DOI: 10.15199/59.2022.5.1

Co stymuluje rozwój współczesnej teleinformatyki i jakie są istotne kierunki tego rozwoju?

What stimulates the development of modern ICT and what are the main directions of this development?

Prof. dr hab. inż. Józef WOŹNIAK,
Politechnika Gdańska,
jowoz@eti.pg.edu.pl
Dr hab. inż. Jordi MONGAY BATALLA, prof. PW
Politechnika Warszawska,
jordi.mongay.batalla@pw.edu.pl
Dr hab. inż. Andrzej BĘBEN,
Politechnika Warszawska,
andrzej.beben@pw.edu.pl
Dr hab. inż. Marek NATKANIEC, prof. AGH
Akademia Górniczo-Hutnicza w Krakowie,
natkanie@agh.edu.pl
Dr hab. inż. Zbigniew PIOTROWSKI, prof. WAT
Wojskowa Akademia Techniczna,
zbigniew.piotrowski@wat.edu.pl
Dr hab. inż. Krzysztof SZCZYPIORSKI, prof. PW
Politechnika Warszawska,
krzysztof.szczypiorski@pw.edu.pl

STRESZCZENIE: Corocznie dokonuje się oceny stanu sztuki i tendencji w rozwoju światowej telekomunikacji i (tele)informatyki przywołując „mierzalne" i „niemierzalne" zmiany. W artykule przedstawiono charakter tych zmian oraz wskazano wyzwania badawcze i wdrożeniowe istotne dla rozwoju tych dyscyplin. Zaprezentowano i scharakteryzowano ewolucję infrastruktury sieciowej prowadzącą do sieci programowalnych SDN (*Software Defined Network*) oraz wykorzystania technik wirtualizacji funkcji sieciowych NFV (*Network Function Virtualisation*), prezentując też kierunki rozwoju nowych aplikacji i usług oferowanych z wykorzystaniem zasobów chmur obliczeniowych oraz technik przetwarzania danych na brzegu sieci (*Edge/Fog computing*). Szczególną uwagę poświęcono systemom i sieciom piątej generacji 5G, adresującym problemy różnych grup użytkowników i odpowiadającym na bardzo zróżnicowane wymagania jakościowe, energetyczne czy zasięgowe. Zaprezentowano też podstawowe obszary zastosowań Internetu Rzeczy oraz Wszechrzeczy IoT/IoE, prezentując w tym kontekście potrzeby i korzyści związane z użyciem technik uczenia maszynowego oraz sztucznej inteligencji do zapewniania efektywniejszego wykorzystania zasobów sieci IoT, czy też istotnego komponentu sieci 5G jakim jest Przemysł 4.0. Dokonano też krótkiej analizy zagrożeń oraz zasad wdrażania cyberbezpieczeństwa i zapewniania bezpieczeństwa informacji w systemach i sieciach teleinformatycznych.
SŁOWA KLUCZOWE: Technologie ICT, trendy w rozwoju, kierunki zmian, charakterystyka, separacja oprogramowania i sprzętu: VFN, SDN, sieci 5G, IoT/E, aplikacje chmurowe, obliczenia na brzegu sieci: Edge/Fog computing, cyberbezpieczeństwo: zagrożenia i metody przeciwdziałania

ABSTRACT: What stimulates the development of modern ICT and what are the main Abstract: The state of the art and trends in the development of global telecommunications and (tele) informatics, or simply ICT (Information and Communication Technology), are assessed annually, recalling „measurable" and „immeasurable" changes. The paper presents the nature of such changes and indicates research and implementation challenges, significant for the development of ICT in the coming years. The evolution of network infrastructure leading to programmable – SDN (Software Defined Network) networks and the use of network function virtualization techniques NFV (Network Function Virtualization) were presented and characterized, and the directions of development of new applications and services offered with the use of cloud computing resources and data processing techniques at the edge of the network were presented. (Edge (MEC Multi-access Edge Computing)/Fog computing). Particular attention was paid to the fifth generation – 5G systems and networks, addressing the problems of various user groups and responding to very diverse quality, energy and range requirements. The basic areas of the Internet of Things (Everything) (IoT/ IoE) applications were also presented together with the needs and benefits related to the use of machine learning techniques and artificial intelligence to ensure more effective use of IoT network resources, also in order to support very important component of the 5G network, i.e. Industry 4.0. There was also a short analysis of threats and rules for implementing cybersecurity and ensuring information security in ICT systems and networks.
KEYWORDS: ICT, development trends, directions of changes, characteristics, separation of software and hardware: VFN, SDN, 5G networks, IoT / E, cloud applications, computing at the edge of the network: Edge / Fog computing, cybersecurity: threats and methods of counteracting

Zmiany obserwowane w technologiach informacyjno-komunikacyjnych (ICT – *Information and Communication Technology*) określamy zwykle mianem ewolucyjnych, chociaż przyspieszenie tych zmian w ostatnich dziesięcioleciach jest ogromne. Łamiemy i przekraczamy kolejne bariery. Więcej, szybciej, lepiej, efektywniej, oszczędniej, to naturalne oczekiwania ludzi, nie zapominając oczywiście o niezawodności oraz bezpieczeństwie i poufności w przekazie i przechowywaniu danych. Coraz powszechniejsze staje się podejście do bezpieczeństwa jako istotnej usługi.

Corocznie dokonuje się oceny stanu sztuki i tendencji w rozwoju światowej telekomunikacji i (tele)informatyki. Należy tutaj mocno zaakcentować, że oba te obszary (telekomunikacja i informatyka) – znaczące

dla rozwoju wszystkich dziedzin życia i dyscyplin naukowych (nie tylko dla powołanej stosunkowo niedawno dyscypliny: Informatyka techniczna i telekomunikacja), wzajemnie się przenikające – cechuje ogromna dynamika i obejmowanie swym zasięgiem coraz to nowych sfer ludzkiej aktywności.

Dokonując takiej oceny z perspektywy aktualnych prac i dokonań, można wymienić co najmniej kilka wyzwań badawczych i wdrożeniowych istotnych czy wręcz kluczowych dla rozwoju telekomunikacji i teleinformatyki w najbliższych latach.

W artykule wskażemy na charakter „mierzalnych" i „niemierzalnych" zmian obserwowanych w sieciach teleinformatycznych, w tym:

- rosnącą wielkość generowanego ruchu oraz zmieniające się charakterystyki tego ruchu (przekazy strumieniowe), pociągające za sobą nowe wymagania na pasmo,
- rosnącą liczbę urządzeń sieciowych o bardzo zróżnicowanych wymaganiach,
- wielofunkcyjność tych urządzenia (dwa lub więcej interfejsy sieciowe),
- heterogeniczność środowiska sieciowego,

aby na tej podstawie postawić „diagnozę" i sformułować wybrane sposoby rozwiązania problemów, z którymi muszą sie mierzyć projektanci sieci, w tym:

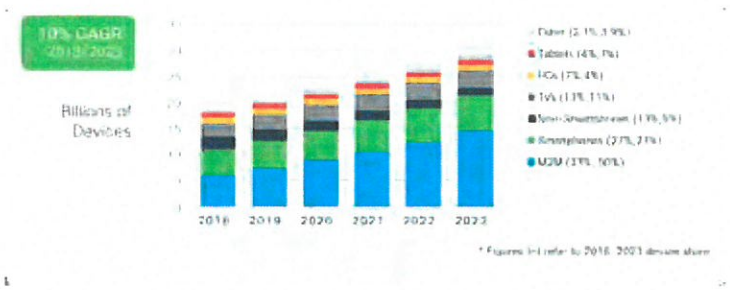
- nowe architektury sieciowe,
- zmieniające się zasady zarządzania zasobami sieci,
- istotne wyzwania dotyczące zabezpieczania informacji i walki z „cyberprzestępstwem".

JAKIE SĄ PODSTAWOWE OBSERWACJE I WNIOSKI ZWIĄZANE Z RUCHEM W SIECIACH?

By odpowiedzieć na to pytanie przyjrzyjmy się podstawowym charakterystykom ruchu IP. W tym celu dokonamy analizy wybranych wskaźników sygnalizowanych w *Raporcie Cisco,* opublikowanym w 2020 roku [1]. Z lektury tego Raportu wynika, że do 2023 roku prawie dwie trzecie światowej populacji będzie miało dostęp do Internetu, co oznacza, że liczba użytkowników Internetu sięgnie 5,3 miliarda, w porównaniu z 3,9 miliarda (51% światowej populacji) w 2018 roku.

Z kolei, do 2023 roku liczba urządzeń podłączonych do sieci IP będzie znacznie ponad trzykrotnie większa od światowej populacji, co oznacza 29,3 miliarda urządzeń sieciowych podłączonych do Internetu, w porównaniu z 18,4 mld w 2018 roku (*rys. 1*). Tym samym na mieszkańca przypadać będzie 3,6 urządzeń sieciowych, w porównaniu z 2,4 urządzeniami sieciowymi w 2018 r.

Szczególnie istotna zmiana dotyczy połączeń M2M (*Machine-to-Machine*), które będą stanowić połowę globalnej liczby połączeń i podłączonych urządzeń. Udział połączeń maszyna-maszyna (M2M) wzrośnie z 33 procent w 2018 roku do 50 procent w 2023 r. Do 2023 roku będzie zatem 14,7 miliarda podłączonych układów typu M2M.



» *Rys. 1. Szacowane zmiany liczby urządzeń generujących ruch IP (Źródło: [1])*

» *Rys.2. Zależność pomiędzy jakością przekazu TV 4K, a wymaganiami pasma (szybkość transmisji). Zmiany liczby urządzeń TV standardu 4K (Źródło: [1])*

Jednocześnie bardzo ważny segment konsumencki będzie miał prawie trzy czwarte udziału w łącznej liczbie urządzeń i połączeń do 2023 roku W skali globalnej udział tego segmentu w łącznej liczbie urządzeń i połączeń wyniesie 74 procent. Pozostałe 26 procent przypadnie na segment biznesowy.

W kategorii połączeń M2M, określanej również jako IoT (Internet of Things) największy udział będą miały aplikacje domowe. Wśród nich aplikacja związana z podłączeniem samochodu będzie się rozwijała najszybciej. Do 2023 roku aplikacje określane jako domowe będą miały prawie połowę udziału w M2M, przy czym aplikacje wykorzystywane w samochodach będą rosły najszybciej, z przyrostem 30% CAGR (*Compound Annual Growth Rate*) w okresie prognozy (2018–2023).

Równie ciekawe są obserwacje dotyczące zmieniającego się zestawu urządzeń i rodzajów połączeń oraz wymagań szeregu urządzeń, co wpływać będzie istotnie na wzorce ruchu. W szczególności przewiduje się, że urządzenia wideo mogą mieć „iloczynowy" wpływ na wzrost ruchu. Telewizor HD, który pobiera treści z Internetu przez dwie – trzy godziny dziennie, będzie generował średnio tyle ruchu internetowego, ile obecnie całe gospodarstwo domowe. Wpływ urządzeń wideo na wielkość ruchu bardzie szczególnie duży w przypadku strumieniowego przesyłania wideo w standardzie *Ultra-High-Definition* (UHD) i 4K. TV o takich parametrach wymagać będą przesyłu z szybkością 15 do 18 Mb/s, czyli ponad dwukrotnie większą niż szybkość transmisji wideo HD i dziewięciokrotnie większą niż szybkość transmisji wideo w standardowej rozdzielczości (SD). Szacuje się, że do 2023 r. dwie trzecie (66 proc.) zainstalowanych płaskich telewizorów będzie pracowało w trybie UHD, w porównaniu z 33 proc. w 2018 r. (*rys. 2*).

Wymagania na pasmo „zgłaszane" przez UHD TV są jednakże tylko ułamkiem procenta w stosunku do zapotrzebowania związanego z urządzeniami UHD VR (*Virtual Reality*), co dobrze ilustruje *rys. 3*.

Charakterystycznym elementem prognoz Cisco jest fakt, że ponad 70 procent światowej populacji będzie miało do roku 2023 łączność mobilną. Całkowita liczba abonentów telefonii komórkowej na świecie wzrośnie z 5,1 miliarda (66% populacji) w 2018 roku do 5,7 miliarda (71% populacji) do 2023 roku.

W tej grupie urządzenia i połączenia 5G będą stanowić, do roku 2023, ponad 10% globalnych urządzeń i połączeń mobilnych, a globalna liczba urządzeń mobilnych wzrośnie z 8,8 miliarda w 2018 roku do 13,1 miliarda w 2023 roku. z czego 1,4 miliarda będzie obsługiwać 5G.

Najdynamiczniej rozwijającą się kategorią urządzeń mobilnych będą te typu M2M, a następnie smartfony. Przewiduje się, że w latach 2018-2023 w kategorii mobilnych urządzeń M2M odnotowywany będzie wzrost 30% (CAGR). W tym samym okresie udział smartfonów będą rósł w tempie 7-procentowym.

Wszystkie te prognozowane zmiany wymagać będą istotnego wzrostu globalnej wydajność sieci, w tym w szczególności przyspieszania szybkości pracy sieci i poszczególnych urządzeń.

Wszystkie te prognozowane zmiany wymagać będą istotnego wzrostu globalnej wydajność sieci, w tym w szczególności przyspieszania szybkości pracy sieci i poszczególnych urządzeń.

Szybkości pracy stałych łączy szerokopasmowych wzrosną w prognozowanych okresie (do 2023 roku) ponad dwukrotnie. Do 2023 roku globalne szybkości stałych łączy szerokopasmowych osiągną 110,4 Mb/s, w porównaniu z 45,9 Mb/s w 2018 roku. W tym samym okresie szybkości pracy urządzeń mobilnych (telefonów komórkowych) wzrosną ponad trzykrotnie, a średnia szybkość połączenia w sieci komórkowej, która w 2018 roku wyniosła 13,2 Mb/s, wzrośnie w 2023 roku do 43,9 Mb/s.

Szybkości rozwijanych i wdrażanych obecnie systemów 5G będą do 2023 roku 13 razy wyższe niż wspomniane powyżej średnie szybkości w sieci komórkowej, osiągając w 2023 roku 575 Mb/s.

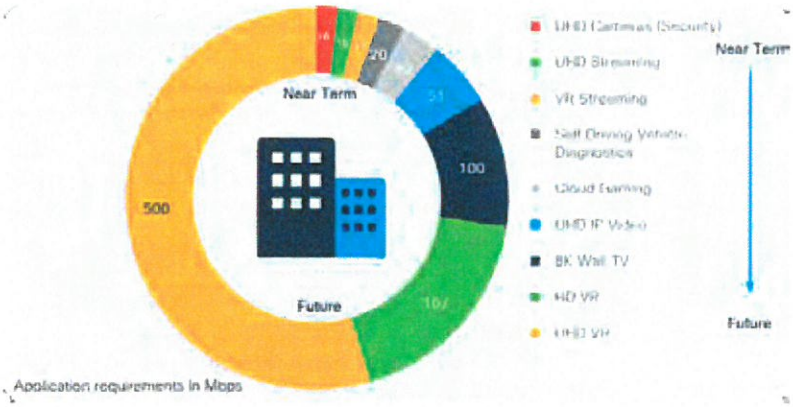
Radykalne zmiany są też przewidywane w segmencie sieci WLAN. Szybkości pracy sieci Wi-Fi z urządzeń mobilnych potroją się do 2023 roku. Na całym świecie średnia szybkość Wi-Fi wzrośnie z 30,3 Mb/s w 2018 roku do 92 Mb/s w roku 2023.

W okresie 2018-2023 liczba hotspotów Wi-Fi wzrośnie czterokrotnie osiągając na całym świecie, do roku 2023, prawie 628 milionów instalacji publicznych hotspotów Wi-Fi, w porównaniu z 169 milionami hotspotów w 2018 roku. W segmencie sieci bezprzewodowych standardu IEEE 802.11 wdrażane są już aktualnie rozwiązania 6 generacji (oraz powstają zarysy WiFi7). Liczba hotspotów Wi-Fi6 wzrośnie od 2020 do 2023 roku 13-krotnie i do 2023 roku będzie stanowić 11% wszystkich publicznych hotspotów Wi-Fi.

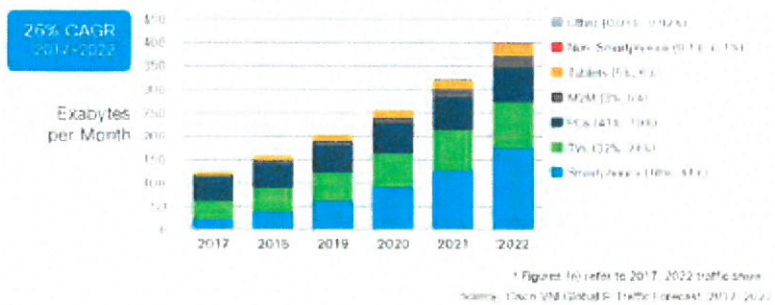
Do 2023 r. na świecie zostanie pobranych prawie 300 mln aplikacji mobilnych. Najpopularniejszymi aplikacjami do pobrania będą przy tym aplikacje związane z mediami społecznościowymi oraz gry i aplikacje biznesowe.

Zmiany związane z liczbą urządzeń i wolumenem generowanego ruchu pociągają za sobą nieuchronnie coraz większe problemy z zapewnieniem poufności i integralności danych wysłanych przez sieć. Liczba naruszeń i całkowita liczba rekordów narażonych przez każde naruszenie wciąż rośnie. Na całym świecie odnotowano 776% wzrost liczby ataków między 100 Gb/s a 400 Gb/s rok do roku od 2018 do 2019 roku, a całkowita liczba ataków DDoS zapewne podwoi się z 7,9 mln w 2018 r. do 15,4 mln do 2023 roku.

Porównując przytaczane powyżej zmiany do innych zjawisk (często katastroficznych) obserwowanych w przyrodzie możemy jednoznacznie powiedzieć: jest to niewątpliwie Data Tsunami... (*rys. 4*).



» ***Rys. 3. Wymagania na pasmo w przypadku wybranych urządzeń, w zależności od jakości przekazów (Źródło: [1])***



» ***Rys. 4. Globalny ruch IP z podziałem na urządzenia (Źródło: [2]).***

CO ZATEM POWINNO SIĘ ROBIĆ?

Konieczne staje się ciągłe dostosowywanie sieci do zmieniających się potrzeb (większe szybkości, mniejsze opóźnienia, wyższa niezawodność, nowe usługi, nowe scenariusze pracy, obniżanie kosztów eksploatacji, poprawa elastyczności pracy, itp.) Bez wątpienia możemy przy tym wskazać szereg zmian zachodzących w architekturze i zasadach funkcjonowania systemów i sieci telekomunikacyjnych - teleinformatycznych.

Szczególnie obserwujemy wyraźną tendencję, podobnie jak w klasycznej informatyce, oddzielania oprogramowania od sprzętu. Podstawą dla takich rozwiązań stają się platformy wirtualizacyjne i powiązane z nimi techniki wirtualizacji, konteneryzacji oraz technologie chmurowe. Bazując na takim rozdziale oprogramowania i sprzętu, sieci zyskują zarówno na elastyczności (zmiany są dokonywane wyłącznie w oprogramowaniu) jak i efektywności ekonomicznej, dzięki zmniejszaniu kosztów (infrastruktura sprzętowa staje się zasobem o dłuższej skali czasowej). Jednocześnie ogromną wagę przykłada się do energooszczędności i ograniczania emisji CO_2.

Realizowane na świecie prace badawczo-wdrożeniowe są odpowiedzią na zidentyfikowane powyżej trendy oraz potrzeby użytkowników sieci teleinformatycznych, którymi w szczególności są unowocześnienia oraz propozycje nowych technologii i architektur sieciowych jak również rozwiązania dedykowane pozwalające efektywnie:

- obsłużyć rosnącą liczbę użytkowników i urządzeń sieciowych,
- obsłużyć rosnący ruch sieciowy,
- zapewnić ciągłość pracy sieci,
- zapewnić poufność i integralność danych oraz
- zapewnić dostępność zasobów sieciowych.

W dzisiejszym, coraz bardziej cyfrowym świecie obserwujemy dynamiczny rozwój systemów dostępowych do usługowej infrastruktury telekomunikacyjnej i teleinformatycznej. Rośnie, jak nigdy wcześniej, zagęszczenie urządzeń mobilnych. Z tym faktem związane są nowe generacje systemów RAN (*Radio Access Networks*). Pomimo coraz większych oferowanych przez nie szybkości pracy ich wyraźnym mankamentem są ograniczenia wynikające z dostępnego widma częstotliwościowego.

W kontekście rosnącego wolumenu ruchu szerokopasmowy dostęp światłowodowy staje się ważniejszy niż kiedykolwiek. Światłowody, zarówno w instalacjach dostępowych, jak i w szczególności w instalacjach szkieletowych zapewniają szybką łączność, tak bardzo pożądaną w dobie pandemii i koniecznego przejścia na pracę w domu, zdalną naukę i utrzymywania kontaktu z bliskimi.

Jednocześnie, właśnie teraz, gdy wychodzimy z tego okresu, zapotrzebowanie na zwiększone szybkości i pojemności wciąż rośnie, napędzane przez nowe coraz bardziej zasobochłonne aplikacje konsumenckie, a także przez nowe funkcje i architektury sieciowe, takie jak przetwarzanie w chmurze, czy też przetwarzanie realizowane na brzegu sieci.

Wraz z nadejściem chmury obliczeniowej zmianie uległo wiele paradygmatów usługowo-biznesowych ekosystemu ICT, by zapewniając wysoką jakość i dostępność usług wyeliminować mankamenty w kosztownym procesie utrzymania infrastruktury IT.

Poprawa wydajności pracy, w szczególności zwiększenie szybkości przetwarzania realizowanego w serwerach, routerach czy przełącznikach sieciowych zmieniło podejście projektantów do metod zarządzania siecią oraz świadczenia specjalizowanych usług. Do niedawna programowe rozwiązania tych urządzeń nie mogły konkurować w wydajności i funkcjonalności z ich specjalizowanymi, dedykowanymi i fizycznymi odpowiednikami. Poprawa parametrów takich urządzeń zainicjowała trend rozdziału oprogramowania od elementów sprzętowych. Tym samym możliwe stało się oferowanie specjalizowanych mikrousług w sposób programowy oraz ich separacja (uniezależnienie) od wykorzystywanego sprzętu. Dzięki temu zarządzanie siecią mogło być dużo bardziej elastyczne, a podstawą tej elastyczności stała się wspomniana atomizacja „software'u", tj. wytwarzanie programów implementujących konkretne, ale zwykle niewielkie funkcjonalności (*Network Functions*) wykorzystywane do zarządzania. Idąc o krok dalej i zakładając, że funkcje te współdzielą logicznie zasoby fizyczne urządzeń (procedury wirtualizacji) otrzymujemy koncepcję wirtualizacji funkcji sieciowych (NFV – *Network Function Virtualization*).

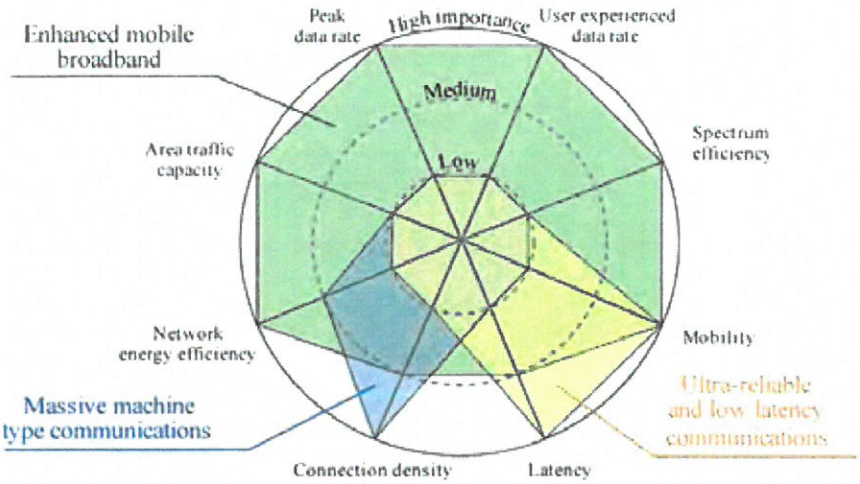
Wspomniana powyżej separacja elementów programowych i sprzętowych stała się podstawa do przyjęcia przez operatorów sieci telekomunikacyjnych nowych koncepcji: sieci definiowanej programowo (SDN) i wspomnianej powyżej wirtualizacji funkcji sieciowych (NFV).

NFV wprowadza i wdraża nowe funkcje sieciowe w otwartym i ustandaryzowanym środowisku ICT, podczas gdy SDN ma na celu zmianę sposobu funkcjonowania sieci. SDN i NFV to technologie uzupełniające się; nie są wprost od siebie zależne. Obie koncepcje można jednakże połączyć, w celu zapewnienia korzyści płynących z użycia z SDN w wielu środowiskach, takich jak centra danych, sieci centrów danych, czy też rozwiązaniu *Network as a Service* (NaaS) [3].

Zaawansowane technologie, takie jak Przemysłowy Internet Rzeczy (IIoT), prywatne przedsiębiorstwo 5G i Wi-Fi6E, wymagają zmodernizowanej infrastruktury sieciowej, aby zapewnić wyjątkową obsługę. Adaptacyjna sieć wykorzystuje zbiór funkcji zdefiniowanych programowo, aby zapewnić wysoką wydajność, elastyczność i bezpieczną łączność z przedsiębiorstwami i kompleksami przemysłowymi. Aby usprawnić procesy i poprawić wydajność, firmy inwestują w zewnętrznych, niezależnych dostawców usług. Dostawcy usług zarządzanych mają wyjątkową pozycję, aby jak najlepiej doradzać i wdrażać zaawansowane rozwiązania dla przedsiębiorstw w różnych specjalizacjach, zapewniając optymalizację i prostotę na poziomie korporacyjnym.

Sieci definiowane programowo oraz wirtualizacja funkcji sieciowych są głównymi składnikami nowych generacji sieci korzystających w głównej mierze z oprogramowania. Te nowe techniki pozwalają na jeszcze większą elastyczność poprzez oddzielenie płaszczyzn sterowania i danych oraz przekształcenie złożonego zarządzania siecią

» *Rys. 5. Podstawowe parametry, wymagania i scenariusze użycia 5G (Źródło ITU)*



Bezpieczeństwo danych i systemów informatycznych urasta z poziomu „rozwiązania wymuszanego" do wręcz fundamentalnego wymagania we wszystkich nowych technologiach.

w znacznie prostszy łańcuch usług lub mikrousług, który może stać się mniej lub bardziej autonomiczny.

Efektem takich działań są sieci bazujące na oddzielnych, dedykowanych fragmentach oprogramowania, które można wdrożyć w całości w chmurze, a gdy potrzebne są niewielkie opóźnienia, to także na brzegu sieci, w pobliżu użytkowników, a nawet we mgle (w postaci rozproszonej), wykorzystując niektóre zasoby użytkowników końcowych. Mgła stwarza wiele wyzwań dla bezpieczeństwa, w szczególności ochrony poufności i integralności danych, ale zwiększa dostępność „usługową" systemu.

Bezpieczeństwo danych i systemów informatycznych urasta z poziomu „rozwiązania wymuszanego", w przypadku starych rozwiązań, do wręcz fundamentalnego wymagania we wszystkich nowych technologiach.

5G jest dobrym przykładem kierunku, w którym zmierzamy, polegającego na rozdzieleniu sprzętu i oprogramowania oraz integracji różnych sieci (przewodowych i bezprzewodowych) w ramach jednego wspólnego zarządzania. Sieć staje się wtedy bezpieczną platformą łączności, przeźroczystą dla aplikacji, dzięki czemu aplikacje mogą szybko ewoluować , czego przykładem jest szeroki zakres scenariuszy IoT/IoE.

W pracy (oraz prawdopodobnie kolejnych pracach cyklu) prezentujemy wybrane wnioski oraz zidentyfikowane przez autorów istotne obszary badawczo-wdrożeniowe w sieciach, stanowiące odpowiedź na zdefiniowane powyżej potrzeby użytkowników [4].

Przedmiotem naszych rozważań będą szczególnie:

1. *Systemy i sieci cyfrowe piątej generacji – 5G* – adresujące problemy różnych grup użytkowników i odpowiadające na bardzo zróżnicowane wymagania jakościowe, energetyczne czy zasięgowe.
2. *Problematyka Internetu Rzeczy oraz Wszechrzeczy* – IoT – IoE – łącząca komunikację M2M oraz P2M z wszystkimi możliwymi wariantami i nowymi obszarami aplikacji (inteligentne miasta i domy, inteligentne fabryki, zdrowie...).
3. Ewolucja infrastruktury sieciowej w kierunku sieci programowalnych SDN (*Software Defined Network*) oraz wykorzystania technik wirtualizacji NFV (*Network Function Virtualisation*).
4. *Rozwój nowych aplikacji i usług* oferowanych z wykorzystaniem zasobów chmur obliczeniowych oraz technik przetwarzania danych na brzegu sieci (*Edge/Fog computing*).
5. *Cyberbezpieczeństwo oraz bezpieczeństwo informacji:* Newralgiczne dla funkcjonowania wszystkich systemów (globalnych i lokalnych) są zagadnienia bezpieczeństwa i poufności przekazu, jak również przetwarzania i przechowywania danych, w tym usługowego spojrzenia na bezpieczeństwo (SaaS).

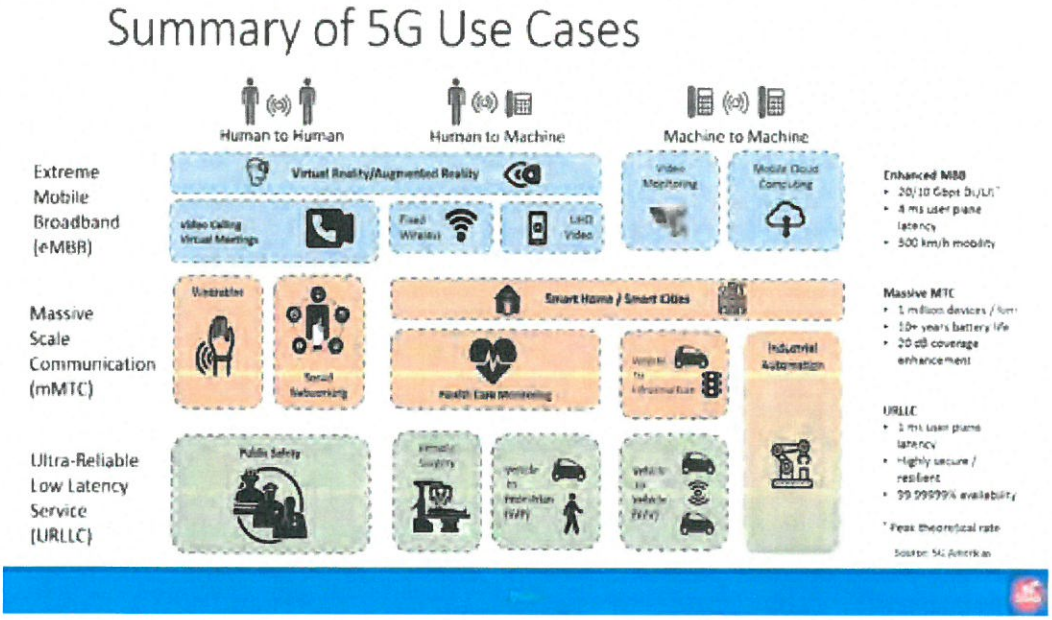
OGÓLNA CHARAKTERYSTYKA 5G

Implementacja oraz postępująca komercjalizacja sieci 5G jest jednym z gorących tematów z obszaru sieci i usług teleinformatycznych. Komunikacja 5G zaczyna być traktowana jako klucz do sukcesu we wzbogacaniu zarówno oferty konsumenckiej jak też, a może przede wszystkim, do cyfrowej transformacji przemysłowej. Gospodarki światowe oczekują, że 5G stanie się istotną częścią i katalizatorem długoterminowego rozwoju przemysłowego. Bez wątpienia technologia 5G, ze swoimi szeroko zorientowanymi scenariuszami znajdzie zastosowanie nie tylko na rynku konsumenckim, ale i w tysiącach rozwiązań branżowych.

Wszystkie nowe usługi i aplikacje 5G ukierunkowane są na ich implementację i wykorzystanie w trzech podstawowych scenariuszach użycia, definiowanych przez ITU (*rys. 5*), pozwalających na praktyczne wykorzystanie 5G we wręcz nieograniczonej liczbie przypadków (*rys. 6*, [5]):

a) *Enhanced Mobile Broadband* (eMBB) – systemy te znajdą zastosowanie np. w przekazach treści multimedialnych o wysokich wymaganiach jakościowych (wideo 4K/8K, wideo na 360°). Transmisje eMBB cechować będzie bardzo wysoka przepływność, duża efektywność widmowa w systemach o szerokim pokryciu terenu i dużej gęstości terminali.

b) *Massive Machine Type Communications* (mMTC) – ten typ systemów dedykowany będzie masowej transmisji od/do wielu tanich urządzeń o zasilaniu bateryjnym o wieloletniej trwałości, mającej na celu przekazywanie w postaci krótkich komunikatów danych pomiarowych, np. z liczników energii czy czujników, w tym umieszczanych np. na ciele człowieka.



» Rys. 6. Graficzna reprezentacja podstawowych trzech klas (scenariuszy) zastosowania systemów 5G wraz z przykładowymi aplikacjami i podstawowymi wymaganiami (Źródło:[5])

c) *Ultra Reliable Low Latency Communications* (URLLC) – rozwiązania te będą oferowały realizację aplikacji wymagających bardzo małych opóźnień oraz wysoką niezawodność, zapewniając quasi-ciągłą dostępność. Dotyczyć to będzie komunikacji o znaczeniu krytycznym, jak np.: operacje chirurgiczne wykonywane na odległość, sterowanie pojazdami autonomicznymi (komunikacja między pojazdami oraz pojazdami i infrastrukturą), systemy sterowania przemysłowego (komunikacja między robotami), Internet dotykowy, czy też liczne zastosowania na rzecz bezpieczeństwa publicznego.

Zaprezentowane scenariusze pozwolą na udostępnianie aplikacji i usług szerokiej gamie klientów, zwłaszcza klientów biznesowych. Zróżnicowane scenariusze i związane z nimi specyficzne aplikacje i usługi nakładają na sieć 5G wiele wymagań, co z kolei pociąga za sobą konieczność implementacji nowych technologii i mechanizmów na różnych poziomach.

Typowe wymagania dla sieci 5G (nawet jeśli nie są wyjątkowe – w porównaniu z 4G), to w szczególności [4]:

a. 1000-krotny wzrost wartości wolumenu danych (≥ 10 Tb/s/km^2),

b. 100-krotny wzrost wartości maksymalnej szybkości transmisji (≥ 10 Gb/s),

c. 1000-krotny wzrost liczby dołączonych urządzeń (≥ 1 M urządzeń/km^2),

d. 10-krotny (1/10) spadek konsumpcji energii przez urządzenie, w porównaniu do roku 2010,

e. 5-krotne (1/5) skrócenie dotychczasowej wartości opóźnienia (≤ 1 ms dla niektórych aplikacji),

f. 5-krotny spadek (1/5) kosztów operacyjnych sieci – OPEX,

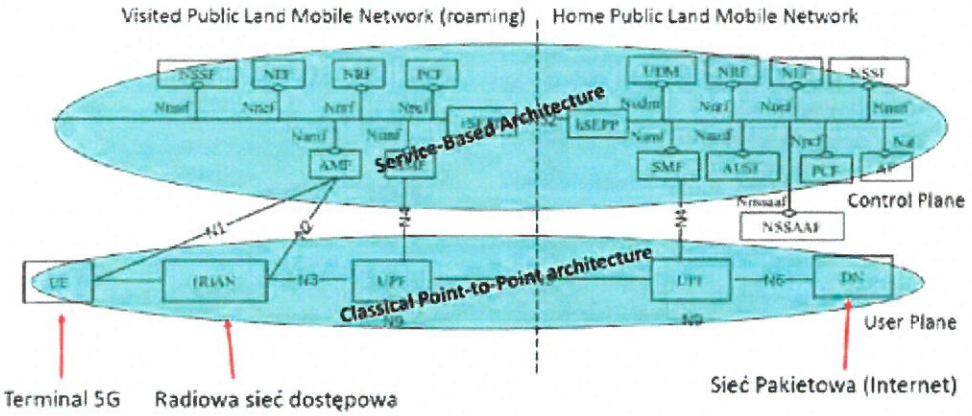
g. 1000-krotne skrócenie (1/1000) dotychczasowego czasu wdrażania usługi (≤ 90 minut).

Wymagania te będą mogły być spełnione tylko wtedy, gdy sieć wprowadzi wiele nowych mechanizmów, z których nie wszystkie są ściśle związane z telekomunikacją (np. nowe rozwiązania pochodzące od dostawców energii, które zdecydowanie zmniejszą zużycie energii).

Wśród charakterystycznych dla 5G zasad funkcjonowania najistotniejsze to:

- Zasada wirtualizacji sieci na podstawie oprogramowania;
- Zastosowanie rozwiązań chmurowych dla sieci rdzeniowej (*Core Network*) ale i stacji bazowych (separacja *Distributed Unit* i *Centralized Unit* – CU w chmurze lokalnej w pobliżu sieci radiowej);
- Zastosowanie segmentacji sieci (*Network Slicing*) ze względu na bardzo zróżnicowane parametry poszczególnych grup usług;
- Uproszczenie komunikacji wewnątrz sieci rdzeniowej dzięki *Service Based Architecture* (SBA), co gwarantuje elastyczność i możliwość szybkiego rozwinięcia sieci;
- Zastosowanie elastycznych parametrów warstwy fizycznej (transmisja wielotonowa OFDM) z możliwością dopasowania zasobów radiowych do poszczególnych grup usług.

W przypadku 5G paradygmat projektowania sieci rdzeniowej przesuwa się w kierunku charakterystycznym dla architektury opartej na usługach (SBA – *Service Based Architecture*), powszechnie stosowanej w np. rozwiązaniach chmurowych. Zgodnie z tą koncepcją, funkcje płaszczyzny sterowania sieci (*Control Plane Functions*) współdziałają ze sobą za pośrednictwem wspólnej magistrali komunikacyjnej, określanej jako zorientowany usługowo interfejs (*Service Based Interface* – SBI). Dzięki temu, dwie Funkcje Sieciowe, które chcą się wzajemnie komunikować nie muszą definiować interfejsu punkt-punkt, co sprawia, że każda Funkcja Sieciowa może komunikować się z dowolną inną poprzez opublikowanie usług oferowanych przez tę Funkcję. Umożliwia to w szczególności łatwy rozwój sieci i nowych modułów Funkcji Sieciowych. Sieć jest dużo bardziej skalowalna i elastyczna (Funkcje Sieciowe mogą być dedykowane dla pewnej grupy użytkowników, jak to ma miejsce w przypadku Network Slicing („plastereki" – sieci wydzielone logicznie, dedykowane dla pewnych użytkowników).



» *Rys.7. Referencyjna architektura sieci 5G (Źródło: 3GPP) Opis: Access and Mobility Management Function AMF; Session Management Function SMF; Policy Control Function PCF; User Plane Function UPF; Unified Data Managemnet Function UDM; Unified Data Repository UDR; Authentication Server Function AUSF; Network Exposure Function NEF; Security Edge Protection Proxy SEPP; Network Slice Selection Function NSSF; Network Repository Function NRF; Application Function AF.*

Należy też zwrócić uwagę na fakt, że rozwiązanie 5G jest otwarte na obsługę użytkowników dołączanych do 5GC (*5G Core*) zarówno poprzez sieci dostępowe RAN (*Radio Access Networks*) standaryzowane przez 3GGP, jak i sieci inne, takie jak np. bardzo popularne sieci przewodowe Ethernet, czy bezprzewodowe Wi-Fi, traktowane jako zaufane (*trusted*) lub niezaufane (*untrusted*) - w zależności od relacji biznesowej między operatorem mobilnym i operatorem danej sieci dostępowej. Przykładową architekturę szkieletowej sieci 5G ilustruje *rys. 7.*

IoT/IoE

Internet rzeczy (IoT) to duża szansa biznesowa dla operatorów telefonii komórkowej. Właśnie dlatego sieć 5G została zaprojektowana od podstaw, aby obsługiwać wymagające przypadki użycia i wymagania IoT — w tym te, z którymi obsługa za pośrednictwem 4G i Wi-Fi jest trudna.

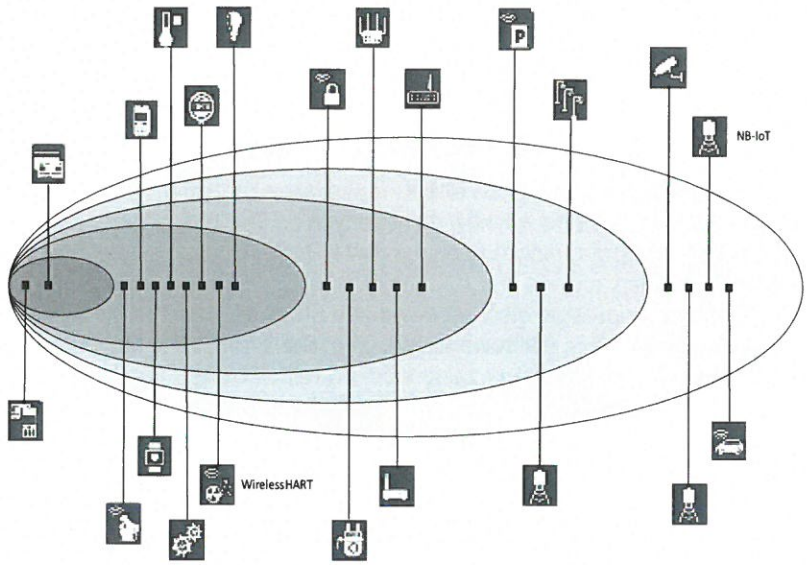
5G ma do zaoferowania trzy zestawy funkcji, które są idealne do zastosowań w koncepcjach Przemysłu 4.0. Należą do nich, w szczególności scenariusze: *Ultra-Reliable Low-Latency Communications* (URLLC), z zestawem funkcjonalności, który oferuje zmniejszenie opóźnienia do zaledwie jednej milisekundy, kluczowym dla zastosowań o znaczeniu krytycznym, takich jak sieci wrażliwe na czas (*Time Sensitive Networks* — TSN) oraz *Massive Machine-Type Communications* (mMTC), umożliwiający sieciom 5G obsługę do miliona urządzeń IoT na kilometr kwadratowy, takich jak autonomiczne przenośniki materiałów, roboty przemysłowe i czujniki. Ostatnim zestawem funkcji jest ulepszona mobilna łączność szerokopasmowa (eMBB), która obsługuje aplikacje wymagające dużej przepustowości, takie jak kamery wideo 4K na terenie zakładu i wokół niego, w celu monitorowania produkcji, zapewniania bezpieczeństwa pracowników i ochrony fizycznej.

Nawet przy tych i innych zaawansowanych możliwościach operatorzy komórkowi będą potrzebować dodatkowych narzędzi, aby zapewnić, że ich sieci 5G będą mogły w pełni wykorzystać możliwości IoT. Tak jest również w przypadku operatorów prywatnych sieci 5G, które, według ankiety *Analysys Mason*, planuje wdrożyć do 2024 roku 76 proc. producentów [6, 7].

Według raportu *IoT Use Case Adoption* z 2021 r. liczba przypadków użycia Internetu rzeczy stale rośnie [8]. *Raport* opiera się na ponad 200 wywiadach z użytkownikami końcowymi systemów IoT, którzy wdrożyli ponad 1600 projektów IoT w ciągu ostatnich kilku lat w 48 różnych zastosowaniach użycia. *Raport* pokazuje, gdzie firmy inwestują i planują inwestować w obszar IoT, jakie branże i regiony znajdują się w czołówce oraz które przypadki użycia obiecują najwyższy zwrot z inwestycji. Z raportu wynika, że w 2021 r. przeciętna duża firma (produkcyjna, motoryzacyjna, detaliczna, energetyczna lub zajmująca się e-zdrowiem) wprowadziła osiem różnych zastosowań obejmujących obszar IoT. Ciekawostką jest, że firmy z sektora energetyki znacznie wyprzedziły inne firmy, wprowadzając średnio 15 różnych zastosowań systemów IoT. *Raport* nie uwzględnia takich przypadków użycia jak inteligentne ogrzewanie, wentylacja i klimatyzacja oraz inteligentnych systemów transportowych. Analiza nie uwzględnia również przypadków konsumenckich zastosowań IoT, takich jak np. *Smart Home*. Sześć z 10 najczęstszych obecnie przypadków użycia IoT ma na celu usprawnienie procesów produkcyjnych, usprawnienie prac konserwacyjnych lub przyspieszenie jakichkolwiek innych operacji np. wytwarzanie energii w przypadku firmy energetycznej. Trzy z 10 najczęstszych przypadków użycia IoT dotyczą inteligentnych łańcuchów dostaw, a tylko jeden dotyczy inteligentnych produktów w terenie. Strzałka trendu wskazuje, czy firma zamierza inwestować w dane rozwiązanie w najbliższych 2 latach (por. *rys. 8* [8]).

Okazuje się, że zdalne monitorowanie zasobów (wyłącznie do odczytu danych) jest zarazem najprostszym, jak i najczęściej stosowanym przypadkiem użycia IoT (pozwala m.in. na wizualizowanie danych zasobów, ale bez możliwości interakcji z danym zasobem). Stanowi ono 34% wszystkich zastosowań. Takie użycie IoT zostało docenione zwłaszcza w okresie ostatniej pandemii. Aż 36% ankietowanych twierdzi, że planuje znacznie zainwestować w taki właśnie przypadek zastosowania IoT w ciągu najbliższych dwóch lat. Z kolei automatyzację procesów opartą na IoT wdrożyło 33% firm. Firmy wprowadzają ten przypadek użycia IoT w celu zwiększenia elastyczności i sprawności procesu operacyjnego. W przyszłości pozwoli im to na zmianę określonych etapów procesu, co jest szczególnie ważne

» *Rys. 8. Najpopularniejsze zastosowania Internetu Rzeczy oraz Wszechrzeczy – IoT – IoE (Źródło: [8])*



» *Rys. 9. Technologie bezprzewodowe dla IoT względem zasięgu ich działania*

w aspekcie dostosowywania przez firmy swoich procesów produkcyjnych i operacyjnych do stale zmieniających się wymagań klientów. Zdalne monitorowanie i kontrola zasobów zarówno do odczytu, jak i zapisu stanowi rozszerzenie pierwszego przypadku. Oprócz odczytywania parametrów użytkownik może również zdalnie wpływać na kontrolę zasobów. Ten przypadek użycia zyskał na popularności w dobie pandemii COVID-19, gdzie dostęp do niektórych zasobów przez zespoły serwisowe był mocno utrudniony. Pomimo stosunkowo dużych kosztów wdrożenia (również instalacji i konserwacji) takie rozwiązanie zwraca się w stosunkowo krótkim okresie czasu – 51% respondentów zgłosiło amortyzację w czasie krótszym niż 2 lata. Z kolei zarządzanie pojazdami we flocie to obecnie numer jeden w łańcuchu dostaw segmentu IoT. Im większa flota samochodów do zarządzania, tym większa złożoność. Z tego też powodu 31% firm wdrożyło rozwiązanie do zarządzania flotą pojazdów w celu gromadzenia informacji w czasie rzeczywistym. W większości przypadków do transmisji danych stosowana jest sieć komórkowa, ale w najbliższym czasie przewiduje się również użycie tanich technologii satelitarnych jak np. Starlink (część SpaceX) lub Hiber (sieć satelitarna dedykowana zastosowaniom IoT). Śledzenie lokalizacji zasobu jest również jednym z najczęściej stosowanych przypadków użycia. Z tego też powodu aż 31% firm zastosowało to rozwiązanie. Jest ono korzystne zarówno dla dostawcy produktów (np. poprzez zrozumienie sposobu użytkowania przedmiotu), jak i dla użytkownika końcowego (np. poprzez jego odszukanie w przypadku zagubienia). Zastosowanie IoT do optymalizacji wydajności aktywów/zakładów, które również stanowi 31% zastosowań IoT, integruje najnowocześniejsze narzędzia do przechwytywania i integracji danych, aby analizować w jaki sposób zasoby mogą być uruchamiane i utrzymywane na optymalnym poziomie. (np. zoptymalizowane interwały konserwacji). Jest to jeden z przypadków użycia o najwyższym oczekiwanym tempie wzrostu (42% firm planuje w tym celu znaczne inwestycje). Kolejno, kontrola i zarządzanie jakością oparte na IoT obejmuje wykorzystanie danych z czujników IoT do wykrywania problemów z działaniem urządzeń w czasie rzeczywistym. Taki rodzaj zastosowania zwraca się szczególnie szybko: z 30% firm, które wdrożyły ten przypadek użycia IoT, dwie trzecie zgłasza amortyzację w czasie krótszym niż 2 lata. Monitorowanie stanu towarów ma szczególne znaczenie w branżach takich jak farmaceutyka i przemysł spożywczy. Przykładowo, prawidłowe wartości czujnika temperatury w całym łańcuchu dostaw gwarantują bezpieczeństwo produktu końcowego (np. podczas transportu szczepionek). Takie rozwiązania były wykorzystywane przez 29% ankietowanych. Aby przewidzieć pozostały okres użytkowania zasobów i zapewnić ich naprawę przed wystąpieniem awarii, 29% wszystkich firm zainwestowało w rozwiązania na styku sztucznej inteligencji i konserwacji. W konserwację predykcyjną planuje zainwestować w nadchodzących 2 latach aż 40% ankietowanych. Dostępność tanich czujników spowodowała, że śledzenie towarów stało się łatwe i stosunkowo tanie. Spośród ankietowanych firm, aż 29% wdrożyło takie właśnie rozwiązanie.

Różne scenariusze wykorzystania IoT wiążą się z bardzo zróżnicowaną gamą systemów, zwykle łączności bezprzewodowej, zilustrowanych na *rys. 9*.

Ciekawe analizy dotyczące obszaru Przemysłu 4.0 są zawarte w [9], gdzie dokonano oceny kierunków rozwoju tego ważnego dla IoT/IoE komponentu. Wskazano tam, że warunkiem tego rozwoju jest sztuczna inteligencja i uczenie maszynowe (AI *Artificial Intelligence*/ ML *Machine Learning*). Krytyczne przypadki użycia w Przemyśle 4.0

wymagają przy tym wydajności AI/ML w czasie rzeczywistym. Oznacza to, że w przypadku użycia sieci 5G ich funkcjonalność nie może być dodawana do sztucznej inteligencji. Musi to być AI natywna, co ma miejsce, gdy możliwości AI/ML są wbudowane w funkcje sieciowe 5G. Jednym z przykładów może być integracja AI/ML w celu poprawy harmonogramu kontroli dostępu do medium (MAC) w dostępowej sieci radiowej (RAN). Dzięki analizie predykcyjnej realizowanej w czasie rzeczywistym sieć może inteligentnie wpływać na poprawę jakości świadczonych usług (QoS/QoE). Ma to wręcz kluczowe znaczenie w przypadkach użycia, takich jak inteligentna produkcja, gdzie cyfrowa para AI/ML, może poprawić wydajność i zwiększyć bezpieczeństwo. Co istotne, ten rodzaj ulepszeń AI/ML nie zamyka operatora w ograniczonym ekosystemie i nie uzależnia go od wybranego dostawcy. Operatorzy mogą skorzystać z rozwiązań Open RAN (O-RAN), oferujących większy wybór i większą elastyczność, by zmaksymalizować wydajność wykorzystania widma. Pozwala im to przezwyciężyć jedno z głównych ograniczeń dzisiejszej architektury RAN – zarządzanie zasobami radiowymi, które często jest statyczne, bez możliwości szybkiego dostosowywania do zmieniających się warunków ruchu i zachowań abonentów.

Pokazuje to również, w jaki sposób sztuczna inteligencja (i uczenie maszynowe) zasadniczo przekształci systemy komunikacji 5G oraz jak będą one projektowane i wdrażane w przyszłości. AI/ML umożliwi kontrolowanie funkcji warstwy fizycznej (PHY) i dostępu do medium (MAC). Wszystko to powinno przynieść korzyści IoT, wzbogacając w szczególności scenariusze użycia Przemysłu 4.0 ale nie tylko - teraz i w przyszłości.

Mówiąc o IoT nie można pominąć technologii *„fog computing"*, określanej dla uproszczenia mianem FOG. Zagadnieniu temu poświęcimy nieco więcej uwagi w dalszej części artykułu. W przypadku technologii FOG istotną rolę pełnią routery i/lub kontrolery sieci dostępowej, instalowane na brzegu sieci, które odbierają dane z urządzeń IoT i następnie przekazują analizującym je aplikacjom (wykorzystującym algorytmy AI, dzięki którym dane te mogą być w odpowiedni sposób zinterpretowane i przetworzone).

Technologia FOG doczekała się już „wzorcowego" rozwiązania w postaci standardu IEEE 1934 [10].

Podkreślmy raz jeszcze, że architektura ramowa dla natywnej sztucznej inteligencji i 5G jest w pełni skonteneryzowana. Jest ona także natywna dla chmury, gdzie może stanowić zbiór niezależnych i luźno powiązanych mikrousług. Gwarantuje to wysoką skalowalność i możliwość wykorzystania w chmurach publicznych, prywatnych i hybrydowych. Pozwala to jednocześnie operatorom na większą elastyczność i większą swobodę wyboru, a wraz z komponentami monitoringu i zarządzania, na realizację bezpiecznej komunikacji.

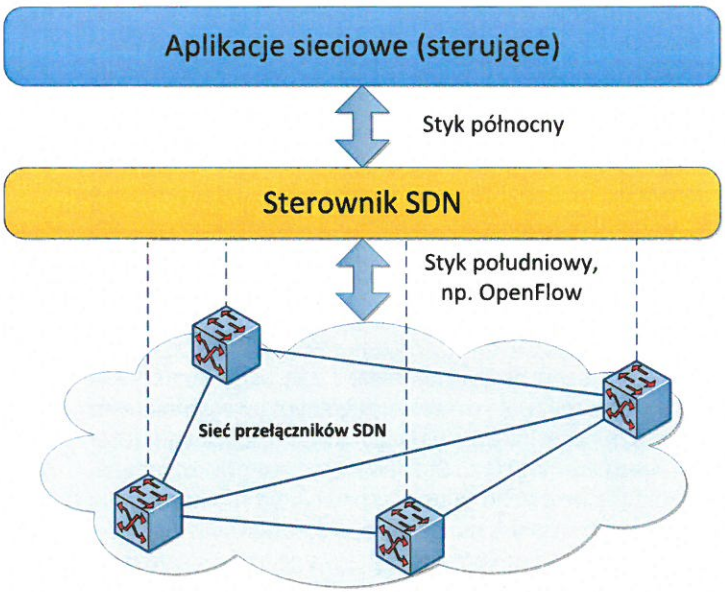
Mówiąc o IoT nie można pominąć technologii „fog computing", określanej dla uproszczenia mianem FOG.

SIECI PROGRAMOWALNE SDN (*SOFWARE DEFINED NETWORKS*) ORAZ WIRTUALIZACJA FUNKCJI SIECIOWYCH NFV (*NETWORK FUNCTION VIRTUALIZATION*)

Sieci definiowane programowo SDN oraz wirtualizacja funkcji sieciowych NFV to istotne koncepcje związane z obserwowanymi w ostatnim dziesięcioleciu trendami w rozwoju technologii sieciowych.

W przypadku SDN mamy do czynienia z separacją warstwy sterowania i zarządzania siecią od warstwy transmisji danych. Celem takiej separacji jest stworzenie systemu sieciowego, który może być centralnie i programowo zarządzany, co pozwala na lepsze wykorzystanie dostępnych zasobów sieciowych. Ideę SDN ilustruje *rys. 10*.

Technika SDN zakłada wykorzystanie logicznie scentralizowanego sterowania pracą siecią, co umożliwia elastyczne kierowanie poszczególnymi przepływami w sieci. Sterowanie jest realizowane przez aplikację sieciową, która wykorzystuje ujednolicony, abstrakcyjny model sieci utworzony przez sterownik SDN. Model ten zawiera pełną informację o topologii sieci, dostępnych zasobach sieciowych oraz aktualnie realizowanych przepływach. Wykorzystanie abstrakcyjnego modelu sieci oraz zdefiniowanie standardowego styku do konfiguracji urządzeń, tzw. styku południowego, realizowanego np. przez protokół OpenFlow, pozwala na uniezależnienie systemu sterowania od producentów węzłów, co w istotny sposób zmniejsza koszty zarządzania siecią w przypadku wykorzystywania heterogenicznych urządzeń. Ponadto, logika sterownia siecią jest realizowana w postaci



» *Rys. 10. Ogólna koncepcja architektury SDN*

aplikacji sieciowej wykorzystującej standardowy styk API (tzw. styk północny sterownika), co umożliwia łatwe wdrażanie do sieci nowych aplikacji sterujących i świadczenie nowych usług. Dzięki standaryzacji styku północnego aplikacje sterujące mogą być tworzone przez firmy niezależne od dostawców sprzętu i oprogramowania SDN. Poza rozdzieleniem funkcji przekazu danych (funkcje węzłów) od funkcji sterowania (funkcja realizowana przez sterownik sieci), sieci SDN pozwalają na uproszczenie zarządzanie siecią i jej elementami. Aplikacje zarządzające są odpowiedzialne między innymi za zbieranie informacji o dostępnych elementach i ich zasobach, monitorowanie ich stanu, a także zarządzanie dostępnymi zasobami.

Niektóre rozwiązania SDN wykorzystują programowe platformy do zarządzania, które kontrolują standardowe urządzenia sieciowe. Inne wykorzystują oprogramowanie zintegrowane z fizycznymi urządzeniami. W przypadku rozwiązań SDN wyróżniamy też podkategorie, takie jak SD-WAN, odnoszące się do programowego sterowania siecią rozległą, czy też systemy SDN wykorzystywane do segmentacji sieci w celu zapewnienia wyższego poziomu zabezpieczeń przed zagrożeniami.

Warto również zwrócić uwagę na nowe podejście do problematyki zarządzania sieciami SDN, obejmującymi dołączane ad-hoc węzły mobilne. Jest to szczególnie ważne w sieciach wykorzystywanych do celów wojskowych i zapewnienia komunikacji na szczeblu taktycznym [11]. Realizowane wówczas strategie routingu, w przypadku dołączania węzłów lub ich usuwania z sieci, zakładają użycie zróżnicowanych polityk bezpieczeństwa. Wyższe warstwy sieci, aż do orkiestratora, muszą uwzględniać ruch między- i wewnątrz domenowy o różnych politykach bezpieczeństwa.

Jednym z proponowanych rozwiązań problemu bezpiecznego routingu i zarządzania siecią SDN może być implementacja Skrytej Warstwy Danych (*Hidden Data Layer*, HDL) w nowym standardzie, opracowywanym obecnie przez Europejską Agencję Obrony. Warstwa ta, poprzez swoje elementy wykonawcze: Głównego Rezydenta (*Main Resident*, MR), Interpretera Skrytego Protokołu (*Hidden Protocol Interpreter*, HPI) czy też Skryty Most Protokołowy (*Hidden Protocol Bridge*, HPB) gwarantuje alternatywne zarządzanie siecią SDN w przypadku zainfekowania lub kompromitacji podstawowej architektury sieci wraz z jego sterownikiem. Ponadto, rozwiązanie takie jest dedykowanie do systemu federacyjnego, gdzie kilka sterowników sieci np. przynależnych do różnych administratorów realizuje utrzymanie ruchu międzydomenowego. Wymienione elementy wykorzystują metody steganografii sieciowej.

W sieciach SDN coraz szerzej i powszechniej do wykrywania naruszeń bezpieczeństwa i zagrożeń stosowane jest uczenie maszynowe ze szczególnym uwzględnieniem metod sztucznej inteligencji i algorytmów Głębokiego Uczenia (Deep Learning) [12]. Stosowane są metody rozpraszania ruchu sieciowego w celu zapewniania równoważenia obciążenia transmisji danych przez kluczowe węzły w sieci SDN (load balancing) oraz priorytetyzację usług sieciowych w przypadku niemożliwości zapewnienia wszystkich usług w sieci z uwagi na eliminację wybranych węzłów.

Podobnie jak w przypadku SDN i akceptacji abstrakcyjnego modelu sieci, niezależnego od producentów sprzętu, również w odniesieniu do koncepcji NFV podstawowym założeniem stało się tworzenie mikrousług oraz ich separacja od wykorzystywanego sprzętu. W praktyce oznacza to wykorzystanie standardowych serwerów do uruchamiania oprogramowania służącego do obsługi usług świadczonych w sieci. Wcześniej oprogramowanie takie było z reguły ściśle pozwiązane ze sprzętem. Należy przy tym zwrócić uwagę na fakt, że do niedawna programowe rozwiązania przełączników czy routerów nie mogły współzawodniczyć w wydajności i funkcjonalności z ich specjalizowanymi, dedykowanymi i fizycznymi odpowiednikami. Jednakże wraz z rozwojem technologii wirtualizacji, zwłaszcza metod wirtualizacji wspieranych sprzętowo, tj. DPDK (*Data Plane Development Kit*), SR- IOV (*Single Root I/O Virtualization*), czy P4, sytuacja się uległa istotnej zmianie. W szczególności programowe realizacje funkcji sieciowych, nawet tych związanych z przekazem danych (UPF) pozwalają na uzyskanie zbliżonych wydajności dzięki zrównolegleniu procesu obsługi strumieni ruchu. Należy podkreślić, że istotną przewagą techniki NFV względem zastosowania dedykowanych urządzeń jest znacząco większa elastyczność we wdrażaniu nowych rozwiązań oraz skalowalność, gdyż programowe realizacje funkcji sieciowych pozwalają na elastyczne dostosowanie wydajności danej funkcji do aktualnego zapotrzebowania i są lepiej przystosowane do pracy w środowisku wirtualnym. Tym samym wdrażanie technologii NFV staje się nie tylko możliwe ale wręcz konieczne w środowiskach sieciowych wymagających podwyższonej efektywności i elastyczności oraz wysokiej skalowalności i niskich kosztów eksploatacji.

Łączne wykorzystanie obu, w zasadzie niezależnych koncepcji sieciowych, czyli programowego sterowania siecią (*Sofware Defined Networks*) oraz wirtualizacji funkcji sieciowych (*Network Function Virtualization*) zapewnia operatorowi sieci [4]:

- łatwe wprowadzanie nowych lub modyfikację oferowanych usług i innowacyjnych rozwiązań sieciowych,
- brak zależności od dostawców sprzętu,
- kreowanie nowego rynku dostawców aplikacji sieciowych,
- lepsze wykorzystanie zasobów przez ich współdzielenie, wydzielanie (*network slicing*) lub skalowanie,
- zmniejszenie kosztów utrzymania infrastruktury sieci.

Równolegle z implementacją SDN oraz NFV realizowanych jest szereg przedsięwzięć mających na celu wprowadzanie nowych aplikacji i usług w chmurze oraz technik przetwarzania danych na brzegu sieci (FOG/MEC).

NOWE APLIKACJE I USŁUGI W CHMURZE ORAZ TECHNIKI PRZETWARZANIA DANYCH NA BRZEGU SIECI (FOG/MEC)

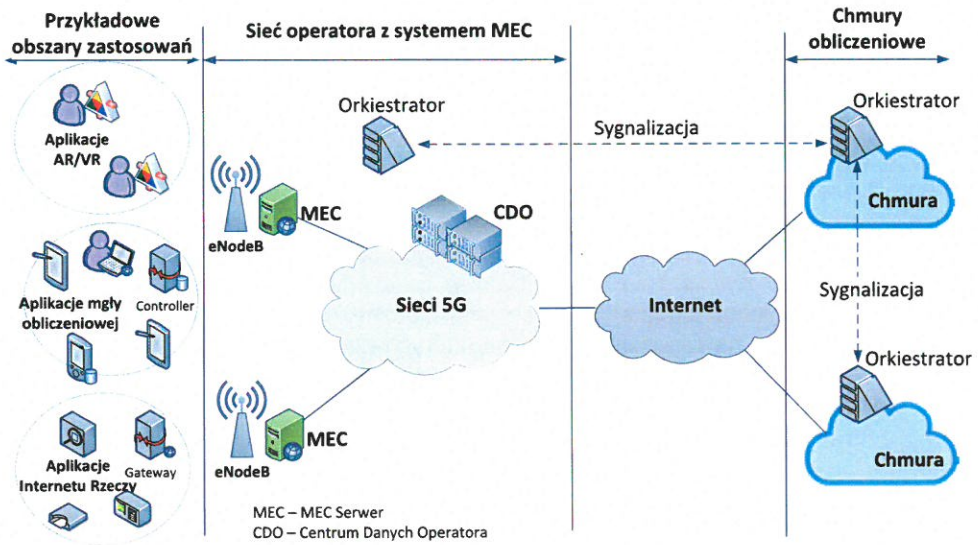
Dalszy rozwój aplikacji i usług oferowanych z wykorzystaniem techniki chmur obliczeniowych (*Cloud Computing*) jest już niewątpliwie trwałym kierunkiem rozwoju teleinformatyki. Wykorzystanie koncepcji usług chmurowych

w istotny sposób ułatwia wdrażanie nowych usług, głównie ze względu na elastyczny sposób oferowania swoich zasobów. Dostawcy usług chmurowych oferują wiele modeli dzierżawy zasobów, nazywanych jako XaaS (*X as a Service*), od dzierżawy fizycznych zasobów w modelu IaaS (*Infrastructure as a Service*) aż po bezpośrednią dzierżawę oprogramowania w modelu SaaS (*Software as a Service*). Istotnym czynnikiem ułatwiającym wdrożenie nowych usług jest również możliwość delegowania realizacji złożonych funkcji zarządzania zasobami, utrzymania infrastruktury czy też zapewnienia bezpieczeństwa do dostawcy usług chmurowych. Wykorzystanie usług chmurowych pozwala usługodawcom na istotne ograniczenie ponoszonych kosztów inwestycyjnych i operacyjnych (CAPEX/OPEX) w porównaniu do tradycyjnych rozwiązań bazujących na utrzymaniu własnej infrastruktury teleinformatycznej. Niższe koszty wynikają przede wszystkim z wysokiego stopnia agregacji zasobów w centrach danych, lepszego wykorzystania zasobów, wynikającego z zasady „ekonomii współdzielenia" oraz powszechnego przyjęcia modelu „płać za użycie", w którym to modelu usługodawca ponosi jedynie koszty aktualnie wykorzystywanych zasobów unikając wysokich kosztów wynikających z konieczności przewymiarowania systemu dla prognozowanego największego obciążenia. Ponadto, rozwiązania chmurowe umożliwiają automatyczne skalowanie wydajności aplikacji przez dostosowanie liczby instancji poszczególnych komponentów aplikacji oraz ich lokalizacji do aktualnego obciążenia.

Należy jednakże zwrócić uwagę, iż rynek dostawców usług chmurowych jest silnie niezrównoważony. Obecnie obserwujemy dominującą pozycję kilku światowych hipergigantów, np. Google, Amazon, Microsoft, których rozwiązania są powszechnie wykorzystywane i stają się de facto standardem w świecie usług chmurowych. Rozwiązania oferowane przez pojedynczych europejskich i krajowych dostawców usług chmurowych charakteryzują się znacznie mniejszą skalą, istotnym rozdrobnieniem i heterogenicznością, które to cechy nie pozwalają na utrzymanie konkurencyjności wobec największych dostawców usług chmirowych. Rozważanym rozwiązaniem jest zapewnienie skutecznej współpracy pomiędzy małymi i średnimi dostawcami usług, którzy dzięki tej współpracy, np. na zasadzie federacji ,mogą skutecznie konkurować nawet z największymi dostawcami usług chmurowych. W tym celu w Europie powołano inicjatywę GAIA-X [13], która ma dostarczyć ekosystem rozwiązań i usług chmurowych dla użytkowników europejskich, proponując ofertę jako alternatywę dla koncernów amerykańskich.

Rozwiązania stanowią istotny krok w rozwoju infrastruktury telekomunikacyjnej w kierunku przyszłej, zintegrowanej infrastruktury komunikacyjno-obliczeniowej.

Choć dalszy rozwój rynku usług chmurowych jest niewątpliwym faktem, jednakże obecnie dostrzega się istotne ograniczenia. Podstawowym ograniczeniem jest konieczność przesyłania danych pomiędzy użytkownikiem a centrum danych, które jest często zlokalizowane w znacznej odległości od użytkownika. W efekcie użytkownik doświadcza znacznego opóźnienia przekazu danych, które uniemożliwia realizację usług wymagających przetwarzania danych w czasie zbliżonym do rzeczywistego [14]. Przykładami takich usług są zyskujące na popularności usługi rozszerzonej/wirtualnej/mieszanej rzeczywistości AR/VR/MR (*Augmented Reality/ Virtual Reality/ Mixed Reality*), interaktywne gry wideo, aplikacje sterowania w czasie rzeczywistym wymagane w zastosowaniach Przemysłowego Internetu Rzeczy, systemów pojazdów autonomicznych oraz usługi strumieniowania obrazów wideo 360 o wysokiej rozdzielczości [15].



» *Rys. 11. Ilustracja scenariuszy użycia techniki MEC i FOG*

Proponowanym rozwiązaniem jest zastosowanie koncepcji przetwarzania danych na brzegu sieci w infrastrukturze operatora, określanej jako *„edge computing"* [16] lub bezpośrednio na urządzeniach końcowych tworzących tzw. mgłę obliczeniową „fog computing" [17]. Oba rozwiązania zakładają przeniesienie newralgicznych komponentów usługi z odległych centrów danych w otoczenie użytkownika i z tego względu są określane jako rozwiązania „edge/fog computing". Należy jednakże zwrócić uwagę, że rozwiązania przetwarzania danych na brzegu sieci są rozwiązaniami opracowanymi dla operatorów sieci, które zakładają rozszerzenie infrastruktury telekomunikacyjnej o serwery oferujące zasoby obliczeniowe użytkownikom lub innym dostawcom usług (w tym dostawcom usług chmurowych). Spośród tej grupy rozwiązań należy wyróżnić propozycję architektury MEC (*Multi-access Edge Computing*), która została opracowana przez organizację standaryzacyjną ETSI [18]. Rozwiązanie ETSI MEC stanowi obecnie integralną cześć infrastruktury sieci 5G i przyszłej 6G, ale może być również zastosowane w sieciach LTE oraz innych sieciach dostępowych. Przykładową sieć wykorzystującą technikę MEC przedstawia *rys. 11*.

Rozwiązania te stanowią istotny krok w rozwoju infrastruktury telekomunikacyjnej w kierunku przyszłej, zintegrowanej infrastruktury komunikacyjno-obliczeniowej.

Podsumowując, należy podkreślić, iż europejski rynek dostawców usług chmurowych charakteryzuje się znacznym stopniem rozdrobnienia, które stanowi istotną barierę w jego rozwoju i barierę konkurencyjności wobec największych światowych dostawców. Z tego względu są obecnie prowadzone prace dotyczące opracowania rozwiązań zapewniających efektywną współpracę wielu małych i średnich dostawców usług chmurowych. Pierwsze wyniki projektów europejskich [13] oraz prac teoretycznych wskazują na wysoką efektywność takich rozwiązań [19]. Opracowanie takich rozwiązań daje szansę na zbudowanie przewagi konkurencyjnej wobec dominującej pozycji „hiper-gigantów" w obszarze dostawców usług chmurowych.

Należy podkreślić, iż w przypadku systemów obliczeń na brzegu, w przeciwieństwie do rozwiązaniach chmurowych, ich rozproszenie paradoksalnie stanowi przewagę względem oferty największych dostawców. Wynika to z faktu, iż systemy obliczeń na brzegu zakładają rozproszenie zasobów obliczeniowych, w szczególności oferowanych w otoczeniu użytkownika. Z tego względu, istnienie wielu lokalnych dostawców zasobów obliczeniowych, w tym zasobów oferowanych w ramach dostawców skojarzonych dostawcami usług internetowych, stanowi dobrą podstawę dla zbudowania efektywnego rozwiązania. Warunkiem koniecznym jest jednak opracowanie architektury systemu umożliwiającego utworzenie federacji dla zapewnienia konsolidacji usług, agregacji zasobów i zwiększenia ich dostępności, a także zapewnienia wszechobecności oferowanych usług, gwarantujących wsparcie mobilności użytkownika/aplikacji.

Cyberbezpieczeństwo i/lub cyberniebezpieczństwo staje się elementem nie tylko dyskusji technicznych, ale też ważnych koncepcji filozoficznych i ekonomicznych.

CYBER(NIE)BEZPIECZEŃSTWO

We wszystkich obszarach funkcjonowania sieci i systemów teleinformatycznych kluczowe jest bezpieczeństwo [20] .

Bezpieczeństwo przestało być traktowane, w ostatnich dekadach, jako zagadnienie ortogonalne do przekazów w systemach telekomunikacyjnych – stało się ich integralną i niezbędną częścią, mając kluczowe znaczenie na wszystkich etapach – od projektowania, poprzez implementację, do konfiguracji systemów i sieci.

Należy jednakże zwrócić uwagę na fakt, że cyberbezpieczeństwo i/lub cyberniebezpieczństwo staje się elementem nie tylko dyskusji technicznych, ale też ważnych koncepcji filozoficznych i ekonomicznych [21].

Pod koniec okresu zimnej wojny, w 1985 roku, po raz pierwszy w odniesieniu do teorii przywództwa, w książce „Leaders. The Strategies For Taking Charge" Warrena Bennisa i Burta Nanusa [22], pojawiła się koncepcja modelowana świata o akronimie VUCAw celu odpowiedniego wyrażenia jego zmienności (*volatility*), niepewności (*uncertainty*), złożoności (*complexity*) i niejednoznaczności (*ambiguity*). Model zaadoptowany przez środowiska wojskowe, a następnie biznesowe wyrażał tragiczny paradygmat regularnych, często dotkliwych i mylących zmian. Katastroficzny świat VUCA pasujący także do spojrzenia na cyberprzestrzeń, stał się jednak po prawie 35 latach mocno wyeksploatowany, stąd też zaktualizowanym podejściem zaprezentowanym przez Jamaisa Cascio w 2020 roku [23, 24] jest BANI–*brittle* (kruchy), *anxious*, (niespokojny), *non-linear* (nieliniowy), *incpreceptible* (niezrozumiały).W pierwszym spojrzeniu można traktować świat BANI jako świat VUCA z nowym językiem opisu, jednak głębsze spojrzenie pozwala mieć, być może absurdalną nadzieję, że istnieje metoda „kontrolowania" chaosu przez torowanie drogi dla proaktywnych rozwiązań tworzących nowe mapy drogowe dla przytłaczającego świata uformowanego w ostatnich paru latach przede wszystkim przez pandemię COVID-19, a obecnie przez działania wojenne na Ukrainie. Świat BANI znakomicie opisuje wyzwania jakie stoją przed współczesnym cyberbezpieczeństwem, które w zetknięciu z istniejącymi zjawiskami nie ma szansy całkowicie wyleczyć świata, ze wszystkich niespodziewanych podatności, obronić przed wszystkimi atakami i ich, często nieznanymi, skutkami. Wciąż pokutuje myślenie, że posiadając standardowe narzędzia służące do walki, czyli miecz i tarczę (w obu przypadkach z przedrostkiem cyber) można wygrywać cyberbitwy. Nie jest to niestety prawdą, gdyż narzędzia bardzo szybko i nieliniowo ewoluują, co przekłada się na niemożność opisania stanu sztuki w cyberbezpieczeństwie w sposób pewny i dokładny. Nieoznaczoność jest wpisana w cyberbezpieczeństwo i możemy się poruszać w tej dyscyplinie, typując obszary najbardziej narażone na atak. Przede wszystkim są to obszary strategiczne, często należące do infrastruktury krytycznej, których elementem kluczowym są sieci telekomunikacyjne. Od strony ekonomicznej są to obszary, gdzie cyberprzestępcy mogą czerpać najszybsze i największe zyski, z drugiej strony rozwój usług typu Hacking as a service (HaaS), sprawia, że grono cyberprzestępców będzie w sposób niekontrolowany rozwijać się. Najbardziej prostym, a jednocześnie dotkliwym atakiem na sieci telekomunikacyjne,

w skład których wchodzą często zasoby chmurowe, jest odmowa usługi, dzięki któremu infrastruktura przestaje być dostępna i wielu jej użytkowników traci możliwość pracy. Redundancja zasobów, która sprowadza się do rozproszenia zasobów chmurowych jest dość kosztowna, ale dostępna wśród dostawców usług, co pozwala zachować ciągłość działania. Ogólnie trend *Security as a service* (SaaS) pozwala na lepszy dostęp do wielu usług bezpieczeństwa, które były dotychczas dość kosztowne, ze względu na zakup i eksploatację dedykowanych do cyberbezpieczeństwa urządzeń takich jako sondy sieciowe, systemy wykrywania włamań, czy też systemy detekcji anomalii. W systemach typu SaaS proces tworzenia sygnatur ataków może zostać istotnie przyspieszony, przez pełniejszy dostęp do większych wolumenów ruchu z wieloma próbkami ataków.

Przez ostatnie lata ewolucja ataków podążyła w kierunku ich automatyzacji i zwiększenia stopnia ich skomplikowania, przez równoległe i skorelowane użycie szeregu podatności. Sposób prowadzenia ataków jest znamienny dla konkretnych grup przestępczych i przynajmniej częściowo pozwala na analizę ataków mocno rozproszonych w czasie i cyberprzesteni (APT–*Advanced Persistent Threats*).

Należy podkreślić, iż europejski rynek dostawców usług chmurowych charakteryzuje się znacznym stopniem rozdrobnienia, które stanowi istotną barierę w jego rozwoju i barierę konkurencyjności wobec największych światowych dostawców.

Automatyzacja często jest wspierana przez techniki wykorzystujące sztuczną inteligencję (SI), czy też uczenie maszynowe. Oczywiście zgodnie z zasadą omnes qui acceperint gladium, gladio peribunt techniki SI używane są nie tylko jako metody ofensywne, ale także jako metody defensywne, co pokazuje, że cyberbitwy często są, przynajmniej w pewnych etapach, pojedynkami maszyn. Warto podkreślić, że nastąpiła zmiana myślenia o atakach w ciągu ostatniej dekady: aspekty ofensywnej ochrony nie są już wstydliwe, wygląda na to, że znów wracamy do pewnych pryncypiów impetus est optima defensio. Pewnym gorsetem, przynajmniej w świecie niezwiązanym z obronnością, jest legislacja, która z opóźnieniem podąża, za rozwojem cyberprzesteni.

W kwestii sztucznej inteligencji istotny wydaje się aspekt odpowiedzialnego uczenia maszynowego który w kontekście cyberbezpieczeństwa jest mocno dyskusyjny i sprowadza się do problemu: czy można prowadzić wojnę w sposób etyczny?

Pojawia się wiele innych trudnych pytań: jaka jest granica, której nie można przekroczyć podczas ataku? Czy inaczej traktować systemy wirtualne, a inaczej cyberfizyczne? Jak cyberataki przenoszą się na zdrowie i życie ludzi? Jaki poziom komfortu atakowanych jest akceptowalny?

Oczywiście odpowiedzi na te pytania, przełożą się wcześniej, czy później na kwestie prawne, co wydaje się procesem długotrwałym. Uczenie maszynowe w cyberbezpieczeństwie ma jeszcze jedną istotną słabą stronę: wiarygodność metod samych w sobie. Z jednej strony jest to kwestia regularnego trenowania algorytmów, tak aby działały z jak największą dokładnością i generowały jak najmniejszą liczbę fałszywych alarmów, z drugiej są to błędy w konstrukcji samych algorytmów, które obniżają ich bezpieczeństwo i często nie gwarantują prywatności. Cyberbezpieczeństwo bardzo dynamicznie rozwija się od ponad dekady, rośnie świadomość podatności i możliwości skutków przeróżnych ataków, jest to oczywiście związane z cyfryzacją społeczeństwa, elektronizacją usług i dostępem do nich z dowolnego miejsca na Ziemi.

Trzy priorytety na najbliższe lata wydają się następujące:
1) zwiększenie nacisku na cyberedukację,
2) rozwój metod obrony przed atakami ze wsparciem sztucznej inteligencji, a także
3) mentalne i techniczne przygotowanie na eliminację klasycznych systemów kryptograficznych.

W świetle wciąż niespełnionej wizji komputera kwantowego, czyli programowalnej maszyny, a nie tylko demonstratora eksperymentów fizycznych, „stara kryptografia" musi dać miejsce algorytmom postkwantowym, zapewne, na dziś, wciąż niewystarczająco wydajnym do zastosowań przy obsłudze dużych i szybkich strumieni danych. Na „starej kryptografii" jest zbudowanych sporo systemów kryptowalut, co jest prognostykiem, że ze współczesnego złota w pewnym momencie zmienią się w tombak.

Warto zauważyć, że cyberbezpieczeństwo dotyczy także ważnego obszaru oddziaływań elektromagnetycznych, często pomijanych w rozważaniach nad bezpieczeństwem sieci komputerowych. W radiokomunikacji właściwa alokacja pasm częstotliwości determinuje jakość usług i bezpieczeństwo realizowanych przekazów.

W wielu sytuacjach jako sieci dostępowe do Internetu wykorzystujemy popularne sieci WLAN. Barierami wzrostu przepływności w tego typu jednokanałowych sieciach bezprzewodowych, z najczęściej transmisją dookólną, są zjawiska: tłumienia sygnału radiowego w potęgowej funkcji odległości od nadajnika, tj. ograniczenie zasięgu odbioru oraz interferencje w kanale radiowym, wywołane, w znacznym stopniu, przez kolizje ramek danych. Zjawiska te odzwierciedla się zwykle przy pomocy tzw. modelu fizycznego bądź modelu protokolarnego. W pierwszym przypadku pokonywanie ograniczeń wiąże się z osiąganiem założonej minimalnej wartości SINR – stosunku sygnału do szumu i interferencji w punkcie odbioru sygnału, w drugim zaś z redukcją zbioru stacji jednocześnie transmitujących ramki danych, eliminacją stacji ukrytych i minimalizacją stacji eksponowanych. Jednakże, nawet w efekcie stosowania protokołów spełniających ww. postulaty sumaryczna przepływność sieci ze wzrostem liczby węzłów N nie skaluje się dla sieci lokalnych i spada dla sieci wieloskokowych. Ciekawym przedmiotem badań, w kontekście szeroko rozumianego bezpieczeństwa pracy sieci WLAN jest też problem niekooperatywnych zachowań wybranych użytkowników, związany z uzurpacją uprawnień, i przejmowaniem dostępu do medium poprzez ograniczanie wartości istotnego para-

metru jakim jest losowe opóźnienie w dostępie do medium po okresie jego zajętości.

W sieciach teleinformatycznych obserwujemy trend do tworzenia kanałów o coraz szerszych i dynamicznie modyfikowanych pasmach. Z kolei mnogość modulacji cyfrowych dla wybranych usług i na wybranych obszarach sprawia, że do właściwego doboru pasma, a takżemetod i parametrów emisji radiowej coraz częściej wykorzystujemy efektywne algorytmy sztucznej inteligencji. Szerokopasmowe analizatory widma wspierane sztuczną inteligencją, nazwane Kognitywnymi Analizatorami Widma (*Cognitive Spectrum Analysers driven by Artificial Intelligence*, CSA AI) [25] potrafią dokonać optymalnego wyboru parametrów emisji dla danego środka łączności lub grupy środków łączności, przewidywać zajętość poszczególnych częstotliwości w tzw. oknach czasowych oraz dokonywać klasyfikacji emisji w czasie rzeczywistym.

Analizatory kognitywne wspierają Kognitywne Radio i Kognitywne Radary, poprzez dedykowane interfejsy pozwalające na zmianę parametrów tych urządzeń w czasie rzeczywistym. Analizatory tej klasy stanowią integralne części radiostacji lub radarów. W zastosowaniach wojskowych takie kognitywne analizatory widma wspierane przez sztuczną inteligencję potrafią staczać ze sobą „walki" w celu zapewnienia albo dobrej jakości łącza radiowego i tym samym utrzymania łączności albo skutecznego zakłócenia środka radiowego przeciwnika. Odbywa się to poprzez natychmiastowy dobór właściwych parametrów emisji względem przewidywanej aktywności radiowej drugiej strony. Ręczne dostrajanie radiostacji lub stacji radiolokacyjnej i nastawianie ich na dane radiowe lub radarowe powoli odchodzi do przeszłości. Automat zrobi to szybciej i lepiej. Efektywność wykorzystania pasma radiowego dla automatycznych nastaw CSA AI jest bliska optymalnej. To bez wątpienia przyszłość radiokomunikacji, w szczególności radiokomunikacji wojskowej.

WNIOSKI KOŃCOWE

W sieciach telekomunikacyjnych - czy bardziej teraz teleinformatycznych, obserwujemy wyraźną tendencję, podobnie jak w informatyce, oddzielania oprogramowania od sprzętu. Podstawą dla takich rozwiązań stają się platformy wirtualizacyjne i powiązane z nimi techniki wirtualizacji, konteneryzacji oraz technologie chmurowe.

Bazując na takim rozdziale oprogramowania i sprzętu, sieci zyskują zarówno na elastyczności (zmiany są dokonywane wyłącznie w oprogramowaniu) jak i efektywności ekonomicznej, dzięki zmniejszaniu kosztów (infrastruktura sprzętowa staje się zasobem o dłuższej skali czasowej).

Sieci definiowane programowo oraz wirtualizacja funkcji sieciowych są głównymi składnikami nowych generacji sieci korzystających w głównej mierze z oprogramowania. Te nowe techniki pozwalają na jeszcze większą elastyczność poprzez oddzielenie płaszczyzn sterowania i danych oraz przekształcenie złożonego zarządzania siecią w znacznie prostszy łańcuch usług lub mikrousług, który może stać się mniej lub bardziej autonomiczny.

Efektem takich działań są sieci bazujące na oddzielnych, dedykowanych fragmentach oprogramowania, które można wdrożyć w całości w chmurze, a gdy potrzebne są niewielkie opóźnienia, to także na brzegu sieci, w pobliżu użytkowników, a nawet we mgle (w postaci rozproszonej), wykorzystując niektóre zasoby użytkowników końcowych. Mgła stwarza wiele wyzwań dla bezpieczeństwa, w szczególności ochrony poufności i integralności danych, ale zwiększa dostępność „usługową" systemu.

Bezpieczeństwo danych i systemów informatycznych urasta z poziomu „rozwiązania wymuszanego", w przypadku starych rozwiązań, do wręcz fundamentalnego wymagania we wszystkich nowych technologiach.

Wdrażane obecnie sieci piątej generacji 5G są dobrym przykładem kierunku, w którym zmierzamy, polegającego na rozdzieleniu sprzętu i oprogramowania oraz integracji różnych sieci (przewodowych i bezprzewodowych) w ramach jednego wspólnego zarządzania. Sieć staje się wtedy bezpieczną platformą łączności, przeźroczystą dla aplikacji, dzięki czemu aplikacje mogą szybko ewoluować, czego przykładem jest szeroki zakres scenariuszy IoT/IoE, w szczególności zagadnień Przemysłu 4.0.

* * *

W artykule zaprezentowano główne kierunki rozwoju współczesnych systemów i sieci telekomunikacyjnych (teleinformatycznych). Naszkicowane w artykule koncepcje i ich rozwiązania stanowią w znacznej mierze efekt prac własnych autorów tego opracowania, w tym realizowanych przez nich projektów badawczych:

1. PL-5G: Krajowe laboratorium sieci i usług 5G wraz z otoczeniem. Projekt z tzw. Mapy Drogowej Infrastruktur Krytycznych, realizowany w ramach Działania 4.2 Programu Operacyjnego Inteligentny Rozwój 2014-2020; OPI: 2021-2023 [26].
2. SyMEC: System MEC dla wspierania zaawansowanych aplikacji w środowisku sieci przewodowych i bezprzewodowych 3G/4G/5G. Projekt zrealizowany w ramach Działania 4.1 Programu Operacyjnego Inteligentny Rozwój 2014-2020, NCBiR: 2019-2022 [27, 28, 29].
3. netBaltic: Internet na Bałtyku – realizacja wielosystemowej, samoorganizującej się szerokopasmowej sieci teleinformatycznej na morzu dla zwiększenia bezpieczeństwa żeglugi poprzez rozwój e-nawigacji. Projekt zrealizowany w ramach Programu Badań Stosowanych, PBS3/A3/20/2015, NCBiR: 2015-2018 [30, 31, 32].
4. SOFTANET: "Software defined tactical & theatre network". Projekt EDA Cat B 2021-2024.
5. CRAI 1: "Communications and Radar systems hardened with Artificial Intelligence in a contested electronic warfare environment 1 (CRAI 1)". Projekt EDA Cat B 2020-2023 [33].
6. NGIatlantic.eu A Collaborative platform for EU-US ‚Next Generation Internet' experiments: „Experiment on security features of mobile network infrastructure", 2022-. H2020 Grant Agreement No. 871582 [34, 35].
7. EU Celtic-Next Programme „Imminence: Intelligent Management of next generation MobIle NEtworks aNd serviCEs", 2021-2024. Celtic-Next, EU Eureka Initiative [36, 37].
8. Program CyberSecIdent IV „Security framework for 5G network based on multiple providers: specification, implementation and development of evaluation process", 2021-2024. Dofinansowany przez NCBiR [38, 39].
9. Program Sonata bis „Context-Aware Adaptation for eMBB services in 5G networks", 2019-2022. Dofinansowany przez Narodowe Centrum Nauki [40, 41, 42].

BIBLIOGRAFIA:

[1] Cisco Annual Internet Report (2018–2023). White Paper 2020.
[2] Cisco Annual Internet Report (2017–2022), White Paper 2019.
[3] M. Jammal, T. Singh, A. Shami, R. Asal, Y. Li: Software-Defined Networking: State of the Art and Research Challenges https://www.pipelinepub.com/Digital-Transformation-2022/article_index
[4] Tendencje w rozwoju polskiej i światowej telekomunikacji i teleinformatyki Wyd. WAT, 2020.
[5] 5G Americas: https://www.5gamericas.org/white-papers.
[6] Analysys Mason: https://www.analysysmason.com.
[7] Accelerating Smart Manufacturing with Private 5G Networks., 2021.https://go.accedian.com/accelerating-smart-manufacturing-with-private-5g-networks.
[8] P. Wegner, The top 10 IoT Use Cases IoT Analytics: Market Insights for the Internet of Things, October 2021 https://iot-analytics.com/top-10-iot-use-cases.
[9] S. Pal: IoT, 5G, & O-RAN: Gearing Up for Industry 4.0 with Native AI and ML/ Pipeline Magazine /Digital Transformation (pipelinepub.com), April 2022, Volume 18, Issue 6.
[10] IEEE 1934-2018 IEEE Standard for Adoption of OpenFog: Reference Architecture for Fog Computing. https://standards.ieee.org/news/2018/ieee1934-standard-fog-computing/.
[11] https://www.gov.pl/web/obrona-narodowa/polska-przystapila-do-kolejnych-projektow-badawczych-europejskiej-agencji-obrony.
[12] M. Bistron, Z.Piotrowski: Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. Electronics 2021, 10, 871.
[13] GAIA X: https://gaia-x.eu/.
[14] A. Kesevan: Comparing the Network Performance of AWS, Azure and GCP. Thousand Eyes, 2019,https://pc.nanog.org/static/published/meetings/NANOG75/ 1909/20190218_Kesavan_Comparing_The_Network_v1.pdf.
[15] P. Ren, X. Qiao, J. Chen, S. Dustdar: Mobile Edge Computing–a Booster for the Practical Provisioning Approach of Web-Based Augmented Reality. IEEE/ACM Symposium on Edge Computing (SEC), 2018, ISBN 978-1-5386-9445-9.
[16] AT&T Labs, "AT&T Edge Cloud (AEC) - White Paper", 2017. https://about.att.com/content/dam/innovationdocs/Edge_Compute_White_Paper%20FINAL2.pdf (dostęp 16.06.2022).
[17] R. K. Naha et al.: Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions. IEEE ACCESS, vol. 6, pp. 47980 – 48009, 2018.
[18] ETSI standard, Multi-access Edge Computing (MEC); Framework and Reference Architecture, ETSI GS MEC 003 V3.1.1, marzec 2022.
[19] W. Burakowski, A. Bęben, H. van Den Berg, et al.: Traffic Management for Cloud Federation. Autonomous Control for a Reliable Internet of Services (Red.: I. Ganchev, R.D. van der Mei, H. Van Den Berg), Lecture Notes In Computer Science, vol. 10768, 2018, pp. 269-312.
[20] K. Szczypiorski: Cyber(in)security. Int. J. Electron. Telecommun. 2020, 66, 243–248 DOI: 10.24425/ijet.2020.131870.
[21] Krzysztof Szczypiorski Cybersecurity and Data Science. Electronics. 2022; 11(15):2309. https://doi.org/10.3390/electronics11152309.
[22] W. Bennis, B. Nanus: Leaders. The Strategies for Taking Charge. Collins Business Essentials. 2007, (https://doi.org/10.1002/hrm.3930240409) .
[23] J. Cascio: Facing the Age of Chaos. 2020. https://mediun.com/@cascio/facing-the-age-of-chaos-b00687b1f51d.
[24] J. Cascio: BANI: A New Framework to Make Sense of a Chaotic World? 2022. (https://thinkinsights.net/leadership/bani/).
[25] T. Shakeel, S. Gul, S. Habib and A. Naseer: A Systematic Literature Review on Cognitive Radio Networks," 2021 International Conference on Innovative Computing (ICIC), 2021, pp. 1-11..
[26] W. Burakowski i inni: Planowane krajowe laboratorium badawcze sieci 5G i usług wraz z otoczeniem. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2022, Z.4.
[27] A. Bęben i inni: Implementacja architektury SyMEC. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2022, Z.4.
[28] B. Krakowiak i inni: System sterowania i zarządzania SyMEC (SyMEC control and management system). Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2022, Z.4.
[29] M. Hoeft i inni: Wdrożenie systemu SyMEC w sieciach WLAN: Moduł współpracy serwera MEC z siecią dostępową WLAN (MEC system implementation in WLAN networks: MEC server module providing integration with WLAN access networks). Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2022, Z.4.
[30] J. Woźniak, M. Hoeft: Cel i główne zadania badawcze projektu netBaltic (Aim and main research tasks of the netBaltic project). Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2016, T.12, 1301-1303.
[31] K. Gierłowski, M. Hoeft, J. Woźniak: netBaltic - Heterogeniczny system bezprzewodowej łączności na Morzu Bałtyckim. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne. 2016, T.8-9. 1196-1200.
[32] M.Hoeft, K. Gierłowski J. Rak, J. Woźniak, K. Nowicki: Non-Satellite Broadband Maritime Communications for e-Navigation Services. IEEE Access, 2021, 9, pp. 62697–62718.
[33] P. Ścibiorek, Z. Piotrowski: Protection of resources of an SDN virtual network that utilises Hidden ID tags, a Hidden Network Driver and HS witch Hidden Switching. Elektronika - Konstrukcje, Technologie, Zastosowania. LX (9/2019):16-18.
[34] J. Mongay Batalla, S. Sujecki, H. Song, C. X. Mavromoustakis, T. Wichary: Theoretical analysis of QBER for Quantum Key Distribution in 5G multi-site networks. IEEE Smart Data-2022, Espoo (Finland), Aug. 22-25, 2022.
[35] G. Khayat, C. X. Mavromoustakis, G. Mastorakis, J. Mongay Batalla, E. Pallis: Swarm UAV Network Constraints in Damaged Infrastructures. IEEE International Conference on Communications ICC 2022. Seoul (South Korea), 16–20 May 2022.
[36] J. Mongay Batalla, S. Sujecki, J. Oko, J. Kelner: Cost-effective measurements of 5G radio resources allocation for Telecom market Regulator's monitoring, The Nineteenth ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN), Montreal (Canada), October 2022.
[37] A. Andreou, C.X. Mavromoustakis, G. Mastorakis, J. Mongay Batalla, E. Pallis: Energy Conservation by using the Integration of Distributed Energy System in Smart Vehicles, in Proceedings of The IEEE International Energy Conference (IEEE Energycon 2022), Riga (Latwia), 2022.
[38] J. Mongay Batalla, M. Moshin, C. X. Mavromoustakis, K. Wesołowski, G. Mastorakis, K. Krzykowska-Piotrowska: On deploying the Internet of Energy with 5G Open RAN technology including beamforming mechanism, Energies 2022, 15, 2429.
[39] G. Peinado Gomez, J. Mongay Batalla, Y. Miche, S. Holtmanns, C. X. Mavromoustakis, G. Mastorakis, N. Haider: Security policies definition and enforcement utilizing policy control function framework in 5G, Computer Communications, Vol. 172, Pp. 226-237, 2021.
[40] J. Mongay Batalla, E. Andrukiewicz, G. Peinado Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, M. Imran: Security Risk Assessment for 5G networks - national perspective. IEEE Wireless Communications, vol. 27, no. 4, pp. 16-22, Aug. 2020.
[41] J. Mongay Batalla, C. Mavromoustakis, G. Mastorakis, N. Naixue Xiong, J. Wozniak: Adaptive positioning system based on multiple wireless interfaces for Industrial IoT in harsh manufacturing environments, IEEE Journal on Selected Areas of Communications, 2020.
[42] J. Granat, J. Mongay Batalla, C. Mavromoustakis, G. Mastorakis: Big data analytics for event detection in the IoT - multicriteria approach. IEEE Internet of Things Journal. May 2020.