Parlament Europejski
2014-2019

Dokument z posiedzenia

B8-0153/2019

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))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
w imieniu grupy EFDD

B8-0153/2019

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 komunikaty Komisji z dnia 14 września 2016 r. pt. „Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego” (COM(2016)0587) oraz „Sieć 5G dla Europy: plan działania” (COM(2016)0588),

– uwzględniając zmieniony wniosek Komisji dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 29 stycznia 2016 r. w sprawie dostępu towarów i usług z państw trzecich do rynku wewnętrznego Unii w zakresie zamówień publicznych oraz procedur wspierających negocjacje dotyczące dostępu unijnych towarów i usług do rynków zamówień publicznych państw trzecich (COM(2016)0034),

– 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[1],

– uwzględniając wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 13 września 2017 r. 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 dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej[2],

– uwzględniając wniosek Komisji dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 12 września 2018 r. ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji (COM(2018)0630),

– uwzględniając postępowanie w ramach WTO z dnia 1 czerwca 2018 r. dotyczące rozstrzygania sporów (WT/DS549/6) dotyczące pewnych środków nałożonych przez Chiny w związku z transferem zagranicznych technologii do Chin,

– uwzględniając swoje stanowisko przyjęte w pierwszym czytaniu w dniu 14 lutego 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych w

[1] Dz.U. L 194 z 19.7.2016, s. 1.
[2] Dz.U. L 321 z 17.12.2018, s. 36.

Unii Europejskiej[3],

– uwzględniając trwające negocjacje między UE a Chinami w sprawie kompleksowej umowy o inwestycjach,

– uwzględniając art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że ostatnie postępy w dziedzinie technologii informacyjno-komunikacyjnych (ICT), w tym telekomunikacja piątej generacji (5G), stworzyły nowe możliwości produkcji, dystrybucji i wykorzystywania towarów i usług oraz interakcji między urządzeniami i obywatelami, administracją publiczną i innymi podmiotami społeczno-ekonomicznymi, stwarzają zatem potencjał wzmocnienia europejskiej gospodarki;

B. mając na uwadze, że cyberbezpieczeństwo technologii informacyjno-komunikacyjnych, ochrona informacji szczególnie chronionych, poszanowanie praw indywidualnych i zabezpieczenie przed zewnętrznymi zagrożeniami cybernetycznymi stanowią warunki wstępne dla zapewnienia suwerenności technologicznej obywateli UE oraz ostatecznie dobrobytu i wspierania demokracji w UE;

C. mając na uwadze, że badania i testy dotyczące sieci 5G nie nadążają za presją związaną z jej wdrażaniem i komercjalizacją, mimo iż liczne badania naukowe wskazują na obawy i wątpliwości co do jej zabezpieczeń i bezpieczeństwa, szczególnie pod względem zagrożeń związanych z zanieczyszczeniem elektromagnetycznym dla zdrowia ludzi i środowiska;

D. mając na uwadze, że zapewnienie cyberbezpieczeństwa sieci 5G stanowi nowe i złożone wyzwanie z uwagi na wirtualny i zdecentralizowany charakter sieci 5G oraz jej rozdrobniony i wysoce wyspecjalizowany łańcuch wartości, od produkcji po dostawę, montaż, konfigurację, działanie, utrzymanie i aktualizacje oprogramowania; mając na uwadze, że UE musi usunąć luki w cyberbezpieczeństwie swojej infrastruktury krytycznej, m.in. w sektorach telekomunikacji, energii, transportu, zdrowia, obrony i bezpieczeństwa;

E. mając na uwadze, że zapewnienie bezpiecznych sieci 5G jest zadaniem przewyższającym możliwości pojedynczych producentów lub operatorów systemów, wymagającym skutecznych, skoordynowanych działań po stronie wszystkich odpowiednich władz krajowych i międzynarodowych;

F. mając na uwadze, że UE może stać się liderem rozwoju technologii cyberbezpieczeństwa przez wspieranie europejskich przedsiębiorstw w tym sektorze i promowanie wszystkich zmian w łańcuchu wartości, które mogą zmniejszyć uzależnienie UE od zagranicznych technologii;

G. mając na uwadze, że UE opracowała zestaw środków zapewniających cyberbezpieczeństwo, w tym dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium

[3] Teksty przyjęte, P8_TA(2019)0121.

Unii oraz akt ws. bezpieczeństwa cybernetycznego, które należy niezwłocznie wdrożyć i stale monitorować, aby zapewniać ich stałą skuteczność w drodze niezbędnych aktualizacji i przeglądów;

H. mając na uwadze, że zwiększona obecność dostawców technologii z Chin i innych państw trzecich, szczególnie przedsiębiorstw państwowych i firm charakteryzujących się brakiem przejrzystości, stała się widoczna na unijnym rynku sieci 5G;

I. mając na uwadze, że wzajemność jest jednym z najskuteczniejszych sposobów dokonywania postępów na rzecz równych warunków działania na świecie;

J. mając na uwadze, że zagraniczne przedsiębiorstwa muszą obecnie zmierzyć się z rozbieżnościami w unijnych normach ochrony danych wynikającymi z różnic między ogólnym rozporządzeniem o ochronie danych a różnymi wymogami przepisów krajowych;

K. mając na uwadze, że od 2013 r. UE i Chiny prowadzą negocjacje w sprawie kompleksowej umowy o inwestycjach; mając na uwadze, że proponowane porozumienie pomogłoby rozwiązać problemy z dostępem do rynku oraz ustanowić ramy ochrony inwestycji i podstawowe normy w dziedzinie praw pracowniczych i środowiska;

L. mając na uwadze, że pojawiły się, jakkolwiek nierozstrzygające, dowody na obecność luk w zabezpieczeniach w sprzęcie dostarczanym przez dostawców z państw trzecich, w tym z Chin, które to luki mogą zagrażać prawu osób fizycznych do prywatności i ochrony informacji szczególnie chronionych w UE;

1. podkreśla, że podczas wdrażania i komercjalizacji sieci 5G należy przestrzegać zasady ostrożności, a wszystkie podmioty społeczno-gospodarcze powinny przewidywać jej możliwe skutki dla bezpieczeństwa oraz przyjąć proporcjonalne środki ostrożnościowe, w tym niezwłocznie ujawniać czynniki mogące zagrażać zdrowiu publicznemu lub środowisku;

2. podkreśla, że oddziaływanie społeczne i gospodarcze sieci 5G oraz technologii, które ona umożliwia, od internetu rzeczy po sztuczną inteligencję, należy dokładnie ocenić oraz podjąć środki, aby umożliwić sprawiedliwą i równą dla wszystkich transformację w kierunku europejskiego społeczeństwa gigabitowego opartą na odpowiedzialności etycznej;

3. wzywa Komisję i państwa członkowskie do stworzenia środowiska sprzyjającego innowacjom dla dostawców unijnych, aby mogli oni opracowywać nowe produkty, usługi i technologie, oraz do wspierania unijnych przedsiębiorstw we wdrażaniu i komercjalizacji bezpiecznej sieci 5G, przy zapewnieniu, aby jej potencjał był dostępny dla wszystkich przedsiębiorstw w gospodarce cyfrowej UE, w tym małych i średnich przedsiębiorstw;

4. przypomina, że cyberbezpieczeństwo stanowi obecnie jedno z głównych wyzwań dla UE oraz że błędy w tej dziedzinie mogą zagrażać poszanowaniu prywatności i praw podstawowych unijnych konsumentów i producentów, poważnie podważyć zaufanie obywateli do produktów i usług w dziedzinie ICT oraz ostatecznie spowodować

poważne szkody gospodarcze; apeluje o zapewnianie bezpieczeństwa sieci już w fazie projektowania i o domyślne zapewnianie bezpieczeństwa sieci;

5. wzywa Komisję i państwa członkowskie do ścisłej współpracy we wdrażaniu strategii UE w dziedzinie cyberbezpieczeństwa oraz do łączenia środków unijnych i krajowych, aby minimalizować ryzyko luk w zabezpieczeniach i naruszeń ochrony danych w całym łańcuchu wartości; uważa, że takie środki powinny obejmować unijną certyfikację cyberbezpieczeństwa, wymogi dotyczące konfiguracji oraz procedury i praktyki operacyjne, a także promocję cyberhigieny i edukacji cyfrowej;

6. uważa, że agencja UE ds. cyberbezpieczeństwa (Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji – ENISA) ma do odegrania zasadniczą rolę w analizie możliwych zagrożeń, jakie mogą stwarzać zagraniczni dostawcy, w tym z Chin, oraz w koordynacji wspólnego podejścia między państwami członkowskimi, aby eliminować zagrożenia dla cyberbezpieczeństwa i cyberataki;

7. wzywa Komisję i państwa członkowskie do szybkiego wdrożenia pakietu dotyczącego gospodarki o obiegu zamkniętym i poprawy gospodarki surowcami w trakcie całego cyklu życia oraz do recyklingu odpadów, aby poprawić dostęp UE do surowców krytycznych, który ma podstawowe znaczenie dla zaawansowanych technologicznie produktów i pojawiających się innowacji;

8. uważa, że należy pilnie rozwiązać problem możliwych zagrożeń dla bezpieczeństwa technologicznego wynikających z obecnej penetracji rynku przez zagranicznych dostawców, w tym z Chin, przez przyjęcie przez państwa członkowskie wspólnego podejścia w dziedzinie bezpieczeństwa i ochrony danych osobowych;

9. wzywa Komisję i państwa członkowskie do analizy i monitorowania bezpieczeństwa tych systemów ICT, w których technologie z państw trzecich są silnie obecne, także przez przeprowadzanie testów warunków skrajnych;

10. podkreśla, że nie należy dyskryminować dostawców z państw trzecich ze względu na kraj pochodzenia, jednak należy brać pod uwagę przejrzystość tych przedsiębiorstw, stosowane przez nie normy cyberbezpieczeństwa i przestrzeganie zasady wzajemności względem europejskich przedsiębiorstw w ich państwie pochodzenia, aby zapewnić równość szans;

11. podkreśla, że dostawcy i operatorzy z Chin lub innych państw trzecich w żadnym wypadku nie powinni stwarzać zagrożeń dla poszanowania praw indywidualnych zagwarantowanych na mocy prawa UE, nawet jeśli w prawie krajowym obowiązującym w ich państwie pochodzenia istnieją inne wymogi;

12. zwraca się do Rady o pozytywne rozpatrzenie ponownego otwarcia rozmów dotyczących nowego, zmienionego wniosku Komisji w sprawie procedury ograniczającej dostęp zagranicznych produktów do rynku zamówień UE w razie braku wzajemnego dostępu;

13. przypomina o znaczeniu dalszych postępów w negocjacjach w sprawie współpracy regulacyjnej w dziedzinie technologii cyfrowej z państwami trzecimi oraz zapewnienia ich większego zaangażowania w działania międzynarodowych organów

normalizacyjnych;

14. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie i Komisji.