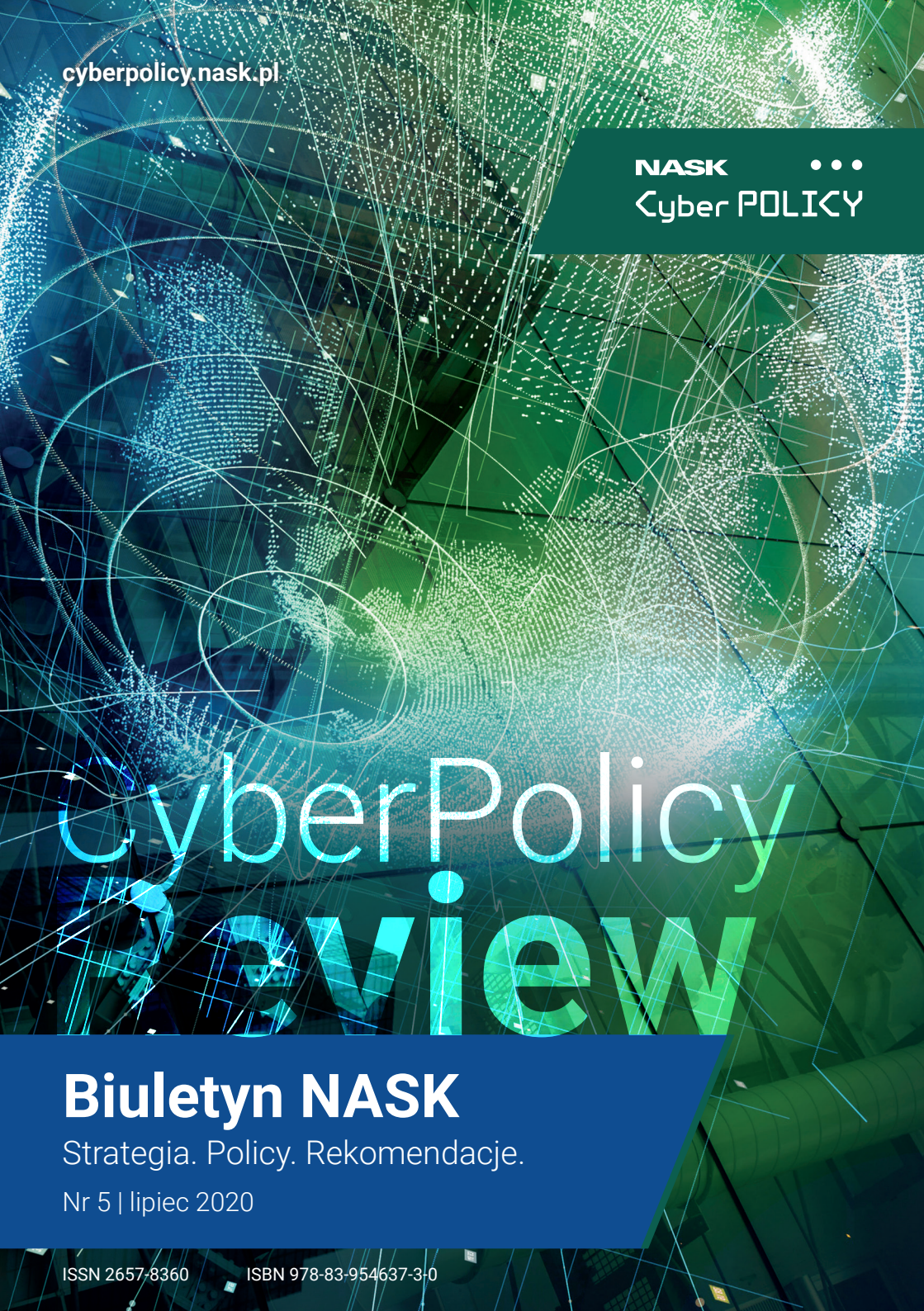


Biuletyn NASK

Strategia. Policy. Rekomendacje.

Nr 5 | lipiec 2020

ISSN 2657-8360 ISBN 978-83-954637-3-0

NASK Cyber POLICY

Biuletyn NASK

Strategia. Policy. Rekomendacje.

5 G – technologia i polityka

Nr 5 | lipiec 2020

Redakcja: dr Magdalena Wrzosek

Opracowanie graficzne: Piotr Klicki

NASK PIB | Warszawa | 2020

ISSN 2657-8360

978-83-954637-3-0

ISBN 978-83-954637-3-0

9 788395 463730

Słowo wstępu

To już piąty numer Biuletynu *CyberPolicy Review.* Wraz z rozwojem wydawnictwa, zdecydowaliśmy, że każdy kolejny numer będzie zorientowany wokół konkretnego tematu. Tym razem będzie to sieć 5G, w szczególności w aspekcie cyberbezpieczeństwa.

W zeszłym roku mało było tematów, które tak bardzo elektryzowały dyskusję publiczną i technologiczną jak sieć 5G. Bardzo istotnym elementem tej dyskusji stała się debata na temat kwestii bezpieczeństwa oraz kontekst suwerenności cyfrowej. Na przykładzie sieci nowych generacji bardzo wyraźnie widać też, jak technologia wkracza w wielką politykę i gospodarkę oraz w jaki sposób poszczególne państwa podejmują to wyzwanie. Dlatego proponujemy Państwu, z jednej strony wybór tekstów ekspertów z NASK oraz Instytutu Łączności, ale także głos pochodzący z rynku (firma IS-Wireless oraz Samsung). Na koniec pokazujemy kontekst geopolityczny i prezentujemy analizy ekspertów z Ośrodka Studiów Wschodnich na temat tego, jak wyzwania związane z siecią 5G są adresowane w Niemczech, Rosji i Chinach.

Zapraszam do lektury.

Krzysztof Silicki
Zastępca Dyrektora NASK PIB
– Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Spis treści

Słowo wstępu **2**

5G, a sprawa Polska. Komentarz NASK **5**

Sieć 5G, czyli (r)ewolucja sieci bezprzewodowych **7**

5G w Unii Europejskiej. Komentarz NASK **14**

Wspólne podejście Unii Europejskiej do cyberbezpieczeństwa sieci 5G jako istotny czynnik bezpieczeństwa i stabilnego rozwoju gospodarczego Europy **17**

Jak należy zaadresować wyzwania związane z bezpieczeństwem w ochronie sieci 5G? **28**

Bezpieczeństwo sieci 5G w ujęciu holistycznym **39**

Cyfrowa suwerenność w kontekście 5G. Komentarz NASK **54**

5G i Open RAN – sieć nowej generacji w perspektywie dyskusji o cyfrowej suwerenności **57**

5G w perspektywie politycznej. Komentarz NASK **66**

5G w Niemczech – szanse, perspektywy, kontrowersje **67**

Rozwój sieci mobilnej 5G w Rosji kluczowym elementem programu cyfryzacji gospodarki **70**

Huawei i 5G: chińska droga do światowej czołówki w branży ICT **73**

NASK Cyber POLICY

Komentarz NASK

5G, a sprawa Polska

W Polsce, proces budowy sieci 5G rozpoczął się w 2017 roku, kiedy przyjęto **porozumienie na rzecz Strategii 5G dla Polski.** Celem porozumienia było zainicjowanie współpracy pomiędzy sektorem publicznym, akademickim i prywatnym. Dokument został podpisany m.in. przez Urząd Komunikacji Elektronicznej i Instytut Łączności PIB, a także przedstawicieli operatorów, dostawców sprzętu, izby gospodarcze oraz uczelnie techniczne. Efektem porozumienia było wypracowanie projektu strategii *5G dla Polski*, której konsultacje rozpoczęły się w styczniu 2018 roku. Po zakończeniu konsultacji, prace nad strategią zostały wstrzymane, a do końca 2019 roku dokument nie został oficjalnie przyjęty.

Natomiast w czerwcu 2018 roku opublikowano *Krajowy Plan działań zmiany przeznaczenia pasma 700 MHz w Polsce*, które docelowo ma być przeznaczone na usługi szerokopasmowe (sieć 5G). Obecnie pasmo zajmuje naziemna telewizja cyfrowa, która musi być przeniesiona w zakres 470-694 MHz (bez straty jakości).

Jednak w tym celu konieczne jest osiągnięcie porozumienia z Federacją Rosyjską, która użytkuje w paśmie 700 MHz systemy radiokomunikacyjne oraz telewizyjne. Dotąd się to nie udało. Z tego powodu przyjęta w lipcu 2019 roku aktualizacja *Krajowego Planu* wprowadziła zmianę terminu wykorzystania pasma 700 MHz dla sieci 5G do 30 czerwca 2022 roku.

W sierpniu 2019 roku Sejm RP przyjął **ustawę o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw.** Tzw. megaustawa obowiązuje od października. Nowe przepisy mają wspierać usuwanie barier administracyjno-prawnych dla budowy sieci szerokopasmowych. Krótszy i prostszy ma być proces inwestycyjno-budowlany, dzięki czemu spadną koszty inwestycji, a operatorzy będą mogli w większym stopniu wykorzystywać infrastrukturę techniczną. Ustawa powołała także Fundusz Szerokopasmowy z rocznym budżetem 140 mln. zł. Środki te posłużą m.in. na dofinansowanie budowy i rozwoju sieci telekomunikacyjnych.

W październiku 2019 roku Polski Fundusz Rozwoju, Exatel, a także przedstawiciele T-Mobile, Orange i Polkomtela podpisali memorandum w sprawie analizy modelu biznesowego **dla spółki #Polskie5G.** Spółka ma być hurtowym operatorem ogólnopolskiej bezprzewodowej sieci 5G w paśmie 700 MHz i zapewniać dostęp do usług 5G w całej Polsce. Zaproponowany model zakłada, że poprzez spółkę celową, to właśnie państwo będzie właścicielem jednolitej infrastruktury dla pasma pokryciowego 700 MHz. Efektem będzie kontrola państwowa nad tym, jakie firmy zostaną dopuszczone do budowy sieci 5G w Polsce. Takie rozwiązanie pozwoli na obniżenie kosztów budowy infrastruktury telekomunikacyjnej, co przełoży się na konkurencyjne ceny usług.

Bardzo ważne było także opublikowanie 29 czerwca 2020 roku Rozporządzenia Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Rozporządzenie określa minimalne środki techniczne i organizacyjne jakie są zobowiązani stosować przedsiębiorcy telekomunikacyjni w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług i odnosi się także do dostawców sieci piątej generacji (5G). Operatorzy 5G zobowiązani są do uwzględnienia rekomendacji pełnomocnika rządu ds. cyberbezpieczeństwa, dotyczących stosowania urządzeń informatycznych oraz oprogramowania. Powinni także uwzględnić w swoich strategiach uniezależnienie się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej, przy jednoczesnym zapewnieniu interoperacyjności usług. W rozporządzeniu mowa jest również o konieczności zastosowania przez nich podwyższonej odporności na zakłócenia sieci i usługi telekomunikacyjnej.

NASK Cyber POLICY

Rafał Babraj

Sieć 5G, czyli (r)ewolucja sieci bezprzewodowych

Rafał Babraj – Starszy specjalista w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach dotyczących szeroko pojętej komunikacji w cyberbezpieczeństwie: dezinformacja, komunikacja strategiczna, technologie mobilne. Doświadczenie zdobywał jako dziennikarz i redaktor, a także w administracji rządowej. Absolwent Instytutu Edukacji Medialnej i Dziennikarstwa na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Prywatnie pisarz oraz pasjonat literatury fantastycznej.

Rewolucja cyfrowa zmienia sposób w jaki funkcjonujemy. Nasze mieszkania powoli stają się *smart home*. Smartfony przejmują rolę pilota, którym kontrolować można cały szereg innych inteligentnych urządzeń. Zakupy online to już codzienność. Po filmy, muzykę lub książki również coraz częściej sięgamy za pośrednictwem platform internetowych. Ogromne zmiany przechodzi cały przemysł, w którym obserwujemy postępującą robotyzację, automatyzację procesów produkcyjnych czy wykorzystywanie algorytmów uczenia maszynowego do usprawnienia zarządzania[1].

Tymczasem przepustowość Internetu ma pewne granice. Najdobitniej uwidoczniła to pandemia koronawirusa. Wiele firm przeszło w tryb pracy zdalnej, edukacja odbywała się online, a ludzie podczas kwarantanny chętniej sięgali po rozrywkę w sieci. W tej sytuacji w marcu 2020 roku Komisja Europejska wezwała serwisy *streamingowe*, operatorów sieci komórkowych oraz samych użytkowników do wspólnych działań, które miałyby zapobiec przeciążeniu sieci[2]. Wśród zaleceń znalazły się obniżenie rozdzielczości udostępnianych multimediów oraz zachęcanie użytkowników do korzystania z Wi-Fi zamiast transferu danych komórkowych.

Dlaczego potrzebujemy sieci 5G?

- Wzrastający transfer danych – Instytut Łączności PIB przewiduje, że w ciągu 2-3 lat obecna konfiguracja sieci nie będzie w stanie obsłużyć prognozowanego ruchu.
- Coraz więcej urządzeń online – według różnych szacunków w 2020 roku do sieci podłączonych może być nawet ponad 20 mld urządzeń.
- Wzrost znaczenia usług multimedialnych – *streaming* wideo odpowiada za 65% transmisji danych. Blisko 13% ruchu mobilnego generują serwisy społecznościowe.
- Stałe i niskie opóźnienia, co pozwoli wdrażać nowoczesne technologie i rozwiązania w większym zakresie (np. autonomiczne samochody).

Czym jest sieć 5G?

Z punktu widzenia operatorów telekomunikacyjnych to po prostu kolejny standard technologii mobilnej. Również, jeśli chodzi o wykorzystanie fal radiowych, mamy do czynienia z tymi samymi zjawiskami fizycznymi. Pewną nowością w kontekście częstotliwości będzie zastosowane w sieciach komórkowych wysokiego pasma z zakresu 26 GHz. Dopiero, gdy weźmiemy pod uwagę budowę systemu, a także możliwości jakie zaoferuje on użytkownikom, możemy stwierdzić, że 5G

[1] Więcej informacji m.in. o Przemyśle 4.0 w raporcie *Krótka opowieść o społeczeństwie 5.0, czyli jak żyć i funkcjonować w dobie gospodarki 4.0 i sieci 5G* (https://www.digitalpoland.org/assets/publications/krotka-opowiesc-50/krotka-opowiesc-s50.pdf)

[2] *Commission calls on streaming services, operators and users to prevent network congestion, discusses issue with European regulators* (https://ec.europa.eu/commission/presscorner/detail/en/mex_20_489)

istotnie przyczyni się do napędzenia trwającej rewolucji cyfrowej. Sieć nowej generacji zaoferuje nie tylko szybszy transfer danych i mniejsze opóźnienia, ale też większą pojemność.

Kolejna generacja sieci komórkowej

W ciągu ostatnich 40 lat telefonia komórkowa przeszła ogromną przemianę. Pierwsza generacja, czyli tzw. sieć 1G, umożliwiała jedynie analogowe połączenia głosowe. Wdrożona w latach dziewięćdziesiątych ubiegłego wieku sieć 2G wprowadziła łączność cyfrową, a razem z nią wiadomości tekstowe. Sieć 3G pozwalała już na połączenia z Internetem, choć dopiero sieć 4G umożliwiła swobodne korzystanie z multimediów oraz usług online. Obecnie jesteśmy u progu wprowadzenia sieci 5G, która przyniesie fundamentalną zmianę – z **ery smartfonów** przejdziemy do **ery Internetu Rzeczy**[3].

Internet ludzi, rzeczy i usług

Do czego będziemy wykorzystywać sieć nowej generacji? Trzy główne rodzaje usług, czyli tzw. scenariusze zastosowań dla 5G, określił Międzynarodowy Związek Telekomunikacyjny (ITU) w standardzie IMT-2020[4]. Będą to:

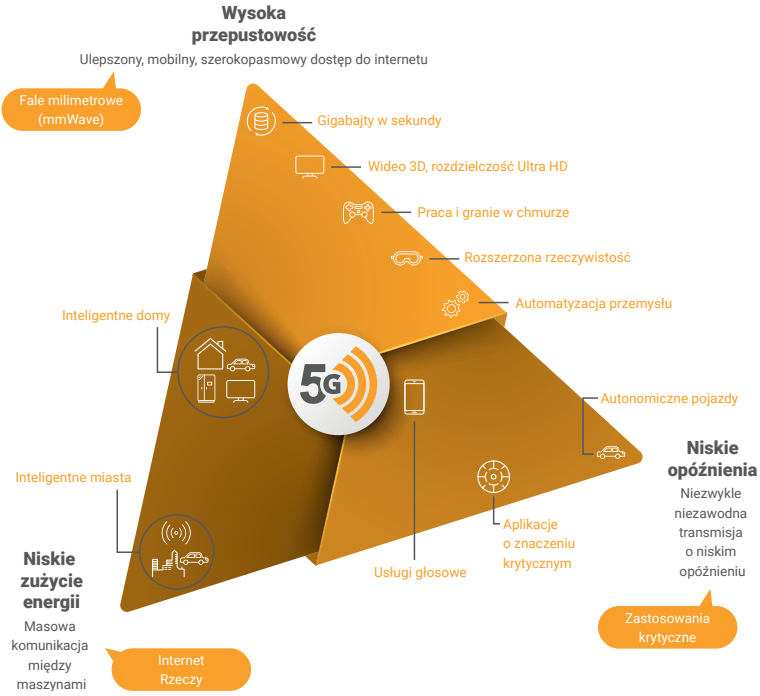
- **Ulepszony, mobilny, szerokopasmowy dostęp do internetu** (eMBB, *enhanced Mobile Broadband*) – bardzo szybka transmisja danych i przetwarzanie informacji w czasie niemal rzeczywistym.
- **Masowa komunikacja między maszynami** (mMTC, *massive Machine Type Communications*) – umożliwi podłączenie przy minimalnych opóźnieniach blisko stukrotnie większej liczby urządzeń niż obecnie.
- **Niezwykle niezawodna transmisja o niskim opóźnieniu** (URLLC, *Ultra-Reliable Low Latency Communications*) – minimalne opóźnienia umożliwią połączenia w czasie rzeczywistym, również w zastosowaniach krytycznych.

Mówiąc bardziej obrazowo, sieć 5G została zaprojektowana w taki sposób, aby umożliwić rozwój Intenetu w trzech odsłonach:

- **Internet ludzi** – z dużo większej szybkość transmisji danych oraz przepustowości skorzystają użytkownicy rozszerzonej (AR) i wirtualnej rzeczywistości (VR), czy kinomaniacy, ceniący bardzo wysoką rozdzielczość multimediów.
- **Internet Rzeczy** – obsługa nawet miliona urządzeń na kilometr kwadratowy pozwoli projektować inteligentne budynki, a nawet miasta.
- **Internet usług** – niezwykle niskie opóźnienia i niezawodność otworzą drogę do wdrożenia ekosystemu autonomicznych pojazdów czy rozwinięcia telemedycyny (np. zdalne operacje). Umożliwią też automatyzację przemysłu.

[3] Internet Rzeczy (*Internet of Things*) to swoisty ekosystem, w którym urządzenia podłączone do sieci wymieniają dane, czyli komunikują się ze sobą – często bez udziału człowieka. Terminu „Internet Rzeczy" użył po raz pierwszy w 1999 roku brytyjski przedsiębiorca Kevin Ashton.

[4] Standard IMT-2020 to wymagania przedstawione przez I*TU Radiocommunication Sector* (ITU-R) w 2015 roku dla sieci, urządzeń i usług 5G. Standard ma zostać ukończony w 2020 roku. Częściowo został sfinalizowany wcześniej, na przykład w obszarze dotyczącym technologii dostępu radiowego *(5G New Radio)*.



(Źródło: Międzynarodowy Związek Telekomunikacyjny, ITU)

Standard 5G – duża prędkość, niskie opóźnienia i wielka pojemność

Standardy stanowią podstawę naszego funkcjonowania. Oczekujemy na przykład, że nasz smartfon połączy się bezprzewodowo z Internetem, bez względu na lokalizację i rodzaj urządzenia. Ufamy, że został zaprojektowany w zgodzie z przyjętymi standardami branżowymi, które mogą być inne w różnych krajach. Dlatego tak ważne jest opracowanie wspólnego standardu 5G. Pozwoli on m.in. zapewnić **określony poziom wydajności nowej sieci** (np. szybkość transmisji danych), a producenci na całym świecie będą mogli wytwarzać **kompatybilny sprzęt** oraz urządzenia.

Międzynarodowy Związek Telekomunikacyjny (ITU) rozpoczął pracę nad specyfikacją dla sieci 5G już w 2012 roku[5]. Kompletny standard ma być gotowy w 2020 roku. Jednak częściowe specyfikacje zostały opublikowane już w listopadzie 2017 roku. Były to *Minimalne wymagania dotyczące wydajności technicznej dla interfejsów radiowych IMT-2020*[6].

[5] *ITU towards IMT for 2020 and beyond* (https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx)

[6] *Minimum requirements related to technical performance for IMT-2020 radio interface(s)* (https://www.itu.int/pub/R-REP-M.2410-2017)

Kluczowe aspekty określone w standardzie IMT-2020

Wskaźnik	Specyfikacja
Maksymalna szybkość transmisji	• 20 Gb/s – łącze w dół (*downlink*) • 10 Gb/s – łącze w górę (*uplink*)
Doświadczana przez użytkownika szybkość transmisji danych	• 100 Mb/s w łączu w dół • 50 Mb/s w łączu w górę
Opóźnienie maksymalne	W warstwie użytkownika: • 1 ms (URLCC) • 4 ms (eMBB) W warstwie sterowania: 10-20 ms
Gęstość połączenia	1 mln urządzeń na km^2
Mobilność	Zapewniona do 500 km/godz

Po opublikowaniu wymagań przez ITU, twórcy technologii dostępu radiowego mogli zacząć opracowywać specyfikacje technologii 5G, które spełniałyby określone wytyczne. Proces ten rozpoczął się na początku 2016 roku w ramach prac **3GPP**, czyli kluczowego ciała standaryzacyjnego dla globalnych systemów komunikacji mobilnej[7]. Został podzielony na dwa etapy:

- **Release 15 – pierwsza faza standardu 5G (2018).**
  - **Grudzień 2017**: standard dla sieci niesamodzielnych (*NSA, Non-Standalone*) –opiera się na istniejącej infrastrukturze, np. 4G. Uaktualniona do 5G zostaje tylko sieć dostępu radiowego. Zwiększy to wydajność mobilnego internetu.
  - **Czerwiec 2018**: standard dla sieci samodzielnych (*SA, Standalone*) – umożliwi wdrożenie funkcji sieci rdzeniowej 5G oraz wprowadzenie nowych funkcjonalności. Wymaga znacznie większych zmian w architekturze sieci.
- **Release 16 – druga faza standardu 5G planowana na rok 2020.**

5G a widmo elektromagnetyczne

Widmo elektromagnetyczne składa się z różnego rodzaju fal[8]. Wszystkie one mają inne właściwości, które wpływają na to, jak można je wykorzystać. Systemy telefonii komórkowej wykorzystują **fale radiowe oraz mikrofale**, które są używane również m.in. na potrzeby transmisji radiowych (AM i FM), telewizji cyfrowej oraz satelitarnej, Wi-Fi czy Bluetooth. **W przypadku 5G nowością będzie wykorzystanie częstotliwości milimetrowych z pasma**

[7] *5G Research & Standards* (https://ec.europa.eu/digital-single-market/en/research-standards)

[8] Wyróżniamy: fale radiowe, mikrofalowe, promieniowanie podczerwone, światło widzialne, promieniowanie ultrafioletowe, promieniowanie rentgenowskie oraz promieniowanie gamma.

wysokiego (np. 26 GHz), których dotychczas nie używano w sieciach komórkowych.

Aby móc obsłużyć zwiększający się ruch w sieciach komórkowych, konieczne było przydzielenie nowych częstotliwości na potrzeby 5G. Ich identyfikacja rozpoczęła się na Światowej Konferencji Radiokomunikacyjnej 2015 w Genewie (**WRC-15**). Podczas **WRC-19** w Sharm el-Sheik zidentyfikowano dodatkowe pasma wyższych częstotliwości, łącze 17,25 GHz widma, z czego 14,75 GHz zharmonizowanych na całym świecie[9].

Spośród wskazanych pasm wytypowano trzy, które w pierwszej kolejności będą wykorzystane do uruchomienia sieci 5G[10]:

- pasmo niskie: **700 MHz**, czyli tzw. pokryciowe, zapewniające dostęp na dużym obszarze przy stosunkowo małych nakładach na infrastrukturę. Fale rozchodzą się równomiernie i nie są aż tak pochłaniane przez przeszkody.
- pasmo średnie: **3,4–3,8 GHz**, czyli tzw. pojemnościowe, stanowi dobrą równowagę zasięgu i pojemności. Może być wykorzystywane w miastach o dużej gęstości zabudowy, a także do usług wymagających niezawodnej transmisji i niskich opóźnień.
- pasmo wysokie: **26 GHz**, może być używane do zapewnienia płynnej obsługi użytkowników w bardzo zatłoczonych miejscach (dworce, stadiony). Pasmo to wykorzystywać mogą urządzenia wymagające niskiego opóźnienia (np. Przemysł 4.0).

5G a nowoczesne technologie

W pierwszej fazie wdrażania 5G (*Non-Standalone*) sieci będą opierać się o już istniejącą infrastrukturę np. 3G i 4G. Jednak pełne wdrożenie planowanych funkcjonalności będzie wymagało odejścia od tradycyjnej architektury. Niezwykle ważne stanie się oprogramowanie, ponieważ sieć będzie musiała być odpowiednio elastyczna, aby zapewnić realizację różnorodnych usług. Na przykład dla pojazdów autonomicznych najistotniejsze będzie niskie opóźnienie, dla Internetu Rzeczy – duża pojemność sieci, a dla wielbicieli kina, oglądających filmy na swoich smartfonach – odpowiednia przepustowość.

Wśród nowych rozwiązań technologicznych, warte podkreślenia są przede wszystkim zmiany w **sieci rdzeniowej**:

- **Wirtualizacja funkcji sieciowych** (*NFV, Network Functions Virtualization*) pozwoli oddzielić sprzęt od oprogramowania sieciowego. Konkretne funkcje oraz usługi nie będą wymagały dedykowanego sprzętu, co znacznie obniży koszty.

[9] *WRC-19 identifies additional frequency bands for 5G* (https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/)

[10] *Radio Spectrum Policy Group Strategic Roadmap towards 5G for Europe. Opinion on spectrum related aspects for next-generation wireless systems* (5G) (https://rspg-spectrum.eu/wp-content/uploads/2013/05/RPSG16-032-Opinion_5G.pdf)

- **Programowalne sieci/sieci definiowane programowo** (*SDN, Software Defined Network*) pozwolą oddzielić płaszczyzny sterowania i przekazywania danych. W SDN urządzenie sieciowe odpowiadać będzie tylko za przesyłanie danych. Zarządzanie siecią trafi do scentralizowanej warstwy kontrolnej i odbywać się będzie przy użyciu oprogramowania.
- **Dzielenie/segmentacja sieci** (*NS, Network Slicing*) – podział jednej sieci fizycznej, bazującej na wspólnej infrastrukturze, na wiele odizolowanych sieci wirtualnych, a także ich konfiguracja zgodnie z konkretnymi potrzebami.

Zauważalne modyfikacje czekają również **radiową sieć dostępową**. Najbardziej widoczną zmianą będzie znacznie **większa liczba stacji bazowych** – zwłaszcza w miastach. Urządzenia 5G po raz pierwszy będą wykorzystywać fale o częstotliwości 26 GHz, które mają bardzo ograniczony zasięg. Dlatego stacje bazowe będą musiały znajdować się bliżej siebie.

Rodzaj stacji bazowej	Makrokomórka	Mikrokomórka	Pikokomórka
Zasięg	do kilkunastu kilometrów	do dwóch kilometrów, najczęściej kilkaset metrów	nie przekraczający kilkudziesięciu metrów
Częstotliwość	700 MHz	3,6 GHz	26 GHz
Zastosowanie	Usługi głosowe, Smart home, Smart city	Smart city, e-zdrowie, autonomiczne pojazdy	Przemysł 4.0, VR, AR

5G w Unii Europejskiej

Jednym z najważniejszych tematów, podejmowanych w UE 2019 roku, było właśnie wdrożenie sieci 5G. Zdaniem KE będzie ona miała kluczowe znaczenie dla rozwoju społeczno-gospodarczego Unii Europejskiej. W związku z tym podjęto działania zmierzające do zapewnienia wysokiego poziomu cyberbezpieczeństwa sieci 5G na obszarze całej UE, a także koordynacji wysiłku państw członkowskich w tym zakresie.

Najpierw, **26 marca** Komisja Europejska opublikowała rekomendacje *Cybersecurity of 5G networks*[11]. Celem dokumentu, który zawierał opis działań operacyjnych na poziomie Unii Europejskiej i państw członkowskich, było wypracowanie wspólnego podejścia do bezpieczeństwa sieci 5G. KE zwróciła uwagę na konieczność przyjęcia specjalnych regulacji i ustanowienia spójnej polityki reagowania na incydenty w cyberprzestrzeni. Zdaniem Komisji podstawowym narzędziem, wspierającym wprowadzanie sieci 5G w państwach członkowskich, powinny być europejskie ramy certyfikacji cyberbezpieczeństwa, które w przyszłości zapewnią wysoki poziom bezpieczeństwa w całym cyklu sieci 5G.

[11] *Commission Recommendation of 26.3.2019 Cybersecurity of 5G networks.* (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154)

Ponadto państwa członkowskie zostały zobowiązane do przeprowadzenia krajowej analizy ryzyka sieci oraz aktualizacji wymagań bezpieczeństwa i zarządzania ryzykiem. Termin przekazania krajowych ocen ryzyka do ENISA został wyznaczony na 15 lipca 2019 roku. KE postanowiła również powołać działającą na szczeblu unijnym Grupę Współpracy, która do końca roku miała stworzyć niezbędny zestaw narzędzi do reagowania na incydenty zagrażające bezpieczeństwu sieci[12]. W rekomendacjach zalecono państwom członkowskim ścisłą współpracę z unijnymi organami przy tworzeniu wymogów bezpieczeństwa dla zamówień publicznych dotyczących sieci 5G.

Istotnym krokiem w kierunku wdrożenia sieci 5G w Europie było podjęcie przez Komisję Europejską Decyzji wykonawczej w dniu 14 maja 2019[13] w celu zharmonizowania widma radiowego w paśmie 24,25-27,5 GHz. KE zobligowała państwa członkowskie do wyznaczenia i udostępnienia na zasadzie braku wyłączności, zakresu częstotliwości 24,25-27,5 GHz na potrzeby naziemnych systemów świadczących szerokopasmowy dostęp do usług cyfrowych. Zakres tych częstotliwości został przyjęty przez KE jako odpowiedni do celów standardu Międzynarodowej Telekomunikacji Ruchomej (IMT-2020), opracowanego przez Sektor Radiokomunikacji Międzynarodowego

[12] *Toolbox* został ostatecznie opublikowany w dniu 29 stycznia 2020 roku.

[13] *Commission Implementing Decision(EU) 2019/784 of 14 May 2019 on harmonisation of the 24,25-27,5 GHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services in the Union* (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019D0784).

Związku Telekomunikacyjnego (ITU). Termin wykonania zarządzenia upływa 30 marca 2020 roku. Państwa członkowskie zostały zobowiązane do złożenia KE sprawozdań z wykonania tej decyzji.

19 lipca 2019 roku Komisja Europejska wydała oświadczenie w sprawie przedłożenia przez państwa członkowskie UE krajowych ocen ryzyka bezpieczeństwa sieci 5G. Oceny te zostały następnie przeanalizowane przez KE i ENISA. Opis najważniejszych zagrożeń, podatności, słabych punktów i przykładowych scenariuszy ryzyka sieci 5G został opublikowany **9 października 2019 roku** w raporcie Grupy Współpracy NIS *EU coordinated risk assessment of the cybersecurity of 5G networks*[14]. Autorzy ekspertyzy zwrócili uwagę na szczególną rolę operatorów sieci komórkowych i producentów sprzętu telekomunikacyjnego w zapewnieniu cyberbezpieczeństwa sieci 5G. Warto podkreślić, że 17 maja 2019 roku Rada UE wydała rozporządzenie w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim[15]. Pod koniec roku, **21 listopada 2019 roku** ENISA opublikowała raport *ENISA Threat Landscape for 5G Network*[16]. Publikacja przedstawia krajobraz zagrożeń i wyzwań związanych z bezpieczeństwem sieci 5G ze szczególnym uwzględnieniem architektury i komponentów sieci 5G. Raport stanowi uzupełnienie i rozwinięcie skoordynowanej unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G stworzonej przez Grupę Współpracy NIS w październiku 2019 roku. Publikacja zawiera również rekomendacje dotyczące UE, interesariuszy i właściwych organów krajowych. Wśród zaproponowanych przez autorów działań znalazły się m.in. dzielenie się wiedzą na temat 5G z interesariuszami, promowanie współpracy między zainteresowanymi stronami, a także aktualizowanie informacji na temat zagrożeń teleinformatycznych i udostępnianie ich interesariuszom.

[14] *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049).

[15] Rozporządzenie w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (https://eur-lex.europa.eu/legal content/PL/TXT/PDF/?uri=CELEX:32019R0796&from=EN).

[16] *ENISA Threat Landscape for 5G Network* (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks).

NASK Cyber POLICY

Maciej Siciarek

Wspólne podejście Unii Europejskiej do cyberbezpieczeństwa sieci 5G jako istotny czynnik bezpieczeństwa i stabilnego rozwoju gospodarczego Europy

Maciej Siciarek – Specjalista w dziedzinie bezpieczeństwa teleinformatycznego. Od wielu lat zaangażowany w projekty, których odbiorcami są zarówno administracja, jak sektor prywatny. Kieruje Działem Innowacji i Rozwoju Cyberbezpieczeństwa w NASK PIB prowadząc projekty związane z budowaniem krajowego potencjału w zakresie cyberbezpieczeństwa, jak również techniczne

analizy nowych rozwiązań ICT. Współautor polskiego podejścia do szacowania ryzyka w sieciach 5G, jak również dokumentów wypracowanych przez Komisję Europejską – *EU coordinated risk assessment of the cybersecurity of 5G networks* oraz *Cybesecurity of 5G networks – EU Toolbox of risk mitigating measures*. Pracuje w grupie roboczej NIS Work Stream on 5G Cybersecurity.

Przyśpieszony rozwój technologii 5G, połączony z przygotowaniami operatorów usług mobilnych do implementacji rozwiązań technicznych w swoich sieciach, a także procedury przyznawania licencji na stosowne pasma częstotliwości zostały zaklasyfikowane przez Radę Europejską jako jedne z głównych priorytetów rozwoju Jednolitego Rynku Cyfrowego.

W marcu 2019 roku, podążając za wytycznymi Rady, **Komisja Europejska wydała rekomendacje wskazujące na konieczność uzgodnienia przez państwa członkowskie wspólnego podejścia do bezpieczeństwa sieci 5G**. Zalecenia te podkreślają m.in. istotną rolę sieci piątej generacji jako technologicznej podstawy dla szerokiego spektrum usług kluczowych dla gospodarki oraz społeczeństwa. Szczególnie wyróżniono sektory energii, transportu, bankowości, ochrony zdrowia, jak również przemysłowe systemy sterowania. Zdaniem Komisji zakłócenia działania sieci w tych sektorach, mogłyby spowodować bardzo poważne konsekwencje. Ze względu na ponadpaństwowy charakter zarówno infrastruktury teleinformatycznej, jak i usług świadczonych przez operatorów, koordynacja podejścia do bezpieczeństwa sieci jest szczególnie istotna. W tej sytuacji Unia Europejska powinna zapewnić wspólny, wysoki poziom bezpieczeństwa. Jest to niezwykle ważne, ponieważ rośnie liczba ataków teleinformatycznych, a także poziom ich wyrafinowania.

Ważnym aspektem wskazanym przez Komisję Europejską oraz Radę Europejską jest tzw. cyfrowa suwerenność Europy. Zdaniem autorów dokumentu należy pamiętać o europejskich wartościach, otwartości i wolnym handlu. Jednak z drugiej strony trzeba mieć na uwadze, że inwestycje zagraniczne mogą stać się zagrożeniem dla bezpieczeństwa wewnątrz UE. Mogłoby do tego dojść, gdyby np. podmioty spoza Unii Europejskiej nabyły kluczowe aktywa technologiczne i infrastrukturalne w Unii, a także odpowiadały za dostawy sprzętu stosowanego w obszarach o krytycznym znaczeniu.

W zaleceniu znalazło się bardzo ważne stwierdzenie, że przy definiowaniu obszarów ryzyka i szacowaniu ryzyka dla sieci 5G, powinny zostać wzięte pod uwagę zarówno czynniki techniczne, jak i pozatechniczne. Istotnymi elementami, wymagającym zauważania i analizy, są podatności sprzętu i oprogramowania, które mogą być wykorzystane w celach szpiegowskich lub przestępczych. Taka złośliwa działalność może wynikać z pobudek ekonomicznych

lub politycznych, a jej skutkiem jest uzyskanie nieautoryzowanego dostępu do informacji i danych lub ich zniszczenie. Równie ważna jest jednak ochrona sieci, polegająca na uwzględnieniu pochodzenia technologii, bezpieczeństwa łańcucha dostaw, sposobu zakupu oraz aspektów wdrożenia, utrzymania, rozbudowy elementów sieci czy ich aktualizacji – zwłaszcza w aspekcie zmian w oprogramowaniu. To ostatnie zagadnienie jest niezwykle istotne, gdy kluczowe funkcje infrastruktury są realizowane przez oprogramowanie poddawane ciągłej modernizacji i aktualizacji, co stwarza ryzyko pojawiania się nowych, niepożądanych i niebezpiecznych funkcji w elementach sieci.

Prace nad skoordynowanym szacowaniem ryzyka 5G

Konsekwencją rekomendacji Komisji Europejskiej było rozpoczęcie przez państwa członkowskie prac nad krajowymi ocenami ryzyka oraz powołanie Grupy Roboczej ds. bezpieczeństwa sieci 5G w nurcie prac *NIS Cooperation Group*[17].

Państwa członkowskie zostały zobowiązane do przeprowadzenia na poziomie krajowym szacowania ryzyka związanego z implementacją sieci piątej generacji. Termin na to zadanie upłynął w czerwcu 2019 roku. Efektem analiz krajowych było stworzenie przez Komisję Europejską, we współpracy z Europejską Agencją ds. Cyberbezpieczeństwa (ENISA), kwestionariusza, który następnie pozwolił sporządzić ramy dla skoordynowanego szacowania ryzyka sieci 5G na poziomie unijnym.

Kwestionariusz, podsumowujący dokumenty wypracowane przez państwa członkowskie, wskazał na konieczność uwzględnienia w procesie szacowania ryzyka perspektywy:

- rządów (aspekty legislacyjne oraz regulatorzy rynku);
- interesariuszy (m.in. operatorzy i dostawcy);
- pozostałych podmiotów i instytucji (np. podmioty realizujące zadania ustawowe w zakresie cyberbezpieczeństwa i telekomunikacji, odpowiednie służby, także specjalne).

Efektem tych prac był wysokopoziomowy raport przygotowany przez państwa członkowskie przy wsparciu Komisji Europejskiej oraz ENISA. Raport ten, razem z dostarczonym przez Agencję dokumentem ***ENISA Threat Lanscape for 5G networks***, stał się podstawą do opublikowania 9 października 2019 roku ostatecznego dokumentu. **Skoordynowane podejście do szacowania ryzyka w sieciach 5G na poziomie Unii Europejskiej** (*EU coordinated risk assessment of the cybersecurity of 5G networks*).

[17] Grupa współpracy powołana w 2016 roku Dyrektywą NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).

Cyberbezpieczeństwo sieci 5G: szacowanie ryzyka i skoordynowane podejście

Opublikowany w październiku 2019 roku dokument dotyczący skoordynowanego podejścia do szacowania ryzyka, skupia się na pokazaniu zależności pomiędzy zagrożeniami, aktorami zagrożeń, zasobami i aktywami, podatnościami jakie występują w sieci 5G oraz możliwymi scenariuszami ryzyka. Śledząc cały proces podejścia państw członkowskich do cyberbezpieczeństwa systemów 5G, warto prześledzić i pokrótce opisać to podejście.

Zagrożenia i aktorzy związani z ich wykorzystaniem – czyli skąd pochodzą zagrożenia?

Dokument prezentuje następujące źródła zagrożeń:

- przypadkowe,
- hakerzy i cyberprzestępcy,
- tzw. haktywiści (motywacje polityczne),
- zorganizowane grupy przestępcze,
- tzw. *insider,* czyli pracownik lub podwykonawca operatorów telekomunikacyjny,
- państwo lub podmiot przez to państwo wspierany (motywacje politycze),
- cyberterroryści,
- przedsiębiorstwa i korporacje (walka rynkowa).

Zagrożone zasoby i aktywa

Definicja kluczowych zasobów technicznych, wymagających uwzględnienia w planowaniu zabezpieczeń i analizowaniu możliwych scenariuszy zagrożeń, została oparta o wskazane w normie 3GPP zasoby tj.:

- podstawowe funkcje szkieletu sieci;
- zarządzanie funkcjami odpowiedzialnymi za wirtualizację sieci – NFV (*Network Function Virtualization*) oraz zarządzanie i orkiestracja zasobów sieciowych w środowisku opartym o architekturę chmurową – MANO (*Management and orchestration*);
- systemy zarządzania i usługi wspierające inne niż MANO – w tej kategorii, w trakcie prac grupy roboczej, szczególnie wyróżniono systemy zarządzania bezpieczeństwem jako istotnie wrażliwy element mogący podlegać różnym atakom (oprócz generalnej kategorii systemów zarządzania wszechobecnych w każdej infrastrukturze teleinformatycznej, a więc również w sieciach operatorskich);
- radiowa sieć dostępowa;

Aktywa niewynikające wprost z normy 3GPP:

- funkcje realizowane na rzecz transportu i transmisji, dotyczące sprzętu sieciowego niskiego poziomu, takiego jak: przełączniki

sieciowe, routery oraz związane z filtrowaniem ruchu zapory sieciowe i sondy analizujące bezpieczeństwo (IPS, IDS itp.);

- funkcje związane z międzysieciową wymianą ruchu oraz usługami sieciowymi świadczonymi przez zewnętrzne podmioty.

Warto podkreślić, że do **grupy zasobów o krytycznej lub wysokiej wrażliwości**, których naruszenie może zagrozić poufności, dostępności i integralności wszystkich usług sieciowych, zaliczono zarówno **bazowe funkcje szkieletu sieci 5G**, jak i **systemy zarządzania**. Być może w przyszłości w przypadku aktualizacji dokumentu, pożądanym byłoby wydzielenie systemów zarządzania bezpieczeństwem infrastruktury do oddzielnej kategorii i zakwalifikowanie ich do zasobów krytycznych.

Mimo pozornie mniejszej roli systemów dostępu radiowego, dobrze że znalazły się one w kategorii wysokiego ryzyka, gdyż rozwój tzw. *edge computingu* wpłynie na wzrost znaczenia sieci dostępowej.

Uznając za istotne podkreślenie pojęć wprowadzonych przez Dyrektywę NIS, do aktywów innych niż techniczne zaliczono zdefiniowane w dokumencie dyrektywy podmioty oraz wrażliwe usługi przez nie świadczone tj.:

- operatorów usług kluczowych;
- podmioty rządowe, organy ścigania, organy związane z ochroną ludności i działaniem antykryzysowym oraz wojsko;
- kluczowe sektory oraz podmioty nieobjęte do tej pory regulacjami dotyczącymi cyberbezpieczeństwa;
- podmioty prywatne o strategicznym znaczeniu.

W kategorii istotnych aktywów wymieniono też inne podmioty, które w przypadku utraty usług sieci piątej generacji, utracą ciągłość działania z braku rozwiązań zapasowych. Wskazano również skupiska ludności zdefiniowane jako „obszary geograficzne", których funkcjonowanie jest uzależnione od rozwiązań technologicznych (np.: społeczności korzystające w coraz większym stopniu z usług inteligentnych miast).

Podatności i braki w zabezpieczeniach

Na poziomie szacowania ryzyka zidentyfikowane zostały następujące grupy podatności:

- podatności związane ze sprzętem, oprogramowaniem, politykami i procedurami;
- podatności specyficzne dla dostawców;
- podatności wynikające z braku różnorodności dostawców – uzależnienie od dostawcy.

Warto podkreślić, że już na poziomie rekomendacji Komisji Europejskiej, wskazane zostały gospodarki, których interesy mogą być reprezentowane ponad miarę przy implementacji systemów 5G w Europie. Nie wchodząc zbyt głęboko w geopolitykę, trzeba zaznaczyć, że każde uzależnienie od pojedynczego dostawcy niesie za sobą

ryzyko. Wzrasta ono do poziomu krytycznego w kilku sytuacjach:

- braku możliwości oceny bezpieczeństwa łańcucha dostaw u konkretnego producenta;
- wątpliwości co do konkurencyjnej gry rynkowej między producentami;
- wątpliwości dotyczących politycznych (na tyle o polityce trzeba jednak wyraźnie powiedzieć) motywacji i okoliczności, w których dochodzi do zaburzenia tej konkurencyjności.

Dlatego tak obszerna część dokumentu szacowania ryzyka została ostatecznie poświęcona zagadnieniom związanym w głównej mierze z dostawcami technologii.

Podatności związane ze sprzętem, oprogramowaniem, politykami i procedurami

Bezpieczeństwo produktów, które w coraz większej mierze oparte są o wytwarzane masowo oprogramowanie, jak również rosnąca komplikacja świadczonych we współdzielonym modelu chmurowych usług, wymagają bardzo wnikliwej oceny. **Bezpieczeństwo produktów, ich sformalizowane wytwarzanie i należyte testowanie, będzie stawało się coraz istotniejszym czynnikiem decydującym o bezpieczeństwie świadczonych usług**. Nowe podatności, a także luki technologiczne, które wpływają na możliwość właściwej segmentacji sieci oraz na systemy wirtualizacji, mogą w znaczący sposób obniżyć bezpieczeństwo danych i zakłócić ciągłość usług.

Dokument skoordynowanego podejścia do szacowania ryzyka wskazuje na zagrożenia zarówno dla operatorów sieci komórkowych, jak i innych podmiotów w ekosystemie usług świadczonych przez sieci 5G. Jako główne obszary podatności zdefiniowano:

- brak wyspecjalizowanego personelu;
- potencjalny brak mechanizmów kontroli procesów oraz niewystarczające bezpieczeństwo używanej infrastruktury IT;
- niewłaściwą architekturę rozwiązań, wpływającą na ciągłość ich działania;
- brak zarządzania procedurami bezpieczeństwa, a zwłaszcza skomplikowanymi i kompleksowymi procesami aktualizacji oraz procedurami zdalnego dostępu.

Podatności specyficzne dla dostawców

Wskazana została potrzeba oceny poszczególnych dostawców i zbudowanie dla nich profilu ryzyka. Jako kluczowe aspekty wymieniono w dokumencie m.in:

- potencjalny związek dostawców z rządem kraju pochodzenia. Zwłaszcza w sytuacji, gdy nie są zbudowane trwałe relacje w postaci umów o bezpieczeństwie lub ochronie danych pomiędzy UE, a krajem z którego pochodzą urządzenia i oprogramowanie;

- umiejętność potwierdzenia ciągłości dostaw, a co za tym idzie – ocena konsekwencji ich przerwania. Do przerwania ciągłości dostaw może dojść zarówno z przyczyn leżących po stronie kraju, w którym technologia jest wytwarzana, jak i w przypadku sankcji wynikających z polityki UE;
- ogólna jakość, rozumiana również jako udokumentowany proces podejścia do zagadnienia wytwarzania bezpiecznych rozwiązań (*security by design*).

Podatności wynikające z braku różnorodności dostawców – uzależnienie od dostawcy

Zarówno polityka cenowa dostawców, jak i możliwe wsparcie finansowe rządu dla producenta w kraju pochodzenia technologii, może doprowadzić do działań uzasadnionych ekonomicznie, ale **zmierzających do braku różnorodności rozwiązań stosowanych przez operatorów telekomunikacyjnych w UE**. Taka sytuacja może z kolei doprowadzić do zwiększenia ogólnej wrażliwości infrastruktury w sieciach 5G w przypadku korzystania z dostawców o wysokim poziomie ryzyka. W dłuższej perspektywie może też skutkować zaburzeniem rynku firm, które wytwarzają oprogramowanie i rozwiązania. Brak stałych kontraktów może oznaczać wyeliminowanie z gry rynkowej uznanych za zaufanych, ale niestety mniej atrakcyjnych cenowo jej uczestników.

Możliwe scenariusze – jak zagrożenia mogą zmaterializować się w rzeczywistości

Identyfikacja kluczowych uczestników, procesów, aktywów oraz konkretnych zagrożeń, pozwala na esencjonalne podsumowanie kluczowych scenariuszy ryzyka.

Scenariusz 1 – Niewystarczające środki bezpieczeństwa.

Scenariusz ten może polegać na niezgodnej z prawidłami konfiguracji sieci oraz niewłaściwej konfiguracji praw dostępu. Doprowadzi to do skompromitowania podstawowych funkcji sieci, nieuprawnionych działań osób lub podwykonawców posiadających uprawnienia administratorów, a w konsekwencji do naruszenia dostępności, integralności i poufności.

Scenariusz 2 – Ryzyko związane z łańcuchem dostaw elementów sieci 5G.

Niska jakość sprzętu oraz procesu wytwarzania oprogramowania może ułatwić złośliwym osobom lub podmiotom, czyli tzw. aktorom, nieuprawnione działania, np. akty szpiegostwa i cyberterroryzm.

Zależność od ograniczonej liczby dostawców może skutkować mniejszą odpornością systemów na awarię. Przerwanie łańcucha dostaw może spowodować brak możliwości odtwarzania systemów lub przerwanie działań serwisowych, naprawczych i rozwojowych.

Scenariusz 3 – Groźne działania aktorów posiadających motywacje polityczne lub przestępcze.

Zarówno wroga motywacja polityczna, jak i przestępcza, związana z wykorzystaniem niezamierzonych luk i błędów w technologii, czy też z intencjonalnym wpływem na producentów i dostawców komponentów sieci 5G, jest szczególnie niebezpieczna. Stwarza ona nowe, bardzo szerokie pole do działań, mogących zakłócić działanie usług nie tylko w celu kradzieży danych, oszustwa czy wymuszenia okupu, ale również w celu destabilizacji konkretnych społeczności i krajów.

Scenariusz 4 – Zależność sieci 5G i systemów krytycznych dla gospodarki oraz państwa.

Rozwój sieci 5G doprowadzi do sytuacji, w której również krytyczne systemy zostaną wyeksponowane na ataki kierowane na infrastrukturę 5G. Mogą to być np. systemy sterowania przemysłowego w kluczowych sektorach gospodarki, lub systemy związane z działaniem służb ratunkowych. Taka współzależność systemów, w połączeniu z innymi przedstawionymi scenariuszami, może spowodować zakłócenia w sektorach szczególnie wrażliwych dla gospodarki, ale również bezpośrednio dla bezpieczeństwa i życia ludności.

Scenariusz 5 – Przejęcie urządzeń końcowych świadczących usługi w sieci 5G.

Rosnąca liczba urządzeń końcowych, zwłaszcza w dobie rozwoju technologii IoT, oraz zróżnicowany poziom wymagań bezpieczeństwa dla poszczególnych rozwiązań, stwarzają ryzyko przejmowania kontroli nad urządzeniami o błahych zastosowaniach, a więc o niskim wymaganym poziomie bezpieczeństwa. Konsekwencją tej z pozoru niewinnej sytuacji może być zarówno przeciążenie sieci niepożądanym ruchem generowanym przez bardzo liczne urządzenia końcowe, jak i stworzenie mocnych przyczółków do bardziej wyrafinowanych, masowych ataków np. w wyniku zarażenia słabo zabezpieczonych urządzeń złośliwym oprogramowaniem.

Toolbox – efekt pracy

Opisując ubiegłoroczne działania na poziomie UE wokół bezpieczeństwa sieci piątej generacji, warto wspomnieć o ***ENISA Threat Landscape for 5G Network***. Dokument ten stanowił cenne wsparcie przy opracowywaniu ostatecznego kształtu dokumentów szacowania ryzyka 5G oraz działań zaradczych zawartych w *toolboxie*, czyli zestawie narzędzi, wspierających w eliminowaniu zidentyfikowanych zagrożeń dla cyberbezpieczeństwa.

Efektem prac, który trudno uznać za ostateczny, ale który kończy pierwszy etap prac inspirowanych przez Komisję Europejską, a prowadzonych wspólnie przez pastwa członkowskie, jest dokument ***Cybersecurity of 5G networks EU Toolbox of risk mitigation***

measures (tzw. *toolbox*). Biorąc pod uwagę jego charakter, zasługiwałby on na osobną publikację, analizującą konkretne zalecenia. Dla uzupełnienia zarysowanego w niniejszym artykule spektrum zagadnień warto jednak przedstawić przynajmniej najważniejsze jego tezy.

We wstępie dokument opisuje funkcjonujący w Unii Europejskiej kontekst ram prawnych i regulacji, które definiują istniejące już środki łagodzące zagrożenia dla cyberbezpieczeństwa. Wymieniane są m.in.:

- Dyrektywa NIS – *NIS Directive (Directive on Security of Network & Information Systems)*;
- *Cybersecurity Act*;
- Europejski Kodeks Łączności Elektronicznej (EKŁE), (*European Electronic Communications Code*, EECC).

Dokument wskazuje też szereg innych regulacji związanych m.in. z ochroną handlu oraz zamówieniami publicznymi, a także podkreśla, że już w obecnym systemie prawnym operatorzy telekomunikacyjni są zobowiązani do:

- szacowania ryzyka i stosowania odpowiednich środków bezpieczeństwa;
- stosowania środków zapewniających odporność na zakłócenia w działaniu sieci i usług;
- zgłaszania znaczących incydentów bezpieczeństwa odpowiednim organom krajowym.

W dalszej części szczegółowo wymieniono interesariuszy: rządy państw członkowskich UE i odpowiednie władze na poziomie krajowym, Komisję Europejską oraz ENISA, operatorów telekomunikacyjnych, operatorów infrastruktury krytycznej czy dostawców sprzętu.

Dokument wskazuje na zalecane do wdrożenia środki zabezpieczeń. Są one podzielone na:

- środki strategiczne;
- środki techniczne;
- działania wspierające, których celem jest zwiększenie efektywności w wymienionych obszarach.

Plany postępowania i łagodzenia ryzyka podzielone są na dziewięć obszarów, będących odzwierciedleniem i rozwinięciem scenariuszy opisanych już powyżej, a przedstawionych w dokumencie szacowania ryzyka zagrożeń w sieci 5G. Dla każdego z planów zostały zaproponowane indywidualnie:

- oczekiwana skuteczność wdrożenia;
- czynniki kluczowe dla wdrożenia konkretnego planu;
- wskazany i oczekiwany czas realizacji – od perspektywy krótkoterminowej (0-2 lata), poprzez średnioterminową (2-5 lat), do długoterminowej (powyżej 5 lat).

Co dalej? Współpraca i solidarność, a może interesy państw członkowskich?

Niedawno minął rok od wydania przez Komisję Europejską rekomendacji wskazującej na potrzebę koordynacji przez państwa członkowskie działań zmierzających do wypracowania podejścia do bezpieczeństwa sieci 5G. W tym czasie wiele się wydarzyło. Państwa członkowskie mogą oprzeć krajowe działania o wypracowane wspólnie raporty i ramy w nich zawarte. Dokumenty te, mimo że powstały wśród licznych wątpliwości, niejednokrotnie przy rozbieżnościach pomiędzy państwami członkowskimi, są wyraźnym sygnałem dla operatorów telekomunikacyjnych oraz producentów rozwiązań dla sieci 5G, pokazującym jakie podejście może być przyjęte w Europie.

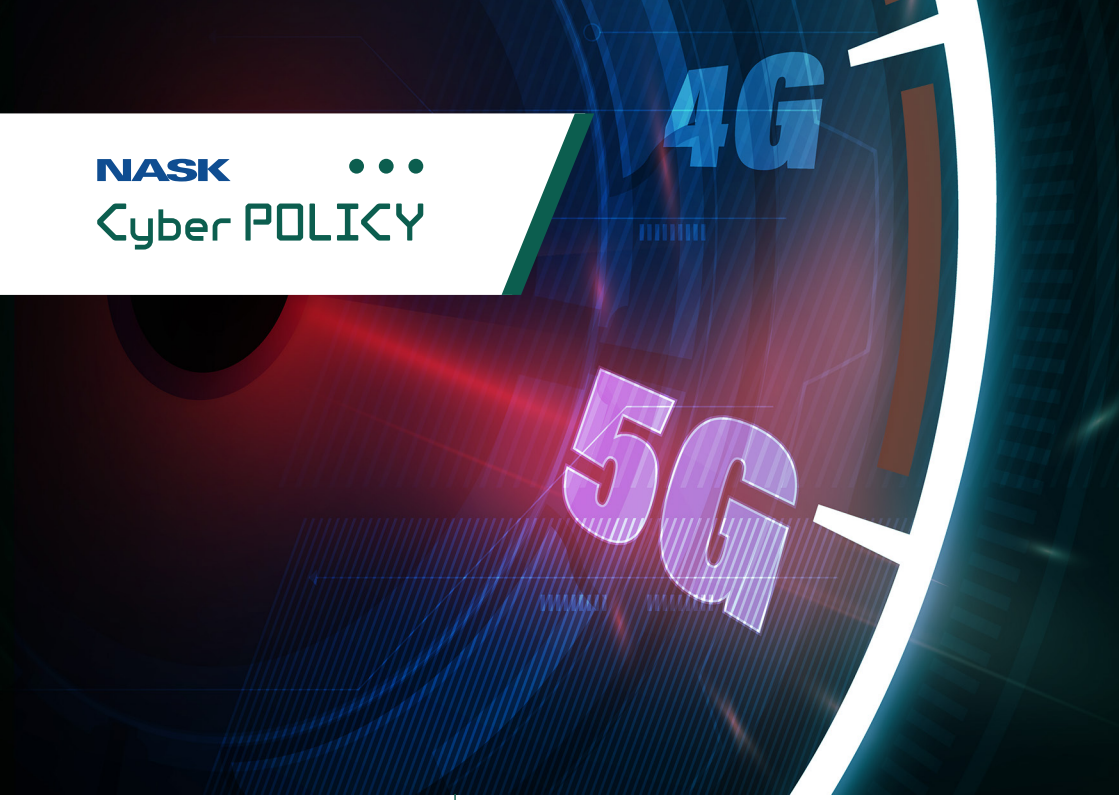
Harmonizacja rozwiązań prawnych i technicznych to ogromne wyzwanie, ale znacznie istotniejsze jest postawienie pytań na poziomie strategicznym. Cyberbezpieczeństwo, jak wiele innych działań strategicznych związanych z bezpieczeństwem Europy, wymaga zrozumienia, że prowadzone indywidulanie działania silosowe, bez uwzględnienia wspólnego podejścia do kluczowych kwestii, oznaczają utratę korzyści dla wszystkich i zmarnowany wysiłek.

Sukces działań, podjętych dla uzyskania wspólnego podejścia do bezpieczeństwa

sieci 5G, będzie zależał teraz od tego, czy implementację wypracowanych mechanizmów uda się przeprowadzić w podobny sposób w całej UE. Brak wewnętrznych, krajowych opartych na wspólnych założeniach rozwiązań prawnych w tym zakresie może doprowadzić do sytuacji, w której **uzgodnione na poziomie modelu podejście okaże się w praktyce niezbyt efektywne. To z kolei prowadziłoby do politycznego osłabienia Unii i podważałoby wiarygodność podjętych działań.**

Zrozumiałe jest, że dla operatorów telekomunikacyjnych, którzy będą ponosili część wysiłku i kosztów związanych z ujednoliceniem podejścia do bezpieczeństwa, stanowi to pewne obciążenie i niedogodność. Warto jednak podkreślić, że raz zbudowany system współpracy, może być opłacalny również w przyszłości, ponieważ uprości przyszłe debaty łączące politykę, ekonomię i technologię. Cyberbezpieczeństwo – podobnie jak sieci telekomunikacyjne – to obszary ponadnarodowe i ponadpaństwowe. Zbudowanie silnej i odpornej na zagrożenia podstawy dla dalszego rozwoju jednolitego rynku cyfrowego powinno być w interesie wszystkich.

Dlatego z satysfakcją trzeba zauważyć, ze w ramach grupy współpracy pojawiła się inicjatywa zmierzająca do zaproponowania na poziomie europejskim wspólnego podejścia do certyfikacji elementów sieci 5G. Certyfikacja, a zwłaszcza jej utrzymanie dla produktów, których jakość i bezpieczeństwo jest uzależnione od oprogramowania i jego aktualizacji, to duże wyzwanie. Jest to jednak również ogromny impuls do tego, by kontynuować pracę podjętą w 2019 roku i ułatwić zarówno bezpieczną implementację sieci 5G w Europie, jak i utrzymanie tego bezpieczeństwa na oczekiwanym poziomie.



Dr hab. inż. Jordi Mongay Batalla

Jak należy zaadresować wyzwania związane z bezpieczeństwem w ochronie sieci 5G?

Jordi Mongay Batalla – dyrektor ds. naukowych w Instytucie Łączności – PIB. Jest także związany z Politechniką Warszawską, gdzie uczy sieci mobilnych czwartej i piątej generacji. Jego zainteresowania badawcze koncentrują się głównie na technologiach (mobilnych: 4G i 5G, przewodowych: sieć usług sieciowych, SDN) i aplikacjach (Internet Rzeczy, Smart Cities, multimedia, blockchain) dla Internetu przyszłości. Napisał ponad 150 artykułów naukowych w renomowanych międzynarodowych czasopismach (IEEE ComMag, IEEE JSAC, IEEE WCM, ACM CSUR, etc.) i konferencjach, a także jest członkiem rad edytorskich kilku czasopism (IEEE CL, Springer HCIS, etc.).

Rozwój sieci 5G, zwanej także siecią nowej generacji, jest związany z nowatorskimi elementami technicznymi. Jej funkcje są różne, od tych znanych z sieci 4G. Ma to bezpośredni wpływ na wyzwania z zakresu bezpieczeństwa, jakie stoją przed sieciami mobilnymi. Dlatego ważna jest ich analiza. W tym kontekście, coraz istotniejsza staje się kwestia tego, w jaki sposób dostawcy sprzętu i oprogramowania 5G odpowiedzieli na wyzwanie, jakim jest zapewnienie bezpieczeństwa oraz, jak inni użytkownicy sieci (w tym także władze publiczne) mogą adresować to wyzwanie, poprzez zapewnienie planów oceny ryzyka.

Cechy sieci 5G

W najbliższych latach zostaną wprowadzone setki nowych usług i aplikacji, które będą korzystać z zaawansowanych funkcji sieci 5G. Nowe scenariusze przewidziane w 5G to:

- **Ultra niezawodna komunikacja o niskim opóźnieniu** (*Ultra Reliable Low Latency Communication*, URLLC), w tym aplikacje o ścisłych wymaganiach dotyczących opóźnienia i niezawodności w komunikacji o znaczeniu krytycznym, takie jak zdalna medycyna, w tym operacje prowadzone zdalnie, autonomiczne pojazdy lub dotykowy Internet (*Tactile Inetrnet*);
- **Ulepszony mobilny Internet szerokopasmowy** (*enhanced Mobile BroadBand*, eMBB), który obejmuje przypadki użycia oparte na danych, wymagające wysokich prędkości transmisji danych w szerokim obszarze zasięgu;
- **Masowa komunikacja między maszynami** (*massive Machine-Type Communication*, mMTC), która obsługuje bardzo dużą liczbę urządzeń na niewielkim obszarze, mogących wysyłać dane tylko sporadycznie, na przykład przypadki użycia Internetu Rzeczy (*Internet of Things*, IoT).

Koncepcja dzielenia sieci umożliwia tworzenie dedykowanych sieci dla każdego z wyżej wymienionych scenariuszy. Wydzielone segmenty są wdrażane za pomocą oprogramowania i współużytkują pojedynczą, zwirtualizowaną infrastrukturę. Scenariusze 5G wprowadzą nowatorskie, rewolucyjne aplikacje i usługi dla klientów, szczególnie dla klientów biznesowych, nazywane po angielsku *verticals*:

- Aplikacje **URLLC** wymagają umieszczenia węzłów serwisowych blisko dostępu radiowego, aby zminimalizować ogólne opóźnienie usługi. Ta koncepcja znana jest jako *Multi-access Edge Computing* (MEC) i stanowi ewolucję przetwarzania w chmurze. MEC przenosi hosting aplikacji ze scentralizowanych środków danych na skraj sieci, bliżej konsumentów i danych generowanych przez aplikacje.
- **eMBB** będzie wykorzystywać długotrwałą sesję i wygeneruje ogromny ruch potrzebny do transmisji strumieniowej 4k/8k lub rzeczywistości rozszerzonej/wirtualnej. Sprawne świadczenie usług

eMBB za pośrednictwem nowo powstałej sieci mobilnej będzie odgrywać kluczową rolę w realizacji koncepcji inteligentnych rozwiązań.

Wiele postulatów dotyczących inteligentnych miast, takich jak *smart entertaimnent*, *smart tourism* czy *smart monitoring*, jest związanych z transmisją strumieniową multimediów, która stanowi kluczowy element scenariusza eMBB. Aplikacje *Smart City* są powiązane ze znaczną ilością danych, które mają być przetwarzane i analizowane, co jest trudne, szczególnie w gęstym środowisku miejskim.

- **mMTC** odnosi się do transmisji istotnych, małych pakietów, szczególnie z czujników IoT. Jednak niektóre scenariusze mMTC mogą obejmować komunikację krytyczną (np. czujniki awaryjne) i/lub mogą wymagać transmisji dużych ilości danych między maszynami (np. w celu nadzoru).

Wymienione aplikacje i usługi nakładają na sieć 5G szereg wymagań, takich jak: duże wolumeny przesyłanych danych, wysoka pojemność sieci, bardzo liczne podłączone do sieci urządzenia, zmniejszenie konsumpcji energii, niskie opóźnienie, reedukacja kosztów operacyjnych (*Operational Expenditures*, OPEX) i redukcja czasu wdrożenia usługi. Wymagania te zostały szczegółowo omówione poniżej.

- **Duże wolumeny danych** i wysoka pojemność związane są ze znacznie wyższą przepływnością, potrzebną w sieciach 5G, w porównaniu z poprzednimi sieciami mobilnymi.

- **Wyższe prędkości transmisji** zostaną osiągnięte przy dostępie radiowym dzięki zwiększonej dostępnej szerokości pasma, wyższej wydajności medium i wyższej gęstości komórek. 5G obejmie następujące pasma w Europie: **700 MHz** zostanie wykorzystane do zapewnienia płynnego zasięgu na dużych obszarach. **3,5 GHz** będzie pasmem podstawowym, przyjmującym najwięcej aplikacji i zostanie podzielone na bloki szerokopasmowe. **26 GHz** będzie wykorzystywane w mikrokomórkach jako np. zarządzanie przejazdami drogowymi. Wyższa wydajność medium zostanie osiągnięta w 5G poprzez wprowadzenie kilku mechanizmów, takich jak mechanizmy zarządzające interferencjami sygnału lub mechanizm *Multiple-Input Multiple-Output* (MIMO), które umożliwiają transmisję i odbiór wielu sygnałów i danych jednocześnie przez ten sam kanał radiowy. Wyższą gęstość komórek osiąga się przez zapewnienie wielu pikokomórek. Dzięki temu liczba użytkowników, którzy mają być obsługiwani w danej szerokości pasma, zmniejsza się, co powoduje wzrost przepustowości na użytkownika.

- **Liczne urządzenia** zostaną podłączone do sieci dzięki technologii używającej wąskie pasmo (*Narrowband*) stosowanej

specjalnie w aplikacjach *Internet of Things* (IoT). *Narrowband-IoT* oferuje duży zasięg przy niskich kosztach i ulepszonych mechanizmach bezpieczeństwa w porównaniu do innych platform komunikacyjnych IoT, takich jak LoRa lub WiFi.

- **Mniejsza konsumpcja energii** (w porównaniu do roku 2010) nie jest ściśle związana z siecią, ale z postępem technologii materiałowych, które umożliwiają zmniejszenie zużycia energii we wszystkich urządzeniach. Dodatkowo w sieci 5G istnieją pewne mechanizmy ukierunkowane na oszczędność zużycia energii. Dobrym przykładem jest pojedynczy dostęp do kanału lub wielodostęp z nie-ortogonalnym podziałem częstotliwości, zaproponowany dla łączy od terminala do radiostacji (*uplink*). Pojedynczy i nie-ortogonalny wielodostęp cechuje mniejsza niż w przypadku dostępu ortogonalnego wydajność, natomiast jednocześnie mniejszy jest narzut na sygnalizację między terminalem i anteną, co pozwala na redukcję zużycia baterii w terminalach końcowych.
- **Niskie opóźnienia** są możliwe dzięki technologii MEC oraz wirtualizacji funkcji sieciowych, co umożliwia szybkie wykonanie operacji związanych z tymi usługami sieciowymi.
- Bardzo ważna dla biznesu będzie redukcja OPEX i **redukcja czasu wdrożenia usługi**. Zostanie to osiągnięte dzięki nowemu podejściu do podstawowej części sieci opartemu na wirtualizacji i programowaniu (otwartości) sieci. Wirtualizacja zapewnia separację usług i aplikacji, co z kolei przyspiesza wdrażanie nowych usług w sieci. Oprogramowanie to znacznie obniża koszty i umożliwia dostosowanie sieci do nowych usług (wysoka elastyczność).

Bezpieczeństwo sieci 5G

Fakt, że jako nowa technologia sieć 5G jest obecnie rozwijana i wdrażana, stwarza możliwość stworzenia nowego podejścia do bezpieczeństwa. Nie tylko poprzez odpowiedź na zagrożenia, ale także poprzez **uwzględnienie potencjalnych zagrożeń, już na etapie projektowania sieci i rozpoczęcia rozwoju jej elementów**. Warto przy tym podkreślić, że całkowite bezpieczeństwo nigdy nie będzie możliwe do osiągnięcia.

Powszechnie istnieją różne podejścia do bezpieczeństwa 5G, w zależności od interesariusza zaangażowanego w bezpieczeństwo. W tym tekście analizowane są dwa z nich: podejście podjęte przez dostawcę sprzętu i przez regulatora rynku.

Dostawcy elementów sieci 5G (HW i SW), przy projektowaniu sieci, starają się przyjąć całościowe podejście do bezpieczeństwa. Czasami to samo podejście przyjmują również operatorzy, szczególnie najwięksi z nich. Inne zainteresowane strony, takie jak rządy i organy regulacyjne, oraz twórcy oprogramowania i użytkownicy końcowi (np. firmy korzystające z sieci do celów biz-

nesowych), skupiają się przede wszystkim na ocenie ryzyka i wdrożeniu na jej podstawie środków zaradczych.

Podejście oparte na bezpieczeństwie od podstaw (*security-by-design*)

Dla dostawców rozwijających 5G, sieć wprowadza dużą liczbę zagrożeń, które wymagają całościowego podejścia do bezpieczeństwa. Jest ono nazywane bezpieczeństwem od podstaw (*security by design*). Oznacza to, że kwestie bezpieczeństwa są uwzględnienie już na najwcześniejszych etapach rozwoju systemu, tj. na etapie koncepcji oraz w krytycznych momentach wdrożenia samej sieci. Dzięki ciągłej analizie wymagań dotyczących ryzyka, dostawcy sprzętu i operatorzy będą mieli większą szansę na sprostanie niektórym wyzwaniom związanym z bezpieczeństwem 5G. W razie potrzeby operatorzy mogą włączyć dodatkowe mechanizmy ochronne.

W zintegrowanym środowisku 5G istnieje wiele elementów sieci, w których potencjalnie mogą pojawić się różnego rodzaju problemy z bezpieczeństwem. Te elementy to:

- aplikacje i usługi sieciowe (warstwa aplikacyjna),
- urządzenia końcowe (wszystkie warstwy),
- połączenia sieciowe (warstwa sieciowa),
- infrastruktura fizyczna.

Bezpieczeństwo od podstaw zakłada wbudowanie mechanizmów bezpieczeństwa w protokoły komunikacyjne i systemy infrastruktury, obejmujące wszystkie aspekty kompleksowego systemu komunikacji.

Usługi i aplikacje obejmują każde oprogramowanie dla użytkowników działające w środowisku 5G. Do użytkownika można się odwoływać na różne sposoby: systemy, klienci indywidualni, partnerzy biznesowi, klienci biznesowi, itp. Z punktu widzenia bezpieczeństwa istotna jest analiza interakcji usługi lub aplikacji z innymi usługami/aplikacjami, urządzeniami, na których działa, sieciami, które przenoszą generowane wiadomości, a także z samą infrastrukturą.

Także same urządzenia końcowe w sieci 5G, przedstawiają liczne wyzwania związane z zabezpieczeniami. Przewiduje się, że do infrastruktury mobilnej 5G, za pomocą różnych technologii dostępu, podłączonych będzie szereg urządzeń. W efekcie, obsługa standardowych mechanizmów bezpieczeństwa może nie być łatwo dostępna na każdym urządzeniu. Wymaga to analizy poszczególnych przypadków dla każdego typu urządzenia.

Sieci 5G zintegrują połączenia używające różnych technologii dostępu do sieci i komunikujące się z różnymi systemami z sieci Internet (chmura, mgła). Każde połączenie może być potencjalnie zarządzane przez różnych operatorów (wielodomenowe połączenie) lub przez osoby trzecie (np. zewnętrzne firmy zarządzające pewnym ruchem).

Aby osiągnąć większą elastyczność i skalowalność w działaniu systemów, sieci 5G będą miały zintegrowane rozwiązania wirtualizacji funkcji sieciowych (*Network Function Virtualization*, NFV). Chodzi o zwirtualizowany system, który jest uruchomiony na bazie infrastruktury wirtualnej, wspierający autonomiczne zarządzanie usługami sieciowymi. Operatorzy już dostrzegają korzyści płynące z uruchamiania usług wirtualizacji w systemach 4G. W 5G, technologie wirtualizacji funkcji sieciowych NFV oraz *Software Defined Networking* (SDN), czyli realizacja funkcji sieciowych w oparciu o oprogramowanie, będą kluczowe jako technologie wspierające.

Wirtualizacja ta różni się radykalnie od starszych systemów mobilnych, działających na stałych rozwiązaniach sprzętowych. Ma to liczne zalety w zakresie bezpieczeństwa. Przede wszystkim, zapewnia logiczną architekturę bezpieczeństwa. Powinno to pozwolić na większą elastyczność, zmniejszając krytyczne znaczenie fizycznej alokacji funkcji bezpieczeństwa, jak miało to miejsce w przypadku starszych systemów. Jest to następstwem wirtualizacji usług i istnieniem wielu domen działania z udziałem różnych podmiotów. Logiczna architektura pozwoliłaby na elastyczne modele zaufania, zarządzanie bezpieczeństwem i dynamiczne dzielenie funkcji sieciowych.

Poza oprogramowaniem, usługami i aplikacjami, niezwykle ważne jest, aby sprzęt fizyczny infrastruktury nie był modyfikowany i był bezpiecznie instalowany. Dostęp do niego powinni mieć tylko uprawnieni pracownicy. Właśnie dlatego, niezwykle istotne jest aby cały system, ze wszystkimi elementami i relacjami między nimi, rozpatrywać w kontekście zapewnienia bezpieczeństwa, już w fazie projektowania.

Podejście do oceny ryzyka

W celu zapewnienia tak zwanej ekonomii cyberbezpieczeństwa, wielu interesariuszy musi przyjąć podejście polegające na ocenie ryzyka. Ocena ryzyka to równowaga między kosztem ryzyka, a kosztem środków ograniczających ryzyko. Koszt może dotyczyć zarówno aspektów funkcjonalnych, takich jak wydajność, jak i pieniędzy.

Każda metodologia ukierunkowana na ocenę ryzyka 5G powinna uwzględniać fakt, że 5G jest siecią jeszcze nieznaną. Z tego powodu w każdym planie oceny ryzyka należy uwzględnić następujące kroki:

- Wybranie odpowiednich kryteriów oceny i akceptacji ryzyka w oparciu o kontekst.
- Zidentyfikowanie odpowiednich zdarzeń i scenariuszy ryzyka (identyfikacja ryzyka).
- Zidentyfikowanie możliwych konsekwencji dla danego zdarzenia i prawdopodobieństwa scenariuszy ryzyka (analiza ryzyka).
- Zastosowanie kryteriów akceptacji ryzyka do ocenianego ryzyka (oszacowanie ryzyka).

Pierwszy z tych kroków jest uznawany za najtrudniejszy, zwłaszcza wobec małej jeszcze wiedzy o szerszym kontekście funkcjonowania sieci 5G. Można jedynie zdefiniować kontekst dotyczący znanych faktów w sieci i własnej analizy zagrożeń bezpieczeństwa, które mogą z nich wynikać.

Kontekst musi uwzględniać bezpośredni związek koncepcji architektury 5G z zagrożeniami bezpieczeństwa i potencjalnymi działaniami łagodzącymi.

Można wyróżnić następujące cechy sieci 5G:

- jest oparta na usługach,
- istnieje oddzielenie płaszczyzn użytkownika i sterowania,
- jest dynamicznie zarządzana,
- opiera się na otwartych interfejsach z możliwie małymi funkcjami na interfejs (umożliwia to interoperacyjność wielu dostawców),
- architektura jest otwarta na rozdzielenie ruchu w zależności od aplikacji,
- obsługuje różnorodne technologie dostępu radiowego, oprócz dostępu 5G.

Każda mobilna sieć telekomunikacyjna, a 5G nie jest w tym zakresie wyjątkiem, składa się z kilku części, z których dwie są szczególnie istotne w ocenie bezpieczeństwa:

- **sieć rdzeniowa**, która jest centralnym elementem sieci podłączonej do szerszego Internetu, i odpowiada za kontrolowanie funkcjonowania sieci i połączeń od końca do końca;
- **sieć dostępu radiowego** odpowiedzialna za podłączanie urządzeń do sieci i składająca się ze stacji bazowych, które z kolei są połączone z siecią rdzeniową. Te dwie części są nazywane odpowiednio *5G Core* i *5G New Radio*.

Rdzeń 5G (*5G Core, 5GC*). Architektura systemu 5G ma budowę modułową, w której elementy sieci rdzeniowej mogą być tworzone wielokrotnie, aby zapewnić tzw. *slice* sieci. *Slice* sieciowy umożliwia zróżnicowane traktowanie (w zależności od wymagań) każdego klienta, gdzie klientem jest użytkownik biznesowy wynajmujący dany *slice*. W ten sposób, operator sieci może uznać użytkowników za należących do różnych rodzajów dzierżawców i zaoferować im różne usługi na podstawie subskrypcji. Każdy *slice* zapewnia separację ruchu dla różnych aplikacji biznesowych. Organizacja, czy też orkiestracja, *sliceów* pozwala na wysoką modułowość wycinków. Warto podkreślić, że 3GPP[18] określa podział sieci (*slice*) w zakresie zasobów określonych przez 3GPP (rdzeń i radio), a nie obligatoryjnie na poziomie całej sieci Internet. Zakłada się jednak, że operatorzy będą wymuszać pewną kontrolę w odniesieniu do zasobów nieokreślonych przez 3GPP, lub będą przynosić usługi do kontrolowanej sieci komórkowej.

[18] 3GPP to najważniejsza międzynarodowa organizacja normalizacyjna mająca na celu rozwój systemów telefonii komórkowej. Standardy 3GPP są dominujące w sieciach GSM (2G), UMTS (3G), LTE (4G) i teraz także 5G.

Jedną z głównych cech architektury jest rozdzielenie operacji sterowania połączeń (płaszczyzna sterowania) i operacji przekazania pakietów danych (płaszczyzna użytkownika, *User Plane Function, UPF*). **Operacje płaszczyzny użytkownika** są kontrolowane przez **funkcję zarządzania sesją** (*Session Management Function, SMF*), która znajduje się na płaszczyźnie sterowania. Inne operacje płaszczyzny sterowania są scentralizowane w **funkcji zarządzania dostępem** (*Access Management Function*, AMF), która oferuje szybkie ustanawianie i modyfikowanie nowych nośników. Tak więc ważną cechą 5GC jest separacja między UPF, SMF i AMF. Dzięki tej separacji, implementacja sieci (całe oprogramowanie) może być podzielona w różnych modułach i łatwo jest powielać niektóre z nich dla różnicowania poszczególnych ruchów (na przykład różnicowania usługi krytycznej od usługi głosowej).

Inną ważną cechą 5GC jest oparcie na usługach, tj. elementy architektury płaszczyzny sterowania, a przynajmniej większość z nich, są zdefiniowane jako funkcje sieciowe. Oferują one obsługę za pośrednictwem interfejsu z dowolnymi, innymi funkcjami sieciowymi. Istnieje również ustalona platforma do identyfikacji i wywołania usług oferowanych przez inne funkcje sieciowe (w tym pamięć).

Nowe mechanizmy takie jak MEC, który przeniesie do krawędzi sieci (tj. obliczenie brzegowe) inne funkcje oprócz transportu płaszczyzny użytkownika, potrzebują innego zarządzania sesjami. Dlatego 5GC obsługuje trzy różne tryby ciągłości sesji i usług, które obejmują mechanizm zwalniania powiązań transportowych terminala użytkownika (*User Equipment*, UE) z jednego AMF i ponownego wiązania z innym AMF. **Ta elastyczność powiązań transportowych pozwala na równoważenie obciążenia procesów w systemie**. Warto równocześnie podkreślić, że elastyczność ta bywa czasami czysto teoretyczna (opis architektury), natomiast jej implementacja ma ograniczenia, co zostanie opisane poniżej.

Inną ważną cechą rdzenia 5G jest możliwość pracy z wieloma technologiami dostępu radiowego (*multi-Radio Access Technology*, multi-RAT), w szczególności z technologiami nielicencjonowanymi. Technologie dostępu bezprzewodowego poza zakresem technologii 3GPP (tj. inne niż 2G/3G/4G/5G), mogą być zaufanym lub niezaufanym dostępem bezprzewodowym. Decyduje o tym operator sieci. 5GC pozwala AMF obsługiwać niezaufane technologie i przekazywać bieżące transmisje (połączenia są zakotwiczone w AMG 5GC). Z pewnością istnieje wiele aspektów, które należy wziąć pod uwagę w scenariuszach z wieloma RAT, na przykład uwierzytelnianie użytkowników i jakość usług.

Nowe radio 5G (*5G New Radio*, 5G NR). 5G NR zachowuje cechy 5GC w odniesieniu do separacji sygnalizacji i transportu, czyli płaszczyzny użytkownika i sterowania.

Dzieje się tak nawet w schemacie adresowania, uproszczenia interfejsów i możliwości tworzenia *sliceów* (wycinków, plastrów, segmentów) w dostępie radiowym. Jedną z najnowszych funkcjonalności jest zachowanie sieciowych *sliceów*. Ważne, aby podkreślić, że ich liczba na poziomie radiowym jest ograniczona do kilkuset. To powinno wystarczyć dla większości operatorów. Z kolei urządzenie użytkownika końcowego może obsługiwać tylko kilka *sliceów*. Różne wycinki są przeznaczone do różnej obsługi ruchu (na podstawie umów o poziomie usług). Osiąga się to poprzez egzekwowanie zasad z różnicowaniem jakości usługi. Ponadto, 5G NR powinno zapewniać izolację wycinków, aby przepełnienie ruchu jednego nie wpłynęło na inne. Dwie ważne kwestie, z punktu widzenia oceny bezpieczeństwa, to z jednej strony fakt, że funkcje obsługiwane przez każdy wycinek (w tym izolacja zasobów) nie są zdefiniowane w standardzie i będą zależeć od implementacji. Z drugiej strony, dostępność fragmentów sieci w radiu nie jest zapewniona w żadnym fizycznym miejscu użytkownika.

5G NR wdraża twarde mechanizmy bezpieczeństwa oparte na szyfrowaniu (w celu zapewnienia poufności danych) i integralności. Warto zauważyć, że klucze bezpieczeństwa 5G NR są wyraźnie oddzielone od kluczy 5GC.

Z punktu widzenia bezpieczeństwa 3GPP (patrz 3GPP TS 33.501) wprowadzono dodatkowe opcje lub obowiązkowe zasady gwarancji bezpieczeństwa w NR podłączonej do 5GC. Główne zasady przedstawione przez 3GPP to:

- W przypadku **danych użytkownika** (nośniki danych, *Dedicated Radio Bearer*, DRB) szyfrowanie zapewnia poufność danych, a ochrona integralności zapewnia nietykalność danych użytkownika. Szyfrowanie i ochrona mogą być (opcjonalnie) skonfigurowane dla DRB. W każdym razie szyfrowanie i ochrona integralności są wymagane dla wszystkich DRB należących do sesji jednostki danych pakietowych (*Packet Data Unit*, PDU) z wymaganą ochroną płaszczyzny użytkownika (UP) (patrz 3GPP TS 23.502);
- W przypadku **sygnalizacji RRC** (*Radio Resource control*), tj. sygnalizacyjne nośniki radiowe (*Signaling Radio Bearer*, SRB) szyfrowanie zapewnia poufność danych sygnalizacyjnych i ochronę integralności tych danych. W sygnalizacji RRC szyfrowanie jest obowiązkowe.
- W przypadku **zarządzania kluczami i przetwarzania danych**, każdy podmiot przetwarzający czysty tekst powinien być chroniony przed atakami fizycznymi i znajdować się w bezpiecznym środowisku;
- Klucze gNB (*Access Stratum*, AS) są kryptograficznie oddzielone od kluczy 5GC (*Non-Access Stratum,* NAS);
- Stosowane są oddzielne procedury poleceń trybu bezpieczeństwa (SMC) na poziomie AS i NAS;

- Numer sekwencyjny (COUNT) jest wykorzystywany jako dane wejściowe do szyfrowania i ochrony integralności. Dany numer sekwencyjny musi być użyty tylko raz dla danego klucza (z wyjątkiem identycznej ponownej transmisji) na tym samym nośniku radiowym, w tym samym kierunku.

Oprócz architektury 5G, plany oceny ryzyka muszą uwzględniać funkcjonujące implementacje w takiej formie, w jakiej się pojawiają.

Architektura 5G określona przez 3GPP, ze względu na elastyczność i skalowalność, została zdefiniowana z wysokim poziomem otwartości. Jednak zagadnienie to komplikuje się w obliczu implementacji. Jednym z największych wyzwań we wdrażaniu sieci mobilnych, jest współpraca urządzeń pochodzących od wielu dostawców. Interoperacyjność nie będzie łatwa, chociaż taki jest cel architektury 5G.

Ze względów bezpieczeństwa, ograniczenia interoperacyjności sprzętu wielu dostawców mają szczególne znaczenie, ponieważ ogranicza to otwartość sieci. Poniżej przedstawiono dwa przykłady, które pojawiają się lub będą pojawiać przy pierwszych wdrożeniach sieci:

- **Interoperacyjność 5G NR**. Ewolucja z 4G/LTE do 5G NR proponuje zmianę w zakresie odpowiedzialności funkcjonalnej: funkcje zapewniane w 4G/LTE przez BBU + RRU zostaną w 5G wdrożone w 3 modułach: Jednostka centralna (*Central Unit*, CU), jednostka rozproszona (*Distributed Unit*, DU) i jednostka zdalnego radia (*Remote Radio Unit*, RRU). 5G ETSI pracują nad interfejsem radiowym ORI-Open, jednak do tej pory zainteresowanie operatorów było niewielkie, aby wdrożyć ten standard. Niektórzy liderzy wśród operatorów tak jak np.: Vodafone pracują nad Open RAN. Oba te standardy mają na celu zdefiniowanie tych samych reguł komunikacji (protokołów i formatów danych) w taki sam sposób dla wszystkich urządzeń, co rozwiązałoby wiele problemów związanych ze współpracą. Jednak prawda jest taka, że standardy te nie zostały jeszcze sfinalizowane i nie jest jasne, czy zdobędą prawdziwą pozycję na rynku.

  Standardem bardziej zaawansowanym jest eCPRI 2.0, który jest specyficzną dla 5G ewolucją *Common Public Radio Interface* (CPRI), standardu szeroko stosowanego w 4G/LTE przez wielu dostawców i operatorów, takich jak Ericsson, Nokia, Huawei i NEC. Ten standard określa niektóre dane „specyficzne dla dostawcy" w warstwie 2, co bardzo utrudnia integrację modułów od różnych dostawców.

- **Kompleksowe rozwiązania chmurowe**. Nawet jeśli architektura *5G Core* została zdefiniowana pod kątem wysokiej modułowości i elastyczności, prawdopodobne jest, że wdrożone rozwiązania 5GC są zintegrowane w jednym systemie zawie-

rającym wszystkie funkcje 5GC, a nawet dostęp radiowy. Takie rozwiązania będą działały w centrach danych w chmurze i będą one kontrolować wszystkie funkcjonalności sieci rdzeniowej i niektóre funkcje sieci dostępu radiowego (w przypadku masowych anten MIMO). Będą one również obejmować ujednolicone zarządzanie bazą danych. Rozwiązania te są dość atrakcyjne dla operatorów sieci, ponieważ rozwiązują wiele problemów związanych ze współpracą między sprzętem różnych dostawców, jednak z punktu widzenia bezpieczeństwa całego systemu stanowi to pewne wyzwanie, ponieważ zintegrowanie wszystkich modułów zostawia całe rozwiązanie bezpieczeństwa w rękach jednego dostawcy, blokując współpracę wielu silosowych rozwiązań.

Podsumowując, sieć 5G (i przyszłe sieci mobilne) jest jednym z najbardziej obiecujących postępów technologicznych naszych czasów i stanie się podstawą rozwoju cyfrowego świata w nadchodzących latach. Dlatego tak ważne jest, aby w pełni zrozumieć korzyści i zagrożenia, które zapewni. Niezwykle istotne wdaje się także podejmowanie zdecydowanych działań, zarówno w zakresie maksymalizacji korzyści, jak i minimalizacji ryzyka.

Ten artykuł jest owocem pracy zrealizowanej w ramach projektu „5G@PL: Wdrażanie sieci 5G w gospodarce polskiej", realizowanego w ramach strategicznego programu badań naukowych i prac rozwojowych Gospostrateg z Narodowego Centrum Badań i Rozwoju.

dr inż. Jacek Falkiewicz, Ericsson

Bezpieczeństwo sieci 5G w ujęciu holistycznym

dr inż. Jacek Falkiewicz – Ekspert z ponad dwudziestoletnim doświadczeniem w branży ICT. Ukończył Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, na którym uzyskał również stopień naukowy doktora nauk technicznych. W latach 1999-2006 pracował jako asystent naukowo-dydaktyczny Politechniki Warszawskiej specjalizując się w cyfrowym przetwarzaniu sygnałów w zastosowaniach telekomunikacyjnych.

W firmie Ericsson w Polsce pracuje od 2006 roku. Kierował działem serwisowym firmy odpowiedzialnym za realizację projektów i kontraktów usługowych. Obecnie pełni funkcje dyrektora sprzedaży oraz pełnomocnika Zarządu firmy ds. współpracy z jednostkami naukowo-badawczymi.

Nowe formy łączności bezprzewodowej wywołują cyfrową transformację, która zmienia całe branże i zmusza do ponownego przemyślenia tradycyjnych metod pracy. Transformacja ta zmienia nie tylko sposób, w jaki pracujemy z urządzeniami IT, narzędziami biurowymi i systemami administracyjnymi, ale tworzy także nowe możliwości biznesowe. Łańcuchy wartości stają się sieciami wartości, w których relacje pomiędzy dostawcami, sprzedawcami, operatorami i użytkownikami końcowymi są przekształcane w ekosystemy partnerów i współtwórców.

Dzięki Internetowi rzeczy (IoT) i Przemysłowi 4.0, z nowymi i szerszymi zbiorami aplikacji zostanie połączonych wiele nowych typów urządzeń o mniejszej jednorodności niż dzisiejsze komputery PC i smartfony. Dotyczy to nie tylko aplikacji i treści opartych na dostępie do Internetu, ale także krytycznych, pracujących w czasie rzeczywistym systemów kontroli przemysłowej, takich jak przemysłowe systemy automatyki i sterowania. Kolejna era cyfrowa nie będzie więc ograniczona do danych za ekranami i klawiaturami, ale za sprawą robotów, czujników i autonomicznych procesów cyberfizycznych wejdzie w domenę cyberfizyczną.

Transformacja cyfrowa wprowadzi również nowe wymiary wektorów ataku, wartości i podatności. Internet Rzeczy wiąże się z nowymi problemami, takimi jak bezpieczeństwo i niezawodność systemów cyberfizycznych. W związku z tym, w wielu obszarach przemysłu pojawią się nowe rodzaje ataków, a także nowe przepisy dotyczące prywatności i bezpieczeństwa teleinformatycznego.

Temat bezpieczeństwa i prywatności budzi żywiołowe reakcje oraz wysokie oczekiwania zarówno wśród obywateli, jak i rządów. Równocześnie bezpieczeństwo informacji stanowi główny problem dla przedsiębiorstw rozpoczynających transformację cyfrową. Konieczne jest zatem, aby mechanizmy bezpieczeństwa zastosowane w domenie Internetu Rzeczy zapewniały ochronę danych osobowych, informacji wrażliwych dla biznesu, jak również zabezpieczały infrastrukturę krytyczną. Dlatego wyraźnie widać oczekiwanie, że organy regulacyjne zachowają równowagę między ochroną prywatności, ochroną bezpieczeństwa narodowego, stymulowaniem wzrostu gospodarczego i korzyściami płynącymi dla całego społeczeństwa. Warunkiem sukcesu transformacji 5G jest rozpoznanie nowych zagrożeń i znalezienie sposobów ich łagodzenia.

Zagrożenia w sieci 5G

W ciągu ostatnich dziesięciu lat, zagrożenia dla cyberbezpieczeństwa, przed którymi stoją społeczeństwa i różne branże nie uległy znaczącym zmianom. Powszechnym sposobem infekowania urządzeń i zdobywania przyczółków dostępu do systemu informatycznego będącego celem ataku nadal jest stosunkowo proste złośliwe oprogramowanie. Jednocześnie sieci telekomuni-

kacyjne, do budowy których wykorzystywany jest specjalistyczny sprzęt, mogą być atakowane przez złośliwe oprogramowanie, które jest dużo bardziej skomplikowane. Oprócz różnorodności i poziomu wyrafinowania zagrożeń technicznych, z biegiem czasu zmienia się także sposób działania podmiotów atakujących, a także spektrum zagrożeń cybernetycznych.

Crime-ware – zestawy narzędzi służące do ataków cybernetycznych są obecnie sprzedawane jako usługa uzupełniona o opcje takie jak okresy próbne, wsparcie użytkownika 24/7, dedykowane fora dyskusyjne oraz wielojęzyczna dokumentacja. Przyczyniło się to do gwałtownego wzrostu częstotliwości cyberataków. Podniosło to również niestety atrakcyjność tego typu działań – cyberataki stanowią przestępstwo o niskim ryzyku i wysokiej opłacalności. Ze względu na wysoki stopień cyfryzacji branż i usług publicznych zwiększona częstotliwość ataków sprawia, że ataki takie są bardziej dotkliwe. Kiedy w grę wchodzą pieniądze zainteresowanie ze strony przestępców rośnie. Pochodzą oni głównie z wrogich podmiotów zewnętrznych, ale mogą to być również osoby z wewnątrz organizacji, np. pracownicy lub podwykonawcy. Przykładowo dostęp do systemu fakturowania i pobierania opłat w sieci telekomunikacyjnej umożliwia popełnianie przestępstw przez osoby o złych intencjach. Innymi typowymi grupami napastników są hakerzy – motywowani politycznie sabotażyści, którzy zamierzają zakłócać świadczenie usług, niszczyć strony internetowe lub kraść poufne informacje z zamiarem spowodowania strat finansowych lub wysyłania komunikatów politycznych. Inną powszechną kategorią napastników są zagrożenia wewnętrzne, takie jak byli, niezadowoleni pracownicy lub tacy, którzy starają się wykorzystać swoją pozycję do uzyskania korzyści osobistych.

Grupy, które atakują różne branże, atakują również operatorów sieci. Sieci telekomunikacyjne mają jednak pewne unikalne cechy, które czynią je interesującym celem także dla innych państw oraz organizacji wywiadowczych. To właśnie w nich przechowywane są i przesyłane dane lokalizacji oraz poufne informacje, takie jak wiadomości i rozmowy głosowe między ważnymi osobami, np. urzędnikami rządowymi, decydentami i przywódcami wysokiego szczebla. Dane docelowe mogą zawierać informacje, takie jak kto co powiedział, kiedy i do kogo. Są one bardzo interesujące dla szpiegów z różnych części świata.

Ze względu na to, że coraz więcej wartościowych zasobów firm jest tworzonych, przechowywanych i udostępnianych cyfrowo, szpiegostwo przemysłowe przeniosło się do świata cyfrowego. Celem działań przestępców jest uzyskanie dostępu do tajemnic firmy, takich jak dokumentacja finansowa, informacje o cenach, własności intelektualnej (nowe technologie czy innowacje), a także wrażliwe informacje o klientach. Cechą wspólną tych działań jest wykorzy-

stywanie uzyskanych informacji dla swojej korzyści. Podmioty państwowe lub podmioty wspierane przez państwo zawsze w jakiś sposób monitorowały działania innych państw. W miarę jak działalność społeczna, gospodarcza i polityczna coraz częściej przenosi się do przestrzeni cyfrowej, obsługiwanej przez publiczne sieci telekomunikacyjne, operacje polegające na gromadzeniu danych wywiadowczych idą w tym samym kierunku.

Powszechne wykorzystanie sieci 5G rozwinie tradycyjne relacje pomiędzy konsumentami, użytkownikami biznesowymi a operatorami sieci komórkowych. Ekspansja obejmie nowe relacje w postaci zdigitalizowanych i zautomatyzowanych procesów biznesowych przedsiębiorstw oraz sterowania i eksploatacji maszyn w firmach przemysłowych. Co więcej, cyfrowo-fizyczne współzależności pomiędzy sieciami telekomunikacyjnymi a inteligentną łącznością innych dostawców infrastruktury (miasta, energetyka, media, transport itp.) stworzą nowe sposoby dostępu do sieci mobilnej. Ostateczny kształt rozbudowanych relacji będzie natomiast zależał od zaufania pomiędzy różnymi interesariuszami.

Użycie sieci 5G do masowej i krytycznej komunikacji typu maszynowego pociągnie za sobą konieczność przesyłania nowych rodzajów ruchu (nowych typów danych) w sieciach mobilnych. Chociaż mobilny Internet szerokopasmowy jest dostępny na rynku od dłuższego czasu (został wprowadzony wraz z siecią 3G), **oczekuje się, że wraz z siecią 5G wprowadzone zostaną nowe ulepszenia jakościowe i ilościowe, takie jak wyższa szybkość transmisji danych, niższe opóźnienia, większa ilość urządzeń, które mogą jednocześnie łączyć się ze stacją bazową oraz większa przepustowość na większym obszarze**. Przewiduje się, że powstanie ogromna liczba stosunkowo prostych urządzeń, które podłączone do sieci będą tworzyć wartościowe zbiory danych. Na przykład w przypadku inteligentnego zamka do drzwi, naruszenie poufności i/lub integralności pojedynczego zamka jest prostym włamaniem. Dokonanie takiej operacji wobec miliona zamków jest już operacją wywiadowczą.

Aplikacje, które działają w oparciu o krytyczną komunikację maszynową 5G będą korzystać z ultra-niezawodnej łączności o niskim opóźnieniu, gdzie dane będą występować w ogromnej ilość i będą to dane krytyczne dla biznesu. W tym przypadku komunikującymi się punktami końcowymi są inteligentne maszyny, pojazdy i roboty sterowane przez ludzi lub samodzielne – autonomiczne. Branże i usługi, które będą wykorzystywać taką łączność to: **opieka zdrowotna, produkcja przemysłowa, transport i branża dóbr konsumpcyjnych**.

Mimo, że technologia IoT jest już dostępna, a nawet można z niej korzystać z wykorzystaniem technologii dostępu 4G, jak i technologii dostępu innych niż zdefiniowane przez standard 3GPP, **to komunikacja typu maszy-**

nowego w sieciach 5G zapewni IoT niedostępne do tej pory możliwości sieciowe, takie jak ultra niski poziom opóźnienia. W celu osiągnięcia niezbędnego poziomu bezpieczeństwa w sieciach mobilnych, należy wziąć pod uwagę wiarygodność podłączonych urządzeń IoT. Fakt ten pociąga za sobą konieczność zapewnienia kontroli tożsamości urządzeń IoT, a także kontroli dostępu, a w istocie przywilejów dostępu i poufności powiązanych danych generowanych przez urządzenie IoT. Z punktu widzenia sieci 5G zaufanie do IoT opiera się na wiarygodności sprzętu, oprogramowania oraz konfiguracji. W związku z tym, wiarygodność staje się kumulatywna i jest definiowana na podstawie tego, jak dobrze operatorzy sieci i osoby zarządzające eksploatacją urządzeń IoT kontrolują:

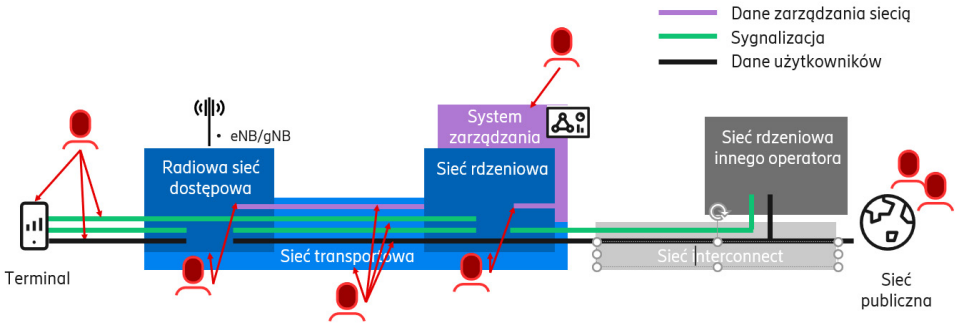
- tożsamości i dane,
- bezpieczeństwo i prywatność,
- zgodność podmiotów z uzgodnionymi politykami bezpieczeństwa.

Z perspektywy podłączonego do sieci urządzenia IoT poziom zaufania pomiędzy podmiotami i tożsamościami zależy od istnienia, wydajności i przejrzystości mechanizmów zaufania, takich jak zaufany sprzęt i oprogramowanie, zaufane tożsamości, komunikacja, dane i prywatność oraz zaufane operacje. Ostatecznie wiarygodność zależy od właściwej kombinacji mechanizmów zaufania.

Z punktu widzenia zasobów sieciowych zagrożenia w sieci 5G można podzielić na trzy domeny:

- zagrożenia poufności danych (*confidentiality*) – przechowywane, przesyłane lub przetwarzane dane w szerokim rozumieniu (tj. dane użytkowników, sygnalizacja w sieci, dane monitorowania i zarządzania siecią) mogą zostać przechwycone przez podmioty atakujące,
- zagrożenia integralności danych (*integrity*) – wyżej wymienone typy danych mogą zostać zmienione w celu uzyskania efektu pożądanego przez atakującego,
- zagrożenia dostępności sieci (*availability*) – przerwy w działaniu sieci szczególnie istotne w aplikacjach krytycznych czy zastosowaniach militarnych.

Na rysunku 1 przedstawiono typowe wektory ataków możliwych do przeprowadzenia w sieci mobilnej, których celem mogą być wszystkie typy danych przechowywanych, przesyłanych i przetwarzanych w sieci, jak również wszystkie elementy sieciowe i łączące je interfejsy.



Rysunek 1. Wektory ataków w sieci mobilnej[19]

Cel stawiany technologii 5G to przekształcenie się w niezawodną i zaufaną platformę innowacji dla firm i organizacji mających na celu tworzenie i dostarczanie nowych usług. Dominuje również pogląd, że technologia 5G stanowi czynnik umożliwiający cyfryzację i modernizację najważniejszych infrastruktur krajowych, takich jak sieci energetyczne, transport, itp. Drugi cel podnosi poprzeczkę dla systemów 5G i wymaga zapewnienia większej dostępności i większego bezpieczeństwa usług telekomunikacyjnych. Dlatego też, jak przedstawiono na rysunku 1, poziome bezpieczeństwo ogólnosystemowe obejmuje sieć od urządzenia użytkownika do punktu odniesienia, w którym operator kończy dostarczanie swoich usług.

Bezpieczeństwo poziome osiąga się przez połączenie i koordynację wielu środków kontroli bezpieczeństwa w różnych domenach sieci telekomunikacyjnych, w tym w domenie dostępu radiowego (np. moduły radiowe, jednostki przetwarzające w paśmie podstawowym, anteny), w domenie sieci transportowej (np. urządzenia optyczne, mostki Ethernet, routery IP/MPLS, kontrolery SDN), w domenie sieci rdzeniowej (np. węzły MME, S-GW, PGW, HSS), a także w usługach wsparcia sieci (np. DNS, DHCP), infrastrukturze chmury oraz w różnych systemach zarządzania (np. zarządzanie siecią, zarządzanie jakością usług klienta, zarządzanie bezpieczeństwem). Bezpieczeństwo we wszystkich tych domenach musi być skoordynowane, by zapewnić dostępność usług oraz poufność i integralność danych, które są wysyłane, przechowywane i przetwarzane w systemie 5G.

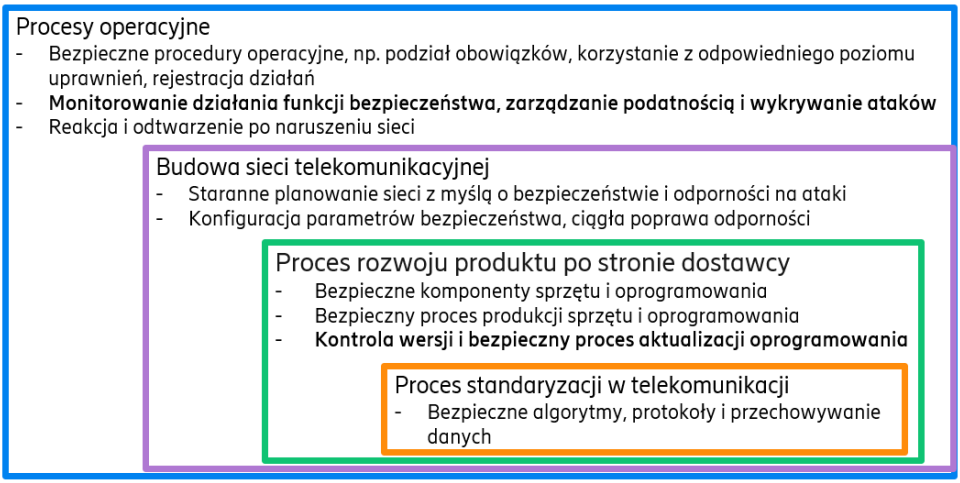
Holistyczna koncepcja bezpieczeństwa sieci telekomunikacyjnych

Budowa bezpiecznej sieci 5G wymaga holistycznego podejścia, a nie skupiania się na pojedynczych elementach technicznych. Interakcje pomiędzy procesem uwierzytelniania użytkownika, szyfrowaniem ruchu,

[19] Źródło: opracowanie własne firmy Ericsson

mobilnością, przeciążeniami oraz różnymi aspektami odporności sieci należy rozpatrywać łącznie. Ważne jest również, aby zdefiniować oraz zrozumieć ryzyka i stworzyć odpowiednie metody przeciwdziałania już na poziomie projektowania sieci. Sposób, w jaki wszystkie technologie związane z siecią 5G są budowane, zintegrowane, eksploatowane i kontrolowane stanowi główne zagadnienie zarządzania zaufaniem, szczególnie w przypadku korzystania z infrastruktury krytycznej jaką niewątpliwie stanowi sieć 5G.

Każdy z uczestników rynku telekomunikacyjnego ma inne priorytety w zakresie cyberbezpieczeństwa. Wykorzystując proces standaryzacji, operatorzy i dostawcy sprzętu uzgadniają w jaki sposób sieci na całym świecie będą ze sobą współpracować oraz w jaki sposób można chronić sieci i użytkowników przed podmiotami złośliwymi. **Dostawcy sprzętu telekomunikacyjnego przekładają potem uzgodnione standardy na fizyczne elementy i systemy sieciowe.** Procesy projektowania i produkcji, wykonywane przez dostawców sieci, mają kluczowe znaczenie dla zapewnienia bezpieczeństwa i funkcjonalności produktu końcowego. Planowanie i konfiguracja sieci w fazie jej budowy musi również uwzględniać konieczność zapewnienia docelowego poziomu jej bezpieczeństwa oraz dalszego zwiększania odporności sieci. Wykorzystywane w fazie eksploatacji sieci procesy operacyjne muszą być również projektowane z myślą o zapewnieniu wysokiego poziomu bezpieczeństwa. Należy jednak pamiętać, że skuteczność tych procesów jest w wysokim stopniu zależna od wcześniejszych etapów projektowania elementów sieciowych oraz planowania i budowy sieci.



Rysunek 2. Holistyczne podejście do zapewnienia bezpieczeństwa sieci telekomunikacyjnej

Holistyczna filozofia cyberbezpieczeństwa sieci 5G (rysunek 2) opiera się na czterech podstawowych wzajemnie powiązanych aspektach bezpieczeństwa sieci telekomunikacyjnej, które nazywamy „stosem zaufania" (*trust stuck*). **Każdy z czterech poziomów wzajemnie na siebie oddziałuje i tylko synergia narzędzi bezpieczeństwa na każdym z nich zapewni w pełni zabezpieczoną sieć**. Przykładowo, sama certyfikacja nie wystarczy, jeśli popełnimy błędy w planowaniu sieci. Z kolei operatorzy nie będą w stanie zapewnić odpowiedniego poziomu cyberbezpieczeństwa, jeśli urządzenia lub oprogramowanie wyprodukowane przez dostawców będzie podatne na ataki.

Kluczowe trendy technologiczne w ewolucji sieci telekomunikacyjnych

Dzięki rozwojowi technologii opartych na przetwarzaniu danych w chmurze, oprogramowanie można teraz odłączyć od konkretnego urządzenia fizycznego eliminując potrzebę tworzenia funkcji sieciowych zależnych od sprzętu. Realizację takiego podejścia umożliwiają technologie SDN (*Software Defined Networking*) i NFV (*Network Function Virtualization*). SDN oferuje elastyczność sposobu konfiguracji ścieżek routingu pomiędzy dynamicznie konfigurowanymi zwirtualizowanymi funkcjami sieciowymi. Wprowadzenie Sztucznej Inteligencji i coraz mocniejszych komputerów, wraz z przetwarzaniem w chmurze jest kluczowym motorem napędowym procesów automatyzacji. W konsekwencji dominujący trend technologiczny powoduje, że sieci telekomunikacyjne są coraz bardziej oparte na oprogramowaniu. Rozproszone przetwarzanie w chmurze umożliwia tworzenie partycji dla zapewnienia lepszej odporności i mniejszych opóźnień. Z punktu widzenia bezpieczeństwa, jeśli nie zostaną zaimplementowane odpowiednie narzędzia, rozproszona chmura może stwarzać nowe ścieżki ataku na sieci 5G. Zagadnienie to szeroko analizowano w wielu pozycjach bibliograficznych[20]. Z drugiej strony, rozproszona chmura może być postrzegana jako kolejny element zwiększający bezpieczeństwo, ze względu na możliwość wprowadzenie odpowiednich funkcjonalności i mechanizmów, a tym samym ograniczanie zasięgu ataku do lokalnego, zamkniętego obszaru.

Dodatkowo rozproszone przetwarzanie w chmurze umożliwia specyficzną i bardzo ważną funkcjonalnością sieci 5G – tzw. „plasterkowanie sieci" (*network slicing*). Plasterkowanie sieci polega na oddzielaniu różnych rodzajów ruchu użytkowników i tworzeniu ad-hoc dedykowanych sieci rdzeniowych tak, aby umożliwić cały zakres różnych zastosowań sieci 5G. Dzięki temu mamy możliwość tworzenia podsieci dla danego typu urządzeń, sektora przemysłowego, a także podsieci specyficznych dla danego klienta. Mechanizm kontroli plasterkowania sieci musi zapewniać odpowiednie możliwo-

[20] Czytaj wiecej na ten temat: I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov , "5G Security: Analysis of Threats and Solutions", 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017; I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, "Overview of 5G Security Challenges and Solutions", IEEE Communications Standards Magazine, March 2018, pp. 36-43; R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions", IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, 2020, pp. 196-248.

ści zarządzania segmentami, konfigurację kontroli dostępu i bezpieczną izolację, jednocześnie umożliwiając autoryzację udostępnionych zasobów. Segmenty sieciowe zaprojektowane dla usług o znaczeniu krytycznym mogą również korzystać ze współdzielonych zasobów, ale wymagają starannej izolacji. Usługi krytyczne wymagają wysokiej niezawodności, odporności, poziomu bezpieczeństwa, ochrony, a często także prywatności. Wymaga to kompleksowego podejścia do bezpieczeństwa, w tym zautomatyzowanego zarządzania zasobami i weryfikacji zgodności polityk bezpieczeństwa.

Funkcje bezpieczeństwa sieci 5G określone w standardzie 3GPP

Wprawdzie standardy 3GPP dla sieci 5G opisują funkcje bezpieczeństwa, które są oparte na mechanizmach sprawdzonych już w sieci 4G, definiują również znaczące ulepszenia[21]. Najważniejsze z nich to:

- nowy schemat uwierzytelniania abonentów,
- zwiększona ochrona prywatności użytkowników,
- architektura oparta na usługach SBA (*Service Based Architecture*) i bezpieczeństwo połączeń międzysieciowych (*interconnect security*),
- ochrona integralności danych użytkowników.

Centralną procedurą bezpieczeństwa we wszystkich generacjach sieci 3GPP jest uwierzytelnianie dostępu, określane w standardach bezpieczeństwa 3GPP 5G jako uwierzytelnianie podstawowe. Procedura ta jest zwykle wykonywana podczas pierwszej rejestracji (*initial attach*), na przykład, kiedy urządzenie jest włączane po raz pierwszy. Pomyślne uruchomienie procedury uwierzytelniania prowadzi do ustanowienia kluczy szyfrujących dla sesji, które służą do ochrony komunikacji między urządzeniem a siecią. Procedura uwierzytelniania w zabezpieczeniach 3GPP 5G została zaprojektowana jako platforma do obsługi rozszerzonego protokołu uwierzytelniania EAP (*Extensible Authentication Protocol*) – protokołu bezpieczeństwa określonego przez organizację *Internet Engineering Task Force* (IETF), który jest dobrze zakorzeniony i szeroko stosowany w środowiskach IT. Zaletą tego protokołu jest to, że pozwala on na użycie różnych rodzajów poświadczeń oprócz tych powszechnie używanych w sieciach komórkowych i zwykle przechowywanych na karcie SIM, takich jak certyfikaty, klucze współdzielone oraz nazwa użytkownika i hasło. **Ta elastyczność metody uwierzytelniania jest kluczowym czynnikiem umożliwiają-**

[21] N. Ben Henda, M. Wifvesson, Ch. Jost, "An overview of the 3GPP 5G security standard", Ericsson Research Blog, 2019, https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

cym korzystanie z technologii 5G zarówno w przypadku zastosowań przemysłowych, np. w fabrykach, jak i w innych aplikacjach spoza branży telekomunikacyjnej.

Obsługa protokołu EAP nie kończy się na podstawowej procedurze uwierzytelniania, ale ma również zastosowanie do innej procedury zwanej uwierzytelnieniem wtórnym. Procedura ta jest wykonywana w celu autoryzacji podczas zestawiania połączenia do transmisji danych użytkownika (*setup of user plane*). Umożliwia to operatorowi przekazanie autoryzacji stronie trzeciej. Typowym przypadkiem użycia jest tak zwane połączenie sponsorowane, na przykład do ulubionej transmisji strumieniowej lub witryny sieci społecznościowej, gdzie inne istniejące poświadczenia (np. nazwa użytkownika i hasło) mogą zostać użyte do uwierzytelnienia użytkownika i autoryzacji połączenia. Korzystanie z protokołu EAP pozwala zaspokoić szeroki zakres typów poświadczeń i metod uwierzytelniania wdrożonych i używanych przez popularnych dostawców aplikacji i usług.

Bezpieczeństwo w standardzie 3GPP 5G znacznie zwiększa ochronę prywatności abonenta przed fałszywymi stacjami bazowymi popularnie zwanymi łapaczami IMSI (*IMSI catchers*) lub płaszczkami (*stingrays*)[22]. W standardzie 5G zaproponowano mechanizm uniemożliwiający dokonanie ataku przechwytującego IMSI. Jest to możliwe dzięki technice, w której długoterminowy identyfikator użytkownika nigdy nie jest przesyłany przez interfejs radiowy w postaci czystego tekstu. Ponadto 5G zwiększa częstotliwość aktualizacji tymczasowych identyfikatorów użytkowników, co dodatkowo poprawia poziom prywatności. Dodatkowo, standard 5G jest zaprojektowany proaktywnie w taki sposób, aby utrudnić atakującym korelowanie komunikatów protokołu i identyfikację pojedynczego abonenta. Uzyskuje się to dzięki przesyłaniu tylko ograniczonego zestawu informacji jako zwykły tekst, nawet w początkowych komunikatach protokołu. Pozostałe informacje są zawsze ukryte. Kolejnym rozwiązaniem są ogólne zasady wykrywania fałszywych stacji bazowych[23], które są głównym zagrożeniem dla prywatności. Wykrywanie, które opiera się na informacjach o stanie warunków radiowych przesyłanych przez urządzenia abonenckie znacznie utrudnia fałszywym stacjom bazowym pozostawanie w ukryciu.

Rozwój technologii 5G spowodował przesunięcie paradygmatu w architekturze sieci mobilnych od klasycznego modelu z interfejsami punkt-punkt między funkcjami sieciowymi do interfejsów opartych na usługach SBI (*Service Based Interfaces*). W architekturze opartej na usługach SBA różne funkcjonalności elementów sieciowych przekształcane zostają w usługi, które są dalej oferowane i udostępniane na żądanie innym jednostkom w sieci[24]. Umożliwia to bardziej elastyczny rozwój nowych

[22] N. Ben Henda, M. Wifvesson, Ch. Jost, "An overview of the 3GPP 5G security standard", Ericsson Research Blog, 2019, https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

[23] P. K. Nakarmi, K. Norrman, "Detecting false base stations in mobile networks", Ericsson Research Blog, 2018, https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks.

[24] J. Arkko, "Service-Based Architecture in 5G", Ericsson Research Blog, 2017, https://www.ericsson.com/en/blog/2017/9/service-based-architecture-in-5g.

usług dzięki możliwości łączenia różnych komponentów bez wprowadzania nowych specyficznych interfejsów sieciowych. Zastosowanie podejścia SBA wymusiło również ochronę na wyższych warstwach protokołu, tj. transportowym i aplikacyjnym, oprócz ochrony komunikacji między jednostkami sieci rdzeniowej na warstwie protokołu internetowego (IP) zapewnianej zazwyczaj za pomocą IPsec. Funkcje sieci rdzeniowej 5G obsługują najnowocześniejsze protokoły bezpieczeństwa, takie jak TLS 1.2 i 1.3, aby chronić komunikację w warstwie transportowej i platformę autoryzacyjną OAuth 2.0 w warstwie aplikacji, aby zapewnić, że tylko autoryzowane funkcje sieciowe mają dostęp do usług oferowanych przez inną funkcję.

Ulepszenie zapewniane przez 3GPP SA3 w zakresie bezpieczeństwa połączeń między różnymi sieciami operatorów (*interconnect security*) składa się z trzech elementów:

1. w architekturze 5G wprowadzono nową funkcję sieci SEPP (*Security Edge Protection Proxy*), przez którą ma być przechodzić cały ruch sygnalizacyjny w sieciach operatorów,
2. wymagane jest uwierzytelnienie między funkcjami SEPP, co umożliwi skuteczne filtrowanie ruchu przychodzącego z połączeń typu *interconnect*,
3. zostało zaprojektowane nowe rozwiązanie bezpieczeństwa warstwy aplikacji na interfejsie N32 między funkcjami SEPP w celu zapewnienia ochrony wrażliwych atrybutów danych.

Głównymi komponentami bezpieczeństwa w architekturze SBA są więc uwierzytelnianie i ochrona transportu między funkcjami sieciowymi przy użyciu TLS, autoryzacja z wykorzystaniem platformy OAuth2 oraz wzmocnione bezpieczeństwo połączeń przy użyciu nowego protokołu bezpieczeństwa zaprojektowanego przez 3GPP.

W standardzie 5G wprowadzono funkcję ochrony integralności danych użytkownika (*integrity protection of the user plane*) między terminalem użytkownika UE a stacją bazową gNB. Podobnie jak funkcja szyfrowania, obsługa funkcji ochrony integralności jest obowiązkowa zarówno na urządzeniach UE, jak i węzłach gNB, podczas gdy użycie jest opcjonalne i kontrolowane przez operatora. Należy zauważyć, że ochrona integralności wymaga użycia zasobów sieciowych i że nie wszystkie urządzenia będą w stanie ją obsługiwać w połączeniu z pełną szybkością transmisji danych. Mając to na uwadze, w systemie 5G możliwe jest negocjowanie szybkości transmisji odpowiednich dla określonej funkcji.

Aspekty dotyczące wdrożenia systemu 5G są w bardzo ograniczonym stopniu normalizowane przez 3GPP. To, czy niektóre funkcje są wdrożone na poszczególnych serwerach fizycznych (fizycznie izolowane i oddzielone) lub wdrożone jako maszyny wirtualne w chmurze lub w środowisku zwirtualizowanym (sprzęt współdzielony), zależy od implementacji i możliwości wdrożenia przez operatora. Oznacza to, że nie ma

prostej zasady opartej na standardach 3GPP dotyczącej rozdzielenia funkcji sieci RAN i sieci rdzeniowej. Dominuje raczej elastyczność i, nawet w pojedynczej sieci fizycznej, możliwa jest inna konfiguracja dla różnych przypadków użycia 5G. Skutkuje to kilkoma odmiennie skonfigurowanymi sieciami logicznymi działającymi w jednej sieci fizycznej. W przypadku funkcji wdrożonych w tradycyjny niezwirtualizowany sposób, 3GPP we współpracy z GSMA opracowuje specyfikacje zapewniania bezpieczeństwa, które określają wymagania dla niektórych aspektów implementacji.

Sieci komórkowe stanowią podstawę komunikacji we współczesnych społeczeństwach, a w systemach prawnych większości państw klasyfikowane są nawet jako infrastruktura krytyczna. Z tego powodu zapewnienie bezpieczeństwa jest szczególnie istotne. Branża telekomunikacyjna szybko zdała sobie sprawę, że oprócz bezpiecznego standardowego systemu i protokołów, potrzebne jest zapewnianie bezpiecznych wdrożeń. Dlatego 3GPP i GSMA podjęły inicjatywę stworzenia systemu zapewniania bezpieczeństwa NESAS (*Network Equipment Security Assurance Scheme*), który byłby odpowiedni dla cyklu życia sprzętu telekomunikacyjnego. NESAS składa się dwóch głównych elementów: wymagania bezpieczeństwa i infrastruktura audytowa. Wymagania z zakresu bezpieczeństwa są określane w 3GPP wspólnie przez operatorów i dostawców. Wymagania te są obecnie zdefiniowane dla poszczególnych węzłów i zebrane w tak zwanych specyfikacjach SCAS (*SeCurity Assurance Specifications*). Istnieje jedna specyfikacja określająca wymagania bezpieczeństwa dla stacji bazowych 4G. Obok niej funkcjonują różne rodzaje wymagań, w tym stosowanie funkcjonalnych zasad bezpieczeństwa, takich jak minimalna długość haseł, ale także wymagania jakościowe dotyczące testowania odporności. Infrastrukturą audytową zarządza GSMA – globalna organizacja operatorów telefonii komórkowej. To właśnie GSMA wyznacza firmy audytorskie, które przeprowadzają audyty dostawców po kątem procesów rozwoju, produkcji i testowania. GSMA przyznaje również certyfikaty dostawcom, którzy przechodzą audyt i unieważnia certyfikaty tym, którzy nie spełniają zdefiniowanych wymagań. Celem NESAS jest spełnienie wielu krajowych i międzynarodowych przepisów cyberbezpieczeństwa, takich jak unijne ramy certyfikacji bezpieczeństwa.

Architektura bezpieczeństwa w sieci 5G

Odporność całego systemu 5G osiągana jest przez połączenie i koordynację wielu środków kontroli bezpieczeństwa w różnych domenach sieci telekomunikacyjnych. Są to między innymi domena dostępu radiowego, domena sieci transportowej, domena sieci rdzeniowej, jak również usługi wsparcia sieci, infrastruktura chmury oraz systemy

zarządzania siecią. W związku z tym konieczna jest koordynacja funkcji i działań zabezpieczających we wszystkich tych domenach w taki sposób, żeby zapewnić dostępność usług oraz poufność i integralność danych, wysyłanych, przechowywanych i przetwarzanych w systemie. Oprócz funkcji bezpieczeństwa zdefiniowanych w standardzie 3GPP i wykorzystywanych głównie w obszarze dostępu radiowego, należytej uwagi wymagają również zagadnienia bezpieczeństwa właściwe dla domeny transportowej i domeny chmury obliczeniowej. Mają one kluczowe znaczenie dla bezpieczeństwa całego systemu 5G rozpatrywanego w sposób holistyczny.

Sieci transportowe zapewniają szybkie usługi łączności o niskim opóźnieniu między wszystkimi funkcjami sieci 5G. W związku z tym, dostępność sieci transportowych przekłada się bezpośrednio na dostępność systemu 5G i świadczonych przez niego usług. W celu zapewnienia dostępności usług transportowych podczas awarii węzła, zerwania przewodu lub światłowodu lub zdarzeń związanych z przeciążeniem, w sieciach transportowych mogą być zastosowane różne rozwiązania techniczne:

- geo-redundantne ścieżki, które pozwalają na przekierowanie ruchu w przypadku wystąpienia awarii ścieżki,
- nadmiarowość łączy służąca do szybkiego przełączania awaryjnego w przypadku wystąpienia awarii portu lub łącza,

- mechanizmy redundancji ścieżek, które pozwalają na przekierowanie ruchu w przypadku awarii ścieżki lub przeciążenia łącza,
- zapewnienie wysokiej dostępności krytycznych węzłów sieciowych umożliwiającej obsługę w czasie awarii węzłów,
- zastosowanie mechanizmów segmentacji ruchu (np. VLAN i MPLS) w celu logicznego rozdzielenia ruchu pomiędzy różnymi domenami,
- wprowadzenie dywersyfikacji poziomu jakości usług QoS przy użyciu mechanizmów kolejkowania ruchu, ograniczania prędkości i kontroli ruchu w celu zarządzania zasobami i kontroli przeciążeń,
- mechanizmy wykrywania i mitygacji ataków DDoS,
- uwierzytelnianie na portach w celu sprawdzenia, czy do sieci podłączone są autoryzowane urządzenia sieciowe,
- wykorzystanie IPsec lub MACsec umożliwiające tworzenie uwierzytelnionych i zabezpieczonych kryptograficznie tuneli do przesyłania danych między elementami sieci.

Architektura oparta na usługach SBA oraz podział funkcji w tradycyjnej jednostce przetwarzania w pasmie podstawowym (*baseband unit*) otwierają się na wdrożenia w środowiskach chmurowych. Ta elastyczność daje wiele możliwości realizacji nowych usług, ale obnaża również nowe zagrożenia i wektory ataków, które należy kontrolować. Działania i mechanizmy kontroli mające na celu zwiększenie wiarygodności w środowisku chmury obliczeniowej to między innymi:

- podnoszenie odporności środowiska wirtualizacji funkcji sieciowych NFV, np. wzmocnienie systemu operacyjnego hosta OS, bezpieczna konfiguracja środowiska hiperwizora lub środowiska kontenerowego,
- separacja dzierżawców (*tenant*) w taki sposób, aby dzierżawcy nie byli w stanie ingerować wzajemnie w swoje dane, nie mogli mieć do nich nieautoryzowanego dostępu, jak również nie mieli możliwości przechwytywania ruchu generowanego przez innych dzierżawców,
- monitorowanie zgodności dzierżawców mające na celu upewnienie się, że spełniają oni określoną politykę bezpieczeństwa,
- generowanie szczegółowych ścieżek audytowych wspierających szybką reakcję na incydenty oraz umożliwiających prowadzenie działań przywracających,
- zarządzanie obciążeniami w celu zapewnienia bezpiecznego włączania wirtualnych funkcji sieciowych, weryfikacji integralności oprogramowania podczas uruchamiania, a także integralności obciążeń w czasie pracy funkcji sieciowej oraz bezpiecznego wycofywania obciążeń.

Logicznym konstruktem stosowanym do opisania segregacji usług sieciowych o różnych poziomach wydajności i bezpieczeństwa jest segment („plasterek") sieci (*network slice*). Wyżej wymienione mechanizmy sterujące i wytyczne projektowe mogą być wykorzystane do stworzenia różnych segmentów sieci. Na przykład aplikacja o kluczowym znaczeniu, która wymaga wysokiego poziomu dostępności, priorytetowego dostępu do zasobów oraz izolacji od innych usług, może być realizowana przy użyciu usług z redundancją ścieżki geograficznej z szybkim przełączaniem awaryjnym, uwierzytelniana z zachowaniem poufności i integralności przy użyciu protokołu IPsec i przetwarzana przez dedykowane funkcje sieci rdzeniowej 5G wdrożone na zaaprobowanych serwerach typu *blade* oraz przez funkcje bezpieczeństwa sieci wdrożone z zachowaniem zasad dostosowanych do konkretnych wymagań aplikacji.

Podsumowanie

Szybka ewolucja sieci telekomunikacyjnych, obejmująca wirtualizację, Internet Rzeczy i Przemysł 4.0 niesie ze sobą zarówno ogromne możliwości rozwoju nowych zastosowań i aplikacji w rozmaitych branżach, gałęziach przemysłu i dziedzinach życia, jak również nowe wyzwania i oczekiwania w zakresie zapewnienia bezpieczeństwa systemów ICT. Sieć 5G umożliwi realizację nieznanych dotąd usług, których powszechne i bezpieczne wykorzystanie przez społeczeństwo będzie wymagało spełnienia najwyższych standardów bezpieczeństwa. Wiarygodność sieci telekomunikacyjnej, od której w wielu przypadkach może zależeć ludzkie życie, wymaga holistycznego podejścia obejmującego nie tylko implementację standardowych funkcji bezpieczeństwa, ale także odpowiednie zasady projektowania elementów sieciowych, planowania i budowy sieci oraz stale ulepszanych procesów operacyjnych.

Cyfrowa suwerenność w kontekście 5G

Suwerenność cyfrowa to pojęcie dość nowe, które nie doczekało się jeszcze pełnej definicji. W zeszłym roku, przy okazji dyskusji na temat wdrożenia sieci 5G było jednak często przywoływanym hasłem.

W stosunkach międzynarodowych, suwerenność oznacza formalny status państwa, pozwalający na samodzielny i nieograniczony udział w życiu międzynarodowym[25]. Tylko państwo suwerenne może, bez zgody i upoważnienia kogokolwiek, podejmować wszelką aktywność międzynarodową, we własnym imieniu, w wiążący sposób, oraz ponosić pełną odpowiedzialność za swoje działania.

Jako pierwsi zwrotu „cyfrowa suwerenność" użyli Francuzi. W 2011 roku Pierre Bellnger[26] zdefiniował cyfrową suwerenność jako „kontrolę nad naszą teraźniejszością i przyszłością związaną z wykorzystaniem technologii i sieci komputerowych"[27]. Ta krótka definicja bardzo dobrze oddaje esencję całej dyskusji.

[25] S.D. Krasner, *Power, the State, and Sovereignty, Routledge*, London – New York, 2009.

[26] Założyciel i CEO francuskiej stacji radiowej Skyrock oraz sieci społecznościowej skyrock.com.

[27] F. Gueham, *Digital Sovereignty*, Foundation Pour L'Innovation Politique, Styczeń 2017.

Chodzi o zapewnienie niezależności działań państwa w nowej sferze aktywności – cyberprzestrzeni. Na poziomie Unii Europejskiej dyskusja na ten temat toczy się już od dłuższego czasu, przy czym zagadnienie to nazywane jest suwerennością cyfrową dopiero od niedawna.

W *Tallinn Manual 2.0*, academickim podręczniku analizującym sposób implementacji prawa międzynarodowego w cyberprzestrzeni[28] zagadnieniu temu poświecono cały rozdział. Autorzy opisują pięć zasad cyfrowej suwerenności[29]:

1. **Zasada suwerenności państwa obowiązuje w cyberprzestrzeni.**

2. **Suwerenność wewnętrzna** w cyberprzestrzeni jest związana z infrastrukturą teleinformatyczną, osobami oraz aktywnością mającą miejsce na terytorium państwa, z zastrzeżeniem międzynarodowych zobowiązań prawnych.

3. **Suwerenność zewnętrzna** w cyberprzestrzeni jest związana z wolnością do podejmowania działań w cyberprzestrzeni w relacjach międzynarodowych, z zastrzeżeniem międzynarodowych zobowiązań prawnych.

[28] Wydawnictwo jest owocem prac międzynarodowej grupy ekspertów, powołanej przy *Cooperative Cyber Defence Centre of Excellence* w Tallinie, która pracowała w latach 2009-2012. Grupa prowadzona była przez prof. Michaela N. Schmitta, przewodniczącego departamentu prawa międzynarodowego w *United States Naval War College*.

[29] *Tallinn Manual 2.0 on the International Law application to Cyber Operations*; Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge 2017.

4. **Naruszenie suwerenności** w cyberprzestrzeni odnosi się do zakazu podejmowania operacji w cyberprzestrzeni, naruszających suwerenność innego państwa.

5. **Immunitet suwerenności i nienaruszalności** oznacza, że jakakolwiek ingerencja państwa w infrastrukturę teleinformatyczną należącą do innego państwa, niezależnie od tego gdzie się znajduje, stanowi naruszenie suwerenności.

Na podstawie tych zasad państwo ma m.in. prawo odłączenia od sieci każdej infrastruktury teleinformatycznej, która znajduje się na jego terytorium, i której działanie może stanowić naruszenie suwerenności państwa[30]. Dodatkowo, suwerenność wewnętrzna oznacza, że państwo może, częściowo lub w całości, ograniczyć dostęp do sieci osobom znajdującym się na jego terytorium, w szczególności do określonych treści online[31]. Istnieje także zasada powstrzymywania się od wrogich działań w cyberprzestrzeni[32]. Suwerenność zewnętrzna oznacza natomiast, że państwa mogą angażować się w działalność w cyberprzestrzeni w stosunkach międzynarodowych, zgodnie z własnymi decyzjami, o ile nie naruszają norm prawa międzynarodowego[33]. Naruszeniem suwerenności jest każda ingerencja w granicach terytorium państwa, związana z działaniami w cyberprzestrzeni. Jako przykład eksperci podają użycie przez dane państwo nośnika USB ze złośliwym oprogramowaniem, żeby zakłócić działalność systemów na terytorium innego państwa[34]. W tym celu konieczne jest jednak dokonanie atrybucji, a więc przedstawienie dowodów, że za działanie to odpowiada inne państwo.

Przy okazji dyskusji nad **bezpieczeństwem sieci 5G** oraz jej wdrażaniem, trwa dyskusja na temat cyfrowej suwerenności. Poruszany jest tu kontekst dostawców usług i niezależności technologicznej Europy oraz poszczególnych państw członkowskich.

30 *Tallinn Manual 2.0 on the International Law application to Cyber Operations*; Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge 2017, s. 12-13.

31 Ibidem, s. 15.

32 Ibidem, s. 16.

33 Ibidem, s. 16.

34 Ibidem, s. 19

NASK

Cyber POLICY

Sławomir Pietrzyk, Andrzej Miłkowski

5G i Open RAN – sieć nowej generacji w perspektywie dyskusji o cyfrowej suwerenności

Sławomir Pietrzyk – współzałożyciel oraz prezes IS-Wireless, pierwszego polskiego dostawcy mobilnych sieci przyszłości. Posiada tytuł doktora Delft University of Technology (2005) i jest jednym z pionierów technik wielodostępu dla 4G i 5G. Autor wielu publikacji, w tym wydanej w 2006 roku w USA książki "OFDMA for Broadband Wireless Access".

Andrzej Miłkowski – Product Manager w IS-Wireless, gdzie odpowiada za zarządzanie produktem zdefiniowanej programowo Radiowej Sieci Dostępowej. Pasjonat i innowator technologii w obszarze telekomunikacji mobilnej i IT, związany z cyfrową telekomunikacją mobilną od początku jej rozwoju w Polsce. Współtworzył takie marki jak Era, Heyah oraz PLAY, wspierając rozwój firm wieloletnim doświadczeniem we wdrażaniu nowoczesnych technologii.

Dookoła 5G narosło wiele przeinaczeń oraz niedomówień, dlatego warto zacząć od podstaw, czyli od definicji. 5G to nie jest technologia. Niestety pokutuje w naszym języku ta błędna kalka z języka angielskiego, potęgująca dodatkowo wrażenie tajemniczości. 5G (*5th Generation*) to nic innego jak kolejna generacja komórkowych systemów łączności, które cyklicznie po sobie następują i wnoszą nowe rozwiązania techniczne oraz umożliwiają nowe usługi. I tak 5G następuje po 4G, które z kolei nastąpiło po 3G i tak dalej. Cykliczność tych generacji jest w przybliżeniu równa dekadzie.

Ciałem standaryzacyjnym, znacząco zaangażowanym w powstawanie 5G, jest 3GPP. Zgodnie z 3GPP pierwsza grupa specyfikacji opisujących 5G to Rel. 15. W oparciu o nią powstały pierwsze implementacje infrastruktury 5G hucznie wdrażane w różnych miejscach na świecie jako 5G NR (*New Radio*), a dokładniej 5G NR NSA (*Non-Stand Alone*), ponieważ obecnie uruchamiane stacje bazowe 5G potrzebują infrastruktury LTE (4G).

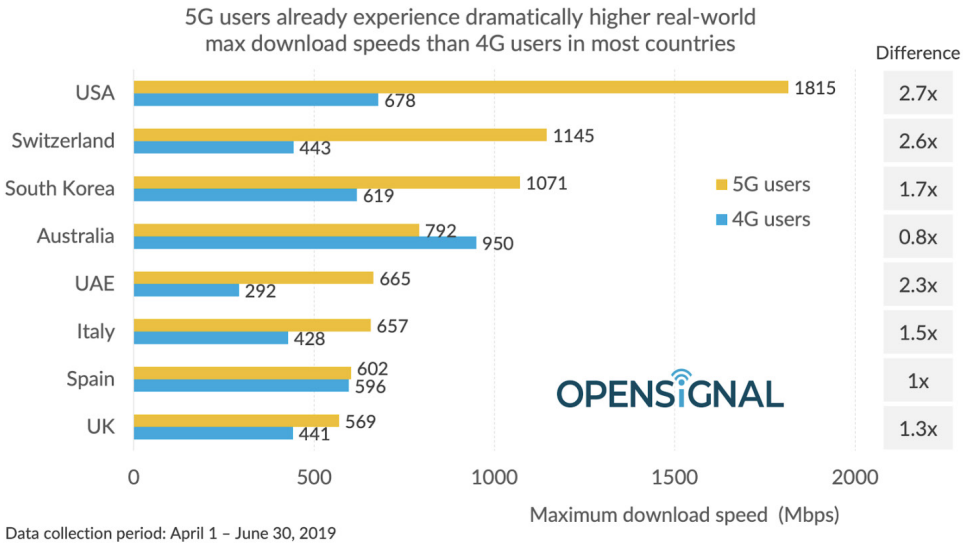
Z punktu widzenia technicznego, to co jest nazywane przełomem, w gruncie rzeczy jest powtórzeniem koncepcji znanych z LTE. Istotą interfejsu radiowego jest oparcie się na wielotonowej metodzie transmisji (OFDM/OFDMA *Orthogonal Frequency Division Multiplexing/Orthogonal Frequency Division Multiple Access*), która umożliwia osiąganie wysokich przepływności oraz efektywne wykorzystanie zasobów radiowych. Zastosowanie OFDM/OFDMA skutkuje dwuwymiarową ramką (czas/częstotliwość), która co do zasady jest niezmienna w stosunku do 4G. Nie ma zatem w 5G tak znaczącej zmiany koncepcji interfejsu radiowego względem 4G, jak obserwowaliśmy w przypadku przejścia z 3G na 4G (CDMA na OFDMA), czy 2G na 3G (TDMA na CDMA). Podsumowując, 5G NR to nowy „stary" interfejs radiowy z nową numerologią pozwalającą na większą elastyczność w przyszłości.

Istota 5G nie leży w technice. Istota 5G leży w nowych modelach biznesowych, które ta generacja może umożliwiać. Czy tak się stanie – to zależy w jaki sposób i w oparciu o jaką architekturę (zamkniętą czy otwartą) 5G będzie wprowadzone.

Rzeczywistość 5G

Rysunek 1 ilustruje wyniki pomiarów przepływności ostatnio powstałych sieci 5G (kwiecień-czerwiec 2019) w porównaniu z wynikami 4G. W większości przypadków **można zaobserwować zwiększenie przepływności od 1,3 do 2,7 razy**. W jednym przypadku w 5G jest tak samo jak w 4G, a w jednym gorzej niż 4G. Czy te osiągi są satysfakcjonujące? Przepływność 1,8 Gbit/s (przypadek najbardziej korzystny dla 5G) robi wrażenie i dlatego bywa bardzo często eksponowana w przekazie medialnym jako dowód na wyższość 5G. Problem tylko w tym, że nie do końca porównujemy „jabłka z jabłkami", gdyż przypadki wyższej prze-

pływności 5G polegają głównie na zastosowaniu szerszych kanałów lub wykorzystaniu techniki agregacji widma. 4G wykorzystujące taką samą szerokość kanału dałoby zbliżone przepływności. Nawet gdybyśmy zwiększyli przepływność kilkukrotnie, to i tak jesteśmy daleko od celu ustanowionego przez ITU (*International Telecomunications Union*), czyli 100 krotnego zwiększenia przepływności.



Rysunek 1. Porównanie pomiarów przepływności w sieci 5G oraz 4G[35].

Oznacza to, że wprowadzenie takiego 5G sprowadzi się jedynie do pojawienia się nowej ikonki „5G" na telefonie przy ikonce symbolizującej zasięg. Zmienimy więc wiele, aby nie zmieniło się nic.

Sposób budowy sieci nie zmienił się od dekad i skutkuje tzw. *vendor-lock*, czyli korzystnym dla dużych producentów zmuszeniem ich klientów (operatorów) do zakupu sprzętu i funkcjonalności (oprogramowania) u tego samego dostawcy.

Takie „silosowe" modele biznesowe, eksplorowane przez dekady (od 1G do obecnie wprowadzanego 5G), niestety nie sprawdzają się w dobie wysokiego zapotrzebowania na usługi telekomunikacyjne. Przede wszystkim dlatego, że prowadzą do wysokich kosztów i zamykają rynek dla nowych graczy, umacniając obecnych.

Nie dziwi zatem obserwacja, że czołowi producenci infrastruktury 5G naciskają na jej jak najszybsze wdrożenie, co sprowadzi się

[35] https://www.opensignal.com/

do zakupu infrastruktury u nich. Przez analogię: wyobraźmy sobie lidera fotografii analogowej Kodak, naciskającego na hurtowe zakupy jego sprzętu zaraz przed wprowadzeniem cyfrowej fotografii.

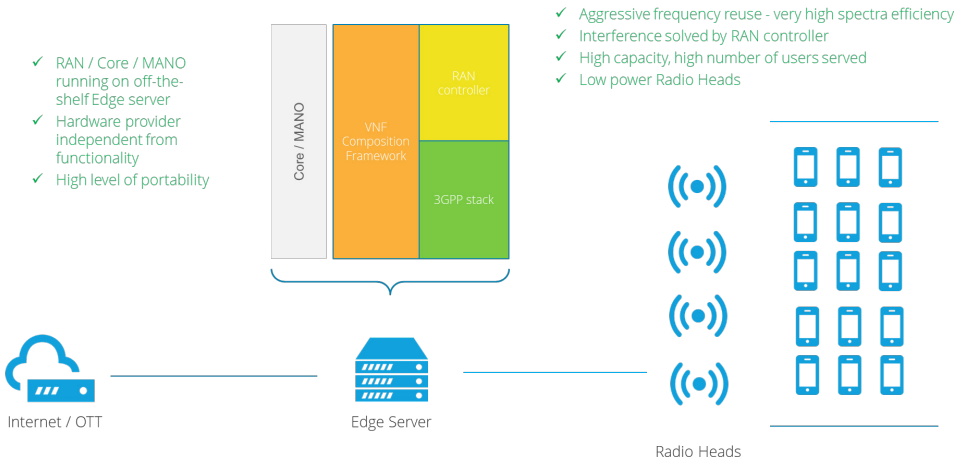
Radiowa Sieć Dostępowa

Radiowa sieć dostępowa (*Radio Access Network*, RAN) jest najdroższą i najliczniejszą (wyrażoną w liczbie węzłów/urządzeń) częścią infrastruktury telekomunikacyjnej. Ze względu na to, że RAN działa w oparciu o fizyczny kanał radiowy, jest ona również najbardziej międzydyscyplinarną i najtrudniejszą do opracowania częścią infrastruktury. Tworzy to wysoki próg wejścia dla nowych firm i dostawców. Obecnie operatorzy mobilni stoją przed dużym problemem, gdyż ruch w sieci rośnie niewspółmiernie do przychodów. Operatorzy bronią się przed przeciążeniem sieci, zakładając miesięczne limity na transfer danych. Sytuacja taka wymusza na nich, w dłuższej perspektywie, szukanie oszczędności. Efektem będzie więc przejście na infrastrukturę, która zmniejszy koszt dostarczenia [GB] danych, na przykład poprzez bardziej efektywne zarządzanie dostępnymi zasobami.

Vendor lock powoduje, że funkcjonalności RAN, zaimplementowane jako oprogramowanie stacji bazowej, są nierozerwalnie związane z dostarczanym sprzętem. Innymi słowy: dostawcą funkcjonalności i sprzętu musi być ta sama firma. Nie ma zatem mowy o tym, że jakaś inna firma wyspecjalizuje się w danej części systemu i będzie uczestniczyła w nowym łańcuchu dostaw. Taka sytuacja skutecznie blokuje nowe pomysły oraz konkurencję. Obrazując tą sytuację można przywołać analogię z branżą samochodową 100 lat temu, kiedy wszystkie podzespoły do samochodu były produkowane przez jednego dostawcę.

Wracając do funkcjonalności RAN, oprogramowanie stworzone w ramach *vendor lock* jest zoptymalizowane pod konkretny sprzęt (często chipset) i nieprzenoszalne na inne układy (jeśli nie technicznie, to biznesowo). A zatem główne braki i problemy obecnej infrastruktury RAN są następujące:

- kluczowe parametry jakościowe oczekiwane od 5G nie mogą być spełnione z wykorzystaniem obecnej infrastruktury (np. tysiąckrotne zwiększenie pojemności sieci wyrażone w [bit/s/Hz/m2] czy obniżenie opóźnień do 1 ms.;
- koszty dostarczenia [GB] oraz utrzymania infrastruktury są zbyt wysokie;
- obecne rozwiązania RAN są zoptymalizowane pod konkretny sprzęt, przez co nie można ich przenieść na inny sprzęt;
- obecne rozwiązania RAN oferują nieoptymalne parametry jakościowe, gdyż są oparte (w zakresie przydziału zasobów radiowych) na paradygmacie rywalizacji o zasoby, a nie na zasadzie współpracy. Kosztowne zasoby radiowe nie są efektywnie wykorzystywane, a przez to ich użycie jest drogie.



Rysunek 2. Zdefiniowana programowo funkcjonalność sieci RAN[36]

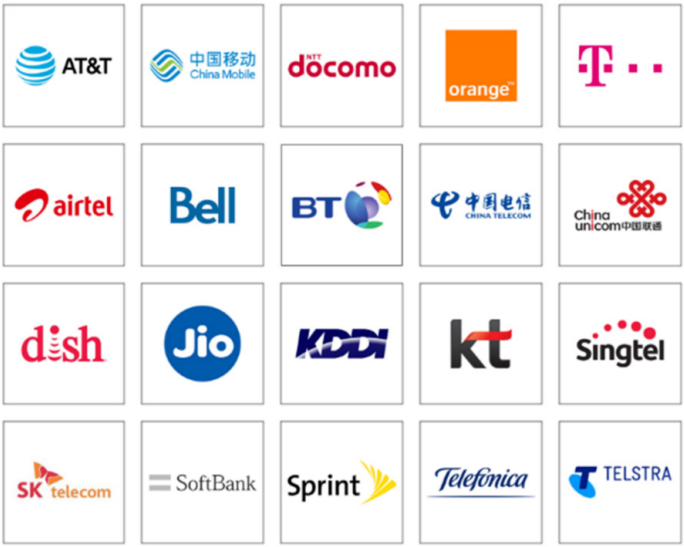
Open RAN

Rozwiązaniem wymienionych problemów jest architektura otwarta, pozbawiona *vendor-lock'a*. W takim ujęciu funkcjonalność (oprogramowanie) jest odseparowana od sprzętu i to klient (np. operator) decyduje, o tym kto będzie dostawcą sprzętu i oprogramowania.

Open RAN to otwarta architektura sieci RAN, w której funkcjonalność RAN jest zdefiniowana programowo. Oznacza to, że jest gotowa do umieszczenia na dowolnych zasobach sprzętowych (np. serwerach kupowanych „z półki") i obsługuje głowice radiowe (*Radio Heads*) wielu dostawców, jak pokazano na Rysunku 2. Funkcjonalność RAN składa się ze zwirtualizowanego stosu protokołów wspierających dowolne G (np. 4G, 5G), Kontrolera RAN oraz interfejsów do głowic radiowych, a także sieci szkieletowej (Core). Kontroler RAN, będący „mózgiem" RAN, implementuje strategie inteligentnego przydziału zasobów radiowych, żeby zminimalizować interferencje oraz zoptymalizować parametry jakościowe.

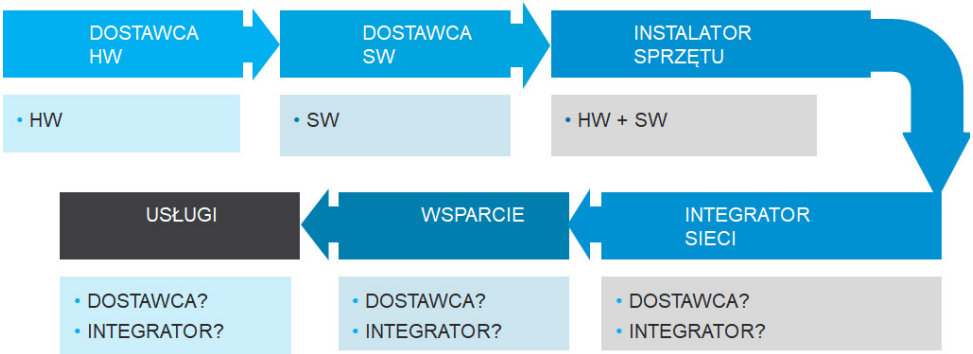
Open RAN (ORAN) jest przedmiotem standaryzacji Open RAN Alliance, czyli aliansu strategicznego firm i instytucji zainteresowanych zbudowaniem rozwiązania sieciowego, dającego klientowi szersze pole manewru (Rysunek 3). Open RAN Alliance dopełnia 3GPP. Jedyną polską firmą należącą do ORAN Alliance jest IS-Wireless.

[36] https://www.is-wireless.com



Rysunek 3. Główni partnerzy ORAN[37]

Pierwszym znaczącym wdrożeniem ORAN jest sieć 4G (i wkrótce 5G) operatora Rakuten z Japonii. Rakuten sam zdecydował od kogo kupi głowice radiowe RH, na jakich serwerach postawi oprogramowanie, a wreszcie sam wybrał najlepszy dla swoich potrzeb system do zarządzania całą siecią. Jednak tym, co najlepiej obrazuje korzyści płynące z takiej elastyczności, jest wybranie przez Rakuten niezależnej firmy, która dostarcza algorytmy „szybkiego zarządzania zasobami SON". Będą one instalowane na serwerach, sterując oprogramowaniem i sprzętem innych firm. Elastyczność podziału funkcji w łańcuchu dostaw infrastruktury obrazuje Rysunek 4.



Rysunek 4. Potencjalny Łańcuch dostawców[38]

[37] https://www.o-ran.org

[38] https://www.is-wireless.com

Suwerenność technologiczna

Terminem nabierającym w ostatnim czasie szczególnego znaczenia jest suwerenność technologiczna. W dobie ryzyka wszechobecnej inwigilacji, zasadne wydaje się poszukiwanie rozwiązań, które w jak największym stopniu uniezależnią nas od zewnętrznych wpływów. Zwiększy to także poziom bezpieczeństwa. Wspomniany wcześniej *vendor-lock* z definicji skazuje nas na rozwiązania obce, niezależnie od tego z której części świata one pochodzą. Zatem zwiększenie konkurencyjności łańcucha dostaw przez wprowadzenie większej liczby graczy jest dobrym sposobem na zwiększenie suwerenności technologicznej. Dostrzegła to Komisja Europejska, która w styczniu 2020 roku, opublikowała dokument *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*. Podkreślono w nim, że dywersyfikacja dostawców oraz łańcucha wartości to podstawowe narzędzia do zmniejszenia ryzyka R4, czyli zależności od jednego dostawcy (*dependency on a single supplier*). Dostrzega to również USA. Kongres zaproponował dofinansowanie w wysokości co najmniej 1 mld. dolarów na tworzenie alternatywnych rozwiązań 5G.

Dostępność pasma

Potrzebą analogiczną do otwarcia architektury i usunięcia *vendor-lock* z łańcucha dostaw infrastruktury telco, jest umożliwienie korzystania z pasm 5G przez graczy mniejszych, niż tylko krajowi operatorzy komórkowi. Do tych graczy możemy zaliczyć porty, lotniska, dworce, galerie handlowe, biurowce, zakłady pracy, szpitale i wiele, wiele innych. To oni mają największą świadomość potrzeb końcowego klienta. Często dysponują także gotową infrastrukturą, którą można wykorzystać do budowy sieci telco. Przykładem są chociażby miasta dysponujące latarniami, które mogą być z powodzeniem wykorzystane jako słupy do instalacji małych końcówek radiowych czy serwerów brzegowych.

Oczywiście idące w miliardy złotych kwoty oczekiwane z aukcji licencji na 5G, znajdują się poza ekonomicznym zasięgiem tych małych graczy. Dlatego w niektórych krajach, np. w Niemczech dopuszczono do licencjonowania pasm na prywatne sieci 5G w modelu, gdzie za kanał radiowy (10 MHz) ponosi się opłatę w rozliczeniu na obsługiwaną jednostkę powierzchni. Co oznacza koszt około 1000 EUR za 10 MHz na 10 lat na 10km2.

Podsumowanie

5G należy postrzegać w szerszym kontekście. Stoimy u progu rewolucji sieciowej. Aby sobie ją wyobrazić cofnijmy się w czasie około 10 lat i przypomnijmy sobie rynek telefonów komórkowych. Istniały już wtedy aplikacje mobilne, ale było ich niewiele, ponieważ były dostarczane przez producentów telefonów (sprzętu). W tym obszarze istniał więc *vendor-lock*. Dopiero wprowadzenie otwartych systemów operacyjnych pozwoliło na „odpięcie" aplikacji (oprogramowania) od telefonu (sprzętu). Efektem była eksplozja przedsiębiorczości na rynku aplikacji mobilnych, powstanie nowych modeli biznesowych, a co za tym idzie: powstanie nowych gałęzi przemysłu. Przez analogię, rewolucja sieciowa spowodowana otwarciem infrastruktury sieciowej doprowadzi do podobnych, a nawet o wiele dalej idących zmian na rynku telekomunikacyjnym.

Istota 5G nie leży w aktualnie wprowadzanym 5G NR. Sprowadza się raczej do ostatecznego oddzielenia funkcjonalności od sprzętu, czyli wirtualizacji sieci, szczególnie w części radiowej. Jest to warunek konieczny, aby znacząco obniżyć koszt dostarczenia GB danych. Wirtualizacja pozwala agregować funkcjonalność i upraszczać najliczniejsze elementy, czyli końcówki radiowe (do niedawna stacje bazowe). Zagęszczenie siatki sieci radiowej jest jedynym sposobem, aby zbliżyć się do ambitnych celów pojemnościowych postawionych przed 5G tj. tysiąc razy większej pojemności (na m^2) względem poprzedniej generacji. Wirtualizacja pobudza także nowe modele biznesowe, obniża próg wejścia do biznesu i umożliwia tworzenie funkcjonalności (*network programmability*) oraz usług praktycznie przez każdego. Istota 5G sprowadza się zatem do powstania zupełnie nowych modeli biznesowych.

Open RAN stwarza operatorom możliwość wyeliminowania *vendor-lock*, blokującego swobodę doboru optymalnych rozwiązań, a także znacząco zwiększa przewagę negocjacyjną. Dla potencjalnego operatora krajowego, oparcie się na architekturze Open RAN to znaczące obniżenie kosztów budowy samej sieci. To także możliwość poprawy bezpieczeństwa, gdyż każdy niedziałający element będzie można łatwo wymienić.

Stoimy w przededniu znaczącego skoku technologicznego i cywilizacyjnego. Z kilku powodów dotyczy to szczególnie Polski. Po pierwsze, nasz rodzimy rynek IT jest nastawiony głównie na dostosowywanie czyichś rozwiązań, dorabianie peryferii czy wprost sprzedawanie czasu pracy naszych specjalistów. Nie tworzymy istotnych części systemów, nie budujemy „silników". To smutne, a w zestawieniu z faktem, że nasi specjaliści plasują się regularnie w światowej czołówce top 3 rankingów deweloperów[39], wygląda na niewykorzystanie ogromnego potencjału. Po drugie, tworzenie „silników" zawsze daje o wiele większą marżę niż dorabianie „peryferii". Co więcej, 5G niesie ze sobą ostateczne „odpięcie" funkcjonalności od sprzętu. Mobilne sieci

[39] https://www.cybercom.com/pl/Poland/software-house/blog/ranking-of-developers/

przyszłości będą oparte na oprogramowaniu. To stwarza ogromną szansę dla naszego kraju, jeśli tylko znajdziemy swój udział w ich tworzeniu, a nie jedynie w uruchamianiu czy dopasowywaniu.

IS-Wireless jest polską firmą wysokiej techniki, która skupia się na budowie, implementacji oraz globalnej komercjalizacji mobilnych sieci przyszłości, w tym 5G. Firma specjalizuje się w Radiowej Sieci Dostępowej i jest członkiem ORAN Alliance oraz TIP.

5G w perspektywie politycznej

5G to nie tylko temat technologiczny, ale także polityczny. Kontekst cyfrowej suwerenności oraz wielka dyskusja na temat dostawców, udowodniły, że zarówno państwa europejskie, jak i pozaeuropejskie postrzegają 5G nie tylko jako nową rewolucję, która przyspieszy cyfrową technologię, ale także jako narzędzie polityczne. We wspomnianym wcześniej Toolboxie, jednym z ważniejszych rekomendacji na poziomie UE jest dywersyfikacja dostawców.

Dr Konrad Popławski

5G w Niemczech – szanse, perspektywy, kontrowersje

Konrad Popławski – Kierownik Zespołu Środkowoeuropejskiego Ośrodka Studiów Wschodnich. Autor kilkunastu artykułów naukowych, ponad 100 analiz i kilkunastu opracowań dotyczących gospodarki Niemiec, ich handlu zagranicznego i relacji ekonomicznych z Europą Środkową. Doktor nauk ekonomicznych (rozprawa doktorska pt. „Zmiany w handlu zagranicznym Niemiec po przystąpieniu do strefy euro", obroniona z wyróżnieniem w Szkole Głównej Handlowej). Kierownik i członek kilku zespołów badawczych przygotowujących analizy w ramach projektów Międzynarodowego Funduszu Wyszehradzkiego.

Stan rozbudowy sieci 5G

12 czerwca 2019 roku zakończyła się aukcja na częstotliwości dla sieci 5G. Czterech niemieckich operatorów Deutsche Telekom, Vodafone, Telefónica i 1&1 Drillisch zapłaciło za nabyte pasma w sumie 6,5 mld euro. Ambicją prezesa odpowiedzialnej za przetarg Federalnej Agencji Sieci jest, żeby do 2022 roku przynajmniej 98% gospodarstw domowych uzyskało dostęp do 5G, a także żeby tego typu sieć została rozbudowana wzdłuż niemieckich dróg krajowych (federalnych) i linii kolejowych.

W lipcu 2019 roku **Vodafone** jako pierwszy rozpoczął instalację 150 anten 5G i zamierza do końca 2020 roku podłączyć do sieci nowej generacji 10 mln ludzi, a do końca 2021 roku – 20 mln ludzi. **Deutsche Telekom** zainstalował do tej pory 450 anten 5G, a sieć piątej generacji jest dostępna w określonych częściach 8 miast: Berlina, Bonn, Frankfurtu, Lipska, Hamburga, Darmstadt, Kolonii i Monachium. Do końca 2020 roku liczba anten ma się zwiększyć do 1500 (zlokalizowanych w 20 miastach). Koncern chce udostępnić sieć 5G dla 99% populacji i na 90% powierzchni kraju do 2025 roku **Telefónica** deklaruje zamiar zapewnienia dostępu do 5G w 30 miastach (z 16 mln mieszkańców) do końca 2022 roku i rozpoczęła już pierwsze prace. Ostatni z operatorów, czyli **1&1 Drillisch**, nie ogłosił dokładnych planów, ani nie zaczął budowy sieci 5G.

Niezbyt szybkie wdrażanie 5G, w stosunku do rozbudowy sieci 4G, przez niemieckie telekomy wynika ze świadomej strategii. Z jednej strony chcą one, żeby zwróciły im się koszty poniesione na budowę sieci LTE. Z drugiej strony nie są jeszcze pewne zastosowań sieci 5G, dlatego zamierzają inwestować w obszary o najwyższym potencjale zysków: miejsca z dużym ruchem turystycznym (ścisłe centra miast, dworce) i obszary targowe.

Duże zainteresowanie niemieckiego biznesu

Według organizacji Bitkom niemieckie przedsiębiorstwa uważają sieć 5G za kluczową technologię determinującą pozycję Niemiec w globalnej gospodarce. 84% przedsiębiorców jest zdania, że sieć 5G znacząco zwiększy ich produktywność, a 73% uznaje ją za kluczową dla sukcesów na rynkach zagranicznych. Nowa generacja sieci mobilnych ma według nich również:

- zapewnić łączność między urządzeniami produkcyjnymi (54%),
- pozwolić wykorzystać w produkcji systemy rozszerzonej rzeczywistość (50%),
- zapewnić komunikację w czasie rzeczywistym między maszynami (49%),
- umożliwić uruchomienie autonomicznych pojazdów do przewozu osób i transportu dóbr (39%),

- zwiększyć stopień użytkowania mobilnych robotów (31%).

Jeśli więc niemieckie przedsiębiorstwa uzyskają dostęp do sieci 5G z opóźnieniem, to ryzykują pogorszeniem swojej konkurencyjności.

Jednocześnie biznes jest niezadowolony z dotychczasowego rozwoju sieci mobilnych w Niemczech. Według danych firmy Opensignal Niemcy, z pokryciem kraju siecią 4G/LTE na poziomie 65,7%, znajdują się dopiero na 70. miejscu na świecie. Tymczasem główni konkurenci Niemiec znajdują się czołówce rankingów: Korea Południowa jest pierwsza (97,5%), Japonia druga (94,7%), a Stany Zjednoczone piąte (90,3%). Dla porównania Polska z pokryciem na poziomie 72,8% sytuuje się na 50. miejscu.

To właśnie presja niemieckiego biznesu spowodowała zagwarantowanie części częstotliwości (100 MHz z dostępnych 400 MHz w paśmie 3,6 GHz) wyłącznie dla potrzeb lokalnych, co pozwoli niemieckim koncernom samodzielnie (bądź we współpracy z telekomami) budować sieci 5G na potrzeby konkretnych fabryk.

Kontrowersje wokół Huawei

W sytuacji niedostatecznego rozwoju sieci mobilnych w Niemczech, Huawei jest kluczowym kandydatem do rozbudowy 5G. Chińska firma jest liderem rynkowym i ma długą tradycję współpracy z niemieckimi telekomami. Obecnie około 45% z 75 tys. stacji bazowych sieci 4G/LTE w Niemczech pochodzi od Huawei, podczas gdy udział tej firmy w instalacjach w całej Europie to około 33%.

W ostatnich miesiącach okazało się jednak, że dopuszczenie Huawei do rozbudowy 5G w Niemczech nie jest pewne. Choć w październiku 2019 roku Federalna Agencja Sieci zezwoliła na udział wszystkich zagranicznych przedsiębiorstw w budowie 5G w Niemczech, to w kolejnych miesiącach część posłów koalicji rządzącej chadecji i socjaldemokratów zażądała debaty na ten temat w Bundestagu. Przekonała ich prowadzona przez cały ubiegły rok kampania informacyjna Stanów Zjednoczonych, wskazująca, że technologie 5G od Huawei mogą być zagrożeniem dla bezpieczeństwa narodowego RFN ze względu na oskarżenia o bliską współpracę z organami bezpieczeństwa Chin. Dopuszczenie Chińczyków do rozbudowy 5G w Niemczech mogłoby nawet grozić ograniczeniem współpracy wywiadowczej, co jest bardzo ważną kwestią dla niemieckich służb specjalnych. Na razie nie ma pewności, jak dalej potoczy się debata. Bundestag chce podjąć ostateczną decyzję w tej sprawie w ciągu najbliższych miesięcy. Część telekomów zamroziła do tego czasu współpracę z Huawei w rozbudowie 5G.

Pogłębione analizy na ten temat są dostępne na stronie www.osw.waw.pl

NASK

Cyber POLICY

Iwona Wiśniewska

Rozwój sieci mobilnej 5G w Rosji kluczowym elementem programu cyfryzacji gospodarki

Iwona Wiśniewska – Analityczka Ośrodka Studiów Wschodnich od 2000 roku, zatrudniona w Zespole Rosyjskim. W latach 2012–2014 dyplomata ds. ekonomicznych Ambasady RP w Astanie, w latach 2014–2016 kierownik Wydziału Ekonomicznego Ambasady RP w Moskwie.

Tematy badawcze: Rosyjska gospodarka: trendy makroekonomiczne, polityka gospodarcza Federacji Rosyjskiej (FR), zmiany własnościowe, polityka inwestycyjna Rosji; Zagraniczna polityka gospodarcza Federacji Rosyjskiej (FR), w tym integracja regionalna w ramach Euroazjatyckiej Unii Gospodarczej.

Cyfryzacja gospodarki Rosji stała się jednym z priorytetów działań rządu w IV kadencji prezydenta Putina. Za wzrostem znaczenia cyfryzacji stoją co najmniej trzy główne powody. Po pierwsze, jest to rosyjska odpowiedź na transformację technologiczną na świecie i konieczność przeciwdziałania dalszemu pogłębianiu się dystansu między FR i liderami światowej gospodarki. Po drugie, rosyjskie władze upatrują w cyfryzacji gospodarki potencjalne nowe źródło rosyjskiego wzrostu gospodarczego, które mogłoby zastąpić wyczerpujący się model rozwoju oparty na sektorze surowcowym. Po trzecie, kosztowny proces cyfryzacji – w większości finansowany z budżetu państwa – jest okazją do uzyskania dostępu do publicznych środków i dalszego bogacenia się rosyjskiej elity polityczno-biznesowej.

Kluczowym elementem procesu cyfryzacji gospodarki Rosji jest rozwój infrastruktury teleinformatycznej, w tym przede wszystkim budowa sieci mobilnej piątej generacji. Przy czym warto zaznaczyć, że struktury siłowe postrzegają sferę wirtualną jako przestrzeń quasi-militarnej konfrontacji, co sprawia, że rozwój sektora cyfrowego, w tym sieci 5G, podporządkowany jest kwestiom bezpieczeństwa. To one dominują nad efektywnością i kosztami.

Pomiędzy strukturami siłowymi, głównymi decydentami w kwestiach cyfryzacji, a podmiotami branżowymi (np. operatorami komórkowymi) zarysowały się poważne sprzeczności interesów. Spowodowały one, że wypracowanie koncepcji rozwoju i wdrażania sieci 5G w Rosji przeciąga się. Zgodnie z przyjętymi założeniami, początkowo infrastruktura 5G ma być budowana w największych miastach Rosji (powyżej 1 miliona mieszkańców), przede wszystkim na potrzeby wybranych sektorów gospodarki (obecnie nie zostały one sprecyzowane). Rozwój 5G, jak i wdrażanie całego programu cyfryzacji rosyjskiej gospodarki, ma być oparty w jak największym stopniu na rosyjskich: technologii, oprogramowaniu i urządzeniach. Tak aby znaczna część nakładów na rozwój 5G trafiła do rosyjskich podmiotów, głównie państwowych lub powiązanych z rosyjską elitą władzy.

Według oficjalnych szacunków łączne koszty rozwoju sieci 5G w Rosji mogą wynieść nawet 650 mld rubli (ok. 10 mld USD), przy czym znaczna część tych środków ma pochodzić z budżetu państwa. Obecny poziom rozwoju ICT w Rosji wymusza jednak współpracę z zagranicznymi koncernami, dlatego też Rosja stara się dywersyfikować kontrahentów (Ericsson, Nokia, Huawei) i wymuszać na nich lokalizację choć części produkcji w Rosji.

Rosyjska elita, zgodnie z dotychczasową logiką rządzenia, dąży do utrzymania pełnej kontroli również nad sektorem cyfrowym. Wbrew przedstawianym negatywnym analizom, Kreml forsuje koncepcję zmonopolizowania rynku przez Jedynego Operatora Infrastruktury. Ponadto *siłowicy*, zasłaniając się kwestiami bezpieczeństwa, blokują

dostęp do pasma 3,4-3,8 GHz. Na żądanie ministerstwa obrony wstrzymane zostały w 2019 roku testy sieci 5G na tych częstotliwościach. Struktury siłowe postulują rozwój sieci 5G na początkowym etapie na częstotliwościach używanych przez operatorów komórkowych na potrzeby niższych standardów (3G i 4G) i nowym paśmie 4,4-4,99 GHz. W przypadku pasma 694-790 MHz, zajmowanego obecnie przede wszystkim przez nadawców telewizyjnych, w zasadzie nie toczy się publiczna debata. Formalnie operatorzy komórkowi uzyskali dostęp do „700-tki" już w 2012 roku na potrzeby LTE, w praktyce jednak pasmo to dotychczas nie zostało uwolnione. Sami operatorzy również zbytnio nie naciskają na przekazanie im tego pasma ze względu na to, że 5G nie będzie początkowo rozwijane poza dużymi miastami. Dodatkowym aspektem jest konieczność synchronizacji działań dotyczących pasma 694-790 MHz między Rosją a sąsiadującymi krajami. Dlatego niewykluczone, że Kreml może chcieć wykorzystać kwestię częstotliwości radiowych jako element nacisku wobec sąsiednich państw UE oraz Brukseli.

Trudno wyrokować kiedy zostanie podjęta ostateczna decyzja w Rosji o wydzieleniu częstotliwości radiowych dla 5G. Zgodnie z wcześniej przyjętym harmonogramem miało to nastąpić do października 2019 roku. Analizując przygotowania do rozwoju 5G w Rosji można stwierdzić, że Kremlowi nie zależy na forsowaniu tempa przy wdrażaniu sieci nowej generacji. Proces ten nie jest ograniczony żadnymi sztywnymi terminami, o czym świadczą dotychczasowe opóźnienia. W praktyce wdrażanie sieci 5G będzie odbywać się najprawdopodobniej stopniowo, przede wszystkim na obszarach o największym popycie na tego typu usługi: Moskwa, Petersburg i okolice.

Tekst powstał na podstawie raportu dotyczącego procesu cyfryzacji rosyjskiej gospodarki i rozwoju sieci 5G, który w najbliższych miesiącach ukaże się na stronie OSW.

Jakub Jakóbowski

Huawei i 5G: chińska droga do światowej czołówki w branży ICT

Jakub Jakóbowski – Główny Specjalista w Programie Chińskim Ośrodka Studiów Wschodnich. Specjalizuje się w badaniach chińskiej polityki gospodarczej i przemysłowej. Doktorant w Kolegium Ekonomiczno-Społecznym SGH, przygotowuje rozprawę doktorską na temat chińskiej zagranicznej polityki ekonomicznej wobec państw rozwijających się.

Telekomunikacja jest od lat strategicznym priorytetem chińskiej polityki przemysłowej, a także jednym z jej największych dotychczasowych sukcesów. Chińskie firmy i inżynierowie znajdują się w globalnej czołówce w tym obszarze. Ma to zarówno podłoże polityczne, jak i gospodarcze. Z punktu widzenia Komunistycznej Partii Chin, rozwój rodzimych technologii telekomunikacyjnych

ma istotne znaczenie z punktu widzenia bezpieczeństwa wewnętrznego, w tym zastosowania nowych technologii (m.in. Big Data, Sztuczna Inteligencja, łączność) do inwigilacji i kontroli społeczeństwa. Nowoczesna infrastruktura cyfrowa, a także rozwinięty przemysł ICT, mają być też jednym z nowych kół zamachowych chińskiej gospodarki i wiodącym produktem eksportowym.

Technologia 5G ściśle wpisuje się w zarysowaną wyżej agendę, została więc określona jako narodowy priorytet w ramach ogłoszonej w 2013 r. strategii Made in China 2025 (postulującej m.in. maksymalizację udziału chińskich spółek w tworzeniu standardów 5G). 5G zostało również wpisane do XIII Planu Pięcioletniego (2016-2020) i szeregu chińskich sektorowych strategii. Przekłada się to na:

- znaczące wsparcie administracyjne dla firm technologicznych,
- priorytet dla wdrożeń 5G w działaniach legislacyjnych,
- mobilizację ogromnych zasobów na badania i rozwój,
- finansowe wsparcie zagranicznej ekspansji chińskich firm.

Efektem polityki chińskich władz są stosunkowo szybkie i szerokie wdrożenia 5G na terenie Chin, rozpoczęte komercyjnie w listopadzie 2019 roku. W 2020 roku trzy państwowe spółki telekomunikacyjne – China Mobile, China Unicom i China Telecom – planują łącznie instalację ok. 600 tys. stacji bazowych. Do 2025 roku sieć 5G objąć ma ok. 600 mln użytkowników (ok. 40% rynku). W obliczu spowolnienia gospodarczego związanego z epidemią koronawirusa, rozwój sieci 5G stał się jeszcze ważniejszym priorytetem politycznym – chińskie władze liczą, że rozwój sieci napędzi wzrost nowych sektorów gospodarki, a także przyspieszy modernizację chińskiego przemysłu.

Niekwestionowanym liderem chińskiego rynku urządzeń telekomunikacyjnych jest firma Huawei, dominująca pod względem skali i zaawansowania technologicznego nad innymi chińskimi firmami, m.in. ZTE. Huawei założony został w 1987 roku w chińskim Shenzhen, przez byłego pracownika instytutu badania łączności Chińskiej Armii Ludowo-Wyzwoleńczej, Ren Zhengfeia. Huawei nie jest formalnie zależny od chińskich struktur państwowych, znajduje się jednak w bliskich związkach z partią komunistyczną – Ren posiada 1,4% udziałów Huawei, a reszta należy do działającego w spółce, kontrolowanego przez partię związku zawodowego. Mimo powiązań z władzą poprzez kanał partyjny, przyjęty model zarządzania wpłynął na rozwój spółki, otwierając ją na bodźce konkurencji rynkowej. Na początku istnienia Huawei – w przeciwieństwie do wielkich państwowych koncernów branży ICT – miał ograniczony dostęp do państwowych subsydiów i sterowanych przez państwo transferów zagranicznych technologii. Firma musiała walczyć o mniej lukratywne i trudniejsze regionalne rynki telekomunikacji w Chinach.

Doprowadziło to do wytworzenia w Huawei unikatowej, elastycznej struktury organizacyjnej, a także stosunkowo rozbudowanego pionu R&D wewnątrz firmy. Huawei wszedł również w komercyjne segmenty telekomunikacji, stając się m.in. czołowym producentem telefonów komórkowych. Po sukcesie firmy na rynku lokalnym, została ona dostrzeżona przez rząd centralny i od ok. 2004 roku traktowana jest jako „narodowy czempion", otrzymujący szerokie wsparcie od państwa. Koncern dokonał dzięki temu znacznych inwestycji zagranicznych, m.in. w Europie, włączając się w tworzenie nowych standardów dla branży telekomunikacyjnej. Huawei posiada jednak kilka słabych punktów, m.in. polega w dużej mierze na dostawach zagranicznych półprzewodników, a w sektorze elektroniki komercyjnej – również na zagranicznym oprogramowaniu.

Obok technologicznych i organizacyjnych atutów firmy, a także znacznego udziału w tworzeniu standardu 5G, pozycję Huawei należy też wiązać ze znaczącym wsparciem, które firma otrzymuje od chińskiego rządu. Tyczy się to m.in. niemal nieograniczonego dostępu do kapitału z chińskiego państwowego sektora bankowego, a także oferowania korzystnych kredytów eksportowych przez China Development Bank (CDB), pod warunkiem zakupów sprzętu Huawei. Efektem ekspansji Huawei jest obecność w ok. 140 państwach, w tym wielu państwach rozwijających się, a przez to wyprzedzenie europejskich producentów w rynkowym udziale produkcji sprzętu telekomunikacyjnego. Huawei utrzymuje pozycję lidera (31%), przed Ericssonem (27%) i Nokią (22%). Firma ma również ok. 75 proc. udziałów w silnie chronionym rynku chińskim, co zapewnia jej znaczące korzyści skali. Choć w przypadku 4G chińskie ceny w dużej mierze zrównały się cenami europejskiej konkurencji, to w pierwszych wdrożeniach 5G Huawei – korzystając z państwowego zaplecza finansowego – ponownie zaczął agresywną konkurencję cenową. W jednym z przetargów w Holandii zaoferował ceny nawet 60% niższe od Ericssona czy Nokii.

Wejście Huawei do globalnej czołówki producentów sprzętu telekomunikacyjnego to pierwszy tej skali sukces chińskiej polityki przemysłowej, o istotnych reperkusjach międzynarodowych. Dla administracji prezydenta Trumpa powstrzymywanie Huawei stało się pierwszą bitwą w chińsko-amerykańskiej wojnie technologicznej. Dla USA rozwój i eksport chińskich technologii – szczególnie w branżach wrażliwych – oznacza zwiększenie politycznych wpływów Chin na świecie, eksport autorytarnych narzędzi kontroli społeczeństwa, nowe wyzwania dla cyberbezpieczeństwa, a w dłuższej perspektywie potencjalną utratę prymatu USA w technologiach wojskowych. Z drugiej strony, ekspansja Huawei jest przykładem tego, jak chińska polityka przemysłowa i znaczne wsparcie państwa są w stanie zaburzyć międzynarodową konkurencję, stawiając na straconej pozycji zagranicznych producentów. Widoczne jest to

w szczególności na terenie Unii Europejskiej, która posiada co prawda własnych silnych dostawców w dziedzinie infrastruktury 5G, ale pozostaje asymetrycznie otwarta na ekspansję chińskich koncernów – w ten sposób pogłębiając zależność od Chin, a jednocześnie tracąc konkurencyjność w najbardziej rokujących technologiach.

Pogłębione analizy na ten temat są dostępne na stronie www.osw.waw.pl

NASK

Cyber POLICY

NASK Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

ISBN 978-83-954637-3-0

cyberpolicy.nask.pl