PL 2022

03

Sprawozdanie specjalne

Wprowadzenie sieci 5G w UE –

opóźnienia we wdrażaniu i nierozwiązane kwestie związane z bezpieczeństwem

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

Spis treści

Streszczenie

I Piąta generacja systemów telekomunikacyjnych, czyli 5G, to nowy globalny standard sieci bezprzewodowych, który oferuje znacznie większą przepustowość i prędkość transmisji danych. Usługi 5G są niezbędne dla szerokiego wachlarza innowacyjnych zastosowań mogących przyczynić się do transformacji wielu sektorów gospodarki, a także ulepszyć codzienne życie obywateli. 5G ma zatem strategiczne znaczenie dla całego jednolitego rynku.

II W swoim planie działania dotyczącym sieci 5G z 2016 r. Komisja wyznaczyła cel polegający na zapewnieniu do 2025 r. niezakłóconego zasięgu 5G na obszarach miejskich i wzdłuż głównych szlaków transportowych. W marcu 2021 r. rozszerzyła ona ten cel, przyjmując, by do 2030 r. zasięgiem sieci 5G objęte zostały wszystkie zaludnione obszary.

III Chociaż technologia 5G może potencjalnie stworzyć wiele możliwości wzrostu gospodarczego, wiążą się z nią również pewne zagrożenia. W zaleceniu z 2019 r. dotyczącym cyberbezpieczeństwa sieci 5G Komisja przestrzegła, że świadczenie wielu usług o znaczeniu krytycznym w oparciu o sieci 5G sprawi, iż ewentualne zakłócenia na wielką skalę będą mieć szczególnie dotkliwe skutki. Ponadto z uwagi na transgraniczny charakter zagrożeń istotna wrażliwość na zagrożenia w cyberprzestrzeni bądź wystąpienie cyberincydentów w jednym państwie członkowskim mogą mieć negatywne skutki odczuwalne w całej UE. Jedną z konsekwencji wydania przez Komisję zalecenia było opracowanie unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, który został przyjęty w styczniu 2020 r.

IV Całkowity koszt wdrożenia technologii 5G na terenie całej UE może sięgnąć 400 mld euro. W latach 2014–2020 UE zapewniła finansowanie w wysokości ponad 4 mld euro na rzecz projektów 5G.

V Trybunał zbadał, czy Komisja skutecznie wspierała państwa członkowskie w dążeniu do osiągnięcia celów UE w zakresie wprowadzania sieci 5G oraz przy rozwiązywaniu, w skoordynowany sposób, problemów związanych z bezpieczeństwem sieci 5G. W tym celu przeanalizował on kwestie dotyczące zarówno wdrażania sieci 5G, w przypadku którego rok 2020 był kluczowy, jak i ich bezpieczeństwa. Celem niniejszego sprawozdania jest przedstawienie spostrzeżeń i zaleceń, które przyczynią się do terminowego wdrożenia bezpiecznych sieci 5G we wszystkich krajach UE. Przeprowadzając kontrolę, Trybunał skoncentrował się wprawdzie na Komisji, ale przeanalizował również rolę krajowych organów administracji i innych podmiotów.

VI Kontrola wykazała, że w państwach członkowskich występują opóźnienia we wprowadzaniu sieci 5G. Do końca 2020 r. 23 państwa członkowskie uruchomiły komercyjne usługi z wykorzystaniem sieci 5G i osiągnęły pośredni cel polegający na zapewnieniu dostępu do takich sieci w co najmniej jednym dużym mieście. Nie wszystkie państwa członkowskie uwzględniły jednak cele przyjęte przez UE na 2025 i 2030 r. w swoich krajowych strategiach dotyczących sieci 5G lub planach szerokopasmowych. Ponadto w kilku krajach nie dokonano jeszcze transpozycji Europejskiego kodeksu łączności elektronicznej do prawa krajowego, a przydział częstotliwości na potrzeby sieci 5G się opóźnił. Opóźnienia w przydziale częstotliwości mogą wynikać z różnych przyczyn: z niskiego popytu ze strony operatorów sieci łączności ruchomej, problemów w zakresie koordynacji transgranicznej z państwami nienależącymi do UE położonymi wzdłuż wschodnich granic, wpływu pandemii COVID-19 na terminy aukcji oraz niepewności co do tego, jak rozwiązać kwestie bezpieczeństwa. Opóźnienia we wdrażaniu technologii 5G po stronie państw członkowskich zagrażają osiągnięciu celów przyjętych przez UE. Komisja zapewniała wprawdzie państwom członkowskim wsparcie w realizacji przyjętego przez nią w 2016 r. planu działania dotyczącego sieci 5G poprzez wiążące i niewiążące inicjatywy, a także wytyczne i finansowanie badań naukowych w dziedzinie technologii 5G, nie określiła jednak w jednoznaczny sposób oczekiwanej jakości usług sieci 5G.

VII W unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G określono szereg środków strategicznych i technicznych oraz działań wspierających służących przeciwdziałaniu zagrożeniom dla bezpieczeństwa sieci 5G, a także wskazano podmioty właściwe dla każdego z tych środków i działań. Kilka środków dotyczy problemu dostawców sprzętu 5G obarczonych wysokim ryzykiem. Zestaw narzędzi został zatwierdzony przez Komisję i Radę Europejską. Przewidziane w nim kryteria stanowią ramy operacyjne przydatne do oceny profilu ryzyka poszczególnych dostawców w skoordynowany sposób przez wszystkie państwa członkowskie. Niemniej jednak przeprowadzanie takiej oceny leży w dalszym ciągu w kompetencji organów krajowych. Zestaw narzędzi został przyjęty na wczesnym etapie wdrażania technologii 5G, lecz mimo to wielu operatorów sieci ruchomej zdążyło już wcześniej dokonać wyboru dostawców. Od momentu przyjęcia zestawu narzędzi poczyniono postępy, jeśli chodzi o zapewnienie większego bezpieczeństwa sieci 5G, a większość państw członkowskich wprowadziła ograniczenia w odniesieniu do dostawców wysokiego ryzyka lub przygotowuje się do ich wprowadzenia. Przewiduje się, że przyjęcie przez państwa członkowskie przepisów dotyczących bezpieczeństwa sieci 5G w oparciu o zestaw narzędzi w nadchodzących latach może przełożyć się na bardziej zharmonizowane podejście do dostawców technologii 5G obarczonych wysokim ryzykiem. Ponieważ jednak żaden z zaproponowanych dotychczas środków nie ma mocy wiążącej prawnie, Komisja nie może ich egzekwować. W związku z tym wciąż

istnieje ryzyko, że zestaw narzędzi sam w sobie nie będzie w stanie zagwarantować skoordynowanego podejścia ze strony państw członkowskich do kwestii bezpieczeństwa sieci.

VIII Komisja zaczęła przyglądać się zagranicznym subsydiom dla dostawców technologii 5G w kontekście potencjalnych zagrożeń dla bezpieczeństwa sieci. Komisja nie posiada wystarczających informacji na temat podejścia państw członkowskich do kwestii ewentualnych kosztów zastąpienia, które mogłyby powstać, gdyby operatorzy sieci ruchomej zostali zobowiązani do wyeliminowania z unijnych sieci – bez okresu przejściowego – sprzętu od dostawców wysokiego ryzyka.

IX Trybunał zaleca, aby Komisja:

- promowała równomierne i terminowe wdrażanie sieci 5G na terenie UE;
- promowała skoordynowane podejście państw członkowskich do bezpieczeństwa sieci 5G;
- monitorowała podejście państw członkowskich do kwestii bezpieczeństwa sieci 5G oraz przeanalizowała wpływ rozbieżności w tym zakresie na skuteczne funkcjonowanie jednolitego rynku.

Wstęp

Charakter i znaczenie 5G

01 Piąta generacja systemów telekomunikacyjnych, czyli 5G, to nowy globalny standard sieci bezprzewodowych. W porównaniu z sieciami 3G i 4G oferuje ona znacznie większą przepustowość i prędkość transmisji danych. Technologia 5G obejmuje wprawdzie pewne elementy sieci opierające się na poprzednich generacjach technologii łączności mobilnej i bezprzewodowej, ale stanowi coś więcej niż tylko stopniową ewolucję tych sieci. Zapewnia ona uniwersalną łączność o ultrawysokiej przepustowości i niskim poziomie opóźnień dla użytkowników indywidualnych i urządzeń podłączonych do internetu.

02 Sieć 5G pozwoli na połączenie większej liczby urządzeń niż kiedykolwiek wcześniej w ramach tzw. internetu rzeczy. Szacuje się, że do końca 2018 r. na całym świecie w użyciu były 22 miliardy urządzeń podłączonych do internetu. Z prognoz wynika, że do 2030 r.[1] liczba ta wzrośnie do około 50 miliardów, czego skutkiem będzie ogromna sieć wzajemnie połączonych urządzeń – od smartfonów po urządzenia kuchenne. Jednocześnie oczekuje się, że globalny poziom transmisji danych w łączności ruchomej wzrośnie z 12 eksabajtów miesięcznie w 2017 r.[2] do ponad 5 000 eksabajtów w 2030 r.[3]

03 Usługi 5G są niezbędne dla szerokiego wachlarza innowacyjnych zastosowań, które mogą przyczynić się do transformacji wielu sektorów gospodarki UE i ulepszyć codzienne życie obywateli (zob. ***rys. 1***). Badanie przeprowadzone w 2017 r. na zlecenie Komisji wykazało, że korzyści z wprowadzenia sieci 5G w czterech kluczowych strategicznych sektorach przemysłu (motoryzacja, zdrowie, transport i energia) mogą sięgnąć nawet 113 mld euro rocznie[4]. W badaniu tym przewiduje się również, że wdrożenie technologii 5G mogłoby przyczynić się do stworzenia 2,3 mln miejsc pracy

---

[1] Statista, „Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030".

[2] „Cisco Visual Networking Index:Global Mobile Data Traffic Forecast Update, 2017–2022", luty 2019 r.

[3] ITU-R, „IMT traffic estimates for the years 2020 to 2030".

[4] „Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe", luty 2017 r.

w państwach członkowskich. W badaniu z 2021 r. oszacowano z kolei, że w latach 2021–2025 technologia 5G doprowadzi do wzrostu europejskiego produktu krajowego brutto (PKB) o 1 bln euro i może przyczynić się do stworzenia lub przekształcenia nawet 20 mln miejsc pracy we wszystkich sektorach gospodarki[5].

Rys. 1 – Technologia 5G obejmie wszystkie aspekty naszego życia

Źródło: Komisja Europejska.

Obawy związane z bezpieczeństwem

04 Chociaż technologia 5G ma potencjał do tego, by stworzyć wiele możliwości wzrostu gospodarczego, wiąże się z nią również pewne ryzyko (zob. ***załącznik I*** przedstawiający najważniejsze możliwości i zagrożenia związane z technologią 5G). Jednym z obszarów ryzyka jest bezpieczeństwo. Systemy telekomunikacyjne od zawsze były narażone na ryzyko cyberataków (zob. ***załącznik II***)[6]. Kwestie bezpieczeństwa są przedmiotem szczególnej uwagi w przypadku sieci 5G, ponieważ ze względu na charakter tej technologii, a w szczególności jej zależność od oprogramowania, jest ona bardziej narażona na ataki niż systemy telekomunikacyjne 3G lub 4G[7].

---

[5] Strategia Accenture, „The Impact of 5G on the European Economy”, luty 2021 r.

[6] Przegląd nr 02/2019 pt.„Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją (Dokument analityczny)”; „Kompendium kontroli. Cyberbezpieczeństwo w UE i państwach członkowskich UE” z 2020 r. oraz Biuro Analiz Parlamentu Europejskiego – Europejskie Centrum Mediów Naukowych.

[7] Grupa współpracy ds. bezpieczeństwa sieci i informacji, „EU coordinated risk assessment of the cybersecurity of 5G networks”, 9 października 2019 r., pkt 3.4.

05 W związku z tym, że sieci 5G będą stanowić podstawę szerokiego wachlarza usług i zastosowań, ich dostępność stanie się głównym wyzwaniem w zakresie bezpieczeństwa na szczeblu krajowym i unijnym. Jeżeli bowiem hakerom udałoby się uzyskać dostęp do sieci 5G, mogliby zakłócić ich podstawowe funkcje w celu uniemożliwienia świadczenia usług lub przejęcia kontroli nad infrastrukturą krytyczną (np. sieciami energetycznymi), która w UE często ma wymiar transgraniczny. Z rozmaitych badań wynika, że globalne skutki gospodarcze cyberprzestępczości mogą sięgać nawet 5 000 mld euro rocznie, tj. ponad 6% światowego PKB w 2020 r.[8]

06 Kolejnym wyzwaniem związanym z bezpieczeństwem sieci 5G jest fakt, że rozwój i obsługa tych sieci opierają się w krytycznym stopniu na ograniczonej liczbie dostawców. Wiąże się z tym większe ryzyko przerwy w dostawach w przypadku uzależnienia od jednego dostawcy, zwłaszcza jeśli dostawca jest obarczony wysokim ryzykiem, ponieważ przykładowo może podlegać interwencji ze strony kraju spoza UE. W 2019 r. grupa współpracy ds. bezpieczeństwa sieci i systemów informatycznych, złożona z przedstawicieli państw członkowskich i organów UE, zwróciła uwagę na ryzyko uzyskania łatwego dostępu do sieci 5G przez „wrogie podmioty państwowe" poprzez uprzywilejowany dostęp, wywieranie nacisku na dostawcę lub powoływanie się na krajowe wymogi prawne[9] (zob. ***ramka 1***). To właśnie w tym kontekście UE przystąpiła do opracowania inicjatyw w dziedzinie bezpieczeństwa sieci 5G.

Ramka 1

Obawy dotyczące bezpieczeństwa w kontekście współpracy UE z Chinami w zakresie sieci 5G

- W 2015 r. UE podpisała z Chinami wspólną deklarację w sprawie strategicznej współpracy w zakresie sieci 5G, zobowiązując się do wzajemności i otwartości w dostępie do finansowania badań nad technologią 5G oraz dostępie do rynku[10].
- W 2017 r. Chiny przyjęły ustawę o wywiadzie krajowym, zgodnie z którą wszystkie chińskie organizacje i obywatele mają obowiązek współpracować

[8] Światowe Forum Ekonomiczne, „Wild Wide Web – Consequences of Digital Fragmentation", 2021.

[9] Grupa współpracy ds. bezpieczeństwa sieci i informacji, „EU coordinated risk assessment of the cybersecurity of 5G networks", 9 października 2019 r.

[10] https://ec.europa.eu/commission/presscorner/detail/pl/IP_15_5715

w ramach wywiadu krajowego. Przewidziano w niej również mechanizmy ochrony tajności danych wywiadowczych[11]. W reakcji na tę ustawę USA podjęły w 2018 r. działania, aby ograniczyć działalność kilku chińskich firm, w tym Huawei, kluczowego dostawcy technologii 5G.

W marcu 2019 r. również Parlament Europejski wyraził obawy co do tego, że chińscy dostawcy technologii 5G mogą stanowić zagrożenie dla bezpieczeństwa UE ze względu na przepisy obowiązujące w ich kraju pochodzenia.

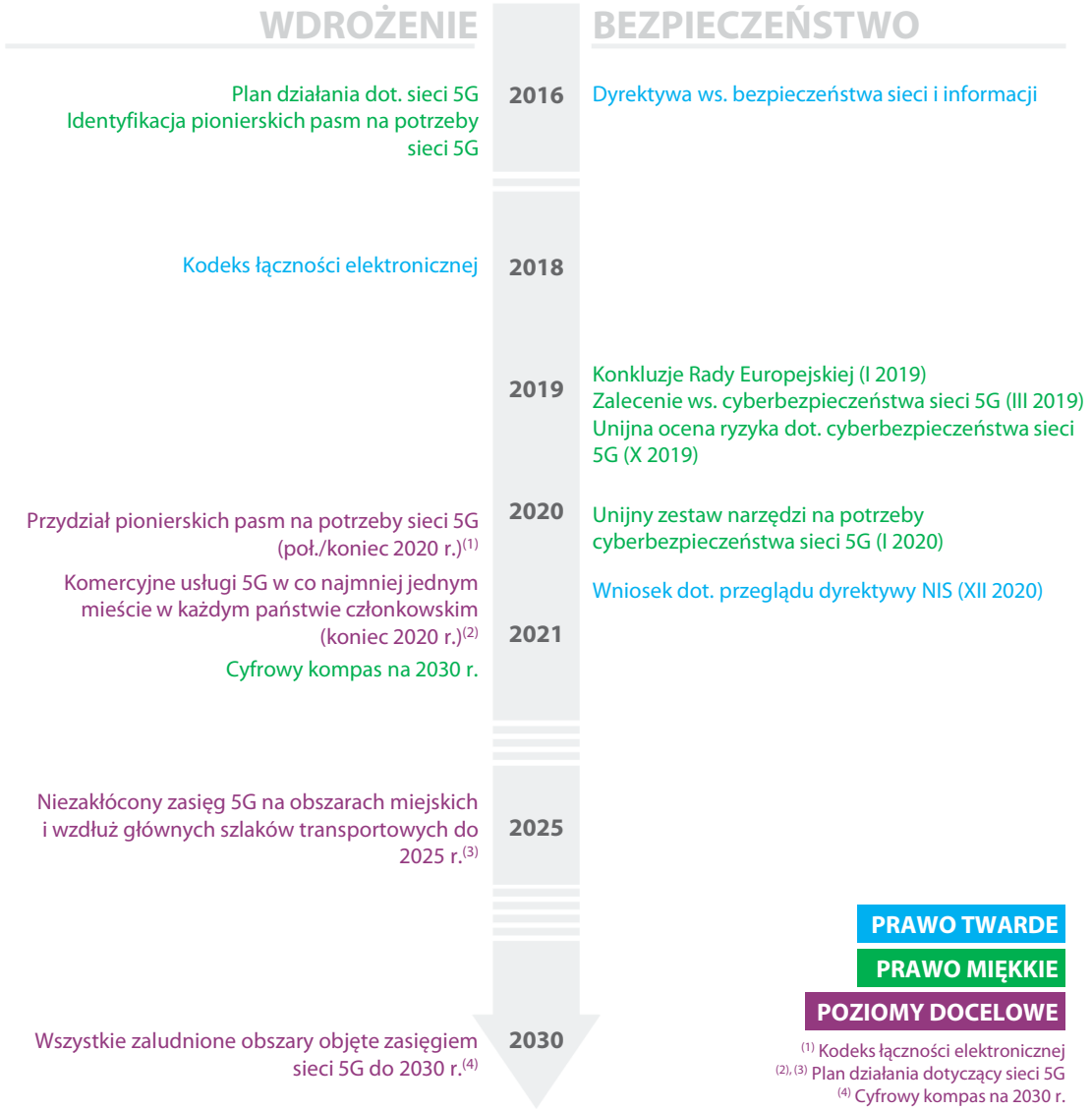
07 Potencjalnie zagrożone są również poufność i prywatność, ponieważ operatorzy telekomunikacyjni często przekazują dane do centrów danych. Istnieje zatem ryzyko, że takie dane będą przechowywane na urządzeniach dostawców technologii 5G, znajdujących się w krajach nienależących do UE, w których poziom ochrony prawnej i ochrony danych jest inny niż w UE.

Inicjatywy dotyczące sieci 5G podjęte na szczeblu UE

08 Na ramy polityczne dotyczące sieci 5G i jej bezpieczeństwa składa się zarówno „prawo twarde", które jest wiążące i możliwe do wyegzekwowania (np. rozporządzenia), jak i niewiążące „prawo miękkie" (np. komunikaty Komisji). W ***załączniku III*** przedstawiono odnośne ramy prawne i ramy polityki. Na ***rys. 2*** wskazano z kolei najważniejsze dokumenty programowe wraz z kluczowymi celami.

[11] Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r.; ustawa w sprawie wywiadu krajowego Chińskiej Republiki Ludowej, art. 14. Zob. również tłumaczenie na stronie https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Rys. 2 – Główne dokumenty programowe i kluczowe cele związane z wdrożeniem i bezpieczeństwem sieci 5G



Źródło: Europejski Trybunał Obrachunkowy.

Zadania i obowiązki

09 Chociaż operatorzy sieci ruchomej są odpowiedzialni za bezpieczne wprowadzenie sieci 5G przy użyciu sprzętu pochodzącego od dostawców technologii, a państwa członkowskie odpowiadają za bezpieczeństwo narodowe, bezpieczeństwo sieci 5G jest kwestią o znaczeniu strategicznym dla całego jednolitego rynku i dla suwerenności technologicznej UE[12]. W związku z tym w przypadku aspektów

[12] https://ec.europa.eu/commission/presscorner/detail/pl/IP_20_12

technicznych i aspektów związanych z bezpieczeństwem sieci 5G Komisja i agencje UE wspierają i koordynują działania państw członkowskich.

10 W *tabeli 1* przedstawiono dalsze wyjaśnienia dotyczące najważniejszych zadań i obowiązków w odniesieniu do sieci 5G.

Tabela 1 – Zadania i obowiązki

	Komisja i agencje UE	Organy państw członkowskich	Operatorzy sieci ruchomej i dostawcy technologii 5G
Przydział pionierskich pasm dla sieci 5G		✓	
Określenie unijnej polityki w zakresie sieci 5G	✓	✓	
Wdrażanie sieci 5G			✓
Inwestycje i finansowanie	✓	✓	✓
Bezpieczeństwo narodowe		✓	
Bezpieczeństwo sieci 5G		✓	✓
Wsparcie i koordynacja działań państw członkowskich	✓		

Źródło: Europejski Trybunał Obrachunkowy.

Koszt wdrożenia sieci 5G i powiązane wsparcie finansowe UE

Całkowity koszt wdrożenia sieci 5G we wszystkich państwach członkowskich może wynieść nawet 400 mld euro

11 W 2021 r. całkowity koszt wdrożenia sieci 5G we wszystkich państwach członkowskich do 2025 r. oszacowano na 281 do 391 mld euro, przy czym kwota ta rozkłada się po równo na budowę nowej infrastruktury 5G i modernizację istniejącej infrastruktury stacjonarnej, tak by mogła ona obsługiwać prędkości gigabitowe[13]. Większa część tych inwestycji musi zostać sfinansowana przez operatorów sieci ruchomej.

[13] Szacunki opracowane przez Komisję na podstawie danych EBI, Analysys i GSMA, zapowiedzi przedsiębiorstw oraz raportu ETNO – European Telecommunications, „Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All", marzec 2021 r.

W latach 2014–2020 UE wsparła rozwój sieci 5G kwotą ponad 4 mld euro

12 W latach 2014–2020 UE wsparła rozwój sieci 5G kwotą ponad 4 mld euro, zarówno bezpośrednio z budżetu UE, jak i poprzez finansowanie z Europejskiego Banku Inwestycyjnego (EBI). Z budżetu UE finansowano projekty związane wyłącznie z działalnością badawczą, natomiast ze środków EBI wspierano zarówno badania, jak i wdrażanie.

13 EBI zapewnia największe finansowanie ze środków UE na projekty związane z siecią 5G. Do sierpnia 2021 r. udzielił on kredytów na łączną kwotę 2,5 mld euro na rzecz dziewięciu projektów 5G w pięciu państwach członkowskich[14]. Ponadto w okresie 2014–2020 z budżetu UE udostępniono około 1,9 mld euro. ***Tabela 2*** zawiera zestawienie najważniejszych źródeł unijnego wsparcia finansowego na rzecz sieci 5G.

Tabela 2 – Finansowanie sieci 5G ze środków UE (2014–2020)

Finansowanie z UE	Kwota
EBI	2,485 mld EUR[1]
Europejski Fundusz na rzecz Inwestycji Strategicznych (EFIS)	1 mld EUR[2]
„Horyzont 2020”	755 mln EUR [3]
EFRR	Co najmniej 147 mln EUR[4]

1) Wykaz projektów EBI.
2) Wykaz projektów EFIS.
3) Tablica wskaźników programu „Horyzont 2020”.
4) „Dataset of projects co-funded by the ERDF during the multi-annual financial framework 2014-2020”.

Źródło: Europejski Trybunał Obrachunkowy.

14 W ramach EFIS (obsługiwanego przez EBI) udzielono wsparcia na rzecz dwóch projektów mających na celu gęstsze rozmieszczenie nadajników i wspieranie standaryzacji. Całkowity koszt inwestycji w ramach tych projektów wyniósł 3,9 mld euro, w tym 1 mld euro finansowania z EFIS (zob. ***załącznik IV***).

15 Od 2014 r. Komisja współfinansowała również bezpośrednio ponad 100 projektów dotyczących sieci 5G ze środków z programu „Horyzont 2020” oraz w mniejszym stopniu z EFRR. W ***załączniku V*** przedstawiono przykłady takich projektów.

[14] Wykaz projektów EBI.

Instrument na rzecz Odbudowy i Zwiększania Odporności zapewni dodatkowe środki unijne na wdrażanie sieci 5G w nadchodzących latach

16 Instrument na rzecz Odbudowy i Zwiększania Odporności (RRF) będzie stanowił dodatkowe źródło środków finansowych na wdrażanie sieci 5G w nadchodzących latach. Według stanu na wrzesień 2021 r. 16 państw członkowskich planowało finansować wdrażanie sieci 5G za pośrednictwem RRF, a 10 państw podjęło decyzję o niekorzystaniu z tych środków na ten cel. Jeśli chodzi o jedno pozostałe państwo członkowskie, brak było jak dotąd odnośnych informacji.

Zakres kontroli i podejście kontrolne

17 W ramach niniejszej kontroli Trybunał ocenił, czy Komisja skutecznie wspiera państwa członkowskie w:

- dążeniach do osiągnięcia unijnych celów na lata 2025 i 2030 w zakresie wdrożenia i rozpowszechnienia sieci 5G w państwach członkowskich,
- skoordynowanym rozwiązywaniu problemów związanych z bezpieczeństwem sieci 5G.

W przypadku obu tych kwestii Trybunał przeanalizował również środki i działania podejmowane przez państwa członkowskie.

18 Poprzez „bezpieczeństwo sieci 5G" Trybunał rozumie cyberbezpieczeństwo i bezpieczeństwo sprzętu/oprogramowania. Trybunał przeanalizował zarówno bezpieczeństwo, jak i wdrażanie sieci 5G, w przypadku których rok 2020 był kluczowy (zob. ***rys. 2***). Celem niniejszego sprawozdania jest przedstawienie spostrzeżeń i zaleceń, które przyczynią się do terminowego wdrożenia bezpiecznych sieci 5G w UE.

19 Przeprowadzona przez Trybunał kontrola obejmuje okres od 2016 r. do maja 2021 r. W miarę możliwości uwzględniono również bardziej aktualne informacje. W ramach prac kontrolnych Trybunał:

- dokonał przeglądu prawodawstwa UE, inicjatyw Komisji i innych istotnych dokumentów;
- przeprowadził wywiady z przedstawicielami Komisji, EBI, Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC), Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), stowarzyszeń telekomunikacyjnych, operatorów sieci ruchomej, dostawców technologii 5G i organizacji międzynarodowych oraz z ekspertami w tej dziedzinie, aby zebrać stosowne informacje, a także wywiady z przedstawicielami organów władz w Finlandii, Hiszpanii, Niemczech i Polsce. Te państwa członkowskie zostały wybrane na podstawie kryteriów takich jak wysokość środków unijnych przeznaczonych na projekty dotyczące sieci 5G i stan wdrożenia tych projektów, a także z uwzględnieniem równowagi geograficznej;
- przeprowadził ankietę wśród wszystkich 27 krajowych organów regulacyjnych ds. telekomunikacji w UE, aby uzyskać szerszy obraz sytuacji w zakresie wyzwań dotyczących sieci 5G w państwach członkowskich;

- dokonał przeglądu dziesięciu projektów współfinansowanych przez UE (EFIS, EFRR i „Horyzont 2020”) dotyczących sieci 5G, które zostały wybrane w celach poglądowych.

20 Trybunał wykorzystał również informacje z niedawno opublikowanego przez siebie przeglądu dotyczącego odpowiedzi UE na państwową strategię inwestycyjną Chin[15], jak również ustalenia z innych sprawozdań dotyczących na przykład łączności szerokopasmowej[16], inicjatywy w sprawie cyfryzacji europejskiego przemysłu[17] oraz polityki UE w zakresie cyberbezpieczeństwa[18].

[15] Przegląd nr 03/2020 pt. „Reakcja UE na państwową strategię inwestycyjną Chin”.

[16] Sprawozdanie specjalne nr 12/2018 pt. „Sieci szerokopasmowe w państwach członkowskich UE – pomimo poczynionych postępów nie wszystkie cele strategii »Europa 2020« zostaną osiągnięte”.

[17] Sprawozdanie specjalne nr 19/2020 pt. „Cyfryzacja europejskiego przemysłu – ambitna inicjatywa, której powodzenie zależy od trwałego zaangażowania ze strony UE, rządów i przedsiębiorstw”.

[18] Przegląd nr 02/2019 pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją (Dokument analityczny)”.

Uwagi

Opóźnienia we wdrażaniu sieci 5G zagrażają osiągnięciu celów UE na lata 2025 i 2030

21 W odniesieniu do terminowego wdrażania sieci 5G Trybunał zbadał, czy:

- państwa członkowskie są na dobrej drodze do wdrożenia sieci 5G;
- Komisja zapewniła państwom członkowskim odpowiednie wsparcie;
- państwa członkowskie wyeliminowały główne przeszkody utrudniające szybkie wprowadzenie sieci 5G.

Państwa członkowskie pozostają w tyle pod względem wdrażania sieci 5G

Komisja określiła terminy wdrożenia sieci 5G w swoim planie działania dotyczącym sieci 5G z 2016 r.

22 W swoim planie działania dotyczącym sieci 5G z 2016 r. Komisja zaproponowała terminy wdrożenia tych sieci w UE: państwa członkowskie zostały zobowiązane do tego, by uruchomić pierwsze sieci 5G do końca 2018 r. i w pełni komercyjne usługi 5G w co najmniej jednym dużym mieście do końca 2020 r. oraz by zapewnić niezakłócony zasięg 5G na obszarach miejskich i wzdłuż głównych szlaków transportowych do 2025 r.

23 W marcu 2021 r. Komisja wyznaczyła kolejny termin: objęcie zasięgiem sieci 5G wszystkich zaludnionych obszarów do 2030 r.[19]

23 państwa członkowskie uruchomiły komercyjne usługi 5G przed końcem 2020 r.

24 Do końca 2020 r. 23 państwa członkowskie osiągnęły cel polegający na zapewnieniu dostępu do usług 5G w co najmniej jednym dużym mieście. Jedynie Cypr, Litwa, Malta i Portugalia nie osiągnęły tego celu. Według stanu na koniec października

[19] Komisja Europejska, „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie”, COM(2021) 118 final.

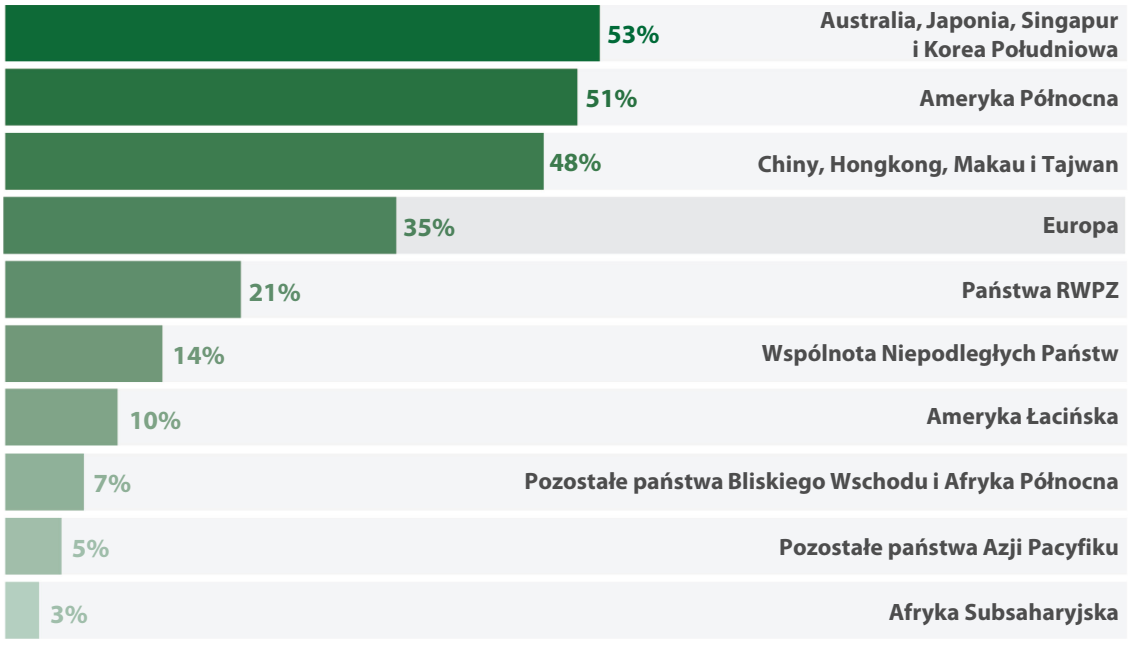
2021 r. tylko Litwa i Portugalia nie zapewniły jeszcze dostępu do usług 5G w żadnym ze swoich miast.

Istnieje ryzyko, że większość państw członkowskich nie dotrzyma terminów wyznaczonych na 2025 i 2030 r.

25 Jak wynika z niedawnego badania Komisji, jedynie 11 państw członkowskich będzie najprawdopodobniej w stanie zapewnić do 2025 r. niezakłócony zasięg 5G na wszystkich obszarach miejskich i wzdłuż głównych szlaków transportu naziemnego[20] W przypadku pozostałych 16 państw członkowskich Komisja uważa, że prawdopodobieństwo osiągnięcia tego celu jest średnie (Austria, Czechy, Estonia, Niemcy, Irlandia, Polska, Litwa i Słowenia) albo niskie (Belgia, Bułgaria, Chorwacja, Cypr i Grecja).

26 W 2021 r. organizacja branżowa Global System for Mobile Communications Association (GSMA) zauważyła, że wdrażanie sieci 5G w UE przebiega w innym tempie niż w innych częściach świata. Na przykład szacuje się, że do 2025 r. 51% wszystkich połączeń mobilnych w Ameryce Północnej będzie opierać się na technologii 5G, podczas gdy w Europie (w tym w krajach spoza UE) odsetek ten wyniesie jedynie 35% (zob. *rys. 3*).

Rys. 3 – Udział procentowy połączeń 5G w ogólnej liczbie połączeń komórkowych do 2025 r.



Źródło: GSMA, „The Mobile Economy 2021”.

[20] Badanie Komisji dotyczące krajowych planów szerokopasmowych w UE-27.

27 Przy obecnym tempie wdrażania istnieje duże ryzyko, że większość państw członkowskich nie dotrzyma terminu 2025 r., a zatem również terminu 2030 r. wyznaczonego na objęcie zasięgiem wszystkich zaludnionych obszarów. W tym kontekście Trybunał przeanalizował, czy Komisja skutecznie wspierała państwa członkowskie w realizacji unijnych celów 5G na lata 2025 i 2030 w zakresie wdrażania i rozpowszechniania sieci 5G.

We wsparciu zapewnianym przez Komisję państwom członkowskim wystąpiły pewne uchybienia

Komisja nie określiła oczekiwanej jakości usług w sieciach 5G

28 Jak dotąd Komisja nie określiła oczekiwanej jakości usług sieci 5G, na przykład pod względem minimalnej prędkości przesyłu danych czy maksymalnego poziomu opóźnień. Co więcej, w planie działania z 2016 r. państwa członkowskie zostały wprawdzie zobowiązane do uruchomienia „w pełni komercyjnych" usług 5G w Europie do końca 2020 r., ale nie zdefiniowano w nim tych pojęć pod względem jakościowym.

29 Ów brak jasności co do oczekiwanej jakości usług stwarza ryzyko, że pojęcia te będą różnie interpretowane przez państwa członkowskie. Trybunał odnotował przykłady rozbieżnych podejść w zakresie wdrażania sieci 5G w poszczególnych państwach członkowskich (zob. ***ramka 2***).

Ramka 2

Przykłady rozbieżnych podejść w zakresie wdrażania sieci 5G

Prędkość przesyłu danych i poziom opóźnień to dwa kluczowe aspekty decydujące o wydajności usług wykorzystujących 5G. Na przykład zdalna chirurgia lub automatyka przemysłowa 5G wymagają bardzo dużej prędkości przesyłu danych i niewielkich opóźnień. Jak dotąd jednak tylko dwa państwa członkowskie (Niemcy i Grecja) określiły minimalne wymogi dotyczące prędkości przesyłu danych i maksymalnych opóźnień[21].

Konieczność zapewnienia „do końca 2020 r. […] dostępu do usług 5G w co najmniej jednym dużym mieście" jest różnie interpretowana przez państwa członkowskie. Prowadzi to do sytuacji, w której miasto sklasyfikowane jako „posiadające dostęp do usług 5G" może oznaczać zaledwie kilka ulic objętych zasięgiem, jak w Luksemburgu, lub prawie cały jego obszar, jak w przypadku Helsinek. W ***załączniku VI*** przedstawiono przykłady zasięgu w wybranych miastach.

30 Jeśli sytuacja ta będzie się utrzymywać, może doprowadzić do nierówności w dostępie do usług 5G i ich jakości w UE (tzw. przepaść cyfrowa): mieszkańcy niektórych państw UE będą mieli większy dostęp do usług 5G o lepszej jakości niż inni. Przepaść cyfrowa może również niekorzystnie wpłynąć na potencjał rozwoju gospodarczego, ponieważ technologia 5G może zrewolucjonizować takie sektory jak opieka zdrowotna, edukacja i siła robocza, ale jedynie pod warunkiem, że sieci 5G będą się wykazywać wystarczającą przepustowością.

31 Jasne informacje co do oczekiwanej wydajności sieci 5G są również potrzebne w świetle inicjatywy Komisji mającej na celu wprowadzenie wymogu większej przejrzystości co do jakości usług świadczonych przez operatorów sieci ruchomej w roamingu, w związku z którą to inicjatywą Komisja przedstawiła niedawno wniosek ustawodawczy[22].

---

[21] Sprawozdanie kwartalne nr 12, Obserwatorium 5G, sytuacja do czerwca 2021 r.

[22] Komisja Europejska, Wniosek dotyczący rozporządzenia w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (wersja przekształcona), COM(2021) 85 final z 24.2.2021 r.

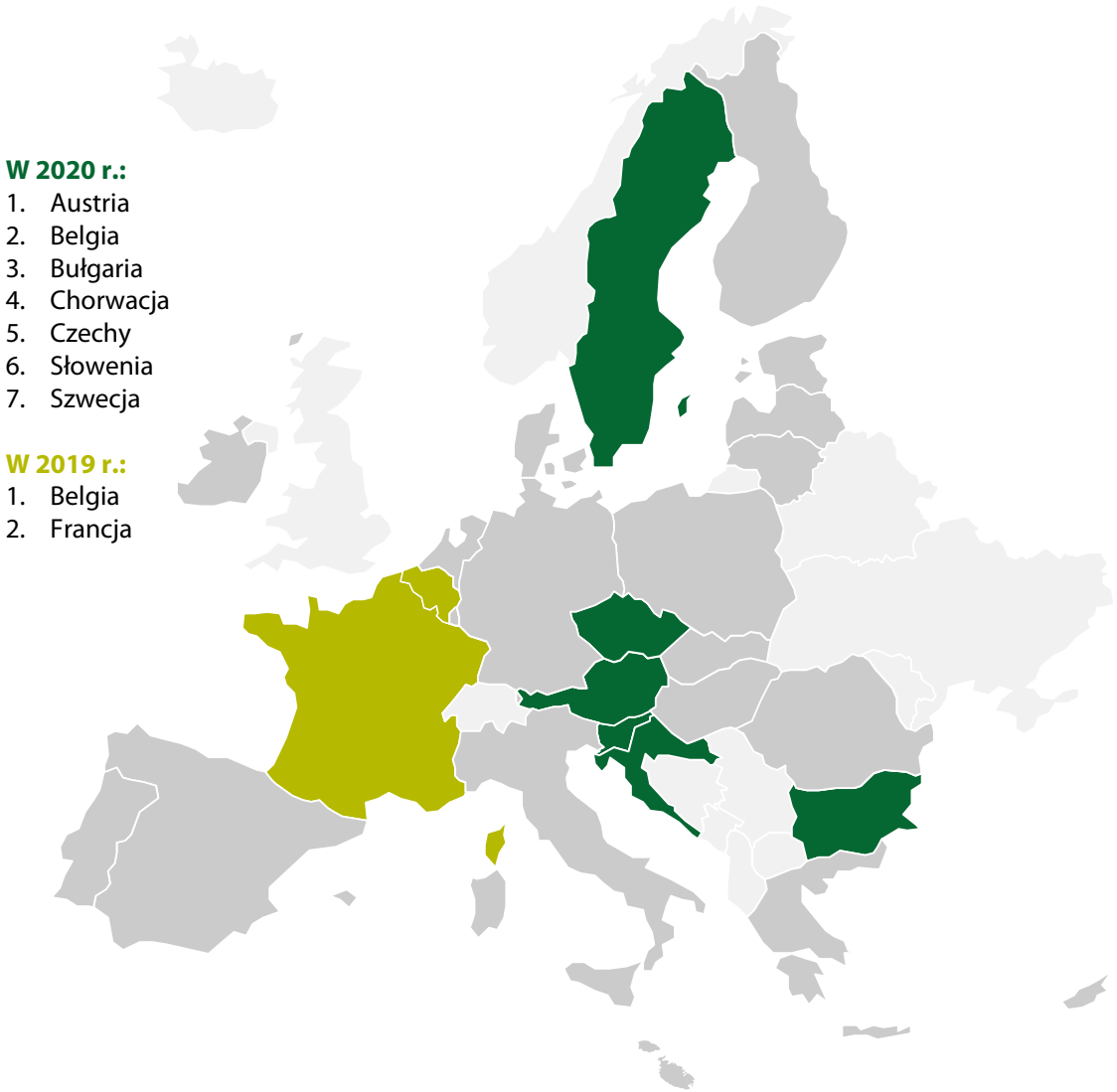
Kwartalne sprawozdania Komisji na temat wprowadzania sieci 5G nie zawsze są wiarygodne

32 Komisja monitoruje poziom wdrożenia sieci 5G w państwach członkowskich za pośrednictwem Obserwatorium 5G. Obserwatorium co kwartał przedstawia informacje na temat wdrażania sieci 5G oraz strategii państw członkowskich w tym zakresie. Trybunał ustalił jednak, że w przypadku dwóch z czterech krajów objętych przeglądem informacje zawarte w tych sprawozdaniach nie zawsze były wiarygodne. Na przykład w sprawozdaniu kwartalnym nr 10, w którym przedstawiono informacje do końca grudnia 2020 r., podano znacznie mniejszą liczbę gmin w Finlandii posiadających 5G niż liczba rzeczywista (40 zamiast 70) i nie podano informacji o tym, że aukcje częstotliwości 5G w Polsce zostały odroczone (zob. pkt ***42***).

Komisja dopiero niedawno zaczęła korzystać z procesu europejskiego semestru do monitorowania postępów państw członkowskich we wdrażaniu sieci 5G

33 Trybunał ustalił, że w ciągu ostatnich dwóch lat Komisja w większym stopniu wykorzystywała proces europejskiego semestru, aby zachęcać państwa członkowskie do postępów we wdrażaniu sieci 5G. Liczba zaleceń dla poszczególnych państw o bezpośrednim znaczeniu pod względem wdrażania sieci 5G wzrosła: w 2019 r. takie zalecenia skierowano do dwóch państw członkowskich, a w 2020 r. do siedmiu (zob. *rys. 4*).

Rys. 4 – Zalecenia dla poszczególnych krajów dotyczące 5G



Źródło: Europejski Trybunał Obrachunkowy na podstawie zaleceń dla poszczególnych krajów.

Państwa członkowskie wciąż muszą wyeliminować najważniejsze przeszkody na drodze do szybkiego wprowadzenia sieci 5G

34 Aby osiągnąć cele UE w zakresie wdrożenia sieci 5G na lata 2025 i 2030, państwa członkowskie muszą wprowadzić trzy główne elementy: strategiczny – poprzez zapewnienie, by cele te zostały uwzględnione w krajowych strategiach 5G lub krajowych planach szerokopasmowych[23]; legislacyjny – poprzez transpozycję Europejskiego kodeksu łączności elektronicznej z 2018 r.[24]; biznesowy – poprzez przydzielenie częstotliwości[25]. W ***tabeli 3*** przedstawiono przegląd postępów państw członkowskich we wprowadzaniu tych trzech elementów.

[23] Badanie Komisji dotyczące krajowych planów szerokopasmowych w UE-27.

[24] Dyrektywa (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej.

[25] Komunikat Komisji Europejskiej „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi”, COM(2020) 50 final.

Tabela 3 – Postępy we wprowadzaniu głównych elementów sprzyjających osiągnięciu celów na 2025 r.

Państwo członkowskie	Krajowy plan szerokopasmowy zgodny z celami na 2025 r.	Transpozycja Europejskiego kodeksu łączności elektronicznej	Pionierskie pasma na potrzeby sieci 5G (sierpień 2021 r.)			Prawdopodobieństwo osiągnięcia celu
			700 MHz	3,6 GHz	26 GHz	
Belgia				Tymczasowe korzystanie		niskie
Bułgaria		✓		✓		niskie
Czechy	✓	✓	✓	✓		średnie
Dania		✓	✓	✓	✓	wysokie
Niemcy	✓	✓	✓	✓	✓	średnie
Estonia						średnie
Irlandia				✓		średnie
Grecja	✓	✓	✓	✓	✓	niskie
Hiszpania	✓		✓	✓		wysokie
Francja	✓	✓	✓	✓		wysokie
Chorwacja			✓	✓	✓	niskie
Włochy			✓	✓	✓	wysokie
Cypr	✓		✓	✓		niskie
Litwa	✓					średnie
Łotwa				✓		wysokie
Luksemburg			✓	✓		wysokie
Węgry	✓	✓	✓	✓		wysokie
Malta		✓				średnie
Niderlandy	✓		✓			średnie
Austria	✓	✓	✓	✓		średnie
Polska	✓					średnie
Portugalia				Tymczasowe korzystanie		średnie-wysokie
Rumunia						wysokie
Słowenia	✓		✓	✓	✓	średnie
Słowacja			✓			wysokie
Finlandia	✓	✓	✓	✓	✓	wysokie
Szwecja	✓		✓	✓		wysokie

Źródło: Badanie Komisji dotyczące krajowych planów szerokopasmowych w UE-27, Obserwatorium 5G i Zespół ds. Polityki Spektrum Radiowego.

W swoich strategiach dotyczących sieci 5G niewielka liczba państw członkowskich uwzględniła cele dotyczące wdrożenia na lata 2025 i 2030

35 Państwa członkowskie wyznaczają swoją politykę w zakresie 5G za pomocą specjalnych krajowych strategii 5G lub poprzez aktualizację istniejących krajowych planów szerokopasmowych. W badaniu Komisji z 2021 r. dotyczącym krajowych planów szerokopasmowych[26] zauważono, że tylko 14 państw członkowskich uwzględniło w swojej strategii 5G lub w zaktualizowanej wersji planu szerokopasmowego unijny cel polegający na „zapewnieniu niezakłóconego zasięgu 5G na wszystkich obszarach miejskich i głównych szlakach transportu naziemnego do 2025 r." (zob. ***tabela 3***). Tymczasem uwzględnienie tego celu ma kluczowe znaczenie dla pomyślnej realizacji polityki.

Większość państw członkowskich nie dokonała do końca 2020 r. transpozycji dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej

36 Dyrektywa ustanawiająca Europejski kodeks łączności elektronicznej – w której określono zadania krajowych organów regulacyjnych i innych właściwych podmiotów oraz wyznaczono terminy przyznawania pionierskich pasm na potrzeby sieci 5G – miała zostać transponowana przez państwa członkowskie do 21 grudnia 2020 r. Do końca lutego 2021 r. tylko trzy państwa członkowskie (Finlandia, Grecja i Węgry) zadeklarowały, że przyjęły wszystkie środki niezbędne do transpozycji dyrektywy. W związku z tym Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko pozostałym 24 państwom członkowskim[27].

37 Według stanu na koniec listopada 2021 r. 23 postępowania są wciąż w toku. O ile w przypadku sześciu państw członkowskich (Austria, Bułgaria, Czechy, Francja, Malta i Niemcy) Komisja spodziewa się rychłego zakończenia postępowań, o tyle w przypadku pozostałych 17 państw może ona podjąć decyzję o skierowaniu sprawy do Trybunału Sprawiedliwości[28] (zob. ***tabela 3***).

Przydział pionierskich pasm 5G jest opóźniony

38 W 2016 r. Komisja i państwa członkowskie wskazały trzy pionierskie pasma, które mają być wykorzystywane na potrzeby usług 5G:

---

[26] Badanie Komisji dotyczące krajowych planów szerokopasmowych w UE-27.

[27] Komunikat prasowy Komisji IP/21/2016 z 4 lutego 2021 r.

[28] Komunikat prasowy Komisji IP/21/4612 z 23 września 2021 r.

- pasmo częstotliwości 700 MHz, które ułatwia przenikanie sygnałów bezprzewodowych do budynków i pozwala operatorom na zapewnienie większego zasięgu (setki kilometrów kwadratowych). Niemniej prędkość przesyłu danych i poziom opóźnień w sieci 5G są wyższe tylko o jeden poziom od 4G (150 do 250 megabitów na sekundę);

- pasmo średnich częstotliwości 3,6 GHz, które umożliwia przesyłanie dużych ilości danych (do 900 megabitów na sekundę) na znaczne odległości (promień kilku kilometrów);

- pasmo wysokich częstotliwości 26 GHz, które umożliwia wysokie prędkości przesyłu danych od 1 do 3 gigabitów na sekundę na krótkich dystansach (tj. poniżej 2 km), ale przy większej wrażliwości na zakłócenia.

39 Państwa członkowskie miały udostępnić zakres niskich częstotliwości do użytkowania najpóźniej do 30 czerwca 2020 r.[29], a zakres średnich i wysokich częstotliwości do 31 grudnia 2020 r.[30] Do końca 2020 r. państwa członkowskie przydzieliły jednak mniej niż 40% wszystkich dostępnych pionierskich pasm częstotliwości (zob. ***tabela 4***):

- pasmo 700 MHz zostało przydzielone w 13 państwach członkowskich;

- pasmo 3,6 GHz zostało przydzielone w 17 państwach członkowskich (w tym w dwóch państwach członkowskich, które zezwoliły na jego tymczasowe użytkowanie);

- pasmo 26 GHz zostało przydzielone w czterech państwach członkowskich.

Do końca października 2021 r. odsetek przydzielonych pasm wzrósł do 53%[31].

[29] Decyzja (UE) 2017/899 w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz.

[30] Dyrektywa (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej.

[31] Obserwatorium 5G i Zespół ds. Polityki Spektrum Radiowego.

Tabela 4 – Przydział pionierskich pasm na potrzeby sieci 5G: sytuacja na grudzień 2020 r.

Państwo członkowskie	700 MHZ	3,6 GHZ	26 GHZ
Belgia		Tymczasowe korzystanie	
Bułgaria			
Czechy	✓	✓	
Dania	✓	✓	✓
Niemcy	✓	✓	✓
Estonia		-	
Irlandia		✓	
Grecja	✓	✓	✓
Hiszpania		✓	
Francja	✓	✓	
Chorwacja			
Włochy		✓	✓
Cypr	✓	✓	
Łotwa		✓	
Litwa			
Luksemburg	✓	✓	
Węgry	✓	✓	
Malta			
Niderlandy	✓		
Austria	✓	✓	
Polska			
Portugalia		Tymczasowe korzystanie	
Rumunia			
Słowenia			
Słowacja	✓	✓	
Finlandia	✓	✓	✓
Szwecja	✓	✓	

Źródło: Obserwatorium 5G i Zespół ds. Polityki Spektrum Radiowego.

Opóźnienia w przydzielaniu pionierskich pasm wynikają z rozmaitych przyczyn

40 Trybunał ustalił, że opóźnienia w przydzielaniu pasma 26 GHz wynikają głównie ze słabego popytu ze strony operatorów sieci ruchomej. Na przykład w Hiszpanii do wykorzystania na potrzeby sieci 5G dostępne jest łącznie 1,5 GHz z pasma 26 GHz. Jak wynika z konsultacji publicznych zakończonych w lipcu 2019 r., pasmo to nie zostało jednak jeszcze przydzielone operatorom, ponieważ nie ma na nie popytu. Do końca 2021 r. planuje się przeprowadzenie kolejnych konsultacji publicznych, a w drugim

kwartale 2022 r. sprzedaż tego pasma w drodze aukcji. Również operatorzy sieci ruchomej w Finlandii poinformowali, że nie ma jeszcze większego zainteresowania ani uzasadnienia biznesowego dla pasma 26 GHz.

41 Do opóźnień w przyznawaniu częstotliwości 5G przyczyniają się ponadto problemy z transgraniczną koordynacją działań z państwami spoza UE położonymi wzdłuż wschodniej granicy (Białoruś, Rosja i Ukraina). Te kraje, na mocy obowiązujących umów międzynarodowych, wykorzystują pasmo 700 MHz do transmisji telewizyjnych oraz pasmo 3,6 GHz na potrzeby wojskowej łączności satelitarnej. Ów problem dotyczy głównie krajów bałtyckich (Estonii, Łotwy i Litwy) oraz Polski. Z informacji udzielonych przez Komisję wynika, że osiągnięto pewne postępy w rozmowach z Ukrainą i Białorusią, które powinny uwolnić pasmo 700 MHz do końca 2022 r. Rozmowy dwustronne z Rosją nie posunęły się natomiast jeszcze do przodu. W związku z tym Estonia i Polska wystąpiły o odroczenie terminów na przydział pasma 700 MHz do połowy 2022 r.

42 Ponadto w Polsce i Hiszpanii aukcje częstotliwości na potrzeby sieci 5G przełożono na późniejszy termin podczas pandemii COVID-19 (zob. ***ramka 3***).

Ramka 3

Przykłady spowodowanych przez pandemię COVID-19 opóźnień w przydzielaniu częstotliwości 5G

- W marcu 2020 r. Polska ogłosiła aukcję na pasmo 3,6 GHz, które miało zostać przydzielone do 30 czerwca 2020 r. Po wybuchu pandemii władze polskie podjęły decyzję o zawieszeniu wszystkich postępowań administracyjnych na czas jej trwania. Według stanu na wrzesień 2021 r. procedura przydziału tego pasma w drodze aukcji nadal nie została zakończona.
- W Hiszpanii aukcję na pasmo 700 MHz planowano początkowo na marzec 2020 r. Według władz hiszpańskich pandemia COVID-19 opóźniła jednak uwolnienie tego pasma, które jest wykorzystywane na potrzeby telewizji cyfrowej. W związku z tym aukcja została odroczona do maja 2020 r., a następnie przesunięta na pierwszy kwartał 2021 r. Po zmianie hiszpańskiego ustawodawstwa w kwietniu 2021 r. w celu dostosowania okresu obowiązywania licencji do Europejskiego kodeksu łączności elektronicznej aukcję przesunięto na lato 2021 r., a pasmo 700 MHz zostało ostatecznie przydzielone w lipcu 2021 r.

43 Kolejnym czynnikiem, który spowodował opóźnienia w przydziale pionierskich pasm 5G, jest różne podejście państw członkowskich do kwestii bezpieczeństwa sieci 5G oraz opóźnienia w przyjmowaniu przepisów dotyczących tej kwestii, co powoduje niepewność biznesową (zob. pkt ***74*** i ***75***):

- W Hiszpanii regulamin aukcji na pasmo pionierskie zawierał ogólną klauzulę, zgodnie z którą posiadacze koncesji publicznych muszą przestrzegać wszystkich obowiązków w zakresie bezpieczeństwa sieci 5G ustanowionych w dowolnym momencie w przyszłości w przepisach europejskich lub krajowych. Hiszpański operator sieci ruchomej, z którym kontrolerzy przeprowadzili wywiad, zauważył, że w wyniku tej klauzuli musi podejmować decyzje dotyczące strategii i zakupów w warunkach niepewności. Zwrócił również uwagę, że władze krajowe nie były skłonne doprecyzować niektórych kluczowych warunków, takich jak możliwość uzyskania rekompensaty, jeżeli przyszłe przepisy, których przyjęcie planuje się do końca 2022 r., wymagałyby od operatorów wymiany sprzętu.

- W Polsce jednym ze wskazanych powodów odroczenia przydziału częstotliwości 5G była konieczność oczekiwania na przepisy precyzujące wymogi niezbędne dla bezpieczeństwa sieci 5G.

Konieczne są dalsze wysiłki, by wyeliminować problemy dotyczące bezpieczeństwa sieci 5G na etapie ich wdrażania

44 W odniesieniu do aspektów dotyczących bezpieczeństwa sieci 5G Trybunał zbadał, czy:

- Komisja podjęła niezbędne kroki w celu promowania solidnej koncepcji ram bezpieczeństwa i zapewniła odpowiednie wsparcie państwom członkowskim;

- państwa członkowskie w skoordynowany sposób wdrażają bezpieczne sieci 5G, przyjmując środki łagodzące przewidziane w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G i aktualizując swoje prawodawstwo.

Komisja zareagowała szybko, gdy bezpieczeństwo sieci 5G stało się źródłem poważnych obaw na szczeblu UE

45 W planie działania dotyczącym sieci 5G z 2016 r. nie uwzględniono żadnych kwestii związanych z bezpieczeństwem. Bezpieczeństwo sieci 5G i nadmierne poleganie na dostawcach z państw trzecich, w szczególności z Chin, uznano za kwestie o krytycznym znaczeniu w marcu 2019 r. Parlament Europejski w swojej rezolucji

z 12 marca 2019 r.[32] wyraził obawy dotyczące dostawców 5G spoza UE, którzy mogą stanowić zagrożenie dla bezpieczeństwa UE ze względu na przepisy obowiązujące w ich krajach pochodzenia. Tego samego dnia Komisja w swojej perspektywie strategicznej dotyczącej stosunków UE-Chiny podkreśliła, że potrzebne jest wspólne unijne podejście do kwestii bezpieczeństwa sieci 5G, tak aby zabezpieczyć się przed potencjalnie poważnymi skutkami dla bezpieczeństwa krytycznej infrastruktury cyfrowej[33]. Rada Europejska w swoich konkluzjach z 21 i 22 marca 2019 r. zwróciła się do Komisji o wydanie zalecenia w sprawie wspólnego podejścia do kwestii bezpieczeństwa sieci 5G[34].

46 Kilka dni później Komisja wydała zalecenie przewidujące zestaw środków zarówno na szczeblu krajowym (np. ocena ryzyka w odniesieniu do sieci 5G), jak i unijnym (np. skoordynowana ocena ryzyka), mających na celu zapewnienie wysokiego poziomu cyberbezpieczeństwa sieci 5G w całej UE[35].

47 Prawie wszystkie państwa członkowskie zakończyły swoje krajowe oceny ryzyka w terminie do lipca 2019 r.[36] W październiku 2019 r. grupa współpracy ds. bezpieczeństwa sieci i informacji wydała sprawozdanie dotyczące skoordynowanej na szczeblu unijnym oceny ryzyka w zakresie cyberbezpieczeństwa sieci 5G, a w styczniu 2020 r. unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G[37] (zob. ***załącznik VII***). Zestaw narzędzi został następnie szybko zatwierdzony przez Komisję i Radę Europejską[38].

---

[32] Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. (2019/2575(RSP)).

[33] JOIN(2019) 5 final z 12.3.2019 r. UE-Chiny – perspektywa strategiczna.

[34] Konkluzje Rady Europejskiej z dnia 21 i 22 marca 2019 r.

[35] Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G.

[36] Komunikat prasowy z dnia 19 lipca 2019 r.

[37] „Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures", Grupa współpracy ds. bezpieczeństwa sieci i informacji, 01/2020.

[38] Komunikat Komisji Europejskiej „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi", COM(2020) 50 final; konkluzje Rady Europejskiej z dnia 1 i 2 października 2020 r. (EUCO 13/20).

W unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G z 2020 r. po raz pierwszy określono środki służące przeciwdziałaniu zagrożeniom dla bezpieczeństwa na szczeblu UE, przy czym nie nadano im charakteru normatywnego

Podejście do bezpieczeństwa sieci 5G jako do kwestii bezpieczeństwa narodowego ogranicza możliwości podejmowania działań przez Komisję

48 W traktatach UE[39] określono zakres działań mających na celu sprostanie wyzwaniom takim jak wdrażanie bezpiecznych sieci 5G na szczeblu unijnym. Zakres ten jest jednak szeroki i pozostawia Komisji i państwom członkowskim pole do interpretacji (zob. ***ramka 4***).

Ramka 4

Kompetencje UE w odniesieniu do sieci 5G: kompetencje dzielone czy kwestia bezpieczeństwa narodowego?

Sieci 5G wchodzą zasadniczo w zakres kompetencji UE w obszarze jednolitego rynku (kompetencje dzielone), zarówno jako usługa (świadczenie usług przez operatorów sieci ruchomej), jak i towar (sprzęt 5G zakupiony przez operatorów sieci ruchomej w celu stworzenia sieci 5G). W ramach kompetencji dzielonych UE (Komisja i inne instytucje UE) może przyjmować środki prawnie wiążące (przepisy), aby zapewnić ustanowienie jednolitego rynku i wspierać jego należyte funkcjonowanie. Bezpieczeństwo sieci 5G można też postrzegać szerzej, jako kwestię związaną z unijną przestrzenią wolności, bezpieczeństwa i sprawiedliwości. W tym sensie bezpieczeństwo można rozumieć jako ogólne pojęcie związane z zapobieganiem i zwalczaniem przestępczości, co oznaczałoby, że wchodzi ono w zakres kompetencji dzielonych, w przypadku których UE również może przyjmować prawnie wiążące środki.

Węższa interpretacja bezpieczeństwa polegałaby natomiast na postrzeganiu go wyłącznie przez pryzmat zagrożeń dla bezpieczeństwa narodowego państw członkowskich. Jako że w takiej sytuacji wchodziłoby ono w zakres wyłącznych kompetencji krajowych, możliwości podejmowania działań przez UE ograniczałyby się do działań wspierających wysiłki państw członkowskich na rzecz zapewnienia bezpieczeństwa ich sieci 5G.

[39] Traktat o funkcjonowaniu Unii Europejskiej.

49 Kwestia bezpieczeństwa sieci 5G ma charakter przekrojowy: wchodzi w zakres kompetencji krajowych i unijnych oraz jest istotna w kontekście bezpieczeństwa narodowego. W ramach swojego podejścia Komisja postrzega ją z perspektywy zagrożeń dla bezpieczeństwa narodowego i w związku z tym zdecydowała się polegać na środkach „prawa miękkiego". Oznacza to, że UE nie może przyjmować prawnie wiążących środków, które nakładałyby na państwa członkowskie obowiązek stosowania jednolitych środków zmniejszających ryzyko lub wdrożenia wymogów możliwych do wyegzekwowania na drodze prawnej. Komisja może wydawać jedynie niewiążące zalecenia i komunikaty, pomagać w rozpowszechnianiu najlepszych praktyk i koordynować działania państw członkowskich na szczeblu krajowym. Możliwe byłoby też jednak inne podejście. Za przykład może posłużyć dyrektywa NIS[40], akt prawny UE dotyczący bezpieczeństwa sieci i systemów informatycznych w całej Unii. Została ona zaproponowana przez Komisję i przyjęta w ramach podstawy prawnej „jednolitego rynku", mimo iż cyberbezpieczeństwo to kwestia należąca w dużej mierze do kompetencji państw członkowskich[41].

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G został przyjęty na wczesnym etapie wdrażania, lecz mimo to niektórzy operatorzy sieci ruchomej zdążyli już wcześniej dokonać wyboru dostawców

50 W styczniu 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji przyjęła unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, w którym określono szereg środków strategicznych i technicznych oraz działań wspierających służących przeciwdziałaniu zagrożeniom dla bezpieczeństwa sieci 5G, a także wskazano podmioty właściwe dla każdego z tych środków i działań. Ten zestaw narzędzi, zatwierdzony przez Komisję i Radę Europejską, przyjęto zaledwie dziewięć miesięcy po tym, jak Parlament Europejski i Rada po raz pierwszy wyraziły obawy dotyczące bezpieczeństwa sieci 5G. W ostatnim czasie ów unijny zestaw narzędzi został wspomniany w nowej europejskiej strategii na rzecz wsparcia inteligentnych, ekologicznych i bezpiecznych powiązań w systemach cyfrowych na całym świecie, w której został on uznany za narzędzie służące do ukierunkowania inwestycji w infrastrukturę cyfrową[42].

---

[40] Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[41] Przegląd nr 02/2019 pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją (Dokument analityczny)", pkt 36.

[42] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego, Komitetu Regionów i Europejskiego Banku Inwestycyjnego „Brama na świat", JOIN(2021) 30 final z 1.12.2021 r.

Zastosowane przez Komisję podejście oparte na prawie miękkim przyczyniło się do szybkiego wdrożenia środków w celu radzenia sobie z zagrożeniami dla bezpieczeństwa również na poziomie UE oraz ułatwienia współpracy państw członkowskich w tej transgranicznej kwestii. Dla porównania w przypadku dyrektywy NIS upłynęły ponad trzy lata od wniosku Komisji[43] do jej przyjęcia[44], a w przypadku dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej – ponad dwa lata[45]. Jeszcze więcej czasu potrzeba było na transpozycję dyrektyw do krajowych systemów prawnych państw członkowskich (zob. również pkt ***36*** i ***37***).

51 Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G przyjęto cztery lata po przedstawieniu polityki w zakresie 5G w planie działania dotyczącym sieci 5G i w tym samym roku, w którym miały zostać osiągnięte cele pośrednie w zakresie wdrażania określone w tym planie działania. W tym kontekście przedstawiciele ministerstw państw członkowskich i krajowych organów regulacyjnych oraz operatorzy sieci ruchomej, z którymi przeprowadzono wywiady na potrzeby niniejszej kontroli, uznali, że działania dotyczące bezpieczeństwa sieci 5G rozpoczęto zbyt późno.

52 Z drugiej strony zestaw narzędzi został opublikowany w momencie, gdy wdrażanie sieci 5G i odnośnych planów w większości państw członkowskich wciąż znajdowało się na wczesnym etapie. Większość umów na sprzęt 5G pomiędzy dostawcami i operatorami została zawarta w 2020 i 2021 r. Jak jednak wynika z informacji udzielonych przez Stowarzyszenie Europejskich Operatorów Sieci Telekomunikacyjnych (ETNO), część operatorów sieci ruchomej dokonała wyboru dostawców, zanim udostępniony został unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G.

---

[43] COM(2013) 48 final z 7.2.2013 r.

[44] Dyrektywa (UE) 2016/1148.

[45] COM(2016) 590 final/2 z 12.10.2016 r. i dyrektywa (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej.

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G zapewnił ramy na potrzeby oceny profilu ryzyka poszczególnych dostawców, lecz nie wyeliminowano wszystkich niedociągnięć

W opinii niektórych państw członkowskich i organów krajowych część kryteriów wykorzystywanych w celu zaklasyfikowania dostawców jako obarczonych wysokim ryzykiem nie jest wystarczająco jasna

53 Kluczowym elementem unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G jest konieczność dokonania przez państwa członkowskie oceny dostawców oraz nałożenia – w odniesieniu do kluczowych zasobów uznanych za krytyczne – ograniczeń na dostawców zaklasyfikowanych jako obarczeni wysokim ryzykiem. Państwa członkowskie powinny dokonać tej oceny na podstawie niewyczerpującej listy kryteriów pochodzących ze skoordynowanej oceny ryzyka w UE. Takimi kryteriami są na przykład:

- prawdopodobieństwo, że dostawca będzie przedmiotem ingerencji ze strony państwa spoza UE, na przykład ze względu na silne powiązania między dostawcą a rządem państwa spoza UE lub ze względu na ustawodawstwo takiego państwa, zwłaszcza w przypadku braku ustawodawczych lub demokratycznych mechanizmów kontroli i równowagi lub w przypadku braku umów dotyczących bezpieczeństwa lub ochrony danych między UE a państwem spoza UE;
- zdolność dostawcy do zapewniania dostaw;
- ogólna jakość produktów dostawcy i stosowanych przez niego praktyk w zakresie cyberbezpieczeństwa.

54 Zestaw narzędzi został opracowany z myślą o uniknięciu fragmentacji i wspieraniu spójności na rynku wewnętrznym. Przewidziane w nim kryteria stanowią ramy operacyjne przydatne do oceny profilu ryzyka poszczególnych dostawców w skoordynowany sposób przez wszystkie państwa członkowskie. Umożliwił on również Komisji – wraz z państwami członkowskimi – szybką reakcję na pojawiające się obawy co do bezpieczeństwa sieci 5G. Jednocześnie to w zakres obowiązków organów krajowych wchodzi stosowanie tych kryteriów przy ocenie ryzyka poszczególnych dostawców. Do października 2021 r., uwzględniwszy te ramy, 13 państw członkowskich przyjęło lub zmieniło przepisy dotyczące bezpieczeństwa sieci 5G (zob. pkt ***75*** i ***rys. 6***).

55 Niemniej jednak przedstawiciele dwóch z czterech ministerstw w państwach członkowskich, z którymi przeprowadzono wywiady w ramach niniejszej kontroli, byli zdania, że niektóre kryteria wykorzystywane przy klasyfikacji dostawców 5G mogą być interpretowane na różne sposoby i w związku z tym wymagają dalszego

doprecyzowania. W ich opinii Komisja powinna zapewnić dodatkowe wsparcie i wytyczne na potrzeby klasyfikowania dostawców obarczonych wysokim ryzykiem. Przedstawiciele państw członkowskich, z którymi kontrolerzy przeprowadzili wywiady, uznali również, że sytuacja ta stwarza ryzyko stosowania przez poszczególne państwa członkowskie rozbieżnych podejść względem dostawców stwarzających wysokie ryzyko (zob. także pkt ***74*** i ***75*** oraz ***ramka 5***). Podobne obawy wyraziło 11 krajowych organów regulacyjnych, które wzięły udział w ankiecie i które w różnym stopniu są zaangażowane w kwestię zapewnienia bezpieczeństwa sieci 5G.

Ocena ryzyka w zakresie bezpieczeństwa różni się w zależności od kraju pochodzenia dostawców sieci 5G

56 Dostawcy sieci 5G różnią się pod względem cech korporacyjnych i pochodzą z krajów o różnych powiązaniach z UE. Na ***rys. 5*** przedstawiono podobieństwa i różnice pomiędzy głównymi dostawcami sieci 5G i krajami ich pochodzenia, w szczególności w obszarach, o których mowa w unijnym zestawie narzędzi, a które mogą mieć wpływ na ocenę ich profilu ryzyka (zob. pkt ***53***).

Rys. 5 – Podobieństwa i różnice pomiędzy dostawcami sieci 5G i ich krajami pochodzenia

Źródło: Europejski Trybunał Obrachunkowy na podstawie następujących źródeł: członkowie WTO; członkowie OECD; wskaźnik restrykcyjności handlu usługami OECD; Bank Światowy: wskaźniki dobrego rządzenia na świecie – Worldwide Governance Indicators Dataset, 2019; Światowe Forum Ekonomiczne: globalny indeks konkurencyjności – Global Competitiveness Dataset, ranking w 2018 r.; decyzje stwierdzające odpowiedni stopień ochrony; Statista, „Who is leading the 5G patent race?"; dane firmy Ericsson; dane firmy Nokia; dane firmy Qualcomm; dane firmy Sharp; dane firmy LG; dane firmy Samsung; dane firmy Huawei oraz dane firmy ZTE. Kursy walutowe na dzień 31.12.2020 r.

57 Jednym z czynników ryzyka jest stopień, w jakim kraj pochodzenia dostawcy przestrzega podstawowych wartości politycznych i gospodarczych Unii Europejskiej. Aspekty o charakterze krajowym takie jak praworządność, niezawisłość sądów, otwartość na inwestycje zagraniczne i istnienie porozumień o ochronie danych można uznać za miarę ochrony prawnej przedsiębiorstwa przed ingerencją rządu, a także ochrony, jaką przedsiębiorstwo może zapewnić swoim klientom.

58 O ile dostawcy z siedzibą w państwach członkowskich UE są zobowiązani do przestrzegania norm i wymogów prawnych UE, o tyle nie dotyczy to sześciu głównych dostawców z siedzibą w krajach spoza UE, którzy działają na podstawie ustawodawstwa tych krajów (zob. ***rys. 5***). Tamtejsze przepisy mogą znacznie odbiegać od standardów UE, na przykład jeśli chodzi o ochronę danych przyznawaną obywatelom, skuteczność tej ochrony lub – bardziej ogólnie – sposób zapewnienia niezawisłości sądów za pomocą ustawodawczych lub demokratycznych mechanizmów kontroli i równowagi. Jeśli chodzi o niezawisłość sądownictwa, USA i Japonia uzyskują lepsze wyniki niż inne kraje pochodzenia dostawców sieci 5G, natomiast w przypadku praworządności to Korea Południowa uzyskuje najlepsze wyniki spośród tych krajów.

59 Sieci 5G opierają się w przeważającej mierze na oprogramowaniu. Fakt, że niektórzy dostawcy działają w ramach ustawodawstwa państw nienależących do UE, może budzić szczególne obawy, zwłaszcza gdy ośrodki kontroli oprogramowania także znajdują się poza granicami UE. Oznacza to bowiem potencjalnie, że użytkownicy z UE podlegają ustawodawstwu państw trzecich.

60 Aby zminimalizować te obawy, Komisja przystąpiła do działania, wychodząc z założenia, że każde przedsiębiorstwo świadczące usługi dla obywateli UE powinno przestrzegać zasad i wartości UE[46]. W tym kontekście rozpoczęła ona dialog z kilkoma krajami w celu zapewnienia skutecznej ochrony prywatności danych osobowych[47]. Na ***rys. 5*** pokazano również, że Komisja uznała już adekwatność systemów ochrony danych funkcjonujących w Japonii (i w przeszłości w Stanach Zjednoczonych). Należy jednak zauważyć, że tego typu decyzje w sprawie adekwatności systemów mogą zostać zakwestionowane i są objęte ścisłą kontrolą sądową. Na przykład w 2015 r. Trybunał Sprawiedliwości UE unieważnił obowiązujący wówczas instrument prawny umożliwiający wymianę danych ze Stanami Zjednoczonymi, tj. porozumienie

---

[46] Komunikat Komisji Europejskiej, „Kształtowanie cyfrowej przyszłości Europy” (COM(2020) 67 final).

[47] UE-Chiny – perspektywa strategiczna.

„bezpieczna przystań”[48], a następnie w 2020 r. orzekł, że tzw. tarcza prywatności – która zastąpiła „bezpieczną przystań” – nie zapewnia odpowiedniej ochrony obywatelom UE[49]. W związku z tym obecnie brak jest decyzji w sprawie adekwatności systemów, która dotyczyłaby Stanów Zjednoczonych. W ujęciu bardziej ogólnym i abstrahując od istnienia systemu ochrony danych, należy ponadto wziąć pod uwagę szerzej rozumiane ramy prawne i instytucjonalne, w tym na przykład przestrzeganie praworządności czy sposób zapewnienia niezawisłości sądów.

61 Na ***rys. 5*** pokazano również znaczne zróżnicowanie pomiędzy dostawcami sieci 5G pod względem udziału w patentach 5G, przychodów i liczby pracowników. Wpływa to na zasoby, jakimi one dysponują, co z kolei może mieć wpływ na ich odporność i zdolność do zapewnienia ciągłości dostaw. Na przykład Samsung i Huawei są dostawcami, którzy mają największy udział w patentach 5G, generują największe przychody jako korporacje i zatrudniają największą liczbę pracowników ogółem.

62 Kolejnym istotnym czynnikiem określonym w zestawie narzędzi jako decydujący o profilu ryzyka jest prawdopodobieństwo, że dostawca będzie podlegał ingerencji ze strony rządu kraju spoza UE. W tym kontekście istotną rolę odgrywa struktura własności przedsiębiorstwa, ponieważ właściciele posiadający dużą liczbę udziałów mogą być w stanie wywierać nacisk lub wpływać na decyzje zarządu. Ponadto spółki będące własnością prywatną lub państwową są uważane za mniej skłonne do poddawania się kontroli publicznej w postaci audytów i rozliczalności w porównaniu ze spółkami publicznymi, które podlegają rygorystycznym wymogom ujawniania informacji przez cały rok, z korzyścią dla inwestorów i organów regulacyjnych. Większość dostawców sieci 5G jest notowana na giełdzie, zarówno w kraju pochodzenia, jak i za granicą. Chińscy dostawcy są natomiast trudniejsi do sklasyfikowania i są ogólnie postrzegani jako blisko powiązani z chińskim rządem[50].

---

[48] Wyrok w sprawie C-362/14 oraz https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pl.pdf

[49] Wyrok w sprawie C-311/18 oraz https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pl.pdf

[50] https://www.europarl.europa.eu/doceo/document/E-9-2020-004305_EN.html oraz https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

Państwa członkowskie uznały wsparcie ze strony Komisji i ENISA za przydatne na etapie wdrażania unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

63 Komisja wspierała państwa członkowskie poprzez ułatwianie wymiany najlepszych praktyk w odniesieniu do niektórych kluczowych środków zawartych w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, w tym w odniesieniu do dostawców wysokiego ryzyka. Wsparciu temu, udzielanemu często w kontekście grupy współpracy ds. bezpieczeństwa sieci i informacji, towarzyszyły konkretne działania prowadzone przez ENISA, takie jak organizacja seminariów internetowych czy zapewnianie wytycznych na temat:

- wdrażania zestawu narzędzi ze szczególnym uwzględnieniem środków technicznych,
- najlepszych praktyk w zakresie bezpieczeństwa sieci, w szczególności w odniesieniu do:
  - krajobrazów zagrożeń sieci 5G[51];
  - przygotowania krajowych ocen ryzyka związanego z 5G;
  - środków bezpieczeństwa w ramach Europejskiego kodeksu łączności elektronicznej[52], w tym osobnych wytycznych dotyczących bezpieczeństwa sieci 5G[53].

64 Komisja zleciła również ENISA opracowanie unijnego systemu certyfikacji cyberbezpieczeństwa sieci 5G, który powinien pomóc w ograniczeniu ryzyka związanego z technicznymi słabościami sieci i w dalszym wzmacnianiu cyberbezpieczeństwa[54]. Chociaż certyfikacja ta może przyczynić się do poprawy bezpieczeństwa, nie jest w stanie zapobiec zagrożeniom powstającym w systemach w następstwie aktualizacji oprogramowania.

65 Wszyscy przedstawiciele organów państw członkowskich, z którymi kontrolerzy przeprowadzili wywiady na potrzeby niniejszej kontroli, podkreślali przydatność

---

[51] ENISA, „Threat Landscape for 5G Networks”, 14.12.2020 r.

[52] ENISA, „Guideline on Security Measures under the EECC”, 10.12.2020 r.

[53] ENISA, „5G supplement to the Guidelines on Security Measures under the EECC”, 7.7.2021 r.

[54] Komunikat prasowy z 3 lutego 2021 r.

wsparcia Komisji i ENISA we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Ponadto większość krajowych organów regulacyjnych ds. telekomunikacji (15 z 21) stwierdziła, że Komisja lub ENISA wspierały organy krajowe w wymianie najlepszych praktyk dotyczących wdrażania kluczowych środków strategicznych.

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G przyjęto zbyt późno, aby mógł zostać uwzględniony w projektach współfinansowanych przez UE w latach 2014–2020

66 Jednym z celów unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G jest dopilnowanie, aby w projektach 5G współfinansowanych przez UE uwzględniano ryzyko związane z cyberbezpieczeństwem. Zestaw narzędzi został jednak przyjęty dopiero w styczniu 2020 r. Ponieważ wszystkie projekty objęte niniejszą kontrolą wybrano przed przyjęciem unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, nie można oczekiwać, że zastosowano w nich zalecane podejście do cyberbezpieczeństwa, w tym w odniesieniu do dostawców wysokiego ryzyka. Na przykład w próbie dobranej do kontroli Trybunał zidentyfikował jeden projekt w ramach programu „Horyzont 2020” i dwa projekty w ramach EFRR w Hiszpanii, w których wykorzystano chiński sprzęt 5G, zakazany na późniejszym etapie w Szwecji (zob. pkt ***15***).

67 W okresie 2021–2027 Komisja zamierza promować spójne podejście do kwestii bezpieczeństwa 5G w projektach współfinansowanych przez UE i dopilnować, by przestrzeganie kryteriów zawartych w zestawie narzędzi było warunkiem uzyskania finansowania ze środków UE. Będzie się to jednak różnić w zależności od trybu wdrażania:

- W programach zarządzanych bezpośrednio przez Komisję (na przykład program „Horyzont Europa” na lata 2021–2027) możliwe będzie wykluczenie dostawców podlegających ingerencji ze strony rządu państwa spoza UE. Takie podejście powinno zagwarantować, że w projektach finansowanych przez UE uwzględnione będzie ryzyko związane z cyberbezpieczeństwem, oraz powinno zapobiec sytuacjom, w których dostawca otrzymujący dofinansowanie UE w jednym państwie członkowskim jest uznawany za stwarzającego wysokie ryzyko i wykluczony w innym państwie.

- W przypadku programów realizowanych w ramach zarządzania dzielonego w przepisach nie określono wymogów dotyczących ryzyka w zakresie cyberbezpieczeństwa. Z tego względu Komisja planuje promować włączenie odniesienia do unijnego zestawu narzędzi w umowach partnerskich z państwami

członkowskimi, tak aby przy finansowaniu z EFRR projektów związanych z 5G uwzględniano zagrożenia dla cyberbezpieczeństwa.

- W przypadku programu InvestEU (zastępującego EFIS)[55] i RRF Komisja planuje zachęcać właściwe organy do zamieszczania odwołania do unijnego zestawu narzędzi w umowach o finansowaniu.

Państwa członkowskie nie podchodzą jeszcze w sposób skoordynowany do kwestii bezpieczeństwa przy wdrażaniu sieci 5G

Informacje na temat podejścia państw członkowskich do kwestii bezpieczeństwa są niewystarczające

68 Komisja monitoruje postępy we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G i informuje o nich za pośrednictwem grupy współpracy ds. bezpieczeństwa sieci i informacji, rozmów dwustronnych z państwami członkowskimi oraz pośrednio w mediach. Pierwsze wyniki tego monitorowania zostały opublikowane w lipcu 2020 r.[56] W grudniu 2020 r. Komisja opublikowała również sprawozdanie na temat wpływu jej zalecenia w sprawie cyberbezpieczeństwa sieci 5G[57]. Według stanu na wrzesień 2021 r. nie planuje się kolejnych sprawozdań w przyszłości.

69 W wyżej wymienionych sprawozdaniach brakuje jednak wspólnego zestawu kluczowych wskaźników efektywności i nie przedstawiono w nich porównywalnego zestawu szczegółowych informacji na temat tego, w jaki sposób państwa członkowskie podchodzą do kwestii bezpieczeństwa sieci 5G.

70 Ponadto niewiele jest publicznie dostępnych informacji na temat podejścia państw członkowskich względem dostawców wysokiego ryzyka, tj. ich identyfikacji oraz tego, czy są wykluczani z dostaw sprzętu 5G, a dostępne informacje te są sprzeczne i niekompletne. Na przykład:

---

[55] Rozporządzenie (UE) 2021/523 ustanawiające Program InvestEU.

[56] Sprawozdanie z postępów poczynionych przez państwa członkowskie we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, lipiec 2020 r.

[57] Sprawozdanie na temat skutków zalecenia Komisji z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G, SWD(2020) 357 final z 16.12.2020 r.

- W sprawozdaniu z lipca 2020 r. w sprawie postępów państw członkowskich we wdrażaniu unijnego zestawu narzędzi (zob. pkt ***68***) Komisja stwierdziła, że około połowy państw członkowskich (14 z 27) dokonało oceny profilu ryzyka dostawców i nałożyło ograniczenia w stosunku do dostawców uznanych za stwarzających wysokie ryzyko.

- W sprawozdaniu z grudnia 2020 r.[58] Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) zauważył, że tylko dziewięć państw członkowskich wprowadziło takie ograniczenia, a siedem z pozostałych 18 państw członkowskich nie zamierza wprowadzać takich ograniczeń w przyszłości.

71 Nawet jeśli państwa członkowskie przyjęły przepisy dotyczące bezpieczeństwa sieci 5G (zob. również pkt ***75***), nadal nie wyjaśniono w nich podejścia względem dostawców wysokiego ryzyka. Wszelkie konkretne decyzje będą prawdopodobnie podejmowane wyłącznie w drodze aktów wykonawczych bądź niepublicznych decyzji administracyjnych lub handlowych.

72 Według zainteresowanych stron i decydentów (np. Parlamentu Europejskiego), z którymi kontrolerzy przeprowadzili wywiady, informacje niepubliczne (np. zawarte w sprawozdaniach Komisji lub grupy ds. bezpieczeństwa sieci i informacji) na temat podejścia państw członkowskich do dostawców wysokiego ryzyka są również skąpe, a podmioty te muszą polegać na mediach i źródłach nieoficjalnych.

73 Pomimo transgranicznego charakteru zagadnień związanych z bezpieczeństwem sieci 5G dostępnych jest niewiele informacji publicznych na temat tego, w jaki sposób państwa członkowskie podchodzą do kwestii bezpieczeństwa, a w szczególności do dostawców wysokiego ryzyka. Utrudnia to wymianę wiedzy między państwami członkowskimi oraz możliwość stosowania skoordynowanych środków, a także ogranicza możliwości zaproponowania przez Komisję rozwiązań zmierzających do poprawy bezpieczeństwa sieci 5G.

Istnieją przesłanki wskazujące na to, że niektóre państwa członkowskie mają rozbieżne podejścia względem dostawców sieci 5G

74 Organy krajowe mają duży margines swobody przy wdrażaniu kluczowych środków dotyczących bezpieczeństwa sieci 5G (zob. pkt ***48*** i ***49***). W unijnym zestawie narzędzi uwzględniono krajowe kompetencje i istotne czynniki o charakterze krajowym

[58] BEREC, sprawozdanie wewnętrzne dotyczące środków strategicznych 5 i 6 (dywersyfikacja dostawców i wzmocnienie odporności krajowej) unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, BoR 20 (227), 10.12.2020 r.

(ocena zagrożeń przez krajowe służby bezpieczeństwa, terminy na wdrożenie sieci 5G, obecność dostawców, zdolności w zakresie cyberbezpieczeństwa). Jak dotychczas państwa członkowskie stosowały rozbieżne podejścia w odniesieniu do kwestii takich jak korzystanie ze sprzętu określonych dostawców czy zakres ograniczeń nakładanych na dostawców wysokiego ryzyka (zob. przykłady czterech państw członkowskich w ***ramce 5***).

Ramka 5

Przykłady rozbieżnych podejść państw członkowskich względem chińskich dostawców sieci 5G

Przyjęto ramowe zasady i nakładane są ograniczenia[1]

W październiku 2020 r. szwedzki krajowy organ regulacyjny ds. telekomunikacji (PTS) ustalił następujące warunki udziału w aukcji na częstotliwości 5G:

— nowe instalacje i wdrażanie funkcji centralnych na potrzeby wykorzystania radiowego w pasmach częstotliwości nie mogą być wykonywane przy użyciu produktów pochodzących od chińskich dostawców;

— wszelka istniejąca infrastruktura pochodząca od takich dostawców musi zostać stopniowo wycofana najpóźniej do 1 stycznia 2025 r.

Przyjęto ramowe zasady, lecz nie są one jeszcze stosowane[2], [3], [4]

W Niemczech ustawa o bezpieczeństwie IT 2.0 z maja 2021 r. przewiduje obowiązkową certyfikację komponentów krytycznych przed dopuszczeniem ich do użytku. Niemieccy operatorzy sieci ruchomej, z którymi Trybunał przeprowadził wywiady, opowiadają się za jednolitą europejską procedurą certyfikacji pod auspicjami ENISA, która miałaby odgrywać rolę europejskiego „punktu kompleksowej obsługi", zamiast konieczności uzyskiwania potencjalnie dużej liczby certyfikatów krajowych. Ustawa zezwala również Federalnemu Ministerstwu Spraw Wewnętrznych na zakazanie stosowania krytycznych komponentów, w razie gdyby mogły one stanowić zagrożenie dla bezpieczeństwa narodowego.

W Austrii na mocy znowelizowanej ustawy telekomunikacyjnej, która została przyjęta pod koniec października 2021 r., właściwy minister ma prawo klasyfikować dostawców jako stwarzających wysokie ryzyko oraz nakładać na nich ograniczenia bądź wykluczać z rynku. Jak wynika z publicznie dostępnych informacji z października 2021 r., Austria rozwija obecnie sieć 5G, korzystając z technologii zapewnianej przez chińskiego dostawcę Huawei.

Brak ramowych zasad[5], [6]

Zgodnie ze stanem na wrzesień 2021 r. Węgry nie nałożyły ograniczeń na żadnego dostawcę sieci 5G i prawdopodobnie nie zrobią tego w najbliższej przyszłości. Węgry oficjalnie odmówiły również przystąpienia do międzynarodowego programu „5G Clean Network Program", promowanego przez USA, który ma na celu ograniczenie obecności chińskich dostawców w sieciach szkieletowych 5G.

(1) Decyzja 18-8496 z 20 października 2020 r. w sprawie warunków przeprowadzenia aukcji na pasma częstotliwości 3,5 GHz i 2,3 GHz.

(2) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

(3) Austriacka ustawa telekomunikacyjna.

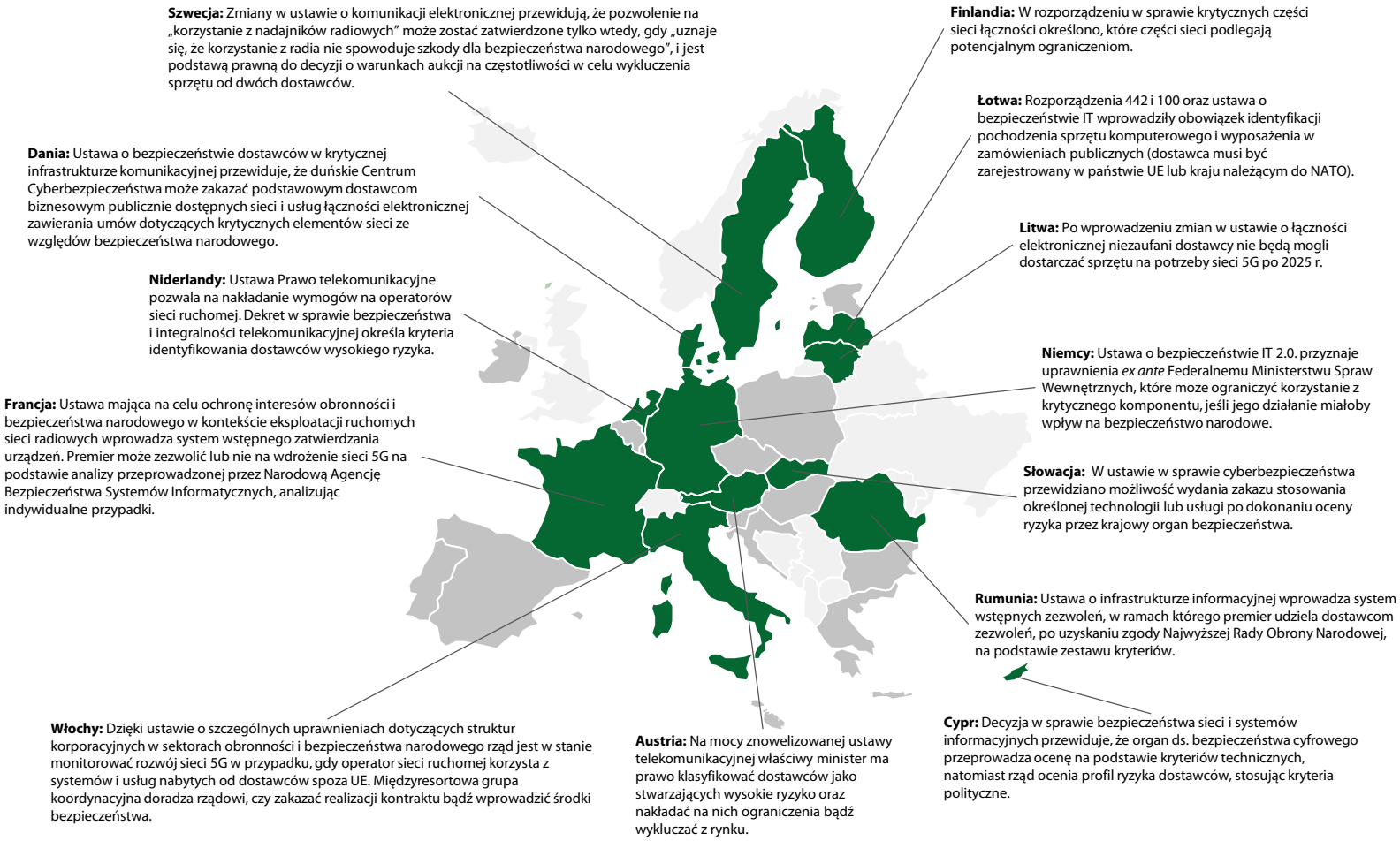
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(5) https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf

(6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/hungary

75 Od momentu przyjęcia zestawu narzędzi poczyniono postępy, jeśli chodzi o zapewnienie większego bezpieczeństwa sieci 5G, a większość państw członkowskich wprowadziła ograniczenia w odniesieniu do dostawców wysokiego ryzyka lub przygotowuje się do ich wprowadzenia. Według stanu na koniec 2021 r. 13 państw członkowskich przyjęło lub zmodyfikowało przepisy krajowe w dziedzinie bezpieczeństwa sieci 5G. Te środki regulacyjne uwzględniają wprawdzie kryteria określone w zestawie narzędzi, ale opierają się na różnych podejściach (zob. ***rys. 6***). Kolejne państwa członkowskie są na etapie proponowania takich przepisów. W nadchodzących latach może to się przełożyć na bardziej zharmonizowane podejście do dostawców 5G obarczonych wysokim ryzykiem, przynajmniej wśród tych państw członkowskich, które przyjęły odnośne przepisy.

Rys. 6 – Państwa członkowskie, które przyjęły przepisy umożliwiające wyłączenie sprzętu pochodzącego od dostawców wysokiego ryzyka, stan na październik 2021 r.



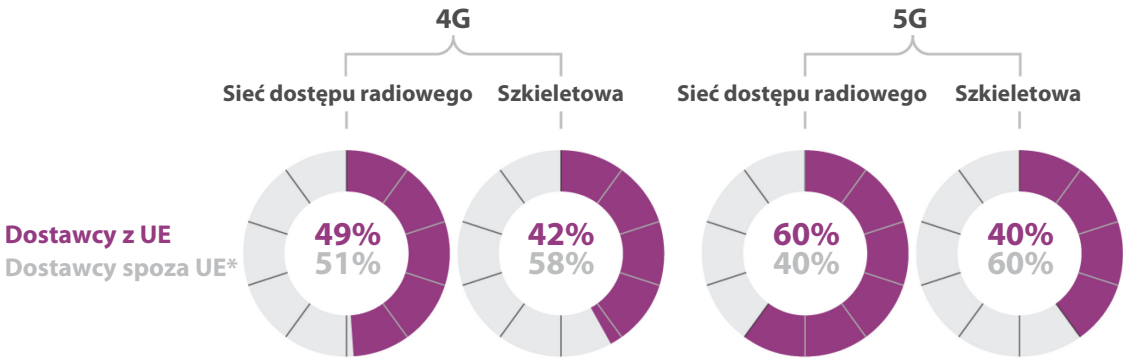
Źródło: Europejski Trybunał Obrachunkowy na podstawie danych Komisji Europejskiej.

76 Komisja nie oceniła jak dotąd, jaki byłby wpływ rozbieżnych podejść, na przykład w sytuacji budowy sieci 5G przez jedno państwo członkowskie z wykorzystaniem sprzętu pochodzącego od dostawcy uznanego przez inne państwo członkowskie za stwarzającego wysokie ryzyko. Taki wpływ mógłby być obserwowalny, jeśli chodzi o bezpieczeństwo transgraniczne lub konkurencję między operatorami sieci ruchomej działającymi na jednolitym rynku UE.

Komisja zaczęła ostatnio zajmować się kwestią subsydiów zagranicznych zakłócających rynek wewnętrzny

77 Według stanu na grudzień 2020 r. ponad połowa wszystkich urządzeń 4G i 5G w UE pochodziła od dostawców spoza UE (zob. *rys. 7*).

Rys. 7 – Udział operatorów sieci ruchomej korzystających ze sprzętu dostawców z UE / spoza UE*



* *Termin „spoza UE" odnosi się do dostawców z Ameryki Północnej, Azji i Australii.*

Źródło: Europejski Trybunał Obrachunkowy na podstawie danych BEREC. Sprawozdanie wewnętrzne dotyczące środków strategicznych 5 i 6 (dywersyfikacja dostawców i wzmocnienie odporności krajowej) z unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. BoR (20) 227.

78 Według stanu na koniec 2019 r. 286 mln klientów w UE-27 (64% ludności) korzystało z sieci telekomunikacyjnych opartych na urządzeniach 4G pochodzących od chińskich dostawców[59]. W październiku 2020 r. grupa posłów do Parlamentu Europejskiego zwróciła się do ministrów ds. telekomunikacji i handlu państw członkowskich oraz do Komisji, wyrażając swe obawy, że jedną z przyczyn dużego udziału chińskich dostawców w rynku jest fakt, że korzystają oni z nieuczciwej przewagi ekonomicznej, tj. z subsydiów publicznych, które nie są dostępne dla unijnych

[59] StrandConsult, „Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks".

dostawców zgodnie z unijnymi zasadami pomocy państwa[60]. W niedawno opublikowanym przeglądzie Trybunał zwrócił uwagę na podobne zagrożenia w tym względzie[61]. Takie subsydia mogą zakłócić funkcjonowanie rynku wewnętrznego, tworząc nierówne warunki konkurencji dla dostawców sieci 5G, co może mieć wpływ na bezpieczeństwo. Aby rozwiązać ten problem, w maju 2021 r. Komisja przedstawiła wniosek dotyczący nowego rozporządzenia[62], w którym określono procedury badania takich subsydiów i korygowania związanych z nimi zakłóceń.

Komisja nie posiada wystarczających informacji na temat potencjalnych kosztów zastąpienia sprzętu pochodzącego od chińskich dostawców

79 Zgodnie ze sprawozdaniem z czerwca 2020 r.[63] ograniczenie działalności jednego z kluczowych dostawców infrastruktury 5G w UE doprowadziłoby do wzrostu całkowitych kosztów inwestycji o prawie 2,4 mld euro rocznie w ciągu następnej dekady (tj. łącznie o 24 mld euro). Według innego badania[64] europejscy operatorzy już teraz stoją przed koniecznością modernizacji sieci 4G zbudowanych w latach 2012–2016, ponieważ standardową praktyką biznesową jest naprawa i modernizacja sprzętu sieciowego, który ma więcej niż trzy-cztery lata. W badaniu tym oszacowano, że całkowity koszt odinstalowania i wymiany sprzętu nadającego się do modernizacji zakupionego od chińskich dostawców od 2016 r. wyniesie około 3 mld euro.

80 Wysoki udział sprzętu pochodzącego od chińskich dostawców w połączeniu z ewentualnym zakwalifikowaniem tych dostawców do kategorii wysokiego ryzyka w niektórych państwach członkowskich może wiązać się z koniecznością poniesienia kosztów zastąpienia rzędu miliardów euro, jeśli operatorzy sieci ruchomej musieliby wyeliminować urządzenia chińskich dostawców z sieci europejskich i zastąpić je innymi urządzeniami bez okresu przejściowego (zob. pkt ***77***–***79***). Co do zasady nie ma możliwości, by operatorom udzielić pomocy państwa tytułem rekompensaty kosztów

---

[60] Pismo posłów do PE do ministrów telekomunikacji i handlu UE oraz komisarzy Thierry'ego Bretona, Margrethe Vestager i Valdisa Dombrovskisa, 14.10.2020 r.

[61] Przegląd Europejskiego Trybunału Obrachunkowego nr 03/2020 pt. „Reakcja UE na państwową strategię inwestycyjną Chin".

[62] Wniosek dotyczący rozporządzenia w sprawie subsydiów zagranicznych zakłócających rynek wewnętrzny, COM(2021) 223 final z 5.5.2021 r.

[63] Oxford Economics, „Restricting competition in 5G network equipment throughout Europe", czerwiec 2020 r. (sponsorowany przez Huawei).

[64] StrandConsult, „The real cost to 'rip and replace' Chinese equipment from telecom networks".

wywiązania się ze zobowiązań prawnych, chyba że państwa członkowskie będą w stanie przekonać Komisję, że spełnione zostały niezbędne wymogi w tym zakresie (takie jak efekt zachęty). W ramach analizy przeprowadzonej przez Trybunał stwierdzono jeden przypadek, w którym na mocy przepisów krajowych można by wykorzystać krajowe środki publiczne do pokrycia kosztów zastąpienia sprzętu (zob. fińska ustawa w sprawie usług łączności elektronicznej[65]). Państwa członkowskie mają obowiązek zgłoszenia Komisji ewentualnych przypadków pomocy państwa na rzecz operatorów sieci ruchomej tytułem rekompensaty takich kosztów. Z informacji udzielonych przez Komisję wynika, że jak dotąd żadne państwo członkowskie ani inny podmiot nie zwróciły się do niej w celu przedyskutowania możliwości udzielenia pomocy państwa na pokrycie kosztów zastąpienia sprzętu. W opinii przedstawicieli branży, z którymi przeprowadzono wywiady w trakcie kontroli, niepewność co do tego, jak państwa członkowskie będą podchodzić do kwestii tych kosztów, jak również potencjalne różnice w ich podejściu podważają pewność prowadzenia działalności gospodarczej i mogą mieć wpływ na terminowe wdrożenie sieci 5G.

[65] Ustawa 1207/2020 w sprawie usług łączności elektronicznej z 30.12.2020 r., art. 301.

Wnioski i zalecenia

81 W ogólnym ujęciu kontrola Trybunału wykazała, że pomimo wsparcia ze strony Komisji występują znaczne opóźnienia we wdrażaniu sieci 5G przez państwa członkowskie oraz że konieczne są dalsze wysiłki, by rozwiązać problemy w zakresie bezpieczeństwa ich wdrożenia.

82 W swoim planie działania dotyczącym sieci 5G z 2016 r. Komisja wezwała do objęcia zasięgiem 5G wszystkich obszarów miejskich i głównych szlaków transportowych do 2025 r., a w marcu 2021 r. – do objęcia całego terytorium UE zasięgiem sieci do 2030 r. Według stanu na koniec 2020 r. 23 państwa członkowskie uruchomiły komercyjne usługi sieci 5G i osiągnęły pośredni cel polegający na zapewnieniu dostępu do takich usług w co najmniej jednym dużym mieście. Kontrolerzy ustalili jednak, że nie wszystkie państwa członkowskie uwzględniły cele Komisji w swoich krajowych strategiach dotyczących sieci 5G lub planach szerokopasmowych. Ponadto w kilku krajach nie dokonano jeszcze transpozycji Europejskiego kodeksu łączności elektronicznej do prawa krajowego, a przydział częstotliwości na potrzeby sieci 5G się opóźnił. Opóźnienia w ich przydziale mogą wynikać z różnych przyczyn: z niskiego popytu ze strony operatorów sieci ruchomej, problemów w zakresie koordynacji działań z państwami nienależącymi do UE położonymi wzdłuż wschodnich granic, wpływu pandemii COVID-19 na terminy aukcji oraz niepewności co do tego, jak rozwiązać kwestie bezpieczeństwa. Z informacji udzielonych przez Komisję wynika, że jedynie 11 państw członkowskich ma szansę osiągnąć cel wyznaczony na 2025 r. (zob. pkt ***22***–***43***).

83 Komisja wspierała państwa członkowskie w realizacji przyjętego przez nią w 2016 r. planu działania dotyczącego sieci 5G poprzez inicjatywy, wytyczne i finansowanie badań naukowych w dziedzinie technologii 5G. Nie określiła jednak oczekiwanej jakości usług sieci 5G, na przykład pod względem takich parametrów jak minimalna prędkość przesyłu danych czy maksymalny poziom opóźnień. Doprowadziło to do sytuacji, w której termin „jakość 5G” jest różnie rozumiany przez państwa członkowskie. Trybunał odnotował rozbieżne podejścia państw członkowskich, jeśli chodzi o wdrażanie usług 5G, na przykład fakt, że tylko dwa państwa członkowskie określiły minimalną prędkość przesyłu danych i maksymalny poziom opóźnień. Ostatecznie te rozbieżne podejścia niosą ze sobą ryzyko nierówności w dostępie do usług 5G i ich jakości w UE, co raczej zwiększy niż zmniejszy tzw. przepaść cyfrową między państwami członkowskimi i regionami (zob. pkt ***22***–***31***).

Zalecenie 1 – Promowanie równomiernego i terminowego wdrażania sieci 5G w UE

Komisja powinna:

a) wraz z państwami członkowskimi opracować wspólną definicję oczekiwanej jakości usług w sieciach 5G, np. wymogi dotyczące wydajności, jaką powinny one oferować pod względem minimalnej prędkości przesyłu danych i maksymalnego poziomu opóźnień;

b) zachęcać państwa członkowskie do uwzględnienia celów na lata 2025 i 2030 w zakresie wdrożenia sieci 5G, a także środków potrzebnych do ich osiągnięcia, przy okazji kolejnych aktualizacji krajowych strategii cyfrowych, strategii dotyczących sieci 5G lub planów szerokopasmowych;

c) wspierać państwa członkowskie w rozwiązywaniu problemów związanych z koordynacją wykorzystania widma z państwami sąsiadującymi spoza UE, na przykład poprzez naciskanie na włączenie tego zagadnienia do porządku obrad wszystkich odnośnych spotkań.

Termin realizacji: grudzień 2022 r.

84 Kwestie dotyczące bezpieczeństwa sieci 5G dopiero niedawno stały się źródłem poważnych obaw na szczeblu UE. W 2019 r. Rada Europejska podkreśliła potrzebę działań w tym obszarze na szczeblu UE, wzywając państwa członkowskie do skoordynowanego podejścia i współpracy w tej transgranicznej kwestii. Komisja – wraz z państwami członkowskimi – szybko zareagowała na pojawiające się obawy co do bezpieczeństwa sieci 5G. W 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji przyjęła unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, w którym określono szereg środków strategicznych i technicznych oraz działań wspierających służących przeciwdziałaniu zagrożeniom dla bezpieczeństwa sieci 5G, a także wskazano podmioty odpowiedzialne za każdy z tych środków i działań. Kilka środków dotyczy problemu dostawców sprzętu 5G obarczonych wysokim ryzykiem. Zestaw narzędzi został następnie zatwierdzony przez Komisję i Radę Europejską (zob. pkt ***45***–***47***). Jako że stanowi on instrument prawa miękkiego, przewidziane w nim środki nie są wiążące dla państw członkowskich. W ostatnim czasie ów unijny zestaw narzędzi został wspomniany w nowej europejskiej strategii na rzecz wsparcia inteligentnych, ekologicznych i bezpiecznych powiązań w systemach cyfrowych na całym świecie, w której został on uznany za narzędzie służące do ukierunkowania inwestycji w infrastrukturę cyfrową (zob. pkt ***50***).

85 Przewidziane w nim kryteria stanowią ramy operacyjne przydatne do oceny profilu ryzyka poszczególnych dostawców w skoordynowany sposób przez wszystkie państwa członkowskie. Niemniej jednak przeprowadzanie takiej oceny leży w dalszym ciągu w kompetencji organów krajowych (zob. pkt ***54***).

86 Od momentu przyjęcia zestawu narzędzi poczyniono postępy, jeśli chodzi o zapewnienie większego bezpieczeństwa sieci 5G, a większość państw członkowskich wprowadziła ograniczenia w odniesieniu do dostawców wysokiego ryzyka lub przygotowuje się do ich wprowadzenia. Do października 2021 r., uwzględniwszy te ramy, 13 państw członkowskich przyjęło lub zmieniło przepisy dotyczące bezpieczeństwa sieci 5G. Pozostałe państwa członkowskie są na etapie proponowania takich przepisów, które będą uwzględniać kryteria przewidziane w unijnym zestawie narzędzi (zob. pkt ***54*** i ***75***).

87 Zestaw narzędzi został przyjęty na wczesnym etapie wdrażania technologii 5G, lecz mimo to wielu operatorów sieci ruchomej zdążyło już wcześniej dokonać wyboru dostawców sprzętu 5G (zob. pkt ***52***). Nieuwzględnienie kwestii bezpieczeństwa na etapie opracowywania założeń polityki grozi negatywnymi skutkami na etapie jej realizacji, przykładowo tym, że oczekiwane korzyści (np. wzrost PKB) zostaną zniweczone przez koszty wyeliminowania zagrożeń (np. koszty cyberprzestępczości) (zob. pkt ***02*** i ***04***).

88 W unijnym zestawie narzędzi uwzględniono krajowe kompetencje i istotne czynniki o charakterze krajowym. Kontrola Trybunału wykazała, że jak dotąd państwa członkowskie stosowały bardzo różne podejścia, jeśli chodzi o wykorzystanie sprzętu pochodzącego od dostawców obarczonych wysokim ryzykiem lub zakres ograniczeń (np. tylko części szkieletowe lub części krytyczne sieci 5G, sieć dostępu radiowego bądź jej część) (zob. pkt ***74*** i ***75***).

89 Przewiduje się, że przyjęcie przez państwa członkowskie przepisów dotyczących bezpieczeństwa sieci 5G w oparciu o zestaw narzędzi w nadchodzących latach może przełożyć się na bardziej zharmonizowane podejście do dostawców technologii 5G obarczonych wysokim ryzykiem. Ponieważ jednak żaden ze środków przewidzianych w zestawie narzędzi nie ma mocy wiążącej prawnie, Komisja nie może ich egzekwować. W związku z tym wciąż istnieje ryzyko, że zestaw narzędzi sam w sobie nie będzie w stanie zagwarantować skoordynowanego podejścia państw członkowskich do kwestii bezpieczeństwa (zob. pkt ***49***–***75***).

90 Wielu dostawców technologii 5G ma siedzibę poza UE i w związku z tym działa zgodnie z ustawodawstwem państw trzecich, które może znacznie odbiegać od standardów UE, na przykład pod względem skuteczności ochrony danych przyznawanej obywatelom, a w bardziej ogólnym ujęciu pod względem sposobu zapewnienia niezawisłości sądów za pomocą ustawodawczych lub demokratycznych mechanizmów kontroli i równowagi. Fakt, że sieci 5G opierają się w przeważającej mierze na oprogramowaniu, może również stanowić szczególny problem w zakresie bezpieczeństwa, jeżeli ośrodki kontroli takiego oprogramowania znajdują się w państwach spoza UE. Oznacza to bowiem potencjalnie, że obywatele UE podlegają ustawodawstwu państw trzecich. Aby zminimalizować te obawy, Komisja przystąpiła do działania, wychodząc z założenia, że każde przedsiębiorstwo świadczące usługi dla obywateli UE powinno przestrzegać zasad i wartości UE. W tym kontekście rozpoczęła ona dialog z kilkoma krajami w celu zapewnienia skutecznej ochrony prywatności danych osobowych (zob. pkt ***56***–***62***).

91 Pomimo transgranicznego charakteru zagadnień związanych z bezpieczeństwem sieci 5G brak jest informacji publicznych na temat tego, w jaki sposób państwa członkowskie podchodzą do kwestii bezpieczeństwa, a także na temat ich zależności od dostawców wysokiego ryzyka. Komisja monitoruje wdrażanie unijnego zestawu narzędzi i informuje o osiągniętych postępach. W sporządzonych przez nią sprawozdaniach nie przedstawiono jednak szczegółowych i porównywalnych informacji na temat tego, w jaki sposób państwa członkowskie podchodzą do kwestii bezpieczeństwa sieci 5G. Ponadto według stanu na wrzesień 2021 r. nie planuje się kolejnych sprawozdań w przyszłości. Tymczasem brak takich informacji utrudnia wymianę wiedzy między państwami członkowskimi oraz możliwość stosowania skoordynowanych środków. Ogranicza również możliwość zaproponowania przez Komisję rozwiązań zmierzających do poprawy bezpieczeństwa sieci 5G (zob. pkt ***68***–***73***).

Zalecenie 2 – Promowanie skoordynowanego podejścia państw członkowskich do bezpieczeństwa sieci 5G

Komisja powinna:

a) zapewniać dalsze wytyczne lub działania wspierające dotyczące kluczowych elementów unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, takich jak kryteria oceny dostawców 5G i ich klasyfikowania jako dostawców wysokiego ryzyka, a także kwestii związanych z ochroną danych.

Termin realizacji: grudzień 2022 r.

b) promować przejrzyste informacje na temat podejść państw członkowskich do kwestii bezpieczeństwa sieci 5G, prowadząc monitorowanie i sprawozdawczość na temat wdrażania środków bezpieczeństwa przewidzianych w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. W tym celu powinna ona korzystać ze wspólnego zestawu kluczowych wskaźników efektywności.

Termin realizacji: grudzień 2022 r.

c) wraz z państwami członkowskimi ocenić, w przypadku których aspektów bezpieczeństwa sieci 5G istnieje potrzeba określenia wymogów możliwych do wyegzekwowania na drodze prawnej oraz, w stosownych przypadkach, podjąć prace nad odnośnymi przepisami.

Termin realizacji: grudzień 2022 r.

92 Komisja zaczęła podejmować działania w związku z zarzutami dotyczącymi nieuczciwej przewagi gospodarczej wynikającej z subsydiów zagranicznych. Takie subsydia mogą bowiem zakłócić funkcjonowanie rynku wewnętrznego, tworząc nierówne warunki konkurencji dla dostawców sieci 5G, co może mieć wpływ na bezpieczeństwo (zob. pkt ***78***).

93 Komisja nie posiada wystarczających informacji na temat podejścia państw członkowskich do kwestii ewentualnych kosztów zastąpienia, które mogłyby powstać, gdyby operatorzy sieci ruchomej zostali zobowiązani do wyeliminowania z unijnych sieci – bez okresu przejściowego – sprzętu od dostawców wysokiego ryzyka. Tymczasem różnice w podejściu do tej kwestii mogą podważyć pewność prowadzenia działalności gospodarczej i mieć negatywny wpływ na terminowe wdrożenie sieci 5G (zob. pkt ***79*** i ***80***). Co więcej, rozbieżne podejścia państw członkowskich do kwestii bezpieczeństwa sieci 5G, a w szczególności brak skoordynowanego podejścia na poziomie całej UE, mogą niekorzystnie wpływać na skuteczne funkcjonowanie jednolitego rynku. Do tej pory Komisja nie przeanalizowała jednak tej kwestii (zob. pkt ***74***–***76***).

Zalecenie 3 – Monitorowanie podejść państw członkowskich do kwestii bezpieczeństwa sieci 5G oraz analiza wpływu rozbieżności w tym zakresie na skuteczne funkcjonowanie jednolitego rynku

Komisja powinna:

a) promować przejrzyste i spójne podejście państw członkowskich do kwestii kosztów zastąpienia sprzętu 5G zakupionego przez operatorów sieci ruchomej od dostawców wysokiego ryzyka poprzez regularne monitorowanie i sprawozdawczość na ten temat w ramach wdrażania unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G;

b) przeanalizować, jaki wpływ na jednolity rynek miałaby budowa sieci 5G przez jedno państwo członkowskie z wykorzystaniem sprzętu pochodzącego od dostawcy uznanego przez inne państwo członkowskie za stwarzającego wysokie ryzyko.

Termin realizacji: grudzień 2022 r.

Niniejsze sprawozdanie zostało przyjęte przez Izbę II, której przewodniczy członkini Trybunału Obrachunkowego Iliana Ivanova, w Luksemburgu w dniu 15 grudnia 2021 r.

W imieniu Europejskiego Trybunału Obrachunkowego

Klaus-Heiner LEHNE
Prezes

Załączniki

Załącznik I – Główne szanse i zagrożenia związane z siecią 5G

SZANSE	ZAGROŻENIA
Rozwój nowych technologii przez przedsiębiorstwa	**Zagrożenia dla prywatności**
Większa mobilność i **modernizacja** systemu transportowego	**Zagrożenia** dla bezpieczeństwa narodowego
Dalsze **umożliwienie** wzajemnych połączeń między przedmiotami fizycznymi codziennego użytku	**Zależność** od łańcucha dostaw
Korzystanie na większą skalę z procesów elektronicznych w opiece zdrowotnej (e-zdrowie)	**Cyberataki**
Zwiększenie bezpieczeństwa obywateli	**Negatywne skutki** dla zdrowia
Wsparcie zmian zachodzących w korzystaniu z mediów przez społeczeństwo	**Utrata miejsc pracy** spowodowana wzrostem wydajności
Stymulowanie tworzenia miejsc pracy w wielu sektorach i **transformacja** rynku pracy	
Wzmocnienie demokracji	
Zmniejszenie przepaści cyfrowej	

Źródło: Europejski Trybunał Obrachunkowy na podstawie danych Biura Analiz Parlamentu Europejskiego – Europejskie Centrum Mediów Naukowych.

Załącznik II – Przykłady obrazujące skutki cyberincydentów i zakłóceń w działaniu sieci telekomunikacyjnych

Awaria numerów telefonów alarmowych we Francji[66,67]

01 3 czerwca 2021 r. awaria sieci w Orange, największej francuskiej firmie telekomunikacyjnej, uniemożliwiła wykonywanie połączeń na numery alarmowe przez kilka godzin. Chociaż wykluczono, że przyczyną był cyberatak, incydent ten pokazuje, jaki wpływ może mieć zakłócenie krytycznej infrastruktury sieciowej.

Ataki z użyciem oprogramowania typu ransomware na irlandzką publiczną służbę zdrowia[68,69,70]

02 W maju 2021 r. irlandzka służba zdrowia (Health Service Executive) wyłączyła wszystkie swoje systemy informatyczne z powodu ataku za pomocą oprogramowania ransomware. Atak ten miał wpływ na wszystkie aspekty opieki nad pacjentami, ponieważ spowodował trudności w dostępie do ich dokumentacji, zwiększając ryzyko opóźnień i błędów. Chociaż irlandzcy urzędnicy nie stwierdzili, by doszło do kradzieży danych pacjentów, upublicznienie dokumentacji zdrowotnej mogłoby doprowadzić do różnego rodzaju powiązanych przestępstw, takich jak oszustwa i szantaż. Według dyrektora generalnego służby zdrowia szacunkowe koszty wznowienia funkcjonowania systemów wyniosą prawdopodobnie 500 mln euro (600 mln dolarów amerykańskich).

---

66 https://www.euronews.com/2021/06/03/french-telecom-operator-orange-apologises-after-emergency-numbers-crash-nationwide

67 https://www.reuters.com/business/media-telecom/orange-blames-network-outage-software-failure-audit-2021-06-11/

68 https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875

69 https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

70 https://www.cert.europa.eu/cert/moreclusteredition/en/blog_DataBreachTodayinRSSSyndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds[71,72,73]

03 Solarwinds to amerykańska firma, która tworzy oprogramowanie dla przedsiębiorstw oraz agencji państwowych i federalnych, aby pomóc w zarządzaniu ich sieciami, systemami i infrastrukturą informatyczną. Na początku 2020 r. oprogramowanie firmy Solarwinds stało się obiektem ataku. Hakerom udało się również zaatakować klientów Solarwinds poprzez aktualizacje oprogramowania zawierające złośliwy kod. Kod ten umożliwił dostęp do platform klientów, ułatwiając ataki i instalację złośliwego oprogramowania i programów szpiegujących.

[71] https://www.solarwinds.com/

[72] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[73] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

Załącznik III – Ramy prawne i ramy polityki

Komisja Europejska

Rada Europejska / Rada UE

Prawodawstwo

Grupa współpracy ds. bezpieczeństwa sieci i informacji

2016 – Dyrektywa NIS, lipiec 2016 r. – zapewnienie środków prawnych w celu poprawy ogólnego poziomu cyberbezpieczeństwa w UE

2016 – Plan działania dotyczący sieci 5G, wrzesień 2016 r. – dążenie do uruchomienia usług 5G we wszystkich państwach członkowskich najpóźniej do końca 2020 r., a następnie szybka rozbudowa sieci w celu zapewnienia niezakłóconego zasięgu 5G na obszarach miejskich i wzdłuż głównych szlaków transportowych do 2025 r.

2018 – Europejski kodeks łączności elektronicznej, grudzień 2018 r. – dążenie do stworzenia rynku wewnętrznego w zakresie sieci i usług łączności elektronicznej

2019 – Konkluzje Rady Europejskiej, marzec 2019 r. – w oczekiwaniu na zalecenie Komisji w sprawie skoordynowanego podejścia do bezpieczeństwa sieci piątej generacji

2019 – Zalecenie w sprawie cyberbezpieczeństwa sieci 5G, marzec 2019 r. – zalecenie dla państw członkowskich dotyczące oceny zagrożeń dla cyberbezpieczeństwa mających wpływ na sieci 5G na szczeblu krajowym oraz dotyczące podjęcia niezbędnych środków bezpieczeństwa

2019 – Konkluzje Rady w sprawie znaczenia sieci 5G dla gospodarki europejskiej, grudzień 2019 r. – podkreślenie, że szybkie i bezpieczne wprowadzenie sieci 5G ma kluczowe znaczenie dla zwiększenia konkurencyjności UE i wymaga skoordynowanego podejścia w UE

2020 – Zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, styczeń 2020 r. – określenie ewentualnego wspólnego zestawu środków, które mogłyby złagodzić główne zagrożenia dla cyberbezpieczeństwa sieci 5G

2020 – Bezpieczne wprowadzenie sieci 5G w UE – wdrożenie unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, styczeń 2020 r. – Komisja Europejska zatwierdza zestaw narzędzi i wytycza kolejne kroki (np. sprawozdanie z wdrożenia do czerwca 2020 r.)

2020 – Konkluzje Rady w sprawie kształtowania cyfrowej przyszłości Europy, czerwiec 2020 r. – poparcie konieczności wdrożenia skoordynowanego podejścia w celu złagodzenia głównych zagrożeń z myślą o bezpiecznym wprowadzeniu sieci 5G w UE

2020 – Konkluzje Rady Europejskiej, październik 2020 r. – zatwierdzenie zestawu narzędzi cyberbezpieczeństwa sieci 5G, w szczególności konieczności stosowania odpowiednich ograniczeń w odniesieniu do dostawców wysokiego ryzyka

2020 – Zalecenie dotyczące [...] dostępu do widma radiowego 5G, wrzesień 2020 r. – określenie wytycznych dotyczących opracowania najlepszych praktyk w zakresie wspierania łączności i zapewnienia terminowego i sprzyjającego inwestycjom dostępu do widma radiowego 5G

2020 – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, grudzień 2020 r. – dokument prawa miękkiego, w którym określono priorytety Komisji i planowane działania w zakresie cyberbezpieczeństwa w ujęciu ogólnym, w tym sieci 5G

2020 – Wniosek dotyczący dyrektywy NIS 2, grudzień 2020 r. – ma na celu modernizację i rozszerzenie zakresu obecnej dyrektywy, obejmując również w bardziej wyraźny sposób cyberbezpieczeństwo sieci 5G

2020 – Wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych, grudzień 2020 r. – dążenie do zmniejszenia podatności na zagrożenia infrastruktur krytycznych, które mają zasadnicze znaczenie dla funkcjonowania społeczeństwa i gospodarki UE

2020 – Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, marzec 2021 r. – wyznaczenie drogi do wspólnej wizji i działań dla Europy w celu osiągnięcia sukcesu w cyfrowej dekadzie

2021 – Konkluzje Rady w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, marzec 2021 r. – wspieranie kolejnych kroków, które należy podjąć w zakresie cyberbezpieczeństwa sieci 5G, zgodnie ze strategią Komisji dotyczącą cyberbezpieczeństwa

Załącznik IV – Przykłady projektów współfinansowanych przez EFIS

Projekty dotyczące 5G realizowane w ramach EFIS

Obydwa projekty EFIS, które Trybunał poddał przeglądowi, dotyczyły inwestycji w badania, rozwój i innowacje z myślą o rozwoju portfela produktów sieci 5G. Obejmowały one rozwój sprzętu i oprogramowania dla sieci dostępu radiowego, jak również sieci szkieletowej. Projekty te przyczyniły się do gęstszego rozmieszczenia nadajników, wsparły standaryzację i ułatwiły przeprowadzenie kluczowych eksperymentów technologicznych.

Projekty zainicjowano w 2018 r., a zakończono w grudniu 2020 r. Całkowity koszt inwestycji w ich ramach wyniósł 3,9 mld euro, w tym 1 mld euro finansowania z EFIS.

Załącznik V – Przykłady projektów w ramach programu „Horyzont 2020” i EFRR

Projekt dotyczący 5G realizowany w ramach programu „Horyzont 2020”

W ramach tego projektu wykorzystywane są urządzenia wszystkich trzech głównych dostawców 5G (Ericsson, Huawei i Nokia) w celu testowania technologii 5G w transgranicznym korytarzu łączącym miasta Metz (Francja), Merzig (Niemcy) i Luksemburg. Projekt rozpoczęto w listopadzie 2018 r. i został zaplanowany na 31 miesięcy. UE przyznała na jego poczet 12,9 mln euro, przy czym całkowity budżet ma wynieść 17,1 mln euro.

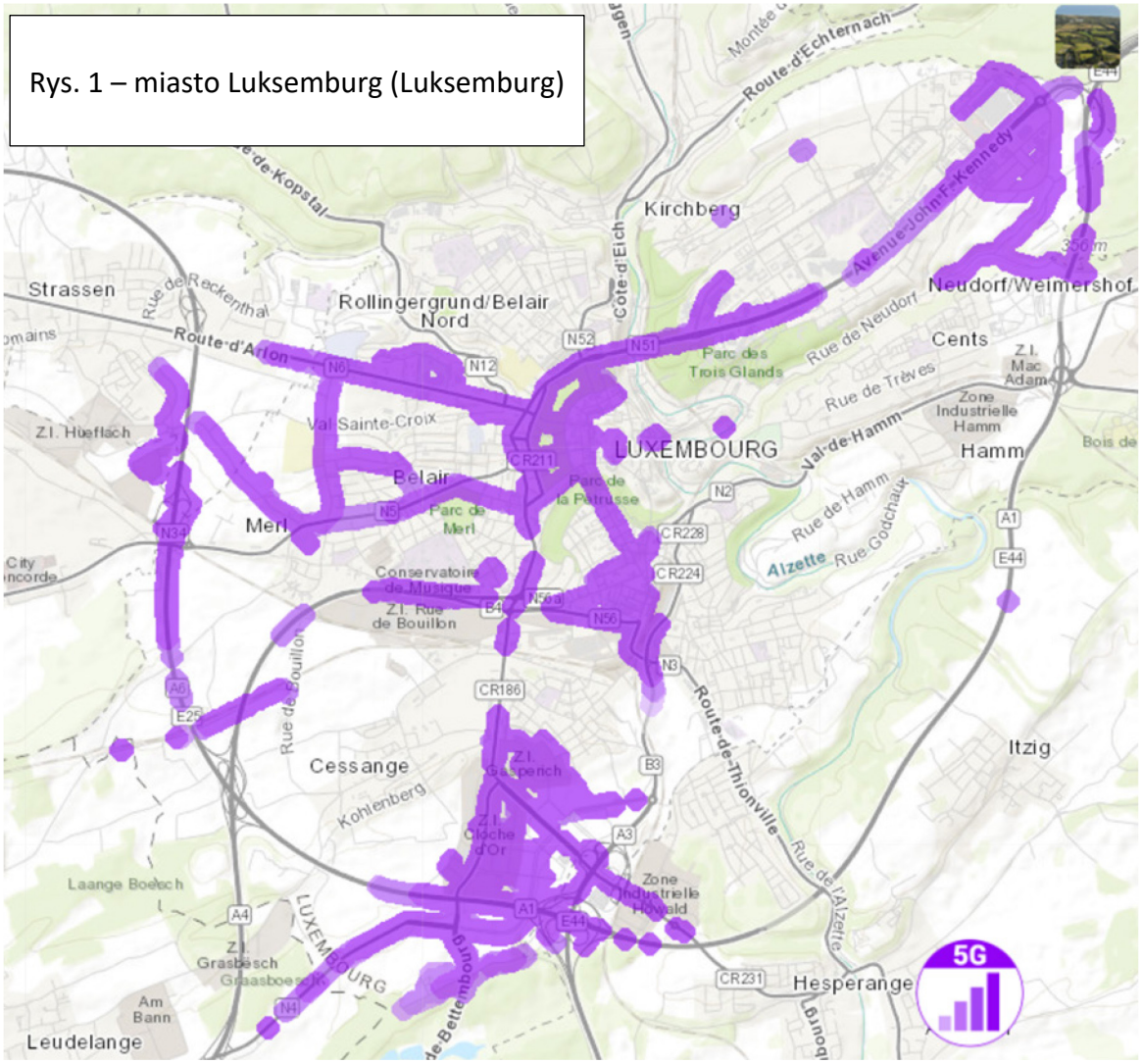
Projekt dotyczący 5G realizowany w ramach EFRR

Projekt ten, realizowany w Hiszpanii, ma na celu zapewnienie wiedzy na temat wdrażania sieci 5G. Obejmuje on eksperymentowanie z technikami zarządzania siecią, które można wprowadzić dzięki technologii 5G. Są to przykładowo wirtualizacja sieci, przetwarzanie brzegowe, dynamiczny przydział usług sieciowych lub warstwowanie sieci, a także opracowanie przypadków praktycznych użytkowania 5G. Projekt rozpoczęto w 2019 r. i został zaplanowany na 30 miesięcy. UE zapewniła wkład w kwocie 2,2 mln euro na poczet całkowitych przewidywanych kosztów w wysokości 7,1 mln euro.

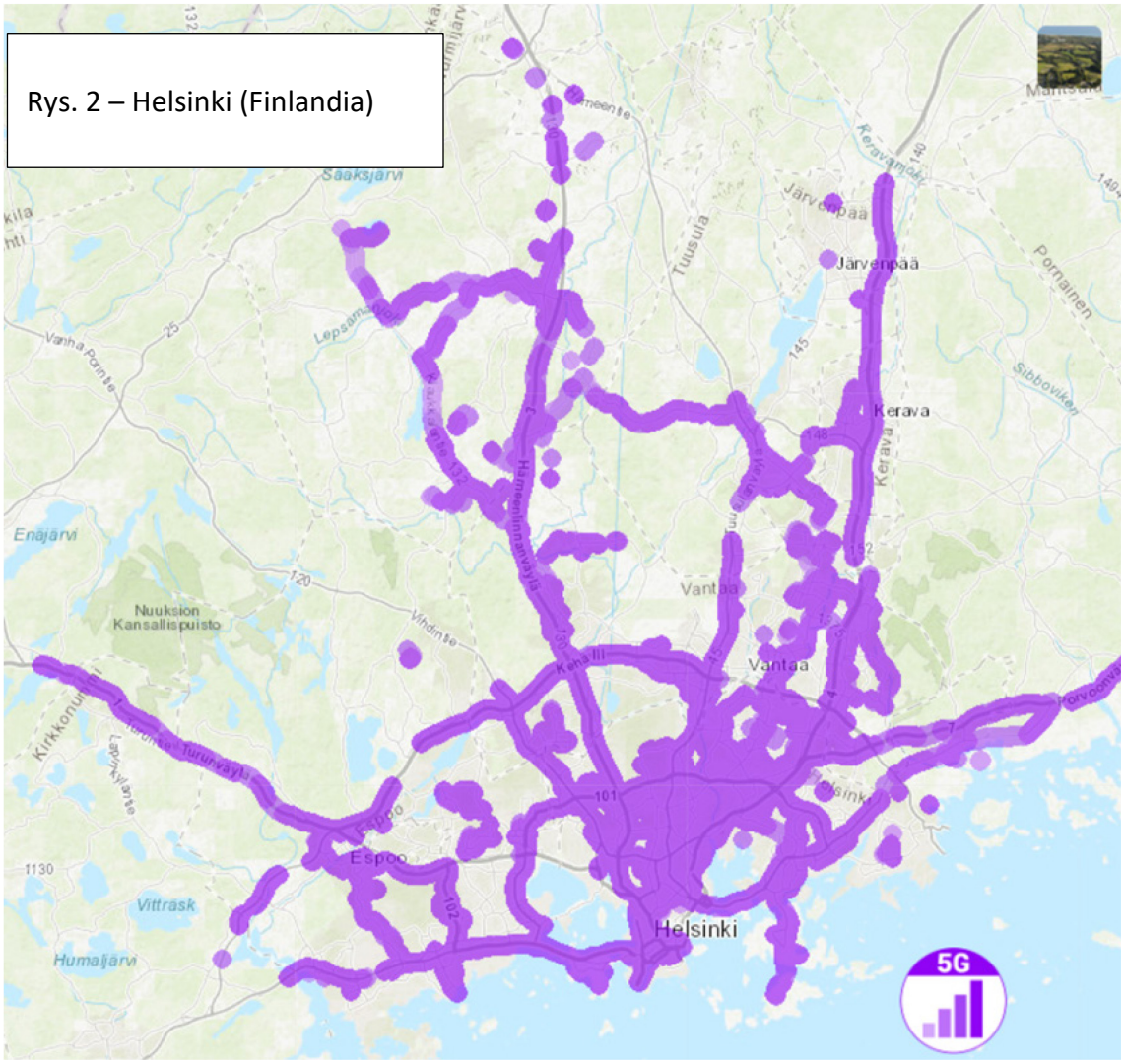
Załącznik VI – Zasięg 5G w wybranych miastach

Rysunki poniżej sporządzono na podstawie danych dotyczących łączności szerokopasmowej w sieciach ruchomych, zebranych na podstawie testów przeprowadzonych przez użytkowników aplikacji Nperf. Obszary, w których wykryto obecność sieci 5G, niekoniecznie są otwarte pod względem komercyjnym. Wydajność sieci zależy od poszczególnych operatorów sieci ruchomej, dlatego poniższe mapy, pobrane w dniu 4 października 2021 r., przedstawiają jedynie zasięg, a nie parametry takie jak prędkość przesyłu danych i opóźnienia.

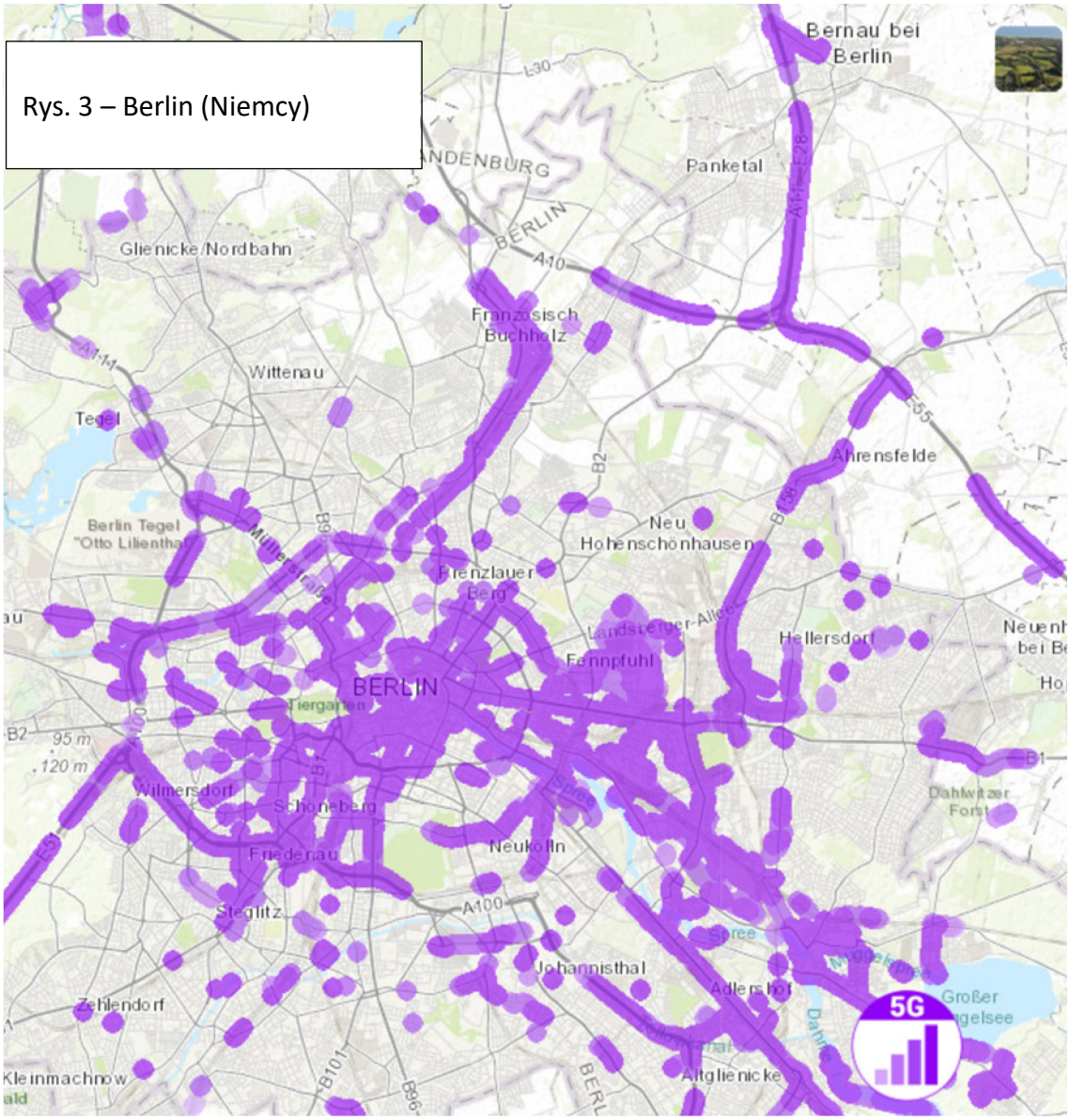
Rys. 1 – miasto Luksemburg (Luksemburg)



© nPerf.

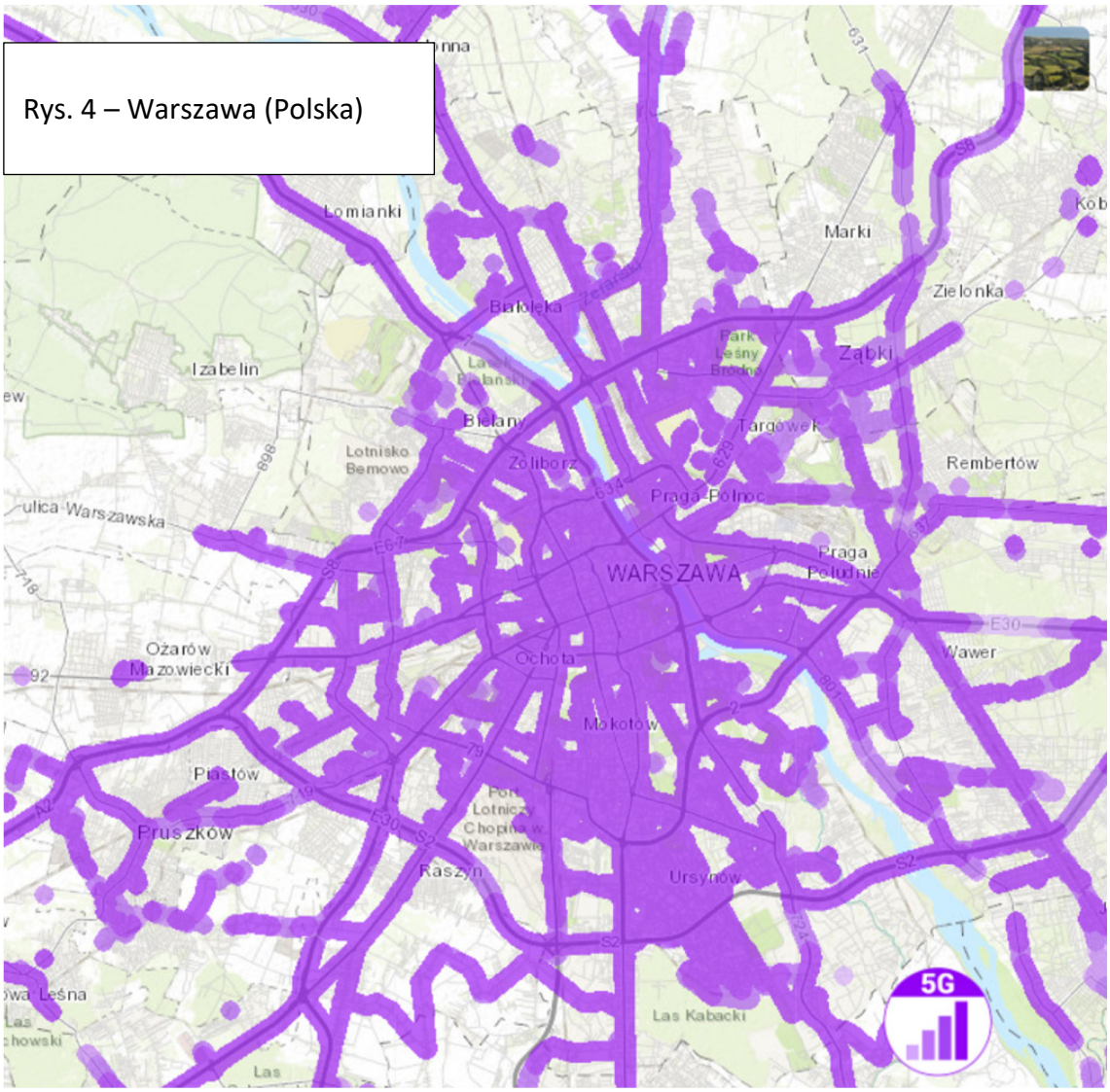

Rys. 2 – Helsinki (Finlandia)
Järvenpää
Kerava
Vantaa
Espoo
Helsinki
Nuuksion
Kansallispuisto
Enäjärvi
Vittrask
Humaljärvi
5G

© nPerf.

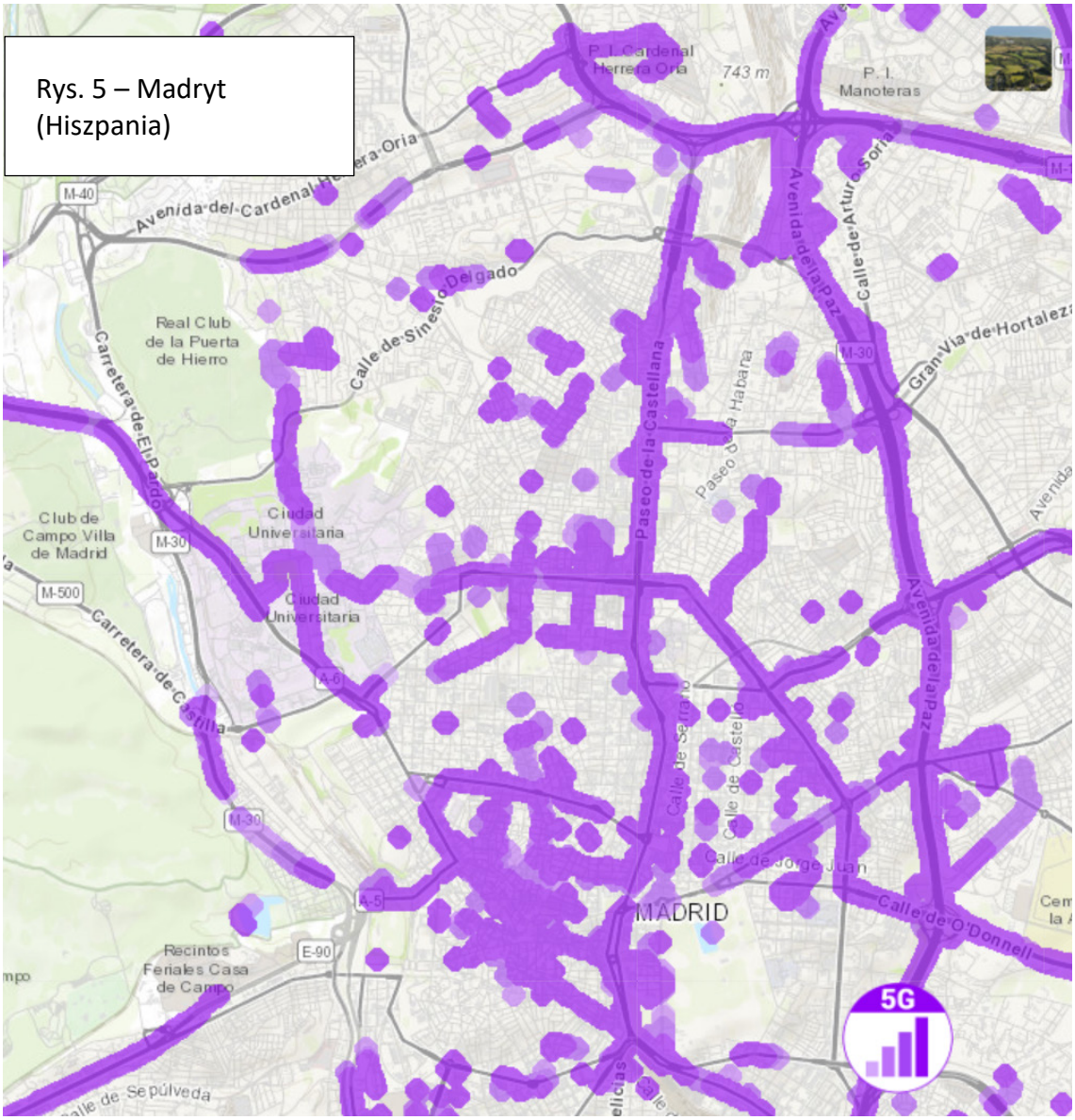


Rys. 3 – Berlin (Niemcy)

© nPerf.


Rys. 4 – Warszawa (Polska)
Łomianki
Marki
Zielonka
Białołęka
Izabelin
Bielany
Ząbki
Lotnisko Bemowo
Żoliborz
Targówek
Rembertów
Praga-Północ
ulica Warszawska
WARSZAWA
Praga-Południe
Ochota
Wawer
Ożarów Mazowiecki
Mokotów
Piastów
Pruszków
Raszyn
Ursynów
Las Kabacki
5G

© nPerf.



Rys. 5 – Madryt (Hiszpania)

Załącznik VII – Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, przyjęty przez grupę współpracy ds. bezpieczeństwa sieci i informacji i zatwierdzony przez Komisję, obejmuje trzy rodzaje niewiążących środków (środki strategiczne, techniczne i działania wspierające), które powinny zostać wdrożone przez różne podmioty, jak podsumowano poniżej.

Środki	Właściwe podmioty				
	Organy państw członkowskich	Operatorzy sieci ruchomej	Komisja Europejska	ENISA	Zainteresowane podmioty (w tym dostawcy)
Środki strategiczne					
SM01 – Wzmocnienie roli władz krajowych	✓	✓			
SM02 – Przeprowadzanie audytów u operatorów i żądanie informacji	✓	✓			
SM03 – Ocena profilu ryzyka dostawców i nakładanie ograniczeń w stosunku do dostawców uznanych za obarczonych wysokim ryzykiem, w tym zastosowanie niezbędnych wyłączeń w celu skutecznego zmniejszenia ryzyka w odniesieniu do kluczowych zasobów	✓	✓			
SM04 – Kontrolowanie korzystania z dostawców usług zarządzania i wsparcia trzeciej linii dostawców sprzętu	✓	✓			
SM05 – Zapewnienie różnorodności dostawców dla poszczególnych operatorów sieci ruchomej poprzez odpowiednie strategie z udziałem wielu dostawców	✓	✓			
SM06 – Zwiększenie odporności na szczeblu krajowym	✓	✓			
SM07 – Określenie kluczowych zasobów oraz wspieranie zróżnicowanego i zrównoważonego ekosystemu 5G w UE	✓		✓		
SM08 – Utrzymanie i rozwijanie różnorodności i potencjału UE w zakresie przyszłych technologii sieciowych	✓		✓		✓
Środki techniczne					
TM01 – Zapewnienie zastosowania podstawowych wymogów bezpieczeństwa (bezpieczny projekt i architektura sieci)	✓	✓			

Środki	Właściwe podmioty				
	Organy państw członkowskich	Operatorzy sieci ruchomej	Komisja Europejska	ENISA	Zainteresowane podmioty (w tym dostawcy)
TM02 – Zapewnienie środków bezpieczeństwa w istniejących standardach 5G i ocena ich wdrożenia	✓	✓			✓
TM03 – Zapewnienie ścisłej kontroli dostępu	✓	✓			
TM04 – Zwiększenie bezpieczeństwa wirtualnych funkcji sieciowych	✓	✓			
TM05 – Zapewnienie bezpiecznego zarządzania, obsługi i monitorowania w przypadku sieci 5G	✓	✓			
TM06 – Wzmocnienie bezpieczeństwa fizycznego	✓	✓			
TM07 – Wzmocnienie integralności oprogramowania oraz zarządzania aktualizacjami i pakietami naprawczymi	✓	✓			
TM08 – Podniesienie standardów bezpieczeństwa w procesach dostawców poprzez solidne warunki zakupów	✓	✓			✓
TM09 – Korzystanie z certyfikatu UE w przypadku komponentów sieci 5G, sprzętu klienta lub procesów dostawców	✓	✓	✓	✓	✓
TM10 – Korzystanie z certyfikatu UE w przypadku innych produktów i usług ICT niezwiązanych z 5G (urządzenia podłączone do sieci, usługi w chmurze)	✓		✓	✓	✓
TM11 – Wzmocnienie planów odporności i ciągłości usług	✓	✓			✓
Działania wspierające					
SA01 – Przegląd lub opracowywanie wytycznych i najlepszych praktyk w odniesieniu do bezpieczeństwa sieci	✓	✓		✓	
SA02 – Wzmocnienie zdolności w zakresie badań i audytu na szczeblu krajowym i unijnym	✓		✓	✓	
SA03 – Wspieranie i kształtowanie standaryzacji sieci 5G	✓	✓	✓	✓	✓
SA04 – Opracowanie wytycznych dotyczących wdrażania środków bezpieczeństwa w istniejących standardach 5G	✓			✓	
SA05 – Zapewnienie stosowania standardowych technicznych i organizacyjnych środków bezpieczeństwa poprzez specjalny ogólnounijny system certyfikacji	✓			✓	✓
SA06 – Wymiana najlepszych praktyk w zakresie wdrażania środków strategicznych, w szczególności krajowych ram oceny profilu ryzyka dostawców	✓				

Środki	Właściwe podmioty				
	Organy państw członkowskich	Operatorzy sieci ruchomej	Komisja Europejska	ENISA	Zainteresowane podmioty (w tym dostawcy)
SA07 – Poprawa koordynacji w zakresie reagowania na incydenty i zarządzania kryzysowego	✓			✓	
SA08 – Przeprowadzanie audytów współzależności pomiędzy sieciami 5G a innymi usługami krytycznymi	✓				
SA09 – Wzmocnienie mechanizmów współpracy, koordynacji i wymiany informacji	✓			✓	
SA10 – Zapewnienie, aby projekty dotyczące sieci 5G, które otrzymują wsparcie ze środków publicznych, uwzględniały ryzyko związane z cyberbezpieczeństwem	✓		✓		

Źródło: Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G.

Wykaz akronimów i skrótów

BEREC – Organ Europejskich Regulatorów Łączności Elektronicznej

EBI – Europejski Bank Inwestycyjny

EFIS – Europejski Fundusz na rzecz Inwestycji Strategicznych

EFRR – Europejski Fundusz Rozwoju Regionalnego

ENISA – Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

NIS – bezpieczeństwo sieci i informacji

PKB – produkt krajowy brutto

RAN – sieć dostępu radiowego

RRF – Instrument na rzecz Odbudowy i Zwiększania Odporności

RSPG – Zespół ds. Polityki Widma Radiowego

Glosariusz

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – agencja UE utworzona w celu rozwijania i utrzymywania wysokiego poziomu bezpieczeństwa sieci i informacji we wszystkich sektorach życia prywatnego i publicznego.

Eksabajt – miara pojemności przechowywania informacji cyfrowych, odpowiadająca miliardowi gigabajtów.

Europejski Fundusz na rzecz Inwestycji Strategicznych – mechanizm wsparcia inwestycyjnego utworzony przez Europejski Bank Inwestycyjny (EBI) i Komisję jako część planu inwestycyjnego dla Europy w celu pobudzenia prywatnych inwestycji w projekty o strategicznym znaczeniu dla UE.

Global System for Mobile Communications Association (GSMA) – organizacja branżowa reprezentująca interesy operatorów sieci łączności ruchomej z całego świata, a także firm produkcyjnych i usługowych oraz organizacji zainteresowanych infrastrukturą ruchomą.

Grupa współpracy ds. bezpieczeństwa sieci i systemów informatycznych – organ ustanowiony na mocy dyrektywy NIS w celu zapewnienia współpracy i wymiany informacji pomiędzy państwami członkowskimi. W jego skład wchodzą przedstawiciele państw członkowskich UE, Komisji Europejskiej oraz Agencji Unii Europejskiej ds. Cyberbezpieczeństwa.

Internet rzeczy – obiekty fizyczne wyposażone w czujniki, oprogramowanie i inne technologie, które umożliwiają im bezprzewodowe połączenie i wymianę danych z innymi urządzeniami i systemami.

Krajowe plany szerokopasmowe – dokumenty państw członkowskich wytyczające strategiczne kierunki działań z myślą o osiągnięciu unijnych celów w zakresie łączności szerokopasmowej.

Operator sieci ruchomej – firma telekomunikacyjna, która zapewnia bezprzewodową komunikację głosową i transmisję danych dla użytkowników telefonów komórkowych korzystających z jej usług.

Opóźnienie – w sieciach komputerowych: czas wymagany dla przemieszczenia się zbioru danych między dwoma punktami.

Oprogramowanie typu ransomware – złośliwe oprogramowanie, które pozbawia ofiarę dostępu do systemu komputerowego lub uniemożliwia odczytanie plików, zmuszając ją do zapłacenia okupu w celu przywrócenia dostępu.

Organ Europejskich Regulatorów Łączności Elektronicznej – organ składający się z przedstawicieli krajowych organów regulacyjnych państw członkowskich, który wspiera te organy i Komisję we wdrażaniu ram regulacyjnych UE w celu stworzenia jednolitego rynku łączności elektronicznej.

Sieci szerokopasmowe – szybka, jednoczesna transmisja wielu formatów informacji (takich jak dane, głos i wideo).

Sieć dostępu radiowego – główny element nowoczesnej technologii telekomunikacyjnej, łączący poszczególne urządzenia z innymi częściami sieci za pomocą połączeń radiowych.

Widmo radiowe – część widma elektromagnetycznego odpowiadająca częstotliwościom radiowym.

Zespół ds. Polityki Widma Radiowego – grupa doradcza wysokiego szczebla, składająca się z przedstawicieli państw członkowskich, która wspiera instytucje UE i doradza im w zakresie rozwoju jednolitego rynku produktów i usług bezprzewodowych.

Odpowiedzi Komisji

https://www.eca.europa.eu/pl/Pages/DocItem.aspx?did=60614

Kalendarium

https://www.eca.europa.eu/pl/Pages/DocItem.aspx?did=60614

Zespół kontrolny

Sprawozdania specjalne Trybunału prezentują wyniki kontroli dotyczących obszarów polityki i programów unijnych bądź kwestii związanych z zarządzaniem w wybranych obszarach budżetowych. Trybunał wybiera i opracowuje zadania kontrolne tak, aby osiągnąć jak największe oddziaływanie, biorąc przy tym pod uwagę kryteria takie jak zagrożenia dla wykonania zadań lub zgodności, poziom dochodów lub wydatków w danym obszarze, nadchodzące zmiany oraz interes polityczny i społeczny.

Niniejsza kontrola wykonania zadań została przeprowadzona przez Izbę II zajmującą się takimi obszarami wydatków jak inwestycje na rzecz spójności, wzrostu i włączenia społecznego. Izbie tej przewodniczy członkini Trybunału Iliana Ivanova. Niniejszą kontrolą kierowała członkini Trybunału Annemie Turtelboom, a w działania kontrolne zaangażowani byli: Florence Fornaroli, szefowa gabinetu i Celil Ishik, attaché; Niels-Erik Brokopp, kierownik; Paolo Pesce, koordynator zadania, oraz kontrolerzy: Jussi Bright, Rafał Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov i Nils Westphal.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7408-1	ISSN 1977-5768	doi:10.2865/130076	QJ-AB-21-029-PL-N
HTML	ISBN 978-92-847-7388-6	ISSN 1977-5768	doi:10.2865/859912	QJ-AB-21-029-PL-Q

Szacuje się, że w latach 2021–2025 technologia 5G doprowadzi do wzrostu europejskiego PKB o 1 bln euro i może przyczynić się do stworzenia lub przekształcenia nawet 20 mln miejsc pracy we wszystkich sektorach gospodarki. Kontrolerzy Trybunału zauważyli, że opóźnienia we wdrażaniu sieci 5G zagrażają osiągnięciu celów UE w tym zakresie, a ponadto konieczne są dalsze wysiłki, by wyeliminować problemy dotyczące bezpieczeństwa. W związku z tym w sprawozdaniu przedstawili oni szereg zaleceń skierowanych do Komisji, które mają przyczynić się do sprawniejszego wdrażania bezpiecznych sieci 5G w UE w terminowy i skoordynowany sposób.

Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego przedstawiono na mocy art. 287 ust. 4 akapit drugi TFUE.

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

Urząd Publikacji Unii Europejskiej

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
12 rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Formularz kontaktowy: eca.europa.eu/pl/Pages/ContactForm.aspx
Strona internetowa: eca.europa.eu
Twitter: @EUAuditors