Wtorek, 12 marca 2019 r.

I

(Rezolucje, zalecenia i opinie)

REZOLUCJE

PARLAMENT EUROPEJSKI

P8_TA(2019)0156

Zagrożenia dla bezpieczeństwa wynikające z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia

Rezolucja Parlamentu Europejskiego z dnia 12 marca 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 (2019/2575(RSP))

(2021/C 23/01)

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 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]),

— uwzględniając wniosek Komisji z 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 12 września 2018 r. dotyczący rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych (COM(2018)0630),

— uwzględniając fakt, że 28 czerwca 2017 r. chińskie Zgromadzenie Przedstawicieli Ludowych przyjęło nową ustawę o wywiadzie narodowym,

— uwzględniając oświadczenia Rady i Komisji z 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,

([1]) Dz.U. L 321 z 17.12.2018, s. 36.
([2]) Dz.U. L 194 z 19.7.2016, s. 1.
([3]) Dz.U. L 218 z 14.8.2013, s. 8.

— uwzględniając przyjęcie przez rząd australijski decyzji o rządowych reformach dotyczących bezpieczeństwa sektora telekomunikacji, która weszła w życie w dniu 18 września 2018 r.,

— uwzględniając swoje stanowisko przyjęte 14 lutego 2019 r. w pierwszym czytaniu w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii Europejskiej ([1]),

— uwzględniając swoje wcześniejsze rezolucje w sprawie stosunków między UE a Chinami, w szczególności rezolucję z 12 września 2018 r. ([2]),

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

— uwzględniają swoją rezolucję z 1 czerwca 2017 r. w sprawie łączności internetowej na rzecz wzrostu gospodarczego, konkurencyjności i spójności: europejskie społeczeństwo gigabitowe i 5G ([3]),

— 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) ([4]),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013 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 ([5]),

— uwzględniając wniosek Komisji z 6 czerwca 2018 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" na lata 2021–2027 (COM(2018)0434),

— uwzględniając art. 123 ust. 2 i 4 Regulaminu,

A. mając na uwadze, że UE musi realizować program na rzecz cyberbezpieczeństwa, aby wykorzystać swój potencjał i zająć czołową pozycję w tym obszarze oraz wykorzystać ją z korzyścią dla swojego przemysłu;

B. mając na uwadze, że słabe punkty w zabezpieczeniach sieci 5G można wykorzystać do zakłócenia funkcjonowania systemów informatycznych, co może potencjalnie spowodować poważne szkody w gospodarce na szczeblu europejskim i krajowym; mając na uwadze, że zminimalizowanie ryzyka wymaga podejścia opartego na analizie ryzyka w całym łańcuchu wartości;

C. mając na uwadze, że sieć 5G będzie podstawą naszej infrastruktury cyfrowej, rozszerzy możliwości połączenia różnych urządzeń z siecią (internet rzeczy itp.) oraz przyniesie nowe korzyści i możliwości społeczeństwu i przedsiębiorstwom w wielu dziedzinach, w tym w krytycznych sektorach gospodarki, np. w transporcie, energetyce, służbie zdrowia, finansach, telekomunikacji, obronności, sektorze kosmicznym i sektorze bezpieczeństwa;

D. mając na uwadze, że stworzenie odpowiedniego mechanizmu reagowania na wyzwania dotyczące bezpieczeństwa umożliwiłoby UE aktywne działanie w wyznaczaniu standardów sieci 5G;

E. mając na uwadze podnoszone obawy dotyczące sprzedawców sprzętu z państw trzecich, mogących zagrażać bezpieczeństwu UE z powodu przepisów obowiązujących w państwach pochodzenia, zwłaszcza w związku z przyjęciem chińskiej ustawy o bezpieczeństwie państwowym, która zobowiązuje wszystkich obywateli, przedsiębiorstwa i inne podmioty do współpracy z państwem w ochronie bezpieczeństwa państwowego, w powiązaniu z bardzo szeroką definicją bezpieczeństwa narodowego; mając na uwadze, że nie ma gwarancji, że obowiązki te nie są stosowane eksterytorialnie, a także mając na uwadze, że ustawy chińskie spotkały się z różnymi reakcjami w różnych państwach, począwszy od przeprowadzenia ocen stanu bezpieczeństwa, a skończywszy na wprowadzeniu całkowitego zakazu;

([1]) Teksty przyjęte, P8_TA(2019)0121.
([2]) Teksty przyjęte, P8_TA(2018)0343.
([3]) Dz.U. C 307 z 30.8.2018, s. 144.
([4]) Dz.U. L 119 z 4.5.2016, s. 1.
([5]) Dz.U. L 348 z 20.12.2013, s. 129.

Wtorek, 12 marca 2019 r.

F. mając na uwadze, że w grudniu 2018 r. czeski krajowy organ ds. cyberbezpieczeństwa wydał ostrzeżenie przed zagrożeniami dla bezpieczeństwa stwarzanymi przez technologie dostarczane przez chińskie przedsiębiorstwa Huawei i ZTE; mając na uwadze, że następnie w styczniu 2019 r. czeskie organy podatkowe wykluczyły Huawei z przetargu na utworzenie portalu służb podatkowych;

G. mając na uwadze, że potrzebne jest szczegółowe dochodzenie, by wyjaśnić, czy dane urządzenia lub dostawcy stanowią zagrożenie dla bezpieczeństwa ze względu na takie elementy jak umożliwiające dostęp do systemu luki w zabezpieczeniach (backdoor);

H. mając na uwadze, że rozwiązania należy koordynować i analizować na szczeblu UE, by uniknąć różnic w poziomie bezpieczeństwa i potencjalnych luk w dziedzinie cyberbezpieczeństwa, a koordynacja na szczeblu światowym jest konieczna, by móc zdecydowanie reagować;

I. mając na uwadze, że korzyści płynące z jednolitego rynku wiążą się z obowiązkiem przestrzegania unijnych norm i przepisów, a także mając na uwadze, że dostawcy nie powinni być traktowani odmiennie w zależności od państwa pochodzenia;

J. mając na uwadze, że rozporządzenie w sprawie monitorowania bezpośrednich inwestycji zagranicznych, które powinno wejść w życie pod koniec 2020 r., zwiększa zdolność państw członkowskich do monitorowania inwestycji zagranicznych na podstawie kryteriów dotyczących bezpieczeństwa i porządku publicznego oraz ustanawia mechanizm współpracy pozwalający Komisji i państwom członkowskim współpracować przy ocenie zagrożeń dla bezpieczeństwa, w tym cyberbezpieczeństwa, stwarzanych przez newralgiczne inwestycje zagraniczne, i obejmujący również projekty i programy leżące w interesie Unii, np. transeuropejskie sieci telekomunikacyjne i program „Horyzont 2020";

1. uważa, że Unia musi odegrać pierwszoplanową rolę w dziedzinie cyberbezpieczeństwa dzięki wspólnemu podejściu skutecznie i wydajnie wykorzystującemu specjalistyczną wiedzę UE, państw członkowskich i przemysłu, ponieważ mozaika rozbieżnych decyzji krajowych miałaby szkodliwy wpływ na jednolity rynek cyfrowy;

2. wyraża głębokie zaniepokojenie niedawnymi doniesieniami, zgodnie z którymi sprzęt 5G tworzony przez chińskie przedsiębiorstwa może mieć wbudowane luki w zabezpieczeniach (typu backdoor) umożliwiające producentom i organom nieuprawniony dostęp do danych prywatnych i danych osobowych oraz do połączeń telekomunikacyjnych z UE;

3. jest równie zaniepokojony możliwością występowania istotnych słabych punktów w zabezpieczeniach sprzętu 5G opracowanego przez tych producentów, gdyż sprzęt taki może być potencjalnie instalowany w związku z wdrażaniem sieci 5G w nadchodzących latach;

4. 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 cyberbezpieczeństwa; apeluje do Komisji o opracowanie strategii, która pozwoli Europie zająć czołową pozycję w dziedzinie technologii cyberbezpieczeństwa i będzie mieć na celu zmniejszenie zależności Europy od zagranicznych technologii w dziedzinie cyberbezpieczeństwa; jest zdania, że we wszystkich przypadkach, gdy nie można zagwarantować zgodności z wymogami bezpieczeństwa, należy zastosować odpowiednie środki;

5. wzywa państwa członkowskie do informowania Komisji o wszelkich środkach krajowych, jakie zamierzają podjąć, by zapewnić skoordynowaną reakcję Unii i zagwarantować najwyższe normy cyberbezpieczeństwa w całej Unii, oraz przypomina, że należy powstrzymać się od wprowadzania nieproporcjonalnych środków jednostronnych, które prowadziłyby do fragmentacji jednolitego rynku;

6. ponownie podkreśla, że wszelkie podmioty dostarczające sprzęt lub usługi w UE, niezależnie od państwa pochodzenia, muszą wypełniać obowiązki dotyczące praw podstawowych oraz przestrzegać prawa UE i państw członkowskich, w tym przepisów o ochronie prywatności, ochronie danych i cyberbezpieczeństwie;

7. wzywa Komisję do przeprowadzenia oceny solidności przepisów Unii, by rozwiać obawy dotyczące występowania w sektorach strategicznych i infrastrukturze podstawowej urządzeń zawierających luki w zabezpieczeniach; wzywa Komisję do przedstawienia inicjatyw, w tym – w stosownych przypadkach – wniosków ustawodawczych, by na czas usunąć wszelkie braki stwierdzone, odkąd w Unii zapoczątkowano proces stałego identyfikowania i eliminowania problemów w zakresie cyberbezpieczeństwa oraz zwiększania odporności UE pod względem cyberbezpieczeństwa;

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

9. apeluje do Komisji i państw członkowskich o zapewnienie właściwego stosowania mechanizmów sprawozdawczych wprowadzonych w dyrektywie w sprawie bezpieczeństwa sieci i informacji; zwraca uwagę, że Komisja i państwa członkowskie powinny podejmować szczegółowe działania następcze w stosunku do wszelkich incydentów dotyczących bezpieczeństwa lub niewłaściwych reakcji dostawców, by wyeliminować wykryte luki;

10. wzywa Komisję, by przeanalizowała potrzebę dalszego rozszerzania zakresu dyrektywy w sprawie bezpieczeństwa sieci i informacji na inne sektory i usługi krytyczne nieobjęte szczegółowymi przepisami sektorowymi;

11. przyjmuje z zadowoleniem i popiera osiągnięte porozumienie dotyczące aktu ws. cyberbezpieczeństwa i wzmocnienia mandatu Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), by lepiej wspierać państwa członkowskie w przeciwdziałaniu zagrożeniom i atakom w dziedzinie cyberbezpieczeństwa;

12. wzywa Komisję, by upoważniła agencję ENISA do priorytetowego traktowania prac nad systemem certyfikacji sprzętu 5G w celu zapewnienia wdrożenia sieci 5G w Unii zgodnej z najwyższymi normami bezpieczeństwa i odpornej na występowanie luk w zabezpieczeniach typu backdoor i innych słabych punktów mogących 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;

13. z dużym zadowoleniem przyjmuje wnioski dotyczące centrów kompetencji w dziedzinie cyberbezpieczeństwa i sieci krajowych ośrodków koordynacji, mających wspierać UE w utrzymaniu i rozwoju zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa, niezbędnych do zabezpieczenia jednolitego rynku cyfrowego UE; przypomina jednak, że certyfikacja nie powinna wykluczać monitorowania łańcucha dostaw przez właściwe organy i operatorów w celu zapewnienia integralności i bezpieczeństwa urządzeń działających w krytycznych środowiskach i sieciach telekomunikacyjnych;

14. przypomina, że cyberbezpieczeństwo wymaga zachowania wysokich standardów bezpieczeństwa; apeluje o tworzenie sieci bezpiecznych domyślnie i już w fazie projektowania; wzywa państwa członkowskie, by wraz z Komisją przeanalizowały wszelkie dostępne środki mające zapewniać wysoki poziom bezpieczeństwa;

15. wzywa Komisję i państwa członkowskie, by we współpracy z agencją ENISA opracowały wytyczne dotyczące metod zwalczania cyberzagrożeń i eliminowania słabych punktów przy zamawianiu sprzętu 5G, na przykład przez zakup różnorodnych urządzeń od różnych dostawców lub wprowadzenie wieloetapowych procedur udzielania zamówień;

16. potwierdza swoje stanowisko w sprawie programu „Cyfrowa Europa" nakładającego wymogi dotyczące bezpieczeństwa i przewidującego nadzór Komisji nad podmiotami mającymi siedzibę w UE, lecz kontrolowanymi z państw trzecich, zwłaszcza w odniesieniu do działań związanych z cyberbezpieczeństwem;

17. wzywa państwa członkowskie do zagwarantowania, że instytucje publiczne i przedsiębiorstwa prywatne uczestniczące w zapewnianiu właściwego funkcjonowania sieci infrastruktury krytycznej, np. w telekomunikacji, energetyce, służbie zdrowia i systemach socjalnych, będą wykonywać stosowne oceny i analizy ryzyka z uwzględnieniem zagrożeń dla bezpieczeństwa związanych konkretnie z cechami technicznymi danego systemu lub z zależnością od zewnętrznych dostawców technologii w odniesieniu do sprzętu i oprogramowania;

18. przypomina, że obecne przepisy dotyczące usług telekomunikacyjnych zobowiązują państwa członkowskie do zapewnienia, że operatorzy sieci telekomunikacyjnych przestrzegają wymogu integralności i dostępności publicznych sieci łączności elektronicznej, w tym – w stosownych przypadkach – pełnego szyfrowania transmisji; podkreśla, że zgodnie z Europejskim kodeksem łączności elektronicznej państwa członkowskie mają bardzo szerokie uprawnienia do badania produktów na rynku UE i stosowania dużego zakresu środków zaradczych w razie niezgodności z przepisami;

19. wzywa Komisję i państwa członkowskie, by uznały bezpieczeństwo za obowiązkowy element wszystkich procedur udzielania zamówień publicznych na stosowną infrastrukturę zarówno na szczeblu UE, jak i na szczeblu krajowym;

20. przypomina państwom członkowskim, że według przepisów UE, zwłaszcza dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne, mają obowiązek nakładać sankcje na osoby prawne, które dopuściły się takich przestępstw jak ataki na tego rodzaju systemy; podkreśla, że państwa członkowskie powinny również korzystać z możliwości nakładania na te osoby prawne innych sankcji, np. tymczasowego lub trwałego zakazu prowadzenia działalności gospodarczej;

21. wzywa państwa członkowskie, agencje ds. cyberbezpieczeństwa, operatorów telekomunikacyjnych, producentów i dostawców usług w dziedzinie infrastruktury krytycznej, by zgłaszali Komisji i agencji ENISA wszelkie dowody na istnienie luk w zabezpieczeniach typu backdoor i innych poważnych luk mogących zagrozić integralności i bezpieczeństwu sieci telekomunikacyjnych lub naruszać prawo Unii i prawa podstawowe; oczekuje od krajowych organów ochrony danych i Europejskiego Inspektora Ochrony Danych przeprowadzenia dogłębnej analizy przesłanek wskazujących na naruszenie ochrony danych przez zewnętrznych sprzedawców oraz nakładania odpowiednich kar i sankcji zgodnie z europejskim prawem w dziedzinie ochrony danych;

22. z zadowoleniem przyjmuje wejście w życie rozporządzenia ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych pod względem bezpieczeństwa i porządku publicznego oraz podkreśla, że w rozporządzeniu tym po raz pierwszy wprowadzono wykaz dziedzin i czynników, w tym komunikacji i cyberbezpieczeństwa, istotnych dla bezpieczeństwa i porządku publicznego na szczeblu UE;

23. wzywa Radę do przyspieszenia prac nad wnioskiem w sprawie rozporządzenia o prywatności elektronicznej;

24. ponownie podkreśla, że UE musi wspierać cyberbezpieczeństwo w całym łańcuchu wartości, od badań naukowych po wdrażanie i wykorzystanie kluczowych technologii, rozpowszechniać istotne informacje oraz propagować higienę cyberbezpieczeństwa i wspierać programy nauczania obejmujące cyberbezpieczeństwo, a ponadto uważa, że skutecznym narzędziem w tej dziedzinie będzie m.in. program „Cyfrowa Europa”;

25. wzywa Komisję i państwa członkowskie do podjęcia niezbędnych działań, w tym przyjęcia solidnych programów inwestycyjnych, w celu stworzenia w UE środowiska sprzyjającego innowacyjności, które powinno być dostępne dla wszystkich przedsiębiorstw gospodarki cyfrowej UE, w tym dla małych i średnich przedsiębiorstw (MŚP); apeluje ponadto, by środowisko takie umożliwiało sprzedawcom europejskim opracowywanie nowych produktów, usług i technologii, umożliwiających im konkurencyjność;

26. wzywa Komisję i państwa członkowskie, by uwzględniły powyższe wnioski w zbliżających się rozmowach o przyszłej strategii UE-Chiny, jako warunki utrzymania konkurencyjności UE oraz zapewnienia bezpieczeństwa jej infrastruktury cyfrowej;

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