|  |  |
| --- | --- |
| Parlament Europejski2014-2019 |  |

Dokument z posiedzenia

<NoDocSe>B8‑0160/2019</NoDocSe>

<Date>{06/03/2019}6.3.2019</Date>

<TitreType>PROJEKT REZOLUCJI</TitreType>

<TitreSuite>złożony w następstwie oświadczeń Rady i Komisji</TitreSuite>

<TitreRecueil>zgodnie z art. 123 ust. 2 Regulaminu</TitreRecueil>

<Titre>w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia</Titre>

<DocRef>(2019/2575(RSP))</DocRef>

<RepeatBlock-By><Depute>Reinhard Bütikofer</Depute>

<Commission>{Verts/ALE}w imieniu grupy Verts/ALE</Commission>

</RepeatBlock-By>

B8‑0160/2019

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]](#footnote-2),

– 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]](#footnote-3),

– uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW[[3]](#footnote-4),

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

– uwzględniając przyjętą w Chinach ustawę o wywiadzie narodowym z dnia 28 czerwca 2017 r. oraz ustawę dotyczącą bezpieczeństwa państwowego z dnia 1 lipca 2015 r.,

– 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 przyjęcie przez rząd Australii rządowych reform dotyczących bezpieczeństwa sektora telekomunikacji, które weszły w życie z dniem 18 września 2018 r.,

– 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 Unii Europejskiej[[4]](#footnote-5),

– 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[[5]](#footnote-6),

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

– 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[[6]](#footnote-7),

– 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)[[7]](#footnote-8),

– uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013/UE z dnia 11 grudnia 2013 r. ustanawiające instrument „Łącząc Europę”, zmieniające rozporządzenie (UE) nr 913/2010 oraz uchylające rozporządzenia (WE) nr 680/2007 i (WE) nr 67/2010[[8]](#footnote-9),

– uwzględniając program „Cyfrowa Europa”,

– uwzględniając art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że UE wspiera cyfryzację swojego przemysłu oraz wykorzystywanie sieci i urządzeń nowej generacji, a także podjęła szereg działań, aby wyznaczać standardy dla sieci 5G;

B. mając na uwadze możliwość wykorzystywania luk w zabezpieczeniach sieci 5G, aby zagrozić bezpieczeństwu systemów informatycznych, co potencjalnie mogłoby prowadzić do bardzo poważnych szkód dla gospodarek na szczeblu europejskim i krajowym; mając na uwadze, że w celu minimalizacji zagrożeń niezbędne jest przyjęcie podejścia opartego na analizie ryzyka w całym łańcuchu wartości;

C. mając na uwadze, że sieć 5G będzie stanowiła trzon europejskiej infrastruktury cyfrowej, zwiększając możliwości połączenia różnych urządzeń z sieciami (internet rzeczy itp.), oraz zapewni społeczeństwu i przedsiębiorstwom nowe korzyści i możliwości w wielu dziedzinach, w tym w kluczowych sektorach gospodarki, takich jak transport, energetyka, ochrona zdrowia, finanse, telekomunikacja, obrona, przestrzeń kosmiczna i bezpieczeństwo;

D. mając na uwadze wielokrotne apele Parlamentu o opracowanie europejskiej strategii na rzecz większej niezależności w dziedzinie IT i prywatności w internecie, która stałaby się bodźcem dla sektora informatycznego w UE;

E. mając na uwadze, że podniesione zostały obawy dotyczące sprzedawców sprzętu z państw trzecich mogących zagrażać bezpieczeństwu UE z powodu przepisów obowiązujących w ich państwach pochodzenia, w szczególności w następstwie przyjęcia chińskiej ustawy dotyczącej bezpieczeństwa państwowego, która zawiera bardzo szeroką definicję bezpieczeństwa narodowego i zobowiązuje wszystkich obywateli, przedsiębiorstwa i inne podmioty do współpracy z państwem w celu ochrony bezpieczeństwa państwa; mając na uwadze, że nie ma gwarancji, że obowiązki te nie mają zastosowania eksterytorialnego; mając na uwadze, że przepisy przyjęte w Chinach spotkały się z różnymi reakcjami państw, w tym Stanów Zjednoczonych, Australii i Nowej Zelandii, począwszy od ocen stanu bezpieczeństwa po ustanowienie całkowitego zakazu;

F. mając na uwadze, że dostęp do rynku jest już uwarunkowany przestrzeganiem europejskich przepisów w przypadku znacznej liczby produktów, lecz cyberbezpieczeństwo nie stanowi jeszcze wymogu, a systemy certyfikacji zgodnie z aktem ws. cyberbezpieczeństwa nie zapewniają odpowiedniej odpowiedzi na pilny charakter sytuacji, w szczególności w odniesieniu do powszechnej łączności konsumentów i urządzeń podłączonych do sieci;

G. mając na uwadze, że zdarzały się już incydenty związane z bezpieczeństwem w UE ze względu na luki w zabezpieczeniach sieci komunikacyjnych, w tym miał miejsce nieuprawniony dostęp do belgijskiego operatora telekomunikacyjnego świadczącego usługi na rzecz instytucji UE;

H. mając na uwadze, że potrzebna jest wnikliwa analiza w celu wyjaśnienia, czy urządzenia biorące udział w tych incydentach lub wszelkie inne urządzenia lub dostawcy stwarzają zagrożenie dla bezpieczeństwa ze względu na cechy takie jak luki w zabezpieczeniach typu backdoor;

I. mając na uwadze konieczność koordynacji i rozpatrywania rozwiązań na szczeblu UE w celu uniknięcia różnic w poziomie bezpieczeństwa i potencjalnych luk w dziedzinie cyberbezpieczeństwa; mając na uwadze, że koordynacja jest również konieczna na szczeblu światowym w celu zagwarantowania zdecydowanej reakcji;

J. mając na uwadze, że korzyści płynące z jednolitego rynku wiążą się z obowiązkiem przestrzegania unijnych norm i ram prawnych; mając na uwadze, że dostawcy nie powinni spotykać się z różnym traktowaniem w zależności od państwa pochodzenia;

K. mając na uwadze, że w przyszłym rozporządzeniu UE ustanawiającym ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii Europejskiej przewidziano wykaz czynników uznawanych za związane z bezpieczeństwem i porządkiem publicznym, które obejmują infrastrukturę krytyczną, w tym infrastrukturę komunikacyjną, technologie krytyczne, cyberbezpieczeństwo, dostęp do szczególnie chronionych informacji oraz swobodę kontrolowania tych informacji; mając na uwadze, że czynniki takie jak fakt, czy inwestor zagraniczny jest pośrednio kontrolowany przez rząd państwa pochodzenia, powinny być uznawane za istotne dla bezpieczeństwa i porządku publicznego; mając na uwadze, że w rozporządzeniu uwzględniono również projekty i programy leżące w interesie Unii, takie jak transeuropejskie sieci telekomunikacyjne i program „Horyzont 2020”; mając na uwadze, że w rozporządzeniu ustanowiono mechanizm umożliwiający Komisji i państwom członkowskim współpracę w dziedzinie oceny zagrożeń dla bezpieczeństwa związanych z bezpośrednimi inwestycjami zagranicznymi;

1. uważa, że Unia powinna objąć wiodącą rolę w dziedzinie cyberbezpieczeństwa za pośrednictwem wspólnego podejścia w oparciu o skuteczne i wydajne wykorzystywanie specjalistycznej wiedzy na poziomie UE, państw członkowskich i przemysłu, ponieważ mozaika rozbieżnych decyzji na szczeblu krajowym miałaby szkodliwy wpływ na jednolity rynek cyfrowy;

2. podkreśla znaczenie szybkiego przyjęcia unijnego podejścia do bezpieczeństwa infrastruktury w perspektywie wdrażania technologii 5G przy uwzględnieniu zagrożeń dla bezpieczeństwa i porządku publicznego na skutek ingerencji i wpływu państw trzecich; podkreśla, że jest to kwestia własnego bezpieczeństwa i podstawowych interesów UE;

3. z zadowoleniem przyjmuje zbliżające się wejście w życie rozporządzenia ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych ze względów bezpieczeństwa i porządku publicznego oraz podkreśla, że rozporządzenie to po raz pierwszy ustanawia wykaz obszarów i czynników mających znaczenie dla bezpieczeństwa i porządku publicznego na szczeblu UE;

4. wyraża głębokie zaniepokojenie z powodu niedawnych doniesień dotyczących możliwego wyposażenia urządzeń 5G opracowanych przez chińskie przedsiębiorstwa w luki w zabezpieczeniach (backdoor) zapewniające producentom i organom nieuprawniony dostęp do danych i połączeń telekomunikacyjnych obywateli i przedsiębiorstw UE; jest równie zaniepokojony możliwą obecnością istotnych luki w zabezpieczeniach w urządzeniach 5G opracowanych przez tych producentów w przypadku ich montażu w ramach wdrażania sieci 5G w nadchodzących latach; apeluje do Komisji i państw członkowskich, aby rozważyły zakaz korzystania ze sprzętu 5G producentów niezdolnych do zapewnienia odpowiednich gwarancji w dziedzinie bezpieczeństwa;

5. podkreśla, że skutki dla bezpieczeństwa sieci i sprzętu są podobne na całym świecie i wzywa UE do wyciągnięcia wniosków z dostępnych doświadczeń, aby móc zapewnić najwyższe normy w zakresie cyberbezpieczeństwa; jest zdania, że w przypadku braku możliwości zagwarantowania zgodności z wymogami w dziedzinie bezpieczeństwa należy zastosować odpowiednie środki; zauważa, że w ramach oceny adekwatności pod względem bezpieczeństwa UE powinna wymagać znaczących i wiarygodnych gwarancji, w szczególności w przypadku gdy akcje danego przedsiębiorstwa nie są przedmiotem publicznego obrotu, przedsiębiorstwo ma niejasne struktury organizacyjne i nie zapewnia przejrzystości w odniesieniu do źródeł finansowania i podejmowania decyzji;

6. wzywa państwa członkowskie, aby informowały Komisję o wszelkich istotnych środkach krajowych, jakie zamierzają podjąć, aby zapewnić skoordynowaną reakcję Unii w celu zagwarantowania najwyższych norm cyberbezpieczeństwa w całej Unii;

7. ponownie podkreśla, że wszelkie podmioty dostarczające sprzęt lub usługi w UE, niezależnie od ich państwa pochodzenia, muszą spełniać zobowiązania w zakresie praw podstawowych oraz zapewniać zgodność z prawem obowiązującym w UE i państwach członkowskich, w tym ramami prawnymi w dziedzinie ochrony prywatności, ochrony danych i cyberbezpieczeństwa;

8. wzywa Komisję do dokonania oceny solidności ram prawnych Unii, aby rozwiać obawy dotyczące obecności urządzeń zawierających luki w zabezpieczeniach w sektorach strategicznych i infrastrukturze szkieletowej; wzywa Komisję do przedstawienia inicjatyw, w tym – w stosownych przypadkach – wniosków ustawodawczych, aby w odpowiednim czasie usunąć wszelkie braki stwierdzone od początku trwającego unijnego procesu identyfikacji i eliminowania problemów w zakresie cyberbezpieczeństwa i zwiększania odporności UE pod względem cyberbezpieczeństwa;

9. wzywa państwa członkowskie, które nie transponowały jeszcze w pełni dyrektywy w sprawie bezpieczeństwa sieci i informacji, aby dokonały tego niezwłocznie; wzywa Komisję do ścisłego monitorowania procesu transpozycji, aby zapewnić właściwe stosowanie i egzekwowanie przepisów dyrektywy oraz lepszą ochronę europejskich obywateli przed zewnętrznymi i wewnętrznymi zagrożeniami dla bezpieczeństwa;

10. z zadowoleniem przyjmuje i popiera porozumienie dotyczące aktu ws. cyberbezpieczeństwa i wzmocnienia mandatu Agencji UE ds. Bezpieczeństwa Sieci i Informacji (ENISA) w celu lepszego wspierania państw członkowskich w walce z zagrożeniami i atakami w dziedzinie cyberbezpieczeństwa;

11. przypomina, że cyberbezpieczeństwo wymaga stawiania wysokich wymogów w dziedzinie bezpieczeństwa; apeluje o zapewnianie bezpieczeństwa sieci i produktów już w fazie projektowania i o domyślne zapewnianie ich bezpieczeństwa; wzywa Komisję, aby zobowiązała agencję ENISA do priorytetowego traktowania prac dotyczących systemu certyfikacji sprzętu 5G w celu zapewnienia, aby wdrożenie sieci 5G w Unii spełniało najwyższe normy bezpieczeństwa i gwarantowało odporność na luki w zabezpieczeniach typu backdoor i inne luki mogące zagrażać bezpieczeństwu sieci telekomunikacyjnych UE i usług zależnych; zaleca zwrócenie szczególnej uwagi na powszechnie stosowane procesy, produkty i oprogramowanie, które ze względu na samą skalę zastosowania mają istotny wpływ na codzienne życie obywateli i gospodarkę;

12. z dużym zadowoleniem przyjmuje wnioski dotyczące centrów kompetencji w dziedzinie cyberbezpieczeństwa i sieci krajowych ośrodków koordynacji mającej wspierać UE w utrzymaniu i rozwoju zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa, niezbędnych do zabezpieczenia jednolitego rynku cyfrowego UE;

13. z zadowoleniem przyjmuje program „Cyfrowa Europa” nakładający szereg wymogów w dziedzinie bezpieczeństwa oraz nadzór Komisji nad podmiotami mającymi siedzibę na terenie UE, lecz kontrolowanymi z państw trzecich, zwłaszcza w odniesieniu do działań związanych z cyberbezpieczeństwem; podkreśla znaczenie wykluczenia możliwości ingerencji w kwestie bezpieczeństwa za pośrednictwem żądań organów wykonawczych państw trzecich dotyczących współpracy wywiadowczej;

14. wzywa państwa członkowskie do zagwarantowania, aby instytucje publiczne i prywatne przedsiębiorstwa uczestniczące w zapewnieniu właściwego funkcjonowania sieci infrastruktury krytycznej, w tym w dziedzinie telekomunikacji, energetyki, ochrony zdrowia i systemów socjalnych, dokonały stosownych ocen i analiz ryzyka z uwzględnieniem zagrożeń dla bezpieczeństwa szczególnie związanych z cechami technicznymi danego systemu lub zależności od zewnętrznych dostawców technologii w dziedzinie sprzętu i oprogramowania;

15. przypomina, że obecne ramy prawne dotyczące usług telekomunikacyjnych upoważniają państwa członkowskie do zapewnienia, aby operatorzy sieci telekomunikacyjnych przestrzegali wymogu integralności i dostępności publicznych sieci łączności elektronicznej oraz aby szyfrowanie, zwłaszcza pełne szyfrowanie, było jednym ze sposobów wyeliminowania niektórych problemów związanych z bezpieczeństwem; podkreśla, że zgodnie z Europejskim kodeksem łączności elektronicznej państwom członkowskim przysługują wszelkie niezbędne uprawnienia do badania i stosowania szerokiego wachlarza środków dochodzenia roszczeń w przypadku niezgodności produktów oferowanych na rynku UE;

16. wzywa Komisję i państwa członkowskie, aby uczyniły bezpieczeństwo aspektem obowiązkowym wszystkich procedur zamówień publicznych dotyczących odpowiedniej infrastruktury zarówno na szczeblu UE, jak i na szczeblu krajowym, w tym – w stosownych przypadkach – przy wykorzystaniu europejskich norm i wymagań technicznych mających na celu zwiększenie odporności i wyeliminowanie zagrożeń dla bezpieczeństwa;

17. oczekuje od krajowych organów ochrony danych i Europejskiego Inspektora Ochrony Danych przeprowadzenia dogłębnej analizy przesłanek wskazujących na naruszenie ochrony danych przez zewnętrznych sprzedawców oraz do nałożenia odpowiednich kar i sankcji zgodnie z europejskim prawem w dziedzinie ochrony danych;

18. ponownie podkreśla, że UE musi wspierać cyberbezpieczeństwo w całym łańcuchu wartości, od badań naukowych po wdrażanie i zastosowanie kluczowych technologii, rozpowszechniać istotne informacje oraz wspierać programy kształcenia w dziedzinie cyberbezpieczeństwa; uważa m.in., że program „Cyfrowa Europa” będzie skutecznym narzędziem w tym zakresie;

19. wzywa Komisję i państwa członkowskie do podjęcia niezbędnych działań w celu stworzenia środowiska sprzyjającego innowacyjności w UE, które powinno być dostępne dla wszystkich przedsiębiorstw w ramach cyfrowej gospodarki UE, w tym małych i średnich przedsiębiorstw (MŚP), a także powinno umożliwiać europejskim sprzedawcom opracowywanie nowych produktów, usług i technologii, pozwalając im na odzyskanie udziału w rynku utraconego na rzecz konkurentów z państw trzecich;

20. wzywa Komisję do dokonania oceny nadzoru i kontroli rynku pod względem cyberbezpieczeństwa oraz do przedstawienia środków zapewniających skuteczne wyeliminowanie zagrożeń w tej dziedzinie; przypomina, że unijne podmioty z branży, zwłaszcza MŚP, są narażone na nieuczciwą konkurencję ze strony przedsiębiorstw finansowanych przez państwo, strategiczne przejęcia i nieuprawniony dostęp do posiadanych danych; stwierdza, że te podmioty z branży powinny być zaangażowane w opracowanie możliwych środków ustawodawczych;

21. wzywa Komisję do włączenia wymogów bezpieczeństwa systemów informatycznych do przeglądu nowych ram prawnych dotyczących bezpieczeństwa produktów;

22. wzywa Radę do przyspieszenia prac nad wnioskiem dotyczącym rozporządzenia w sprawie prywatności w sieci oraz do uwzględnienia obowiązkowego pełnego szyfrowania i zakazu stosowania zlecanych przez rządy luk w zabezpieczeniach zgodnie z wnioskiem Parlamentu przedstawionym w stanowisku przyjętym w pierwszym czytaniu;

23. wzywa Radę Europejską, aby rozważyła podjęcie działań zgodnie z zaleceniami wskazanymi w niniejszej rezolucji podczas kolejnego posiedzenia w dniu 21 marca 2019 r.;

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

1. Dz.U. L 321 z 17.12.2018, s. 36. [↑](#footnote-ref-2)
2. Dz.U. L 194 z 19.7.2016, s. 1. [↑](#footnote-ref-3)
3. Dz.U. L 218 z 14.8.2013, s. 8. [↑](#footnote-ref-4)
4. Teksty przyjęte, P8\_TA(2019)0121. [↑](#footnote-ref-5)
5. Teksty przyjęte, P8\_TA(2018)0343. [↑](#footnote-ref-6)
6. Dz.U. C 307 z 30.8.2018, s. 144. [↑](#footnote-ref-7)
7. Dz.U. L 119 z 4.5.2016, s. 1. [↑](#footnote-ref-8)
8. Dz.U. L 348 z 20.12.2013, s. 129. [↑](#footnote-ref-9)