Redakcja | Jarosław Wołejszo, Grzegorz Rdzanek, Anna Zagórska

UNUS PRO MULTIS

Państwa i organizacje międzynarodowe wobec wyzwań i zagrożeń bezpieczeństwa XXI wieku

DOM WYDAWNICZY ELIPSA

UNUS PRO MULTIS.
Państwa i organizacje międzynarodowe wobec wyzwań i zagrożeń bezpieczeństwa XXI wieku

UNUS PRO MULTIS.
Państwa i organizacje międzynarodowe wobec wyzwań i zagrożeń bezpieczeństwa XXI wieku

Redakcja
Jarosław Wołejszo, Grzegorz Rdzanek, Anna Zagórska

DOM WYDAWNICZY ELIPSA

WARSZAWA 2019

Recenzenci

Prof. dr hab. Ryszard Niedźwiecki,
Uniwersytet Humanistyczno-Przyrodniczy im Jana Długosza w Częstochowie
Dr Sławomir Czapnik,
Uniwersytet Opolski

Projekt okładki

Agnieszka Miłaszewicz

Opracowanie redakcyjne i korekta

Hanna Januszewska

ISBN 978-83-8017-292-0

DOM WYDAWNICZY ELIPSA

Realizacja wydawnicza:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel. 22 635 03 01, e-mail: elipsa@elipsa.pl, www.elipsa.pl

SPIS TREŚCI

WSTĘP

Problematyka bezpieczeństwa narodowego i międzynarodowego od kilku już dekad jest przedmiotem niezliczonych analiz, raportów, publikacji. Każdego roku, tylko na polskim rynku wydawniczym, ukazują się dziesiątki publikacji, na kartach których ich autorzy starają się opisać, wyjaśnić, czy też zgłębić, przeróżne wymiary i aspekty współczesnego bezpieczeństwa, tak w jego militarnym, jak i poza-militarnym, wymiarze. Jedni analizują potencjalne zagrożenia dla państw i narodów, inny prowadzą rozważania dotyczące instrumentów stosowanych przez państwa w działaniach służących przeciwdziałaniu tym zagrożeniom. Niesłabnące badawcze i publikacyjne zainteresowanie problematyką bezpieczeństwa narodowego i międzynarodowego wynika z trwałej, niezmiennej przesłanki: u progu trzeciej dekady XXI wieku bezpieczeństwo pozostaje podstawową potrzebą jednostki ludzkiej, a działania na rzecz zapewnienia tejże jednostce określonego poziomu bezpieczeństwa uznawane są za kluczową funkcję współczesnych państw. Szczególnie w ostatnich dekadach narody, zorganizowane w nowoczesne społeczeństwa, domagają się od decydentów politycznych oraz osób kierujących systemami bezpieczeństwa i obrony swych państw spójnych, przemyślanych i długofalowych działań, dzięki którym możliwe będzie skuteczne przeciwdziałanie wszelkim potencjalnym i realnym zagrożeniom dla ich bytu, wolności, możliwości rozwoju ekonomicznego.

Współczesne państwa i społeczeństwa zderzają się i konfrontują z coraz bardziej złożonymi, wielowymiarowymi, nieprzewidywalnymi zagrożeniami. Wystarczy spojrzeć choćby na wielość form przemocy zbrojnej, które stosowane są przez agresywne podmioty państwowe i niepaństwowe. Po 11 września 2001 roku wydawać się mogło planistom i strategom odpowiedzialnym za zarządzenie bezpieczeństwem narodowym i międzynarodowym, że zagrożeniem o największej skuteczności oraz sile rażenia przez kilka kolejnych dekad pozostawać będzie terroryzm, głównie motywowany radykalnymi postawami religijnymi – fundamentalizmem religijnym. Dynamika globalnego bezpieczeństwa bardzo szybko zweryfikowała te prognozy. Oczywiście, terroryzm (szczególnie ten, gdzie walka

ze światem Zachodu stała się siłą napędową niesłabnących działań) pozostaje u progu trzeciej dekady XXI realnym wyzwaniem dla życia i zdrowia obywateli większości współczesnych państw (od Danii po Sri Lankę) oraz dla ich stabilności politycznej i niezakłóconego funkcjonowania. W ciągu ostatnich kilkunastu lat poznaliśmy jednak, jako mieszkańcy współczesnego globu, zupełnie nowe, równie groźne i trudne do zwalczania, zagrożenia. Piractwo morskie, które jak się wydawało, w XXI wieku oglądać powinniśmy jedynie w czasie seansów kinowych, jest dziś codziennością na wodach morskich oblewających Somalię oraz Afrykę Zachodnią. Nigeria, najludniejsze państwo w Afryce, rozrywana jest od wielu lat zbrojnym konfliktem wewnętrznym, w toku którego najpoważniejszym, najaktywniejszym aktorem jest religijno-polityczny ruch islamski Boko Haram. Kraje Ameryki Środkowej od wielu lat bezskutecznie próbują opanować rozlewającą się w zastraszającym tempie falę przemocy i przestępczości, której źródłem są świetnie zorganizowane i niebywale skuteczne kartele narkotykowe. Nawet państwo uznawane obecnie za jedyne supermocarstwo, traktowane jako hegemon militarny, czyli Stany Zjednoczone Ameryki, nie potrafi skutecznie chronić swojej południowej granicy przed napływem tysięcy nielegalnych migrantów z Hondurasu, Panamy, czy Meksyku.

Współczesne państwa stają niezmiennie przez nierozwiązywalnym dylematem, którego istota sprowadza się do pytania: przy pomocy jakich środków i jakich metod działania możliwe jest skuteczne przeciwdziałanie nowym formom zagrożeń (tak o militarnym, jak i niemilitarnym charakterze). Jak już zostało powiedziane, złożoność oraz wielowymiarowość współczesnych zagrożeń dla państw i społeczeństw powodują, że w praktyce działań prewencyjnych czy działań obronnych nie wystarczy już, iż państwo sięgnie po jeden, konkretny instrument, choćby po siły zbrojne. Jak trudnym zadaniem jest dziś prowadzenie polityki bezpieczeństwa oraz zarządzanie różnymi sektorami bezpieczeństwa doskonale widać właśnie na przykładzie kryzysów migracyjnych, które w ostatnich latach dotykały Unię Europejską oraz Stany Zjednoczone. Ani jednostki Gwardii Narodowej operujące wzdłuż granicy Stanów Zjednoczonych z Meksykiem, ani dziesiątki okrętów państw europejskich patrolujących Morze Śródziemne, nie były w stanie zatrzymać kolejnych fal migrantów zdeterminowanych, aby dotrzeć do wymarzonego „raju".

Kiedy zastanawiamy się nad najskuteczniejszym sposobem mierzenia się przez państwa z różnymi typami zagrożeń dla ich bezpieczeństwa, nieuchronnie pojawia się pytanie, w jakim stopniu możliwe jest samodzielne zwalczanie zagrożeń przez poszczególne państwa. Truizmem będzie stwierdzenie, że nawet mocarstwa dysponują dziś ograniczonymi zasobami (ludzkimi, sprzętowymi, technologicznymi), które mogłyby zostać wykorzystanie dla ochrony gospodarek, struktur politycznych, społeczeństw. Stan taki w naturalny sposób wymuszać powinien współpracę oraz integrację państw w dziedzinie bezpieczeństwa. Rozwój europej-

skiej współpracy w dziedzinie bezpieczeństwa i obrony w ramach struktur Unii Europejskiej dowodzi jednakże, że nawet w obliczu poważnych zagrożeń, państwa nie muszą być gotowe oraz silnie zdeterminowane, aby podzielić się zadaniami i kompetencjami w zakresie polityki bezpieczeństwa z innymi państwami, nawet jeśli są to państwa politycznie im bliskie, wręcz sojusznicy.

Unus pro multis – to łacińska formuła, która przywołana została przez Wergiliusza, kiedy sternik Palinurus zostaje rzucony w fale morskie w ofierze Neptunowi, aby uratować towarzyszy podróży. Współcześnie słowa te bywają tłumaczone bardzo różnie. Zazwyczaj jako: *Jeden za wszystkich*, często jednak jako: *Jeden za wielu*. Czytelnik tego zbioru musi jednak zastanawiać się, dlaczego w tytule książki pojawiła się właśnie ta sentencja, a co więcej – dlaczego akurat ona stanowi kanwę rozważań dotyczących współczesnego bezpieczeństwa. Pewną podpowiedź stanowi druga część tytułu: *Państwa i organizacje międzynarodowe wobec wyzwań i zagrożeń bezpieczeństwa XXI wieku.* Już jednak w tym miejscu zasadne wydaje się wyjaśnienie zamysłu, który przyświecał autorom poszczególnych rozdziałów oraz redaktorom niniejszego tomu.

Niezależnie o tego, które z tłumaczeń tej łacińskiej formuł uznamy za lepiej oddające myśl – intencję Wergilusza, trudno nie zgodzić się z twierdzeniem, że współczesne państwa, formułując i realizując każdego dnia politykę bezpieczeństwa, rozstrzygać muszą dylematy podobne do tych, które towarzyszyły podróżnikom poświęcającym sternika, aby zyskać przychylność Neptuna i tym sposobem ratującym własne życie. W latach 90. XX wieku bardzo „modne" i często stosowane przez Stany Zjednoczone Ameryki, Francję, Kanadę, Wielką Brytanię, mniejsze państwa Unii Europejskiej i NATO, były założenia i wytyczne koncepcji globalnego zarządzania kryzysowego oraz działań prewencyjnych. Sojusz Północnoatlantycki oraz Unia Europejska, niezależnie od posiadania bezpośrednich, wymiernych, materialnych interesów, związanych z danym regionem świata, czy danym państwem, interweniowały politycznie i zbrojnie uznając, że zgoda na destabilizację jakiejś części świata oraz przyzwolenie na rozwój na tym obszarze agresywnych, zbrojnych podmiotów zaowocuje w najbliższej przyszłości pojawieniem się tych podmiotów oraz generowanych przez nich zagrożeń u granic euro-atlantyckiej wspólnoty. Innymi słowy, podejmując decyzję o interwencji zbrojnej w Mali, Afganistanie, czy Czadzie przywódcy polityczni oraz szefowie sił zbrojnych Stanów Zjednoczonych Ameryki, Kanady, Francji, Wielkiej Brytanii, stali na stanowisku, że nie należy pozwalać na bezkarny wzrost wpływów sił zmierzających do destabilizacji współczesnego świata. Nie można tolerować bezkarnej aktywności radykalnych podmiotów religijnych, czy politycznych, których istotą aktywności jest przemoc zbrojna.

Niepowodzenie, czy wręcz klęska, zakrojonych na szeroką skalę działań stabilizacyjnych w Afganistanie oraz Iraku, w których uczestniczyły niemal wszystkie

mocarstwa „zachodniego świata", zaowocowały dość poważnym odejściem rządów większości państw Unii Europejskiej i NATO od wcześniejszej, relatywnie aktywnej polityki reagowania na wszelkie przejawy destabilizacji systemu bezpieczeństwa międzynarodowego. Poczynając od Stanów Zjednoczonych Ameryki, poprzez Polskę, a skończywszy na Danii i Nowej Zelandii, wszystkie liczące się podmioty globalnego bezpieczeństwa, zdecydowały się skupić w drugiej dekadzie XXI wieku przede wszystkim na ochronie własnych, narodowych (często wąsko definiowanych) interesów oraz na rozwoju zdolności militarnych ściśle podporządkowanych własnym potrzebom oraz uwarunkowaniom w dziedzinie obronności. Priorytetem dla państw w polityce bezpieczeństwa (szczególnie bezpieczeństwa militarnego) stało się stworzenie podstaw (organizacyjnych, technologicznych, doktrynalnych) dla ochrony i obrony przed zagrożeniami mającymi charakter bezpośredni, czyli generowanymi przez wrogie im podmioty w ich środowisku bezpieczeństwa.

Celem niniejszej publikacji stało się poszukiwanie odpowiedzi na pytanie, w jaki sposób współczesne państwa przygotowują się do ochrony i obrony przed różnymi rodzajami zagrożeń i wyzwań (przede wszystkim o charakterze militarnym). Do współpracy przy tworzeniu książki zaproszono badaczy, którzy z bardzo różnych perspektyw analizują i opisują politykę bezpieczeństwa oraz politykę obronną współczesnych państw. Chodziło o to, aby prowadzone na jej kartach rozważania i dociekania osadzone zostały w możliwie szerokiej perspektywie poznawczej. Pamiętać bowiem należy, że aby poznać i zrozumieć cele, założenia, metody czy środki współczesnej polityki bezpieczeństwa, także polityki obronności, poszczególnych państw lub ugrupowań, konieczne jest spojrzenie wielowymiarowe, uwzględniające: charakter zagrożeń, założenia doktrynalne, uwarunkowania geopolityczne i geostrategiczne, posiadane przez państwo siły i środki militarne, możliwości technologiczne, powiązania instytucjonalne. W rezultacie czytelnik znajdzie w poszczególnych rozdziałach rozważania dotyczące bardzo różnych, często jak mogłoby się wydawać – całkowicie odmiennych, aspektów bezpieczeństwa, takich, jak np. polityka bezpieczeństwa energetycznego Polski i Unii Europejskiej, doktryna użycia sił w operacjach połączonych, założenia szwedzkiej polityki obronnej, nowoczesne formy walki elektronicznej, nowoczesne technologie w działaniach zbrojnych, ochrona systemów cybernetycznych oraz systemów komputerowych przed wrogimi działaniami o charakterze destrukcyjnym.

Lektura poszczególnych tytułów rozdziałów ukazuje w sposób niepodważalny, jak głęboka zmiana dokonała się u progu trzeciej dekady XXI wieku w sposobie postrzegania bezpieczeństwa narodowego i międzynarodowego oraz w procesie doboru środków i metod obrony i ochrony przez aktualnymi i przyszłymi zagrożeniami. Państwo współczesne pozostaje jedynym podmiotem zdolnym do skutecznego podjęcia zorganizowanych działań zbrojnych, nie tylko w przypadku

zbrojnej wrogiej agresji – stanu wojny, ale także w celu przeciwdziałania innym rodzajom zagrożeń militarnych, takich jak np. działania hybrydowe, terroryzm, aktywność radykalnych ruchów polityczno-religijnych. Z tej właśnie przyczyny także wiele uwagi w publikacji poświęcono wybranym problemom planowania, kierowania, dowodzenia oraz użycia sił zbrojnych. Co jednak interesujące, jak się wydaje, nie wystarczy już dziś, aby państwo dysponowało odpowiednio licznymi i właściwie wyposażonymi sprzętowo siłami zbrojnymi. Kluczowym czynnikiem decydującym o powodzeniu wszelkich operacji wojskowych, których celem jest zwalczanie różnorodnych zagrożeń (przybierających formę terroryzmu, piractwa morskiego, operacji niejawnych formacji wojskowych) dla systemu bezpieczeństwa międzynarodowego, okazuje się być nie ilość i jakość sił i środków bojowych, a umiejętność zintegrowania ich w sprawny, funkcjonalny organizm, a następnie efektywne kierowanie i dowodzenie tym organizmem.

Należy jednak zwrócić uwagę na fakt, że bezpieczeństwo współczesnych państw i społeczeństw determinowane jest w coraz większym stopniu przez zagrożenia pojawiające się w sferze wirtualnej, atakujące systemy komputerowe i sieci cyfrowe. Wreszcie, nie powinniśmy lekceważyć kolejnego, bardzo poważnego zagrożenia dla stabilności współczesnych państw oraz funkcjonowania ich gospodarek. Mowa oczywiście o zagrożeniach związanych z zakłóceniami w dostępie do energii. Autorzy poszczególnych rozdziałów, dotyczących tych zagadnień, w sposób bardzo wnikliwy, wszechstronny oraz interesujący przybliżają czytelnikowi te niemilitarne, acz bardzo ważne, wymiary współczesnego bezpieczeństwa.

W żadnej publikacji, nawet najbardziej obszernej, nie jest możliwe wyczerpanie wszystkich wątków, pełne rozwinięcie wszystkich podniesionych tez czy hipotez. Książkę traktować należy jako autorski wkład grupy autorów, będących specjalistami i ekspertami w obrębie wybranych aspektów badawczych, do dyskusji na temat współczesności i przyszłości działań państw i organizacji międzynarodowych na rzecz bezpieczeństwa międzynarodowego. Autorzy oraz redaktorzy tomu żywią głęboką nadzieję, że aktualne treści oraz interesująca ich prezentacja w ramach poszczególnych rozdziałów pozwolą czytelnikowi na lepsze poznanie i zrozumienie, w jakim kierunku zmierza polityka bezpieczeństwa współczesnych państw oraz jakie formy ona przybiera.

Książka zawiera czternaście artykułów, które zostały przygotowane zarówno przez przedstawicieli polskich ośrodków akademickich, jak i pracowników polskiego sektora przemysłu obronnego. Na jej treść składają się teksty poświęcone różnorodnym zagadnieniom. Niejednokrotnie bardzo specjalistyczne, ale zawsze stanowiące ważny wkład w trwającą w świecie naukowych dyskusję dotycząca kierunków ewolucji i stanu bezpieczeństwa międzynarodowego. W pracy odnaleźć można studia dotyczące globalnych trendów w cyberbezpieczeństwie oraz opracowania na temat cyberterroryzmu jako przykładu zagrożenia asymetrycz-

nego. Interesującym i wartościowym uzupełnieniem rozważań odnoszących się do cybernetycznego wymiaru bezpieczeństwa narodowego i międzynarodowego jest bez wątpienia tekst pracowników firmy TELDAT, prezentujący polską myśl technologiczną w zakresie przetwarzania i transmisji danych w operacjach międzynarodowych.

Wiele uwagi poświęcono na łamach części tekstów problematyce uwarunkowań bezpieczeństwa oraz polityki bezpieczeństwa Polski. Do tej grupy opracowań zaliczyć możemy teksty traktujące o: prawnych aspektach polityki bezpieczeństwa RP w kontekście zatrudnienia cudzoziemców, znaczeniu Ministerstwa Energii dla polityki bezpieczeństwa energetycznego Polski, kierunkach współpracy polityczno-wojskowej Polski w XXI wieku.

Do współpracy w przygotowaniu niniejszego tomu udało się także zaprosić wybitnych znawców problematyki bezpieczeństwa militarnego, także ekspertów w zakresie obronności. W rezultacie rozważania dotyczące znaczenia siły militarnej dla współczesnego ładu i porządku międzynarodowego zajmują szczególne miejsce w książce. Analizie poddane zostały między innymi takie kwestie, jak: rola korpusu w strukturach organizacyjnych Wojska Polskiego, system bezpieczeństwa międzynarodowego w świetle przyszłych wojen, znaczenie połączonego wsparcia ogniowego dla powodzenia operacji wojskowych, rola szwedzkiej stacjonarnej artylerii nadbrzeżnej w systemie obronnych Królestwa Szwecji, międzynarodowe zaangażowanie militarne Królestwa Danii, zasady i środowisko walki elektronicznej oraz teoria walki zbrojnej.

Redaktorzy:
Jarosław Wołejszo
Grzegorz Rdzanek
Anna Zagórska

Łukasz Apiecionek*
Robert Palka*
Mateusz Biedziak*
Maciej Tomczak*
Marcin Woźniak*
Piotr Brążkiewicz*

NOWOCZESNE TECHNOLOGIE PRZETWARZANIA I TRANSMISJI DANYCH W OPERACJACH MIĘDZYNARODOWYCH

Streszczenie

W dobie dzisiejszego przepływu informacji, wiadomości o zdarzeniach na świecie przenikają do informacji publicznej bardzo szybko, m.in. poprzez sieć Internet. Również informacje o efektach prowadzonych operacji międzynarodowych przenikają szybko do świadomości społeczeństwa. Dlatego ważnym aspektem ich prowadzenia jest uzyskanie dużej efektywności. W celu uzyskania dużej skuteczności wojska, policji, czy innych służb publicznych konieczne jest zapewnienie szybkiego przepływu informacji do budowy świadomości sytuacyjnej – o stanie jednostki, jej położeniu, siłach i środkach. Do tego potrzeba jednak odpowiednich narzędzi. W artykule przedstawiono nowoczesne technologie transmisji danych w postaci sieci 5G, technologii zwielokrotnienia transmisji danych MPTCP oraz urządzeń mobilnych zdolnych do jej wykorzystania.

Słowa kluczowe: urządzenia mobilne, transmisja danych, sieci 5G, MPTCP

* Dr inż. Łukasz Apiecionek, mgr inż. Robert Palka, inż. Mateusz Biedziak, inż. Maciej Tomczak, mgr inż. Marcin Woźniak, mgr inż. Piotr Brążkiewicz, TELDAT Sp. z o.o. sp.k., ul. Cicha 19-27, 85-650 Bydgoszcz

1. Wstęp

W dobie dzisiejszego przepływu informacji, wiadomości o zdarzeniach na świecie przenikają do informacji publicznej bardzo szybko. Sieć Internet stała się głównym nośnikiem informacji, dzięki któremu dana wiadomość może dotrzeć do praktycznie każdego miejsca. W rezultacie opinia publiczna uzyskała szybki dostęp do informacji, a jednocześnie istnieje możliwość wpływania na jej opinię za pomocą informacji umieszczanych w sieci. Również informacje o efektach prowadzonych operacji międzynarodowych przenikają szybko do świadomości społeczeństwa. Dlatego ważnym aspektem ich prowadzenia jest uzyskanie dużej efektywności. Społeczeństwo oczekuje szybkiego i efektywnego działania służb, których misją jest zapewnienie wysokiego poziomu bezpieczeństwa. W celu uzyskania dużej skuteczności wojska, policji, czy innych służb publicznych, konieczne jest zapewnienie szybkiego przepływu informacji. Świadomość położenia, stanu i siły swoich środków oraz o statusie i fazie aktualnie prowadzonej operacji pozwalają uzyskać większą efektywność działania. Do tego potrzeba jednak odpowiednich narzędzi.

W dalszej części artykułu przedstawiono nowoczesne technologie transmisji danych w postaci sieci 5G, jak i urządzenia mobilne, które potrafią efektywnie z nich korzystać w celu przyspieszenia transmisji danych.

2. Nowoczesne technologie transmisji danych

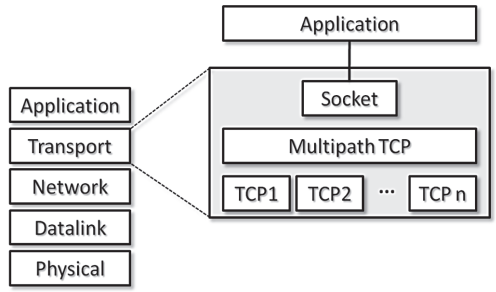
Obecnie najbardziej wyczekiwaną siecią pozwalającą na wykorzystanie nowej technologii transmisji danych jest sieć 5G. Z powodu dużych inwestycji operatorów w sieci GSM/3G/LTE, analitycy przewidują, że będzie to powodem opóźnienia wprowadzenia sieci 5G. Technicznie, transmisja w sieci piątej generacji będzie cechowała się następującymi parametrami[1]:

- opóźnieniem całkowitym (*end-to-end*) wynoszącym 1 milisekundę,
- zwiększeniem 1000 razy pasma na jednostkę zasięgu,
- od 10 do 100 razy większą liczbą urządzeń możliwych do podłączenia,
- zapewnienie dostępności sieci na poziomie 99,999%,
- 100% pokryciem terenu,
- 90% redukcją zapotrzebowania na energię,
- możliwością pracy na baterii (*dla urządzeń o niskim zapotrzebowaniu na prąd*) aż do roku.

[1] *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, gsmaintelligence.com, online 2016.08.15; *5G radio access*, Ericsson White paper, Uen 284 23-3204 Rev C, April 2016.

Spełnienie powyższych parametrów pracy pozwoli określić sieć, jako sieć 5G. Jedną z nowości wprowadzaną przez tę sieć będzie interfejs radiowy RADT[2]. Jedną z ważnych jego cech jest możliwość wykorzystania więcej niż jednego nadajnika/odbiornika. Tę technologię transmisji nazywa się MIMO[3]. Przewiduje się, że sieci 5G będą współdziałały z dotychczasowymi sieciami. Jako połączenia zapasowe planowane jest użycie właśnie dotychczasowych sieci wykorzystując protokoły Ethernet[4]. Takie rozwiązanie jest bardzo istotne ze względu na potrzeby sieci specjalnych, np. wojskowych, czy infrastruktur krytycznych, gdzie poziom dostępności sieci musi być najwyższy[5].

Jedną z istniejących technologii, którą można rozważyć do użycia w sieciach 5G, a która mogłaby wykorzystać technologię MIMO jest Multi Path TCP (*w skrócie MPTCP*)[6].



Rys. 1. Warstwy MPTCP

MPTCP pozwala na wykorzystanie istniejących połączeń do stworzenia jednego stabilnego łącza, którego prędkość transmisji danych może dochodzić do

---

2 *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, gsmaintelligence.com, online 2016.08.15; *View on 5G Architecture*, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15; *5G PPP use cases and performance evaluation models*, editors: Michał Maternia, Salah Eddine El Ayoubi, Version: 1.0, https://5g-ppp.eu, online 2015.08.15.

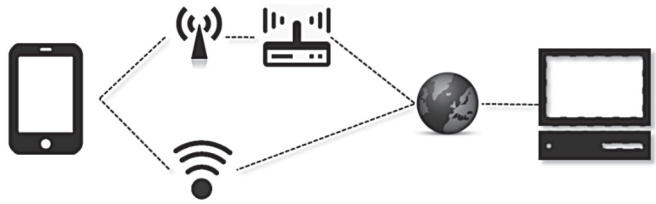
3 *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, gsmaintelligence.com, online 2016.08.15; *5G radio access*, Ericsson White paper, Uen 284 23-3204 Rev C, April 2016; *iew on 5G Architecture*, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15; *5G and Energy*, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15; *5G Automotive Vision*, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15.

4 *Understanding 5G: Perspectives on future technological advancements in mobile*, December 2014, gsmaintelligence.com, online 2016.08.15.

5 *5G and e-Health*, 5G-Infrastructure-Association, September 2015, www.5g-ppp.eu, online 2016.08.15.

6 U. Krieger, *Evolution of Transport Protocols in high-Speed Networks*, Lectures materials Multimedia-Kommunikation in Hochgeschwindigkeitsnetzen (KTR-MMK-M), 2014.

sumy prędkości uzyskiwanych niezależnie na poszczególnych łączach. MPTCP działa w warstwie transportowej modelu TCP i jest przezroczyste dla pozostałych warstw. W ramach swojej pracy otwiera wiele połączeń TCP, które są przez niekontrolowane. Zwiększa to znacząco przepustowość w danej warstwie. Przykładowo, urządzenia mobilne wyposażone w interfejsy Wi-Fi i LTE mogą np. utworzyć jedno stabilne łącze i uzyskać większą prędkość transmisji używając obu łączy jednocześnie, a nie na zmianę.



Rys. 2. Możliwość połączenia smartphone poprzez dwa łącza jednocześnie

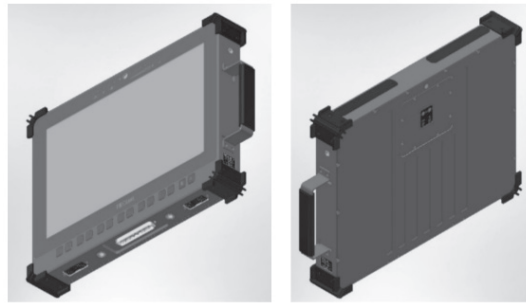
Pierwszym systemem mobilnym, który wspierał MPTCP[7] był iOS 7. Pozwalał on na otrzymanie połączenia w momencie, gdy któryś z interfejsów nie działał. Technologia ta była wykorzystywana do transmisji danych asystenta Siri (*oprogramowanie pełniące funkcję inteligentnego asystenta osobistego*)

3. Urządzenia mobilne o podwyższonej odporności środowiskowej

Aby jednak efektywnie korzystać z nowych technologii potrzebne są urządzenia, które to umożliwią. Firma TELDAT realizując projekt „*Wytworzenie rodziny innowacyjnych urządzeń typu tablet o podwyższonej odporności na warunki mechaniczne i klimatyczne, pozwalających efektywnie wykorzystać najnowsze technologie transmisji danych*" współfinansowany ze środków Narodowego Centrum Badań i Rozwoju, opracowuje właśnie takie rozwiązania. Celem projektu jest właśnie wytworzenie urządzeń typu tablet, które charakteryzować będzie wysoka mobilność (*długa praca na baterii, niska waga urządzenia*) oraz możliwość zastosowania w bardzo trudnych warunkach terenowych. Rezultat projektu będzie wypełniał braki w aktualnym zapotrzebowaniu na urządzenia o podwyższonej odporności. Bowiem obecnie na rynku polskim nie ma rozwiązań typu tablet tworzonych przez polskie przedsiębiorstwa, które jednocześnie spełniają wszystkie rygorystyczne kryteria Norm Obronnych.

---

[7] K.M. Schneider, K. Mast, U.R. Krieger, *Adapting Content-Centric Networking to the Characteristics of Multihomed Mobile Terminals*, 2014.



Rys. 3. Model 3D terminala 12 calowego

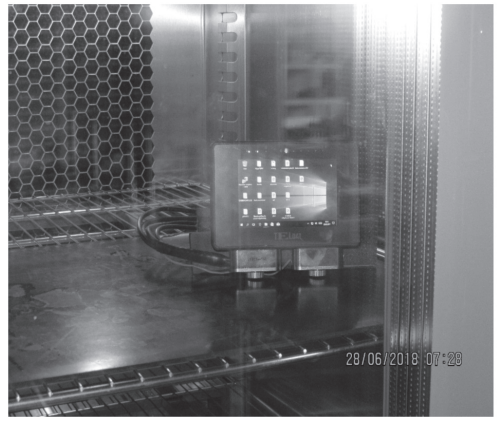
Projektowane urządzenia będą odporne na zapylenie, wstrząsy, wibracje oraz skutki upadku z wysokości 0,75 m na każdą płaszczyznę oraz naroża. Co ważne, norma obronna (*NO-06-A107*) definiująca tą odporność przewiduje, że urządzenie będzie wyłączone. Tymczasem podczas prowadzenia misji, czy realizacji zadań przez odpowiednie służby, żaden użytkownik nie będzie wyłączał urządzenia zanim wypadnie mu ono z ręki. Dlatego wytwarzane produkty będą testowane podczas normalnego działania. Ważnym aspektem jest fakt, że urządzenia te będą mogły przebywać i pracować do 1 m pod wodą, nawet do dwóch godzin.

Aby efektywnie wykorzystać najnowsze technologie transmisji danych, architektura rozwiązania jest tak projektowana, aby istniała możliwość jednoczesnego użycia wszystkich interfejsów transmisji danych, zwiększając szybkość i bezpieczeństwo przesyłanych informacji. W chwili obecnej często występują okoliczności, w których do transmisji danych można użyć kilku technologii, np. łączności 3G, LTE, czy łączności bezprzewodowej w standardzie 802.11 – Wi-Fi. Standardowe, aktualne rozwiązania wykorzystania tych łączy, w danej chwili bazują na wyborze najlepszego. Takie rozwiązania mogą często powodować utratę danych w momencie zerwania łącza, czyli np. utraty zasięgu przez sieć bezprzewodową Wi-Fi.

Dopiero po nawiązaniu połączenia np. LTE wraca możliwość transmisji danych. W przedstawianym rozwiązaniu opracowano i zaimplementowano możliwości jednoczesnej transmisji poprzez wszystkie dostępne łącza danych. Takie podejście pozwala na:

- zwiększenie pewności transmisji informacji – łączność jest utrzymywana niezależnie od chwilowych zaników sygnałów poszczególnych sieci,
- wzrost bezpieczeństwa transmisji informacji – dane są przesyłane przez różne ścieżki, co oznacza, że podsłuchanie jednej z nich nie pozwoli na przechwycenie całości informacji,
- zwiększenie szybkości przesyłania danych – dane przesyłane są poprzez wszystkie aktualnie dostępne łącza, co powoduje, że efektywne pasmo jest równe sumie pasm dostępnych łączy,

- niezależność od aplikacji – poprzez oddzielenie warstwy transmisji od warstwy oprogramowania istnieje możliwość wykorzystania aktualnie używanych aplikacji z nową technologią transmisji, bez konieczności modyfikacji dotychczasowego oprogramowania.



Rys. 4. Badanie modelu terminala 5 calowego
na wpływ wysokiej wilgotności w komorze klimatycznej

Tak zmodyfikowany system transmisji pozwala na zwiększenie możliwości zastosowań technologii mobilnych do:

- monitorowania zdarzeń i systemów: m.in. w ochronie mienia do przesyłania danych, informacji, obrazów video, w monitorowaniu linii produkcyjnych wysokiego ryzyka poprzez zapewnienie ciągłości przesyłania danych,
- systemów dla jednostek pożytku publicznego zapewniając stałą, pewną i szybką łączność w Systemach Zarządzania Kryzysowego, systemach SWD wspomagania dowodzenia Policji, Straży Pożarnej, karetek Pogotowia Ratunkowego,
- systemów dedykowanych dla Wojska poprzez zwiększenie pewności i szybkości przesyłanych danych do miejsc, gdzie zależy od tego ludzkie życie.

Ważną cechą proponowanego systemu łączności jest niezależność od aplikacji. Oddzielenie warstwy transmisji od warstwy aplikacji pozwala na skorzystanie z innowacyjnych funkcji urządzeń przez dowolne aplikacje, nawet te już istniejące. Możliwe jest więc użycie proponowanych tabletów na obecnym polu działania np. w operacjach międzynarodowych, gdzie zwiększy się pewność i szybkość przesyłania potrzebnych informacji bez konieczności modyfikacji istniejących systemów.

4. Wnioski

Obecnie prowadzone operacje międzynarodowe będą wymagać coraz większej efektywności, co można uzyskać poprzez zwiększenie szybkości i pewności przesyłania informacji. W tym celu konieczne jest wykorzystanie nowych technologii, takich jak sieci 5G. Jednak wymagają one odpowiednio przygotowanych urządzeń, które poza faktem posiadania interfejsów transmisji danych będą w stanie wykorzystać je wszystkie jednocześnie z pełną prędkością transmisji. Z pomocą tutaj idą opracowywane w firmie TELDAT modele urządzeń mobilnych typu tablet. Urządzenia te pozwolą wykorzystać wszystkie cechy nowych sieci dostarczając użytkownikom niezbędnego, pewnego i efektywnego narzędzia do realizacji jego celów.

Bibliografia

5G and e-Health, 5G-Infrastructure-Association, September 2015, www.5g-ppp.eu, online 2016.08.15.

5G and Energy, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15.

5G Automotive Vision, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15.

5G PPP Pre-standardisation Working Group, Lisbon, 20 October 2015, https://5g-ppp.eu, online 2015.08.15.

5G PPP use cases and performance evaluation models, editors: Michał Maternia, Salah Eddine El Ayoubi, Version: 1.0, https://5g-ppp.eu, online 2015.08.15.

5G radio access, Ericsson White paper, Uen 284 23-3204 Rev C, April 2016.

Krieger U., *Evolution of Transport Protocols in high-Speed Networks*, Lectures materials Multimedia-Kommunikation in Hochgeschwindigkeitsnetzen (KTR-MMK-M), 2014.

Schneider K.M., Mast K., Krieger U.R., *Adapting Content-Centric Networking to the Characteristics of Multihomed Mobile Terminals*, 2014.

Understanding 5G: Perspectives on future technological advancements in mobile, December 2014, gsmaintelligence.com, online 2016.08.15.

View on 5G Architecture, 5G PPP Architecture Working Group, https://5g-ppp.eu/white-papers/, online 2015.08.15.

MODERN TECHNOLOGIES IN DATAPROCESSING AND DATATRANSMISSION AS A PART OF INTERNATIONAL OPERATIONS

Summary

The aim of the article is to present and discuss some aspects of using modern technologies and technological solutions to command and control different kind of security operations. The emphasise is put mostly on some devices and systems, which are needed in the porcess of dataprocessing and datatransmission.

Keywords: mobile devices, datatransmission, 5G nets, MPTCP

Charakter współczesnych zagrożeń i wyzwań dla bezpieczeństwa międzynarodowego zmusza państwa do tworzenia, a następnie konsekwentnego pogłębiania, różnorodnych form wielostronnej współpracy o charakterze polityczno-militarnym. Proces instytucjonalizacji narodowych polityk bezpieczeństwa, w tym polityk obronnych, w formie wielonarodowych, wielopłaszczyznowych struktur i mechanizmów reagowania kryzysowego stał się w drugiej dekadzie XXI wieku jednym z najważniejszych wyznaczników rozwoju międzynarodowego systemu bezpieczeństwa. Celem publikacji jest przedstawienie, jak współczesne państwa próbują realizować narodowe interesy bezpieczeństwa w ramach różnorodnych form współpracy i współdziałania. W rozważaniach zawartych w książce nacisk położony został w pierwszej kolejności na różnorodne aspekty aktywności militarnej państwa, poczynając od działań bojowych sił zbrojnych w ramach operacji połączonych, a na zagranicznej pomocy wojskowej kończąc. Wiele miejsca poświęcono także innym zagadnieniom, takim, jak choćby: cyberbezpieczeństwo oraz bezpieczeństwo energetyczne.

Redaktorzy

ISBN 978-83-8017-292-0