# Stanowisko Rady ds. Cyfryzacji dotyczące rozwoju technologii 5G w Polsce w kontekście cyberbezpieczeństwa.

## 1. Wstęp

Kształt europejskiej i polskiej gospodarki oraz jakość życia wszystkich Europejczyków zdeterminowane będą w najbliższych latach przez podejście do kwestii takich jak rozwój i implementacja nowych technologii pokroju 5G, cyberbezpieczeństwo czy rozwój w całej UE Jednolitego Rynku Cyfrowego. Wyzwaniem będzie rozpędzenie cyfrowej gospodarki w sposób bezpieczny i spójny w całej wspólnocie. Nowe technologie i digitalizacja przenikają wszystkie jej poziomy – życie każdego z obywateli, działalność przedsiębiorstw, aparatu administracji publicznej i w końcu całej Wspólnoty Europejskiej jako całość. Zadaniem władz unijnych i poszczególnych państw członkowskich, w tym Polski, będzie otwarcie się na te przemiany, skorzystanie z ich potencjału, wzmocnienie gospodarki opartej na cyfryzacji i zwiększenie jakości życia obywateli przy zachowaniu bezpieczeństwa i dbałości o świadomość i edukację obywateli w zakresie zachodzących zmian.

**Największym wyzwaniem dla Europy, w tym dla Polski w nadchodzących latach będzie implementacja technologii mobilnej piątej generacji.** Stawka stojąca za 5G jest ogromna. Technologia ta ma bowiem zapewnić nieporównywalnie większą przepływowość, mniejsze opóźnienia, możliwość obsługi gigantycznej liczby urządzeń jednocześnie. Jej implementacja może także skutkować wielomiliardowym wzrostem PKB, nowymi miejscami pracy oraz bardziej dynamicznym rozwojem gospodarki i nowych jej gałęzi. To pociągnie za sobą powstanie gamy wielu usług, które przez ograniczenia dzisiejszego standardu sieci były dla nas niedostępne. Przede wszystkim jednak, wprowadzenie i wykorzystanie potencjału nowej technologii to być albo nie być dla Europy jako siły gospodarczej na światowej arenie.

Niepokojący jest to, że wiele państw nadal nie zaprezentowało swojej strategii wprowadzenia sieci piątej generacji, bez której prace nad jej upowszechnieniem mogą być trudne lub wręcz niemożliwe. Powszechnym kłopotem jest udostępnienie pasm częstotliwości radiowych potrzebnych operatorom do uruchomienia sprawnej sieci nowej generacji. Nie brakuje też wątpliwości, w jakim stopniu można ufać niektórym z dostawców technologii. To sygnał szczególnie niepokojący w świetle obaw o konsekwencje płynące z monopolu na budowę struktur do obsługi sieci. Tym bardziej, że Stany Zjednoczone od miesięcy alarmują o powiązaniach chińskiego wywiadu z Huawei i przestrzegają państwa NATO i innych swoich sojuszników przed współpracą z Chińską Republiką Ludową przy budowie sieci 5G.

„UE, jak i sama Polska, powinny stworzyć warunki do jak najszybszego nadrobienia zaległości w zakresie budowania europejskiej autonomii w ramach rozwoju sieci 5G. W tym wymiarze należy ją rozumieć, nie tylko jako budowanie w przyszłości polskiego potencjału technolo-

gicznego w oparciu przede wszystkim o rodzime firmy dostarczające rozwiązań technologicznych, we wspierającej (nie dominującej) współpracy z zaufanymi partnerami, ale także jako niekreowanie i niepogłębianie tu i teraz zależności, które wystawią sieć 5G na zagrożenia bezpieczeństwa ze strony krajów trzecich. Należy postawić przede wszystkim na budowę infrastruktury telekomunikacyjnej w oparciu o dostawców – a nie same komponenty – godnych zaufania. Jest to bowiem najważniejsza inwestycja w strategiczną autonomię oraz w globalną pozycję Europy, jaką dzisiaj możemy poczynić”[1]. Weryfikacja na poziomie komponentów bez oceny całościowej ryzyka nie jest właściwa z uwagi na nieuwzględnienie aspektu geopolitycznego oraz nie uwzględnianie w ocenie bezpieczeństwa sieci jako całego systemu. W tym kontekście ważne są procesy implementacyjne, utrzymanie sieci i wsparcie techniczne. Same zaufane komponenty nic nie dadzą przy niewłaściwym ich zastosowaniu. Z całą pewnością Europa ma świetną podstawę do budowania takiej autonomii, z rodzimymi dostawcami technologii, centrami rozwojowymi 5G zlokalizowanymi w Europe – w tym na obszarze Polski – oraz dobrymi doświadczeniami coraz liczniejszych implementacji technologii 5G w krajach europejskich.

**Zadaniem Europy i Polski powinno być wyraźne nakreślenie ram prawnych i wymagań dla dostawców infrastruktury 5G, które będą gwarantowały bezpieczeństwo użytkowników i zadbanie o to, by nie dochodziło do monopolizacji rynku sprzętu do budowania sieci.** Konieczne jest podnoszenie świadomości na temat potencjału technologii zarówno na poziomie obywateli, przedsiębiorców, rządów i władz unijnych.

Choć niełatwo będzie pogodzić konieczność utrzymania wysokiego tempa implementacji nowej technologii z dbałością o bezpieczeństwo i edukacją, to rzeczywistość nie pozostawia nam wyboru. Azja i Stany Zjednoczone, nie będą czekać na Europę, by zacząć korzystać z przewagi, jaką daje ta nowa technologia. Dlatego Europa nie może przegrać tego wyścigu o rozkwit technologiczny starego kontynentu, a technologia 5G warunkuje rozwój takich technologii przyszłości jak m.in. sztuczna inteligencja czy informatyki kwantowej. Stawką w rywalizacji jest także wspomniana strategiczna (cyfrowa) autonomia oraz konkurencyjność europejskiej gospodarki i Przemysłu 4.0. Technologia i sieć 5G zmieni charakter i efektywność procesów produkcyjnych, ale doprowadzi także do dalszej konwergencji cyfrowej, pogłębiając już tę obserwowaną w ramach poszczególnych technologii i branż ICT, ale także rozpoczynając proces łączenia branży ICT ze wszystkimi sektorami gospodarki. W erze rozrywania globalnego łańcucha dostaw (*global supply chain decoupling*) na szali jest także pozycja Europy w nowym krajobrazie łańcuchów dostaw, którego jeden z wymiarów związany jest z rozwojem i wdrożeniem technologii 5G. Dokładnie jak miało to miejsce w przypadku rozwoju sieci 4G, z którego najwięcej benefitów przypadło USA i amerykańskim firmom technologicznym i doprowadziło do dominacji w bezprzewodowych usługach internetowych, tak i teraz po

[1] *Przyszłość 5G czyli Quo Vadis, Europo*?, Instytut Kościuszki, 2019

wdrożeniu sieci 5G spodziewać się możemy rewolucji w zakresie innowacyjnych usług końcowych.

Innym wymiarem konsekwencji wdrożenia sieci 5G jest kluczowy wymiar bezpieczeństwa narodowego krajów Starego Kontynentu, na który składa się z jednej strony potrzeba zapewnienia niezakłóconego działania podłączonych do sieci 5G obiektów, urządzeń i instalacji infrastruktury krytycznej, a z drugiej zabezpieczenie strategicznego i taktycznego zastosowania 5G na zaawansowanym technologicznie polu walki.

Wyzwaniem w najbliższych latach będzie zatem nadanie wysokiego tempa rozwoju digitalizacji bez uszczerbku na bezpieczeństwie i jakości legislacji. Jeśli UE chce konkurować ze światowymi mocarstwami, musi jak najszybciej zacząć korzystać z możliwości oferowanych przez rozwój cyfryzacji oraz sieci i technologii 5G . Wspólnota nie może jednak zapomnieć o kwestiach bezpieczeństwa – musi strzec danych swoich obywateli i zapewnić państwom członkowskim możliwość zadbania o swoje interesy narodowe w zakresie rozwoju gospodarczego i bezpieczeństwa. Bo problematyka sieci 5G to nie jest niszowa sprawa rozwoju usług cyfrowych w krajach członkowskich, tylko strategiczny kierunek cyfryzacji z wieloma kluczowymi implikacjami dla naszego bezpieczeństwa narodowego oraz kierunku rozwoju gospodarki z innowacyjnymi usługami i produktami.

## 2. Zagrożenia związane z wdrożeniem sieci 5G

**2.1.** Uzależnienie się od niewiarygodnego dostawcy technologii 5G. To może rzutować na zagrożenie szeroko rozumianej suwerenności poszczególnego państwa czy Unii Europejskiej – np. poprzez ryzyko utraty prywatności przez obywateli (problem zbierania wrażliwych danych w długim okresie czasu i potencjalnego wykorzystania ich w przyszłości niezgodnie z naszym interesem narodowym). Sami dostawcy technologii w zasadzie nie zbierają danych wrażliwych abonentów, jednak mogą mieć do nich dostęp przez działanie w obszarze wsparcia i utrzymania sieci (*operations, maintenance*). Uzyskują wtedy dostęp jako '*data procesor*' i to może generować zagrożenie.

**2.2.** Ryzyko monopolu: długoterminowe uzależnienie się od technologii danego dostawcy i rozwiązań kompatybilnych ze względu na bardzo wysoki koszt „wyjścia" z danej technologii.

**2.3.** Zagrożenie wynikające z obniżonego poziomu bezpieczeństwa w konsekwencji nie wdrażania przez operatorów kontroli bezpieczeństwa zalecanych przez normy (np. 3GPP) i stosowania najlepszych praktyk bezpieczeństwa. Dodatkowo dochodzą:

**2.3.1.** Ryzyko ekonomiczne - gdyby sieci 5G były niedostępne dla kluczowych przedsiębiorstw bądź wykorzystane do zbieranie danych o ich działaniu (szpiegostwo przemysłowe).

**2.3.2.** Ryzyko w obszarze porządku publicznego (gdyby zakłócone było działanie sieci 5G wspierającej usługi krytyczne: policję, służby, obsługę numeru 112 itp).

**2.3.3.** W przyszłości może dotyczyć także kontroli ruchu drogowego, kolejowego i autonomicznych pojazdów).

**2.4.** Zagrożenia dla bezpieczeństwa narodowego RP w stanie kryzysu (działania hybrydowe) i wojny:

**2.4.1.** Ingerencja w wewnętrzne sprawy RP poprzez:

- Ryzyko utraty poufności przesyłanych danych
- Ryzyko ingerencji w integralność przesyłanych danych
- Ryzyko czasowej i/lub permanentnej utraty usług cyfrowych.

**2.4.2.** Utrata zdolności do wykonywania operacji militarnych w środowisku tzw. smart city.

**2.4.3.** Utrata zdolności do interoperacyjności w ramach współdziałania z wojskami NATO.

## 3. Ryzyka nietechniczne związane z wdrożeniem sieci 5G

Istnieją pewne czynniki ryzyka, którym nie można zapobiec wyłącznie środkami technicznymi. Szkoda może być również spowodowana lub ułatwiona przez tzw. „złośliwych wtajemniczonych" (*malicious insiders*). Wtajemniczeni mogą być tymi, którzy mają dostęp do elementów sieci i jej funkcji kontrolnych lub mają głęboką wiedzę na temat technologii stosowanej w terenie oraz sposobu jej działania lub obu tych kwestii. Mogą to być pracownicy lub konsultanci operatorów sieci, najemcy i partnerzy operatora sieci, dostawcy technologii lub dostawcy usług zarządzanych lub podwykonawcy firm telekomunikacyjnych. „Złośliwy wtajemniczony" może być w stanie naruszać prywatność, manipulować i wprowadzać informacje i dane do sieci, wziąć częściową kontrolę nad siecią 5G.

## 4. Rekomendacje dotyczące budowy cyberbezpiecznej sieci 5G w Polsce

**4.1.** Wprowadzenie obowiązku prawnego i etycznego nałożonego na operatorów sieci telekomunikacyjnych, sprzedawców i dostawców usług opartych na 5G, którzy są świadomi zagrożeń związanych z cyberbezpieczeństwem, do podejmowania wszelkich odpowiednich kroków w celu zminimalizowania tego ryzyka, opierając się na standardowych funkcjach bezpieczeństwa i dostępnych rozwiązaniach dodatkowych.

**4.2.** Ciągła kontrola bezpieczeństwa i monitorowanie konfiguracji zabezpieczeń oraz polityki bezpieczeństwa podmiotów zaangażowanych w budowę, utrzymanie i

wsparcie sieci 5G. Jest to bowiem środowisko bardzo dynamicznie rozwijające się, gdzie konfiguracja może się zmieniać bardzo często.

**4.3.** Operatorzy powinni przeprowadzić ocenę ryzyka uzasadniającą przyjęte decyzje dotyczące bezpieczeństwa. Zgłaszanie takich decyzji może również stanowić część wymogów regulacyjnych. Dziś dostawcy są zobowiązani do wdrożenia obowiązkowych funkcji zabezpieczeń zdefiniowanych przez 3GPP (*3rd Generation Partnership Project*). Jednak z różnych powodów (np. ograniczenia budżetu operatora, różne przepisy w różnych krajach, ćwiczenia związane z akceptacją ryzyka) niektórzy operatorzy sieci nie używają lub nie konfigurują dostępnych funkcji bezpieczeństwa, osłabiając tym samym bezpieczeństwo sieci. Może to narazić sieć i jej użytkowników na niepotrzebne ryzyko.

**4.4.** Wprowadzenie oceny wiarygodności operatorów oraz dostawców sieci 5G i dostawców sprzętu dla sieci 5G – ocena możliwych zależności natury prawnej, organizacyjnej i finansowej.

**4.5.** Obowiązkowe przestrzeganie systemów gwarancji technicznych oceniających cykl życia bezpieczeństwa w danej organizacji. Preferowane są globalne lub co najmniej regionalne systemy certyfikacji. Pozwoli to promować innowacje i zmniejszyć koszty ogólne. GSMA NESAS to obiecujący program, który może stać się jednym z takich globalnych systemów certyfikacji wykorzystujących standardy 3GPP. Nie zaleca się tworzenia nowych systemów certyfikacji, które mogłyby okazać się bardzo kosztowne dla polskiego rynku.

**4.6.** Zalecamy rozważenie **oceny zabezpieczeń** (i potencjalnej certyfikacji), aby ustalić podstawę bezpieczeństwa cybernetycznego dla wszystkich graczy rynku 5G. Analiza obejmowałaby procesy projektowania, budowy, wdrażania i utrzymania produktów. Certyfikacja może być przeprowadzona przez licencjonowanych audytorów zewnętrznych.

**4.7.** **Ocena kluczowych komponentów w infrastrukturze sieci krytycznej.** Zaawansowana ocena oparta na produktach jest zalecana tylko dla elementów krytycznych, które mają większe narażenie na zagrożenie i poważny wpływ na infrastrukturę, gdy zostaną skutecznie zaatakowane. Istnieje kilka schematów oceny do wykonania tej funkcji (np. ISO 15408).

**4.8.** **Wybór zaufanych partnerów.** Ważna jest zdolność dostawcy do zapewnienia i utrzymania bezpiecznego sprzętu i godnego zaufania oprogramowania. Dostawcy powinni wykazywać przejrzystość praktyk bezpieczeństwa i usuwać wady w swoim własnym kodzie, a także w odpowiednich systemach stron trzecich w odpowiednim czasie. Ponadto wykrywanie i dzielenie się incydentami i lukami w zabezpieczeniach musi być zarządzane i obsługiwane między operatorami, rządem i dostawcami.

4.9. **Rozwój działalności badawczo-rozwojowej i innowacyjnej w obszarze 5G** – Rządowe badania zlecone dla państwowych instytutów badawczych, np. NASK, Instytut Łączności. Wybrani dostawcy technologii 5G powinni w Polsce rozwijać swoje R&D, współpracować z uczelniami/instytutami badawczymi oraz korzystać z polskich rozwiązań.

4.10. **Wsparcie dla start-upów** działających w kierunku budowania rozwiązań pomagających zwiększyć cyberbezpieczeństwo usług i rozwiązań opartych na technologii 5G, w ramach np. środków publicznych i inkubatorów przedsiębiorczości.

4.11. **Rozważenie powołania państwowego operatora** w oparciu o spółkę Skarbu Państwa, który odpowiedzialny będzie za stworzenie sieci dla potrzeb realizacji usług krytycznych.

## 5. 5G a zdrowie – fakty i mity

W Polsce i na świecie toczy się publiczna dyskusja na temat wpływu promieniowania fal elektromagnetycznych (PEM) na organizm człowieka. Co jakiś czas pojawiają się np. lokalne protesty mieszkańców przeciwko stawianiu masztów telefonii komórkowej w bliskiej odległości od budynków mieszkalnych. W debacie pojawia się również problem emisji fal z urządzeń elektronicznych, takich jak smartfony i laptopy czy urządzenia bezprzewodowe (sieć WiFi). Środowiska, które aktywnie nagłaśniają kwestię emisji promieniowania elektromagnetycznego domagają się m.in. ograniczenia rozwoju technologii generującej pole elektromagnetyczne (np. 5G). Pojawiają się również postulaty objęcia monitoringiem wszystkich stacji bazowych telefonii komórkowych i stworzenie w dłużej perspektywie mapy zagrożeń dla pacjentów na wzór map zagrożeń w przypadku smogu.

Biorąc pod uwagę rozbudowaną infrastrukturę telekomunikacyjną, planowane wdrożenie sieci 5G oraz ciągle rozwijającą się technologię i pojawianie się na rynku coraz to nowoczesnych urządzeń wykorzystujących łączność bezprzewodową **konieczne jest kontynuowanie i zintensyfikowanie działań w Polsce, które będą rozwiewały obawy związane z emisją pola elektromagnetycznego przez urządzenia elektroniczne.**

Obecnie w Polsce dopuszczalne poziomy pól elektromagnetycznych w środowisku są jednymi z najbardziej restrykcyjnych w Unii Europejskiej. To dokładnie 0,1 $W/m^2$ dla instalacji emitujących pola w częstotliwości od 300 Mhz do 300 GHz. Z kolei w 20 innych unijnych państwach obowiązuje norma wynosząca 10 $W/m^2$, która jest zgodna z zaleceniem Rady 1999/519/WE z dnia 12 lipca 1999 r. w sprawie ograniczenia narażania ludności na pola elektromagnetyczne. To oznacza, że w Polsce dopuszczalne poziomy emisji są stukrotnie niższe. Podobne poziomy obowiązują jeszcze jedynie w trzech krajach UE: we Włoszech, na Litwie i w Bułgarii.

Ponadto w polskim prawie funkcjonuje szereg przepisów, które służą zapewnieniu odpowiedniej ochrony zdrowia ludzkiego przed nadmierną emisją pól elektromagnetycznych. Są

to rozwiązania dotyczące m.in. obowiązków w zakresie pomiarów emisji PEM, monitoringu poziomów pól, kontroli właściwych organów i sankcji pieniężnych oraz karnych. Ogromną rolę odgrywają wojewódzkie inspektoraty ochrony środowiska, które prowadzą stałe monitoringi poziomów pól elektromagnetycznych w środowisku w 15 punktach pomiarowych w każdym województwie (zmienianych losowo co 3 lata). Co ważne, kontrola ta dotyczy globalnej emisji pól elektromagnetycznych ze wszystkich instalacji i urządzeń emitujących te pola, a nie tylko ze stacji bazowych telefonii komórkowej. Wiele doraźnych kontroli instalacji radiokomunikacyjnych wykonywanych przez WIOŚ odbywa się również na wniosek organizacji społecznych i lokalnych społeczności. Tak rozbudowany system pozwala sądzić, że Polska ma jeden z najlepiej zbudowanych mechanizmów ochrony przed nadmierną emisją pól elektromagnetycznych i kontroli tego poziomu. Warto podkreślić, że żadne dotychczasowe kontrole wykonane przez wojewódzkie inspektoraty ochrony środowiska nie wykazały przekroczenia dopuszczalnych poziomów PEM w Polsce. Potwierdziły to także inne badania prowadzone przez polskie instytucje rządowe oraz naukowców.

Mimo wielu badań przeprowadzonych zarówno na świecie, jak i w Polsce, do tej pory nie ma dowodów na negatywne skutki zdrowotne wynikające z narażenia na fale radiowe na poziomie lub poniżej zalecanych limitów. Światowa Organizacja Zdrowia twierdzi, że margines bezpieczeństwa uwzględnia wszystkich członków populacji, w tym osoby starsze, chore, ciężarne i dzieci. WHO już w 2006 roku przeanalizowała obawy społeczeństwa i wyraziła opinię, że szczegółowe badania nie wykazały żadnego zagrożenia związanego z polami radiowymi wytwarzanymi przez technologie bezprzewodowe. W swoich opracowaniach Organizacja jasno mówi, że jakakolwiek zachorowalność na nowotwory w pobliżu anten jest całkowicie przypadkowa.

Do tej pory najszerzej zakrojonymi badaniami nad możliwym związkiem między używaniem telefonu komórkowego a zagrożeniem rakiem mózgu był projekt INTERPHONE w 2000 r. To międzynarodowe badania kliniczno-kontrolne nowotworów w związku z użytkowaniem telefonu komórkowego zostało częściowo dofinansowany ze środków unijnych na kwotę 3,85 mln EUR z programu "Jakość życia i zarządzanie żywymi zasobami". W badaniu wzięło udział ponad 5000 osób chorych na raka z 13 krajów. W skład grupy kontrolnej weszło 7.000 osób zdrowych. Mimo ogromnej skali, badania nie przyniosły jednoznacznych wyników. W ramach projektu INTERPHONE nie doszukano się oznak podwyższonego ryzyka zachorowania na oponiaka wśród użytkowników telefonów komórkowych. Stwierdzono, że konieczne są dalsze badania.

Należy również zwrócić uwagę na badania przeprowadzone przez polskich naukowców z Uniwersytetu Jagiellońskiego: prof. Eugeniusza Rokitę i dra Grzegorza Tatonia[2]. Sprawdzili oni faktyczne efekty działania PEM na organizm człowieka i przeanalizowali dotychczasowe ba-

[2] Źródło: Aspekty medyczne i biofizyczne promieniowania

dania oraz opracowania naukowe na ten temat. Ich zdaniem jedynym potwierdzonym efektem oddziaływania pól elektromagnetycznych na człowieka jest tylko podniesienie temperatury układu biologicznego. Według nich, pomimo wielu zakrojonych na szeroką skalę badań epidemiologicznych, nie ma podstaw do tego, aby jednoznacznie powiązać PEM ze wzrostem zachorowalności na nowotwory mózgu, głowy i okolic szyi na skutek zwiększonej ekspozycji na pole elektromagnetyczne, np. z telefonów komórkowych.

Nie ma też dostatecznych dowodów potwierdzających związek pomiędzy ekspozycją na PEM a nadwrażliwością elektromagnetyczną. W licznych polskich i światowych badaniach nie stwierdzono częstszego występowania u użytkowników smartfonów symptomów zgłaszanych przez osoby, które same określają się jako „nadwrażliwe elektromagnetycznie". Większość autorów prac naukowych w tym aspekcie sugeruje, że w przypadku nadwrażliwości elektromagnetycznej przeważają raczej czynniki psychologiczne. Rozległe badanie epidemiologiczne związane z elektrowrażliwością przeprowadzono w 2015 r. w Holandii na 6 tysiącach uczestników. Okazało się, że nie istnieje istotna korelacja między pacjentami samookreślającymi się jako elektrowrażliwi a ekspozycją na PEM. Autorzy sugerują istnienie czynników psychologicznych w przypadku nadwrażliwości i twierdzą, że może tutaj działać efekt nocebo. Wydaje się, że nie istnieje związek przyczynowo skutkowy – co potwierdza przegląd literatury na ten temat – pomiędzy subiektywnie określanym samopoczuciem a ekspozycją na RF EMF, bez względu na to, czy badani uważają się za nadwrażliwych na RF EMF, czy też nie.

Ze względu na fakt, że mamy do czynienia ze stosunkowo nowym zjawiskiem i z nowymi technologiami, najlepszym rozwiązaniem jest zachowanie ostrożności i prewencja. Jedynie rzetelna edukacja, informacja i dialog z różnymi grupami społecznymi może zniwelować pojawiające się niepewność, niepokój i strach przed wykorzystywaniem urządzeń emitujących pole elektromagnetyczne i blokowaniem rozwoju współczesnych technologii. Najlepszym sposobem na redukcje narażenia społeczeństwa na ekspozycję fal elektromagnetycznych emitowanych z urządzeń elektronicznych jest edukacja obywateli – np. poprzez kampanię w mediach mówiącą o faktach i mitach dotyczących PEM i 5G. Warto, by edukacja była wsparta przez psychologa społecznego.

Józef Orzeł
Przewodniczący Rady
*/podpisano elektronicznie/*

Warszawa, wrzesień 2019 r.