Analiza KBN

Nr 7 (59) / 2020 17 kwietnia 2020 r.

5G w roku COVID-19: jak pandemia wpłynie na polityczną dyskusję o budowie 5G w Europie?

Michał Rekowski

W ostatnich dniach media zapełniły się doniesieniami z Wielkiej Brytanii o podpalaniu masztów stacji bazowych, na których opiera się sieć piątej generacji (w skrócie 5G). Związane jest to z popularną od pewnego czasu teorią spiskową, jakoby rozprzestrzenianie się wirusa SARS-CoV-2 wywoływane było przez fale radiowe wykorzystywane przez 5G. Nie jest to pierwsza – kompletnie nienaukowa – teoria spiskowa dotycząca 5G. Zanim pojawił się koronawirus, 5G oskarżano m.in. o bezpośrednie zagrożenie dla ludzkiego życia, eksterminację ptaków czy nawet kontrolę myśli. Tym niemniej, pandemia koronawirusa może w dłuższej perspektywie rzeczywiście wiązać się z szybszą budową i wdrożeniem sieci 5G w Europie, jednak z zupełnie innych powodów.

Rozwój 5G w Unii Europejskiej

Kwestia wdrożenia technologii i budowy infrastruktury 5G w Unii Europejskiej mieści się w strategii jednolitego rynku cyfrowego przyjętej przez Komisję Europejską w 2015 r. Obejmuje szeroki strumień polityk cyfrowych dotyczących zagadnień tak różnych, jak: budowa infrastruktury szerokopasmowej, usługi cyfrowe, ochrona danych czy cyberbezpieczeństwo. W obrębie Komisji zajmuje się nią przede wszystkim Dyrekcja Generalna ds. Sieci

Komunikacyjnych, Treści i Technologii (DG CONNECT) pod przewodnictwem politycznym komisarza ds. wewnętrznego rynku Thierry'ego Bretona oraz wiceprzewodniczącej Komisji (a zarazem komisarz ds. konkurencji) Margrethe Vestager. Kieruje ona pracami zespołu komisarzy *Europa na miarę ery cyfrowej,* który bierze swą nazwę od jednego z czterech priorytetów obecnej Komisji Europejskiej (KE), i zajmuje się całym spektrum spraw związanych z 5G: od proponowania unijnych regulacji widma radiowego po standardy cyberbezpieczeństwa. Na poziomie jednostek organizacyjnych w DG CONNECT, urzędnicy Komisji prowadzą konsultacje w kwestiach merytorycznych z przedstawicielami społeczeństwa obywatelskiego, przemysłu, grup lobbingowych i innymi aktorami poza-instytucjonalnymi. Jednocześnie, w ramach procesu przygotowania treści propozycji legislacyjnych przez KE, dochodzi do konsultacji z innymi instytucjami UE. W tym kontekście istotnymi podmiotami są: Agencja UE ds. Cyberbezpieczeństa (ENISA) w zakresie cyberbezpieczeństwa, Urząd Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC) w zakresie regulacji, oraz *Radio Spectrum Policy Group* (RSPG) i *EU-5G Observatory* w zakresie obserwacji rynku. Dodatkowo, dyrektywa o bezpieczeństwie sieci i systemów informatycznych (tzw. dyrektywa NIS – 2016/1148) powołała Grupę ds. Współpracy (ang. *Cooperation Group*) składającą się przedstawicieli Komisji, ENISA oraz państw członkowskich, której celem jest utworzenie platformy współpracy w zakresie cyberbezpieczeństwa pomiędzy instytucjami UE i państwami członkowskimi.

Początkowo kwestia wdrożenia technologii 5G była przedstawiana przez Komisję Europejską głównie jako szansa na przyspieszenie rozwoju ekonomicznego, które zrewolucjonizuje wszystkie gałęzi gospodarki i stworzy całkowicie nowe modele biznesowe. W słowach Neelie Kroes, komisarz odpowiedzialnej za agendę cyfrową w latach 2010-2014: „5G jest kluczem do nowego paradygmatu, do połączonego społeczeństwa, do Internetu Rzeczy. Umożliwi ono zupełnie nowe pola zastosowań i nowych rozwiązań dla społeczeństwa". W podobnie optymistycznym tonie w 2013 roku komisarz Kroes ogłosiła szereg projektów badawczych dotyczących technologii 5G w ramach programu Horyzont 2020, na które przeznaczono wówczas z funduszy UE 700 milionów euro. Również w 2013 r. Komisja powołała Stowarzyszenie Przemysłowe 5G (*5G Industrial Association*), którego zadaniem było przyspieszenie budowy 5G w Europie (oprócz europejskich firm członkami stowarzyszenia zostały także chińskie Huawei i ZTE). Tym inicjatywom towarzyszyło także zawarcie międzynarodowych partnerstw w zakresie rozwoju technologii 5G, najpierw z Republiką Korei w 2014 r., a następnie z Japonią i Chińską Republiką Ludową w 2015 roku. W oficjalnym komunikacie wskazano, że Chiny są „największym światowym rynkiem technologii, produktów i usług 5G" i podkreślano potencjalne zyski czekające w Chinach na europejskich dostawców tej technologii. Entuzjastyczny ton dotyczący 5G został pierwotnie podtrzymany przez Komisję J.-C. Junckera (2014-2019), m.in. w 2015 roku ówczesny komisarz odpowiedzialny za portfolio cyfrowe, Günther Oettinger w przemówieniu pt. „Droga do 5G" podczas Mobile World Congress w Barcelonie odnosił się do 5G jako rewolucyjnej technologii, która „stanie się systemem nerwowym społeczeństwa cyfrowego i gospodarki cyfrowej" i z której będzie korzystał każdy. Ta optymistyczna narracja znalazła swoje odbicie także w głównych dokumentach UE przyjętych w następnych latach, m.in. w komunikacie KE pt. „Sieć 5G dla Europy: Plan działania" z 2016 r., czy rezolucji PE z 2017 r. pt. „Europejskie społeczeństwo

gigabitowe i 5G". W tych i podobnych dokumentach z tamtego okresu widoczny jest brak odniesień do zagrożeń cyberbezpieczeństwa wynikających z budowy sieci 5G, szczególnie przy użyciu dostawców sprzętu i usług pochodzących spoza Unii, chociaż należy zauważyć, że ENISA już w 2015 roku opublikowała studium przedstawiające taksonomię zagrożeń cyberbezpieczeństwa związanych z rozwojem 5G.

5G jako front globalnej rywalizacji mocarstw

Wśród producentów sprzętu tworzącego infrastrukturę 5G uformowało się grono globalnych liderów: Huawei posiada ok. 30% udziałów w globalnej infrastrukturze 5G, Samsung - 23,3%; Ericsson - 20,3%; Nokia - 13,6%. Wśród pozostałych istotnych graczy rynkowych znajdują się także: chiński ZTE oraz amerykańskie Cisco i Qualcomm, w zależności od dostarczanych komponentów. Od dwóch lat Huawei promuje się jako zdecydowany lider wyścigu w rozwoju 5G oraz dostarczyciel tańszej i bardziej dojrzałej technologii. Jednocześnie towarzyszy temu wzrost publicznie wyrażanych przez przedstawicieli amerykańskich i europejskich instytucji obaw o bezpieczeństwo sieci budowanej w oparciu o sprzęt dostarczany przez chińskich producentów. Dyskusja o cyberbezpieczeństwie sieci 5G jest przejawem geopolitycznej rywalizacji mocarstw, która w coraz większym stopniu rozgrywa się na polu nowych technologii cyfrowych.

W Stanach Zjednoczonych ofensywa przeciwko Huawei zaczęła się w pierwszej połowie 2018 roku, gdy m.in. w maju Departament Obrony zabronił sprzedaży telefonów produkcji tej firmy (oraz telefonów ZTE) na terenie amerykańskich baz wojskowych, jednocześnie ostrzegając tych, którzy już taki sprzęt posiadali przed zagrożeniami bezpieczeństwa wiążącymi się z używaniem produktów tych dwóch chińskich firm. Z kolei w sierpniu 2018 r. prezydent Donald Trump podpisał przyjęty uprzednio przez Kongres Stanów Zjednoczonych dokument określający budżet obronny i zasady jego wydatkowania na 2019 rok (*National Defense Authorization Act 2019*), który wprowadzał dla amerykańskiej administracji zakaz używania bądź kupowania usług oraz sprzętu telekomunikacyjnego od Huawei, ZTE i szeregu innych chińskich firm (m. in. Hytera Communications Corporation, Hikvision oraz Dahua Technology). Co istotne, zakaz odnosił się także do podwykonawców zatrudnianych przez amerykańskie instytucje i organy rządowe. Warto dodać, iż rząd amerykański już od kilku lat podnosił kwestię zagrożeń związanych z korzystaniem z usług i sprzętu tych chińskich dostawców. W 2012 roku Stała Specjalna Komisja do spraw Wywiadu w Izbie Reprezentantów Kongresu USA przygotowała i opublikowała raport śledczy dotyczący zagrożeń dla bezpieczeństwa narodowego USA związanych z firmami Huawei i ZTE. W kwietniu 2018 roku Departament Handlu zakazał amerykańskim firmom sprzedaży podzespołów dla ZTE z powodu niezastosowania się do środków wymuszonych przez amerykańską administrację za naruszenie w 2017 roku sankcji nałożonych na Iran i Koreę Północną.

Wkrótce podobne działania zaczęli podejmować inni sojusznicy USA. W sierpniu 2018 r. rząd Australii ogłosił, iż będzie oczekiwał od dostawców usług telekomunikacyjnych wykluczenia z budowy sieci 5G firm, które mogą podlegać naciskom ze strony obcego rządu sprzecznym z australijskim prawem. Zostało to usankcjonowane poprzez reformę prawa dotyczącego bezpieczeństwa sektora telekomunikacyjnego miesiąc później. Jednocześnie australijski

oddział Huawei ogłosił, iż został poinformowany przez władze kraju o zakazie udziału w budowie sieci 5G w Australii. W grudniu 2018 r. nowozelandzka agencja wywiadowcza GCSB tymczasowo zabroniła lokalnej firmie telekomunikacyjnej Spark kontynuowania budowy sieci 5G przy użyciu sprzętu Huawei, powołując się na „znaczące ryzyko dla bezpieczeństwa sieci".

Wydarzenia te zbiegły się z aresztowaniem Meng Wanzhou, dyrektor finansowej Huawei, do którego doszło w grudniu 2018 r. w Kanadzie na wniosek administracji USA. W ślad za pozaeuropejskimi sojusznikami USA kolejne kraje europejskie zaczęły podnosić kwestię bezpieczeństwa sieci 5G w kontekście wykorzystania urządzeń pochodzących od chińskich producentów. Pod koniec 2018 r. czeskie Narodowe Centrum Cyberbezpieczeństwa (NÚKIB) wydało komunikat, w którym stwierdzało, iż wykorzystanie produktów Huawei i ZTE stanowi zagrożenie dla cyberbezpieczeństwa. Kilka miesięcy wcześniej, działający w Wielkiej Brytanii ośrodek Huawei Cyber Security Evaluation Centre (HCSEC) wydał raport, w którym stwierdzał odkrycie potencjalnego ryzyka wynikającego z procesu produkcyjnego Huawei. Samo HCSEC zostało powołane w 2010 roku jako wspólna inicjatywa Huawei i rządu Zjednoczonego Królestwa (na czele jego rady nadzorczej stoi prezes brytyjskiej agencji cyberbezpieczeństwa - NCSC), której zadaniem jest monitorowanie bezpieczeństwa sieci w związku z udziałem Huawei w brytyjskiej infrastrukturze telekomunikacyjnej. Z kolei w Polsce na początku 2019 r. miało miejsce aresztowanie dyrektora polskiego oddziału Huawei pod zarzutem szpiegostwa.

Wydarzenia te przyczyniły się do wzmożenia europejskiej debaty nad bezpieczeństwem sieci 5G w związku z udziałem chińskich dostawców w krajowych planach rozwoju 5G w państwach Unii Europejskiej. W marcu 2019 r. Parlament Europejski wydał rezolucję dotyczącą „zagrożeń dla bezpieczeństwa związanych z rosnącą obecnością technologiczną Chin w UE", która nie tylko wskazywała na chińskich dostawców sprzętu 5G jako potencjalne źródło zagrożeń, ale też wzywała państwa członkowskie do podjęcia działań zwiększających ich bezpieczeństwo w tym kontekście. Także w marcu 2019 r. na wniosek Parlamentu Europejskiego Komisja wydała swoje rekomendacje dotyczące cyberbezpieczeństwa sieci 5G i podjęła współpracę z państwami członkowskimi przy przygotowaniu oceny ryzyka związanego z rozwojem sieci 5G na terenie Unii Europejskiej. Taki raport, przygotowany wspólnie przez państwa członkowskie, Komisję i ENISA został opublikowany w październiku 2019 roku. Zidentyfikował on 9 obszarów ryzyka związanego z bezpieczeństwem sieci 5G m. in. możliwość wrogiego wykorzystania łańcuchów dostaw czy wykorzystania zwiększonej podatności na ataki urządzeń w opartym o 5G Internecie Rzeczy przez aktorów państwowych. W kolejnym kroku Komisja Europejska 29 stycznia 2020 roku opublikowała „Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G" (powszechnie zwany *toolboxem*). Celem *toolboxu* jest wypracowanie wspólnego unijnego podejścia do kwestii budowy 5G, co w szczególności oznacza określenie wspólnego zestawu środków ograniczenia ryzyka, jakie mogą być stosowane przez państwa członkowskie w obliczu potencjalnych zagrożeń cyberbezpieczeństwa. W odniesieniu do 9 obszarów ryzyka zidentyfikowanych w raporcie z października 2019 r. dokument proponuje 8 środków strategicznych, 11 środków technicznych oraz 10 działań wspierających. Państwa członkowskie mogą nałożyć wzmocnione zobowiązania na krajowych operatorów sieci w odniesieniu do konieczności uwzględnienia bezpieczeństwa narodowego, ryzyka związanego z możliwością ingerencji kraju trzeciego

w łańcuchy dostaw, unikania uzależnienia od jednego dostawcy i bezpieczeństwa samego sprzętu. Co więcej, państwa członkowskie mogą także ograniczyć udział podmiotów w dostarczaniu kluczowych elementów sieci (takich jak np. funkcje zarządzania i dostępu do sieci). W efekcie oznacza to możliwość wykluczenia przez państwa członkowskie z krajowych planów budowy 5G (na mocy przyjętych kryteriów oceny - np. we wzajemnym porozumieniu lub współdziałaniu z krajowymi operatorami sieci komórkowych) podmiotów, które zostaną powiązane z wysokim stopniem ryzyka. Jednocześnie *toolbox* pozostawia jednak decyzję o podjęciu takiego kroku administracjom rządom państw członkowskich. Zgodnie z założonymi ramami czasowymi, do końca kwietnia 2020 r. państwa członkowskie muszą wdrożyć zestaw strategicznych, technicznych i wspierających środków umieszczonych w *toolboxie,* zaś do końca czerwca 2020 r. Grupa ds. Współpracy ma przedstawić raport ze stanu ich implementacji w każdym państwie UE.

Tymczasem od początku debaty nad potencjalnym wykluczeniem Huawei z przetargów na budowę 5G w Europie, z wielu stolic docierają sprzeczne sygnały odnośnie do ich planów w tej kwestii. Niektóre rządy nie decydują się na zdecydowane kroki pomimo ostrzeżeń i rekomendacji zgłaszanych przez krajowe instytucje bezpieczeństwa. Tak było m.in. w Niemczech, gdzie jeszcze jesienią 2019 roku szef Federalnej Służby Wywiadowczej Bruno Kahl zalecał stanowcze wykluczenie Huawei z rozwoju niemieckiej sieci. Po zaciekłej debacie na forum rządzącej Unii Chrześcijańsko-Demokratycznej (CDU), kanclerz Angeli Merkel udało się wreszcie w lutym przekonać większość członków jej partii do przyjęcia stanowiska, które nie przewiduje eliminacji Huawei z budowy 5G, choć nawet wtedy nie zabrakło głośnych głosów sprzeciwu wśród zarówno posłów z CDU, jak i z kolejnych dwóch największych partii: koalicyjnej SPD i opozycyjnych Zielonych, które stanowczo opowiadały się za wykluczeniem Huawei. We Francji w lutym 2020 r. minister gospodarki i finansów Bruno Le Maire powiedział, że Huawei nie zostanie wykluczony z krajowych planów rozwoju 5G, zaś w marcu br. agencja Reutera doniosła, że również francuska agencja cyberbezpieczeństwa ANSSI zdecydowała się przychylić się do tego stanowiska i zalecić jedynie ograniczenie udziału tej firmy w budowie 5G do tzw. niekluczowych elementów sieci. Podobne stanowisko przedstawił w styczniu br. brytyjski premier Boris Johnson. W Wielkiej Brytanii, gdzie dyskusja nad potencjalnymi zagrożeniami związanymi z wykorzystaniem sprzętu od producenta z Shenzhen trwa od dawna, w marcu br. doszło do kryzysu w rządzącej Partii Konserwatywnej, gdy 36 posłów odmówiło zagłosowania za rządową poprawką do ustawy telekomunikacyjnej. Wyrazili w ten sposób sprzeciw wobec stanowiska premiera Johnsona, który ogłosił na początku roku, iż Huawei zostanie w ograniczonym stopniu dopuszczony do budowy brytyjskiej sieci. Zbuntowani Torysi powoływali się na niski poziom zaufania wobec tej firmy i obawy dotyczące potencjalnego zagrożenia bezpieczeństwa narodowego, powszechne wśród wszystkich anglosaskich sojuszników Zjednoczonego Królestwa. Z kolei we Włoszech, pomimo poważnych zastrzeżeń dotyczących bezpieczeństwa sprzętu Huawei zgłoszonych w grudniu 2019 roku przez parlamentarną komisję ds. wywiadu, wiceminister przemysłu Mirella Liuzzi poinformowała w styczniu br., że nie ma planów wykluczenia Huawei z krajowej budowy 5G. Natomiast żadnych ograniczeń Huawei nie spotyka na Węgrzech, gdzie spółka z Shenzhen zawarła jeszcze w 2019 r. porozumienie z węgierskim rządem o partnerstwie w rozwoju i budowie 5G.

5G a COVID-19

Pomimo szerzących się ataków na stacje bazowe w Europie, rządy nie wykorzystują kryzysu społecznego wywołanego SARS-CoV-2 do odwrócenia uwagi obywateli od przyspieszonych prób budowy infrastruktury 5G. Wręcz przeciwnie – wiele wskazuje na to, że pandemia opóźni proces rozwoju 5G w roku, który miał przynieść pierwsze spektakularne przykłady aplikacji tej technologii. Tym niemniej, gdy gospodarki i rządy wejdą w proces uporządkowanego wychodzenia z kryzysu proces budowy 5G znów może przyspieszyć, także w Europie. Obecny kryzys społeczno-gospodarczy wywołany pandemią COVID-19 doprowadził do przeniesienia wielu procesów gospodarczych, społecznych i politycznych do sieci. Nagle aplikacje takie jak Microsoft Teams, Skype, Zoom czy Webex stały się elementami infrastruktury krytycznej, bez której niemożliwe byłyby działania firm, organizacji pozarządowych, mediów czy rządów i administracji państwowej. Wszystkie kluczowe procesy i funkcje społeczne - od edukacji po dyplomację - zostały przestawione w tryb online. Można się spodziewać, że to gwałtowne przyspieszenie rewolucji cyfrowej nie wyhamuje nawet po ustaniu pandemii. Potrzeba dostępu do precyzyjnych danych, informacji i wysokoprzepustowej łączności, o której pisze m.in. Aleksander Poniewierski, wymusi szybsze i bardziej zdecydowane działania zmierzające do budowy Internetu Rzeczy i trwałej cyfryzacji wielu gałęzi gospodarki i administracji. Wdrażanie rozwiązań administracyjnych i korporacyjnych w oparciu o technologię chmury (*cloud computing*) stanie się koniecznością, podobnie jak coraz częstsze wykorzystanie automatyzacji w sferze publicznej: od diagnostyki medycznej po administrację. To z kolei przyspieszy proces budowy sieci 5G na świecie, w tym w Europie.