lata 2021–2027 (COM(2018)0434),

– uwzględniając wniosek dotyczący rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych (COM(2018)0630),

– uwzględniając oświadczenia Rady i Komisji z dnia 13 lutego 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia,

– uwzględniając swoją rezolucję ustawodawczą z dnia 14 lutego 2019 r. sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii Europejskiej[3],

– uwzględniając swoje rezolucje w sprawie stosunków między UE a Chinami, w szczególności rezolucję z dnia 12 września 2018 r. w sprawie stanu stosunków między UE a Chinami[4],

– uwzględniając komunikat Komisji z dnia 14 września 2016 r. zatytułowany „Sieć 5G dla Europy: plan działania" (COM(2016)0588),

[1] Dz.U. L 321 z 17.12.2018, s. 36.
[2] Dz.U. L 194 z 19.7.2016, s. 1.
[3] Teksty przyjęte, P8_TA(2019)0121.
[4] Teksty przyjęte, P8_TA(2018)0343.

– uwzględniając swoją rezolucję z dnia 1 czerwca 2017 r. w sprawie łączności internetowej na rzecz wzrostu gospodarczego, konkurencyjności i spójności: europejskie społeczeństwo gigabitowe i 5G[5],

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[6],

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013 z dnia 11 grudnia 13162013 r. ustanawiające instrument „Łącząc Europę", zmieniające rozporządzenie (UE) nr 913/2010 oraz uchylające rozporządzenia (WE) nr 680/2007 i (WE) nr 67/2010[7],

– uwzględniając art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że infrastruktura 5G poprawi łączność w gospodarce cyfrowej na niespotykaną dotąd skalę; mając na uwadze, że jest ona kluczowym aspektem w rozwoju społeczeństwa cyfrowego, w szczególności w dziedzinach takich jak transport, energia i zdrowie oraz sektor obrony i bezpieczeństwa, stanowiąc standard dla technologii łączności ruchomej w przyszłości;

B. mając na uwadze, że luki w zabezpieczeniach sieci 5G mogłyby zostać wykorzystane, by zagrozić systemom informatycznym, potencjalnie powodując bardzo poważne szkody dla gospodarek na szczeblu zarówno europejskim, jak i krajowym; mając na uwadze, że konieczne jest podejście oparte na analizie ryzyka;

C. mając na uwadze, że zwiększona rola dostawców technologii z państw trzecich na rynku 5G w UE była źródłem poważnych dyskusji w państwach członkowskich, zwłaszcza w kontekście chińskiej ustawy o wywiadzie narodowym, która weszła w życie w czerwcu 2017 r.;

D. mając na uwadze, że chińska ustawa o wywiadzie narodowym nie określa jasno zakresu i parametrów tego, co władze chińskie nazywają „pracą wywiadowczą"; mając na uwadze, że ustawa ta daje władzom nową podstawę prawną do monitorowania i badania zagranicznych i krajowych osób i instytucji, w tym obywateli i instytucji UE, w celu ochrony bezpieczeństwa narodowego Chin;

E. mając na uwadze, że chińskie przedsiębiorstwa telekomunikacyjne otrzymują od państwa dotacje, co mogłoby jeszcze bardziej wzmocnić ich zdolność do wdrażania ustawy o wywiadzie narodowym, prowadząc do problemów związanych z bezpieczeństwem i dając im także nieuczciwą przewagę ekonomiczną;

F. mając na uwadze, że rozporządzenie w sprawie monitorowania bezpośrednich inwestycji zagranicznych, które powinno wejść w życie do końca 2020 r., wzmacnia

[5] Dz.U. C 307 z 30.8.2018, s. 144.
[6] Dz.U. L 119 z 4.5.2016, s. 1.
[7] Dz.U. L 348 z 20.12.2013, s. 129.

zdolność państw członkowskich do monitorowania inwestycji zagranicznych w oparciu o kryteria bezpieczeństwa i porządku publicznego oraz ustanawia mechanizm współpracy, który umożliwia Komisji i państwom członkowskim współpracę w dziedzinie oceny zagrożeń dla bezpieczeństwa, w tym zagrożeń dla cyberbezpieczeństwa, powstałych w związku z inwestycjami zagranicznymi;

G. mając na uwadze, że dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych miała zostać przetransponowana do 9 maja 2018 r.; mając na uwadze, że dyrektywa ta ma na celu wzmocnienie bezpieczeństwa podstawowej infrastruktury europejskiej oraz zapewnienie zgłaszania poważnych cyberincydentów; mając na uwadze, że dyrektywa ustanawiająca Europejski kodeks łączności elektronicznej nakłada na przedsiębiorstwa telekomunikacyjne obowiązek podejmowania środków w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług oraz powiadamiania organów, a w szczególnych przypadkach także użytkowników, o istotnych incydentach związanych z bezpieczeństwem;

H. mając na uwadze, że Europejski kodeks łączności elektronicznej przewiduje dostępność widma radiowego 5G w UE do 2020 r.; mając na uwadze, że państwa członkowskie organizują niezależne aukcje częstotliwości widma w ramach wprowadzania sieci 5G, co potencjalnie umożliwia przedsiębiorstwom z państw trzecich zdobycie dominującej pozycji na rynku w kilku państwach członkowskich, a w konsekwencji w całej UE; mając na uwadze, że Chiny mają ambitną strategię w dziedzinie sztucznej inteligencji, dla której dane stanowią kluczowy zasób;

1. przypomina o pilnej potrzebie budowania wewnątrz UE potencjału i zdolności w zakresie infrastruktury cyfrowej, przy jednoczesnym wzmocnieniu strategicznej autonomii UE; przypomina o znaczeniu sieci 5G i w związku z tym ponownie podkreśla swoje zaangażowanie w realizację planu działania dla sieci 5G;

2. przypomina, że realizacja sieci 5G zostanie poprawiona przez zapewnienie dostępności odpowiedniego widma radiowego w UE do końca 2020 r., jak przewidziano w Europejskim kodeksie łączności elektronicznej; podkreśla, że głównym wyzwaniem dla operatorów jest brak koordynacji i przewidywalności;

3. ponownie podkreśla potrzebę podjęcia wspólnego działania europejskiego w celu rozwiązania bieżących problemów związanych z dostawcami sprzętu telekomunikacyjnego wspieranymi przez rząd chiński, tak by zwiększyć odporność cyfrową i zapewnić nieulegające dezaktualizacji zabezpieczenia mające na celu ochronę jednolitego rynku; wzywa tymczasem do zwiększenia wymiany informacji między państwami członkowskimi UE;

4. wzywa do zbadania potencjalnych zagrożeń dla bezpieczeństwa związanych z wykorzystaniem zagranicznej technologii oraz do uznania 5G za infrastrukturę krytyczną, tak aby wszystkie przedsiębiorstwa musiały spełniać wyższe standardy bezpieczeństwa;

5. w tym względzie z zadowoleniem przyjmuje i podkreśla element wymiany informacji między państwami członkowskimi w ramach mechanizmu współpracy przewidzianego w rozporządzeniu ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych;

6. podkreśla, że rozporządzenie ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych chroni infrastrukturę krytyczną; przypomina, że przedsiębiorstwa prowadzące działalność w UE korzystają z jednolitego rynku, jednak muszą przestrzegać unijnych standardów i ram prawnych;

7. z zainteresowaniem odnotowuje, że od czasu gdy Komisja po raz pierwszy przedstawiła rozporządzenie ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w 2017 r. zwiększyła się liczba państw członkowskich posiadających mechanizm monitorowania;

8. wspiera Komisję w różnych działaniach już podjętych w celu zwiększenia liczby przyjmowanych środków służących zwalczaniu zagrożeń dla cyberbezpieczeństwa oraz w celu zapewnienia ścisłego wdrożenia odpowiednich środków zarządzania ryzykiem, w tym sankcji wobec dostawców, którzy nie wypełniają swoich obowiązków;

9. z zadowoleniem przyjmuje i popiera osiągnięcie porozumienia dotyczącego aktu ws. cyberbezpieczeństwa oraz wzmocnienie mandatu Agencji UE ds. cyberbezpieczeństwa, aby lepiej wspierać państwa członkowskie w przeciwdziałaniu atakom i zagrożeniom dla cyberbezpieczeństwa;

10. z zadowoleniem przyjmuje i popiera wnioski dotyczące centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz sieci krajowych ośrodków koordynacji, które mają pomóc UE w utrzymaniu i rozwijaniu zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego;

11. z zadowoleniem przyjmuje w tym kontekście program „Cyfrowa Europa”, który nakłada wymogi w zakresie bezpieczeństwa i nadzoru Komisji nad podmiotami, które mają siedzibę w UE, lecz są kontrolowane z państwa trzeciego, w szczególności w odniesieniu do działań związanych z cyberbezpieczeństwem;

12. przypomina, że skuteczne cyberbezpieczeństwo wymaga zachowania wysokich standardów bezpieczeństwa; wzywa do stworzenia sieci, która jest bezpieczna domyślnie i już w fazie projektowania; wzywa państwa członkowskie, by wraz z Komisją zbadały wszelkie możliwe sposoby zapewnienia wysokiego poziomu bezpieczeństwa, w razie potrzeby przez zastosowanie europejskiej certyfikacji cyberbezpieczeństwa;

13. przypomina, że w tak innowacyjnym sektorze konkurencja jest niezbędna; przypomina, że konkurencja gwarantuje, że przedsiębiorstwa są poważnymi konkurentami dysponującymi zasobami, którzy mogą zaspokoić popyt na rynku;

14. wzywa państwa członkowskie do pełnego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych, a Komisję do ścisłego monitorowania tego etapu, tak aby zapewnić prawidłowe egzekwowanie przepisów dyrektywy i lepszą ochronę Europejczyków przed zewnętrznymi zagrożeniami dla bezpieczeństwa;

15. wzywa Komisję do uwzględnienia powyższych wniosków w kolejnych dyskusjach na temat strategii UE–Chiny, aby zagwarantować utrzymanie konkurencyjności UE i

bezpieczeństwo jej infrastruktury cyfrowej;

16. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Komisji, Radzie, rządowi Chińskiej Republiki Ludowej oraz rządom i parlamentom państw członkowskich.