Wojna hybrydowa – mit czy rzeczywistość

Zagrożenia bezpieczeństwa pozamilitarnego

Budowanie efektywnych zespołów ludzkich

PRZEGLĄD SIŁ ZBROJNYCH

Cena 10 zł (w tym 5% VAT)

nr 2 / 2019

marzec–kwiecień

WOJSKOWY INSTYTUT WYDAWNICZY

ISSN 2353-1975

POLSKA-ZBROJNA.PL

HISTORIA
POLSKA ZBROJNA

MAGAZYN O TRADYCJI I CHWALE
POLSKIEGO ORĘŻA

ZAMÓW PRENUMERATĘ
TEL. +48 261 840 400

WOJSKO POLSKIE

Twoja historia – Twoje życie!

Polecam!

Anna Putkiewicz, redaktor naczelna

Szanowni **Czytelnicy!**

WOJSKOWY INSTYTUT
WYDAWNICZY
Aleje Jerozolimskie 97
00-909 Warszawa
e-mail: psz@zbrojni.pl

Dyrektor Wojskowego
Instytutu Wydawniczego:
MACIEJ PODCZASKI
e-mail: sekretariat@zbrojni.pl
tel.: 261 845 365, 261 845 685
faks: 261 845 503

Redaktor naczelny:
IZABELA BORAŃSKA-CHMIELEWSKA
tel.: 261 840 222
e-mail: ibc@zbrojni.pl

Redaktor wydawniczy:
KRZYSZTOF WILEWSKI
tel.: 261 845 186

Redaktor prowadzący:
płk w st. spocz. dr JAN BRZOZOWSKI
tel.: 261 845 186

Opracowanie redakcyjne:
MARYLA JANOWSKA,
KATARZYNA KOCOŃ

Opracowanie graficzne:
WYDZIAŁ SKŁADU
KOMPUTEROWEGO I GRAFIKI WIW

Opracowanie infografik:
PAWEŁ KĘPKA

Kolportaż:
POCZTA POLSKA
USŁUGI CYFROWE sp. z o.o.
ul. Duninowska 9a, 87-823 Włocławek
tel.: 542 315 201, 502 012 187
e-mail:
elzbieta.kurlapska@poczta-polska.pl

Druk: Wojskowe Zakłady Kartograficzne
WZKart sp. z o.o.
ul. Fort Wola 22 bud. 16,
01-258 Warszawa

Zdjęcie na okładce:
IPOPBA/FOTOLIA

Zasady przekazywania redakcji magazynu „Przegląd Sił Zbrojnych" materiałów tekstowych i graficznych opisuje regulamin dostępny na stronie głównej portalu polska-zbrojna.pl.

Krzysztof Wilewski

Kiedy wczesną wiosną albo późną zimą – jak kto woli – 2014 roku na Półwyspie Krymskim pojawili się rosyjscy żołnierze w mundurach nie tylko bez oznaczenia stopni, lecz także bez oznak jednostek, z jakich pochodzą oraz jaki kraj reprezentują, szybko ukuto powiedzenie, że są to tzw. zielone ludziki. Gdy cały świat nie miał wątpliwości, że są to żołnierze Federacji Rosyjskiej, prezydent tego kraju zaprzeczał, argumentując, iż tego typu uniformy można kupić w każdym sklepie z mundurami. A czołgi? Bojowe wozy piechoty? Wyrzutnie pocisków rakietowych Grad? Żołnierze mieli je „bezprawnie pożyczyć". Zapewne na urlopy, na które – jak można było sądzić na podstawie komunikatów z Moskwy – niekiedy udawały się na Ukrainę całe rosyjskie pododdziały.

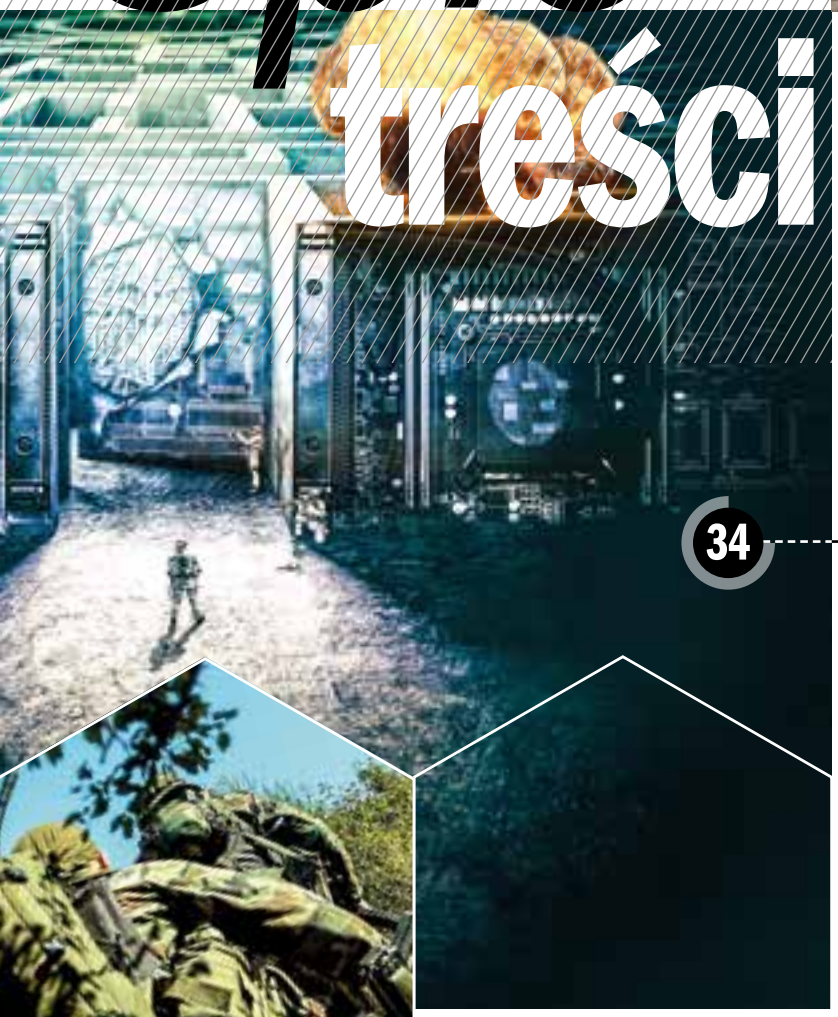
Bardzo szybko media, na wzór niektórych ekspertów, zaczęły nazywać to, co się działo na Krymie, a później na wschodzie Ukrainy, wojną hybrydową. Czy jest to właściwe określenie? Na to pytanie, jedno z wielu związanych z zagrożeniami hybrydowymi oraz działaniami poniżej progu wojny, mam nadzieję – znajdą Państwo odpowiedź w tym numerze „Przeglądu Sił Zbrojnych".

Przygotowaliśmy bowiem aż dziesięć artykułów poświęconych hybrydzie – etymologii tego terminu, charakterystyce zjawiska i odmianom oraz wyzwaniom, jakie stawia przed armią i systemem bezpieczeństwa państwa. Prof. dr hab. inż. Jarosław Wołejszo oraz dr inż. Konrad Malasiewicz uważnie przyjrzeli się historii hybrydowości konfliktów zbrojnych, a ppłk dr Piotr Haręźlak nowemu postrzeganiu wojny hybrydowej. Ppłk dr inż. Norbert Świętochowski zastanawia się, czy ta forma konfliktu stanowi realne zagrożenie dla bezpieczeństwa naszego państwa. Ppłk dr inż. Robert Janczewski analizuje cyberprzestrzeń jako część teatru działań hybrydowych. Ppłk dr Zbigniew Modrzejewski pochyla się nad problemem działań informacyjnych w konflikcie hybrydowym. Kmdr por. Jarosław Keplin oraz ppłk Cezary Pawlak zajmują się genezą działań hybrydowych. Mjr dr Ryszard Kalisiak opisuje użycie pododdziałów lekkich do neutralizowania zagrożeń hybrydowych. Zagadnieniu działań poniżej progu wojny zostały poświęcone również trzy nagrodzone przez redakcję artykuły młodych adeptów sztuki wojennej – majorów dyplomowanych SZRP Grzegorza Otockiego, Mariusza Wojtczyka i Pawła Kowalczyka.

Serdecznie zachęcam do lektury

nr 2 / 2019

Spis treści



TEMAT NUMERU: DZIAŁANIA HYBRYDOWE

KONKURS – NAJLEPSZY ARTYKUŁ

SZKOLENIE

LOGISTYKA

DOŚWIADCZENIA

KONKURS

W NINIEJSZYM NUMERZE ZAMIESZCZONO KOLEJNE PRACE, KTÓRE WPŁYNĘŁY NA KONKURS.

PRACE MODERNIZACYJNE MIAŁY NA CELU ZWIĘKSZENIE ODPORNOŚCI BALISTYCZNEJ CZOŁGU ORAZ UDOSKONALENIE JEGO SYSTEMÓW OBSERWACYJNYCH.

CZOŁG BĘDZIE DYSPONOWAŁ M.IN.: TERMOWIZYJNYMI PRZYRZĄDAMI OBSERWACYJNO-CELOWNICZYMI EMES-15, KLW-1 ASTERIA I KDN-1T NYKS, NOWYM SYSTEMEM KIEROWANIA OGNIEM ORAZ SYSTEMEM OBROTU WIEŻY I ELEWACJI ARMATY EWNA, A TAKŻE WZMOCNIONYM OPANCERZENIEM WIEŻOWYM, ZMODERNIZOWANYM SYSTEMEM PRZECIWPOŻAROWYM W PRZEDZIALE NAPĘDOWYM I PRZECIWWYBUCHOWYM W PRZEDZIALE ZAŁOGI.

RHEINMETALL PK/DZIAŁ GRAFICZNY

LEOPARD 2PL

Wojna hybrydowa – **mit czy rzeczywistość**

WOJNY MAJĄ SWOJE NAZWY. JEDNE SĄ ZWIĄZANE Z MIEJSCEM PROWADZENIA DZIAŁAŃ WOJENNYCH. INNE PODKREŚLAJĄ JEDNĄ LUB DWIE STRONY ZAANGAŻOWANE W WALKĘ.

płk rez. prof. dr hab. inż. Jarosław Wołejszo, płk rez. dr inż. Konrad Malasiewicz

Jarosław Wołejszo jest kierownikiem Katedry Zarządzania i Dowodzenia na Wydziale Nauk Społecznych i Humanistycznych Państwowej Wyższej Szkoły Zawodowej w Kaliszu.

Konrad Malasiewicz jest pracownikiem Wydziału Nauk Społecznych i Humanistycznych Państwowej Wyższej Szkoły Zawodowej w Kaliszu.

Prawa i zasady w nauce rozumiane są niejednoznacznie. W istocie rzeczy, gdybyśmy potraktowali prawo (w sensie naukowym) jako zbiór twierdzeń zasadniczych dla danego zjawiska, to twierdzenia takie znajdziemy we wszystkich częściach naszych rozpatrywań. W rozumieniu praw i zasad zastosujemy więc leksykalne podejście, uznając prawa jako [...] *zasady, prawidłowości rządzące światem, procesami przyrodniczymi i społecznymi, stanowiące cel badań naukowych* [...]. Zasada zaś to teza [...], *w której treści zawarte jest prawo rządzące jakimiś procesami; podstawa, na której coś się opiera, reguła*[2].

ZJAWISKO WOJNY

Prawa walki zbrojnej nie są jednoznaczne i w literaturze nie znalazły wystarczającego odzwierciedlenia. Zazwyczaj podkreśla się, iż mają one charakter obiektywny oraz zostały w historii zweryfikowane i potwierdzone. Zwykle też odzwierciedlają związki i zależności między wojną a podstawowymi czynnikami decydującymi o jej przebiegu i końcowym rezultacie. Najczęściej wyróżnia się dwa podstawowe prawa wojny: zależności wojny od polityki oraz prawo zależności wojny od potencjału wojennego państwa i od stosunku między potencjałami walczących stron.

Pierwsze z wymienionych praw (uznawane często za podstawowe) jest pochodną clausewitzowskiego ujęcia wojny. Wynika z niego bowiem, iż wojna, będąc kontynuacją polityki państwa prowadzonej środkami przemocy, jest od niej bezwzględnie uzależniona. Polityczna treść wojny odzwierciedla wszakże jej charakter, wywierając również wpływ na formy i metody jej prowadzenia. Polityka określa bowiem także doktrynę wojenną państwa (koalicji), formułując jej podstawowe założenia i priorytety. Zależności i związki polityki z walką zbrojną stanowią często o zasięgu przestrzennym, roli i zadaniach sił zbrojnych oraz sposobach prowadzenia walki zbrojnej. Zauważyć przy tym należy, iż prawo to funkcjonowało w niepełnym obszarze rozumienia wojny i walki zbrojnej. Dotyczyło w gruncie rzeczy wojen między państwami. Nie uwzględniało natomiast koalicji oraz wszelkich walk zbrojnych występujących w różnych rzeczywistościach społecznych. W nowym ujęciu powinno się odnosić raczej do geopolityki i uwzględniać politykę przyjętych układów międzynarodowych.

Bardziej wszechstronne jest drugie z wymienionych praw – prawo zależności wojny od potencjału wojennego państwa i od stosunku między potencjałami walczących stron, ujmowane często bardziej wąsko jako prawo zależności przebiegu i wyniku wojny od stosunku między potencjałami wojennymi walczących stron. Podstawowe twierdzenia tego prawa możemy współcześnie ująć następująco: przebieg i wynik walki zbrojnej zależą od stosunku między potencjałami wojennymi walczących stron obejmującymi: siły militarne, ekonomikę, technikę, stosunki społeczne oraz stan moralny i psychologiczny. W aspekcie

[1] *Słownik języka polskiego,* Warszawa 1979, t. 2.
[2] Ibidem, t. 3.

WALCZY TYLKO CZŁOWIEK, GDYŻ TYLKO ON JEST ZDOLNY OKREŚLAĆ CELE WALKI I TYLKO ON MOŻE WALCZYĆ ROZUMNIE.

US DOD

tego można powiedzieć, iż tylko strona posiadająca przewagę w tych obszarach (elementach) może osiągnąć zakładane cele, których efektem jest zwycięstwo. Naturalnie kwestii tej nie należy rozumieć jednoznacznie. Często bowiem w niektórych walkach do osiągnięcia zwycięstwa wystarczy przewaga jednego lub dwóch elementów.

Stanisław Koziej[3] przyjmuje, za W. Sawkinem, dwa prawa walki zbrojnej: sposoby i formy walki zbrojnej zależą od materialnej podstawy walki i operacji[4] oraz wszelka walka lub operacja, w każdym poszczególnym momencie swego rozwoju, działa na korzyść tej strony walczącej, której wojska dysponują większą siłą bojową niż przeciwnik[5]. Pierwsze z wymienionych praw często jest interpretowane – i z tym należy się zgodzić – jako prawo zależności walki zbrojnej od środków technicznych. Drugie zaś wskazuje, iż rezultat walki zbrojnej zależy od stosunku siły bojowej. Co prawda siła bojowa jest tu rozumiana dość szeroko (jako jedność środków materialnych i sił duchowych wojsk, jedność ich aspektów ilościowych i jakościowych), ale w rzeczywistości (w praktyce) stosowano jedynie materialny stosunek sił, co nie odzwierciedlało mechanizmu walki.

W kontekście zaprezentowanych rozważań wojna jako pojęcie naukowe nie jest precyzyjnie zdefiniowana. Co więcej, w różnych obszarach wiedzy dorobiła się swoistych stanowisk naukowych, mieszczących się w granicach od purytańskiego podejścia metodologicznego do naukowego eklektyzmu, próbującego łączyć w całość różnorodne idee i doktryny[6]. Ostatnim przykładem takiego braku precyzji są nieporozumienia związane z treściami i zakresem takich pojęć, jak *wojna* i *konflikt zbrojny*. Wojna jest jednak ważnym terminem nauk społecznych i jednym z podstawowych pojęć nauk o obronności. Sprawdźmy, czy można z niej wyspecyfikować cechy szczegółowe mogące precyzować jego treść. Analizę rozpocznijmy od słowników. Według internetowego *Słownika języka polskiego*, wojna to *zorganizowana walka zbrojna między państwami, narodami lub grupami społecznymi, religijnymi itp., prowadzona dla osiągnięcia zamierzonych celów (np. zagarnięcia obcego terytorium lub obrony własnego); konflikt zbrojny*[7]. W słowniku tym, poza przytoczeniem rodzajów wojny, dodatkowo nadmienia się, że w formie przenośnej słowo to oznacza również kłótnie, spory, awantury i bójki[8].

U Sun-Tzu termin *wojna* jest kategorią służącą do opisywania sporów prowadzonych w skali państwa, rozstrzyganych przy użyciu oręża; termin *walka* jawi się jako podstawowa kategoria wojny i oznacza wszelkie działania armii na wojnie; termin *bitwa* to podstawowa kategoria walki i oznacza bezpośrednie starcie wojsk; *zwycięstwo* zaś to pojęcie, którym autor wartościuje sukces w wojnie i bitwie.

Cechy szczegółowe wojny, które jesteśmy w stanie wskazać, dotyczą w zasadzie:

– równoważności pojęć: *wojna*, *zorganizowana walka zbrojna* i *konflikt zbrojny*;

– wiodącej roli podmiotów społecznych prowadzących wojnę i zamierzonych przez nie celów;

– przenośnego znaczenia wojny w stosunku do kłótni, sporów, awantur i bójek.

Dodatkowo w zakresie rodzajów wojen możemy zauważyć cechy związane z charakterem działań stron (wojna zaczepna, obronna, błyskawiczna, pozycyjna, partyzancka itp.), użytymi środkami (wojna atomowa, biologiczna, chemiczna itp.) i stanami funkcjonowania społeczeństw (wojna religijna, zimna wojna). Przyjmujemy również, iż termin *walka*, w rozumieniu naukowym, pojawił się w 1908 roku, a użył go Emanuel Lasker w pracy *Der Kampf*[9].

Nie sposób zaprzeczyć, iż ogólną teorię walki opracował Tadeusz Kotarbiński i przedstawił ją w studium prakseologicznym pt. *Z zagadnień ogólnej teorii walki*. Zdefiniował w nim najogólniejsze pojęcie *walki*, określił miejsce ogólnej teorii walki na drabinie uogólnień oraz omówił praktyczne dyrektywy w walce, tzw. mistrzowskie chwyty. Studium T. Kotarbińskiego wyzwoliło aktywność twórczą u wielu badaczy z obszaru prakseologii, cybernetyki, sztuki wojennej, filozofii, psychologii, socjologii, teorii gier i dyscyplin sportowych.

Identyfikowanie pojęcia walki jako skupionego w czasie i przestrzeni starcia dwóch przeciwstawnych stron w skali taktycznej[10] zmierza z jednej strony do uwzględnienia w tej kategorii taksonomicznej dwóch, a obecnie nawet większej liczby podmiotów, z drugiej zaś wyraźnie wskazuje na pozostawanie tych podmiotów w pewnej wzajemnej korelacji. Walka łączy i integruje w działaniu co najmniej dwa podmioty, chociaż są to działania przeciwbieżne. S. Koziej podkreśla, że walka to: *bezpośrednie starcie zgrupowań wojsk, wzajemne destrukcyjne oddziaływanie za pomocą posiadanych środków rażenia, to przede wszystkim fizyczne niszczenie i psychologiczne obezwładnianie przeciwnika, jako przeszkody na drodze do celu*[11].

---

[3] S. Koziej: *Teoria sztuki wojennej.* Warszawa 1993, s. 68.

[4] W. Sawkin: *Podstawowe zasady sztuki operacyjnej i taktyki,* Warszawa 1974, s. 138.

[5] Ibidem, s. 153.

[6] J. Reginia-Zacharski: *Wojna w świecie współczesnym. Uczestnicy. Cele. Modele. Teorie*. Łódź 2014, s. 125–128.

[7] https://sjp.pl/wojna/.25.05.2018.

[8] *Słownik języka polskiego.* T. III. Warszawa 1989, s. 744–745.

[9] E. Lasker: *Der Kampf* . Nowy Jork 1908.

[10] *Leksykon wiedzy wojskowej.* Wyd. MON, Warszawa 1979.

[11] S. Koziej: *Teoria sztuki*..., op.cit., s. 16.

Obydwa pojęcia, tj. *ujęcie systemowe* i *walka*, nie należą do tego samego zbioru semantycznego, gdyż termin *system* postrzega się strukturalnie i funkcjonalnie tylko w ujęciu jednej ze stron, a walkę zbrojną identyfikujemy wielopodmiotowo i dwu- lub wielostronnie. W rozumieniu walki zbrojnej mówi się o działaniach przeciwstawnych systemów, a nie jednego nadrzędnego systemu (nadsystemu).

Bardzo przydatne do formułowania twierdzeń dla walki zbrojnej są dociekania prakseologiczne. Prakseologia zajmuje się badaniem warunków sprawności działań. Jednym z jej działów jest ogólna teoria walki (agonistyka), która rozpatruje wszelkie rodzaje walki i postrzega je jako pewnego rodzaju współdziałanie, kooperację negatywną przynajmniej dwóch sprawców, z których każdy stara się osiągnąć cel niezgodny z celem drugiego, przy czym wie o działaniu przeciwnika i przeciwdziała mu. Walką w rozumieniu prakseologii jest zarówno gra w szachy czy inne formy rywalizacji sportowej, jak też współzawodnictwo naukowe czy artystyczne oraz wszelkie formy sporów i dyskusji między podmiotami i zespołami (erystyka: sztuka prowadzenia sporów i przekonywania przeciwników), a także walka zbrojna. W ujęciu prakseologii walka to *splot działań różnych osób lub zespołów osób, kiedy cele działających są niezgodne i jedni drugim usiłują przeszkodzić w dążeniach. Każdy, jeśli walczy rozumnie, chce się znaleźć w pozycji dodatniej względem celu walki i zabiega o to w miarę sił, by przeciwnik znalazł się w pozycji jak najbardziej ujemnej*[12].

Zauważamy rzecz znamienną, walczy tylko człowiek, gdyż tylko on jest zdolny określać cele walki i tylko on może walczyć rozumnie. Istotą walki jest przeszkadzanie przeciwnikowi w osiąganiu stawianych celów. Jest to relacja dwukierunkowa: podmiot A odpowiada podmiotowi przeciwstawnym działaniem, np. na atak odpowiada obroną, na wycofanie się przeciwnika – pościgiem, na rażenie – rażeniem, a wszystko to czyni w miarę swoich możliwości.

Postrzeganie walki jako *splotu działań różnych osób lub zespołów osób* wskazuje, że jest ona pasmem czynów prostych i złożonych, charakteryzujących się celowym zachowaniem podmiotów lub zespołów osób w określonym czasie, przestrzeni i otoczeniu społecznym. By dany zbiór czynów stał się czynem złożonym, trzeba, zdaniem T. Kotarbińskiego, *aby między jego członami zachodził stosunek pozytywnej lub negatywnej kooperacji, a dwie czynności złączone są takim stosunkiem zawsze i tylko, jeżeli jedną z nich druga powoduje, umożliwia, albo gdy obie tak się mają względem jakiejś* trzeciej[13].

W poszukiwaniu wyjaśnień tego faktu wielu autorów odwołuje się do podstawowych kanonów teorii sztuki wojennej. Wydaje się to oczywiste, gdyż postulat mistrzostwa w walce nakazuje wprost opierać się na *najdojrzalszych przepisach sprawnego postępowania.* Zalecają one wprost: [...] *Chcesz osiągnąć cechę B w dowolnym tworzywie? Wykryj takie A, któremu by to B wedle jakiegoś przyrodzonego prawa towarzyszyło stale i odwracalnie, czyli w sposób, nadający się do ujęcia za pomocą zdania adekwatnego. Więc i na temat dzielnej walki, ważną jest rzeczą wiedzieć, co już z takim właśnie układem działań wiąże się swoiście, by uświadomić sobie stopień ogólności tych reguł* [...][14]. Co istotne i na co zwraca uwagę T. Kotarbiński, to fakt, iż *pewne reguły powodzenia w walce nie są związane z walką jako taką, lecz czerpią swą zasadność z ogólnych cech dzielnego czynu jako takiego*[15].

Z pewnością w każdej refleksji o walce muszą się pojawić pytania o: przygotowanie i sprawność działania oraz kierunek i sposób postępowania walczących zespołów (zalecany ze względu na pożądane lub niepożądane skutki). Walka zbrojna jest zdarzeniem celowym i podmiotowym. Ujmując problem syntetycznie, możemy powiedzieć, że jej nośnikiem jest człowiek, ponieważ tylko on może określić jej cele, zakres i sposób działania, zakres i sposób wykorzystania rozporządzalnych sił i środków oraz reguły jej prowadzenia. Ponadto tylko człowiek jest w stanie zaplanować walkę, antycypować jej przebieg i występowanie zakłóceń oraz przewidywać jej skutki w otoczeniu mikro i makro. Walka zbrojna – co już powiedzieliśmy – jest również zjawiskiem społecznym, odpowiada bowiem na zapotrzebowanie społeczne i przebiega w rzeczywistości społecznej.

ZASADY WALKI

Możemy również powiedzieć, że strony w walce zbrojnej zmierzają do racjonalności. *Racjonalność*, jak twierdzi T. Kotarbiński, *pociąga za sobą rzeczowość, rzeczowość zaś – wobec pewnej sumy ważnych danych, obu przeciwnikom wiadomych – stwarza podstawy do przewidywania naszych rozumnych kroków. W podobnych sytuacjach będą one wypadały zapewne w sposób podobny. Rzeczowość łączy się wszak z pewną prawidłowością, pewną systematycznością, pewnym automatyzmem* [...][16]. Stwierdzenie to skłania do postawienia tezy, że walczące strony są zobowiązane działać w zasięgu swoich możliwości i wpływać na tok zdarzeń, albowiem nie można *pozwalać procesom od nas zależnym przebiegać nie wedle naszych zamierzeń*[17]. Muszą zatem pojawić się pytania doty-

[12] T. Kotarbiński: *Problematyka ogólnej teorii walki.* W: *Hasło dobrej roboty.* Warszawa 1968, s. 192.

[13] Idem: *Traktat o dobrej robocie.* Wrocław 1975, s. 67.

[14] Idem: *Z zagadnień ogólnej teorii walki.* Wydawnictwo Sekcji Psychologicznej Towarzystwa Wiedzy Wojskowej, s. 12.

[15] Ibidem, s. 13.

[16] Ibidem, s. 53.

[17] Idem: *Traktat o dobrej...*, op.cit., s. 146.

cące sposobu prowadzenia walki, a zatem muszą istnieć pewne zasady, dyrektywy, reguły, wskazówki pozwalające podjąć i rozwiązać problemy *w takich zawęźleniach działań* [...], *kiedy cele działających są niezgodne i jedni drugim usiłują przeszkodzić w dążeniach*[18]. Strony walki, w swym dążeniu do zwycięstwa, [...] *stawiają sobie cele, wiedzą to lub owo, liczą się z tym a tym w swych czynach*[19]. Odwołują się one ponadto do bazy teoretycznej (zasad sztuki wojennej), bazy technicznej (dyrektyw walki) i bazy instrumentalnej (obejmującej planowanie, organizowanie i działanie). Zasady są punktem wyjścia dla działań, od suje ciągle ten sam układ działania lub naśladuje innych, jest skazany z góry na klęskę.

Walka zbrojna opiera się na zasadach sztuki wojennej i dyrektywach praktycznych, wszystko inne zaś to kwestia improwizacji. Rzecz jednak w tym, zauważa T. Kotarbiński, iż *tajemnicą dobrej improwizacji jest dobre przygotowanie*[23], czyli osiągnięcie stanu kompetencji. Wyraża się on w postulacie mistrzostwa. Ten zaś nakazuje wprost: *W okolicznościach A trzeba (lub dobrze jest, lub wystarczy) zrobić B, by spowodować C*. W tej formule T. Kotarbiński wyróżnił trzy elementy (pojęcia): *trzeba*, *dobrze jest* i *wystarczy*. Poda-

WALKA TO BEZPOŚREDNIE STARCIE ZGRUPOWAŃ ODDZIAŁYWANIE ZA POMOCĄ WYTWORZONYCH

nich albowiem zaczyna się każde działanie. W ujęciu prakseologicznym zasada to ogólnie przyjęte twierdzenie (na podstawie oczywistości, doświadczenia) podające, jak jest w rzeczywistości, które może stanowić punkt wyjścia dla jakiegoś działania albo zaleca wprost, co robić, a czego nie robić[20].

W teorii sztuki wojennej stosowano różne podejścia do formułowania jej zasad. Stanowią je ogólne, naukowo uzasadnione twierdzenia, dotyczące prowadzenia walki na wszystkich szczeblach dowodzenia. Z tej racji mają obiektywny, uniwersalny i dynamiczny charakter. C. von Clausewitz zauważa, iż: *Zasada – jest dla działania pewnym prawem* [...]. *Jest ona tylko duchem i sensem prawa, aby tam, gdzie różnorodność świata rzeczywistego nie da się ująć w ostateczną formę prawną, zostawić naszemu sądowi więcej swobody w jej zastosowaniu*[21].

Wybór zasady czy ich łączenie w walce zbrojnej jest kwestią subiektywną. Jednak mówimy, że zasady sztuki wojennej obowiązują, a to z tej racji, iż zostały wyprowadzone z normy wyższej, tj. z praw walki zbrojnej. Warto też podkreślić, iż zasady sztuki wojennej [...] *nie dają się ująć w żadne instrukcje postępowania, ani przepisy regulaminu*[22]. Wydaje się to oczywiste, ponieważ są one kategorią ogólną. Z reguły są przywoływane w sytuacjach nietypowych, czyli takich, które nie mogą być przezwyciężone za pomocą rutynowych, wielokrotnie sprawdzonych sposobów działania. Zasady stanowią materiał dla podejmowania twórczych decyzji w walce zbrojnej. Ten, kto stoną formułę dyrektywy praktycznej T. Kotarbiński wyjaśnia następująco: *Mówiąc „trzeba", wskazujemy warunek w okolicznościach A niezbędny, czyli bez którego w tych okolicznościach nie może nastąpić C. Mówiąc „wystarczy" wskazujemy warunek w okolicznościach A wystarczający, czyli taki, że po jego dodaniu do tych okoliczności – C musi nastąpić. Mówiąc „dobrze jest", wskazujemy działanie, którego dodanie do okoliczności A czyni zajście C prawdopodobniejszym, niżby to było bez tego działania*[24]. Między elementami formuły zachodzi empiryczna zależność, bowiem wykonanie działania B spowoduje osiągnięcie celu C. Załóżmy, że wykonanie działania B jest warunkiem koniecznym osiągnięcia celu C, np. koniecznym warunkiem oddania celnego strzału jest zgranie muszki ze szczerbinką. Jeżeli go nie spełnimy, to nie trafimy w cel. Warunkiem wystarczającym będzie sprawna broń i amunicja, sprzyjającym zaś – wyszkolenie strzelca i warunki otoczenia.

Z kolei J. Zieleniewski dyrektywę praktyczną ujmuje w następującej formule teoretycznej: *Jeżeli w okolicznościach O podmiot działający P zachowa się w sposób Z, to spowoduje stan S rzeczy R pod względem W. Po jej przekształceniu otrzymamy następującą dyrektywę praktyczną: Jeżeli więc będąc P chcesz osiągnąć stan A rzeczy R pod względem W, w okolicznościach O, to zachowaj się w sposób Z*[25].

Dyrektywy praktyczne wskazują, co należy uczynić (nakazy i zalecenia), ale także czego robić nie

[18] Tenże: *Problematyka ogólnej teorii walki (autoryzowany wykład).* Warszawa 1963, s. 1.

[19] Tenże: *Z zagadnień ogólnej...*, op.cit., s. 7.

[20] T. Pszczołowski: *Mała encyklopedia prakseologii i teorii organizacji.* Wrocław-Warszawa-Kraków-Gdańsk, Ossolineum 1978, s. 290.

[21] C. v. Clausewitz: *O wojnie.* Warszawa 1958, s. 117.

[22] T. Wasilewski: *Pogląd na teorię sztuki wojennej.* Londyn 1954, s. 18.

[23] T. Kotarbiński: *Traktat o dobrej robocie*. Wrocław 1975, s. 172.

[24] Ibidem, s. 435.

[25] J. Zieleniewski: *System dyscyplin i metody nauk ergologicznych.* „Problemy Organizacji" 1968 nr 10.

należy (zakazy i przestrogi). Nakazy i zakazy praktyczne odnoszą się do warunków koniecznych lub dostatecznych, zalecenia i przestrogi zaś do warunków sprzyjających i prawdopodobnych zdarzeń zamierzonych jako cel, aby mogły być skuteczne. Dyrektywy praktyczne postrzegamy w kategoriach normy. Norma zawsze coś określa, na coś wskazuje, przed czymś przestrzega, coś zaleca lub zakazuje. Krótko mówiąc: określa, jak należy działać w warunkach sytuacji zadaniowej, by osiągnąć stanowiony cel. Tak też, jak można sądzić, podchodzono do wyodrębniania zasad sztuki wojennej.

WOJSK, WZAJEMNE DESTRUKCYJNE I POSIADANYCH ŚRODKÓW RAŻENIA

Dyrektywy praktyczne odnoszą się do: doboru konkretnego działania prowadzącego do zamierzonego celu w określonych warunkach, a także do wyznaczania i realizacji celu oraz wykorzystania warunków i działań.

Zdaniem K. Piłejko, dyrektywa praktyczna nakazuje, co i jak należy robić, aby sprawnie wykonać zadanie, dlatego też musi: odwoływać się do rzeczywistości; brać pod uwagę zależności przyczynowe; wskazywać na niezbędność przygotowania elementów działania: tworzywa, aparatury i wykonawców[26].

Dyrektywy walki nakazują stronom zachowywać się aktywnie, maksymalizować wysiłek, rozwijać inicjatywę, dążyć do poszerzenia granic swego działania, a wszystko po to, *by nie pozwalać procesom od nas zależnym przebiegać nie wedle naszych zamierzeń*[27]. Dlatego też strony walki są zobowiązane działać w zasięgu swoich możliwości i wpływać na zastany tok zdarzeń. Uznanie dyrektyw za drogowskazy działania może budzić wątpliwości. Pojawiają się one u L. Wittgensteina, który pyta wprost, czy drogowskaz nie pozostawia żadnych wątpliwości co do drogi, jaką mam obrać? Czy wskazuje, w jakim kierunku powinienem pójść minąwszy go: czy wzdłuż szosy, czy polną drogą, czy może na przełaj? Gdzie jest napisane, w jakim sensie mam według niego postępować, czy w kierunku jego ramienia, czy (np.) w przeciwnym?[28] Drogowskaz – jako wyraz reguły – normalnie jest znakiem wyrażającym ostrzeżenie, zakaz, nakaz, ograniczenie lub informację. Nie ulega wątpliwości co *normalnie* on wskazuje. Ale ów zwrot *normalnie* zakłada opanowanie praktyki posługiwania się drogowskazem. Jednak dla kogoś, kto widzi drogowskaz, otwartych jest wiele możliwości interpretacji i postępowań, nawet takich, które w ogóle nie mają nic wspólnego ze wskazywaniem drogi[29].

WOJNA A WOJNA HYBRYDOWA

Wśród nazw wojen wymienianych przez historyków możemy wskazać wojnę sześciodniową, październikową, siedmioletnią, trzydziestoletnią, a nawet stuletnią, choć wskazany czas trwania konfliktu nie zawsze jest precyzyjny. Nierzadkie są też terminy symboliczne określające zjawisko wojny. Na wyróżnienie w tym wypadku zasługują: wojna dwóch róż, wojna futbolowa, wojna północna i zimna wojna. Zdarza się również, że jedna wojna ma różne nazwy. Na przykład wymieniona już wojna październikowa znana jest również jako wojna ramadanowa albo wojna Jom Kippur.

Osobną grupę nazw stworzyli teoretycy zajmujący się zjawiskiem wojny. W tym wypadku nie chodziło jednak tylko o jej oznaczenie. Ideą, jaką się kierowano, było wskazanie cech wyróżniających. Wśród pierwszych uogólnień spotykamy nazwy z obszaru etyki: wojny sprawiedliwe i niesprawiedliwe. Dyskusja dotycząca charakterystycznych dla nich wyróżników ciągnie się nieprzerwanie od czasów pierwszych filozofów starożytnej Grecji i jest istotnym problemem oceny współczesnych konfliktów.

Dużo nowych nazw przyniosły czasy nowożytne. Polskie tłumaczenie *Zarysu sztuki wojennej* Henriego Jominiego wyróżnia jedenaście nazw i typów wojen. Wśród nich odnajdujemy między innymi wojny zaczepne, obronne, interwencyjne, inwazyjne, domowe i religijne[30]. Liczbę terminów opisujących w nazwie wojnę powiększają prace teoretyków nad sposobami jej prowadzenia. Pojawiają się takie przymiotniki, jak: wojna partyzancka, morska, totalna, błyskawiczna, zmechanizowana i powietrzna[31].

Jednak prawdziwy wysyp nazw próbujących jednym wyrazem lub połączeniem wyrazowym określić charakter wojny dotyczy czasów współczesnych. Gdy czytamy wydane w ostatnich latach publikacje, możemy się spotkać z wojną asymetryczną i symetryczną, kompozytową, nielimitowaną, pełzającą

[26] K. Piłejko: *Prakseologia – nauka o sprawnym działaniu.* Warszawa 1976, s. 186.

[27] T. Kotarbiński: *Traktat...*, op.cit., s. 146.

[28] L. Wittgenstein: *Dociekania filozoficzne.* Przeł. B. Wolniewicz. Warszawa 1972, § 85.

[29] P. Winch: *Etyka a działanie.* Warszawa 1990, s. 20.

[30] H. Jomini: *Zarys sztuki wojennej.* Wydawnictwo MON, Warszawa 1966, s. 34–54.

[31] Por. B. Balcerowicz: *O pokoju, o wojnie. Między esejem a traktatem.* Warszawa 2013, s. 100.

UNITED STATES COAST GUARD

i podprogową. Nie są to oczywiście wszystkie możliwe do wyszukania nazwy. O ich liczbie świadczą dwie prace opublikowane w 2018 roku. Pierwsza, autorstwa prof. Marka Wrzoska, poza omówieniem klasycznych teorii wojen zawiera również takie pojęcia, jak: *cyberwojna*, *wojny antyterrorystyczne*, *przeciwrebelianckie* i *hybrydowe*. Wśród nich tej ostatniej autor poświęca najwięcej miejsca[32]. W drugiej pracy, a właściwie artykule profesora Bolesława Balcerowicza, poza wcześniej wymienionymi nazwami możemy również odnaleźć takie pojęcia, jak: *nowe wojny*, *wojny wirtualne*, *wojny wśród ludności*, *gwiezdne wojny*, *wojny kosmiczne*, *informacyjne*, *cybernetyczne* i wojny robotów.

Wymienieni autorzy nie ukrywają swoich wątpliwości, które dotyczą nazw stosowanych do opisu współczesnych i przyszłych wojen. Mimo rozpoznanego braku precyzji, z dużą tolerancją podchodzą jednak do tych określeń, szczególnie akceptując coraz popularniejsze określenie konfliktu zbrojnego zwanego *wojną hybrydową*. Podobne tendencje prezentują również inne autorytety, niekoniecznie związane z naukami o obronności. Swoboda posługiwania się niektórymi orzecznikami rodzi jednak kilka pytań natury zasadniczej dla nauki o obronności. Dlaczego jakąś wojnę mamy nazywać tak, a nie inaczej? Czy fakt, że pewna nazwa, na przykład hybryda, jest modna i popularna, jest wystarczającą cechą usprawiedliwiająca daną nazwę? A jeśli nie, to jakie cechy musi posiadać taka nazwa, aby była właściwa?

Według różnych definicji wojna hybrydowa to[33]: współczesna odmiana wojny partyzanckiej, prowadzonej za pomocą współczesnych technik wojskowych i metod mobilizacyjnych, połączenie czterech odmian agresji: tradycyjnej, nieregularnej, terrorystycznej i cybernetycznej, odmiana konfliktu asymetrycznego, toczonego na trzech arenach: działań wojskowych, propagandy we własnym państwie oraz propagandy międzynarodowej, kombinacja elementów wojny nieregularnej, domowej, sztucznie wywołanego powstania i terroryzmu, użycie tradycyjnych metod wojennych, działań nieregularnych, terroryzmu i zachowań kryminalnych na polu walki w celu osiągnięcia korzyści politycznych. W „Defence Balance" (2015) czytamy, że wojna hybrydowa to działania polegające na wykorzystaniu militarnych i pozamilitarnych instrumentów w zintegrowanej kampanii, która ma zaskoczyć przeciwnika, a potem umożliwić przejęcie inicjatywy i osiągnięcie korzyści psychologicznych.

Analiza dalszych definicji wojny hybrydowej sprowadza się do postawienia jednoznacznej tezy, że trudno sobie wyobrazić, aby we współczesnej sztuce wojennej, mówiąc o użyciu sił zbrojnych danego państwa, nie rozważać problemów zabezpieczenia działań bojowych i wsparcia logistycznego, prowadzić działania bez rozpoznania i przewagi informacyjnej, maskowania operacyjnego lub taktycznego (to tutaj możemy znaleźć tzw. zielone ludki), metod „tajnej wojny", próby osłabienia przeciwnika stosując różne formy i metody, jak również bez próby wykorzystania mniejszości narodowych w kraju przeciwnika. Wielu teoretyków wojskowych na ten temat pisało już wcześniej. Nie sposób w tym momencie nie przywołać Carla von Clausewitza. Zwrócił on uwagę na dwa odmienne sposoby opisu tego zjawiska. Pierwszy nazwał ciężkim publicystycznym określeniem, będącym próbą kompleksowego ujęcia całego zjawiska. Cecha „publicystyczny" nie dotyczy wyłącznie publicystyki w środkach komunikacji społecznej, lecz obejmuje wszelkiego rodzaju traktaty, w tym i filozoficzne. Ten sposób z założenia został przez C. von Clausewitza odrzucony. Drugi sprowadzał się do pokazania wojny w postaci pierwiastkowej jako rozszerzonego pojedynku, czyli walki dwóch przeciwników, którzy w akcie przemocy chcą narzucić drugiej stronie swoją wolę[34]. Ten sposób opisu, który z racji stanowiska, jakie zajmował i osobistego uczestnictwa w działaniach bojowych, między innymi pod Auerstedt, Witebskiem, Smoleńskiem i Borodino, odpowiadał mu najbardziej. Traktat o wojnie był więc próbą teoretycznego opisa-

[32] Por. M. Wrzosek: *Wojny przyszłości, doktryny, technika, operacje militarne*. Warszawa 2018.

[33] https://pl.wikipedia.org/wiki/Wojna_hybrydowa/20.07.2018.

[34] C. Clausewitz: *O wojnie...*, op.cit., s. 15.

Termin bitwa
to podstawowa kategoria walki i oznacza bezpośrednie starcie wojsk; zwycięstwo zaś to pojęcie, którym wartościuje się sukces w wojnie i bitwie.

nia wojny, traktowanej jako pojedynek z perspektywy wojskowego praktyka, który wojnę rozumiał jako dalszy ciąg polityki *prowadzonej innymi środkami*[35]. Podkreślmy, wojna rozumiana jako dalszy ciąg polityki prowadzonej innymi środkami to nie tylko clausewitzowska definicja wojny, lecz przede wszystkim przyjęty przez C. von Clausewitza punkt widzenia do pisania o zjawisku wojny.

Próba stworzenia teorii wojny z powodu jej zmienności nie zakończyła się pełnym sukcesem. Jednak bardzo ważnym dokonaniem C. von Clausewitza w obszarze teorii było zdefiniowanie jej stałych elementów, czyli cech szczegółowych pojęcia wojny. Pierwszy dotyczy związku wojny z polityką.

Jak związek wojny z polityką rozumie twórca traktatu *O wojnie*? Do określenia wojny w kontekście polityki Clausewitz używa dwóch słów: akt polityczny (*politischer Akt*) i narzędzie polityczne (*politisches Instrument*). Po pierwsze wojna to już nie tylko stan funkcjonowania społeczeństw, tak jak to definiowali filozofowie, lecz akt, czyli czyn polityczny, który *wypływa zawsze z danej sytuacji politycznej i wywołują ją tylko pobudki polityczne*[36]. W związku z tym politycy w akcie podjęcia działań wojennych posiadają narzędzie, instrument, dzięki któremu mogą dalej prowadzić politykę w stosunku do drugiej strony konfliktu politycznego. Myśl ta dopełnia stwierdzenie, że *jeśli uprzytomnimy sobie, że wojna wypływa z celu politycznego, to wyda się nam zupełnie naturalne, że ta pierwsza pobudka, która powołała ją do życia, pozostaje przodującym najwyższym względem również i podczas jej rozgrywania. Jednak ten cel polityczny nie jest przez to jeszcze despotycznym prawodawcą, musi on przystosować się do natury użytych środków i wskutek tego często ulega zmianie, zawsze jednak pozostaje tym, co przede wszystkim należy uwzględnić*[37].

Podkreślenie relacji polityki i wojny umożliwia teoretykowi wprowadzenie trzech pojęć, przywoływanej już tak zwanej clausewitzowskiej trójcy, składającej się z trzech podmiotów funkcjonujących w państwie wraz z cechami, jakimi te podmioty charakteryzują się w obliczu wojny. Pierwsze pojęcie to *lud, naród* (*Volke*), jego gwałtowność, nienawiść i wrogość wobec przeciwnika. Drugie to *wódz*, *dowódca* i *podległe mu wojsko* (*Feldherrn und seinem Heer*), jego odwaga i talent wobec wyzwań i ryzyka wynikającego z przypadkowości i tylko prawdopodobieństwa wystąpienia zdarzeń. Trzecie to *rząd* (*Regierung*), jego rozsądek i racjonalność przejawiające się w zamiarach politycznych, doborze celów i środków do prowadze-

[35] Ibidem, s. 6.
[36] Ibidem, s. 28.
[37] Ibidem, s. 29.

nia wojny[38]. Relacje między tymi pojęciami oraz oddziaływania, jakimi podlegają te podmioty, wyznaczają charakter każdej wojny[39].

Zdefiniowanie cech charakteryzujących wyszczególnione podmioty państwa wprowadza nas, jak określił to Hew Strachan, w klimat wojny[40], zbiór cech szczegółowych, charakterystycznych dla każdej wojny. Elementy kształtujące jej atmosferę i odpowiadające im cechy szczegółowe będące treścią wojny dotyczą następujących zjawisk:

– niebezpieczeństwa, które sprawia, że odwaga jest *najcenniejszą cechą wojownika*[41];

– wysiłku fizycznego, który nakazuje posiadanie odpowiedniej sprawności fizycznej uczestnikom wojny;

– cierpienia, które wskazuje na wymóg posiadania odpowiednich cech psychicznych;

– niepewności (*Mgła wojny*) wymagającej trzeźwego myślenia i roztropności;

– przypadku (*Tarcie)*, który wymaga podjęcia szybkich i trafnych decyzji[42].

O ile pierwsze trzy cechy wydają się zrozumiałe, o tyle pozostałe dwie wymagają wyjaśnienia. Niepewność C. von Clausewitz wiąże z dostępem do informacji: *Wiele wiadomości otrzymywanych na wojnie jest sprzecznych, jeszcze więcej jest fałszywych, a najwięcej – niepewnych*[43]. Natomiast tarcie pruski generał opisuje słowami, że *na wojnie wszystko jest bardzo proste, lecz rzeczy nawet najprostsze są trudne*[44]. Ta ciężka do wytłumaczenia cecha jest opisana przez Thomasa Mahnkena jako zagrożenie ze strony przeciwnika, wysiłek do jakiego trzeba skłonić własne siły, przeszkody związane z fizycznymi właściwościami środowiska i wreszcie, podobnie jak w przypadku niepewności, niedoskonałość przepływu informacji[45].

Pięć cech opisujących atmosferę wojny odnosi się pewnie nie tylko do żołnierzy, lecz również do każdego członka społeczności dotkniętej wojną. Niepewność i przypadek to jednak uczucia, które dotyczą szczególnie dowódców i wiążą się z podejmowaniem decyzji i ryzykiem, jakim te decyzje są obarczone. Jak pisał Carl von Clausewitz: *Ta niepewność wszelkich wiadomości i założeń, to nieustanne wtrącanie się przypadku sprawia, że działający stale znajduje na wojnie rzeczy w innym stanie, niż oczekiwał, i z konieczności ma to swój wpływ na jego plany, a przynajmniej na związane z tymi planami wyobrażenia. Jeśli nawet wpływ ten będzie tak wielki, że obala niezawodnie powzięte postanowienia, to na ich miejsce muszą z reguły powstać nowe, do których znów w pewnym momencie brak danych* […]. *Znajomość sytuacji stała się większa, ale niepewność przez to nie zmniejszyła się, raczej wzrosła*[46].

Cytat ten, poza opisem trudności związanych z podejmowaniem decyzji, wprowadza nas również w dynamikę wojny rozumianą jako zjawisko, które nie ma swojego bezwzględnego końca, lecz jest pewnym ciągiem pomyślnych lub niepomyślnych zdarzeń. Nie można jej traktować jako gwałtowne i jednostkowe zdarzenie. Wojna jest *jakby pulsowaniem gwałtowności, to silniejszym, to znów słabszym, i wyładowuje swoje napięcia oraz wyczerpuje swoje siły to szybciej, to znowu powolniej*, ponieważ *jest ona działaniem sił, które nie rozwijają się całkiem jednakowo i równomiernie*. Może prowadzić *do celu szybko albo powoli, ale zawsze trwa dość długo.* Ma to swoje wyraźne konsekwencje dla polityków i dowódców, którzy przez swoje decyzje mogą nadać jej *ten, czy inny kierunek, a zatem i poddać ją woli kierującego*[47].

Drugi rozdział traktatu o wojnie C. von Clausewitza jest zatytułowany *Teoria wojny*. Już w pierwszym zdaniu zmienia on swoją dotychczasową perspektywę widzenia wojny: *Wojna w swym właściwym znaczeniu jest walką*[48]. Walkę prowadzi się z wykorzystaniem wszelkiego rodzaju środków, począwszy od broni, a skończywszy na uzbrojonej i wyekwipowanej sile zbrojnej. Posługiwanie się w walce tymi środkami to prowadzenie wojny i tak też C. von Clausewitz definiuje sztukę wojenną.

Powyższa definicja sztuki wojennej może wzbudzać kontrowersje, szczególnie w sytuacji, gdy pamiętamy jeszcze prowadzone rozważania o wojnie będącej kontynuacją polityki. Prowadzenie wojny to przecież sprawa polityczna. Celem wojny jest *zmuszenie przeciwnika do spełnienia naszej woli*[49]. W jakim sensie dla omówienia zjawiska prowadzenia wojny przestaje zajmować się prowadzeniem polityki, a zajmuje się sztuką wojenną. Sprzeczność popełniona przez Carla von Clausewitza na styku rozumienia pojęć *wojna* i *walka* nie wynikała ze źle przeprowadzonej analizy, raczej jest pewną charakterystyczną manierą wojskowych podejmujących ten temat również

[38] Por. Ibidem, s. 31.

[39] T.G. Mahnken: *Teoria strategii.* W: *Strategia we współczesnym świecie. Wprowadzenie do studiów strategicznych.* Red. J. Baylis, J. Wirtz, Colin S. Gray, E. Cohen. Tłum. W. Nowicki. Kraków 2009, s. 76.

[40] H. Strachan: *Carl von Clausewitz. O wojnie. Biografia.* Tłum. J. Dzierzgowski. Warszawa 2009, s. 134.

[41] C. Clausewitz: *O wojnie...*, op.cit., s. 45.

[42] Ibidem, s. 44–46.

[43] Ibidem, s. 64.

[44] Ibidem, s. 66.

[45] T.G. Mahnken: *Teoria...*, op.cit, s. 79.

[46] C. Clausewitz: *O wojnie...*, op.cit., s. 46.

[47] Ibidem, s. 29.

[48] Ibidem, s. 73.

[49] Ibidem, 15.

we współczesnych publikacjach. Przykładem takiego wypaczenia pojęć jest choćby praca Jeana Colina związana z przeobrażeniami wojny czy Ferdynanda Focha dotycząca jej prowadzenia. Generał I. Colin w traktacie *Przeobrażenia wojny*[50] podejmuje zagadnienia przeobrażenia postaci walki, następnie rozpatruje zagadnienie bitwy i operacji. Swoje wnioski koncentruje na rozwoju środków walki, ruchu wojsk i ich rozwinięciu. W tak zarysowanej konstrukcji brakuje miejsca na tytułowe przeobrażenia wojny. Podobnie marszałek F. Foch w książce *O prowadzeniu wojny*, traktującej o zwycięskiej dla Prus kampanii 1870 roku, stara się odtworzyć przede wszystkim *życie kwatery głównej*. Wybór ten był nieprzypadkowy, jak mówił bowiem przywołany przez F. Focha Johann Ludwig Yorsk von Wartenburg: *Kto chce zrozumieć wojnę, powinien się starać poznać tych co ją prowadzą. Klucz historii wojen znajduje się w kwaterach głównych*[51]. Twierdzenie brzmi atrakcyjnie, ale jeżeli wojna jest instrumentem polityki, to rodzi się pytanie, czy kwatera główna kształtuje politykę? I z drugiej strony, dlaczego marszałek F. Foch nie analizuje zagadnień politycznych i znaczącej roli Ottona von Bismarcka w tej wojnie?

Kończąc krótką prezentację na ten temat, jeszcze raz podkreślmy, że główną zasługą Clausewitza, mimo trudności, z jakich zdawał sobie sprawę, jest dążenie do precyzowania pojęcia *wojny*. Jego metoda sprowadza się z jednej strony do wskazania na różnorodność desygnatów, jakie możemy określić mianem wojny. Z drugiej, stara się określonej klasie przypisać cechy szczególne. Z pewnością jego tezy są dyskusyjne, a tekst traktatu *O wojnie* jest wymagającą lekturą. Jest on jednak również dobrym przykładem wypełnienia tez i dyrektyw T. Kotarbińskiego dotyczących znaczenia nazwy, a w tym przypadku znaczenia pojęcia *wojna*.

POKONAĆ CHAOS

Artykuł jest osobistą refleksją autorów na istniejącą w publikacjach swobodę posługiwania się niektórymi orzecznikami związanymi ze współczesną wojną. Samo zjawisko swobody określania rzeczywistości wojny nie jest nowe. Wystarczy znać prawa i prawidłowości wojny oraz zasady jej organizowania i prowadzenia, aby móc określać cechy współczesnych wojen (konfliktów zbrojnych). Czasami autorzy różnych artykułów na ten temat wykorzystują tylko tłumaczenia z angielskiego, nie do końca rozumiejąc zjawisko wojny albo przyjmują tzw. nowomodę na zjawiska, które zostały już dawno opisane i zbadane. Wspomina o tym choćby Jan Gotlib Bloch, przytaczając swoje studia nad literaturą wojskową i regulaminami różnych armii, poprzedzające przygotowania do napisania pracy o przyszłej wojnie: *Co za chaos pojęć i zasad, które ścierają się i walczą, a żaden błysk światła stąd nie wytryska. Nic dziwnego zatem, że oficerowie mówią nieraz: Po co się tu uczyć? Niechaj sami profesorowie wprzód porozumieją się i zgodzą na jedno*[52].

Organizując działania zbrojne w ujęciu prakseologicznym, należy przestrzegać wielu dyrektyw walki, zwanych często „mistrzowskimi chwytami". Zostały one zawarte w następujących tezach:

– dla powodzenia w walce nie jest zawsze koniecznym wyrządzać przeciwnikowi jakąkolwiek przykrość oprócz przykrości nieudanych zamierzeń;

– dbać o gładki przebieg i racjonalną kolejność działań oraz odstępować od utartych schematów;

– maksymalnie wyzyskiwać czas, przestrzeń, energię i informację;

– dbać o większą swobodę ruchów własnych sił i aparatury od tej, którą posiada przeciwnik oraz krępować jego siły i aparaturę;

– wyzbywać się pewnych własnych zasobów, jeśli ich uciążliwość w danej sytuacji góruje nad pożytkiem, oraz zużytkować aparaturę przeciwnika lub jego samego wprost w walce przeciw niemu właśnie, i na swoją korzyść;

– rozpraszać (odosabniać) siły strony przeciwnej i od współdziałania usuwać tak, by uzyskać w każdej z rozpraw cząstkowych przewagę sił w rozstrzygającym miejscu i czasie; przy równych warunkach rozpoczynać od likwidacji najsilniejszego przeciwnika;

– koncentrować, zarówno siły składowe walczącego zespołu, jak wreszcie czyny składające się na całość;

– zespalać w całość czyn wielopodmiotowy, koordynować i dbać o spójnię sił własnych oraz ich wzajemne informowanie;

– wymierzać ciosy w punkt całości wyższego rzędu, wyjątkowo uzależniający walczące całości, czyli w człony kierownicze;

– osłaniać z osobliwą pieczołowitością części wyjątkowo uzależniające bronionego obiektu;

– stwarzać fakty dokonane (antycypować);

– odkładać rozstrzygnięcia (kunktatować);

– zagrozić przeciwnikowi (potencjalizować);

– rozstrzygać problemy za pomocą taktyki tzw. języczka u wagi;

– zwiększać procent przewagi drogą skrępowań równoważnych;

– zdobywać wiedzę o stronie przeciwnej, wprowadzać ją w błąd i nieoczekiwanie się zachowywać[53].

Podejmując zagadnienie nazywania jakiegoś typu czy rodzaju wojny, w pierwszej kolejności musimy wskazać jego denotację, następnie wyszczególnić wszystkie te cechy, które dla tej klasy przedmiotów są właściwe. Wśród nich o istocie nazwy będą mówić te właściwości, które dla danej nazwy są wyjątkowe i niezbędne. Bez tych cech pojęcia te może są atrakcyjne, nie mają jednak większej wartości naukowej. ■

[50] J. Colin: *Przeobrażenia wojny*. Warszawa 2010.

[51] F. Foch: *O prowadzeniu wojny*. Tłum. O. Laskowski. Oświęcim 2015, s. 14.

[52] J.G. Bloch: *Wnioski ogólne z dzieła. Przyszła wojna pod względem technicznym, politycznym i ekonomicznym*. Warszawa 1899, XVI.

[53] T. Kotarbiński: *Z zagadnień...*, op.cit., s. 18–54.

Nowe **podejście**

CORAZ WIĘKSZA LICZBA KONFLIKTÓW WEWNĄTRZPAŃSTWOWYCH ORAZ POJAWIANIE SIĘ RÓŻNEGO RODZAJU PODMIOTÓW O POZAPAŃSTWOWYM STATUSIE SPOWODOWAŁY, ŻE ZJAWISKO WOJNY NALEŻY POSTRZEGAĆ INACZEJ NIŻ DOTYCHCZAS.

ppłk dr Piotr Harężlak

Autor jest kierownikiem Zakładu Operacji Instytutu Sztuki Operacyjnej i Taktyki Wydziału Wojskowego Akademii Sztuki Wojennej.

Od pewnego czasu światowa opinia społeczna, a także środowiska wojskowe i naukowe stoją w obliczu konieczności odpowiedzi na wiele pytań związanych z nasilaniem się fenomenu nazywanego wojną hybrydową. Zasadnicze dylematy dotyczą przede wszystkim jej istoty oraz kwestii, na czym polega, jak przebiega, co ją wyróżnia, a także jakie daje możliwości, jak jej przeciwdziałać itp. Kluczowa wydaje się jednak odpowiedź na pytanie, czy problem naprawdę jest nowy.

W POSZUKIWANIU ODPOWIEDZI

Wiele ośrodków naukowo-badawczych, a także środowisk wojskowych podjęło próbę zbadania i wyjaśnienia tego jakże skomplikowanego dylematu naukowego, czy wojna hybrydowa jest w istocie novum. A jeśli tak, to dlaczego? Niniejszy artykuł ma przybliżyć zasadnicze ustalenia w tej sprawie oraz wskazać wynikające z nich kolejne dylematy dotyczące konsekwencji zidentyfikowanych przemian w sztuce wojennej zarówno dla współczesnych sił zbrojnych, jak i systemów obronnych państw stających w obliczu problemu wojny hybrydowej.

Istotną kwestią jest określenie, na czym polega fenomen wojny hybrydowej i co ją odróżnia od wojny klasycznej. Podstawą sytuacji problemowej może być, jak zwykle, teza Clausa von Clausewitza, niezależnie od tego, jak jest obecnie interpretowana, mówiąca o tym, że *wojna jest tylko kontynuacją polityki prowadzonej innymi środkami*[1]. Wyjaśnienia wymaga zatem również termin *polityka*. *Encyklopedia PWN* ujmuje ją jako*: pojęcie należące współcześnie do języka potocznego, występujące także w dyskursie publicznym oraz w naukach społecznych; w rozumieniu potocznym polityka oznacza: umiejętność sprawowania władzy publicznej; działania rządu; zdolność mobilizowania członków zbiorowości do wspólnego wysiłku na rzecz celów społecznych i zyskiwania ich posłuchu dla decyzji władzy; umiejętność skutecznej realizacji wyznaczonych celów społecznych w podzielonym, zróżnicowanym społeczeństwie*[2]. Na podstawie tej definicji można za prawdziwe przyjąć uogólnienie, że polityka jest swoistą sztuką realizacji określonych interesów, którymi na poziomie państwowym będą interesy większości społeczeństwa danego państwa.

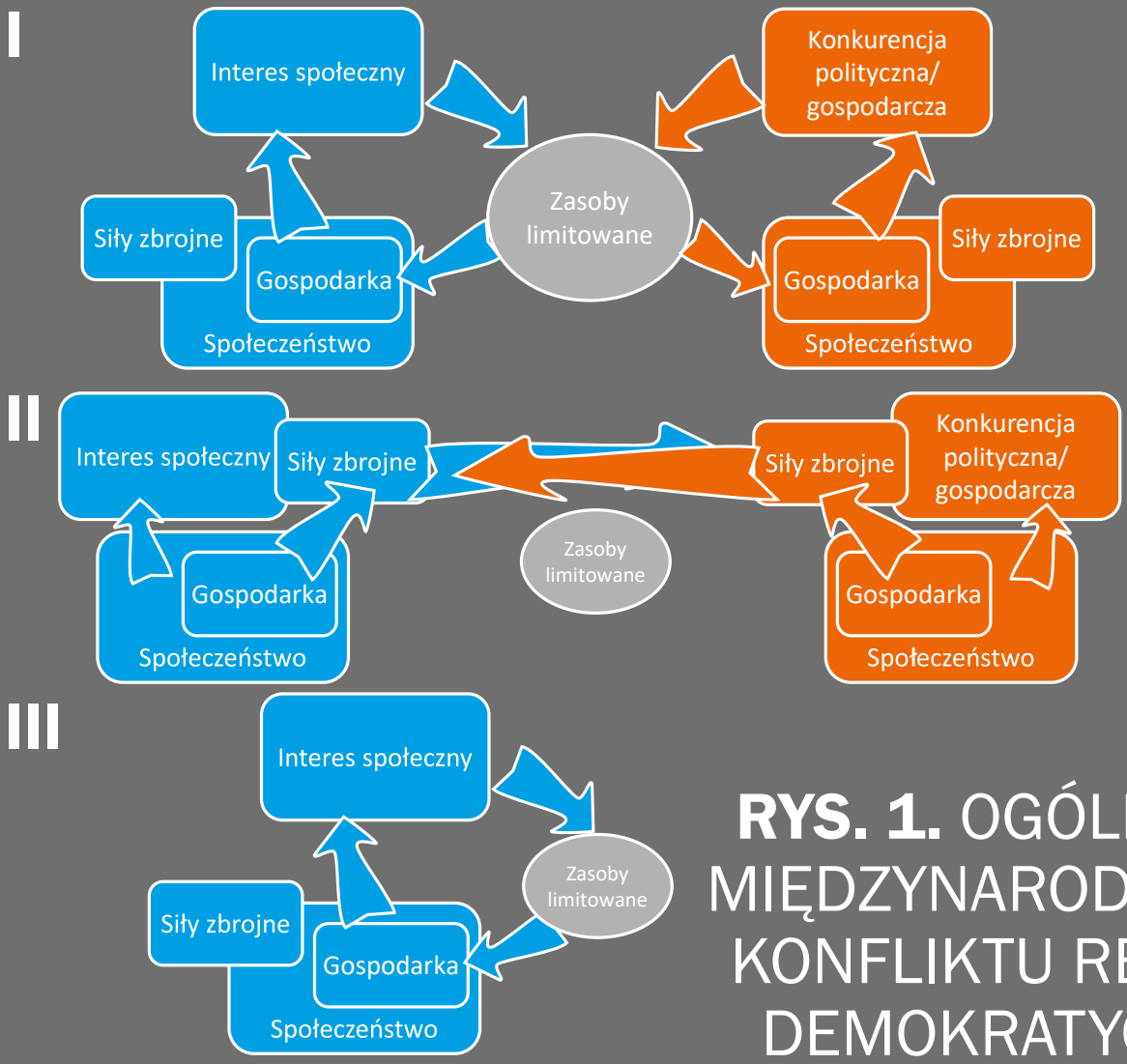
W tak określonych warunkach wojna, do której przywykliśmy, miała zazwyczaj charakter państwowy, a więc instytucjonalny, i mobilizowała cały dostępny oraz niezbędny potencjał danego kraju według pewnego określonego porządku (rys.1).

Na pierwszym etapie (I) konkurencyjne reżimy demokratyczne[3] eksploatują limitowane zasoby, za-

[1] Zob. C. von Clausewitz: *O wojnie*. Warszawa 2006, s. 29, 32–43.

[2] https://encyklopedia.pwn.pl/haslo/polityka;3959606.html. 15.07.2018.

[3] W sytuacji reżimów niedemokratycznych inaczej mogą przebiegać wewnętrzne oddziaływania informacyjne w państwie.



RYS. 1. OGÓLNA IDEA MIĘDZYNARODOWEGO KONFLIKTU REŻIMÓW DEMOKRATYCZNYCH

Opracowanie własne.

ostrzając konkurencję między sobą w ramach gry gospodarczej i politycznej. W miarę zwiększania się potrzeb gospodarek oraz (lub) zmniejszania dostępności zasobów dochodzi do sporu militarnego (II). W jego ramach jest dokonywany nowy ich podział, przy czym gospodarki obu państw wspierają siły zbrojne na drodze do uzyskania supremacji (III). W taki sposób jest postrzegana, również na poziomie intuicyjnym, istota międzynarodowego konfliktu zbrojnego. Pojęcie zasobów limitowanych (konkurencyjnych) zostało tutaj użyte jako ogólna idea i może dotyczyć zarówno dóbr materialnych, jak i wartości niematerialnych, stanowiących często fasadę rzeczywistych interesów. Wojna hybrydowa jest alternatywą dla tak przyjętego porządku i jest nie lada problemem zarówno w jej identyfikacji, jak i przeciwdziałaniu. Źródłem problemu jest sposób rozstrzygnięcia sporu odbiegający od przedstawionego schematu. Według *Słownika języka polskiego PWN hybryda* to m.in.:

1. *coś, co składa się z różnych elementów, często do siebie niepasujących;*

2. *roślina lub zwierzę powstałe ze skrzyżowania dwóch odmian, ras lub gatunków* […][4].

INTERPRETACJA ZJAWISKA

W zamieszczonej w „Przeglądzie Sił Zbrojnych" publikacji pt. *Zdefiniować zagrożenie* ppłk Cezary Pawlak i kmdr por. Jarosław Keplin przytaczają źró-

[4] https://sjp.pwn.pl/szukaj/hybryda.html. 15.07.2018.

dłosłów *hybrydy* jako terminu pochodzącego od *łacińskiego słowa hybryda, które oznacza mieszańca, osobnika powstałego ze skrzyżowania dwóch genetycznie różnych osobników należących do różnych gatunków, odmian czy ras*[5]. Stąd w dalszej części wywodu przedstawiają wnioski Franka G. Hoffmana, który hybrydowość konfliktu zbrojnego postrzega w licznych dychotomiach[6] mogących zachodzić równocześnie i z tego tytułu tworzących novum w postaci mieszańca. Innymi słowy, według tej koncepcji znane wcześniej sposoby postępowania i narzędzia mogą być wykorzystywane do celów wojennych w nieznanych dotychczas zestawieniach i sekwencjach użycia. Najważniejszy jednak wniosek dotyczy sposobu oddziaływania (atakowania) przez przeciwnika prowadzącego działania hybrydowe. W dużym uogólnieniu można uznać, że o ile w poprzednim modelu konfliktu przeciwnicy walczyli w porównywalnych obszarach konkurencji (dziedzinach funkcjonowania społecznego) i tylko pośrednio (lub sporadycznie bezpośrednio) oddziaływali na inne, to w sytuacji konfliktu hybrydowego mamy do czynienia z permanentnym i równoległym atakiem w kilka z nich oraz z wkraczaniem w inne w miarę rozwoju konfliktu.

Ponieważ sztuka wojenna jako dziedzina nauki od dawna korzysta z różnych metod analizy środowiska walki (rys. 2), autorzy artykułu uznali, że wyjaśnienia istoty wojny hybrydowej najlepiej dokonać przez ten właśnie pryzmat. Do swoich rozważań jako najpopularniejszą wykorzystali metodę PMESII[7], dochodząc do wniosku, że *o zagrożeniach o znamionach hybrydowych możemy mówić wtedy, gdy byt państwa jest zagrożony w co najmniej dwóch obszarach PMESII równocześnie, co utrudnia lub uniemożliwia podjęcie jednoznacznej reakcji*[8]. Konkluzja ich rozważań ma istotne walory utylitarne.

Naukowcy reprezentujący różne ośrodki badawcze, mimo pewnych odmienności w kwestiach dotyczących charakteru przebiegu konfliktu, zwykle wskazują na jego dwa zasadnicze etapy:

– poniżej progu wojny,

– otwartych działań wojennych[9].

W szczegółowych analizach dotyczących przebiegu wojny hybrydowej wyróżnia się inną systematykę, czyli np.:

– przygotowanie,

– destabilizację,

– działania militarne,

– rozstrzygnięcie[10].

Na szczególną uwagę zasługuje podział faz zaproponowany przez szefa Sztabu Generalnego Federacji Rosyjskiej Walerija Gierasimowa, który wyróżnia:

- fazę 1 – działań utajnionych,
- fazę 2 – zaostrzenia,
- fazę 3 – rozpoczęcia działań sygnalizujących konflikt,
- fazę 4 – kryzysu,
- fazę 5 – rozstrzygnięcia,
- fazę 6 – przywrócenia pokoju.

W ten sposób Gierasimow podkreśla, że konflikt hybrydowy obejmuje proces eskalacji (pierwsze cztery fazy), a cele osiągnięte w rozstrzygnięciu (faza 5) ulegają utrwaleniu w procesie deeskalacji (fazie 6). Założenia te są zbieżne z modelem operacji połączonej obowiązującym w siłach zbrojnych Stanów Zjednoczonych (rys. 3). To spostrzeżenie nasuwa kolejną refleksję na temat innowacyjności wojennej hybrydy. Otóż jej adaptacyjność odnosi się nie tylko do znanych działań łączonych w nieznane wcześniej sekwencje i proporcje, lecz w sensie kapitalnym odwzorowuje również istotę standardowej operacji. Zaskoczenie przeciwnika natomiast bierze się z rozmachu fazy zmagań poniżej progu wojny, w znacznej części prowadzonej skrycie z zachowaniem wysokiego poziomu maskowania, mylenia i dezinformacji[11].

W tabeli przedstawiono fazy rozwoju konfliktu hybrydowego zgodnie z poglądami wybranych teoretyków, opracowane na podstawie wcześniej cytowanych publikacji.

Jakiego więc archetypowego przebiegu konfliktu można dopatrzyć się w rozważanych systematykach? Próbę odpowiedzi na to pytanie obrazują rysunki 4–6.

W etapie pierwszym konkurujący wyprowadza atak hybrydowy na wszystkich dostępnych płaszczyznach walki oprócz (lub w bardzo ograniczonym zakresie, np.: PROXY) otwartej walki zbrojnej, stopniowo zmniejszając szeroko rozumiane zdolności (możliwości) atakowanego. Prowadzi to do sytuacji, w której następuje istotne pogorszenie funkcjonowania gospodarki oraz systemów społecznych oponenta. Jednocześnie nie daje on powodu do jednoznacznego zinterpretowania jego działań jako planowego i skoordynowanego ataku. Nadając mu pozory zaburzeń

[5] C. Pawlak, J. Keplin: *Zdefiniować zagrożenie.* „Przegląd Sił Zbrojnych" 2017 nr 4, s. 17. Za: *Słownik wyrazów obcych PWN.* Warszawa 1980, s. 290.

[6] Ibidem, s. 16. [...] *konflikt hybrydowy cechuje się zbieżnością fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów [...] sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażeni.*

[7] W tekście oryginalnym zamieszczono opis PEMSII. Zob. ibidem, s. 18.

[8] Por. ibidem, s. 17.

[9] Zob. M. Wrzosek: *Uwarunkowania funkcjonowania systemu rozpoznania wojskowego w wojnie hybrydowej.* „Kwartalnik Bellona" 2017 nr 4, s. 72–73.

[10] Zob. ibidem, s. 73–74.

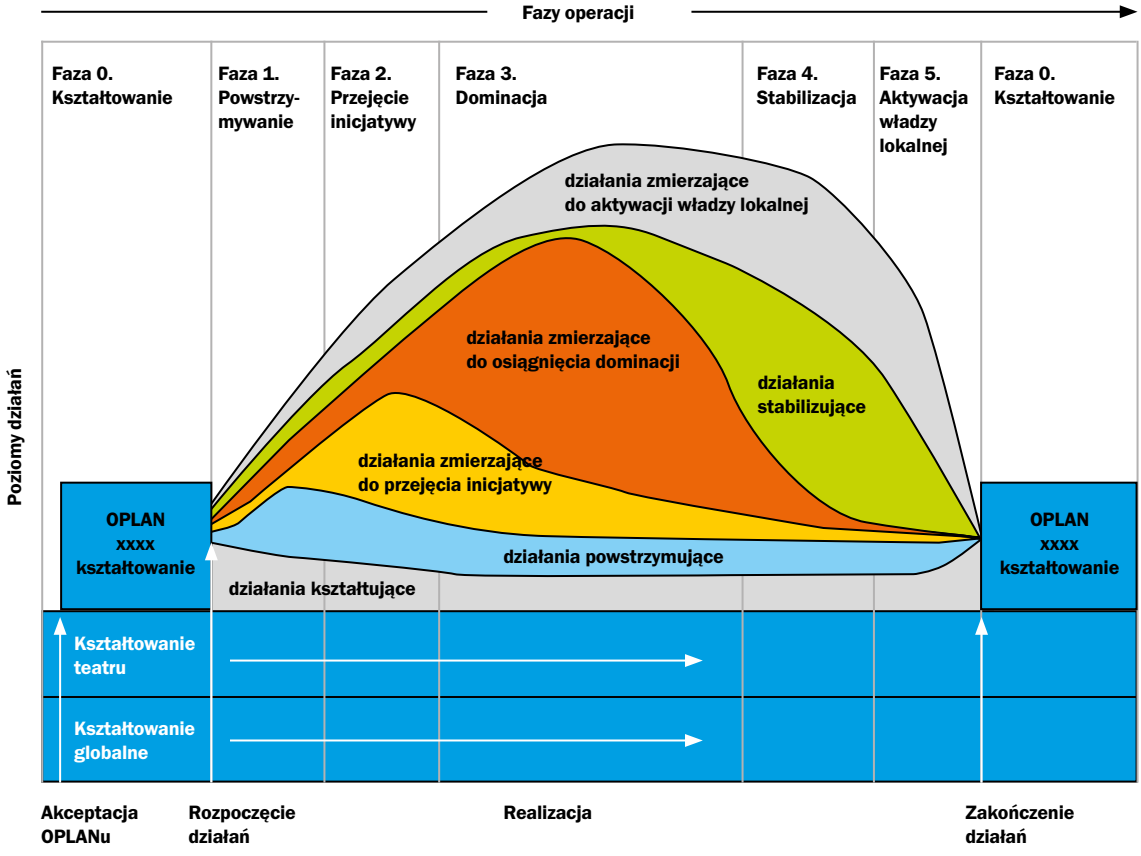
[11] Elementami sprzyjającymi uzyskaniu zaskoczenia od lat niezmiennie są: zachowanie tajemnicy, ukrywanie własnych zamiarów, wprowadzanie przeciwnika w błąd (dezinformowanie), nieszablonowość, śmiałość i szybkość działania. Zob. *Regulamin działań Wojsk Lądowych*. DWLąd, Warszawa 2008, s. 19.

RYS. 2. WYBRANE METODY ANALIZY ŚRODOWISKA DZIAŁAŃ W KONTEKŚCIE ODDZIAŁYWAŃ HYBRYDOWYCH

METT-TC	Mission		Weather	Enemy	Troops & Support	Civilian considerations	Terrain	Time avaliable	
ASCOPE	Area	Structures	Capabilities	Organizations		People			Events
PEST	Political		Economic			Social	Technological		
PESTL			Economic		Legal	Social	Technological		
DIMEFIL	Diplomatic	Financial	Economic	Military		Legal		Inteligence	Information
STEEPLEM	Political	Environmental	Economic	Military	Legal	Social	Technological	Ethnical	
PMESII PT	Political	Phisical environment	Economical	Military		Social	Infrastructure	Time	Information
PMESII	Political		Economical	Military		Social	Infrastructure		Information

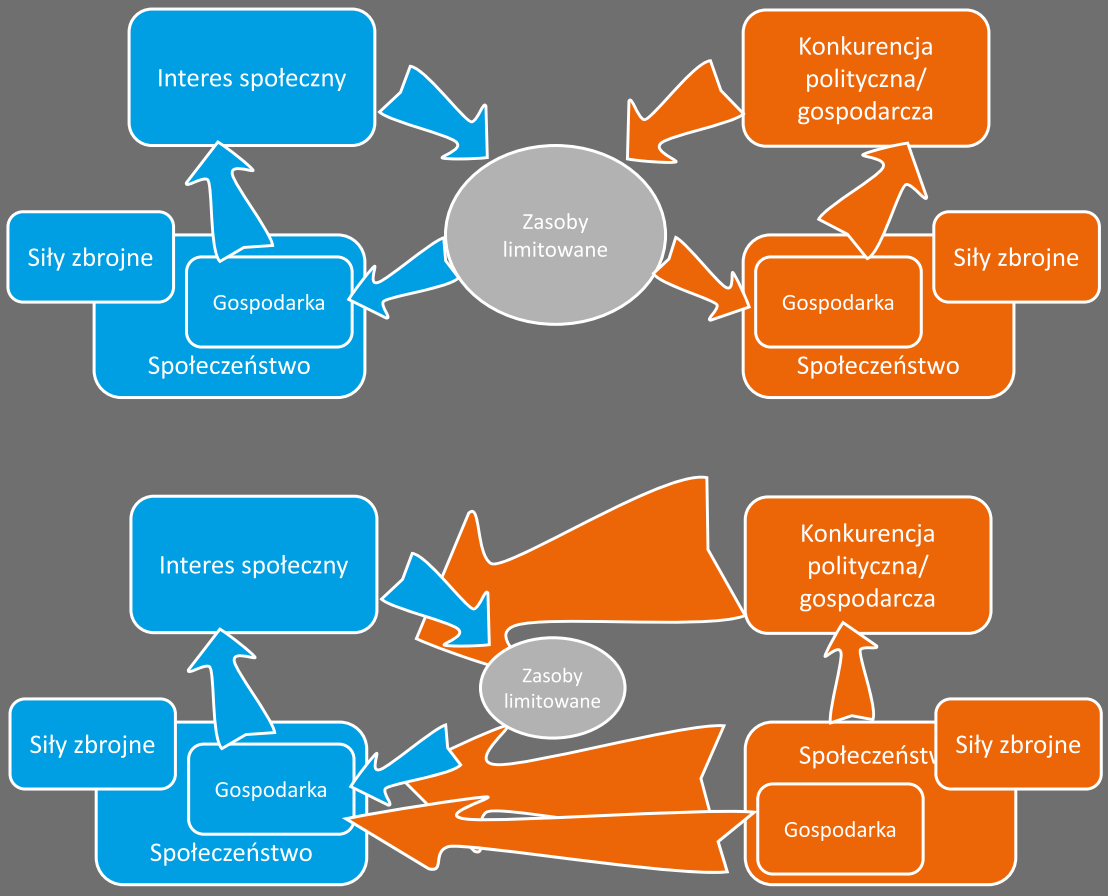
Opracowanie własne na podstawie: P. Paździorek: *Wojskowa myśl operacyjna w konfliktach zbrojnych przełomu XX i XXI wieku*. Toruń 2016.

RYS. 3. MODEL OPERACJI POŁĄCZONEJ



Źródło: *Joint Publication 3-0*. Joint Operations, Washington 2017, s. V-8.

RYS. 4. ZMAGANIA HYBRYDOWE PONIŻEJ PROGU WOJNY

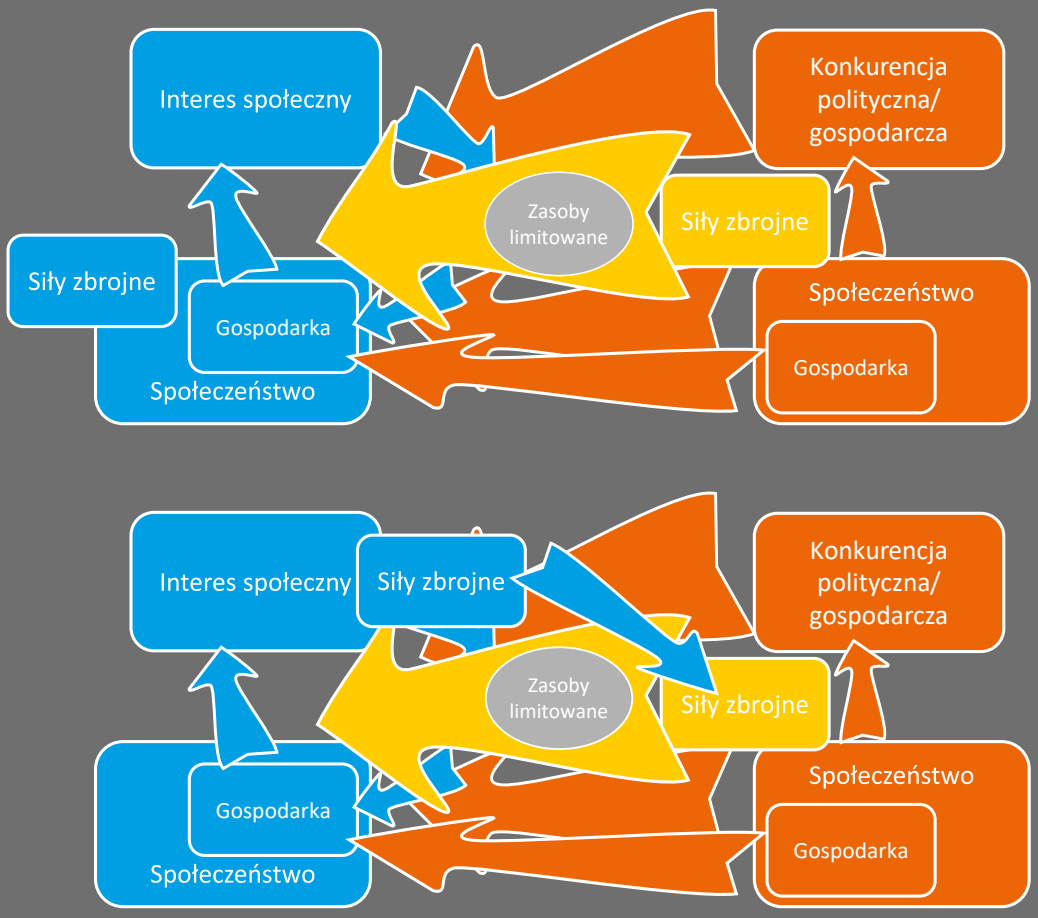


społecznych, wynikających z niesprawności gospodarki, administracji, rządu czy ustroju, stara się doprowadzić do pojawienia się u przeciwnika symptomów państwa pogrążonego w kryzysie.

Kolejny etap obejmuje zdecydowane użycie sił zbrojnych przeciwko wybranym elementom systemu obrony przeciwnika w celu doprowadzenia do rozstrzygnięcia konfliktu. Można do niego przejść dopiero wówczas, gdy powstaną odpowiednie warunki w ramach etapu poprzedniego. Sam konflikt zbrojny może obejmować kilka składowych, np.: skryte rozmieszczenie wyprzedzające, otwarty atak, działania stabilizacyjne itp. Co ważne, część kinetyczna może mieć ograniczony zasięg i błyskawiczny przebieg. Taka konfiguracja obu etapów konfliktu sprawia, że jest on stosunkowo tani. Zwalczanie przeciwnika pogrążonego w kryzysie wymaga znacznie mniejszych środków niż walka ze sprawnym konkurentem, prowadzące zaś do kryzysu *zmagania poniżej progu wojny* również wymagają nakładów o wiele mniejszych od wojennych. Poza tym mogą być przeciągane w czasie aż do uzyskania pożądanego poziomu sprawności (czy raczej niesprawności) przeciwnika bez znaczącego zwiększania nakładów[12].

[12] Chodzi o zastosowanie opisanej przez Tadeusza Kotarbińskiego dyrektywy *kunktacji* jako celowego zwlekania, *tzn.: umiejętność działania, a więc i walki, polega w znacznej mierze na właściwym wyborze chwili odpowiedniego impulsu, i częstokroć najroztropniej działa, kto się z wywarciem takiego impulsu nie spieszy, lecz raczej maksymalnie z tym zwleka. Bywa to na ogół wtedy, kiedy – jak to się mówi – czas działa na naszą korzyść, gdy np. siły przeciwnika w miarę czasu same słabną w większym stopniu niż nasze albo gdy procent przewagi początkowej naszych własnych sił, zrazu nikły, w miarę czasu wzrasta*. Zob. T. Kotarbiński: *Traktat o dobrej robocie.* Warszawa 1965, s. 251–252.

RYS. 5. OTWARTE DZIAŁANIA WOJENNE W RAMACH KONFLIKTU HYBRYDOWEGO



Opracowanie własne (2).

Specjaliści, odnosząc się do takiego modelu przebiegu konfliktu, twierdzą, że w zasadzie nie jest on czymś nowym. Wskazują przy tym, że otwarte konflikty zbrojne zwykle poprzedzały kryzysy, przenosząc się na arenę społeczną, gospodarczą i polityczną. Cóż więc spowodowało, że pojawiła się potrzeba wyróżnienia konfliktu hybrydowego? Wśród czynników mających na to wpływ jako pierwszy można wskazać planowe działanie. W przypadku hybrydy wojennej nie mamy do czynienia z wojną jako skutkiem kryzysu, lecz z kryzysem planowo wywołanym i wykorzystywanym na potrzeby konfliktu.

Kolejny czynnik stanowi wspomniana wcześniej możliwość zmniejszenia kosztów konfliktu (szeroko rozumianych, w tym również strat osobowych) oraz balansowania na granicy wojny z jednoczesnym ciągłym utrzymywaniem wpływu na oponenta. Najważniejszym jednak czynnikiem sprzyjającym rozwojowi hybrydy wydaje się infosfera. Działania w cyberprzestrzeni, jakże wrażliwej w sytuacji konfliktu zbrojnego na oddziaływania kinetyczne i elektromagnetyczne, okazują się być niezwykle skuteczne poniżej progu wojny, a w razie przejścia do otwartego konfliktu nadal można je bez zakłóceń prowadzić poza strefą walk bezpośrednich.

Można zatem wyciągnąć wniosek, że katalizatorem nowego rodzaju wojny (w tym wojny hybrydowej) stał się po raz kolejny rozwój cywilizacyjny, a w szczególności wzrost zdolności i aktywności człowieka w cyberprzestrzeni. Umożliwia ona wpływanie na komunikację nie tylko w aspekcie informacyjno-propagandowym, lecz także, a może przede wszystkim, w aspekcie ekonomicznym. Cyberprzestrzeni nie dotyczą tradycyjne ograniczenia terytorialne, zapewnia ona bowiem jej uczestnikowi nieograniczony zasięg działania. Ponadto pozwala

TABELA. FAZY ROZWOJU KONFLIKTU HYBRYDOWEGO

M. Wrzosek	Pierwszy etap obejmuje zmagania poniżej progu wojny				
Zespół badawczy MON	Faza 1. Przygotowanie		Faza 2. Destabilizacja		
	A. Część skryta	B. Część jawna			
W. Gierasimow	Faza 1. Działania utajnione	Faza 2. Zaostrzenie	Faza 3. Rozpoczęcie działań sygnalizujących konflikt	Faza 4. Kryzys	
Fiński Instytut Stosunków Międzynarodowych	Faza 1. Przygotowanie strategiczne	Faza 2. Przygotowanie polityczne	Faza 3. Przygotowanie operacyjne	Faza 4. Eskalacja napięcia	
Łotewska Narodowa Akademia Obrony	Faza 1. Działania niemilitarne, wpływające negatywnie na społeczność, ekonomię i działania polityczne	Faza 2. Działania ukierunkowane na wprowadzanie w błąd ośrodków dyplomatycznych, politycznych i medialnych	Faza 3. Działania mające na celu zastraszenie ludności i wskazanie bezcelowości dalszego oporu	Faza 4. Działania destabilizacyjne i propagandowe	Faza 5. Działania wprowadzające strefy zakazu lotów

Opracowanie własne.

RYS. 6. ROZSTRZYGNIĘCIE KONFLIKTU HYBRYDOWEGO

Opracowanie własne.

na wywieranie wpływu na życie wszystkich, nawet jeżeli nie są świadomymi uczestnikami globalnej wioski. Obecnie wszelkie istotne relacje zachodzące między podmiotami życia społecznego mają swoje odzwierciedlenie w powiązaniach cyberprzestrzennych, a nawet z cyberprzestrzeni się wywodzą – tam mają swój początek. Co więcej, trend ten wydaje się nasilać. Tak więc panowanie nad infosferą umożliwia nie tylko kreowanie obrazu, a w dalszej perspektywie percepcji otoczenia, lecz także wpływanie na realny stan rzeczy w danej dziedzinie czy danym obszarze. To właśnie infosfera i zjawisko globalnej wioski umożliwiają łączenie efektów oddziaływań kinetycznych i niekinetycznych w nowych proporcjach i sekwencjach pozwalających na świadome aranżowanie konfliktów w postaci wojen hybrydowych.

Państwa stojące w obliczu zagrożeń o charakterze hybrydowym muszą rozstrzygnąć wiele dylematów: czy i od kiedy państwo jest obiektem ataku, jaka jest skala (rozmach) ataku i jego cel, jakie środki (sposoby) działania zostały użyte poniżej progu wojny itp. Mniejszy problem stanowi określenie sposobu reakcji na aktywność przeciwnika powyżej progu wojny. W tym przypadku kluczowe znaczenie mają wnioski z analizy czynników operacyjnych (czas, przestrzeń, siły i informacja). Muszą one być osadzone w kon-

Drugi etap obejmuje otwarte działania wojenne		
Faza 3. Działania militarne	Faza 4. Rozstrzygnięcie	
Faza 5. Rozstrzygnięcie		Faza 6. Przywrócenie pokoju
Faza 5. Obalenie władzy centralnej w regionie docelowym		Faza 6. Ustanowienie alternatywnej władzy
Faza 6. Rozpoczęcie działań militarnych przez intensyfikację rozpoznania i użycie sił specjalnych	Faza 7. Działania wielopłaszczyznowe, w tym informacyjne, dyplomatyczne oraz militarne jako wywieranie presji z użyciem paramilitarnych i regularnych sił zbrojnych	Faza 8. Działania mające na celu zniszczenie sił przeciwnika przez siły specjalne i wojska lądowe oraz precyzyjne uderzenia

Za najważniejsze w przygotowaniach do odpowiedzi na ataki hybrydowe należy uznać zdolność do ich wykrycia, do obrony w infosferze i do podjęcia decyzji dotyczącej użycia adekwatnej siły w obszarze destabilizacji.

tekście szkód wyrządzonych systemowi obronnemu państwa na tym etapie zmagań.

MIEĆ ŚWIADOMOŚĆ

Na podstawie przeprowadzonych rozważań można wyciągnąć kilka ogólnych wniosków dotyczących atakowanego systemu państwowego.

Po pierwsze, muszą istnieć instrumenty i procedury ułatwiające monitorowanie ataków w infosferze oraz przeciwdziałanie im.

Po drugie, ważne jest, by atakowany podmiot miał możliwości i środki służące osiągnięciu stabilizacji sytuacji (reagowanie kryzysowe) w obszarze dotkniętym bezpośrednio atakiem poniżej progu wojny. Środki te powinny pochodzić z domeny wszystkich resortów i instytucji podejmujących działania w ramach reagowania kryzysowego. Duże znaczenie w tych działaniach zyskują terytorialne jednostki obronne zakorzenione w obszarze działań, znające jego specyfikę.

Po trzecie, w czasie zmagań poniżej progu wojny muszą być inicjowane i wdrażane mechanizmy obrony militarnej przed spodziewanym otwartym atakiem. Wreszcie wszystkie te przedsięwzięcia powinny być realizowane w sposób możliwie proporcjonalny do skali ataku, aby z jednej strony nie zwiększać nadmiernie kosztów działania (po stronie atakowanego), z drugiej zaś nie dawać pretekstu do eskalacji konfliktu.

Najważniejsza jednak wydaje się powszechna świadomość odpowiedzialności za działania obronne. Próby właściwego rozwiązania problemu można doszukiwać się w rozwijanej od kilkunastu lat w Stanach Zjednoczonych koncepcji Comprehensive Approach[13]. Polega ona na skoordynowanym zaangażowaniu wszystkich instrumentów państwa w przeciwdziałaniu zagrożeniom multidyscyplinarnym, a właśnie z takimi mamy do czynienia w konflikcie hybrydowym. Podsumowując, należy stwierdzić, że za najważniejsze w przygotowaniach (osiąganie zdolności) do odpowiedzi na ataki hybrydowe należy uznać zdolność do ich wykrycia, do obrony w infosferze i do podjęcia decyzji dotyczącej użycia adekwatnej siły w obszarze destabilizacji. ■

[13] Comprehensive Approach – podejście wszechstronne to podejście integrujące wysiłki rządu, instytucji rządowych, organizacji pozarządowych i partnerów międzynarodowych oraz podmiotów z sektora prywatnego, oparte na powszechnym zrozumieniu zasad i współdziałaniu w ramach procesów prowadzących do osiągnięcia wspólnego celu. Por. *Guiding Principles for Stabilization and Reconstruction*, U.S. Army Peacekeeping and Stability Operations Institute, Washington 2009, Appendix E.

Wojna hybrydowa – zagrożenie **bezpieczeństwa państwa?**

ROZWÓJ TECHNOLOGII INFORMACYJNYCH POZWOLIŁ NA WYKORZYSTANIE NOWYCH ROZWIĄZAŃ MIĘDZY INNYMI W CELU ZMNIEJSZANIA POTENCJAŁU BOJOWEGO PRZECIWNIKA.

ppłk dr inż. Norbert Świętochowski

Autor jest kierownikiem Zakładu Wsparcia Bojowego Instytutu Dowodzenia Akademii Wojsk Lądowych.

Obserwując problemy sąsiedniego państwa, niejako w sposób naturalny nasuwa się pytanie, jakie skutki przyniósłby atak hybrydowy wymierzony przeciwko naszemu krajowi. Czy jest tak samo podatny na działania hybrydowe jak Ukraina, czy też sytuacja społeczno-polityczna oraz ekonomiczna daje nam podstawy sądzić, że jesteśmy odporniejsi na tego typu działania? Mając na uwadze przede wszystkim jednolitą narodowościowo strukturę państwa polskiego, silniejszą pozycję polityczną i ekonomiczną, a przede wszystkim przynależność do Unii Europejskiej oraz Sojuszu Północnoatlantyckiego, można hipotetycznie założyć, że prowadzenie takich działań byłoby trudniejsze. Z pewnością nie oznacza to, że nasz kraj jest wolny od zagrożeń hybrydowych. Jest bowiem poważnie narażony na cyberataki, presję polityczną i ekonomiczną, działania informacyjne, terroryzm i wiele innych czynników, które mogą spowodować jego destabilizację, a w konsekwencji poważnie ograniczyć bezpieczne funkcjonowanie.

GENEZA

Działania o charakterze hybrydowym nie są zjawiskiem nowym. Ponadto nie można przypisywać konkretnemu państwu lub teoretykowi opracowania od podstaw ich koncepcji. W minionych konfliktach zbrojnych strony agresywne starały się stosować wszelkie formy walki zbrojnej oraz inne działania militarne i niemilitarne, które prowadziły do osiągnięcia założonego celu. W latach 1919–1920 irlandzcy powstańcy wykorzystywali jednostki konwencjonalne oraz milicji w połączeniu z aktami terroru w celu oderwania się od brytyjskiej korony, co może już być pierwowzorem dzisiejszych działań hybrydowych. Za prekursorów teorii współczesnej wojny hybrydowej uważani są amerykańscy analitycy wojskowi, a po raz pierwszy pojęcia *zagrożenia hybrydowe* i *wojna hybrydowa* pojawiły się w studium Williama J. Nemetha pod tytułem *Future war and Chechnya: A case for hybrid warfare.* Autor twierdzi, że czeczeńscy bojownicy w walce z siłami Federacji Rosyjskiej stosowali działania hybrydowe, próbując uderzać w słabe punkty silniejszego militarnie i demograficznie przeciwnika[1].

Teoretykiem szczegółowo przedstawiającym problem konfliktu hybrydowego jest Frank G. Hoffman, który w 2007 roku opublikował opracowanie pod tytułem *Conflict in the 21st Century: The Rise of Hybrid War*[2] Już na początku swej analizy zamieszcza definicję zagrożeń hybrydowych, które łączą w sobie różne sposoby walki zbrojnej, w tym działania konwencjonalne oraz nieregularne, akty terrorystyczne z użyciem

[1] W.J. Nemeth: *Future war and Chechnya: A case for hybrid warfare*. Monterey, CA 2002. http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1/. 2.05.2018.

[2] F.G. Hoffman: *Conflikt in the 21st Century: The Rise of Hybrid Wars*. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf/. 8.05.2018.

FOTOLIA/KARELIN DMITRIY

Dotarcie z przekazem telewizyjnym w miejscowym języku lub z innymi audycjami, które mogą kształtować opinię publiczną zgodnie z wolą agresora, ma w działaniach hybrydowych kluczowe znaczenie.

ciem każdej możliwej przemocy skierowanej przeciwko ludzkiemu życiu, a także akty kryminalne. Według niego podstawowe zagrożenia bezpieczeństwa państwa wynikające z ataku hybrydowego to:

– ograniczony atak wojsk konwencjonalnych mający na celu, na przykład, zagarnięcie części terytorium;

– atak wojsk nieregularnych, niezidentyfikowanych sił zbrojnych, do których oficjalnie nikt się nie przyznaje (zielone ludziki);

– dążenie do politycznej izolacji atakowanego państwa;

– sankcje ekonomiczne;

– ograniczanie dostępu do surowców strategicznych, przede wszystkim energetycznych, decydujących o funkcjonowaniu państwa;

– ofensywa propagandowa w mediach, zwłaszcza w telewizji oraz na forach internetowych, w tym wpływanie na opinię publiczną przez przekazywanie stronniczych, a nawet sfałszowanych wiadomości oraz opinii;

– akty sabotażu i dywersji;

– ataki terrorystyczne;

– akty kryminalne.

Podaje on propozycję definicji wojny hybrydowej jako *działań prowadzonych za pomocą różnych sposobów walki, w tym konwencjonalnych działań zbrojnych, działań nieregularnych, aktów terrorystycznych, także tych najgwałtowniejszych i śmiercionośnych, oraz przestępstw kryminalnych*[3]. Według niego o wojnie hybrydowej można mówić dopiero wtedy, gdy pojawi się większość wymienionych zagrożeń jednocześnie i mogą one potencjalnie spowodować poważną destabilizację sytuacji politycznej i ekonomicznej w danym państwie oraz wywołać niezadowolenie dużych grup społeczeństwa.

Podkreśla on przy tym, że współczesne wojny w większym lub mniejszym stopniu były prowadzone metodą działań regularnych i nieregularnych. Jeśli te dwa rodzaje działań bojowych stosowano jednocześnie w sposób skoordynowany, to można mówić o wojnach złożonych (compound wars). Nie jest to stwierdzenie odkrywcze, ponieważ klasycznym przykładem z pewnością jest wojna w Wietnamie, w której rola wojsk nieregularnych (Wietkongu) była niekwestionowana. W wojnie tej zarówno siły regularne, jak i nieregularne walczyły jednocześnie, aby osiągnąć wspólny cel, jakim było wyparcie wojsk amerykańskich oraz obalenie państwa południowowietnamskiego. A to właśnie, jak podaje Hoffman, jest podstawowym wyróżnikiem wojny złożonej[4]. Podobna sytuacja zaistniała w czasie operacji „Iracka wolność" w 2003 roku. Saddam Husajn do obrony przed inwazją sprzymierzonych użył swoistej mieszanki pozostałości sił regularnych oraz nieregularnych jednostek bojowników, zwanych fedainami, którzy mieli za zadanie ata-

[3] Ibidem, s. 29.

[4] Ibidem, s. 20.

kować przeciwnika we wszystkich newralgicznych obiektach po to, by opóźniać marsz na Bagdad.

Hoffman wspomina także o wojnach bez ograniczeń (war beyond limits), których koncepcję wysunęli dwaj chińscy pułkownicy: Qiao Liang i Wang Xsiangsui. Według niego nie dotyczy to form, które może przybierać współczesna wojna, lecz raczej granic, które może przekraczać w dobie postępującej globalizacji. Z jednej strony wojna ta będzie pozbawiona wszelkich hamulców moralnych i nie będzie podlegać ramom żadnych konwencji dotyczących działań zbrojnych, z drugiej zaś będzie prowadzona z użyciem wszelkich dostępnych środków, nie tylko wojskowych, lecz także politycznych, kulturowych, dyplomatycznych, religijnych i innych. W związku z wzajemnym uzależnieniem ekonomicznym i politycznym państw taki konflikt dotknie praktycznie wszystkich.

Wojna hybrydowa według Hoffmana może być toczona zarówno przez państwo, jak i różnorodne organizacje niepaństwowe[5]. Opracowanie tego autora powstało w 2007 roku, to jest przed wydarzeniami na Ukrainie. Swoje przemyślenia oparł zatem w dużej mierze na doświadczeniach amerykańskich z Iraku i Afganistanu, przede wszystkim z działań Hezbollahu w Libanie w roku 2006. Jednak przytoczona przez niego wizja wojny hybrydowej okazała się wręcz prorocza, co potwierdziły późniejsze doświadczenia ukraińskie.

CO TO JEST WOJNA HYBRYDOWA?

Analizując zagrożenia hybrydowe oraz działania rosyjskie na Ukrainie, można zredefiniować pojęcie *wojna hybrydowa* jako działania militarne i niemilitarne wymierzone najczęściej przeciwko państwu, w których zastosowano jednocześnie konwencjonalne działania zbrojne, działania nieregularne, akty terrorystyczne i kryminalne, wspomagane szerokim atakiem informacyjnym oraz walką w cyberprzestrzeni, mającymi zapewnić powodzenie. Działania hybrydowe mogą być skierowane przeciwko całemu państwu, to jest zarówno władzom, jak i społeczeństwu, lub też władzom i wybranym elementom społeczeństwa, które te władze reprezentują. Idea wojny hybrydowej zakłada wykorzystanie wszelkich słabości państwa w wymiarze politycznym, wojskowym, gospodarczym, społecznym, informacyjnym i infrastrukturalnym. Prowadzone w jej ramach działania mogą zostać skierowane przeciwko wszelkim aspektom życia społecznego lub jego kluczowym elementom. Jak łatwo wywnioskować, są tym skuteczniejsze, im słabsze jest państwo, które jest obiektem tych oddziaływań.

W ataku hybrydowym celem są przede wszystkim elementy krytyczne dla sprawnego funkcjonowania państwa (critical functions). Są to najistotniejsze przedsięwzięcia i działania polityczne, wojskowe, ekonomiczne, społeczne, informacyjne i infrastrukturalne, których zatrzymanie lub zakłócenie spowoduje znaczące zmniejszenie zdolności państwa do realizacji stojących przed nim zadań[6]. Elementami krytycznymi mogą być ważni politycy, jednostki wojskowe i uzbrojenie, sieć energetyczna, system prawny i wiele innych.

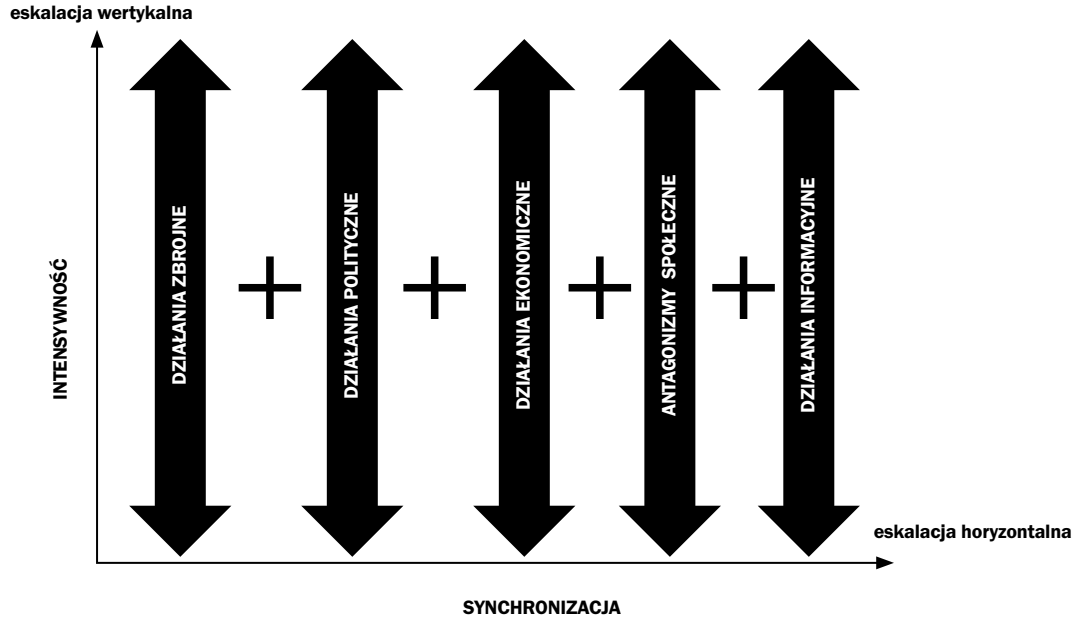
Dla dużej grupy analityków klasycznym przykładem wojny hybrydowej jest agresja rosyjska na Ukrainę. Z perspektywy czasu można stwierdzić, że sposób zaatakowania tego kraju nie powinien być zaskoczeniem, gdyż taki przebieg wojny zapowiadał kilka lat wcześniej rosyjski generał Walery Gierasimow. W jednym ze swoich artykułów wskazał na rozmywanie się granicy między stanem pokoju a stanem wojny. Dokładnie tak stało się na Ukrainie. Formalnie Federacja Rosyjska nie jest agresorem i nie prowadzi wojny przeciwko Ukrainie. Wręcz przeciwnie, politycy rosyjscy oficjalnie wyrażają chęć udziału w negocjacjach między zbuntowanymi republikami donieckimi a ukraińskim rządem. Wojna nie została wypowiedziana, a nawet utrzymywane są stosunki dyplomatyczne (np. porozumienie Mińsk 2), a także ekonomiczne, czego przykładem dostarczanie gazu na Ukrainę przez Rosję. Podkreślając troskę o bezpieczeństwo ludności pochodzenia rosyjskiego zamieszkującej Donbas, rząd rosyjski oficjalnie stara się ograniczać eskalację walki zbrojnej i prowadzi negocjacje pokojowe z udziałem państw zachodnich. Jednocześnie wykorzystuje wszelkie środki prowadzące do osłabienia państwa ukraińskiego, destabilizacji jego sytuacji wewnętrznej oraz izolacji politycznej i gospodarczej, wywierając przede wszystkim presję ekonomiczną (podwyższenie ceny gazu importowanego przez Ukrainę) i stosując dezinformację, propagandę, a nawet dywersję. Rosja nie wzbrania się przed szkoleniem i dozbrajaniem sił zbrojnych samozwańczych republik, a nawet, w razie konieczności, dokonaniem jawnej interwencji zbrojnej. Na obszarze Ukrainy inspirowane są akty przemocy i zamachy terrorystyczne w celu destabilizacji sytuacji wewnętrznej i osłabienia struktur państwa. Podejmowane były także zbrojne działania regularne i nieregularne oraz skoordynowane ataki cybernetyczne na wiele sfer działalności ukraińskiego państwa.

Analizując różne rodzaje agresywnej aktywności Rosji wobec Ukrainy, można wyróżnić cztery zasadnicze etapy wojny hybrydowej, to jest: dywersję polityczną skierowaną przeciwko rządowi ukraińskiemu, budowanie pozycji społecznej i politycznej separatystów, interwencję zbrojną oraz odstraszanie metodą demonstracji potencjału sił konwencjonalnych. Wymienione działania zachodzą na siebie i występują z różnym natężeniem. Mimo ewidentnych dowodów na mieszanie się Rosji w konflikt między Ukrainą a zbuntowanymi republikami, w tym także na inter-

[5] Ibidem, s. 8.

[6] *Understanding Hybrid Warfare*. A Multinational Capability Development Campaign Project, MCDC January 2017, s. 9.

RYS. NARZĘDZIA ODDZIAŁYWANIA W WOJNIE HYBRYDOWEJ



Źródło: *Understanding Hybrid Warfare.* A Multinational Capability Development Campaign Project, MCDC January 2017, s. 9.

wencję wojskową, władze rosyjskie oficjalnie zaprzeczają udziałowi w konflikcie[7].

Majstersztykiem wręcz okazała się aneksja Krymu, przeprowadzona na oczach bezradnej światowej opinii publicznej. Wydawało się, że w obecnym systemie politycznym świata nie jest możliwe oderwanie siłowe części terytorium niepodległego państwa przez inne państwo, które jest członkiem ONZ i powinno przestrzegać międzynarodowych konwencji i regulacji prawnych. Umiejętne zastosowanie przez Rosjan elementów wojny hybrydowej podczas aneksji Krymu, a przede wszystkim uniknięcie otwartej agresji zbrojnej, lecz wysłanie żołnierzy w nieoznakowanych mundurach i usprawiedliwianie aneksji Krymu prawami do tego terytorium wynikającymi jakoby z jego historycznej przynależności do Rosji, pozwoliło w pewnym sensie na oswojenie z tą sytuacją opinii publicznej.

Użycie żołnierzy do realizacji działań nieregularnych podczas wojny hybrydowej przewidział w swoim opracowaniu Hoffman, wskazując wspomnianych już fedainów Saddama Husajna[8]. W zasadzie jest to normalny sposób realizacji zadań, uwzględniony także w naszej doktrynie działań wojsk lądowych[9]. Jednakże żołnierze powinni działać w mundurach z pełnym oznakowaniem. Prowadzenie operacji wojskowych w mundurach nieoznakowanych jest niezgodne z prawem międzynarodowym, a tego w zasadzie w jawny sposób dopuściła się strona rosyjska podczas aneksji Krymu. Świadczy to o tym, że w wojnie hybrydowej nie może być mowy o przestrzeganiu międzynarodowego prawa konfliktów zbrojnych. Automatycznie daje to agresorowi przewagę nad państwem demokratycznym, starającym się prowadzić walkę zbrojną w ramach międzynarodowych konwencji.

METODY WALKI

Jak wynika z powyższych rozważań, wojna hybrydowa jest swoistym połączeniem intensywnego konfliktu konwencjonalnego z działaniami nieregularnymi oraz wszelkim możliwym oddziaływaniem, w tym nawet z aktami terrorystycznymi i kryminalnymi, które mogą służyć do osiągnięcia założonego celu. W przyszłych konfliktach hybrydowych potencjalnymi przeciwnikami mogą być państwa, organizacje i grupy tworzone oraz sponsorowane przez państwa,

[7] M. Banasik, R. Parafianowicz: *Teoria i praktyka działań hybrydowych.* „Zeszyty Naukowe AON" 2015 nr 2(99), s. 11.

[8] Ibidem, s. 28.

[9] *Działania nieregularne mogą być prowadzone zarówno w ramach działań obronnych, jak i powszechnego ruchu oporu, po utracie możliwości prowadzenia zorganizowanej obrony. W związku z powyższym mogą one mieć charakter zamierzony lub wymuszony*. Regulamin działań wojsk lądowych. DWLąd, Warszawa 2008, s. 241–246, pkt 11001.

Po udanej aneksji Krymu Rosja zdecydowała się na wybudowanie mostu łączącego jej terytorium z zajętą prowincją. W zamyśle agresora ma to pobudzić wzrost gospodarki Krymu i usprawnić przepływ ludności rosyjskiej na terytorium utracone przez Ukrainę.

ROZBUDOWA PRZEZ ROSJAN INFRASTRUKTURY TRANSPORTOWEJ OSŁABIA INTEGRALNOŚĆ TERYTORIALNĄ I NIEPODLEGŁOŚĆ UKRAINY.

a także elementy niezależne od państw, powstałe samoczynnie, najczęściej na bazie konfliktów i niezadowolenia społecznego. Przyszły przeciwnik, bez względu na to, do której z wymienionych grup będzie należał, może mieć dostęp do najnowocześniejszych technologii wojskowych, w tym do kodowanego systemu dowodzenia i łączności, przenośnych rakietowych zestawów przeciwlotniczych i innych systemów uzbrojenia, a przy tym stosować także środki walki powstańczej, takie jak zamachy samobójcze, zasadzki, podkładanie improwizowanych urządzeń wybuchowych i inne[10]. Najważniejsza różnica między wojną konwencjonalną a hybrydową polega na tym, że wszystkie niekonwencjonalne działania ofensywne, podejmowane przez siły regularne i nieregularne, nie służą wsparciu walki wojsk operacyjnych (regularnych), lecz same w sobie są narzędziem do osiągnięcia zwycięstwa i zamierzonych korzyści politycznych. Nie są zatem elementem wspierającym, lecz zasadniczym sposobem realizacji zadań.

Wojna hybrydowa toczona przeciwko każdemu państwu (zarówno o mniejszym, jak i większym potencjale militarnym i gospodarczym) ma w zamierzeniu doprowadzić do szybkiego osiągnięcia celów politycznych przez wykorzystanie słabości nawet najsilniejszego pod każdym względem przeciwnika. Jest to przeciwieństwo tradycyjnie pojmowanych konfliktów zbrojnych, w których z zasady zwyciężała strona mającą przewagę wojskową, materialną, technologiczną i inną. W tego typu konflikcie z jednakowym natężeniem mogą być stosowane militarne i niemilitarne środki oddziaływania i nacisku jednocześnie lub w dowolnej sekwencji, na poziomie taktycznym i operacyjnym, jednakże zawsze w sposób zamierzony i skoordynowany dla osiągnięcia celów strategicznych. Można założyć, że działania hybrydowe mogą być wpisane nawet w strategię państwa jako narzędzie polityczne.

Do militarnych elementów wojny hybrydowej należą konwencjonalne działania zbrojne, działania nieregularne oraz akty terrorystyczne, do niemilitarnych natomiast – presja polityczna i ekonomiczna, aktywność służb specjalnych, działania ofensywne w cyberprzestrzeni, działalność dyplomatyczna, a nawet akty kryminalne[11]. Na rysunku przedstawiono wybrane narzędzia oddziaływania stosowane w wojnie hybrydowej. Ich eskalacja horyzontalna może być dużo większa, co zależy od możliwości agresora. Do wymienionych na rysunku można dodać terroryzm, dywersję i sabotaż. Agresor będący organizacją nieformalną nie zawaha się przeprowadzić najkrwawszych zamachów terrorystycznych, jeśli przyniosą one zamierzony efekt. W czasie działań zbrojnych wykorzysta ludność cywilną jako żywą tarczę, tak jak to często robił Hezbollah w Libanie i Strefie Gazy.

[10] F.G. Hoffman: *Conflikt in*..., op.cit., s. 28.

[11] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia.* „Przegląd Bezpieczeństwa Wewnętrznego". Wydanie specjalne. Warszawa 2015, s. 45–47.

KANCELARIA PREZYDENTA FR

Poszczególne narzędzia będą stosowane w taki sposób, by wywołać serię wydarzeń i skutków, które doprowadzą do pożądanego wyniku. Kluczowe jest tu skoordynowanie wielu działań i ataków. Na przykład jesienią 2013 roku Iran zaplanował wywołanie zagrożeń terrorystycznych oraz przeprowadzenie cyberataków i działań propagandowych oraz je zsynchronizował tak, by wpłynęły na decyzję USA i jej sojuszników i powstrzymały ich przed interwencją w Syrii[12].

Ze względu na możliwość stosowania coraz to nowszych i bardziej wysublimowanych narzędzi oddziaływania trudno jest przygotować się na skoordynowany atak hybrydowy. W tym momencie państwo może podjąć środki zmierzające do przeciwdziałania niektórym znanym narzędziom, natomiast całkowita i skuteczna prewencja jest niemożliwa.

Z różną intensywnością mogą być stosowane poszczególne narzędzia w czasie trwania konfliktu, a zatem zróżnicowana będzie ich eskalacja wertykalna. Jedne działania mogą się okresowo nasilać, gdy w tym czasie inne mogą być prowadzone z mniejszą intensywnością, co utrudnia ich powiązanie przez atakowanego.

DETERMINANTY SKUTECZNOŚCI

Atak hybrydowy przeciwko silnemu i przygotowanemu państwu nie przyniesie oczekiwanych skutków i zostanie odparty. Aby przeciwnik osiągnął swój cel, musi przeprowadzić go w sposób skoordynowany z użyciem wielu narzędzi (rozpiętość horyzontalna). Przede wszystkim jednak muszą w danym państwie istnieć czynniki umożliwiające jego zastosowanie. Do podstawowych należy zaliczyć kryzys polityczny lub polityczno-ekonomiczny, skutkujący brakiem możliwości efektywnego przeciwdziałania przez władze państwowe, podział społeczeństwa na grupy dążące do osiągnięcia swoich własnych celów oraz ogólne niezadowolenie społeczeństwa z władz i sposobu funkcjonowania państwa czy też jego ustroju. Oczywiście taki kryzys może zostać wywołany właśnie w wyniku agresji hybrydowej, czyli na przykład przez działania propagandowe, powodujące niezadowolenie i zamieszki społeczne. Może to być swoistym wstępem do dalszych działań w ramach tzw. ciągu wydarzeń prowadzących do zamierzonego celu, przykładowo do osłabienia międzynarodowej pozycji atakowanego państwa lub wyeliminowania go z członkostwa w organizacjach polityczno-gospodarczych i sojuszach wojskowych. Zatem najmniejsze oznaki wskazujące na chęć doprowadzenia do destabilizacji sytuacji w nim należy traktować bardzo poważnie i przeciwdziałać im z całą mocą.

Ważnym czynnikiem ryzyka mogą być mniejszości narodowe lub religijne dążące nie tylko do uzyskania autonomii i praw, co w społeczeństwie demokratycznym powinno przecież w naturalny sposób mieć miejsce, lecz zmierzające do oderwania części terytorium państwa i utworzenia nowego lub przyłączenia do innego. Podsycanie niezadowolenia społecznego mogą wywoływać także sankcje ekonomiczne ograniczające dostęp do surowców energetycznych oraz podstawowych dóbr materialnych. Zatem uzależnienie się państwa od jednego dostawcy może prowadzić do poważnych konsekwencji gospodarczych i społecznych.

Innym sprzyjającym działaniom hybrydowym czynnikiem jest jego słabość militarna. Brak silnych jednostek wojskowych, w tym także, a może przede wszystkim, o charakterze terytorialnym, gotowych do natychmiastowego wykonania zadań w ramach odparcia podprogowej agresji zbrojnej, może doprowadzić do sytuacji, w której kontrolę nad zwaśnionym obszarem przejmą tzw. zielone ludziki. Wydaje się, że gdyby Ukraina dysponowała nawet niezbyt licznymi, lecz dobrze wyszkolonymi i wyposażonymi jednostkami bojowymi o wysokim morale, skryta inwazja zbrojna na Krymie nie byłaby możliwa.

Szczególnie ważnym elementem jest łatwość prowadzenia akcji propagandowej przez agresora na terenie danego państwa. Dotarcie z przekazem telewizyjnym w miejscowym języku lub z innymi audycjami, które mogą kształtować opinię publiczną zgodnie z wolą agresora, ma w działaniach hybrydowych kluczowe znaczenie. W tym przypadku warunkiem powodzenia jest istnienie w atakowanym państwie wolnego rynku

[12] *Understanding Hybrid Warfare*..., op.cit., s. 12.

mediów, na którym silną pozycję ma agresor, lub dostęp społeczeństwa do nowoczesnych technologii telekomunikacyjnych, umożliwiający zapoznawanie się z materiałami propagandowo-informacyjnymi zamieszczanymi na portalach społecznościowych i w witrynach internetowych. Wrażliwym elementem w aspekcie wojny informacyjnej są zwłaszcza portale społecznościowe, na których przez zatrudnionych tzw. trolli internetowych, czyli osoby świadomie, przeważnie dla pieniędzy, rzadziej z przekonania, zamieszczające fake newsy[13] i stronnicze poglądy, można kształtować opinię i świadomość społeczną. Akcja taka może być przez długi czas niezauważalna dla społeczeństwa, a nawet służb, przynosząc jednak zamierzone efekty[14]. Rosja ma w tej dziedzinie bogate doświadczenie oraz przewagę nad państwami Unii Europejskiej, w których funkcjonuje wolny rynek mediów, a zatem możliwe jest osadzanie w nich agencji pracujących dla Rosji lub państw jej przychylnych. Co więcej, w 2011 roku wdrożono w Rosji program Społeczeństwo Informacyjne (2011–2020), którego celem jest zapewnienie rosyjskojęzycznej ludności świata dostępu do państwowych i prywatnych mediów przekazujących strategię Federacji Rosyjskiej[15].

Rosyjska Federalna Agencja Informacyjna, działająca prawdopodobnie od lipca 2013 roku, skupia ponad dziesięć różnych firm informacyjnych o różnych lokalizacjach, w tym na Ukrainie (przykładem strona internetowa Antymajdan), które w większości przygotowują materiały odnoszące się do konfliktu z tym państwem, jego polityki lub rosyjskiej polityki dotyczącej tego kraju, obowiązkowo zwracając uwagę na pozytywną rolę Rosji. Istnieją dowody na to, że rząd Federacji Rosyjskiej zatrudnia personel do prowadzenia aktywnej działalności w sieci i przedstawiania tendencyjnych opinii i komentarzy do przekazywanych informacji o wydarzeniach politycznych. W tzw. fabrykach trolli internetowych pracują internauci podszywający się pod pożądaną narodowość i obywatelstwo, wyrażający opinie na zamówienie.

Wymienione determinanty skuteczności agresji hybrydowej przeciwko danemu państwu należą do tych zasadniczych. Oprócz nich można wymienić także mniej ważne, takie jak kryzys migracyjny (zalewająca kraj fala uchodźców może powodować poważną destabilizację sytuacji w nim), zagrożenia terrorystyczne (ataki terrorystyczne, nawet niezwiązane z agresją hybrydową, mogą wywoływać obawy i niezadowolenie społeczeństwa) czy choćby katastrofy cywilizacyjne i naturalne prowadzące do poważnego zachwiania stanu równowagi państwa, w konsekwencji ułatwiające dokonanie na nie agresji w jakiejkolwiek formie.

JAK PRZECIWDZIAŁAĆ?

Nasz kraj jest prawie jednolity narodowościowo i etnicznie, a nawet religijnie. Zamieszkujące w nim nieliczne mniejszości narodowe i religijne mają zagwarantowane prawa polityczne i autonomię oraz swobodę wyznania. Według narodowego spisu powszechnego przeprowadzonego w 2011 roku narodowość polską zadeklarowało 97,09% ankietowanych (wliczając w to osoby deklarujące również drugą narodowość). Natomiast 2,26% zadeklarowało dwie narodowości – polską i niepolską, w tym 2,05% polską jako pierwszą, a zaledwie 0,22% polską jako drugą. 1,55% zadeklarowało wyłącznie niepolską narodowość, z czego 0,12% – dwie niepolskie narodowości[16]. Co więcej, Rzeczpospolita Polska zajmuje obszar historycznie zamieszkiwany przez ludność pochodzenia polskiego.

Zgodnie z danymi Głównego Urzędu Statystycznego w 2011 roku w Polsce katolicyzm wyznawało 86,9% społeczeństwa, prawosławie – 1,31% i protestantyzm – 0,38%. Oprócz tego można się doliczyć prawie 200 innych wyznań, które jednak mają bardzo znikomy odsetek wyznawców[17]. Biorąc pod uwagę historycznie ukształtowaną i zapewnioną prawnie swobodę wyznaniową, wolność do skupiania się i budowania świątyń[18], ryzyko zaistnienia konfliktu na tle religijnym jest bardzo małe.

Należy natomiast wyraźnie zaakcentować, że istnieje poważne ryzyko zastosowania przeciwko nam dezinformacji medialnej, a przede wszystkim manipulowania opinią publiczną na portalach społecznościowych. Mogą też zostać na nasze państwo nałożone sankcje ekonomiczne i ograniczenia handlowe albo też wstrzymane dostawy ważnych surowców energetycznych. Bardzo groźne mogą okazać się w skutkach ataki cybernetyczne, zwłaszcza na systemy kierowania państwem i infrastrukturę krytyczną, a także system bankowości. Nie można jednak mówić w takim przypadku o wojnie hybrydowej. Musiałby bowiem zostać spełniony jeden ważny warunek, na który zwracał uwagę zarówno Hoffman, jak i Gierasimow, a mianowicie – jednoczesne użycie środków militarnych, niemilitarnych oraz propagandowych na pozio-

[13] Fake news – celowo przekazywane fałszywe informacje, rozprzestrzeniane przez drukowane i nadawcze serwisy informacyjne, media elektroniczne lub serwisy społecznościowe.

[14] Ł. Skoneczny: *Wojna hybrydowa*..., op.cit., s. 49.

[15] O. Wasiuta, S. Wasiuta: Rosyjska mass-medialna manipulacja informacją w wojnie hybrydowej przeciwko Ukrainie. „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2015 nr 20, s. 353.

[16] *Ludność. Stan i struktura demograficzno-społeczna*. Narodowy spis powszechny ludności i mieszkań 2011. GUS, Warszawa 2013.

[17] Departament Badań Społecznych i Warunków Życia GUS: *Wyznania religijne – stowarzyszenia narodowościowe i etniczne w Polsce 2009–2011*. GUS, Warszawa 2013.

[18] Wspólnoty religijne w Polsce działają na mocy przepisów Konstytucji RP o wolności sumienia i religii (m.in. art. 25 i 53) oraz ustawy o gwarancjach wolności sumienia i wyznania z 17 maja 1989 roku.

mie strategicznym, operacyjnym i taktycznym prowadzonego konfliktu.

Znając istotę wojny hybrydowej, należy przede wszystkim zidentyfikować krytyczne dla funkcjonowania państwa determinanty, których ochrona przed takim oddziaływaniem uniemożliwi osiągnięcie celów przez atakującego. Problemem tkwi w tym, że takie elementy mogą występować we wszystkich sferach działalności państwa, zatem należy skupić się na najistotniejszych. Konflikt ukraiński pokazuje, że elementami krytycznymi mogą być np.: surowce energetyczne, finanse państwa, ustrój i system polityczny, stan gospodarki, potencjał bojowy sił zbrojnych, pozycja międzynarodowa, struktura etniczna i narodowościowa ludności i wiele innych.

Kolejnym krokiem powinno być zidentyfikowanie luk i słabości mogących występować w wybranych elementach oraz podjęcie działań zmierzających do zwiększenia odporności na działania hybrydowe. Konieczne jest zorganizowanie współdziałania sił zbrojnych z władzami cywilnymi. Celem współpracy powinno być przede wszystkim ograniczenie negatywnego wpływu ludności cywilnej na prowadzoną operację oraz ustanowienie i utrzymanie pełnego współdziałania sił wojskowych z lokalną społecznością i instytucjami pozamilitarnymi. Bliski kontakt wojska z ludnością cywilną pozwala na szybszą identyfikację zagrożeń hybrydowych (np. stwierdzenie występowania wrogiej propagandy, czy nawet tzw. zielonych ludzików) i ich neutralizację.

W naszych siłach zbrojnych dostrzega się możliwość wystąpienia konfliktu hybrydowego, w związku z tym uwzględniono tę problematykę w programie szkolenia. Podczas ćwiczeń „Borsuk ’16”, w których brała udział 10 Brygada Kawalerii Pancernej, ćwiczono epizody takiego konfliktu. W scenariuszu założono, że nastąpią poważne napięcia społeczne na obszarze kraju, a przez granice zaczną przenikać grupy dywersantów, które będą dopuszczać się sabotażu. Reagując na negatywne zjawiska, ćwiczący dowódca musiał zorganizować współpracę z przedstawicielami układu pozamilitarnego, m.in. administracji państwowej i samorządowej, oraz z policją i strażą pożarną. Ponadto współdziałanie z innymi rodzajami sił zbrojnych oraz z pododdziałami NATO w warunkach zagrożeń hybrydowych było jednym z celów tych ćwiczeń.

Ostatnim i może najważniejszym aspektem związanym z zapobieganiem zagrożeniom hybrydowym jest zbudowanie międzynarodowego systemu współpracy, na przykład w ramach Sojuszu Północnoatlantyckiego lub Unii Europejskiej, pozwalającego na zintegrowanie wysiłków wielu państw. Problem został już dostrzeżony, o czym przekonuje choćby zwiększona obecność wojsk Sojuszu przede wszystkim w krajach nadbałtyckich i Polsce.

WIELE DO ZROBIENIA

Strony będące w stanie wojny zawsze dążyły do zadania ciosu wszelkimi środkami, nie tylko militarnymi. Wraz z pojawieniem się lotnictwa i innych nowoczesnych systemów walki wojny zaczęły oddziaływać na cały obszar państw zaangażowanych w konflikt. Wzajemne uzależnienie państw od dostaw surowców naturalnych, przede wszystkim energetycznych, stworzyło nowe środki nacisku gospodarczego. Ponadto obecny rozwój technologii oraz postępująca globalizacja dają agresorowi kolejne narzędzia, takie jak: dezinformacja, propaganda medialna, manipulowanie opinią publiczną i cyberataki na infrastrukturę krytyczną, które są niezauważalne dla społeczeństwa, a przynoszą poważne negatywne skutki dla bezpieczeństwa państwa i obywateli.

Wojna hybrydowa nie jest zjawiskiem nowym, jej elementy bowiem występowały w większości konfliktów zbrojnych i politycznych. Nowe natomiast jest to, że skoordynowane działania hybrydowe stają się podstawową formą osiągania celów politycznych i ekonomicznych, zastępując walkę zbrojną. Ponadto identyfikacja i zrozumienie tych zagrożeń pozwala na przygotowanie się na ewentualny atak. Nie oznacza to jednak, że nasz kraj jest bezpieczny, ponieważ z łatwością można zastosować przeciwko niemu wiele ataków hybrydowych, np. dezinformację i cyberataki. Pojawienie się zjawiska wojny hybrydowej nie musi oznaczać końca konfliktów konwencjonalnych, do których najczęściej są przygotowywane siły zbrojne. Jest ono natomiast utrudnieniem, generując nowe wyzwania dla bezpieczeństwa państwa. Ważne jest zatem jego zrozumienie przez społeczeństwo, przede wszystkim jednak przez państwa członkowskie NATO, co pozwoli na skuteczniejsze przeciwdziałanie temu zagrożeniu. ■

WEDŁUG NARODOWEGO SPISU POWSZECHNEGO PRZEPROWADZONEGO W 2011 ROKU NARODOWOŚĆ POLSKĄ ZADEKLAROWAŁO 97,09% ANKIETOWANYCH

Cyberprzestrzeń – część teatru działań hybrydowych

ZWIĘKSZAJĄCA SIĘ ZALEŻNOŚĆ OD SIECI I SYSTEMÓW TELEINFORMATYCZNYCH WSKAZUJE NA TO, ŻE BĘDZIE TO OBSZAR CHĘTNIE WYKORZYSTYWANY W SCENARIUSZACH DZIAŁAŃ MILITARNYCH.

ppłk dr inż. Robert Janczewski

Autor jest adiunktem w Zakładzie Bezpieczeństwa Cyberprzestrzeni Instytutu Działań Informacyjnych Wydziału Wojskowego Akademii Sztuki Wojennej.

Na wstępie zaryzykuję stwierdzenie, z pewnością bliską stu procent, że działania w cyberprzestrzeni oraz hybrydowe są określeniami równie popularnymi, jak i niejednoznacznymi. Autorzy podejmujący się opisu cyberprzestrzeni oraz hybrydowości niejednokrotnie nie są zgodni w swoich poglądach. Ich punkty widzenia przedstawione w opracowaniach różnią się od siebie, a wiele opisów jest niestety swoistym podążaniem za cyber- i hybrydmodą. Taki stan jest wyjątkowo niekorzystny, a nawet szkodliwy dla bezpieczeństwa i obronności państwa. Bez paradygmatów w tych sferach działania na rzecz bezpieczeństwa i obronności będą jedynie pozorowane.

Dzisiaj mamy do czynienia z nowym, nieznanym dotychczas (i niedostatecznie zbadanym) fragmentem rzeczywistości. Wrogie podmioty, aby zapewnić sobie przewagę nad ofiarą, stosują coraz nowsze metody i techniki oraz wykorzystują coraz bardziej wyrafinowane narzędzia. Walki toczą się już nie tylko z użyciem bomb i karabinów, lecz także bitów i bajtów.

MROCZNA STRONA SPOŁECZEŃSTWA

W prezentowanym opracowaniu cyberprzestrzeń jest rozumiana jako *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju*

PK/DZIAŁ GRAFICZNY
MOPIC, DIUNO/FOTOLIA

ŚWIAT WIRTUALNY

Dzisiaj walki toczą się już nie tylko z użyciem bomb i karabinów, lecz także bitów i bajtów.

sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[1]. Definicja ta jest rozwinięciem definicji zawartej w ogłoszonej 25 września 2002 roku *Ustawie z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, w której cyberprzestrzeń określono jako *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (DzU 2017 poz. 570), *wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Czytając tę definicję, za sprawą zawartych w niej odsyłaczy do innych aktów prawnych, można odnieść wrażenie, że została napisana przez prawników dla prawników. Natomiast działania hybrydowe będą rozumiane jako […] *szereg różnych rodzajów działań wojennych, obejmujących konwencjonalne zdolności, nieregularne taktyki i formacje, akty terrorystyczne obejmujące masową przemoc i przymus oraz przestępczość kryminalną*[2].

Najnowsza historia konfliktów międzynarodowych wykazała, że wraz ze wzrostem uzależnienia społeczeństw od informatyzacji tylko kwestią czasu było wykorzystanie cyberprzestrzeni do osiągnięcia zarówno taktycznej, operacyjnej, jak i strategicznej przewagi w walce. Ludzkość stanęła zatem w punkcie, w którym działania w cyberprzestrzeni oraz za jej pośrednictwem stały się istotną częścią działań hybrydowych. Dzieje się to za sprawą wzrostu atrakcyjności przejęcia i posiadania kontroli nad sieciami i systemami teleinformatycznymi oraz infrastrukturą dzięki nim funkcjonującą. W rozwiniętych cywilizacjach infrastruktura krytyczna dla funkcjonowania państwa (energia elektryczna, łączność, woda, transport, finanse itd.) opiera się na cyberprzestrzeni. Wojskowe systemy wsparcia dowodzenia i kierowania środkami walki również są od niej uzależnione, podobnie jak wszystkie najbardziej zaawansowane technologie dzisiejszego pola walki.

Doświadczenia współczesnych konfliktów pokazują, jak wyrafinowane i niebezpieczne są działania wykorzystujące cyberprzestrzeń do osiągania, w poczuciu anonimowości, własnych celów. Nawet jeśli prawdopodobieństwo atrybucji jest duże, to dzięki dobremu przygotowaniu cyberataku nie będzie możliwe jednoznaczne wskazanie jego autora, a nawet jeśli, to międzynarodowy porządek prawny nie stwarza warunków do wyciągnięcia konsekwencji wobec adwersarza. Dlatego każde państwo, które ma pewne zdolności w sferze cyberbezpieczeństwa, ale nie prowadzi odpowiedniej polityki w tej dziedzinie, będzie musiało się liczyć w przyszłości z porażką. Cyberoperacje zaplanowane w ramach działań hybrydowych mogą obejmować w szczególności działania wyspecjalizowanych jednostek wojskowych, służb wywiadowczych, organizacji, grup hakerskich lub insajderów.

ATRAKCYJNOŚĆ CYBERPRZESTRZENI

Cyberprzestrzeń jako pole walki charakteryzuje się wyjątkowo atrakcyjnymi z punktu widzenia prowadzenia działań militarnych cechami. Umożliwia oddziaływanie na przeciwnika znajdującego się w znacznej odległości w krótkim czasie, bez ryzyka narażania życia żołnierzy. Prowadzenie działań w domenach fizycznych, czyli na lądzie, morzu lub w powietrzu, jest uzależnione od uwarunkowań geograficznych. Natomiast działania wykorzystujące cyberprzestrzeń nie są ograniczane geograficznie. Działania te zależą jednak od rozproszonych infrastruktur sieciowych, czyli fizycznej warstwy cyberprzestrzeni.

Fizyczną warstwę sieciową tworzą urządzenia teleinformatyczne oraz infrastruktura w pozostałych domenach (ląd, morze, powietrze, przestrzeń kosmiczna). Zapewniają one przechowywanie, transmisję i przetwarzanie informacji oraz bazy danych i połączenia, które przesyłają dane między komponentami sieci. Te zaś obejmują sprzęt i infrastrukturę, np. komputery, urządzenia pamięci, urządzenia sieciowe oraz łącza przewodowe i bezprzewodowe. Składniki fizycznej warstwy sieciowej wymagają fizycznych zabezpieczeń chroniących przed fizycznymi uszkodzeniami lub nieautoryzowanym dostępem fizycznym, dzięki któremu możliwe będzie uzyskanie dostępu logicznego. Fizyczna warstwa sieci podczas cyberdziałań jest pierwszym punktem odniesienia do określenia położenia geograficznego oraz odpowiednich ram prawnych[3].

Mimo iż w cyberprzestrzeni można łatwo i szybko przekraczać granice geopolityczne, nadal istnieją kwestie suwerenności związane z domenami fizycznymi. Każdy materialny składnik cyberprzestrzeni jest własnością publicznego lub prywatnego podmiotu, który może kontrolować (czasem ograniczać) dostęp do własnych zasobów. Te wyjątkowe cechy muszą być brane pod uwagę na wszystkich etapach planowania działań[4]. Z perspektywy cyberochrony i cyberobrony możliwość przeprowadzenia szybkiego cyberataku wymusza posiadanie systemów ochronnych i obronnych automatycznie reagujących na cyberataki w czasie rzeczywistym lub co naj-

[1] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Warszawa 2015.

[2] F. Hoffman: *Conflict in the 21st Century: The Rise of Hybrid Wars. Monograph, Potomac Institute for Policy Students,* Virginia 2007, s. 29.

[3] *Joint Publication 3-12, Cyberspace Operations*, 8 June 2018.

[4] Ibidem.

mniej quasi-rzeczywistym. Systemy te, aby mogły być skuteczne, powinny mieć możliwie najlepsze moce obliczeniowe. Unikatowe cechy cyberprzestrzeni sprawiają, że jest ona atrakcyjna także w przerwach między działaniami konwencjonalnymi. Podczas nich można z powodzeniem przeprowadzać cyberataki.

Cyberprzestrzeń stwarza również warunki do skrytego działania. Identyfikacja cyberdziałań w większości opiera się na metodzie faktów dokonanych. Oznacza to, że analizowane cyberataki to te, które już nastąpiły. Dobrze przygotowany cyberatak, nawet jeśli zawiera elementy już znane, jest inny, nowatorski (techniki, narzędzia) w stosunku do poprzednich. Ponadto wspomniana anonimizacja działań stanowi mocny atrybut podmiotu atakującego. Atakujący ma możliwość anonimowego działania w cyberprzestrzeni bez pozostawienia śladów identyfikacyjnych. Może dzięki zastosowaniu odpowiednich technik i narzędzi ukryć się za innymi podmiotami, takimi jak: indywidualni użytkownicy sieci i systemów teleinformatycznych, grupy hakerskie, podmioty przestępcze lub nawet zagraniczne agencje czy państwa. Cyberprzestrzeń pozwala atakującemu zminimalizować ryzyko ujawnienia, oskarżenia i kontrataku. Świadczy o tym fakt, że dotychczas za przeprowadzenie cyberataków nie zostało ukarane żadne państwo. W działaniach konwencjonalnych na polu walki zazwyczaj wiadomo, kto zaatakował pierwszy, jaka przestrzeń została zdobyta, podczas działań w cyberprzestrzeni nie jest to tak oczywiste lub w ogóle nie jest możliwe do określenia.

Cyberprzestrzeń stwarza warunki do działań skutkujących sprzecznymi konsekwencjami. Z jednej strony możliwość przeprowadzenia kontrataku może być ograniczona, gdyż zaatakowany podmiot nie będzie miał podstaw lub zdolności do odpowiedzi. Z drugiej zaś istnieje możliwość niekontrolowanej eskalacji. Jest to związane z inną cechą działań w cyberprzestrzeni. Otóż wbrew powszechnej opinii, że działania wykorzystujące cyberprzestrzeń są bezkrwawe, cyberataki mogą być przyczyną śmierci dużej liczby ludzi. Zniszczenia i pozbawianie ludzkiego życia mogą nastąpić w wyniku uszkodzenia, zakłócenia działania lub zniszczenia obiektów krytycznych dla funkcjonowania państwa (np. elektrownie, zapory wodne, rafinerie czy zakłady produkcyjne, np. chemiczne), opierających swoje funkcjonowanie na sieciach i systemach teleinformatycznych. Anonimizacja cyberdziałań może sprawić, że nawet jeśli cyberataki spowodują ofiary śmiertelne i ciężkie uszkodzenia zdrowia, nie będzie możliwa adekwatna reakcja lub choćby pociągnięcie do odpowiedzialności żadnego podmiotu ze względu na brak solidnych dowodów tożsamości atakującego. Dlatego możliwość wyrządzania dużych szkód w funkcjonowaniu państwa bez niszczenia jego infrastruktury fizycznej lub zabijania ludzi może zostać uznana za pożądaną cechę cyberprzestrzeni przez planującego wrogie działania.

O atrakcyjności cyberprzestrzeni jako obszaru działań wykorzystywanego w czasie działań hybrydowych może świadczyć ekspercki ranking SANS Institute z 2008 roku. Owa klasyfikacja wskazuje dziesięć najważniejszych cyberzagrożeń:

1. Rosnące wyrafinowanie ataków na witryny sieci Web, wykorzystujących luki w zabezpieczeniach przeglądarek, szczególnie w witrynach „zaufanych".
2. Wzrost zaawansowania i skuteczności ataków botnet[5].
3. Działania cyberszpiegowskie prowadzone przez organizacje dysponujące odpowiednimi zasobami, które chcą pozyskiwać duże ilości danych, w szczególności z wykorzystaniem ukierunkowanego phishingu.
4. Zagrożenia dla telefonów komórkowych, zwłaszcza iPhone'ów i wykorzystujących system Android oraz przeznaczonych do komunikacji VoIP (Voice over Internet Protocol).
5. Ataki insajderów.
6. Zaawansowana kradzież tożsamości z trwałych botów[6].
7. Wzrost złośliwości oprogramowania szpiegującego.
8. Wykorzystywanie luk w zabezpieczeniach aplikacji internetowych.
9. Wzrost wyrafinowania inżynierii społecznej, w tym łączenie phishingu z usługą VoIP czy phishing zdarzeń[7].
10. Ataki łańcucha dostaw infekujące urządzenia konsumenckie (dyski USB, systemy GPS, ramki do zdjęć itp.) rozpowszechniane przez zaufane organizacje.

Kolejna cecha, która powoduje, że cyberprzestrzeń jest wykorzystywana w działaniach hybrydowych, to standaryzacja. Funkcjonowanie cyberprzestrzeni opiera się głównie na rozwiązaniach firm o globalnym zasięgu (np. Microsoft, Cisco, IBM, Hewlett-Packard, Intel, Lenovo, Check Point, 3Com, Juniper Networks, Fortinet czy choćby Huawey), których produkty są rozlokowane na całym świecie. Uniwersalny charakter omawianej domeny kształtują również systemy operacyjne, na przykład Windows,

[5] Botnet to sieć przejętych komputerów wykorzystywanych do rozproszonego ataku odmowy obsługi (DDoS).

[6] Bot (skrót od robot) jest programem komputerowym (np.: aplikacja lub skrypt) realizującym określone funkcje w zastępstwie człowieka – automatyzacja niektórych czynności. Przykładem komercyjnego ich wykorzystania są automatyczni asystenci obsługujący klientów on-line (Chatboty). Boty mogą być użyteczne, np. programy do analizy aukcji internetowych (Allegro), lub szkodliwe, np. programy infekujące komputer oprogramowaniem złośliwym i zamieniające w komputer zombie (Malware Bots).

[7] S.R. Chabinsky: *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*. „Journal of National Security Law & Policy", Vol. 4 No. 1, Washington, DC, August 2010, p. 27–39.

PAWEŁ KĘPKA

NOWY OBSZAR WALKI

Cyberprzestrzeń jako pole walki odznacza się wyjątkowo atrakcyjnymi z punktu widzenia prowadzenia działań militarnych cechami. Umożliwia oddziaływanie na przeciwnika znajdującego się w znacznej odległości w krótkim czasie, bez ryzyka narażania życia żołnierzy.

Unix czy najpopularniejsze dystrybucje Linux. Standaryzacja wiąże się z dużym ryzykiem dla atakowanej strony. Hakowanie komercyjnego (niededykowanego) oprogramowania zabezpieczającego bazy danych może przynieść powodzenie napastnikowi, ponieważ znane są kody źródłowe oraz struktura oprogramowania.

Cyberprzestrzeń stwarza wrogim podmiotom także warunki do pozyskiwania lub zmiany wartości wielu danych z urządzeń podłączonych do sieci i systemów teleinformatycznych. Dane geograficzne, termiczne, mechaniczne lub inne pozyskiwane z pozostałych domen za pomocą czujników (sensorów) w sieciach i systemach teleinformatycznych są przetwarzane na bity i odwrotnie. Jeśli na ich podstawie efektory wykonują określone działanie, to atakujący wykorzystujący cyberprzestrzeń, wchodząc w ich posiadanie i zmieniając ich parametry, może wpłynąć na efekty tego działania, tym samym stwarzając sobie korzystne warunki do prowadzenia ataków w domenach geograficznych.

HISTORIA CYBERDZIAŁAŃ

Niezaprzeczalnie powszechną praktyką podczas rozważań nad przeszłymi, teraźniejszymi lub przyszłymi konfliktami zbrojnymi jest odwoływanie się do historycznych analogii. Jednak cyberprzestrzeń jest nowym obszarem i charakteryzuje się niespotykanymi w przeszłości unikatowymi właściwościami. Pojawia się w związku z tym pewna bariera poznawcza. Dotychczasowe doświadczenia w konfliktach, w kontekście wykorzystania cyberprzestrzeni w działaniach hybrydowych, są mimo wszystko ograniczone. Dlatego też jednoznaczny osąd, dotyczący skutków takich działań oraz potencjału eskalacyjnego, jest trudny. Co więcej, metody, techniki czy narzędzia wykorzystywane przez wrogie podmioty, ich zachowania, które dowódcy czy ich doradcy w dziedzinie cyberbezpieczeństwa muszą uwzględniać w procesie dowodzenia, mogą się okazać bezprecedensowe. Mowa tutaj o: cyberszpiegostwie, zdalnych kradzieżach danych i informacji, politycznych subwencjach na wrogą działalność w cyberprzestrzeni, subwersjach[8] czy cyberterroryzmie. Przykładami cyberataków sponsorowanych przez państwo są: szpiegostwo (np. Titan Rain, Moonlight Maze), wsparcie dla precyzyjnych nalotów wojskowych (np. Operation Orchard) czy sabotaż (np. Stuxnet)[9].

Jednym z klasycznych przykładów wykorzystania cyberprzestrzeni w scenariuszu konfliktu hybrydowego jest przypadek estoński. Zgodnie z decyzją rządu Estonii, wyrażoną w ustawie o likwidacji „zakazanych obiektów" 26 kwietnia 2007 roku, rozpoczęto demontaż i relokację z centrum stolicy na oddalony o kilka kilometrów cmentarz estońskich sił zbrojnych radzieckiego pomnika Wyzwoliciela Tallina, potocznie zwanego Brązowym Żołnierzem. Rozbiórka monumentu i przeniesienie prochów rosyjskich żołnierzy pochowanych obok niego wywołały ostry sprzeciw Rosji i rosyjskiej mniejszości w Estonii. Pomnik ten jest ważny dla Rosjan zamieszkujących Estonię, ponieważ upamiętnia tych, którzy zginęli w walce z hitlerowskim okupantem.

[8] Subwersja (Subversion) to działania mające na celu osłabienie wojskowej, ekonomicznej, psychologicznej, politycznej siły lub morale sprawujących władzę. „Joint Publication 1-02", Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 February 2015), p. 228. 29.07.2018.

[9] S.P. White: *Understanding Cyberwarfare: Lessons from the Russia-Georgia War.* https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

Natychmiast po rozpoczęciu procedury przenoszenia pomnika, od 26 kwietnia do 18 maja 2007 roku, przypuszczono zmasowany cyberatak na Estonię. Był on połączony z demonstracjami rosyjskiej diaspory w Tallinie oraz rosyjskiej organizacji młodzieżowej „Naszi", nazywającej siebie Młodzieżowym Demokratycznym Antyfaszystowskim Ruchem, w ambasadzie estońskiej w Moskwie. Jednocześnie Rosja wprowadziła sankcje wobec Estonii.

Działania w cyberprzestrzeni, polegające na przeprowadzeniu rozproszonych ataków odmowy usługi (distributed denial of services, skrót DDoS), botnet (około miliona komputerów „zombie") czy hakowania objęły estońskie biura rządowe, ministerstwo obrony, ministerstwo sprawiedliwości, partie polityczne, policję, największe banki (Hansapank, SEB Ühispank), infrastrukturę telekomunikacyjną, media, serwery nazw, Internet czy szkoły publiczne[10]. Z punktu widzenia trudności w identyfikacji autora cyberataku znaczące jest użycie botnetów. Ich wykorzystanie wykluczyło jednoznaczne wskazanie źródła ataków (podmiotu odpowiedzialnego za nie). Dość istotnym aspektem tej sytuacji jest fakt, że cyberataki przeprowadzone na Estonię mogły być sondą działania (procedur) estońskich sił obronnych oraz reakcji Unii Europejskiej i NATO. Mimo że władze estońskie obarczyły winą Federację Rosyjską, to w ciągu pięcioletniego śledztwa nie udowodniono jednoznacznego działania państwa rosyjskiego. Z końcem lipca 2012 roku, po wyczerpaniu formuły śledztwa, Biuro Prokuratora Generalnego Estonii zakończyło je bez sukcesu.

Przytoczony przykład wskazuje, iż wykorzystanie cyberprzestrzeni w czasie działań hybrydowych służyło, oprócz wywoływania zamieszek i wprowadzania sankcji, do pogłębiania sytuacji kryzysowej w kraju. Cyberataki były skierowane nie tylko przeciwko jednemu krajowi, lecz także poddały próbie m.in. Sojusz Północnoatlantycki. Skala tych działań była znacząca, ponieważ nie powodowały one jedynie uciążliwości czy niedogodności w państwie, lecz sparaliżowały jego funkcjonowanie.

Kolejny przykład wykorzystania cyberprzestrzeni w działaniach hybrydowych dotyczy konfliktu rosyjsko-gruzińskiego w 2008 roku. Do sierpnia 2008 roku cyberataki były łączone z innymi formami działań, ale nie towarzyszyły działaniom zbrojnym. Co prawda w miesiącach poprzedzających atak USA na Irak w marcu 2003 roku wojskowi planiści Pentagonu oraz amerykańskich agencji wywiadowczych rozważali przeprowadzenie cyberataków przed inwazją. Ich celem byłoby zamrożenie miliardów dolarów na rachunkach bankowych Saddama Husajna oraz przejęcie kontroli i sparaliżowanie systemu finansowego jego rządu, aby pozbawić Irak pieniędzy na dostawy wojenne oraz wypłaty dla żołnierzy. Jednak Amerykanie wycofali się z tego posunięcia, gdyż zdali sobie sprawę, że system finansowy jest systemem ogólnoświatowym, a banki irackie są współzależne z bankami we Francji[11]. Napięte stosunki między Federacją Rosyjską a Republiką Gruzji nie były same w sobie niczym nadzwyczajnym, ponieważ w przeszłości miały miejsce gwałtowne konflikty sięgające dekad. Ze względu na prozachodnią politykę zagraniczną Gruzji napięcia między tymi dwoma krajami wzrastały. Punktem krytycznym w konflikcie rosyjsko-gruzińskim była przeprowadzona 7 sierpnia interwencja wojskowa Gruzji w Osetii Południowej, rzekomo w celu zapobieżenia osetyjskiemu ostrzałowi gruzińskiego terytorium. To posunięcie skłoniło Rosję do dokonania, na dużą skalę, inwazji lądowej, powietrznej i morskiej na Gruzję. Jak podała rosyjska agencja informacyjna Sputnik, jeden z czołowych rosyjskich dyplomatów oskarżył zagraniczne media o progruzińską stronniczość w związku z toczącym się konfliktem. Ponadto według Rosji od początku ofensywy gruzińskie siły zbrojne zabiły około 2 tys. cywili z Południowej Osetii, głównie obywateli Rosji, a 34 tys. mieszkańców zostało zmuszonych do ucieczki do Rosji. W odpowiedzi na gruzińskie ataki Rosja wysłała czołgi i wojska do prowincji oraz przeprowadziła serię nalotów na gruzińskie cele wojskowe[12].

Jednak konflikt między Gruzją a Rosją był bezprecedensowy. Ofensywa przeciwko Gruzji nie rozpoczęła się tradycyjnie od czołgów i myśliwców, lecz w cyberprzestrzeni. Rosyjskie wojska po południowej stronie tunelu Rokijskiego, czyli w Republice Południowej Osetii, pojawiły się rankiem 8 sierpnia 2008 roku, natomiast strony internetowe gruzińskiego rządu oraz mediów uległy awarii 7 sierpnia, czyli na dzień przed inwazją. Przeprowadzone cyberataki wydają się być wysiłkiem w cyberprzestrzeni zsynchronizowanym z wojskowym działaniem na lądzie, w powietrzu i na morzu. W Gruzji Rosja po raz pierwszy połączyła działania kinetyczne z cybernetycznymi, informacyjnymi i psychologicznymi. Warto również zauważyć, że podczas tych walk Maxim Kuznetsov, dyrektor oddziału informatyki rosyjskiego serwisu informacyjnego RIA Novosti, oświadczył, że: *Serwery DNS jak i sama strona są dotkliwie atakowane*. Strona rosyjska oskarżyła o tę aktywność gruzińskich hakerów. Interesujące wydaje się, że na ponad dwa tygodnie przed rosyjską inwazją wojskową, czyli już 20 lipca, nastąpił cyberatak DDoS na Gruzję. Setki tysięcy komputerów „zombie" na całym świecie przejętych przez rosyj-

[10] V. Joubert: *Five years after Estonia`s cyber attacks: lesson learned for NATO?* Research Paper – NATO Defense College, Rome - No. 76, May 2012.

[11] J. Markoff, T. Shanker: *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*. https://www.nytimes.com/2009/08/02/us/politics/02cyber.html/. 25.07.2018.

[12] RIA Novosti hit by cyber-attacks as conflict with Georgia rages, https://sputniknews.com/russia/20080810115936419/. 25.07.2018.

skie wirusy blokowało gruzińskie strony internetowe, w tym strony prezydenta, parlamentu, ministerstwa spraw zagranicznych, agencji prasowych i banków. Te jednak zamknęły serwery przy pierwszych symptomach cyberataku[13]. Ponadto zniszczono stronę internetową gruzińskiego prezydenta (website defacement).

W dniu, kiedy rozpoczęły się walki zbrojne, pojawiły się witryny internetowe, takie jak StopGeorgia.ru, z listą stron nominowanych do cyberataku, instrukcjami, jak je przeprowadzić, a nawet stroną raportu po akcji. Pouczające jest to, że wszystko w serwisie było już gotowe: możliwość rejestracji, złośliwe oprogramowanie do pobrania, plany, sondy oraz instrukcje – to wszystko w pierwszym dniu konfliktu[14]. Zastosowane techniki wskazują, że szczegółowy plan kampanii przeciwko gruzińskim serwisom internetowym opracowano na długo przed konfliktem. Natychmiast po wkroczeniu rosyjskich sił konwencjonalnych użyto specjalnie zaprojektowanego oprogramowania do ich atakowania. Narzędzie wykorzystane do usunięcia jednej ze stron internetowych Gruzji zostało utworzone w marcu 2006 roku, ale zapisane do użytku w kampanii w sierpniu 2008 roku. Atakujący również nadzwyczajnie szybko zarejestrowali nowe nazwy domen i utworzyli nowe strony internetowe, wskazując tym samym, że już przeanalizowali cel, napisali skrypty ataku i być może nawet wcześniej przygotowywali kampanię wojny informacyjnej[15].

Na początkowym etapie konfliktu zbrojnego przeprowadzono cyberataki (zakłócające usługi) na strony internetowe Ministerstwa Obrony, Ministerstwa Spraw Zagranicznych, Parlamentu, Banku Narodowego, angielskojęzyczne dzienniki „The Messenger" i „Civil Georgia", internetowy kanał telewizyjny „Rustavi 2"[16], firmy transportowe oraz prywatnych operatorów telekomunikacyjnych, przy czym strony internetowe Ministerstwa Spraw Zagranicznych i Banku Narodowego zniszczono.

Poza bezpośrednim atakiem na gruzińskie instytucje państwowe działania w cyberprzestrzeni były częścią większej walki informacyjnej między rosyjskimi a gruzińskimi i zachodnimi mediami.

Blokadę internetową powiązano z pięcioma autonomicznymi systemami, czterema w Rosji i jednym w Turcji, kontrolowanymi przez kryminalny syndykat Russian Business Network. Potem pojawiły się fałszywe doniesienia prasowe, które infekowały trojanami komputer każdego, kto kliknął na odpowiedni link. Biorąc pod uwagę dowody kryminalistyczne, sytuację geopolityczną, czas i relacje między rządem a młodzieżą i grupami przestępczymi, nietrudno było wywnioskować, że za tymi zmasowanymi cyberatakami stał Kreml. Jednak podobnie jak w Estonii, jednoznacznego udziału Rosji w działaniach w cyberprzestrzeni nie udowodniono.

CYBERPRZESTRZEŃ DZIĘKI MOŻLIWOŚCI STWARZA WARUNKI DO ZREALIZOWANIA

Znaczenia cyberprzestrzeni dowodzi jeden z komentarzy umieszczony pod artykułem on-line, prezentujący analizę ataku DDoS na serwis internetowy prezydenta Gruzji. Internauta przedstawiający się jako Serge 10 sierpnia 2008 roku o 21.52 napisał: *Jak długo USA i tak zwane „kraje demokratyczne" będą ukrywać prawdę o tej wojnie? Przed jej wybuchem około 1000 żołnierzy piechoty morskiej i instruktorów wojskowych szkoliło żołnierzy gruzińskich. USA, Izrael i Ukraina sprzedały Gruzji ogromne ilości broni. W ostatnich dniach w Południowej Osetii znaleziono martwych afroamerykańskich instruktorów wojskowych. Nowy Hitler, Saakaszwili, który zabił 2000 osób, głównie dzieci, osoby starsze chroniony jest przez USA, Izrael, Ukrainę, i Wielką Brytanię i inne „zaprzyjaźnione państwa". Ludobójstwo dyktatora Saakaszwilego nagradzane jest przez kraje sprzedażą broni. Prasa, telewizja, radio opowiadają tę samą historię o rosyjskiej inwazji, ale nikt nie mówi, że ta wojna to zaplanowane wydarzenie, dawno temu przez dobrze opłacanego dyktatora Saakashviliego. Dlaczego ludzie zachodu nie mają informacji z Południowej Osetii, ale fałszywe informacje z telewizyjnych korporacji? To jest chwila prawdy i wcześniej czy później ludzie i kraje, które się tego dopuściły, zostaną ukarane przez Boga*[17].

[13] T. Wentworth: *How Russia May Have Attacked Georgia's Internet,* https://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111/. 20.07.2018.

[14] D. Smith: *How Russia Harnesses Cyberwarfare.* Defense Dossier, Issue 4, American Foreign Policy Council, Washington, D.C., August 2012, p. 9.

[15] R. Weitz: Global Insights: *Russia Refines Cyber Warfare Strategies,* https://www.worldpoliticsreview.com/articles/4218/global-insights-russia-refines-cyber-warfare-strategies/. 30.07.2018.

[16] Rustawi 2 – gruzińska telewizja prywatna.

[17] J. Nazario: *Georgia On My Mind – Political DDoS*, https://asert.arbornetworks.com/georgia-on-my-mind-political-ddos/. 31.07.2018.

Wpis ten jest doskonałym przykładem oddziaływania na odbiorcę za pośrednictwem Internetu. Nie jest do końca jasne, czy dokonał go niezadowolony internauta, który tak myśli naprawdę, czy może ktoś, kto świadomie spreparował tekst, nadając mu taką właśnie oś narracji.

Reasumując, w przeciwieństwie do cyberataków przeprowadzonych na Estonię w 2007 roku, te w Gruzji były uzupełnieniem bombardowania rosyjskich sił powietrznych oraz rażenia wojsk lądowych w świecie rzeczywistym. Korzystne warunki dla takiego scenariusza działań hybrydowych wynikały z infrastruktury teleinformatycznej Gruzji. Prawie połowa z trzynastu połączeń do Internetu przebiegała przez Rosję. Sytuacja jednak się zmieniła. Jak podał K. Mshvidobadze w czasie spotkania w Georgian Foundation for Strategic and International Studies podczas wystąpienia na temat *State-sponsored Cyber Terrorism: Georgia's Experience": Po 2008 roku kabel światłowodowy Poti (Batumi) – Varna „Kaukaz" obsługuje około 90% gruzińskiego Internetu*[18].

Trzecim wyrazistym przykładem popularności cyberprzestrzeni w działaniach hybrydowych jest konflikt na Ukrainie w 2013 roku. Ten już jest szeroko opisany w piśmiennictwie. W kontekście działań hybrydowych w popularnej encyklopedii internetowej „Wikipedia" możemy już przeczytać na temat wojny w Donbasie oraz konfliktu krymskiego. Według tego źródła wiedzy: *Wojna w Donbasie (konflikt na wschodniej Ukrainie) to wojna hybrydowa na terenie obwodów donieckiego i ługańskiego Ukrainy, rozpoczęta w kwietniu 2014. Zbrojne wystąpienie separatystów (wspieranych przez rosyjską armię i siły specjalne) dążących do oderwania tego terytorium od Ukrainy było poprzedzone przez marcowe wystąpienia prorosyjskie i kryzys krymski, które nastąpiły po rewolucji Euromajdanu*[19]. Natomiast kryzys krymski to *kryzys polityczny zapoczątkowany w 2014 roku na Półwyspie Krymskim na Ukrainie, będący efektem rewolucji Euromajdanu w tym kraju oraz interwencji wojskowej Rosji*[20].

Jednak szczegółowa analiza wydarzeń (w kontekście działań w cyberprzestrzeni) z tamtego czasu wydaje się przeczyć tym informacjom, szczególnie datowaniu początku konfliktu. Opisy te pomijają aspekt, którego nie powinno się pomijać – działań w cyberprzestrzeni. Według G. Pakharenko, cyberataki na Ukrainę rozpoczęły się 2 grudnia 2013 roku, kiedy stało się oczywiste, że protestujący nie zamierzają opuścić Majdanu. Cyberataki typu DDoS zostały skierowane na strony internetowe opozycji, większość z nich pochodziła z komercyjnych botnetów wykorzystujących oprogramowanie złośliwe BlackEnergy and Dirt Jumper[21].

ANONIMIZACJI WŁASNYCH DZIAŁAŃ, CYBERATAKU BEZ OBAWY O ODWET

W środę, 4 grudnia 2013 roku, na stronie „Anonops Communications"[22] umieszczono wpis zatytułowany: *Z miłości do Anonimowej Ukrainy – wyciek prywatnych e-maili niektórych członków ukraińskiego parlamentu*! Uwidocznia on, że działania w cyberprzestrzeni zaczęły się jednak przed 2014 rokiem. Warta przybliżenia jest skala cyberataków przeprowadzonych w czasie referendum w sprawie statusu Krymu przeprowadzonego 16 marca 2014 roku. Jak podaje niezależna międzynarodowa organizacja prasowa „The Christian Science Monitor"[23], „wymiana ognia" w cyberprzestrzeni między Rosją a Ukrainą rozpoczęła się w poniedziałek w tygodniu poprzedzającym referendum (10.03.2014). Działania te osiągnęły wówczas najwyższy poziom. Ukraińskie strony internetowe były atakowane do momentu, aż stały się bezużyteczne. W piątek 14 marca cyberataki tymczasowo sparaliżowały strony internetowe Kremla, rosyjskiego banku centralnego oraz rosyjskiego Ministerstwa Spraw Zagranicznych, choć władze rosyjskie zaprzeczyły, jakoby miały one coś wspólnego z kryzysem na Ukrainie. W niedzielę, czyli w dniu referendum, strony internetowe ukraińskiego rządu zostały uderzone falą 42 cyberataków. Miały one na celu wsparcie oderwania się Krymu od Ukrainy i dołączenia do Rosji. Zaobserwowanymi typami cyberataków były ataki DDoS, które strony internetowe zablokowały fałszywymi

[18] https://gfsis.org/media/download/GSAC/cyberwar/State-sponsored_Cyber_Terrorism.pdf/.20.07.2018.

[19] *Wojna w Donbasie*, https://pl.wikipedia.org/wiki/Wojna_w_Donbasie/.17.07.2018.

[20] *Kryzys krymski,* https://pl.wikipedia.org/wiki/Kryzys_krymski/. 17.07.2018.

[21] G. Pakharenko: *Cyber Operations at Maidan: A First-Hand Account*, [w:] K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine,* NATO CCD COE Publications, Tallinn 2015, pp. 59-66.

[22] *With love from Anonymous Ukraine - leak private emails of some members of the Ukrainian Parliament*!, http://anonopsofficial.blogspot.com/2013/12/with-love-from-anonymous-ukraine-leak.html./20.09.2017.

[23] https://www.csmonitor.com/World/Passcode/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine/. 19.07.2018.

danymi. Ataki te były tymi samymi, które przeprowadzono w roku 2008 w czasie konfliktu z Gruzją.

Ich cechą było to, że wielu napastników nie udało się zidentyfikować, ponieważ ataki zostały rozproszone na zbyt wiele atakujących komputerów na całym świecie. Ale przynajmniej niektóre ataki na Ukrainę można powiązać z dwoma dużymi botnetami przestępczymi – milionami komputerów na całym świecie, które były zainfekowane i kontrolowane przez złośliwe oprogramowanie.

W czasie konfliktu na Ukrainie 23 grudnia 2015 roku przeprowadzono również cyberataki na trzech ukraińskich dostawców energii elektrycznej. Najbardziej dotknięci byli konsumenci Przykarpackiego Zakładu Energetycznego, obsługującego obwód iwanofrankowski. Wyłączono 30 podstacji, a około 230 tys. obywateli tego kraju zostało pozbawionych dostaw prądu. Przerwa trwała od 1 do 6 godzin[24]. Na mniejszą skalę zaatakowano dwóch innych dostawców: Czerniowiecki Zakład Energetyczny, obsługujący obwód czererniowiecki, i Kijowski Zakład Energetyczny, obsługujący obwód kijowski.

Do przeprowadzenia cyberataków przestępcy użyli trojana BlackEnergy. Ukraińskie systemy komputerowe zostały zainfekowane oprogramowaniem złośliwym prawdopodobnie przez pobranie załącznika fałszywej wiadomości w postaci pliku Microsoft Office. Po aktywacji BlackEnergy pobrał kolejne złośliwe oprogramowanie KillDisk, które jest w stanie nie tylko usuwać pliki i dokonywać zmian w systemie komputerowym, lecz również zatrzymywać procesy systemów sterowania przemysłowego.

Skala cyberataków była w stanie zmniejszyć moc energii elektrycznej na obszarze Ukrainy, ponieważ jednocześnie zaatakowano trzech niezależnych jej

[24] K. Zetter: *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. 19.07.2018.

ENERGIA NA CELOWNIKU

Cyberatak jest w stanie zmniejszyć moc energii elektrycznej na obszarze zaatakowanego państwa. Systemy komputerowe elektrowni (dystrybutorów energii) zostają zainfekowane złośliwym oprogramowaniem. W czasie konfliktu na Ukrainie w 2015 roku przeprowadzono uderzenie na trzech ukraińskich dostawców energii elektrycznej. Wyłączono 30 podstacji, a około 230 tys. obywateli tego kraju zostało pozbawionych dostaw prądu. Przerwa trwała od 1 do 6 godzin.

TOOKAPIC/PIXABAY

dystrybutorów. Użyte techniki hakerskie do wspierania i wzmocnienia cyberataku zatrzymywały lub przynajmniej spowalniały procesy przywracania zasilania. W efekcie cyberataki wywołały odmowę usługi w call center. Odbiorcy energii elektrycznej nie byli w stanie zadzwonić do swojego dostawcy, co potęgowało i tak już chaotyczną sytuację.

Złośliwe oprogramowanie podobne do tego, którym zaatakowano trzy ukraińskie firmy energetyczne, zostało wykryte w sieci informatycznej głównego lotniska w Kijowie, Boryspolu. Sieć obejmuje kontrolę ruchu lotniczego na lotnisku.

W czasie ukraińsko-rosyjskiego konfliktu hybrydowego przeprowadzono także cyberatak na siły zbrojne Ukrainy. Jego obiektem była aplikacja Popr-D30.ark. Opracował ją od 20 lutego do 13 kwietnia 2013 roku na terenie Ukrainy oficer 55 Brygady Artylerii Yaroslav Sherstuk. Aplikacji tej używała do 2016 roku co najmniej jedna jednostka artylerii działająca we wschodniej Ukrainie. Umożliwiała ona szybsze przetwarzanie danych do strzelania. Ataku dokonano za pomocą złośliwego programu szpiegującego X-Agent (wersja dla systemu operacyjnego Android), zaprojektowanego do zbierania i przesyłania informacji do serwerów obsługiwanych przez hakerów. Dzięki temu Rosjanie mogli mieć dostęp do dokładnych pozycji ukraińskich żołnierzy. To z kolei ułatwiało namierzanie rozmieszczenia pododdziałów artylerii.

Wersja X-Agent dla Androida nie ma funkcji destrukcyjnej i nie zakłóca działania oryginalnej aplikacji Popr-D30.ark. Ma ona charakter strategiczny i umożliwia uzyskiwanie dostępu do kontaktów, wiadomości tekstowych SMS, dzienników połączeń i danych internetowych. Charakteryzuje ją potencjalna możliwość: mapowania składu i hierarchii jednostki, określania jej planów oraz triangulacji jej przybliżonej lokalizacji. Umożliwia identyfikację stref, w których działają wojska, i pomaga w ustaleniu priorytetów ich działania.

Cyberprzestrzeń stwarza również warunki do zjawiska zwanego trollingiem. W marcu 2015 roku ukraińska służba bezpieczeństwa oficjalnie ogłosiła, że to rosyjska Federalna Służba Bezpieczeństwa (FSB) stoi za propagandowymi działaniami przeciwko Ukrainie. Nie tylko ukraińskie i rosyjskie, lecz także wiarygodne zachodnie media są narażone na ryzyko podawania fałszywych informacji. Na przykład dziennik „Guardian" użył cytatu ze strony Facebooka dr. Rozovsky'ego, który twierdził, że *jest lekarzem leczącym separatystów po konfrontacji z proukraińskimi siłami w Odessie*. Wkrótce strona na Facebooku została ujawniona jako fałszywa i ustalono, że nie było takiej osoby jak dr Rozovsky. „Guardian" zamieścił później co prawda sprostowanie, jednak informacje zostały już rozpowszechnione i biorąc pod uwagę dobrą reputację medium, zostały uznane za prawdziwe[25].

NIEBEZPIECZEŃSTWO ZAGROŻEŃ WEWNĘTRZNYCH

Zarówno wojskowi, jak i osoby niebędące żołnierzami wiedzą o istnieniu oprogramowania złośliwego (malware), a w szczególności programów szpiegujących (spyware), oprogramowania szantażującego (ransomware), koni trojańskich, robaków czy choćby wirusów. Zdają sobie sprawę z zagrożeń pochodzących z inżynierii społecznej (inżynierii socjalnej, socjotechniki), której reprezentacją może być phishing, czyli metoda oszustwa polegająca na podszywaniu się przez oszusta (przestępcę) pod inny podmiot (osobę, organizację czy instytucję) w celu wyłudzenia interesujących go informacji (np. identy-

[25] *Internet trolling as a tool of hybrid warfare: the case of Latvia*, Latvian Institute of International Affairs, Riga Stradins University, Results of the study.

fikatorów użytkownika zwanych powszechnie loginami, haseł, numerów kart kredytowych czy wszelkich numerów PIN) lub nakłonienia ofiary do podjęcia określonych czynności[26]. Niektórzy może nawet bezpośrednio lub pośrednio doświadczyli skutków złowrogich narzędzi czy metod działania w cyberprzestrzeni lub za jej pośrednictwem.

Przytoczone przykłady stanowią zagrożenia zewnętrzne. W działaniach hybrydowych ten rodzaj zagrożeń wydaje się być oczywisty. Tymczasem sieci i systemy teleinformatyczne narażone są również na zagrożenia wewnętrzne. Na pierwszy rzut oka mogło by się wydawać, że te pierwsze są znacznie częstsze. Czy tak jest rzeczywiście? W poszukiwaniu odpowiedzi na to pytanie spójrzmy na działania tzw. insajderów (insider), czyli ludzi lub pracowników w organizacji czy instytucji mających informacje niedostępne dla innych[27]. W kontekście cyberprzestrzeni insajderem może być zarówno wtajemniczona „osoba z wewnątrz", czyli członek organizacji oraz pracownik instytucji, jak i dostarczająca produkty lub świadcząca usługi na rzecz określonego podmiotu (np. tester bezpieczeństwa, programista, administrator czy osoba zajmująca się konserwacją i naprawą sprzętu).

Działania podejmowane przez insajdera, w przeciwieństwie do zewnętrznych cyberataków, nie opierają się na nieautoryzowanym dostępie nieupoważnionych podmiotów do zasobów sieci i systemów teleinformatycznych. Dostęp jest autoryzowany, a osoby upoważnione do dokonywania określonych czynności postępują w granicach procedur bezpieczeństwa. Dlatego ich działalność nie będzie postrzegana jako cyberatak, lecz normalne użytkowanie zasobów. Trudność polega na identyfikacji nieuprawnionego działania i naruszenia zasad bezpieczeństwa przez autoryzowany podmiot. Niestety zagrożenia wewnętrzne w cyberbezpieczeństwie często są kojarzone jedynie ze złośliwymi użytkownikami (złośliwymi insajderami), tymczasem pracownicy postępujący nieumyślnie, nieświadomie powodują niekontrolowane wycieki danych i informacji, stanowiące niejednokrotnie aktywa organizacji bądź instytucji.

Wrogie działanie[28] insajdera ma niebagatelne znaczenie dla bezpieczeństwa i obronności państwa. Kluczowego znaczenia nabiera zdolność do wykrywania działań rządowych, wojskowych czy w sieciach i systemach teleinformatycznych ważnych dla bezpieczeństwa i obronności kraju.

Beztroska użytkowników sieci i systemów teleinformatycznych wynikająca z braku świadomości zachęca do włamania się do systemu. Jeśli pracownik kliknie na link w wiadomości spamowej lub nieświadomie doprowadzi do zainfekowania urządzenia, podmiot przeprowadzający cyberatak utwierdza się w przekonaniu, że obrał właściwy wektor ataku. To z kolei może zachęcić go do przygotowywania bardziej wyrafinowanych cyberataków. Z punktu widzenia cyberbezpieczeństwa równie niepożądane jest popełnianie takich błędów, jak wysyłanie wrażliwych plików na niewłaściwy adres. Takie nieumyślne postępowanie personelu może być zgubne w skutkach. Na te zachowanie adwersarze tylko czekają.

Gdy połączymy incydenty związane ze złośliwymi i nieumyślnymi użytkownikami, może się okazać, że ich liczba znacznie przekracza wszelkie inne cyberzagrożenia. Ponadto niezależnie od tego, czy działanie zostało podjęte złośliwie, czy nie, zostało podjęte przez pracownika lub osobę mającą legalny dostęp do zasobów, co nie jest dobrym prognostykiem na przyszłość.

Zagrożenia wewnętrzne są kosztowne i trudno sobie z nimi poradzić. Po pierwsze, te związane z zachowaniem poufności mogą pozostać niewykryte przez lata. Im dłużej zwleka się z podjęciem próby wykrycia naruszenia lub wycieku, tym więcej kosztów pochłonie usunięcie lub zmniejszenie liczby zdarzeń powodujących ryzyko, ich kontrolowanie oraz ograniczenie niewłaściwych postaw, nawyków czy zachowań.

Ponieważ odróżnianie szkodliwego działania od zwykłej pracy jest trudne, również trudne jest wykrywanie zagrożeń wewnętrznych. Kiedy pracownik pracuje z poufnymi danymi, prawie niemożliwe jest rozpoznanie, czy robi coś złośliwie, świadomie, czy nie. Pracownicy mogą łatwo ukryć swoje działania. Gdy trudno jest wykryć złośliwe działania, to gdy się pojawią, ich wykrycie po fakcie może być prawie niemożliwe. Każdy doświadczony technicznie pracownik będzie wiedział, jak sprzątać po sobie, edytując lub usuwając logi, aby ukryć złośliwe działania.

Trudno jest udowodnić winę. Nawet jeśli uda się wykryć szkodliwe działania, pracownik może po prostu stwierdzić, że błąd popełnił zupełnie nieświadomie, przypadkowo. W takich sytuacjach udowodnienie winy może się okazać niemożliwe.

Myśląc o znaczeniu cyberprzestrzeni w scenariuszu konfliktu hybrydowego, należy brać pod uwagę dwa aspekty działań insajderów:

- świadome, złośliwe na rzecz wrogiego podmiotu;
- nieświadome, których skutki są niekorzystne dla własnej organizacji czy instytucji, natomiast bardzo oczekiwane i pożądane przez przeciwnika lub potencjalnego przeciwnika.

Warto zatem przemyśleć, jak wartościowa jest nasza organizacja (wojskowa) dla potencjalnych

[26] Niebezpieczniejszy dla użytkownika oraz trudniejszy do wykrycia jest będący formą phishingu pharming.

[27] https://sjp.pwn.pl/sjp/insider;2561661.html/.27.06.2018.

[28] Wrogie działanie – coś, co szkodzi komuś lub czemuś, https://sjp.pwn.pl/slowniki/wrogi.html/. 20.07.2018.

złośliwych pracowników. Należy niestety liczyć się z sytuacją, w której w przyszłości efekty zaniedbań mogą być trudne do przewidzenia.

UNIWERSALNOŚĆ

Działania noszące znamiona hybrydowych, wykorzystujące cyberprzestrzeń, nie dotyczą jedynie infrastruktury lądowej. Mogą objąć również wodny transport do przewozu zarówno towarów, jak i pasażerów.

Żegluga jest bardzo starym i tradycyjnym przemysłem, który został niejako zmuszony, m.in. przez uwarunkowania ekonomiczne, do tego, aby stał się wysoce zautomatyzowany i skomputeryzowany. Proces ten niestety przebiega szybciej niż zdolność żeglugi do identyfikacji i zarządzania ryzykiem w obszarze cyber.

Informatyzacja obejmuje w szczególności systemy zarządzania i monitorowania silników, radary, systemy nawigacji, obsługę frachtu. Powszechne uzależnienie od teleinformatyki stwarza warunki do tego, że wiele czynności może zostać zakłóconych. Na przykład źle zaprogramowany lub zainfekowany oprogramowaniem złośliwym komputer zarządzający równowagą statku może doprowadzić do zatopienia go w porcie. Statki są podatne na zhakowanie za pośrednictwem satelitarnych łączy danych, przez które otrzymują aktualizacje oprogramowania oraz map nawigacyjnych. Wiele systemów elektronicznych na mostku może być dostarczanych z niezabezpieczonym kodem źródłowym, ponieważ firmy, które je sprzedają, mogą niewystarczająco chronić je przed skopiowaniem, a to z kolei może być kuszącym celem dla hakerów. Członkowie załogi, którzy zwykle nie są całkowicie przeszkoleni w zakresie cyberryzyka, mogą postępować daleko nierozważnie, np. podłączać telefony komórkowe do gniazd USB na mostku, aby je naładować, a to z kolei może doprowadzić do całkowitego wymazania konsoli nawigacyjnej statku.

Znaczna część całego handlu międzynarodowego odbywa się drogą morską. W zasadzie światowa gospodarka zależy od niezakłóconego funkcjonowania przemysłu żeglugowego. Statki przewożące ropę naftową, gaz czy pszenicę mają wbudowane w zbiorniki czujniki temperatury, ciśnienia czy wilgotności, co ułatwia transport łatwo psujących się artykułów żywnościowych, leków lub innych ładunków. Na największych kontenerowcach, które mogą pomieścić na pokładzie ponad 20 tys. kontenerów, sensory produkują ogromne ilości danych, które są potrzebne do utrzymania ładunku w optymalnym stanie, a także muszą zostać przesłane do centrum danych firmy transportowej. Jeśli więc haker zakłóci działanie czujników, może spowodować uszkodzenie ładunku. Ale jeśli potrafi zamienić te czujniki w botnet IoT (Internet rzeczy – Internet of Things), może ich użyć do ataku na inne systemy, czy to na tym statku, czy gdzie indziej. Podobnie można zmieniać informacje o samych pojemnikach, tak aby po rozładowaniu wszystkie zostały wysłane drogą lądową lub innym statkiem do niewłaściwych miejsc docelowych. Wszystko to może stanowić zagrożenie dla portów lotniczych, ponieważ pojemniki pełne narkotyków mogą zostać przemycone bez sprawdzenia przez służby celne, gdyż system zarządzania pojemnikami będzie zhakowany.

Cyberprzestrzeń stwarza warunki do przeprowadzania ataków, które mogą doprowadzić do bardzo poważnych zniszczeń. Na przykład, jeśli statek kontenerowy w wyniku włamania hakerskiego zatonie z pełnym ładunkiem o dużej wartości, właściciel lub czarterujący może być zagrożony utratą ogromnych sum pieniędzy. Z kolei jeśli do wody wydostanie się ropa naftowa lub skroplony gaz ziemny, może dojść do katastrofy ekologicznej, a firma transportowa może otrzymać kilkumiliardowe kary.

WIELE NIEWIADOMYCH

Cyberprzestrzeń stała się (i wszystko wskazuje na to, że nadal będzie) obszarem chętnie wykorzystywanym w scenariuszach działań hybrydowych. Zwiększająca się zależność od sieci i systemów teleinformatycznych z jednej strony wspiera rozwój gospodarczy, nasze zdrowie, dobrobyt, komunikację i bezpieczeństwo, z drugiej zaś może być podatna na cyberzagrożenia. Wrogie podmioty mogą kontrolować, czy, jak i kiedy działają nasze systemy i czy nasze kluczowe usługi zostaną dostarczone. Nasze osobiste, służbowe czy biznesowe dane i informacje, własność intelektualna lub tajemnice państwowe mogą być niepostrzeżenie zmienione bądź wykradzione.

Cyberprzestrzeń w konflikcie hybrydowym, dzięki możliwości anonimizacji własnych działań, stwarza warunki do przeprowadzenia cyberataku wyrządzającego szkody, bez obawy o odwet. Wykorzystanie cyberprzestrzeni do ataku na infrastrukturę krytyczną może mieć poważne konsekwencje zarówno militarne, jak i ekonomiczne, gospodarcze, społeczne czy humanitarne. Celowe jest zatem wypracowanie mechanizmów identyfikacji, a w konsekwencji zapobiegania cyberzagrożeniom.

Cyberprzestrzeń stwarza warunki do penetrowania sieci i systemów teleinformatycznych czy komputerowych, skompromitowania oprogramowania, a dzięki implantom ukrytym w sprzęcie przejęcia kontroli nad naszymi zasobami (aktywami). Dlatego też warto pamiętać, że kluczowe dane, informacje, sieci i systemy ważne dla dobrobytu gospodarczego państwa, bezpieczeństwa narodowego, obronności kraju czy zdrowia publicznego mogą nie być niezawodne i dostępne w razie potrzeby.

Z taktycznej perspektywy cyberataki mogą się wydawać mało opłacalne. Jednak należy zachować daleko idącą powściągliwość w tym względzie i przygotowywać się na nieznane. Trzeba mieć bowiem świadomość, że wyścig zbrojeń w cyberprzestrzeni już się rozpoczął i charakteryzuje się niespotykaną w żadnej fizycznej domenie skalą i dynamiką. ■

Działania informacyjne **w konflikcie hybrydowym**

EWOLUCJA SPOŁECZNO-GOSPODARCZA NA ŚWIECIE ZAOWOCOWAŁA „TRZECIĄ" FALĄ ROZWOJU CYWILIZACJI, KTÓRA WNIOSŁA DO NASZEGO CODZIENNEGO ŻYCIA ZDOBYCZE W POSTACI ŚRODKÓW MASOWEJ KOMUNIKACJI. NIESTETY, SĄ ONE WYKORZYSTYWANE DO MANIPULOWANIA NASZĄ ŚWIADOMOŚCIĄ.

ppłk dr Zbigniew Modrzejewski

Autor jest kierownikiem Zakładu Działań Informacyjnych w Instytucie Działań Informacyjnych Wydziału Wojskowego ASzWoj.

Konflikt hybrydowy często jest interpretowany jako coś nowego, co zrodziło się dopiero w związku z wydarzeniami na Ukrainie. Jednak analiza literatury pozwala wnioskować, że zdecydowana większość elementów kojarzonych współcześnie z tym zjawiskiem miała miejsce we wszystkich wojnach i konfliktach zbrojnych w przeszłości. Pewnym natomiast novum jest to, że element informacyjny (działania informacyjne) stał się czynnikiem nie mniej ważnym niż militarny (działania bojowe), a niekiedy nawet ważniejszym. Zatem konflikt hybrydowy to jednoczesne łączenie i wykorzystanie wielu wojskowych i niewojskowych narzędzi do osiągnięcia określonego celu.

W tym kontekście należy podkreślić, że wraz z początkiem konfliktu rosyjsko-ukraińskiego i aneksją Krymu wzrosło zainteresowanie działaniami informacyjnymi. W opracowaniach różnych autorów możemy odnaleźć wiele określeń oddziaływania informacyjnego mającego miejsce w tym konflikcie. Nazywane są one *wojną informacyjną*, *walką informacyjną*, *operacją informacyjną* czy też *działaniami informacyjnymi*. W artykule będę używał pojęcia *działania informacyjne*[1].

GRUZIŃSKA LEKCJA

Porównując konflikt na Ukrainie z wojną w Gruzji w 2008 roku, można zauważyć, że rosyjskie działania informacyjne prowadzone wobec Gruzji nie odniosły tak dużego sukcesu. W wojnie tej cyberataki na infrastrukturę krytyczną Gruzji wystąpiły równocześnie z działaniami bojowymi pododdziałów rosyjskich. Podczas tego konfliktu okazało się, że Gruzja była bardziej odporna na oddziaływanie informacyjne. Zmusiło to Rosję do przemyślenia sposobu prowadzenia operacji opartych na informacjach (information-based operations). W przeciwieństwie do prowadzenia równoległych działań informacyjnych, w szczególności cyberataków i atakowania gruzińskich zgrupowań, cyberataki na Krymie unieruchomiły infrastrukturę telekomunikacyjną i główne ukraińskie strony internetowe, zablokowały telefony komórkowe

[1] Zgodnie z obowiązującą w Siłach Zbrojnych RP doktryną: *Działania informacyjne to czynności mające wpływ na obiekty oddziaływania, informacje i systemy informacyjne przy zastosowaniu odpowiednich zdolności oraz narzędzi. Mogą być one realizowane przez któregokolwiek z uczestników działań z uwzględnieniem środków prewencyjnych ograniczających oddziaływanie na własne informacje i systemy informacyjne. Operacje informacyjne DD-3.10(A),* CDiS SZ, Bydgoszcz 2017, s. 15.

MICHAŁ ZIELIŃSKI

TABELA. ROSJANIE NA UKRAINIE

Jednostka administracyjna	Rosjanie [%]	Ludność rosyjskojęzyczna [%]
Sewastopol	71,6	90,6
Krym	58,3	76,6
Obwód ługański	39,0	68,8
Obwód doniecki	38,2	74,9
Obwód charkowski	25,6	44,3
Obwód zaporoski	24,7	48,2
Obwód odeski	20,7	42,0
Obwód dniepropietrowski	17,6	31,9
Obwód mikołajowski	14,1	29,3
Obwód chersoński	14,1	14,1

Opracowanie własne na podstawie: G. Kuczyński, https://www.tvn24.pl/wiadomosci-ze-swiata,2/na-ukrainie-przesladuja-rosjan-kreml-zmyslil-pretekst-do-interwencji,422511.html/. 15.05.2018.

kluczowych urzędników ukraińskich i dopiero wtedy, czyli 2 marca 2014 roku, siły rosyjskie w postaci „zielonych ludzików" wkroczyły na Półwysep Krymski. Ponadto Rosja w szerokim stopniu wykorzystała transmisje telewizyjne do wsparcia działań na Krymie i wzmocnienia przekazu informacyjnego, podkreślających niezbędność interwencji w celu obrony rosyjskich obywateli zamieszkujących ten obszar.

Po zakończeniu wojny z Gruzją Rosja poświęciła wiele uwagi na rolę informacji w świecie nowoczesnych technologii informatycznych, strategii komunikacyjnej i nowoczesnych wojen, zwanych hybrydowymi, nowej generacji lub nieliniowymi. Rezultaty tych wysiłków można było zaobserwować na Krymie, gdzie szybko i bezkrwawo zajęła terytorium, jednocześnie utrzymując na dystans państwa, które mogłyby potencjalnie interweniować.

Jedną z istotnych lekcji wyniesionych z konfliktu w Gruzji było uświadomienie przez Rosjan, jak wszechobecny Internet można wykorzystać do rozpowszechniania informacji, od legalnych i półoficjalnych organizacji, a także przez prywatnych blogerów. Prezydent Władimir Putin, będąc jeszcze premierem w rządzie Borysa Jelcyna, w 1999 roku uznał doniosłą rolę Internetu w wywieraniu wpływu na wyniki regionalnych konfliktów i stwierdził, że Rosja jest w tyle za innymi czołowymi państwami w zakresie wykorzystania tej przestrzeni. Do dziennikarzy zwrócił się ze słowami: *Oddaliśmy ten teren jakiś czas temu, ale teraz ponownie wchodzimy do gry*[2]. Dlatego też Rosja wspiera dziennikarzy, blogerów i osoby prywatne, wszystkich, którzy w mediach społecznościowych wydarzeniom nadają prorosyjską narrację. Należy mieć pewność, że nadal wykorzystuje ona przestrzeń informacyjną do wzmocnienia swoich zdolności: komunikacyjnych, propagandowych i dezinformacyjnych, wspierając w ten sposób osiągnięcie celów geopolitycznych.

ZMAGANIA INFORMACYJNE NA UKRAINIE

Rosyjska wojna informacyjno-psychologiczna z Ukrainą trwa nieprzerwanie od lat. Na początku była to wojna przeciwko „pomarańczowej dżumie" (powszechnie stosowany stereotyp propagandowy), która zapewniła wsparcie zwolennikom Wiktora Janukowycza na przełomie 2003 i 2004 roku, następnie jego zwycięstwo w wyborach prezydenckich (2010). W rzeczywistości rosyjski atak rozpoczął się długo przed Euromajdanem, czyli przed falą największych manifestacji i protestów przelewających się przez Ukrainę (rozpoczęły się 21 listopada 2013 r. demonstracją przeciwko odłożeniu podpisania umowy stowarzyszeniowej z Unią Europejską przez prezydenta W. Janukowycza). Zwycięstwo Rewolucji Godności (Euromajdanu) spowodowało również wzrost tendencji separatystycznych na Krymie, na którym większość mieszkańców stanowili Rosjanie. Region ten od początku odzyskania niepodległości przez Ukrainę miał zarówno formalną, jak i faktyczną autonomię od reszty państwa. W wyniku obalenia Wiktora Janukowycza także na południowo-wschodniej Ukrainie do głosu doszły tendencje separatystyczne, które w kwietniu 2014 roku przerodziły się w konfrontację militarną między ukraińskimi siłami bezpieczeństwa a separatystami prorosyjskimi wspieranymi przez pododdziały Federacji Rosyjskiej, którzy 6 kwietnia proklamowali suwerenność Donieckiej Republiki Ludowej, następnie 27 kwietnia – Ługańskiej Republiki Ludowej.

Analizując wydarzenia na Krymie, należy powrócić do połowy lat pięćdziesiątych XX wieku. W Rosji mówi się, że przywódca ZSRR Nikita Chruszczow oderwał w 1954 roku Krym od radzieckiej Rosji i oddał go radzieckiej Ukrainie, gdyż sam był Ukraińcem. Poszukując źródeł konfliktu rosyjsko-ukraińskiego, należy również zwrócić uwagę na wydarzenia z początku lat dziewięćdziesiątych XX wieku, gdyż mają one bezpośredni związek z późniejszym rozwojem sytuacji. Po 1991 roku i zgodzie władz Ukrainy na ustanowienie republiki autonomicznej w zamian za rezygnację Krymu z niepodległości, Sewastopol został miastem wydzielonym jako siedziba rosyjskiej Floty Czarnomorskiej. W roku 1997 uzgodniono rosyjską dzierżawę Sewastopola na 20 lat, którą w 2010 roku przedłużono aż do roku 2042.

Dlaczego Krym dla Rosji jest taki ważny? Po pierwsze jego przyłączenie znacząco zwiększyło możliwości operacyjne Floty Czarnomorskiej. Ponadto Rosja uzyskała pełną swobodę w zakresie jej liczebności i rozmieszczenia na półwyspie, a także modernizacji i rozbudowy. Dotychczas ograniczały to porozumienia rosyjsko-ukraińskie z 1997 roku, regulujące zasady stacjonowania jednostek Sił Zbrojnych Federacji Rosyjskiej na terytorium Ukrainy. W porozumieniach tych było m.in. zawarte, że Flota Czarnomorska mogła bez pytania się o zgodę strony ukraińskiej przeprowadzać wyłącznie remonty jednostek, a jej komponent lądowy nie mógł przekraczać 2 tys. żołnierzy (obecnie jest ich 22 tys.). Według Klausa Mommsena – eksperta w sprawach marynarki wojennej: *Krym ma strategiczne znaczenie dla Morza Czarnego a półwysep sięga daleko w głąb morza. Otwiera on Rosji drogę w kierunku południowym, a więc w kierunku Morza Śródziemnego i Bliskiego Wschodu. Już w czasach Związku Radzieckiego na Krymie zlokalizowany był przemysł stoczniowy. Dokonywano tam przeglądów technicznych i napraw większych okrętów wojennych*[3].

Włączenie Krymu w skład Federacji Rosyjskiej 18 marca 2014 roku spowodowało przeprowadzenie

[2] P. Goble: *Russia: Analysis from Washington-A Real Battle on the Virtual Fron.* Radio Free Europe/Radio Liberty, October 9, 1999. http://www.rferl.org/content/article/1092360.html/. 24.06.2018.

[3] *Ekspert: Krym stanowi dla Rosji jedyne dojście do Morza Śródziemnego.* WYWIAD. https://www.dw.com/pl/. 4.07.2018.

na bardzo dużą skalę militaryzacji tego półwyspu. Aktualnie zgrupowanie wojskowe na Krymie obejmuje trzy komponenty: lądowy, powietrzny i morski, które są wspierane kontyngentami innych resortów siłowych, m.in. Straży Granicznej, podporządkowanej Federacyjnej Służbie Bezpieczeństwa (FSB), czy wojsk wewnętrznych podległych Ministerstwu Spraw Wewnętrznych, na bazie których powstała Federalna Służba Wojsk Gwardii Narodowej. Przejęcie pozostałej na Krymie ukraińskiej infrastruktury wojskowej, a zwłaszcza bazy morskiej w Sewastopolu, uczyniło z rosyjskiej Floty Czarnomorskiej niekwestionowaną główną siłę militarną w basenie Morza Czarnego. Ponadto po aneksji Krymu można mówić o tym, że rosyjskie ministerstwo obrony oszczędza na opłatach dzierżawnych dla Ukrainy. Moskwa płaciła Ukrainie 97 mln USD rocznie za możliwość stacjonowania Floty Czarnomorskiej na półwyspie, a od 2017 roku ta kwota miała wzrosnąć do 100 mln USD.

ROSYJSKIE DOKUMENTY DOKTRYNALNE

Analizę kluczowych rosyjskich dokumentów doktrynalnych, odnoszących się do prowadzenia oddziaływania informacyjnego, rozpocznę od przypomnienia wydarzeń na Ukrainie i w Federacji Rosyjskiej w powiązaniu z ich opublikowaniem (rys. 1).

Analizując treści na nim przedstawione, jako kluczowy po stronie rosyjskiej można wskazać rok 2000. To właśnie wtedy, dokładnie 26 marca, po raz pierwszy prezydentem Federacji Rosyjskiej zostaje Władimir Putin. Dawał on do zrozumienia i wciąż daje, że rozpad ZSRR był największą katastrofą geopolityczną dwudziestego wieku. Jego marzeniem jest przywrócenie Rosji silnej pozycji międzynarodowej, a jednocześnie utworzenie potężnego ośrodka eurazjatyckiego, skupiającego wszystkie kraje byłego ZSRR. Jest to także rok opublikowania *Doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej,* która została uchwalona 9 września. Określono w niej podstawowe cele, koncepcje działania, szanse i zagrożenia państwa w sferze informacyjnej. Analizując te zapisy, można wnioskować, że władze Rosji traktują bezpieczeństwo informacyjne, w tym bezpieczeństwo w cyberprzestrzeni, jako podstawę całego systemu bezpieczeństwa państwa, jak również jako podstawowe narzędzie do osiągania celów politycznych. Bardzo charakterystyczne jest to, że walkę informacyjną powinno się stosować przede wszystkim, aby osiągnąć efekt psychologiczny. W doktrynie podkreślono rolę sfery informacyjnej jako czynnika aktywnie wpływającego na społeczeństwo informacyjne, kreującego nowy porządek społeczny i odnowę duchową Rosji (patriotyzm, wartości

RYS. 1. KALENDARIUM WYDARZEŃ

Opracowanie własne.

1991
Ukraina uzyskuje niepodległość

2000
Władimir Putin zostaje prezydentem FR

Doktryna bezpieczeństwa informacyjnego FR

2004–2005
Pomarańczowa rewolucja Wiktor Juszczenko zostaje prezydentem

2004
Władimir Putin ponownie zostaje prezydentem Federacji Rosyjskiej

2010
Wiktor Janukowycz zostaje prezydentem

2010
Doktryna wojenna FR

2012
Władimir Putin ponownie zostaje prezydentem Federacji Rosyjskiej

2013–2014
Euromajdan – Wiktor Janukowycz zostaje obalony

Aneksja Krymu. Wojna w Donbasie

2014
Doktryna wojenna FR

2016
Doktryna bezpieczeństwa informacyjnego FR

2017
Dekret *O strategii bezpieczeństwa społeczeństwa informacyjnego Federacji Rosyjskiej na lata 2013–2017*

EZIO GUTZEMBERG/FOTOLIA

moralne i humanizm[4]) przy wsparciu państwa jako głównego gwaranta. Jako jedno z największych zagrożeń dla bezpieczeństwa informacyjnego wskazano wpływ podmiotów zagranicznych, w tym mediów zagranicznych, które dążą do niekorzystnego przedstawiania wizerunku Rosji i działań podejmowanych przez państwo. Przed takim zagrożeniem władze rosyjskie przestrzegają i zamierzają się bronić. W tym kontekście Rosjanie mogą stosować zarówno defensywne, jak i ofensywne metody walki informacyjnej, także w cyberprzestrzeni. Stosowanie tzw. trolli (prowokatorów internetowych) czy ujawnianie tajnych rozmów między decydentami może być doskonałymi przykładami takich metod.

Doktryna ta, zdaniem Roberta Białoskórskiego[5], zainicjowała politykę Rosji w zakresie rozwoju jej przestrzeni informacyjnej w czterech aspektach: technicznym, naukowym, prawnym i organizacyjnym.

NAJBARDZIEJ ZNANĄ ROSYJSKĄ TELEWIZJĄ INFORMACYJNĄ JEST RT, jedna z największych sieci telewizyjnych. Jej przekaz jest odbierany w ponad ***100*** krajach i dociera do ponad ***700*** milionów ludzi na świecie.

Nową doktrynę wojenną zatwierdził 5 lutego 2010 roku prezydent Dmitrij Miedwiediew. Jednoznacznie wskazano w niej na najważniejsze zagrożenia zewnętrzne bezpieczeństwa Rosji. Odniesiono je do NATO, podkreślając, że dąży on do przyznania sobie globalnych funkcji z naruszeniem prawa międzynarodowego oraz przybliżenia swojej infrastruktury wojskowej do granic Federacji Rosyjskiej. Charakteryzując cechy współczesnych konfliktów zbrojnych, wskazywano na kompleksowe użycie sił zbrojnych, sił i środków o charakterze innym niż wojenny oraz zmasowane użycie systemów uzbrojenia i techniki wojskowej, skonstruowanych według nowych zasad i porównywalnych pod względem efektywności do broni jądrowej.

Doktrynę te znowelizowano cztery lata później. W. Putin podpisał ją 26 grudnia 2014 roku. Przy jej opracowaniu wzięto pod uwagę: *Koncepcję długofalowego rozwoju społeczno-gospodarczego Federacji Rosyjskiej na okres do 2020 r.*, *Strategię bezpieczeństwa narodowego Federacji Rosyjskiej do 2010 r.*, a także stosowne założenia *Koncepcji polityki zagranicznej Federacji Rosyjskiej 2008 r.* i *Doktryny morskiej Federacji Rosyjskiej na okres do 2020 r.*[6]. W dokumencie tym powtórzono wiele zapisów z doktryny z roku 2010, ale zawiera on również nowe pojęcia w dziedzinie bezpieczeństwa i definiuje nowe zagrożenia zewnętrzne i wewnętrzne. Podkreślono w nim też przesunięcie zagrożeń i ryzyka wojny w przestrzeń informacyjną i wewnętrzną Federacji Rosyjskiej.

Do zagrożeń zewnętrznych zaliczono m.in.: wykorzystanie technologii informacyjnych i komunikacyjnych do osiągania celów politycznych i wojskowych sprzecznych z prawem międzynarodowym, skierowanych przeciwko suwerenności, niezależności politycznej, integralności terytorialnej państwa i stanowiących zagrożenie dla międzynarodowego pokoju i bezpieczeństwa oraz globalnej i regionalnej stabilności. Natomiast do zagrożeń wewnętrznych, poza destabilizacją polityczno-społeczną sytuacji wewnętrznej w kraju, zaliczono: ataki na system informacyjny, w tym obiekty militarne oraz infrastrukturę krytyczną państwa, destrukcyjne oddziaływanie informacyjne na społeczeństwo, a zwłaszcza na młodych obywateli, mające na celu przerwanie historycznych, duchowych i patriotycznych tradycji w zakresie obrony ojczyzny.

Na szczególną uwagę zasługuje zapis, że Federacja Rosyjska uważa za uprawnione wykorzystanie sił zbrojnych i innych służb do odparcia agresji przeciwko niej i (lub) jej sojuszników, wsparcia (przywrócenia) pokoju zgodnie z postanowieniem Rady Bezpieczeństwa ONZ oraz innych struktur bezpieczeństwa zbiorowego, jak również w celu zapewnienia ochrony swoich obywateli znajdujących się poza granicami państwa, zgodnie z powszechnie uznanymi zasadami i normami prawa międzynarodowego oraz międzynarodowymi umowami Federacji Rosyjskiej. To właśnie w obronie obywateli Rosja rozpoczęła konflikt na Ukrainie. Wprawdzie w doktrynie nie ma bezpośredniego odniesienia do wspomnianego konfliktu, lecz pośrednio niektóre zapisy można odnieść do odstraszania potencjalnych działań innych państw. Wskazują na to chociażby zapisy o odstraszaniu nienuklearnym w postaci stałego utrzymywania wysokiego stopnia gotowości bojowej sił konwencjonalnych oraz o tym, że Rosja mogłaby użyć broni jądrowej w odpowiedzi na użycie broni masowego rażenia przeciwko niej lub jej sojusznikom oraz w razie agresji z użyciem broni konwencjonalnej zagrażającej istnieniu państwa rosyjskiego.

Kolejnym dokumentem jest podpisana 6 grudnia 2016 roku przez prezydenta W. Putina nowa *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej*, zastępująca tę z roku 2000. Wskazuje się w niej na potrzebę pomocy państwa w sferze rozwoju nowoczesnych technologii informatycznych celem efektywniejszego wykorzystania rodzimej myśli technicznej w tej dziedzinie i uniezależnienia się od zachodnich rozwiązań. Zdefiniowano również zagrożenia dla bezpieczeństwa informacyjnego, które podzielono na wewnętrzne i zewnętrzne. Do zagrożeń wewnętrznych zaliczono:

– zły stan krajowego przemysłu informatycznego;

– brak koordynacji między organami i instytucjami państwowymi odnoszącej się do prowadzenia jednolitej polityki bezpieczeństwa informacyjnego;

– nieodpowiednie regulacje prawne w obszarze informacyjnym i brak praktyki ścigania przestępstw w cyberprzestrzeni;

– niewystarczającą liczbę wykwalifikowanych pracowników do kształcenia i szkolenia w tej dziedzinie.

[4] Humanizm – *postawa moralna i intelektualna zakładająca, że człowiek jest najwyższą wartością i źródłem wszelkich innych wartości.* https://sjp.pwn.pl/slowniki/humanizm.html/.7.07.2018.

[5] R. Białoskórski: *Cyberprzestrzenny wymiar polityki bezpieczeństwa i obrony Federacji Rosyjskiej.* W: *Polska-Rosja Polityka bezpieczeństwa Federacji Rosyjskiej kontynuacja I zmiana.* Red. M. Minkina, M. Kaszuba. Siedlce 2016, s. 17–18.

[6] W. Michalski, Z. Modrzejewski: *Doktryny wojenne innych państw.* AON, Warszawa 2015, s. 9.

Natomiast za zewnętrzne źródła zagrożeń uznano:

– aktywność politycznych, gospodarczych, wojskowych, wywiadowczych i informacyjnych struktur zagranicznych, ukierunkowanych na działalność przeciwko interesom Rosji;

– dominację niektórych krajów w przestrzeni informacyjnej oraz ich dążenia do odsunięcia FR od zewnętrznych i wewnętrznych rynków informacyjnych;

– zaostrzenie konkurencji międzynarodowej w sferze technologii informatycznych i zasobów informacyjnych;

– rozwijanie przez niektóre państwa koncepcji wojny informacyjnej.

Następny dokument dotyczący rozpatrywanej problematyki ukazał się 9 maja 2017 roku, kiedy to prezydent W. Putin podpisał dekret *O strategii rozwoju społeczeństwa informacyjnego w Federacji Rosyjskiej na lata 2017–2030*. Zastąpił on obowiązującą od 7 lutego 2008 roku *Strategię rozwoju społeczeństwa informacyjnego Federacji Rosyjskiej*. Obowiązujący dokument jest spójny z *Doktryną bezpieczeństwa informacyjnego Federacji Rosyjskiej* z 5 grudnia 2016 roku, co prawdopodobnie wynika z faktu, że prace nad nimi były prowadzone równolegle. W strategii podkreśla się potrzebę rozszerzania kontroli nad rosyjskim Internetem oraz wprowadzanie rodzimych rozwiązań w miejsce zachodnich. Mowa jest w niej również o uniezależnieniu się od wpływów zewnętrznych w przestrzeni informacyjnej, co może oznaczać chęć kontrolowania dostępu i selekcji informacji jako elementu bezpieczeństwa. Aby uniknąć zagrożeń płynących z wykorzystania zagranicznych technologii oraz przenikania zewnętrznej informacji do społeczeństwa rosyjskiego, proponowane są rozwiązania zmierzające do:

– kształtowania przestrzeni informacyjnej z uwzględnieniem potrzeb obywateli i społeczeństwa, związanych z pozyskiwaniem wartościowych i wiarygodnych informacji;

– rozwoju infrastruktury informacyjnej i komunikacyjnej państwa;

– tworzenia i wykorzystania rodzimych technologii informacyjnych i komunikacyjnych oraz zapewnienia im konkurencyjności na poziomie międzynarodowym;

– kształtowania nowej bazy technologicznej dla rozwoju sfery gospodarczej i społecznej;

– ochrony interesów państwowych w obszarze gospodarki cyfrowej[7].

Reasumując, należy zauważyć, że wraz z dojściem Władimira Putina do władzy Rosja poświęca więcej miejsca przestrzeni informacyjnej.

MODEL GIERASIMOWA

Analizując konflikt na Ukrainie, wielu badaczy wskazuje na wykorzystanie tzw. modelu Gierasimowa. W lutym 2013 roku Walerij Gierasimow, szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, opublikował w tygodniku „Kurier Wojskowo-Przemysłowy" artykuł pod tytułem *Siła nauki jest w przewidywaniu*[8]. Autor, opierając się na taktyce kreowanej w czasach Związku Radzieckiego, połączył ją ze strategicznym myśleniem o wojnie totalnej i na tej podstawie stworzył nową teorię prowadzenia działań wojennych. Polegała ona bardziej na zakulisowym wpływaniu na społeczeństwo przeciwnika niż na otwartych działaniach zbrojnych. W jego ocenie zmieniły się zasady prowadzenia wojny. Podkreślił on wzrost znaczenia niemilitarnych sposobów osiągania celów politycznych i strategicznych, które w wielu przypadkach okazują się bardziej efektywne niż potęga militarna. Dlatego też coraz istotniejsze w jego ocenie jest wykorzystanie różnorodnych instrumentów politycznych, ekonomicznych i humanitarnych w połączeniu z manipulowaniem nastrojami ludności zamieszkującej obszar konfliktu. Działania wspierane przez środki militarne o ukrytym charakterze, w tym operacje informacyjne oraz działania jednostek wojsk specjalnych. Otwarte wykorzystanie oddziałów zbrojnych, najczęściej pod pozorem operacji pokojowych oraz humanitarnych, jest dopuszczalne dopiero w późniejszej fazie konfliktu po to, aby osiągnąć ostateczny cel.

W. Gierasimow wprowadził pojęcie utrzymywania nieostrych linii między stanem wojny a pokojem, między żołnierzami (w mundurze lub bez) a uzbrojonymi cywilami. Położył także większy nacisk na wygraną wojny medialnej wraz z wszelkimi zyskami militarnymi (rys. 2). Przestrzeń informacyjna otwiera szerokie, asymetryczne możliwości redukowania siły przeciwnika – w innym miejscu artykułu natomiast wspomina o wykorzystywaniu […] *wewnętrznej opozycji do tworzenia nieustannie działającego frontu na całym terytorium przeciwnika*.

Na uwagę zasługuje fakt, że wojna informacyjna jest prowadzona z użyciem niemilitarnych środków w stosunku do militarnych wynoszącym 4:1, a więc środki te są dominujące. Osobny artykuł dwóch byłych rosyjskich wojskowych: S.G. Chekinova i S.A. Bogdanova, pt. *Natura i treść wojny nowej generacji*[9] udowadnia, że działania informacyjne wraz z operacjami specjalnymi i skoordynowaną eskalacją będą odgrywały kluczową rolę w przyszłym konflikcie. Artykuł ten niekiedy jest nazywany „instrukcją obsługi" w wypadku aneksji Krymu.

BUDOWA ZAPLECZA INFORMACYJNEGO

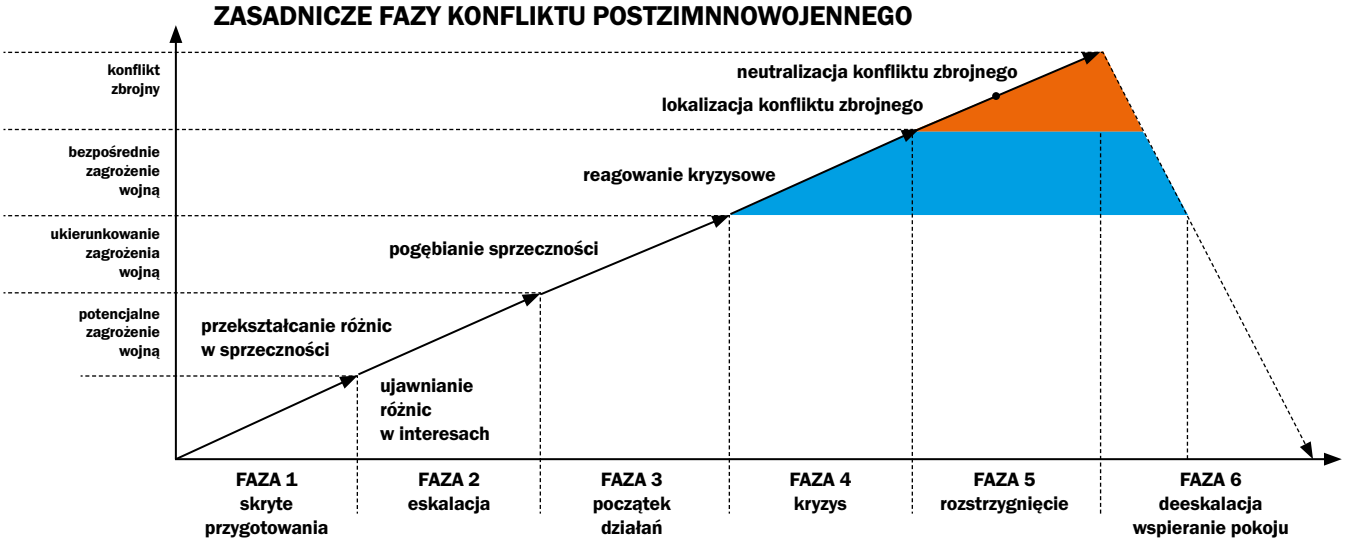
Militarne zaangażowanie Rosji w ukraiński konflikt zostało poprzedzone wiele lat wcześniej zdecydowaną ofensywą informacyjną. W pierwszej kolejności władze rosyjskie podporządkowały sobie własne koncerny

[7] M. Kowalska: *Analiza: Nowa rosyjska strategia rozwoju społeczeństwa informacyjnego*. https://capd.pl/.4.07.2018.

[8] https://www.vpk-news.ru/articles/14632/.17.03.2018.

[9] S.G. Chekinov, S.A. Bogdanov: *The Nature and Content of a New-Generation War.* "Military Thought" październik 2013, nr 4. http://www.eastviewpress.com/.15.05.2018.

RYS. 2. MODEL GIERASIMOWA



Opracowanie własne według: M. Depczyński na podstawie https://www.vpk-news.ru/articles/14632/. 17.03.2018.

medialne, następnie nastąpiła ich ekspansja na rynek ukraiński. W tym celu wykupywano udziały w miejscowych mediach, które należały do ukraińskich oligarchów. W ten sposób zapewniono sobie narzędzia do dokonywania zbiorowej manipulacji umysłami i emocjami społeczeństwa zarówno własnego, jak i ukraińskiego. Towarzyszyła temu koncentracja środowisk prorosyjskich i tworzenie tzw. piątej kolumny, czyli ludzi przychylnych Putinowi i jego polityce.

W bezprecedensowej pod względem skali kampanii dezinformacji na temat sytuacji na Ukrainie uruchomiono wszystkie federalne kanały telewizyjne, radiowe, gazety oraz zasoby internetowe. Front informacyjny wsparli dyplomaci, politycy, politolodzy, eksperci, elita nauki i kultury. Na początku kryzysu ukraińskiego (Euromajdan) sprzężono go z dywersją ideologiczną, polityczną, socjokulturową, prowokacją, aktywnością dyplomacji. Słowem – uruchomiono działania wielokierunkowe i masowe[10].

Rosyjskie międzynarodowe programy telewizyjne nadawane są nie tylko w języku rosyjskim, lecz w angielskim, arabskim, hiszpańskim, francuskim, niemieckim i innych. Najbardziej znaną telewizją informacyjną jest RT (do 2009 roku Russia Today), jedna z największych sieci telewizyjnych. Jej przekaz jest odbierany w ponad 100 krajach i dociera do ponad 700 milionów ludzi na świecie. Finansuje ją Federalna Agencja Prasy i Komunikacji Masowej, która podlega Ministerstwu Łączności i Masowych Komunikacji Federacji Rosyjskiej. Wydanie internetowe RT jest jednym z najpopularniejszych kanałów informacyjnych. Stacja telewizyjna osiągnęła miliard wyświetleń na YouTube. O strategicznym jej znaczeniu świadczy fakt, że prezydent W. Putin podpisał dekret zakazujący jakichkolwiek cięć w jej budżecie. Rozgłośnia jest niewątpliwym ewenementem, gdyż mimo że jest ciągle oskarżana o dezinformację, przekręcanie prawdy i zatajanie faktów, to nadal notuje wzrost oglądalności. Analiza trzech internetowych kanałów informacyjnych: Komsomolskaja Pravda, Regnum i TV Zvezda ujawniła wiele sposobów stosowanych w kampaniach informacyjnych w celu prezentowania negatywnego wizerunku Ukrainy. Prowadzący wojnę informacyjną są w stanie zaspokoić potrzeby różnych odbiorców o różnych gustach i potrzebach związanych z konsumpcją mediów. „Komsomolskaja Pravda" jest przede wszystkim jedną z najstarszych gazet w Rosji (wydawaną od 1925 roku) i mającą największy nakład. Wciąż jest szanowana wśród rosyjskiej ludności i ma duży wpływ nie tylko w Rosji, lecz także na Ukrainie, w Mołdawii, na Białorusi i w innych krajach z dużymi rosyjskimi diasporami, w tym również w krajach bałtyckich. Ma ona również darmowe radio internetowe. TV Zvezda to ogólnokrajowa rosyjska sieć telewizyjna należąca do rosyjskiego ministerstwa obrony. Zvezda określa się jako „patriotyczna" i jest uważana za jeden z najbardziej sensacyjnych i antyzachodnich kanałów w Rosji. TV Zvezda twierdzi głównie, że USA i NATO ingerują w sprawy ukraińskie. W przeszłości opublikowała wiele stronniczych i kontrowersyjnych wiadomości.

OBIEKTY ODDZIAŁYWANIA INFORMACYJNEGO

W działaniach na Ukrainie wysiłek operacji informacyjnych był skupiony na: „humanitarnej" polityce zagranicznej Rosji, prorosyjskich mediach na Ukrainie

[10] J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku.* „Punkt Widzenia" 2014 nr 5, s. 5.

oraz na światowych prorosyjskich mediach ukierunkowanych na Zachód. Celem rosyjskiej „humanitarnej" polityki zagranicznej było zwiększenie na Ukrainie liczby osób posługujących się językiem rosyjskim i liczby obywateli ukraińskich identyfikujących się z kulturą rosyjską. Aby osiągnąć ten cel, władze rosyjskie podjęły następujące działania: finansowanie szkół nauczających w języku rosyjskim, wspieranie prorosyjskich ośrodków kulturalnych i zrzeszających organizacje pozarządowe oraz zachęcanie do zdobywania obywatelstwa rosyjskiego.

Generał major Aleksandr Michajłow, były szef Zarządu FSB ds. Kontaktów ze Społeczeństwem, w swoim wystąpieniu wyliczył podstawowe instrumenty krymskiej wojny informacyjnej. Zaliczył do nich: czynnik psychologiczny (presja i zastraszanie), bezpośrednie zaangażowanie kluczowych decydentów (prezydent FR Władimir Władimirowicz Putin), szantaż oraz sankcje. Ponadto stwierdził, że tego rodzaju działania obejmują liczne elementy składowe, zarówno w realu, jak i w przestrzeni wirtualnej, służące do blokowania wpływu przeciwnika i wywierania presji na wyselekcjonowane obiekty[11]. Według danych z 2007 roku aż około 67% gazet na Ukrainie wydawano w języku rosyjskim, a zaledwie 29% w ukraińskim. Oprócz wychodzących gazet na Ukrainie działa również znaczna liczba rosyjskich stacji telewizyjnych. W lipcu 2008 roku było 45 licencjonowanych programów telewizyjnych z czego aż 37 rosyjskich.

Wszystko to miało na celu zapewnienie poparcia części społeczeństwa ukraińskiego dla działań wojskowych na Ukrainie. Połączenie dezinformacji i krytyki zakłóciło zachodnią narrację wydarzeń w tym kraju. W rezultacie Rosja była w stanie stworzyć przestrzeń informacyjną wspierającą jej operacje wojskowe. Poza wysiłkami medialnymi na Ukrainie przeprowadziła ona skuteczną kampanię informacyjną skierowaną na społeczność międzynarodową. Dzięki tym działaniom odbiorcy wewnętrzni, czyli ludność FR, w większości wyrażali poparcie dla rządu i W. Putina. Z kolei ludność terenów okupowanych: Doniecka, Ługańska i Krymu również prezentowała pozytywną ocenę działań i postawę wobec FR, dyskredytując jednocześnie władze Ukrainy. Społeczeństwa państw sąsiadujących z Ukrainą w większości pozytywnie oceniały działania Rosji. Nie bez znaczenia jest odsetek ludności pochodzenia rosyjskiego.

W tabeli (początek tekstu) przedstawiono dziesięć jednostek administracyjnych Ukrainy, w których udział procentowy Rosjan i ludności rosyjskojęzycznej jest największy.

Analiza danych w niej zawartych upoważnia do wyciągnięcia wniosku, że celem rosyjskich działań stały się te obszary, w których odsetek ludności sprzyjającej Rosji jest największy. Jednym z kłamstw lansowanych przez rosyjską propagandę było rzekome prześladowanie mniejszości rosyjskiej przez rząd ukraiński. Prezydent Rosji od początku powtarzał, że angażuje się w sprawy ukraińskie, gdyż chce chronić mieszkających tam etnicznych Rosjan i ludność rosyjskojęzyczną. Ministerstwo Spraw Zagranicznych Rosji oskarżało władze w Kijowie o prześladowanie nie tylko Rosjan, lecz również innych mniejszości narodowych. Od początku propaganda rosyjska przedstawia obraz Ukrainy jako kraju rządzonego przez faszystów. Twierdzenie, że język rosyjski na Ukrainie jest zagrożony, to bzdura. Po pierwsze, prawo do używania rosyjskiego jest chronione zapisem w konstytucji, a ustawa językowa umożliwia swobodne używanie go jako drugiego urzędowego języka. Po drugie, rosyjskojęzyczne programy telewizyjne, gazety i książki zdecydowanie przeważają nad ukraińskimi. Najbardziej popularne portale, nawet te wrogie Moskwie, mają drugą – rosyjskojęzyczną – wersję strony, niemal nieodbiegającą bogactwem zawartości od wersji ukraińskiej. Zresztą rosyjski dominuje w ukraińskiej sieci. Po trzecie, edukacja po rosyjsku jest powszechnie dostępna – nawet tam, gdzie Rosjanie nie są znaczącą grupą. Nie ma żadnych restrykcji, jeśli chodzi o mówienie po rosyjsku w pracy, nawet w urzędach rządowych. Po czwarte, rosyjski jest językiem biznesu na Ukrainie, dominuje też jako używany na co dzień w wielu regionach, w tym w Kijowie[12].

SPOSTRZEŻENIA

Na podstawie przedstawionego zarysu prowadzenia działań informacyjnych w konflikcie na Ukrainie można sformułować wiele wniosków. Po pierwsze, w konfliktach hybrydowych działania militarne poprzedzone są długofalowymi działaniami informacyjnymi. Po drugie, działania te nie są statyczne, lecz stale się rozwijają. Rosyjskie podejście ewoluuje, rozwija się, adaptuje, identyfikuje sukces i wzmacnia go, i odwrotnie porzuca nieudane próby. Po trzecie, w działaniach informacyjnych wykorzystuje się wszystkie dostępne siły i środki oddziaływania informacyjnego. Po czwarte, należy podkreślić ich doniosłą rolę w mediach tradycyjnych, a w szczególności w telewizji oraz Internecie. Po piąte, propaganda i dezinformacja to główne zdolności działań informacyjnych wykorzystywane w konflikcie hybrydowym. Reasumując, w wypadku relacji rosyjsko-ukraińskich mamy do czynienia z całym szeregiem działań prowadzonych w sferze informacyjnej (komunikowania masowego) rozłożonych w czasie i prowadzonych na podstawie długoterminowej strategii. Ich celem jest uzyskanie przewagi informacyjnej i narzucenie własnej opinii społeczności państwa ukraińskiego oraz międzynarodowej, tzn. właściwej narracji dotyczącej spornych kwestii. ■

[11] T. Kacała: *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa.* „Przegląd Prawa Konstytucyjnego" 2015 nr 2(24), s. 61–62.

[12] G. Kuczyński: *Na Ukrainie prześladują Rosjan? Kreml zmyślił pretekst do interwencji.* http://www.tvn24.pl/. 18.03.2018.

Ujarzmić **hybrydę**

WIELOWYMIAROWOŚĆ ZAGROŻEŃ, KTÓRE NIE BYŁY UWZGLĘDNIANE W SCENARIUSZACH DZIAŁAŃ ZBROJNYCH, W WYNIKU GLOBALIZACJI I WSPÓŁZALEŻNOŚCI EKONOMICZNEJ PAŃSTW WYSUWAJĄ SIĘ NA PIERWSZY PLAN PRZYSZŁYCH KONFLIKTÓW.

kmdr por. Jarosław Keplin, ppłk Cezary Pawlak

Jarosław Keplin jest starszym specjalistą w Oddziale Rozwoju Koncepcji Centrum Doktryn i Szkolenia Sił Zbrojnych.

Cezary Pawlak jest starszym specjalistą w Oddziale Rozwoju Koncepcji Centrum Doktryn i Szkolenia Sił Zbrojnych.

W latach dziewięćdziesiątych XX wieku panowało przekonanie, że doświadczenia II wojny światowej oraz zimnej wojny wyeliminowały zagrożenie klasycznym konfliktem o charakterze militarnym. Początek XXI wieku to okres intensywnych zmian w globalnym środowisku bezpieczeństwa, przede wszystkim w kontekście wzrostu znaczenia zagrożeń asymetrycznych.

Obok klasycznych konfliktów zbrojnych zyskały na znaczeniu działania hybrydowe, obejmujące – oprócz działań konwencjonalnych – działania nieregularne, a także ofensywę w cyberprzestrzeni, działania informacyjne, dezinformacyjne i psychologiczne, uzależnienie ekonomiczne, presję gospodarczą itd. Część z tych zagrożeń ma charakter niemilitarny (np.: fake news, blokady gospodarcze, dyskryminacja gospodarcza, spekulacje finansowe). Ponadto obserwuje się celowe ograniczanie skali prowadzonych operacji zbrojnych (poniżej progu wojny – agresja podprogowa[1]) po to, by uniemożliwić jednoznaczne określenie, czy jest to jeszcze stan pokoju, czy już wojny, a tym samym zapobiec reakcji społeczności międzynarodowej. Kwestia ta jest ważna, ponieważ może mieć w przyszłości wpływ na udzielenie sojuszniczej pomocy jednemu z państw członkowskich NATO. Zgodnie bowiem z art. 5 *Traktatu Północnoatlantyckiego* państwa NATO są zobowiązane do udzielenia sobie wzajemnej pomocy tylko w razie zbrojnej napaści na jedno z nich. Zatem zmiany zachodzące we współczesnym świecie, szczególnie w stosunkach międzynarodowych, sprawiają, że największym wyzwaniem dla państw jest zapewnienie bezpieczeństwa.

We współczesnym środowisku bezpieczeństwa zauważa się zacieranie granicy między jego wymiarem wewnętrznym i zewnętrznym, militarnym i pozamilitarnym. Globalizacja i wzrastająca współzależność ekonomiczna często skutkują nieprzewidywalnością zjawisk, których zasięg nie jest już ograniczony barierami geograficznymi czy systemami politycznymi lub gospodarczymi. Presja globalizacji powoduje, że w dzisiejszym świecie państwa nie są w stanie samodzielnie funkcjonować gospodarczo i ekonomicznie, a współzależność między nimi może być przyczyną kryzysów lub konfliktów. Zagrożenia wynikające z globalizacji stworzyły warunki do działania nowych aktorów, jakimi mogą być – poza państwowymi – aktorzy niepaństwowi (non-state actor), tacy jak organizacje pozarządowe i korporacje transnarodowe o rozproszonej anoni-

[1] *Agresja podprogowa – działania, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiągnięcie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa.* Zob. *(Mini)Słownik BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa,* www.bbn.gov.pl/pl/bezpieczeństwo-narodowe. 22.11.2016.

1.

Rozwój techniczny i gospodarczy państw europejskich spowodował, że z Bliskiego i Środowego Wschodu oraz Afryki Północnej w kierunku Europy przemieszczają się uchodźcy i imigranci, którzy stwarzają problemy o charakterze wcześniej niespotykanym. Na zdjęciu tunezyjscy uchodźcy na włoskiej wyspie Lampedusa.

UN PHOTO/UNHCR/PHIL BEHAN

mowej własności, czyli niepaństwowe podmioty funkcjonujące w „globalnej" przestrzeni ponadpaństwowej czy też transnarodowej. Ponadto rozwój techniczny i gospodarczy państw europejskich spowodował, że z Bliskiego i Środowego Wschodu oraz Afryki Północnej w kierunku Europy przemieszczają się uchodźcy i imigranci (fot. 1), którzy stwarzają problemy o charakterze wcześniej niespotykanym. Złożoność funkcjonowania państw w środowisku geopolitycznym generuje zagrożenia te dobrze znane i zdefiniowane, jak i nowe czy zmodyfikowane. Do grona tych ostatnich należy zaliczyć działania hybrydowe, które mają na celu wykorzystanie podatności państwa na zagrożenia o znamionach hybrydowych. Obecnie zagrożenia te są rezultatem wielu zjawisk i procesów, które były do niedawna poza głównym nurtem zainteresowania polityków i analityków. Wymagają one zasadniczej zmiany nie tylko dotychczasowych doktryn, lecz także innego planowania działań, odpowiedniego wyposażenia sił zbrojnych czy stosownej infrastruktury, jak również nowego myślenia o budowaniu bezpieczeństwa.

Niezbędne jest uczynienie z zagrożeń elementu ryzyka oraz uświadomienie sobie, że *bezpieczeństwo to nie brak zagrożeń, ale niski akceptowalny poziom ryzyka ich wystąpienia*[2]. Przeciwdziałanie zagrożeniom o znamionach hybrydowych[3] dotyczy przede wszystkim bezpieczeństwa narodowego państw i polega w dużej mierze na skoordynowanym działaniu we wszystkich obszarach: politycznym, ekonomicznym, militarnym, społecznym, informacyjnym i infrastruktury. Zatem bezpieczeństwo jako przedmiot badań łączy w sobie wiele dyscyplin, m.in.: politologię, ekonomię, socjologię czy prawo. Współcześnie wiele krajów dąży do trwałego i zrównoważonego rozwoju w warunkach pożądanego stanu bezpieczeństwa narodowego i międzynarodowego. *Zrównoważony rozwój społeczno-gospodarczy wymaga odpowiedniego poziomu bezpieczeństwa, czyli zdolności zapewnienia niezagrożonego wykorzystania możliwości (potencjału) w budowaniu efektywnej gospodarki jako podstawy tworzenia dobrobytu państwa i jego społeczeństwa*[4].

INICJATYWY MIĘDZYNARODOWE

Nowe spojrzenie na zagrożenia o znamionach hybrydowych spowodowało, że UE i NATO stanęły w obliczu jednego z największych wyzwań w dziedzinie bezpieczeństwa w swojej historii. Obecne

[2] *Współczesne zagrożenia bezpieczeństwa.* Red. G. Ciechanowski, M. Romańczuk, J. Pilżys. Szczecin 2017, s. 7–8.

[3] Zagrożenia o znamionach hybrydowych charakteryzują się tym, że trudno je wykryć i przypisać konkretnej stronie. Działania hybrydowe są prowadzone w sposób skryty.

[4] H. Świeboda: *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej.* ASzWoj, Warszawa 2017, s. 8.

zagrożenia przyjmują coraz częściej formy niekonwencjonalne: czy to w postaci przemocy fizycznej, czy terroryzmu (terroru), czy też wykorzystania przestrzeni cyfrowej, albo też bardziej subtelne i ukierunkowane na represyjne wywieranie nacisku, w tym gospodarczego lub społecznego przez manipulowanie mediami. Za ich pomocą próbuje się wpłynąć na sytuację gospodarczą państw i nastroje społeczeństwa, co może skutkować podważeniem podstawowych wartości, takich jak poszanowanie godności ludzkiej, wolności i demokracji. Przyczyną obecnych wyzwań w sferze bezpieczeństwa jest niestabilność w najbliższym sąsiedztwie UE oraz ewoluujące formy zagrożeń. Konflikt na wschodzie Ukrainy (fot. 2), którego wynikiem jest aneksja Krymu, spowodował, że w NATO i UE podjęto prace w obszarze hybrydowości. Podejście takie miało ułatwić nawiązanie współpracy oraz osiągnięcie efektu synergii przez państwa członkowskie UE i NATO w celu przeciwdziałania zagrożeniom o znamionach hybrydowych.

Przewodniczący Komisji Europejskiej Jean-Claude Juncker podkreślił w swoich politycznych wytycznych z 2014 roku[5] potrzebę budowania silniejszej Europy pod względem bezpieczeństwa i obrony, a także skuteczniejszego łączenia w tym celu instrumentów unijnych i narodowych, niż miało to miejsce w przeszłości. W komunikacie Parlamentu Europejskiego i Rady Europejskiej przedstawiono wspólne ramy działania wraz z propozycjami przeciwdziałania zagrożeniom o znamionach hybrydowych i tworzenia odporności na nie UE. Kompleksowe podejście Unii do zagrożeń ma ułatwić kształtowanie świadomości, budowanie odporności, przeciwdziałanie sytuacjom kryzysowym i reagowanie na nie oraz przezwyciężanie skutków kryzysu. Nowo powołana komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (Hybrid Fusion Cell) ma zajmować się wyłącznie ich analizą. Będzie działać w strukturach Centrum Analiz Wywiadowczych Unii Europejskiej, funkcjonującym przy Europejskiej Służbie Działań Zewnętrznych. Ponadto będzie współpracować z podobnymi organami istniejącymi na szczeblu UE[6], by móc szybko analizować zaistniałe incydenty i zapewniać informacje niezbędne w procesie podejmowania przez Unię strategicznych decyzji.

Odpowiedzią na współczesne zagrożenia w obszarze hybrydowości jest również utworzone w Helsinkach Europejskie Centrum Eksperckie (Hybrid CoE). Ma ono na celu przeciwdziałanie zagrożeniom o znamionach hybrydowych. Z inicjatywą jego otwarcia wystąpiła strona fińska, która jest członkiem UE, ale nie należy do NATO. Za takim posunięciem przemawiały wcześniejsze doświadczenia tego kraju w zwalczaniu zagrożeń ze strony ZSRR oraz działania na rzecz „normalizacji obecnych stosunków" z Rosją[7]. Założono, że powstałe Centrum ma służyć wspieraniu wiedzy eksperckiej w celu wzmocnienia zdolności cywilno-wojskowych oraz odporności i gotowości do przeciwdziałania zagrożeniom o znamionach hybrydowych. Planuje się, że będzie upowszechniać doświadczenie i specjalistyczną wiedzę, w tym także wśród państw UE i NATO. Celem Hybrid CoE jest zapewnienie jednolitego i kompleksowego podejścia (comprehensive approach) oraz jednakowego rozu-

2.

Konflikt na wschodzie Ukrainy w Donbasie, którego wynikiem jest aneksja Krymu, spowodował, że w NATO i UE podjęto prace w obszarze hybrydowości.

MICHAŁ ZIELIŃSKI

[5] *Wspólny komunikat dla Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym.* Bruksela 2016.

[6] Przykładem działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością, Europejskie Centrum ds. Zwalczania Terroryzmu, Frontex oraz unijny zespół reagowania na incydenty komputerowe (CERT).

[7] http://www.dw.com/pl/centrum-przedziwdzia%C5%82ania-zagro%C5%BCeniom-hybrydowym-w-helsinkach-stare-jak-ko%C5%84-troja%C5%84ski/a-40803485/. 15.01.2018.

mienia wspomnianych zagrożeń na poziomie strategicznym. Szczegółowe zadania Centrum obejmują:

– współpracę z rządowymi i pozarządowymi ekspertami z UE i NATO z dziedziny bezpieczeństwa w obszarze hybrydowości na poziomie strategicznym;

– prowadzenie badań i analiz dotyczących zagrożeń hybrydowych;

– wybór narzędzi i metod przeciwdziałania im;

– opracowanie koncepcji i doktryn oraz prowadzenie szkoleń i organizowanie ćwiczeń mających na celu zwiększenie zdolności do przeciwdziałania zagrożeniom o znamionach hybrydowych[8].

Warto wskazać, że w 2014 roku NATO nie miało jednego kompleksowego opracowania doktrynalnego, które sankcjonowałoby działania neutralizujące zdarzenia o charakterze hybrydowym. Potwierdzeniem tej tezy są słowa gen. Philipa Breedlove'a – dowódcy sił NATO w Europie, który w wywiadzie udzielonym niemieckiemu dziennikowi „Die Welt", komentując wydarzenia na Ukrainie, powiedział, że *ogromnym problemem dla NATO jest reakcja na nowy sposób prowadzenia wojny. Pracujemy nad tym*[9]. Wynikało z tego, że Sojusz w owym czasie nie miał instrumentów do przeciwdziałania zagrożeniom o znamionach

[8] Zob. więcej: https://www.hybridcoe.fi/about-us/. 8.01.2018.

[9] *Die NATO muss auf grüne Männchen vorbereitet sein*. W: *Die Welt – Politik – Ukraine-Krise* z 17 sierpnia 2014 roku, http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html/. 27.01.2015.

Odpowiedzią na współczesne zagrożenia w obszarze hybrydowości jest również utworzone w Helsinkach Europejskie Centrum Eksperckie (Hybrid CoE). Ma ono na celu przeciwdziałanie zagrożeniom o znamionach hybrydowych.

hybrydowych, z którymi borykały się rząd i siły zbrojne Ukrainy. Nie oznacza to, że nigdy nie prowadził prac dotyczących hybrydowości współczesnych wojen. Odpowiedzią sił zbrojnych USA na pojawiające się tego typu zagrożenia miał być dokument TC 7-100 Hybrid Threat (zagrożenia hybrydowe), zawierający doświadczenia i wnioski z dotychczasowych wojen. Obecnie w NATO w celu przeciwdziałania im podejmuje się działania prawie we wszystkich dziedzinach, czyli obrony kolektywnej (w ramach przyjętego w Walii planu działań na rzecz gotowości – Readiness Action Plan), a także między innymi cyberprzestrzeni i przestrzeni informacyjnej. Wpisują się one w całościowe podejście Sojuszu do zarządzania kryzysowego. Inne jego działania to nawiązanie współpracy z Ukrainą na rzecz poprawy bezpieczeństwa w obliczu zagrożeń hybrydowych. Jest to platforma dialogu – wymiany doświadczeń z krajem, który zdobył ich wiele w tej dziedzinie. Celem tego dialogu jest stworzenie mechanizmu strategicznej oraz eksperckiej współpracy między NATO i Ukrainą w sprawach dotyczących zwalczania zagrożeń hybrydowych. Inne natowskie przedsięwzięcia uwzględniające te zagrożenia to ćwiczenia z zarządzania kryzysowego, przeprowadzone w 2016 roku (CMX – Crisis Management Exercise). Ich celem było sprawdzenie procedur podejmowania decyzji na poziomie strategicznym i politycznym w obliczu zagrożenia bezpieczeństwa Sojuszu. Fikcyjny scenariusz zakładał wspólną obronę w sytuacji działań hybrydowych, czyli uruchomienie artykułów 4 i 5 traktatu waszyngtońskiego.

Odpowiedzią na wydarzenia na wschodzie Ukrainy były również prace podjęte w ramach Wielonarodowej Kampanii Rozwoju Zdolności (MCDC)[10] edycji 2015–2016, w ramach której zrealizowano projekt *Przeciwdziałanie zagrożeniom hybrydowym* (Countering Hybrid Warfare). Przyjęto w nim założenie, by w przyszłości umieć wykryć i identyfikować zagrożenia o znamionach hybrydowych oraz im przeciwdziałać. Dlatego opracowane w tym projekcie dokumenty zostały ukierunkowane na zrozumienie zjawiska hybrydowości oraz wskazanie sposobów właściwej interpretacji ich istoty w aspekcie szeroko pojętego środowiska bezpieczeństwa.

W wyniku projektu powstały następujące dokumenty:

– *Analiza wstępna* (*Baseline Assessment*), w której przedstawiono rozważania dotyczące istoty zagrożeń hybrydowych;

– *Ramy analityczne* (*Analytical Framework*), zawierające propozycję założeń analitycznego modelu, który umożliwiłby analizę tych zagrożeń;

– *Zrozumieć konflikt hybrydowy* (*Understanding Hybrid Warfare*) – dokument zbiorczy uwzględniający studium przypadków (case study) konfliktów o znamionach hybrydowych.

Opracowane dokumenty są efektem prac międzynarodowej grupy roboczej, a nie oficjalnymi poglądami i stanowiskami poszczególnych państw (organizacji) uczestniczących w projekcie.

Ze względu na niewyczerpanie pełnego zakresu prac w edycji MCDC 2016–2017 postanowiono kontynuować projekt w latach 2017–2018 jako Countering Hybrid Warfare # 2. Zdecydowano, że prace będą prowadzone równocześnie w trzech obszarach: identyfikowanie zagrożeń o znamionach hybrydowych (detect), odstraszanie (deterence) oraz wypracowanie skutecznych narzędzi do przeciwdziałania (respond). Planuje się, że efektem końcowym będą dokument koncepcyjny oraz poradnik, zawierające treści dotyczące metod identyfikacji, zbierania informacji i sposobu analizy zagrożeń o znamionach hybrydowych. Opracowane dokumenty pozwolą na sformułowanie wniosków i rekomendacji odnoszących się do roli współczesnych sił zbrojnych jako podstawowego narzędzia gwarantującego bezpieczeństwo wewnętrzne i zewnętrzne państwa w sytuacji wystąpienia zagrożeń o znamionach hybrydowych.

RODZIMA INICJATYWA

Polski wkład w rozwój prac w omawianym obszarze to opracowana w Centrum Doktryn i Szkolenia SZ *Koncepcja udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym,* zatwierdzona przez szefa Sztabu Generalnego 11 grudnia 2017 roku. Przeznaczona jest dla dowództw, sztabów i wojsk realizujących przedsięwzięcia związane z przeciwdziałaniem zagrożeniom o znamionach hybrydowych na poziomie strategicznym i operacyjnym. Dokument zawiera między innymi podstawowe informacje na temat tych zagrożeń, w tym wskazuje ich znaczenie dla współczesnego środowiska bezpieczeństwa naszego kraju oraz ogólne założenia i kierunki rozwoju zdolności sił zbrojnych przeciwdziałania im. Koncepcja ta ma ułatwić udzielenie odpowiedzi na pytania istotne dla współczesnych sił zbrojnych jako kluczowego

[10] Wielonarodowa Kampania Rozwoju Zdolności (Multinational Capability Developement Campaign – MCDC) jest sześcioletnim programem poświęconym tworzeniu nowych zdolności operacyjnych w ramach współpracy międzynarodowej. Stanowi kontynuację programu wielonarodowych eksperymentów (Multinational Experimentation – MNE) zainicjowanego przez Połączony Sztab Sił Zbrojnych USA w 2001 roku w celu umożliwienia lepszego wzajemnego zrozumienia i zwiększenia interoperacyjności partnerów międzynarodowych z różnych kontynentów i kręgów kulturowych.

narzędzia gwarantującego bezpieczeństwo wewnętrzne i zewnętrzne państwa oraz istotnego elementu osłony strategicznej[11]. Pytania te są następujące:

– Jaka jest rola SZRP w przeciwdziałaniu zagrożeniom o znamionach hybrydowych?

– Jakie zdolności powinny mieć i rozwijać siły zbrojne w celu przeciwdziałania tym zagrożeniom?

– W jaki sposób mogą one wesprzeć układ pozamilitarny?

– Czy konieczna jest zmiana aktów prawnych dotyczących użycia SZRP w działaniach poniżej progu wojny?

Koncepcja nie rozwiązuje wszelkich potencjalnych problemów i nie wyjaśnia wątpliwości, jednakże ujmuje istotę zagrożeń o znamionach hybrydowych, podaje kluczowe definicje oraz fazy rozwoju możliwych działań w ramach przeciwdziałania im. Należy podkreślić, że zaproponowane w tym dokumencie rozwiązania dotyczące wykorzystania SZRP do tego celu uwzględniają wnioski wynikające ze zmian funkcjonowania państwa w środowisku geopolitycznym, z konfliktów, w których działania nosiły znamiona hybrydowych oraz z doświadczeń szkoleniowych zarówno SZRP, jak i pozostałych państw NATO. Wyzwaniem dla polityki obronnej i globalnego bezpieczeństwa jest nie tylko budowanie świadomości w dziedzinie zagrożeń, ich identyfikacja i wypracowanie strategii przeciwdziałania im, lecz przede wszystkim działania mające na celu utworzenie systemu wczesnego ostrzegania, który pozwoli na uniknięcie destabilizacji w danym regionie czy też państwie. Określenie poziomu czy też skali zagrożeń jest złożonym przedsięwzięciem, wymagającym dogłębnej analizy badanego środowiska, w tym czynników niemierzalnych, trudnych do przewidzenia. Ważne jest kompleksowe podejście i zbadanie tych dziedzin, które dotychczas były traktowane jako znacznie mniej istotne lub w ogóle pomijane. Tylko takie podejście do kwestii wspólnej polityki zwalczania zagrożeń nowego typu, czyli łączenie instrumentów: politycznych, ekonomicznych, militarnych i społecznych, pozwoli na przeciwdziałanie im.

Umiejętność rozpoznania i przeciwstawienia się zidentyfikowanym zagrożeniom będzie stanowić o zdolności państw do przetrwania w nowym środowisku bezpieczeństwa. Niezbędne jest przy tym wzmocnienie odporności oraz opracowanie narzędzi odstraszania, a także ustanowienie wspólnych ram dla zrozumienia, czym obecnie są zagrożenia hybrydowe i w jaki sposób mogą one wpływać na bezpieczeństwo państw. Jest to możliwe tylko dzięki skoordynowaniu wzajemnej współpracy między państwami. ■

[11] Osłona strategiczna odnosi się do przedsięwzięć militarnych i niemilitarnych i obejmuje działania realizowane stale w czasie pokoju i kryzysu w celu ochrony przed zaskoczeniem oraz różnymi formami przemocy. R. Jakubczak, J. Marczak, K. Gąsiorek: *Założenia polityki i strategii bezpieczeństwa narodowego. Podstawy bezpieczeństwa narodowego Polski w erze globalizacji.* Warszawa 2008, s. 130.

Lekkie pododdziały w neutralizacji **zagrożeń hybrydowych**

PODODDZIAŁY KAWALERII POWIETRZNEJ Z UWAGI NA MOŻLIWOŚCI MANEWROWE MOGĄ BYĆ WYKORZYSTYWANE DO LIKWIDACJI OŚRODKÓW OPORU I ZAPOBIEGANIA ROZPRZESTRZENIANIU SIĘ ZAGROŻEŃ PROWADZĄCYCH DO ZBROJNEGO KONFLIKTU.

mjr dr Ryszard Kalisiak

Autor jest adiunktem w Zakładzie Rozpoznania i Wojsk Aeromobilnych Instytutu Dowodzenia Akademii Wojsk Lądowych.

W artykule przedstawiono rozważania dotyczące technicznych i formalnoprawnych aspektów użycia pododdziałów lekkich w neutralizacji[1] zagrożeń hybrydowych w fazie działań militarnych[2]. Zaprezentowano też propozycje rozwiązań funkcjonalnych, dzięki którym możliwe będzie użycie pododdziałów wojska, w tym sił lekkich[3], bez konieczności wprowadzania stanu wyjątkowego i stanu wojny[4].

WACHLARZ ZAGROŻEŃ

Zamiarem autora nie jest opisywanie przebiegu działań hybrydowych oraz jego elementów składowych, lecz skupienie się na najbardziej spektakularnej ich części, czyli fazie działań militarnych, będącej rozwinięciem fazy destabilizacyjnej. Charakteryzuje się ona stosowaniem coraz agresywniejszych form oddziaływania, do których możemy zaliczyć między innymi działanie grup paramilitarnych złożonych z mniejszości narodowych bądź religijnych. Mogą one być wspierane i wzmacniane żołnierzami regularnych sił zbrojnych agresora bez widocznych oznaczeń. Ich zadaniem będzie prawdopodobnie destabilizowanie sytuacji przez stosowanie aktów terrorystycznych. Będzie to można osiągnąć atakując między innymi takie obiekty, jak: przejścia graniczne, stacje przekaźnikowe, mosty i wiadukty na głównych ciągach komunikacyjnych oraz linie kolejowe i lotniska lub miejsca skupisk ludności. Działania te prawdopodobnie będą prowadzone równolegle z działaniami dyplomatycznymi oraz informacyjnymi, których głównym celem będzie dezinformowanie opinii publicznej, szczególnie międzynarodowej, o rzeczywistej sytuacji w danym regionie[5].

Biorąc pod uwagę prawdopodobny scenariusz przebiegu początkowej fazy działań militarnych, należy podkreślić, iż czynnikiem decydującym o skutecznym działaniu służb i wojska w tym okresie będzie szybka i precyzyjna neutralizacja zagrożeń. Do tego celu powinno się wykorzystać algorytm zawierający takie elementy, jak: identyfikacja przeciwnika, jego izolacja oraz eliminacja (rys. 1).

[1] Neutralizacja – rozumiana jako osłabianie negatywnego oddziaływania lub eliminacja fizyczna bądź psychologiczna.

[2] *Koncepcja udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym (projekt).* Bydgoszcz 2017, s. 13/47.

[3] Do sił lekkich możemy zaliczyć wszystkie jednostki, które nie dysponują ciężkimi pojazdami opancerzonymi.

[4] *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*. DzU 2002 nr 156, poz. 1301.

[5] Ibidem, s. 13/47.

W *identyfikacji*, czyli wykrywaniu i określaniu poziomu zagrożenia, istotne znaczenie ma współdziałanie m.in. służb podległych Ministerstwu Spraw Wewnętrznych i Administracji, Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, z pododdziałami rozpoznawczymi oraz wykorzystanie wojsk obrony terytorialnej. W zadaniach *izolowania* główną rolę powinny odgrywać jednostki Policji, Żandarmerii Wojskowej oraz pododdziały wojsk obrony terytorialnej. Natomiast do *eliminacji* mogą być wyznaczane, po określeniu ważności obiektu, odpowiednio elementy wojsk specjalnych lub jednostki antyterrorystyczne Policji bądź pododdziały zmechanizowane (zmotoryzowane) wojsk lądowych oraz obrony terytorialnej (rys. 2).

PROPOZYCJA

Biorąc pod uwagę obecny stan prawny, takie rozwiązanie wymagałoby wprowadzenia co najmniej stanu wyjątkowego regulowanego na mocy odpowiedniej ustawy. W tym miejscu należy wspomnieć o dość niejednoznacznych i porozrzucanych w wielu miejscach aktach prawnych mówiących o sposobie użycia Sił Zbrojnych RP w stanie innym niż wojenny lub wyjątkowy. Analiza dokumentów normatywnych pozwala skonstatować, iż przy nieznacznych zmianach formalnych między- i wewnątrzresortowych można w ograniczonym stopniu użyć pododdziałów sił zbrojnych do utrzymania porządku publicznego. Szczególnie w pierwszym okresie narastania kryzysu, nim zostaną wyczerpane wszystkie znamiona działań hybrydowych. Należałoby obecnie istniejący system służb dyżurnych w siłach zbrojnych dostosować tak, by mógł skutecznie reagować na potencjalne zagrożenia. Wstępna jego analiza pozwala wyciągnąć następujące wnioski, mające wpływ na przystosowanie go do zagrożeń hybrydowych. Powinno to nastąpić dzięki:

– rozszerzeniu uprawnień wojskowych organów porządkowych w zakresie wsparcia struktur niemilitarnych w utrzymaniu porządku publicznego;

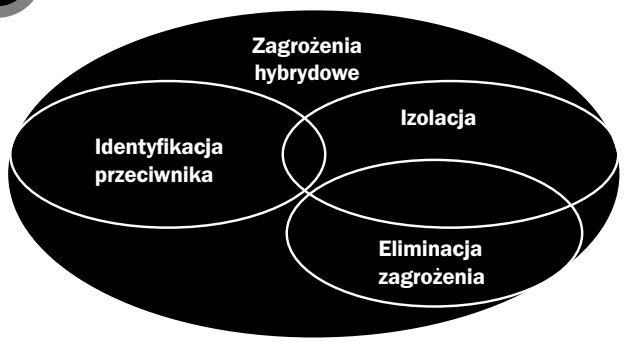
– zwiększeniu składów pododdziałów alarmowych bądź też ich liczby, zarówno w jednostkach, jak i garnizonach z uwzględnieniem poziomu narastania sytuacji kryzysowej;

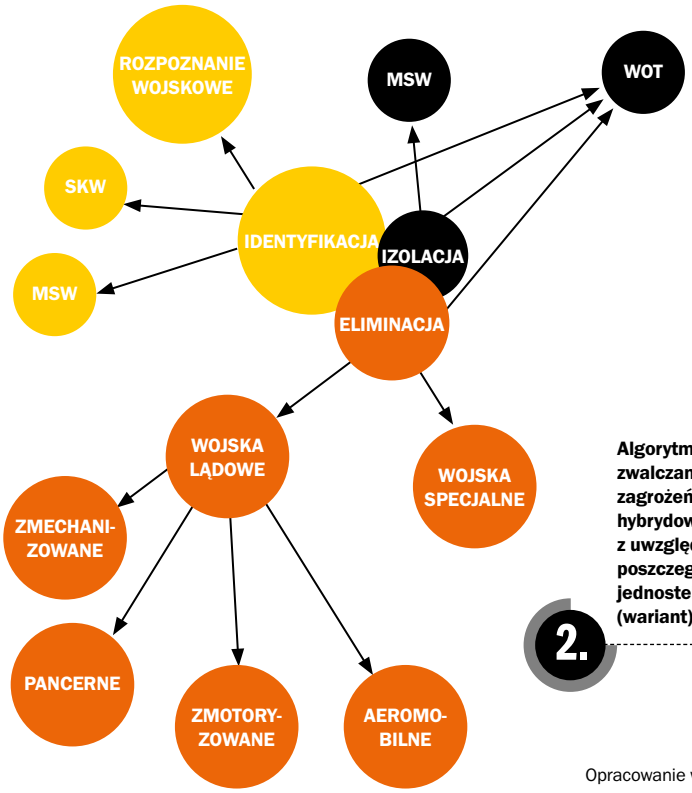
– funkcjonowaniu pododdziałów alarmowych, które powinny dysponować, poza bronią osobistą, transporterami opancerzonymi oraz bronią zespołową;

– włączeniu jednostek WOT w system służb po osiągnięciu przez ten rodzaj sił zbrojnych gotowości operacyjnej.

Jednocześnie analiza literatury przedmiotu oraz osobiste doświadczenia autora pozwalają wyciągnąć wniosek, iż użycie sił lekkich w tej fazie działań będzie w swej naturze bardzo podobne do realizacji takich zadań, jak: przeszukiwanie terenu, czyli operacje Cordon&Search, patrolowanie oraz organizacja posterunków obserwacyjnych, a także stałych i tymczasowych posterunków kontrolnych. Zadania te powinny być wykonywane w połączonych zespołach policyjno-wojskowych.

1. **Algorytm zwalczania zagrożeń hybrydowych (wariant)**





2. **Algorytm zwalczania zagrożeń hybrydowych z uwzględnieniem poszczególnych jednostek i służb (wariant)**

Opracowanie własne (2).

Z uwagi na obwarowania formalne oraz finansowe należy unikać służb 24-godzinnych. Skłaniać się trzeba raczej ku realizowaniu ich w cyklach 6–8-godzinnych lub podobnie jak w jednostkach policji wykonujących zadania patrolowe – 12 na 24 godziny. Należałoby również wprowadzić ustalenia międzyresortowe, aby uszczegółowić zakres współdziałania oraz określić, kiedy i na jakich zasadach będą one wchodzić w życie.

Podstawowym wyzwaniem jest zatem opracowanie systemu dowodzenia i łączności oraz procedur współdziałania na taką okoliczność. By móc sprawnie wdrożyć proponowaną koncepcję, należy poszukać odpowiedzi na takie pytania, jak: kto będzie dowodził takim patrolem oraz w jaki sposób; kto będzie monitorował i kierował realizacją zadań; jak będzie zorganizowany system łączności. ■

JONATHAN ALPEYRIE

ABY SKUTECZNIE PRZECIWSTAWIĆ SIĘ HYBRYDOWYM DZIAŁANIOM, NALEŻY SWOJE WŁASNE DOSTOSOWAĆ DO CHARAKTERU WALKI PROWADZONEJ PRZEZ PRZECIWNIKA.

Historia wojen hybrydowych sięga konfliktu w Osetii Południowej z 2008 roku. Zatargi etniczne doprowadziły do eskalacji działań między Gruzinami a separatystami osetyńskimi i siłami rosyjskimi.

Zagrożenia hybrydowe

WRAZ Z ZAKOŃCZENIEM ZIMNEJ WOJNY I TZW. ERY DWUBIEGUNOWEJ ŚWIATA POWSTAŁ SYSTEM JEDNOBIEGUNOWY Z PRZEWAGĄ AMERYKAŃSKIEJ POTĘGI MILITARNEJ.

mjr dypl. SZRP Grzegorz Otocki

Fakt przynależności naszego kraju do Unii Europejskiej i NATO nie zwalnia nas z konieczności bycia w gotowości do przeciwdziałania potencjalnemu zagrożeniu. Postrzeganie bezpieczeństwa kraju wyłącznie przez pryzmat sojuszniczej pomocy i zawartych traktatów jest świadectwem ignorancji i może doprowadzić do klęski, jaką Polska poniosła w 1939 roku. Już kilka lat po przystąpieniu Polski do Sojuszu Północnoatlantyckiego zauważono, że stan i wyposażenie naszej armii wymagają wprowadzenia pewnych zmian, które wpłyną na zaangażowanie w walkę nie tylko sił zbrojnych, lecz także układu pozamilitarnego. Dopiero taki system obrony, holistycznie powiązany „obszarowo", opierający się na obronnych właściwościach terenu, będzie skuteczną tarczą nie do pokonania w razie jakiejkolwiek agresji. Czynnikiem, który obudził z „letargu" i skłonił do refleksji nad stanem własnych możliwości oraz armii innych krajów europejskich, była aneksja Krymu oraz wybuch konfliktu z prorosyjskimi separatystami w obwodzie donieckim i ługańskim na Ukrainie.

ZAGROŻENIA BEZPIECZEŃSTWA PAŃSTWA

W pierwszej kolejności należy podjąć próbę wyjaśnienia, czym jest *zagrożenie,* oraz ustalenia, jaki ma wpływ na bezpieczeństwo państwa. *Leksykon wiedzy wojskowej* definiuje to pojęcie jako: *sytuację, w której istnieje zwiększone prawdopodobieństwo utraty życia, zdrowia, wolności lub dóbr materialnych. Zagrożenie wywołuje u człowieka niepokój lub strach o różnym stopniu natężenia, do przerażenia lub obezwładnienia włącznie, bądź odruch lub świadomą chęć przeciwdziałania. Zagrożenie może wynikać z przyczyn naturalnych (np. oddziaływanie żywiołów) i spowodowanych przez innego człowieka (np. nieprzyjaciela)*[1]. Podobnie wyjaśnia je *Słownik terminów z zakresu bezpieczeństwa narodowego*, w którym czytamy, że jest to: *sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia: militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenie polityczne, ekonomiczne (gospodarcze), psychospołeczne, ekologiczne, wewnętrzne i inne*[2]. W kolejnej definicji *zagrożenie* określa się jako: *pewien stan psychiki lub świadomości, wyrażany postrzeganiem zjawisk, które są oceniane jako niekorzystne i niebezpieczne, ale też jako czynniki powodujące ten stan niepewności i obaw, czyli rzeczywiste działania innych uczestników życia społecznego, niekorzystne i niebezpieczne dla żywotnych interesów i podstawowych wartości danego podmiotu*[3]. Z przytoczonych definicji wynika, że najczęściej postrzegamy zagrożenie jako pewien stan psychiczny lub świadomościowy wywołany postrze-

Autor jest asystentem w Zakładzie Dowodzenia Instytutu Sztuki Operacyjnej i Taktyki Wydziału Wojskowego Akademii Sztuki Wojennej.

[1] *Leksykon wiedzy wojskowej*. Red. M. Laprus. MON, Warszawa 1979, s. 510.
[2] *Słownik terminów z zakresu bezpieczeństwa narodowego.* Red. B. Zdrodowski. AON, Warszawa 2008, s. 173.
[3] R. Zięba: *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku.* Warszawa 1997, s. 5.

ganiem zjawisk, które ocenia się jako niekorzystne lub niebezpieczne, powodujące stany niepewności i obaw[4] w sytuacji, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia[5]. Z kolei odnosząc się do bezpieczeństwa państwa, możemy określić, że jest to stan niestały i niestabilny. Jest systematycznie zmieniającym się procesem, w którym należy ciągle dostosowywać siły, środki i narzędzia zapewniające bezpieczeństwo stosownie do występujących zagrożeń. Podobne stanowisko prezentuje Ryszard Zięba[6], który twierdzi, że: *bezpieczeństwo narodów i państw jest zjawiskiem zmiennym w czasie. Ewolucja jego subiektywnych i obiektywnych elementów sprawia, że stanowi ono sekwencję zmieniających się stanów i procesów społecznych w skali międzynarodowej. Jest to proces, w którym ścierają się funkcjonujące wyzwania i zagrożenia, percepcja społeczna i koncepcje ich rozwiązywania oraz działania i oddziaływania państw zmierzające do budowania ich pewności przetrwania, posiadania i swobód rozwojowych*[7]. Natomiast zagrożenie bezpieczeństwa w *(Mini)Słowniku BBN* zostało sformułowane jako: *Najbardziej klasyczny czynnik środowiska bezpieczeństwa; rozróżnia się zagrożenia potencjalne i realne; subiektywne i obiektywne; zewnętrzne i wewnętrzne; militarne i niemilitarne; kryzysowe i wojenne; intencjonalne i przypadkowe (losowe)*[8]. W związku z tym takie oddziaływanie może odnosić się do konkretnego podmiotu, jakim jest państwo, i powodować zachwianie jego równowagi przez *splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych – w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp.*[9]

Biorąc pod uwagę czynniki, które cechują społeczeństwa, takie jak odrębność od innych zbiorowości, wzajemne oddziaływania między jego członkami, wspólne terytorium, instytucje, sposób komunikowania się, podobieństwo warunków życia, podział pracy, normy i wzorce postępowania, możemy się spodziewać, że będą występowały zagrożenia społeczne bezpieczeństwa narodowego (państwa) (social threats to national security), odnoszące się do wszystkiego, co zagraża utratą życia i zdrowia, tożsamości narodowej i etnicznej poszczególnych społeczności oraz bezpieczeństwa socjalnego (cywilizacyjnego) i publicznego[10]. Argumenty te skłaniają do określenia współczesnych zagrożeń dla naszego kraju. Z przebiegu zdarzeń na Ukrainie wynika, że istnieje ryzyko konfliktów o charakterze regionalnym i lokalnym. Taki konflikt może oddziaływać na nasz kraj pośrednio lub bezpośrednio wraz z różnymi formami nacisku politycznego, występowaniem fal uchodźców z terenów objętych nim czy nawet agresji zewnętrznej. Zagrożenia te mogą w niesprzyjających okolicznościach przyjąć charakter niemilitarny i militarny. Zagrożenia militarne traktowane jako *splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej – w wyniku zastosowania wobec niego przemocy zbrojnej (militarnej)*[11] mogą przybrać postać zagrożeń kryzysowych oraz wojennych o różnej skali – od działań zbrojnych poniżej progu wojny do mniej prawdopodobnego konfliktu na dużą skalę[12].

Jeżeli wystąpi taki splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopo-

NIEZIDENTYFIKOWANA ORGANIZACJA WIELKIEGO MOCARSTWA, JAK RÓWNIEŻ

[4] S. Korycki: *System bezpieczeństwa Polski*. Warszawa 1994, s. 54.

[5] R. Grocki: *Vademecum zagrożeń*. Bellona, Warszawa 2003, s. 9.

[6] Prof. dr hab. Ryszard Zięba – ekspert w dziedzinie bezpieczeństwa międzynarodowego, polityki zagranicznej i bezpieczeństwa Polski, państw Europy Środkowej i Wschodniej, wielkich mocarstw i Unii Europejskiej. Obecnie jest także ekspertem Polskiej Komisji Akredytacyjnej. http://www. pl. ism. uw.edu .pl/ prof-ryszard-zieba/. 25.03.2018.

[7] R. Zięba*: Instytucjonalizacja bezpieczeństwa europejskiego*. Warszawa 2001, s. 47.

[8] *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*. https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035, Minislownik-Bbn-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html/. 15.03.2018.

[9] S. Dworecki: *Zagrożenia bezpieczeństwa państwa*. AON, Warszawa 1994, s. 61.

[10] *Słownik terminów...,* op.cit., s. 177.

[11] S. Dworecki: *Zagrożenia...,* op.cit., s. 25.

[12] *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej.* Warszawa 2014, s. 20.

dobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, ewentualnie naruszenie jego suwerenności w wyniku zastosowania wobec niego przemocy niezbrojnej, będziemy mieli do czynienia z zagrożeniami niemilitarymi (non-military threats)[13]. Kolejne zagrożenia, na które warto zwrócić uwagę, są związane z rozwojem nowych technologii. Są one niejako wynikiem nieuniknionego postępu cywilizacyjnego, który niesie ze sobą wiele udogodnień, jednak również możliwości negatywnego oddziaływania na poszczególnych ludzi i całe społeczeństwa.

Można dostrzec, że wraz z powstaniem oraz rozwojem Internetu pojawiły się nowe rodzaje zagrożeń, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty czy cyberwojna, które cechują się głównie udziałem podmiotów niepaństwowych lub niezdefiniowanych aktorów. Obecnie wszelkie konflikty i działania w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw ze względu na coraz większe uzależnienie od technologii komputerowych i teleinformatycznych.

ZAGROŻENIA HYBRYDOWE

Po zakończeniu zimnej wojny panowało przekonanie, że ostatecznie minęło zagrożenie konfliktem militarnym na wielką skalę. Większość państw, w tym również i nasz kraj, stawiało na rozwój współpracy politycznej i gospodarczej w celu ustabilizowania środowiska międzynarodowego, tym samym osiągania jak największych korzyści ekonomicznych na drodze współpracy, a nie rywalizacji i konfliktów. Najważniejszym momentem zmiany w postrzeganiu tego, co stanowi największe zagrożenie dla współczesnych państw, był atak 11 września 2001 roku w USA. Cały świat przekonał się, że to nie państwo, tylko niezidentyfikowana organizacja może wstrząsnąć ładem nawet wielkiego mocarstwa, jak również całego ziemskiego globu. Takie działania możemy ująć w ramy zagrożeń aterytorialnych, które są: *zagrożeniami (operacjami) o charakterze nagłym, niespodziewanym, selektywnym, o ograniczonej skali, które nie wiążą się z zamiarem opanowania terytorium zaatakowanego państwa, a jedynie z zadaniem strat dla wymuszenia pożądanych przez agresora zachowań politycznych*[14]. Stosując różne środki i metody oddziaływania w celu obejścia lub zanegowania silnych stron przeciwnika przy jednoczesnym wykorzystaniu jego słabości dla uzyskania niewspółmiernego efektu, dochodzimy do zagrożeń asymetrycznych (asymmetric threats), dotyczących sfery militarnej i niemilitarnej. Postępowanie to obejmuje przemyślenie, organizowanie i prowadzenie działań odmiennych od aktywności przeciwnika, w tym sięganie po wszelkiego rodzaju różnice w szeroko rozumianych potencjałach stron w celu zwiększenia własnej przewagi oraz korzystania ze słabości strony przeciwnej dla uzyskania dominacji nad nią i większej swobody operacyjnej[15].

Podejmując próbę scharakteryzowania hybrydowości oraz definicji związanych z tą problematyką, należy wyjaśnić pojęcie *hybryda* oraz scharakteryzować jej rodzaje. Według *Słownika wyrazów obcych – hybryda to coś, co składa się z różnych elementów, często do siebie niepasujących*[16]. Marek Wrzosek rozpatruje definicje hybrydy w czterech zasadniczych ujęciach.

Po pierwsze *hybryda* to połączenie w całość różnych części, składników wykluczających się, gdy funkcjonują oddzielnie. W praktyce takim połączeniem może być napęd hybrydowy w postaci silnika elektrycznego i spalinowego.

Po drugie jest to wyraz złożony z dwóch elementów językowych o znaczeniu nowo utworzonym w danym języku (neologizm). Przykładem jest powszechnie używane określenie *pirat drogowy*.

Po trzecie to figura heraldyczna powstała z połączenia różnych części zwierząt w całość, na przykład lew ze skrzydłami w postaci gryfa czy też dwugłowy orzeł.

Po czwarte pojęcie hybrydy w odniesieniu do biologii oznacza osobnika powstałego po skrzyżowaniu dwóch różnych genetycznie ras bądź odmian[17].

Niezależnie od rozumienia tego pojęcia w kontekście hybrydowości zagrożeń bezpieczeństwa państwa należy być przygotowanym do przeciwdziałania im w różnych środowiskach z zastosowaniem wszelkich dostępnych metod i środków

MOŻE WSTRZĄSNĄĆ ŁADEM NAWET CAŁEGO ZIEMSKIEGO GLOBU

[13] *Słownik terminów...,* op.cit., s. 176.
[14] *(Mini)Słownik BBN...,* op.cit.
[15] *Słownik terminów...,* op.cit., s. 173.
[16] *Wielki słownik wyrazów obcych PWN.* Warszawa 2008, s. 518.
[17] M. Wrzosek: *Wojny przyszłości. Doktryna, technika, operacje militarne.* Warszawa 2018, s. 315–316.

MICHAŁ ZIELIŃSKI

WOJNA HYBRYDOWA ŁĄCZY W SOBIE RÓŻNE ŚRODKI I METODY PRZEMOCY, W TYM ZBROJNE DZIAŁANIA REGULARNE I NIEREGULARNE, OPERACJE W CYBERPRZESTRZENI ORAZ DZIAŁANIA EKONOMICZNE.

adekwatnie do adwersarza hybrydowego czy też zwanego podprogowym. Przy tym należy wyodrębnić z informacyjnego chaosu różnorodnych definicji i form działań hybrydowych te, które będą odpowiadały realnym zagrożeniom. Istotą działań hybrydowych odróżniającą je od wojny hybrydowej jest fakt utrzymywania przez przeciwnika agresji poniżej progu wojny, którego nie da się jednoznacznie określić i zidentyfikować ze względu na początkowo niejawny charakter jego poczynań.

Analiza konfliktów, w których istotnym elementem były działania hybrydowe, na przykład konflikt na wschodzie Ukrainy i w Libanie czy działania ISIS (Państwa Islamskiego), upoważnia do wniosku, że w ich przebiegu można wyróżnić trzy zasadnicze fazy:

– przygotowania,
– destabilizacji,
– rozstrzygnięcia[18].

Na uwagę zasługuje fakt przeradzania się ukrytego działania w jawne dopiero wtedy, gdy zostaje zauważone przez atakowane państwo. Zazwyczaj jest jednak za późno, gdyż sytuacja uległa już destabilizacji, a organy państwowe nie są w stanie realizować swoich zadań. Następuje wówczas potęgowanie separatyzmów na tle etnicznym, ideologicznym czy religijnym.

Według Williama J. Nemetha[19] wojna hybrydowa cechuje się m.in.:

– organizacją armii odzwierciedlającą poziom rozwoju społeczno-ekonomicznego danej wspólnoty oraz obowiązujące w niej normy,

– innym od zachodniego sposobem percepcji siły militarnej – w przypadku „działań hybrydowych" ich siła ma polegać na masowym wykorzystaniu taktyk partyzanckich, które stwarzają poważne zagrożenie dla hierarchicznie zorganizowanych i wysoko zaawansowanych technologicznie oddziałów

[18] W CDiS SZ w Bydgoszczy w dniach 15–16 września 2015 roku odbyły się warsztaty grupy eksperckiej na temat *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym* z udziałem przedstawicieli resortu obrony narodowej, ośrodków akademickich wojskowych i cywilnych oraz wywiadu i kontrwywiadu wojskowego. W ramach warsztatów uzgodniono treść definicji działań hybrydowych oraz fazy ich przebiegu.

[19] Terminy *działania hybrydowe* oraz *wojna hybrydowa* pojawiły się już w 2002 roku w pracy Williama J. Nemetha: *Future war and Chechnya: A case for hybrid warfare.*

przeciwnika. Ponadto doświadczenia konfliktu rosyjsko-czeczeńskiego wskazują, że wojna hybrydowa jest prowadzona w sposób totalny, ponieważ jest traktowana jako narzędzie ochrony danej wspólnoty przed całkowitą zagładą. W związku z tym tego typu konflikt dopuszcza użycie wszelkich niezbędnych środków, w tym m.in. porwań oraz masowych mordów. Efektem działań hybrydowych jest także doprowadzenie do zatarcia się granicy między osobami zaangażowanymi w walki zbrojne a cywilami,

– umiejętnością zastosowania nowoczesnych technologii w działaniach taktycznych oraz strategicznych. Posiadanie tych umiejętności oznacza również zdolność do innowacyjnego wykorzystania danej technologii w sposób, który nie był przewidziany przez jej twórców[20].

Szef Sztabu Armii USA gen. George W. Casey zdefiniował w 2008 roku hybrydowe zagrożenie jako działanie przeciwnika obejmujące *różnorodne i dynamiczne kombinacje zdolności konwencjonalnych, nieregularnych, terrorystycznych i przestępczych*[21]. Stwierdził, że jest to nowy typ wojny, który będzie coraz powszechniejszy w przyszłości. Natomiast Dowództwo Sił Połączonych USA definiuje hybrydowe zagrożenie jako *każde działanie przeciwnika, który jednocześnie i adaptacyjnie stosuje dopasowaną kombinację konwencjonalnych, nieregularnych, terrorystycznych i kryminalnych środków lub działań w operacyjnej przestrzeni walki. Zamiast pojedynczego bytu, hybrydowym zagrożeniem może być połączenie podmiotów państwowych i niepaństwowych*[22].

W 2011 roku zaś w armii USA zdefiniowano zagrożenie hybrydowe jako *zróżnicowane i dynamiczne połączenie regularnych i nieregularnych sił, elementów kryminalnych lub kombinacja tych sił i elementów, które są zjednoczone, by osiągnąć wzajemnie korzystne efekty*[23]. Według Jaspera Scota w NATO używa się tego terminu do opisania *przeciwników zdolnych do jednoczesnego wykorzystywania konwencjonalnych oraz niekonwencjonalnych środków adaptacyjnie w dążeniu do swoich celów*[24]. Należałoby zatem zadać pytanie, czy wszystkich pojęć odnoszących się do zagrożeń hybrydowych nie można byłoby zdefiniować jako wszelkich sposobów i metod działania ukierunkowanych na wykorzystanie słabych stron przeciwnika.

Istnieje wiele terminów używanych w odniesieniu do pojęcia wojny hybrydowej: agresja podprogowa[25], wojna hybrydowa, zagrożenia hybrydowe, wpływ hybrydowy lub przeciwnik hybrydowy (jak również wojna nieliniowa, wojna nietradycyjna lub wojna specjalna).

Dokonując analizy tej terminologii, można spostrzec, że w ujęciu amerykańskim wojna hybrydowa (hybrid warfare) to połączenie „morderczości" konfliktu międzypaństwowego i przedłużającej się „żarliwości" konfliktu nieregularnego. Skomplikowane kampanie łączą operacje konwencjonalne o małej intensywności z operacjami specjalnymi oraz działania ofensywne w cyberprzestrzeni i operacje psychologiczne z wykorzystaniem mediów społecznościowych z tradycyjnymi w celu wywierania wpływu na opinię publiczną, w tym tzw. trolling, również na poziomie międzynarodowym.

Wojna hybrydowa to strategia polityczno-militarna, która polega na prowadzeniu wojny politycznej i łączeniu działań konwencjonalnych, nieregularnych i cybernetycznych z innymi metodami, takimi jak podawanie fałszywych wiadomości czy stosowanie agresywnej dyplomacji, a ostatecznie na zagranicznej interwencji wyborczej. Przez łączenie operacji kinetycznych z działaniami wywrotowymi agresor zamierza uniknąć odpowiedzialności, ponieważ trudno jest jednoznacznie zdefiniować i jego samego i jego działania. Ze względu na współczesne uregulowania prawnomiędzynarodowe, które nie zawierają jasnych definicji, agresor może uniknąć w takiej wojnie odpowiedzialności[26].

(Mini)Słownik BBN definiuje pojęcie wojny hybrydowej jako wojny łączącej w sobie jednocześnie różne możliwe do zastosowania środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne i psychologiczne, kampanie informacyjne (propaganda) itp.[27] To wreszcie

[20] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia, s. 40–41.* https://www.abw.gov.pl/download/1/1925/skoneczny.pdf/. 19.03.2018.

[21] G. Grant: *Hybrid Wars.* Government Executive. National Journal Group. http://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/. 6.03.2018.

[22] B.P. Fleming: *Hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art.* United States Army Command and General Staff College. https://publicatio-gmun.bitbucket.io/08-nellie-koelpin-sr/9781288253241-hybrid-threat-concept-contemporary-war-military/. 6.03.2018.

[23] Ibidem.

[24] J. Scott: *Moreland Scott The Islamic State is a Hybrid Threat: Why Does That Matter?* "Small Wars Journal". Small Wars Foundation. Retrieved 5.08.2015. http://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter/. 6.03.2018.

[25] *Agresja podprogowa – działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa. (Mini)Słownik...,* op.cit.

[26] G. Grant: *Hybrid Wars...,* op.cit.

[27] *(Mini)Słownik BBN...,* op.cit.

działania polegające na wykorzystaniu wojennych i pozamilitarnych instrumentów w zintegrowanej kampanii, która ma zaskoczyć przeciwnika, a potem umożliwić przejęcie inicjatywy i osiągnięcie korzyści psychologicznych. W tym celu wykorzystuje się na dużą skalę działania dyplomatyczne, „przykrycie" informatyczne i radioelektroniczne, cyberoperacje, ukrywa się jak najdłużej prowadzenie operacji wojskowych i wywiadowczych – wszystko w połączeniu z wywieraniem silnej presji ekonomicznej[28].

Biorąc pod uwagę przedstawione definicje, można stwierdzić, że wojna hybrydowa to nic innego jak *kombinacja otwartych i tajnych działań bojowych, prowokacji i dywersji w połączeniu z negowaniem własnego zaangażowania, co znacznie utrudnia reakcję odpowiednią do tych działań*[29].

NIECO HISTORII

Odzyskanie przez nasz kraj niepodległości po zakończeniu I wojny światowej było dopiero prologiem do długiej walki o jej utrzymanie. Na każdym kroku toczono zaciekłą walkę o istnienie i funkcjonowanie na arenie międzynarodowej.

Trudno się dziwić, że brytyjski dyplomata i pisarz Edgar Vincent uznał zwycięską Bitwę Warszawską za osiemnastą decydującą bitwę w dziejach świata. Jednak walka Polaków o wolność nie zakończyła się 1920 roku. Rosjanie traktowali nasze ziemie jako chwilowo utraconą strefę wpływów i już pod koniec 1921 roku przystąpili do tworzenia specjalnych grup dywersyjnych, których zadaniem było prowadzenie działalności agitacyjnej wśród ludności zamieszkującej wschodnie rubieże kraju oraz dokonywanie zamachów na posterunki graniczne[30].

Rosyjskie siły dywersyjne wykorzystywały zróżnicowanie etniczne ludności pogranicza, gdzie niewiele ponad połowę stanowili Polacy. Celem propagandy byli więc głównie Ukraińcy, Żydzi i Rosjanie. W ciągu czterech lat, od 1921 do 1924 roku, rosyjscy sabotażyści dokonali ponad 200 aktów dywersji na polskie placówki wojskowe i policyjne oraz napadów na polskie majątki ziemskie[31]. To wówczas po raz pierwszy użyto terminu *wojna hybrydowa* w odniesieniu do wojny toczonej bez wypowiedzenia, mającej na celu doprowadzenie do jak największej destrukcji w szeregach przeciwnika. Pozwalało to agresorowi na uniknięcie odpowiedzialności i stosowanie trojakich działań, tzn. walki bezpośredniej oraz propagandy na obszarze objętym wojną i na arenie międzynarodowej[32].

Analizując inne przykłady historyczne, nie sposób nie zauważyć, że do takich działań należy zaliczyć interwencję wojskową z października 1920 roku, zwaną buntem Żeligowskiego. Wykonawcą tej akcji były „zbuntowane" polskie oddziały, które pod dowództwem gen. Lucjana Żeligowskiego, po upozorowanej niesubordynacji wobec Naczelnego Wodza Józefa Piłsudskiego, zajęły Wilno i proklamowały powstanie Litwy Środkowej. Oficjalnie była to samowolna akcja, którą potępiły władze w Warszawie. Jednak za starannie zaplanowaną interwencją militarną stał Józef Piłsudski, który wiedział, że tylko w ten sposób Wileńszczyzna może zostać włączona w obszar Rzeczypospolitej. Zgodnie z opracowanym wcześniej planem gen. Lucjan Żeligowski stanął na czele liczącego 15 tys. zgrupowania wojsk. Główną siłą była 1 Dywizja złożona z żołnierzy pochodzących z Kresów Północno-Wschodnich, wzmocniona dwoma pułkami kawalerii oraz oddziałem ochotniczym mjr. Mariana Kościałkowskiego. Po opanowaniu Wilna wydano dekret proklamujący powstanie Litwy Środkowej oraz powołano Tymczasową Komisję Rządzącą. Na pierwszym posiedzeniu Sejmu Wileńskiego przyjęto uchwałę o przyłączeniu Litwy Środkowej do Polski[33].

Szczególnie trafne spojrzenie na zjawisko hybrydowości zaprezentował dr Leszek Sykulski[34], mianowicie odwołał się do jednego z prekursorów teorii wojen hybrydowych, jakim był rosyjski pułkownik Jewgienij Messner – „źródło" rosyjskiego ujęcia działań hybrydowych. *W latach sześćdziesiątych XX wieku, piszący na emigracji w Argentynie, rosyjski strateg, pułkownik Jewgienij Messner sformułował nową koncepcję prowadzenia konfliktów zbrojnych, którą nazwał wojnami buntowniczymi. Ten nowy typ wojny miał się charakteryzować przewagą prowadzenia walk przez ludność cywilną, kluczowym znaczeniem oddziaływania psychologicznego i decydującym znaczeniem użycia wojsk i służb specjalnych. Messner wskazywał także na rosnącą rolę terroru w prowadzeniu działań zbrojnych. Inną ważną cechą nowej koncepcji było „odpaństwowienie wojny". Walczące grupy społeczne, pododdziały wojskowe i paramilitarne pozbawione miały być oznak rozpoznawczych. O skuteczności koncepcji Messnera można się było przekonać na początku 2014 roku*

[28] M. Dura: *Wojna hybrydowa. Powtórka z historii.* http://www.defence24.pl/wojna-hybrydowa-powtorka-z-historii/. 6.03.2018.

[29] Ibidem.

[30] P. Łepkowski: *Pierwsza wojna hybrydowa.* http://www.rp.pl/Rzecz-o-historii/306169876-Pierwsza-wojna-hybrydowa.html/. 6.03.2018.

[31] Ibidem.

[32] Ibidem

[33] A. Dąbrowska, *Bunt Żeligowskiego, czyli jak Polacy zdobyli Wilno.* http://www.polska-zbrojna. pl/home/ articleshow/20718?t=-Bunt-Zeligowskiego-czyli-jak-Polacy-zdobyli-Wilno/. 30.05.2018.

[34] Leszek Sykulski – nauczyciel akademicki, doktor nauk o polityce, historyk. Pracował jako analityk ds. bezpieczeństwa międzynarodowego w Kancelarii Prezydenta RP w okresie prezydentury Lecha Kaczyńskiego.

podczas tzw. kryzysu krymskiego. Kluczową rolę odgrywało tam podłoże społeczne. Od wielu lat rosyjskie media prowadziły kampanię informacyjną, skierowaną do mniejszości rosyjskiej na półwyspie. Sama zaś operacja zbrojna została przeprowadzona modelowo[35].

Wielu analityków zaskoczył sposób działania Rosji na Krymie i na wschodniej Ukrainie. Twierdzili, że Rosjanie zastosowali nowatorskie metody działania pod parasolem tzw. wojny hybrydowej. Natomiast Rosja dowodzi, że ich taktyka prowadzenia operacji z 2014 roku była stosowana na świecie już od dawna, w tym również przez państwa zachodnie[36]. Nie tylko działania na Ukrainie, lecz również wydarzenia określane mianem Arabskiej Wiosny noszą znamiona koncepcji płk. J. Messnera, wzbogaconej o najnowsze osiągnięcia technologii informacyjnych. W ostatnich latach można również zaobserwować eskalację napięć etnicznych oraz wiele prób przewrotów, jak miało to miejsce w Hiszpanii czy Turcji. Biorąc to pod rozwagę, należy liczyć się z tym, że sytuacja w każdym kraju w Europie może ulec destabilizacji i może dojść do wewnętrznego konfliktu. Poważnym wyzwaniem stały się niekontrolowane oraz ciągle zalewające kontynent europejski fale emigrantów. Przyczyny są zróżnicowane i mają swoje źródło głównie w problemach ekonomicznych i gospodarczych. Są to również migracje z rejonów objętych konfliktami zbrojnymi.

Doświadczenia historyczne wskazują, że należy się zastanowić również nad potencjalnym zagrożeniem ze strony zachodniego sąsiada, czyli RFN. Od niepamiętnych czasów byliśmy obiektem najazdów, wojen, agresji czy pretensji terytorialnych państwa zza Odry. Kiedy uzyskaliśmy pełną suwerenność, RFN stała się jednym z największych naszych sprzymierzeńców popierającym naszą akcesję do Unii Europejskiej oraz NATO. W błyskawicznym tempie podpisano traktat uznający granicę na Odrze i Nysie Łużyckiej oraz traktat o przyjaznej współpracy i dobrym sąsiedztwie. Jednak nie mamy pewności, czy ten stan będzie trwał wiecznie. Historia uczy, że pokój nie jest dany raz na zawsze, zatem wszelkie możliwości należy brać pod uwagę, by być w gotowości do przeciwdziałania ewentualnym zagrożeniom zgodnie ze starym przysłowiem *przyjaciela trzymam blisko siebie, ale wroga jeszcze bliżej*. Należy realnie spojrzeć na zagrożenia, takie jak na przykład realizacja niemiecko-rosyjskiego projektu gazociągu Nord Stream II. Pomijanie członków Unii Europejskiej w podejmowaniu decyzji odnośnie do takich inwestycji może mieć niekorzystny wpływ na nasze bezpieczeństwo w kontekście rozluźnienia więzi łączących państwa wspólnoty[37]. Warto również zwrócić uwagę na fakt, że ponowna współpraca RFN i Rosji może w istotny sposób wpłynąć na osłabienie ekonomiczne naszego kraju. Obecnie Niemcy nie stanowią zagrożenia dla Polski, dopóki istnieje NATO oraz ze względu na wspólne członkostwo w UE. Jednak nie można wykluczyć w przyszłości konfliktu wewnątrz UE, prowadzącego nawet do jej rozpadu[38]. Należy zatem zdawać sobie sprawę, że aby skutecznie przeciwdziałać możliwym zagrożeniom, gotowość do reakcji musi być natychmiastowa w każdym miejscu kraju i w jak najkrótszym czasie. Dlatego też posiadanie właściwie zorganizowanego systemu bezpieczeństwa narodowego powinno być nieodzownym elementem ochrony i obrony każdego nowoczesnego kraju.

BYĆ ELASTYCZNYM

Odnosząc się do powyższych konstatacji, trzeba mieć świadomość, że wojska operacyjne nie są w stanie skutecznie odpowiedzieć na działania hybrydowe. Ponadto, by przeciwdziałać hybrydowemu zagrożeniu, twarda i energiczna reakcja jest często niewystarczająca. Przeważająca siła nie jest już adekwatnym środkiem odstraszania potencjalnego przeciwnika.

Aby skutecznie przeciwstawić się hybrydowym działaniom, należy swoje własne dostosować do charakteru walki prowadzonej przez przeciwnika. Wyjść poza sztywne ramy ograniczeń w postaci często już nieaktualnych regulaminów i instrukcji, *wojować tak, by ponosząc samemu jak najmniejsze straty, zadawać jednocześnie przeciwnikowi jak największe*[39]. Wielu wojskowych nie ma wystarczającej elastyczności działania i nieszablonowego myślenia, by zmieniać na bieżąco priorytety i cele adekwatnie do zagrożenia i sposobu prowadzenia walki przez przeciwnika. Należy być zarazem lwem i lisem. Skutecznie odstraszać przeciwnika swoją siłą i odwagą, gdy będzie próbował konfrontacji. Równocześnie być przebiegłym, używając wyrafinowanego podstępu czy fortelu. Stosować takie same metody działania jak adwersarz, i wyprzedzać go o krok w budowanej na podstępie intrydze. Pojawiać się i znikać, skrycie podchodzić przeciwnika w hybrydowej mgle wojny, zyskując jego zaufanie, by ostatecznie go pokonać. ■

[35] L. Sykulski: *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera*. „Przegląd Geopolityczny" 2015, t. 11, s. 103.

[36] M. Dura: *Wojna hybrydowa...,* op.cit.

[37] M. Merczyńska: *Bezpieczeństwo narodowe państwa polskiego. Uwarunkowania i zagrożenia.* http://dlibra.bg.ajd.czest.pl:8080/Content/968/ResPoliticae4-59.pdf, s. 67–68/. 19.04.2018.

[38] Ibidem.

[39] F. Skibiński: *Rozważania o sztuce wojennej.* Warszawa 1972, s. 59.

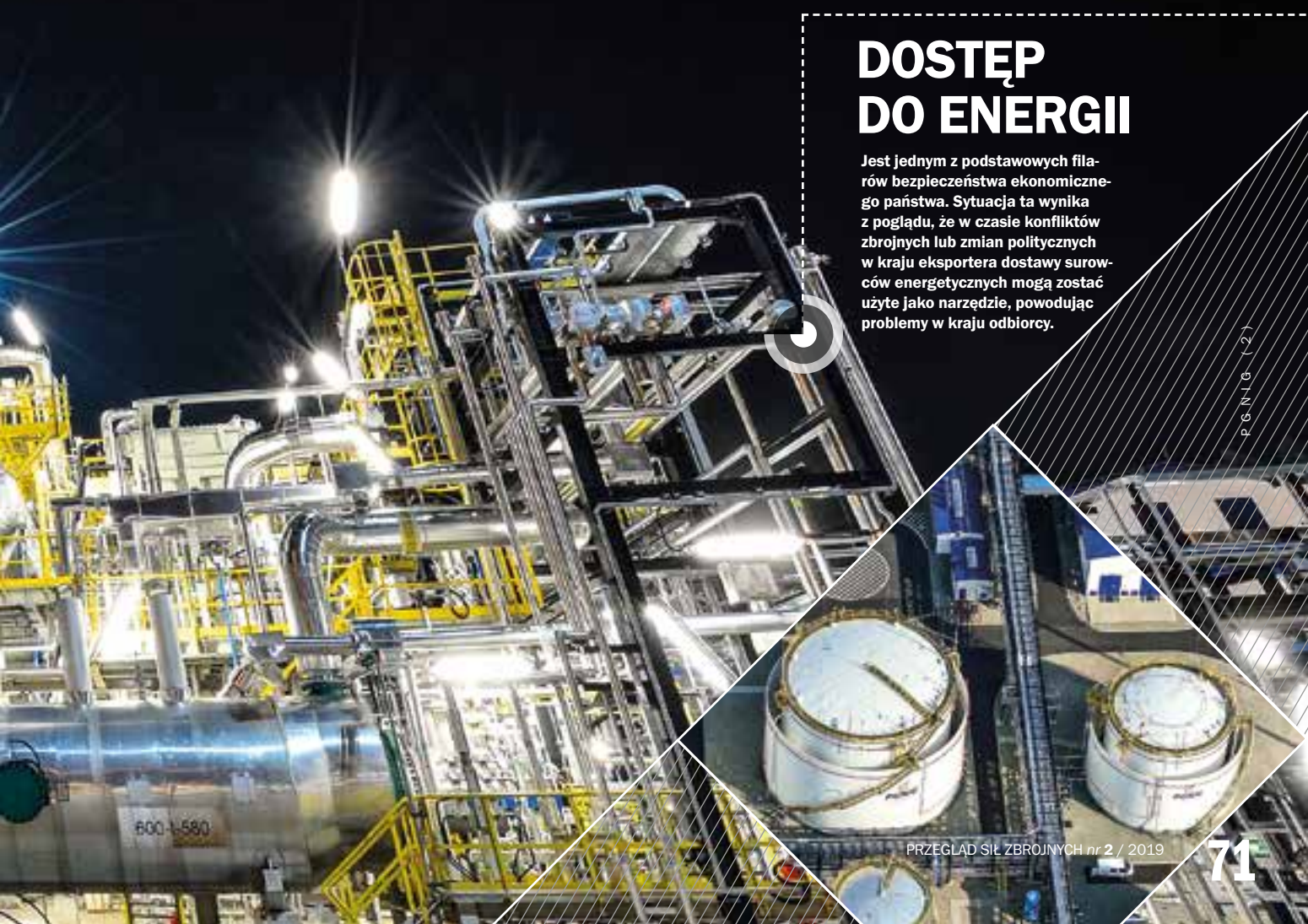
Zagrożenia bezpieczeństwa pozamilitarnego

WSPÓŁCZEŚNIE NIE MOŻNA ODDZIELAĆ OBOWIĄZKÓW PAŃSTWA ZWIĄZANYCH Z OBRONĄ TERYTORIUM OD JEGO OBOWIĄZKÓW DBANIA O JAKOŚĆ ŻYCIA OBYWATELI I FUNKCJONOWANIA PODMIOTÓW GOSPODARCZYCH DZIAŁAJĄCYCH NA JEGO TERENIE I NA PODSTAWIE JEGO PRAWA.

mjr dypl. SZRP Mariusz Wojtczyk

Dzisiejsze rozumienie *bezpieczeństwa* wymaga spojrzenia na jego istotę przez pryzmat uniwersalności tego pojęcia. Termin ten obejmuje wszystkie dziedziny życia, w których występuje zagrożenie, i może być rozpatrywany w wymiarze jednostkowym, grupowym, narodowym, regionalnym, a także międzynarodowym. Ponadto zachodzące zmiany w procesach społecznych, ekonomicznych, kulturowych, technologicznych czy informatycznych kreują kolejne zagrożenia, wpływające zarówno na bezpieczeństwo wewnętrzne, jak i zewnętrzne, czy też na jedno i drugie. Można zatem przyjąć, iż przeobrażenia wynikające z nieustannej ewolucji naukowej człowieka sprawiają, że przyszły świat, a w nim wymiar środowiska bezpieczeństwa, będzie nie tylko różny od dzisiejszego, lecz także od obecnie prognozowanego. Będzie to zatem prawdopodobnie inna rzeczywistość, z różnymi problemami, zupełnie inaczej rozwiązująca problemy współczesnego i realnego świata. Założyć więc można, że przyszłe środowisko bezpieczeństwa w wyniku nadchodzących przeobrażeń jeszcze bardziej może być przepełnione przez *szybsze i dynamiczniejsze zmiany charakteryzujące się m.in. rosnącą złożonością*

Autor jest starszym oficerem Wydziału G3 w Sztabie Wielonarodowej Dywizji Północny Wschód.



DOSTĘP DO ENERGII

Jest jednym z podstawowych filarów bezpieczeństwa ekonomicznego państwa. Sytuacja ta wynika z poglądu, że w czasie konfliktów zbrojnych lub zmian politycznych w kraju eksportera dostawy surowców energetycznych mogą zostać użyte jako narzędzie, powodując problemy w kraju odbiorcy.

i turbulencyjnością, niejasnością i dwuznacznością, a także nieprzewidywalnością następstw, zachowań oraz wciąż rosnącą asymetrią i towarzyszącym jej silnym emocjom[1].

EWOLUCJA POJĘCIA BEZPIECZEŃSTWA

Potrzeba ochrony życia i wolności powodowała, że na bezpieczeństwo stopniowo zaczęto patrzeć przez pryzmat państwa, prawa i sprawnej policji jako trzech filarów ułatwiających zapewnienie bezpieczeństwa. Podstawą takiego myślenia stały się przede wszystkim dzieła Platona (427–347 p.n.e.) i Arystotelesa (384–322 p.n.e.). Choć żaden z nich bezpośrednio nie łączył wprost istnienia państwa z poczuciem bezpieczeństwa, to można w ich pracach te związki znaleźć. Przełomową rolę w określaniu celów funkcjonowania państwa odegrał N. Machiavelli (1469–1527), który wprost uznał, iż: *zbyt małe bezpieczeństwo, jakiego doświadczają ludzie żyjący w rozproszeniu, niemożność samotnego stawiania oporu – bądź z powodu swego położenia, bądź z powodu znikomej liczebności – atakom nadciągającego wroga, trudność z zejściem się na czas przed jego przybyciem, konieczność opuszczenia wtedy kryjówek, które stają się łupem napastników: oto powody dla których pierwsi mieszkańcy danego kraju budują miasta, chcąc uniknąć tych niebezpieczeństw*[2].

W ujęciu etymologicznym termin *bezpieczeństwo* powstał z połączenia dwóch wyrazów: *bez* oraz *pieczy*. *Piecza* to tyle, co otaczanie troską i opieką, z przedrostkiem *bez* zaś oznacza sytuację, w której taka ochrona nie jest potrzebna, wolną od zagrożeń. W okresie zimnej wojny analizy z zakresu bezpieczeństwa odnosiły się do struktur narodowych, które przede wszystkim gwarantowały rozbudowane potencjały militarne, będące w stanie odeprzeć ówczesne zagrożenia. Okres ten był kojarzony z wyścigiem zbrojeń, brakiem demokracji i ciągłym przeciwstawianiem się agresji militarnej. Dziś uważa się, że takie podejście było etnocentryczne i zbyt podporządkowane wybranym czynnikom (głównie kulturowym) i nie uwzględniało wielu aspektów.

Szersze pojęcie bezpieczeństwa upowszechniło się w latach osiemdziesiątych ubiegłego wieku i uwzględniało różne komponenty, a nie tylko zagrożenia militarne[3]. Większego znaczenia zaczynają nabierać czynniki towarzyszące, wspomagające i uzupełniające działania zbrojne. Poszerzanie się zakresu bezpieczeństwa spowodowało wyodrębnienie się wielu płaszczyzn, które mogą być analizowane w sposób niezależny od siebie, mimo że są ze sobą powiązane. Powszechnie obowiązuje teza, że nie ma raz na zawsze ustanowionego bezpieczeństwa. Jest to proces, który zmienia się w zależności od różnych zjawisk występujących w społeczeństwie.

ŚRODOWISKO BEZPIECZEŃSTWA PAŃSTWA

Definiowane jest *jako zespół zewnętrznych oraz wewnętrznych czynników, które warunkują realizację interesów w obszarze bezpieczeństwa*[4]. Interesy danego podmiotu (państwa, narodu, grupy, osoby itp.) to zsyntetyzowane oczekiwania podmiotu wobec otoczenia wynikające i kształtowane przez jego tożsamość, wyznawane wartości, historyczny dorobek, tradycje, bieżące potrzeby oraz dążenia i aspiracje przyszłościowe. Scharakteryzowane mogą być one najpełniej za pomocą czterech podstawowych kategorii, jakimi są: szanse, wyzwania, ryzyka i zagrożenia[5].

Szanse to niezależne od woli podmiotu procesy i zjawiska, które sprzyjają realizacji jego interesów oraz osiąganiu celów. Przykładem dobrze wykorzystanej strategicznej szansy, jaka pojawiła się w latach dziewięćdziesiątych ubiegłego wieku, było wstąpienie naszego kraju do NATO. *Wyzwania* są utożsamiane z dylematami, przed jakimi stoi podmiot w rozstrzyganiu spraw bezpieczeństwa. Często stawiane są przez sojuszników, którzy prezentują pewne oczekiwania i windują standardy obowiązujące w sojuszach lub koalicjach. *Ryzyka* to możliwości negatywnych skutków własnego działania w sferze bezpieczeństwa rozpatrywane dla danego podmiotu. Przykładem mogą być potencjalnie negatywne konsekwencje naszego szerokiego zaangażowania w międzynarodowe operacje wojskowe lub też niebezpieczeństwa związane z lokalizacją na terytorium naszego kraju amerykańskiej bazy przeciwrakietowej. *Zagrożenia* natomiast to bezpośrednie lub pośrednie destrukcyjne oddziaływania na podmiot. Zasadniczo można stwierdzić, że liczba czynników generujących zagrożenia wraz z rozwojem cywilizacyjnym stale wzrasta, mimo stosowania coraz doskonalszych systemów zabezpieczeń. Optymistyczne jest to, że w miarę, jak pojawiają się nowe rodzaje zagrożenia, ludzkość potrafi się im przeciwstawiać, tworząc nowe lub doskonaląc stare sposoby, metody i organizacje zabezpieczania się przed nimi.

Stosownie do omawianych aspektów dotyczących zagrożeń bezpieczeństwa państwa literatura wyróżnia różne podziały typologiczne. Do głównych kryteriów według Z. Ciekanowskiego, J. Nowickiej oraz H. Wyrębka, stosowanych do klasyfikacji zagrożeń, zalicza się: kryterium przedmiotowe, źródła zagrożeń, środowiska zagrożeń, zasięg zagrożeń, ich skalę, skutki, miejsca powstania, dynamikę rozwoju i charakter stosunków społecznych[6] – rys. 1.

[1] R. Kwećka, J. Gryz, M. Kozub, A. Brzozowski: *Strategia podmiotów. Determinanty zmian.* Toruń 2011, s. 36.

[2] Ibidem, s. 28–29.

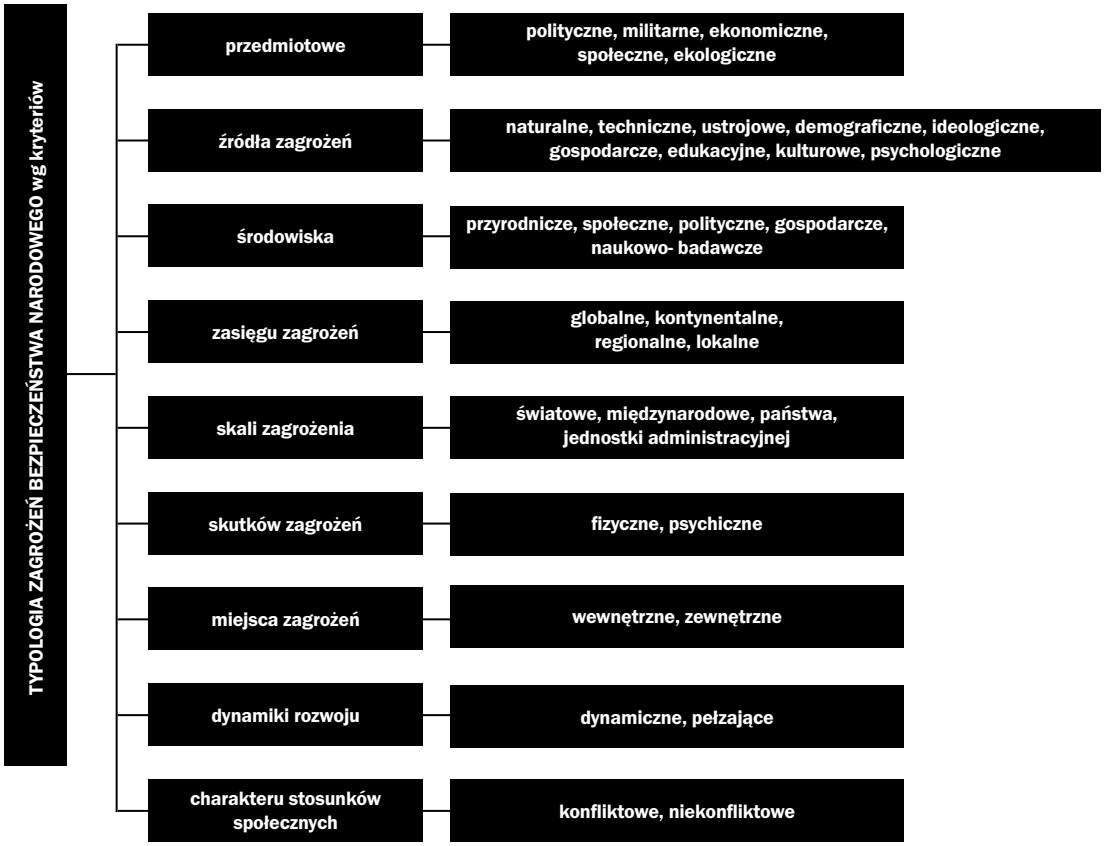
[3] *Pojęcie bezpieczeństwa i jego ewolucja.* Red.: K. Żukrowska, M. Grącik. Warszawa 2006, s. 21–22.

[4] *Współczesne uwarunkowania bezpieczeństwa Polski.* Red.: W. Kustra, J. Truchan, K. Pobuta. Jarosław 2014, s. 14.

[5] S. Koziej: *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*. https://www.bbn.gov.pl/. 29.12.2017.

[6] Ibidem, s. 99.

RYS. 1. TYPOLOGIA ZAGROŻEŃ BEZPIECZEŃSTWA W ZALEŻNOŚCI OD PRZYJĘTEGO KRYTERIUM



Opracowanie własne na podstawie http://yadda.icm.edu.pl/baztech/element/bwmeta1,element baztech- article-BGPK 2860-1288.29.12.2017.

Wnioski odnoszące się do współczesnych uwarunkowań stanowiących zagrożenie dla naszego kraju zostały przedstawione w *Strategicznym przeglądzie obronnym 2016*. Jest on potwierdzeniem postrzegania bezpieczeństwa w nowym wymiarze. Bezpieczeństwo polityczno-militarne wprawdzie nadal pozostaje na pierwszym miejscu, lecz nie jest jedyne. Zwiększa się wpływ czynników pozawojskowych, w tym ekonomicznych, społecznych i ekologicznych, których prawdopodobieństwo zaistnienia wydaje się być większe niż zagrożeń militarnych. Współczesne zagrożenia godzące w bezpieczeństwo wymuszają prowadzenie intensywnych badań źródeł ich powstawania, poszukiwania skutecznych form i metod ich wykrywania, monitorowania oraz likwidowania skutków ich wystąpienia. W dzisiejszym środowisku bezpieczeństwa pozamilitarnego coraz większego znaczenia nabierają zagrożenia związane z aktami terroryzmu, naciskami w zakresie bezpieczeństwa energetycznego i ekologicznego, w sferze gospodarczej i finansowej (na poziomie makroekonomicznym) oraz zagrożenia wynikające z klęsk żywiołowych i przestępczego wykorzystywania cyberprzestrzeni. Wymuszają one dodatkowo konieczność upowszechniania wiedzy o bezpieczeństwie.

TERRORYZM

Poziom zagrożeń wynikających z rozpowszechniania islamskiego terroryzmu od kilku lat systematycznie wzrasta. Nie jest to zjawisko nowe, jednak staje się coraz bardziej powszechne i stanowi coraz większe zagrożenie dla bezpieczeństwa międzynarodowego[7]. Wydarzenia z 11 września 2001 roku pokazały, że nikt w Stanach Zjednoczonych i na całym świecie nie może czuć się bezpiecznie. Dla terrorystów nasz kraj jest celem zastępczym, rezerwowym i jak dotąd nie był obiektem ich ataku. Jeszcze do niedawna jako dość jednolity etnicznie i narodowościowo był uważany za teren, gdzie trudniej jest zaplanować i dokonać skutecznego ataku. Jednak biorąc pod uwagę ogólny wzrost znaczenia zjawiska *home grown terrorism*, argument ten wydaje się dezaktualizować.

[7] M. Adamczuk: *Rodzimy terroryzm jako zjawisko zagrażające bezpieczeństwu w Europie, pozamilitarne aspekty bezpieczeństwa.* http://studylibpl.com/doc/1214185/rodzimy-terroryzm-jako-zjawisko-zagra%C5%BCaj%C4%85ce-bezpiecze%C5%84stwu-w/.18.03.2018.

Dokładna liczebność mniejszości islamskiej w kraju nie jest znana z powodu braku oficjalnych statystyk, jednak liczbę muzułmanów szacuje się – w zależności od ogólnodostępnych źródeł – na 15 000 do nawet 60 000[8]. Także sąsiedztwo RFN, gdzie liczba islamistów wzrasta z roku na rok, stanowi potencjalne źródło kontaktów z radykalną ideologią muzułmańską. Popularne są wyjazdy obywateli Niemiec na szkolenia terrorystyczne do krajów islamskich. Służby niemieckie oceniają, iż obecnie na pograniczu pakistańsko-afgańskim szkoli się około 300 ochotników, którzy po powrocie będą gotowi do przeprowadzenia zamachów w Europie, a na terytorium RFN znajduje się ponad tysiąc niebezpiecznych islamskich ekstremistów[9].

Wzmożenie kontroli środowisk związanych z fundamentalistami islamskimi może powodować, że staniemy się dla terrorystów swojego rodzaju zapleczem logistycznym. Obecnie sprzyjającą sytuacją do przeprowadzania aktów terroryzmu na obszarze Europy jest stały napływ nielegalnych imigrantów, w szczególności z Bliskiego Wschodu i Afryki Północnej, pośród których mogą znajdować się bojownicy-terroryści[10]. Jednak nie oznacza to wykluczenia możliwości przebywania zamachowców związanych ze środowiskiem terrorystycznym na terenie naszego kraju. Przykładem jest zatrzymany w Rybniku 5 września 2016 roku Marokańczyk Mourad T. Zebrane materiały dowodowe w trwającym wówczas śledztwie wskazywały, że miał on bezpośrednie powiązania z tzw. Państwem Islamskim. Według Witolda Gadowskiego[11] jedna z jego sekcji bojowników skupia się na rozpracowywaniu topografii naszego kraju. Dziennikarz powołuje się na źródła m.in. zbierane przez żydowskie organizacje monitorujące skupiska Arabów zbliżone do Mossadu. Nie precyzuje jednak, skąd konkretnie czerpie swoją wiedzę.

CYBERTERRORYZM

Termin ten jest neologizmem, który obrazuje prowadzenie aktów terroru tam, gdzie są wykorzystywane nowości technologii informacyjnej, których celem jest wyrządzenie szkody na tle politycznym lub ideologicznym, zwłaszcza w odniesieniu do infrastruktury o bardzo dużym znaczeniu dla gospodarki lub obronności atakowanego państwa[12]. Pod tym pojęciem należy rozumieć *akcje, mające na celu zakłócenie działania, uszkodzenie lub zniszczenie oprogramowania, komputerów lub sieci informacyjnych jakiegoś państwa bądź organizacji, dokonane przez aktorów niepaństwowych, w odpowiedzi na podobny atak przeprowadzony przez innych aktorów niepaństwowych*[13]. Wojny internetowe są przeniesieniem realnego konfliktu lub napięcia do cyberprzestrzeni, gdzie dochodzi do wirtualnego starcia. Udział w nich biorą mniej lub bardziej zorganizowane grupy hakerów. W praktyce przedmiotem ich zainteresowania są: oprogramowanie, sieci komputerowe rządu, organizacje użyteczności publicznej, wojska oraz firmy, dlatego też działania takie mogą istotnie przyczynić się do obniżenia poziomu bezpieczeństwa narodowego.

Przykładem aktów cyberterroryzmu są cyberataki na Estonię i Gruzję. Do ataków na pierwsze z wymienionych państw doszło w kwietniu 2007 roku. Unieruchomiły one strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, banków, a nawet szkół. Ataki w Estonii są utożsamiane z pierwszymi w historii zmasowanymi cyberatakami przeciw suwerennemu państwu[14]. W obliczu powszechnej obecności w cyberprzestrzeni rządowych instytucji, korporacji międzynarodowych czy rynków finansowych umiejętnie przeprowadzony atak może doprowadzić do katastrof na niewyobrażalną skalę. Wystarczy wyobrazić sobie na przykład włamanie hakera z organizacji terrorystycznej do systemu lotnictwa cywilnego w dowolnym kraju i doprowadzenie do wielu katastrof lotniczych przez zmianę parametrów lotów czy też działanie na rzecz destabilizacji rynków finansowych przez uderzenie w giełdę papierów wartościowych w Tokio czy Nowym Jorku. Wszystkie wymienione zjawiska z uwagi na proces globalizacji i zakres powiązań gospodarczych mogą bezpośrednio lub pośrednio wpłynąć na kondycję naszego państwa i stanowić zagrożenie bezpieczeństwa. Można stwierdzić, że w zasadzie wszystkie rodzaje niebezpieczeństw istniejących w tradycyjnej, fizycznej geoprzestrzeni będą mieć swoje odpowiedniki w cyberprzestrzeni. Takie kategorie, jak: cyberagresja, cyberodstraszanie, cyberwojna już czekają na swoje szerokie opracowanie teoretyczne oraz praktyczne ich uwzględnianie w strategiach bezpieczeństwa poszczególnych państw.

BEZPIECZEŃSTWO ENERGETYCZNE

Jest jednym z podstawowych filarów bezpieczeństwa ekonomicznego państwa. Sytuacja ta wynika z poglądu, że w czasie konfliktów zbrojnych lub w wyniku zmian politycznych w kraju eksportera dostawy surowców energetycznych mogą zostać użyte jako narzędzie, powodując problemy w kraju odbiorcy. Państwo musi więc zapewnić swobodny dostęp do energii oraz dążyć do uzyskania zróżnicowanych źródeł zaopatrzenia w surowce energetyczne. Obecny

[8] Ibidem.

[9] Ibidem.

[10] Ibidem.

[11] Witold Gadowski – ur. w 1964 r. w Zakopanem, polski dziennikarz, publicysta, pisarz i poeta.

[12] *Determinanty bezpieczeństwa człowieka a rozwój regionalny.* Red.: T. Bąk, Z. Ciekanowski, L. Szot Jarosław 2013, s. 47–49.

[13] R. Chrobak: *Zagrożenia bezpieczeństwa państwa*. „Zeszyty Naukowe AON" 2013 nr 4, s. 256.

[14] L. Bełza: *Główne zagrożenia w obecnym i przyszłym środowisku bezpieczeństwa pozamilitarnego*. https://www.bbn.gov.pl/.16.03.2018.

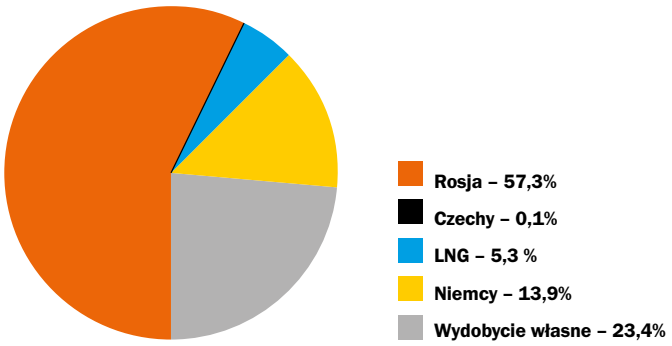
stan bezpieczeństwa w poszczególnych sektorach naszej energetyki jest mocno zróżnicowany. W elektroenergetyce oraz ciepłownictwie, które są oparte na zasobach węgla kamiennego i brunatnego, Polska jest samowystarczalna, gdyż bilans energetyczny w tym przypadku jest korzystny[15]. O ile w sektorze wytwarzania energii elektrycznej sytuacja jest lepsza niż w wielu krajach UE, o tyle sektor gazu ziemnego cechuje duże uzależnienie od dostaw z jednego kierunku i od jednego dostawcy (rys. 2). Gaz odgrywa istotną rolę w polskiej gospodarce energetycznej, będąc ważnym źródłem energii dla przedsiębiorstw oraz gospodarstw domowych. Niestety, nie jesteśmy w stanie we własnym zakresie wydobywać wystarczającej ilości gazu ziemnego, aby zapewnić jego regularne dostawy do wszystkich użytkowników w dłuższym okresie. Z tego też powodu konieczne jest pozyskiwanie tego surowca z innych krajów. Podpisany w 1996 roku i obowiązujący do 2022 kontrakt na dostawy gazu z Rosji powoduje, że nasz wschodni sąsiad jest jego największym dostawcą.

W najbliższych latach najpoważniejsze zagrożenia w obszarze bezpieczeństwa energetycznego będą związane m.in. z nasileniem się procesu uzależnienia bezpieczeństwa dostaw od stanu relacji z producentami i eksporterami nośników energii (Rosja) oraz państwami tranzytowymi (Ukraina, Białoruś), a także z groźbą destabilizacji w nich. Dotychczasowa stabilność dostaw i korzystna cena surowców energetycznych z kierunku wschodniego wiązała się z dogodnym usytuowaniem geograficznym. Jednak w związku z dynamicznymi procesami zachodzącymi w rosyjskim sektorze paliwowo-energetycznym przed Polską pojawiają się wyzwania dwojakiego rodzaju.

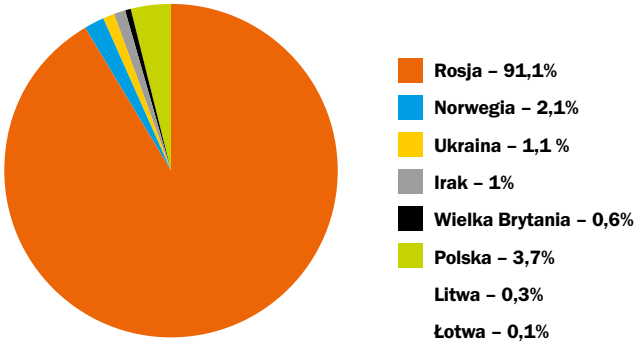
Po pierwsze, chodzi o zwiększenie odporności krajowego systemu energetycznego na potencjalne zakłócenia bądź ograniczenia dostaw paliw kopalnych z Rosji. Po drugie, konieczne jest zbudowanie konkurencyjnego rynku energii (przede wszystkim gazu), który ograniczyłby możliwości wykorzystywania pozycji monopolistycznej najbliższych sąsiadów[16]. W sektorze gazu ziemnego temu celowi posłużyły m.in. budowa w Świnoujściu terminalu morskiego do odbioru gazu skroplonego (LNG) oraz podziemnych magazynów. Podobnie jest z dostawami do naszego kraju ropy naftowej (rys. 3). Dostarczana do Polski ropociągiem „Przyjaźń" ropa naftowa u swego źródła i celu jest kontrolowana przez Rosję. Od niedawna bowiem na obu końcach tej rury mamy już Rosjan, którzy kupili rafinerię w niemieckim Schwedt. Ponadto współpraca niemiecko-rosyjska w dziedzinie energetyki, mimo unijnych sankcji, zbytnio nie ucierpiała[17]. Aby zagrożenie to zminimalizować, ma powstać projekt budowy rurociągu naftowego Odessa-Brody-Płock-Gdańsk, którym miałaby popłynąć kaspijska, a być może i irańska ropa, która w wyniku zawartego ostatnio przełomowego porozumienia Teheranu z Zachodem może stanowić dodatkowe uzasadnienie ekonomiczne i polityczne dla tego projektu[18]. Ukończenie wspomnianego rurociągu wydatnie wzmocni bezpieczeństwo energetyczne i strategiczne nie tylko naszego kraju, lecz także Ukrainy, Gruzji, a opcjonalnie nawet Białorusi i państw bałtyckich.

Na podstawie prowadzonej w ostatnich latach działalności w sektorze energetyki można stwierdzić, iż jej priorytetowym celem jest osiągnięcie odpowiedniego poziomu dywersyfikacji dostaw, gwarantującego bezpieczeństwo energetyczne oraz zrównoważenie bilansu

RYS. 2. ŹRÓDŁA ZAOPATRZENIA POLSKI W GAZ W 2016 ROKU



RYS. 3. ŹRÓDŁA ZAOPATRZENIA POLSKI W ROPĘ NAFTOWĄ W 2016 ROKU



Opracowanie własne (2).

[15] http://www.nowastrategia.org.pl/wybrane-uwarunkowania-bezpieczenstwa-energetycznego-polski/.19.03.2018.

[16] M. Merczyńska: *Bezpieczeństwo państwa polskiego. Uwarunkowania i zagrożenia*. Zeszyty naukowe Akademii im. J. Długosza w Częstochowie. „Bezpieczeństwo Narodowe" 2012 nr III–IV, s. 61–62.

[17] http://biznesalert.pl/wojciechowski-polska-musi-wzmacniac-podmiotowosc-na-szlaku-tranzytowym surowcow-energetycznych/.19.03.2018.

[18] Ibidem.

energetycznego. Rozszerzenie możliwości pozyskiwania gazu ziemnego oraz ropy naftowej przełoży się na stabilne podstawy rozwoju kraju, a tym samym na jego bezpieczeństwo wewnętrzne.

BEZPIECZEŃSTWO EKOLOGICZNE

Zadania państwa w tej dziedzinie powinny się koncentrować na profilaktyce oraz kompleksowej polityce poprawy jakości środowiska. Problemy ekologiczne stwarzają istotne zagrożenie dla zdrowia i dobrostanu człowieka. Środowisko życia stanowi jeden z podstawowych czynników wpływających na zdrowie ludzi. Relacje między czynnikami środowiskowymi a zdrowiem są bardzo złożone. Skutki zdrowotne narażenia na negatywne czynniki pochodzenia środowiskowego są różnorodne i objawiają się w postaci przejściowych lub trwałych zaburzeń funkcjonalnych. Degradacja środowiska przez m.in. zanieczyszczenie powietrza, wody czy utratę obszarów cennych przyrodniczo, w połączeniu ze zmianą stylu życia, może się przyczynić do wzrostu występowania wielu chorób cywilizacyjnych, takich jak: otyłość, choroby serca, cukrzyca, nowotwory, a także choroby i deregulacje układu odpornościowego. Może to również mieć wpływ na problemy związane z rozmnażaniem oraz na zdrowie psychiczne. Istotną kwestią może być także wzrost częstości występowania u dzieci astmy i różnego typu alergii[19]. W raporcie o stanie środowiska w Polsce z 2014 roku[20] przedstawiono wyniki badań dotyczące poruszanego problemu. Ranking obejmował 141 państw świata. Zwyciężyła w nim Finlandia, za nią uplasowała się Islandia, następnie Norwegia. Nasz kraj zajął w nim 48. miejsce. W wielu branych pod uwagę kategoriach zajmowaliśmy miejsca na szarym końcu. Ostateczną pozycję podbudowały dwie kategorie, mianowicie: zdrowie i mała umieralność niemowląt oraz czystość wód, w których zajęliśmy odpowiednio 17. i 35. miejsce[21].

Prowadzone badania przez różnego rodzaju specjalistów dotyczące stanu polskiego środowiska potwierdzają, iż dewastacja pewnych podsystemów ekologicznych lub wprowadzanie w nich zmian może bezpośrednio się przekładać na występowanie anomalii pogodowych, których następstwem są różnego rodzaju katastrofy naturalne.

ZAGROŻENIA NATURALNE

To sytuacja związana z działaniem sił natury, w czasie której jest przewidywane lub występuje niebezpieczeństwo powodujące straty ekonomiczne i pozaekonomiczne, w tym utrata zdrowia, życia, mienia ludności, a także szkody w ekosystemach i infrastrukturze. Zjawisko takie może mieć charakter katastrofy lub klęski żywiołowej. Nasz kraj, ze względu na położenie geograficzne, nie należy do obszarów objętych dużym prawdopodobieństwem występowania zagrożeń naturalnych. Specjaliści nie odnotowują tu podwyższonego ryzyka silnych trzęsień ziemi. Także umiarkowany klimat nie budzi obaw co do zachwiania układu sił panujących w przyrodzie. Długie okresy upałów są z reguły przeplatane opadami, a silne mrozy nie utrzymują się dłużej niż kilka dni. Daje to obraz mieszkańców kraju jako ludzi przyzwyczajonych do komfortu pogodowego, zwykle niemyślących o możliwości doświadczenia anomalii pogodowych. Niestety, wydarzenia pokazują, że kataklizmy i klęski żywiołowe zdarzają się również w pozornie bezpiecznym klimacie umiarkowanym. Najbardziej dotkliwymi w skutkach zagrożeniami naturalnymi są zjawiska hydrologiczne, do których zalicza się powodzie i długotrwałe susze, oraz atmosferyczne, zwłaszcza silne wiatry w postaci trąb powietrznych. Zdarzają się także osuwiska ziemi. W ostatnich latach zjawiska powodziowe występują coraz częściej i mają gwałtowniejszy przebieg, co według niektórych naukowców jest następstwem działalności człowieka. Po pierwsze, dynamiczne zmiany sposobów wykorzystania ziemi, w tym wzrost ilości zabudowy, oddziałuje na spływ powierzchniowy. Niekorzystny wpływ na stosunki wodne mają również nieprawidłowo prowadzone zabiegi melioracyjne. Przez osuszanie znacznej powierzchni bagien i torfowisk, które odgrywają rolę swego rodzaju magazynów zatrzymujących wodę, zdolność retencyjna wielu dorzeczy diametralnie się zmniejszyła. Przykładem nieracjonalnej działalności człowieka jest również przesadna regulacja koryt rzecznych i budowa wałów przeciwpowodziowych w zbyt małej odległości od koryt rzek celem zagospodarowania jak największej części doliny.

Zjawiskiem odmiennym od powodzi są susze, wywołane niewielką, sumaryczną ilością opadów atmosferycznych w półroczu letnim oraz intensywnym parowaniem. W sensie hydrologicznym *susze są definiowane jako okres ekstremalnie niskich stanów wody w korycie rzeki spowodowany ograniczonym jej zasilaniem wynikającym z wyczerpywania się zasobów wodnych zlewni*[22]. Trudno jest określić jej zasięg terytorialny oraz ramy czasowe, nawiązujące ściśle do początku i końca suszy. Wystąpienie suszy na obszarze kraju ma miejsce raz na cztery do siedmiu lat, przy czym od połowy XX wieku obserwuje się dużą regularność w pojawieniu się tego zjawiska. W obliczu prawdopodobnych globalnych zmian klimatycznych w niedalekiej przyszłości może wzrosnąć ryzyko wystąpienia suszy w okresie wiosennym, szczególnie groźnej ze względu na bardzo duże zapotrzebowanie wody w początkowej

[19] *Stan środowiska w Polsce*. Główny Inspektorat Ochrony Środowiska. Warszawa 2014, s. 73.

[20] Zgodnie z art. 25 b *Ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska*. DzU 2013 poz. 686, z późn. zm. Główny inspektor ochrony środowiska opracowuje, nie rzadziej niż raz na cztery lata, raport o stanie środowiska w Polsce.

[21] *Stan środowiska*..., op.cit., s. 4–8.

[22] Ibidem.

fazie procesu wegetacji roślin[23]. Według klimatologów za 10–20 lat skończy się klimat wilgotny. Prawdopodobny jest wzrost średniej rocznej temperatury przy jednoczesnym spadku sumy opadów atmosferycznych. Wówczas regionalne susze będą zjawiskiem coraz częstszym i bardziej dotkliwym.

Kolejnym kataklizmem naturalnym, nawiedzającym coraz częściej terytorium naszego kraju, są gwałtowne wichury. Zerwane dachy i linie energetyczne, zniszczone samochody czy połamane drzewa to tylko niektóre ze skutków niszczycielskich huraganów. Od 2004 roku w Polsce zanotowano ponad 11 orkanów. Jednym z najgroźniejszych był orkan Ksawery, który nadciągnął w grudniu 2013 roku. W jego wyniku śmierć poniosło pięć osób. Ogłoszono wówczas najwyższy stopień zagrożenia huraganem, a w mediach nadawano komunikaty, aby kto może, pozostał w domu[24]. Potężne nawałnice, w sierpniu 2017 roku, doprowadziły do największego kataklizmu w historii lasów państwowych. Jego rezultatem jest 9,8 mln m^3 powalonych i połamanych drzew, 79,7 tys. ha uszkodzonych lasów, w tym 39,2 tys. ha do całkowitego odnowienia. Łączny obszar zniszczeń jest półtora raza większy od powierzchni Warszawy. Niszczycielska siła huraganu przyczyniła się także do odnotowania dwóch przypadków ofiar śmiertelnych[25].

Natura jest nieprzewidywalna i choć naukowcy opracowują specjalistyczne raporty dotyczące aktualnych zagrożeń, ziemskich ruchów tektonicznych czy ocieplenia klimatu, nie możemy być wobec przyrody i matki ziemi zbyt zuchwali. Ważna jest również odpowiedzialność za globalne zasoby – warto oszczędzać wodę i żywność oraz pamiętać o tym, że to, co natura daje, może również zostać przez nią odebrane.

STARZENIE SIĘ SPOŁECZEŃSTWA

W wymiarze wewnętrznym oraz zewnętrznym bezpieczeństwo państwa jest nieodłącznie związane z przetrwaniem oraz zrównoważonym rozwojem społeczeństwa. Tymczasem nasz kraj staje właśnie w obliczu gwałtownego przyspieszenia procesu starzenia się ludności. Prognozowana mediana wieku populacji wzrośnie z 39 lat w 2015 roku do 45 lat w roku 2030. W 2050 roku dosięgnie aż 50 lat, co będzie piątą najwyższą wartością w Unii Europejskiej. W tym samym roku na jedną osobę powyżej 65. roku życia przypadną tylko dwie osoby w wieku 15–64 lat. Szacuje się, że całkowita liczba populacji Polski spadnie o 3% między rokiem 2015 a 2030 i o 10% między rokiem 2015 a 2050. Liczba ludzi w wieku 15–64 zmniejszy się jeszcze bardziej – o 11% między rokiem 2015 a 2030 i aż o 28% między rokiem 2015 a 2050[26]. Prognoza demograficzna Eurostatu wskazuje, że w 2060 roku co trzeci Polak będzie emerytem, a nasz kraj znajdzie się na pierwszym miejscu w Europie, jeśli chodzi o odsetek osób powyżej 65. roku życia. Szacuje się również, że liczba ludności spadnie z 38 mln do około 31 mln. Prognoza ta powstała jedynie na podstawie wyników dotyczących liczby urodzeń i zgonów, nie został w niej uwzględniony czynnik emigracji zarobkowej. Istnieje duże prawdopodobieństwo, że jeśli obecne wzorce uczestnictwa w rynku pracy się utrzymają, w 2050 roku podaż pracy w kraju będzie o 30% mniejsza niż w roku 2015. Spadek ten będzie spowodowany przede wszystkim wzrostem odsetka ludności powyżej 50. roku życia, czyli grupy cechującej się niską aktywnością zawodową. Polscy pracownicy opuszczają bowiem rynek pracy wcześniej w porównaniu z krajami UE. Skutkuje to tym, że liczba lat w cyklu życia, kiedy dochód z pracy przewyższa konsumpcję, jest u nas jednym z najniższych w Europie. Tym samym starzenie się ludności będzie prowadziło nie tylko do obniżenia zatrudnienia, PKB i dochodów indywidualnych, lecz także osłabi możliwości finansowania z budżetu państwa konsumpcji ludzi starszych.

Problem starzenia się społeczeństwa został dostrzeżony przez ekspertów zajmujących się bezpieczeństwem państwa i znalazł miejsce w *Białej księdze bezpieczeństwa narodowego z 2013 roku*. Jednym ze środków zaradczych ma być zahamowanie procesów emigracyjnych. We wnioskach wskazano, iż: *Istotnym elementem bezpieczeństwa państwa powinno być znaczne zmniejszenie liczby osób emigrujących z Polski, szczególnie ludzi młodych i wykształconych. Oferta państwa w zakresie odpowiednich warunków pracy i życia powinna być skierowana także do osób przebywających obecnie za granicą, deklarujących chęć powrotu. Powrót do kraju lub wstrzymanie decyzji o wyjeździe z Polski będą miały istotny wpływ na ograniczenie niekorzystnych trendów demograficznych. Jednocześnie będą jednak poważnym wyzwaniem dla państwa, m.in. przez wzrost liczby osób poszukujących pracy, czy mających problemy z adaptacją, co dotyczyć będzie części reemigrantów, a w szczególności ich dzieci*[27]. Masowe migracje powrotne są mało prawdopodobne, w związku z czym znaczny napływ imigrantów stanie się niezbędny, by powstrzymać wyludnianie się kraju. Konsekwencje zmian w strukturze demograficznej społeczeństwa są wielorakie, od wpływu na szkolnictwo, przez bilansowanie się systemu emerytalnego, po proporcje opieki nad osobami najmłodszymi i najstarszymi (zarówno w skali sektora usług, jak w indywidualnym budżecie każdego z nas). Prognozy są bardzo niepokojące, gdyż takie zjawiska, jak: deformacja

[23] Ibidem.

[24] http://zasady-bezpieczenstwa.pl/kleski-zywiolowe-w-polsce/.21.03.2018.

[25] https://www.lasy.gov.pl/pl/informacje/aktualnosci/najwieksza-taka-kleska-w-historii-polskich-lasow/. 21.03.2018.

[26] P. Lewandowski, J. Rutkowski. *Starzenie się ludności, rynek pracy i finanse publiczne w Polsce*. http://ibs.org.pl/app/uploads/2017/03/Starzenie-si%C4%99-ludno%C5%9Bci-rynek-pracy-i-finanse-publiczne-w-Polsce.pdf/.4.05.2018.

[27] *Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej.* Warszawa 2013, s. 182–183.

struktury wieku ludności i starzenie się społeczeństwa, będą bezpośrednio kreowały problemy zarówno w sferze społecznej, jak i gospodarczej.

SYSTEM OCHRONY ZDROWIA

Zdrowie, oprócz wykształcenia, motywacji, zdolności, doświadczenia czy posiadanej wiedzy fachowej, tworzy kapitał ludzki, będący jednym z głównych czynników wzrostu gospodarczego kraju. Zdrowi pracownicy są bardziej wydajni oraz charakteryzują się mniejszą absencją chorobową. Zdrowsza siła robocza przystosowuje się także szybciej do wszelkich zmian. Zwiększona z kolei produktywność oznacza wzrost gospodarczy kraju, który przez posiadanie odpowiednich zdolności finansowania potrzeb jego obywateli, zapewnia im poczucie bezpieczeństwa. Zdrowie, na ogół mierzone oczekiwanym czasem życia w chwili urodzenia lub śmiertelnością dorosłych, stanowi silny predyktor wzrostu gospodarczego, na co wskazują wyniki właściwie wszystkich badań wyjaśniających zróżnicowanie wzrostu między krajami bogatymi i biednymi[28]. Dlatego też stan zdrowia Polaków należy traktować jako jedno z głównych wyzwań służących rozwojowi gospodarczemu. Zmiany w strukturze społeczeństwa oraz jego rosnące wymagania to warunki, w których funkcjonuje system ochrony zdrowia. Prowadzone analizy dowodzą, że wzrost kosztów opieki zdrowotnej będzie szybszy, niż możliwości ich pokrycia, co dotyczy nie tylko Polski, lecz także całej Europy. Reorganizacje zachodzące w otoczeniu systemu ochrony zdrowia indukują nowe zjawiska, z którymi muszą się mierzyć instytucje w nim funkcjonujące. Do tych warunków system opieki zdrowotnej musi się przystosowywać.

Z przeprowadzonych w latach 2012–2014 badań wynika, że nastąpiła poprawa w ocenie poziomu zadowolenia z funkcjonowania systemu, lecz nadal pozostaje na niskim poziomie: 68% wskazań krytycznych. Kolejne analizy, mające miejsce w latach 2013–2015, stwierdzają, że ocena zaspokojenia potrzeb zdrowotnych nie zmieniła się: 77% wskazań. Niezadowoleniu z funkcjonowania systemu ochrony zdrowia towarzyszy bardzo niska ocena oparta na mierzalnych wskaźnikach. Polska od lat zajmuje niskie miejsca w rankingu systemów ochrony zdrowia. W roku 2014 było to 31. miejsce na 37. ocenianych krajów, a w roku 2015 przedostatnie. I działo się to przy poprawie uzyskanego przez nasz kraj wyniku, co oznacza, że pozostałe oceniane kraje dokonują większych postępów w reformowaniu swoich systemów[29]. Niezbędne są zatem zdecydowane kroki zmierzające do poprawy sytuacji. Należy przy tym brać pod uwagę, że wspomniane rozczarowanie będzie szybciej wzrastać, gdyż w wiek, w którym widoczne jest pogorszenie się stanu zdrowia, weszło pokolenie, którego całe życie zawodowe przebiegało w Polsce demokratycznej i rynkowej. W Polsce 61% praktykujących lekarzy ukończyło 45 lat, a 16% – 65. W latach 2008–2013 średnia wieku pielęgniarek wzrosła z 44,19 do 48,69 lat, co wskazuje, że system nie jest zasilany przez absolwentki pielęgniarstwa. Wskaźniki liczby personelu medycznego przypadającego na populację są bardzo niskie. W roku 2016 wskaźnik aktywnych zawodowo lekarzy na 1000 mieszkańców wynosił w Polsce 2,4, a dla europejskich krajów – 3,8, natomiast dla pielęgniarek – odpowiednio 5,3 i 10,3. Problem ten może wyłącznie narastać, na co wskazuje m.in. zanikanie barier migracyjnych w Europie i duże zapotrzebowanie na personel medyczny w zamożniejszych krajach[30]. W zawodach medycznych rośnie więc luka pokoleniowa, którą niezwykle trudno będzie zlikwidować. Wzrost liczby potrzebujących oraz jednoczesny spadek liczby personelu medycznego to zjawisko pogłębiające się z kolejnym rokiem. Mając na uwadze przywoływane opinie o systemie ochrony zdrowia, można postawić tezę, że jest on zupełnie nieprzygotowany na wzrastające oczekiwania pacjentów.

Wymienione problemy w sektorze ochrony zdrowia z pewnością nie są jedyne i wymagają wprowadzenia znaczących reform. Brak chęci do stawienia czoła narastającym trudnościom sprawia, że ocena rodzimego systemu ochrony zdrowia jest bardzo niska. Konieczne stają się zmiany dotyczące lepszego wykorzystania posiadanych zasobów, rozwoju innych, niż szpitalna form opieki, powrotu do pracy pielęgniarek, zmiany ról personelu medycznego, tj. przekazanie części zadań innym, niż lekarze grupom zawodowym, czy również zwiększenia odpowiedzialności społeczeństwa za zdrowie. Zdrowie oddziałuje nie tylko na liczbę dni czy godzin przeznaczanych na pracę, ale również na decyzje dotyczące pozostawania w sile roboczej. Stan zdrowia społeczeństwa wpływa nie tylko na poziom dochodu, lecz również na jego podział między konsumpcję i oszczędności, a więc także na gotowość do inwestowania, co przekłada się na rozwój gospodarki kraju.

NIERÓWNOŚCI SPOŁECZNE

Rozważania nad nimi towarzyszą najczęściej socjologicznym analizom ubóstwa i wykluczenia społecznego. W literaturze przedmiotu rozwarstwienie dochodowe jest uznawane za najważniejszy miernik tych nierówności. Osiągany dochód jest wyznacznikiem statusu społecznego oraz czynnikiem kształtującym szanse w niemal wszystkich sferach życiowych, takich jak: dostęp do rozrywek, służby zdrowia, uczestnictwo w kulturze, edukacja czy nawet dostęp do władzy.

Najpopularniejszym miernikiem nierówności jest współczynnik Giniego, który informuje o stopniu kon-

[28] E. Nojszewska: *Oddziaływanie zdrowia na gospodarkę – wnioski dla polskiego systemu ochrony zdrwia.*http://bazhum.muzhp.pl/media//files/Problemy_Zarzadzania/Problemy_Zarzadzania-r2017-t15-n3_(1)/Problemy_Zarzadzania-r2017-t15-n3_(1)-s11-24/Problemy_Zarzadzania-r2017-t15-n3_(1)-s11-24.pdf/.7.05.2018.

[29] Ibidem, s. 348.

[30] Ibidem, s. 350–352.

centracji określonych dóbr w społeczeństwie. Przyjmuje on wartości z przedziału od 0 do 1 (niekiedy wartość mnożona jest przez 100 i przedstawiana w przedziale od 0 do 100). Im niższa wartość wskaźnika, tym bardziej równomierna dystrybucja dochodów. Wartość 0 wskazuje na maksymalną równość, tzn. wszyscy członkowie danej zbiorowości osiągają jednakowe dochody lub mają taki sam dostęp do pewnego dobra[31]. W zakresie położenia materialnego rodziny można niestety mówić o dwóch biegunach: obszarze biedy i obszarze dostatku.

Współczesna Polska podzielona jest na trzy segmenty: sektor instytucji prywatnych (Polska sprywatyzowana), sektor instytucji publicznych (Polska budżetowa) i instytucji zabezpieczenia społeczno-socjalnego (Polska na zasiłku). Obszar zwiększonego ryzyka stanowi grupa osób i ich rodzin z trzeciego segmentu. Jego część to stali klienci pomocy społecznej, zgłaszający się po zasiłek wraz z rodzicami i uczący tego swoje dzieci (tzw. dziedziczenie biedy)[32]. W szczególnie trudnej sytuacji jest młode pokolenie, którego część znalazła się na marginesie ustabilizowanego społeczeństwa. Długie pozostawienie tych grup w takiej sytuacji powoduje groźne społecznie frustracje i negatywne skutki w postaci wzrostu patologicznych zjawisk, w tym przestępczości. Młodzież wpływa na kształtowanie struktury społecznej we wszystkich jej obszarach. Postawa i świadomość przyszłego społeczeństwa w dużej mierze będą zależeć od dążeń, aspiracji i planów życiowych młodszej grupy społeczeństwa.

W 2010 roku w Unii Europejskiej współczynnik Giniego kształtował się przeciętnie na poziomie 30,5. Najwyższa nierówność dochodów charakteryzowała Litwę – 36,9 oraz Łotwę – 36,1. Najniższe wartości indeksu Giniego odnotowano zaś w Słowenii – 23,8, na Węgrzech oraz w Szwecji – 24,1. W 2010 roku Polska znalazła się w Unii Europejskiej (UE-28) na dwunastym miejscu pod względem nierówności dochodowych mierzonych analizowanym współczynnikiem[33]. W 2015 roku współczynnik Ginniego kształtował się w przedziale od 23,7 na Słowacji do 37,9 na Litwie, co oznacza, że nierówności dochodowe na Litwie były o 60% wyższe niż na Słowacji. Wysokie nierówności dochodowe powyżej 35 odnotowano również w Rumunii, Bułgarii oraz na Łotwie. Najniższa rozpiętość dochodów – poniżej 26 charakteryzowała Słowację, Słowenię, Czechy, Szwecję i Finlandię. W Polsce miara ta osiągnęła poziom 30,6 i była niewiele wyższa od średniej unijnej, która wyniosła 31[34].

Można zatem zauważyć, że dotychczasowe rządy wprowadziły system selekcji ludności, który bezpowrotnie spycha część społeczeństwa na margines, nie dając w zamian żadnej możliwości godnego życia. Zamiast polityki społecznej rząd uprawia filantropię państwową, która doprowadziła do szybkiego przyrostu podopiecznych, uzależnionych od innych i żyjących z ręką wyciągniętą po pomoc. Sytuacja poszerzającego się obszaru biednych prędzej czy później będzie się odbijać na egzystencji bogatych, przejawiając się w niepokoju o zgromadzone dobra czy izolacji w zbudowanych przez siebie enklawach. W dobie ryzyka globalnego, regionalnego i lokalnego istnieją jedynie złudzenia, że będzie można nad nim zapanować. Wskazać można też na jego wszechobecność niejako pośrednią (np. terroryzm, powodzie, kataklizmy sejsmiczne) dla współczesnego człowieka, ale ryzyko sięga przede wszystkim naszej codziennej egzystencji. Można zatem stwierdzić, że problemy społeczne to przede wszystkim obowiązek i wyzwanie dla rządzących. Brak dążenia do ich rozwiązywania będzie powodował zagrożenia we wszystkich sferach życia społecznego całego państwa.

WŁAŚCIWIE FUNKCJONOWAĆ

Dynamiczny i nieustanny rozwój nowych technologii przynosi wiele ułatwień w życiu codziennym, prowadząc do wzrostu stopy życiowej, ale również pociągając za sobą wiele niebezpieczeństw związanych ze zdrowiem i stanem środowiska. Ponadto zaostrzające się napięcia polityczne, ekonomiczne czy religijne ukazują występujące wśród społeczeństw sprzeczności i zróżnicowania interesów generujące nową falę zagrożeń o wielorakim charakterze, od szantażu energetycznego, ekscesów chuligańskich, infekowania systemów informatycznych do zamachów terrorystycznych.

Obecne źródła zagrożeń szeroko rozumianego bezpieczeństwa naszego kraju wynikają ze splotu wielu czynników destabilizujących, powstających często daleko od naszych granic, których skutki godzą w państwo i jego obywateli. Ze względu na zwrócenie uwagi na zagrożenia o charakterze pozamilitarnym, niezwykle istotne dla prawidłowego funkcjonowania systemu bezpieczeństwa jest zdiagnozowanie obszarów, które stanowią największe wyzwania dla utrzymania stabilności państwa. Należy zatem postrzegać współczesny system bezpieczeństwa nie tylko jako system wewnętrznie zintegrowany, lecz także silnie powiązany z innymi systemami warunkującymi optymalne funkcjonowanie państwa. Przykładem tego może być gospodarka, której stan oraz niezakłócony rozwój przekłada się na bezpieczeństwo państwa, zarówno w sferze militarnej, społecznej, jak i politycznej. Zintegrowane podejście do bezpieczeństwa, zakładające kompleksowe spojrzenie na zadania i cele państwa w tej dziedzinie, sprzyja właściwemu funkcjonowaniu systemu bezpieczeństwa narodowego, warunkując społeczne i gospodarcze podstawy ładu narodowego. ■

WSPÓŁCZESNY SYSTEM BEZPIECZEŃSTWA TO NIE TYLKO SYSTEM WEWNĘTRZNIE ZINTEGROWANY, LECZ TAKŻE SILNIE POWIĄZANY Z INNYMI SYSTEMAMI WARUNKUJĄCYMI OPTYMALNE FUNKCJONOWANIE PAŃSTWA.

[31] Ibidem.

[32] A. Nafalska: *Nierówność społeczna – wyzwanie czy zagrożenie dla współczesnych.* http://www.edukacja.edux.pl/p-3946-nierownosc-spoleczna-wyzwanie-czy-zagrozenie.php/. 7.05.2018.

[33] M. Raczkowska: *Nierówności ekonomiczne w UE.* http://sj.wne.sggw.pl/pdf/PEFIM_2017_n67_s146.pdf/.7.05.2018.

[34] Ibidem.

Pojęciowe **dylematy**

ZJAWISKO WOJNY W CIĄGU OSTATNICH LAT ISTOTNIE SIĘ PRZEOBRAZIŁO, GDYŻ WZROSŁA LICZBA KONFLIKTÓW WEWNĄTRZPAŃSTWOWYCH I CORAZ CZĘŚCIEJ MOŻNA ZAOBSERWOWAĆ ROZMYCIE GRANICY MIĘDZY ŻOŁNIERZAMI A CYWILAMI ORAZ STANEM WOJNY A STANEM POKOJU.

mjr dypl. SZRP Paweł Kowalczyk

Działania elementów sił zbrojnych Federacji Rosyjskiej na Ukrainie przyczyniły się do wznowienia debaty na temat możliwych zagrożeń płynących ze strony tego państwa w kierunku Zachodu. Konflikt rosyjsko-ukraiński spopularyzował, zarówno wśród mediów, jak i polityków, posługiwanie się pojęciami *wojny hybrydowej*, *zagrożeń hybrydowych* czy *hybrydowego pola walki.* Jednak coraz częściej pojawiają się pytania: czym tak naprawdę są wymienione pojęcia, czy odnoszą się faktycznie do nowego zjawiska w sztuce wojennej. Czy poprawne jest używanie tych terminów i czy są one zasadne w odniesieniu do sposobów działania? Czy pojęcie hybrydowości jest całkowicie nowym pojęciem w sztuce wojennej, czy mieliśmy z nim już do czynienia dużo wcześniej? Czy działania hybrydowe są całkowicie nowym sposobem prowadzenia walki, czy jednak nie są niczym nowym, a jedynie opisują stare sposoby działania pod nową nazwą? Są to wątpliwości, które nasuwają się przy próbie bliższego określenia terminu *hybrydowości* w sztuce wojennej.

MNOGOŚĆ DEFINICJI

Mimo że termin *hybrydowość* stał się bardzo popularnym określeniem sposobów działania (stosowanym zwłaszcza przez komponenty armii Federacji Rosyjskiej), to jednak literatura z zakresu sztuki wojennej nie odnosi się wprost w żaden sposób do tego rodzaju konfliktów „pełzających" czy konfliktów poniżej progu wojny.

Wojna hybrydowa często jest wymieniana zamiennie z pojęciami *konfliktu pełzającego* czy *konfliktu poniżej progu wojny*. Jednak określenie wojny hybrydowej zaczęło się pojawiać już w latach dziewięćdziesiątych XX wieku, kiedy mianem tym nazywano konflikty w Afganistanie czy Iraku. Prawdopodobnie po raz pierwszy określenia tego użył Frank Hoffman w raporcie *Conflict in 21st Century: The Rise of Hybrid Wars*, opracowanym w 2007 roku na zlecenie Instytutu Potomac for Policy Studies. W przedmiotowym dokumencie zdefiniował on wojnę hybrydową jako nowe zjawisko, które we współczesnych konfliktach będzie dominowało na polu walki. Jednak terminy *działania hybrydowe* oraz *wojna hybrydowa* pojawiły się już w 2002 roku w pracy mjr. Williama J. Nemetha pt. *Future war and Chechnya: A case for hybrid warfare*[1], w której zastosował pojęcie *hybrydowości* nie tylko w odniesieniu do działań prowadzonych przez czeczeńskich bojowników, lecz także w stosunku do przekroju całego społeczeństwa. Jedną z wielu cech tzw. społeczeństwa hybrydowego jest połączenie nowoczesnych teorii politycznych z tradycyjną organizacją społeczną i obyczajowością[2]. Hybrydowy kształt danego społeczeństwa ma bezpośrednie przełożenie

[1] W.J. Nemeth: *Future war and Chechnya: A case for hybrid warfare*, Naval Postgraduate School, Monterey 2002.
[2] Ibidem, s. 71.

na sposób prowadzenia przez nie wojny. Według W.J. Nemetha wojna hybrydowa cechuje się m.in.[3]:

– organizacją armii odzwierciedlającą poziom rozwoju społeczno-ekonomicznego danej wspólnoty oraz obowiązujące w niej normy – społeczeństwo czeczeńskie jest zdecentralizowane, egalitarne i oparte na strukturze klanowej, dlatego w taki sam sposób byli zorganizowani bojownicy czeczeńscy w trakcie konfliktu z Rosją;

– innym od zachodniego sposobem percepcji siły militarnej – w wypadku działań hybrydowych ich siła ma polegać na masowym zastosowaniu działań partyzanckich, które stwarzają poważne zagrożenie dla hierarchicznie zorganizowanych i zaawansowanych technologicznie oddziałów przeciwnika. Ponadto doświadczenia konfliktu rosyjsko-czeczeńskiego wskazują, że wojna hybrydowa jest prowadzona w sposób totalny, ponieważ jest traktowana jako narzędzie ochrony danej wspólnoty przed całkowitą zagładą. W związku z tym tego typu konflikt dopuszcza użycie wszelkich niezbędnych środków, w tym m.in. porwań oraz masowych mordów. Efektem działań hybrydowych jest także doprowadzenie do zatarcia się granicy między uczestnikami walk a cywilami;

– umiejętnością zastosowania nowoczesnych technologii w działaniach bojowych. W przypadku Czeczenów chodziło np. o wykorzystanie nowoczesnych technologii telekomunikacyjnych (m.in. telefonów komórkowych, satelitarnych) w celu zwiększenia efektywności dowodzenia, a także o prowadzenie działań propagandowych (m.in. rozgłaszanie plotek o przejęciu broni masowego rażenia, która miałaby zostać użyta w jednym z rosyjskich miast, wykorzystanie znajomości języka rosyjskiego w celu dezinformowania oddziałów armii rosyjskiej). Posiadanie tych umiejętności oznacza również zdolność do kreatywnego użycia danej technologii w sposób, który nie był przewidziany przez jej twórców.

Analizując treści przedstawiane przez F. Hoffmana oraz mjr. W.J. Nemetha, można odnieść wrażenie, iż działania nazywane przez nich hybrydowymi noszą znamiona konfliktu prowadzonego poniżej progu wojny, a sama hybrydowość społeczeństwa czeczeńskiego bardziej odnosi się do działań nieregularnych, które nazwane zostały hybrydowymi na potrzeby opisania sposobów walki.

Obecnie jednak pojęcie *działań hybrydowych* najczęściej jest stosowane w odniesieniu do działań Federacji Rosyjskiej na Ukrainie, a także do działań dezinformacyjnych czy też w cyberprzestrzeni skierowanych przeciwko NATO czy Unii Europejskiej. Dlatego bardzo często konflikt prowadzony poniżej progu wojny nazywany jest wojną hybrydową, gdyż mimo że ma on większość cech klasycznego konfliktu zbrojnego, to jednak tak naprawdę nim nie jest. Aby dobrze zrozumieć problematykę wojny hybrydowej, należałoby zacząć od próby zdefiniowania obu pojęć i zrozumienia, czym tak naprawdę są wojna hybrydowa i konflikt poniżej progu wojny oraz do czego się odnoszą.

RYS. HYBRYDOWOŚĆ KONFLIKTU ZBROJNEGO

Opracowanie własne.

Wyjaśnienie znajdziemy w opracowaniu pt. *Teoria i praktyka działań hybrydowych,* w którym jego autorzy określają, iż: *Etymologia terminu „hybrydowość" wywodzi się z łacińskiego słowa hybryda, oznaczającego „mieszańca", osobnika powstałego ze skrzyżowania dwóch genetycznie różnych osobników, należących do różnych gatunków, odmian czy ras.* W innym ujęciu hybrydowość można zdefiniować jako […] *właściwość powstałą w wyniku skrzyżowania lub zmieszania cech, elementów należących do różnych, często odmiennych strukturalnie i odległych genetycznie przeciwstawnych przedmiotów, organizmów lub stanów. Hybrydyzacja oznacza więc scalenie odmiennych istotowo cech wokół jednego, odrębnego bytu, przy zachowaniu specyficznych własności gatunkowych decydujących o „wyższości" nowego, hybrydowego organizmu pod względem, np. odporności na choroby, wytrzymałości czy większych zdolności adaptacyjnych*[4].

Dlatego sama hybrydowość w odniesieniu do konfliktu zbrojnego będzie oznaczać połączenie wielu rodzajów działań (np. regularnych i nieregularnych, militarnych i niemilitarnych, psychologicznych, informatycznych czy działań w cyberprzestrzeni) prowadzonych jednocześnie w określonym czasie dla osiągnięcia celu (rys.). Działania te będą prowadzo-

[3] Ibidem, s. 73–76.

[4] R. Parafianowicz, M. Banasik: *Teoria i praktyka działań hybrydowych*. „Zeszyty Naukowe AON" 2015 nr 2(99).

ne w sposób elastyczny i wyrafinowany, a ponadto bardzo skutecznie.

J.M. Calha definiuje wojnę hybrydową jako *użycie taktyki asymetrycznej w celu wykrycia i wykorzystania słabości (przeciwnika) za pomocą środków pozamilitarnych (np. politycznego, informacyjnego czy ekonomicznego zastraszania i manipulacji) popartych groźbą użycia konwencjonalnych i niekonwencjonalnych środków militarnych*[5]. Definicja ta pojawiła się w dokumentach normatywnych NATO jako odpowiedź na zmiany dotychczasowego pola walki oraz sposobów prowadzenia działań, głównie wskutek wyzwań, jakie przyniósł ze sobą konflikt na Ukrainie oraz działań tzw. Państwa Islamskiego (IS). W *Słowniku Biura Bezpieczeństwa Narodowego* z kolei wojnę hybrydową zdefiniowano jako *wojnę łączącą w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.*[6]. W tym samym słowniku określono również agresję podprogową jako *działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa*[7]. Według Stanisława Kozieja agresja podprogowa może być presją polityczno-militarną, która może płynnie przechodzić w skryte i niejawne, a zarazem ograniczone zastosowanie przemocy zbrojnej. Taką właśnie metodę stosuje z powodzeniem wobec wspieranej przez Zachód Ukrainy Federacja Rosyjska, aby osłabić zarówno uzyskiwane wsparcie, jak i wywrzeć presję na to państwo (głównie ekonomiczną w postaci sankcji)[8].

Po analizie przedstawionych definicji należy stwierdzić, że pojęcie *hybrydowości* mieści się bardziej w ramach prowadzenia działań poniżej progu wojny, a nie odwrotnie. Analizując zasady sztuki wojennej oraz pojęcie *wojny*, należy zwrócić uwagę, że wojna jest *czynem politycznym, dalszym ciągiem stosunków politycznych, wyrażających się w akcie przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli. Przy czym bezpośrednim celem działań wojennych jest rozbrojenie przeciwnika, czyli doprowadzenie jego sił zbrojnych do stanu, w którym nie będą zdolne do dalszej walki*[9]. Dodatkowym uzupełnieniem dokonanym przez F. Skibińskiego jest stwierdzenie, że *wojna nosi charakter krwawej walki zbrojnej, staczanej przez zorganizowane siły, co ma ograniczać pojęcie wojny do tych konfliktów politycznych, w których użyte są obustronnie siły zbrojne*[10].

SZCZEGÓLNĄ ROLĘ MAJĄ DO ODEGRANIA **MOBILNE, MIESZANE ODDZIAŁY BOJOWE,** KTÓRE NIE BĘDĄ ANGAŻOWAŁY SIĘ W OTWARTE WALKI Z PRZECIWNIKIEM

Przytoczone definicje wskazują na to, iż wojna w rozumieniu prawnym będzie oznaczać zerwanie stosunków dyplomatycznych i pokojowych między co najmniej dwoma państwami i przejście do stanu wojny. Zgodnie z konwencjami haskimi z 1899 i 1907 roku, wojna powinna się rozpocząć od oficjalnego jej wypowiedzenia przez strony przeciwko sobie lub jedną ze stron. Wypowiedzenie wojny będzie

WSZYSTKIE DZIAŁANIA BĘDĄ WSPIERANE ŚRODKAMI MILITARNYMI,

ZE SZCZEGÓLNYM UWZGLĘDNIENIEM WOJNY INFORMACYJNEJ ORAZ DZIAŁAŃ WOJSK SPECJALNYCH

[5] J.M. Calha: *Hybrid Warfare: NATO's new strategic challenge?* General Report, Defence Security Committee 2015, s. 3.

[6] Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN/. 27.12.2017.

[7] Ibidem, s. 1.

[8] S. Koziej: *Hybrydowa zimna wojna w Europie.* Warszawa 2016, s. 4.

[9] K. Clausewitz: *O wojnie.* Warszawa 1958, s. 15, 16, 31, 32, 36.

[10] F. Skibiński: *Rozważania o sztuce wojennej.* Warszawa 1973, s. 29.

[11] https://inmoscowsshadows. wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/. 25.12.2017.

DOKTRYNA GIERASIMOWA

Szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej gen. WALERIJ GIERASIMOW

Otwarte wykorzystanie oddziałów wojskowych jest dopuszczalne dopiero w późniejszej fazie konfliktu i to pod pretekstem prowadzenia działań humanitarnych czy pokojowych.

oznaczać swoisty próg, którego przekroczenie wprowadzi dany kraj w stan wojny. Jednak obecnie coraz częściej prowadzi się działania zbrojne lub działania niezbrojne właśnie bez wypowiadania wojny, czyli bez zachowania otwartości konfliktu. Zatem prowadzenie wszelkich działań, o których pisze C. Clausewitz oraz F. Skibiński, bez przekraczania progu wojny, będzie działaniem pod jej progiem, jednak prowadzącym często do tego samego co wojna. Jak widać wojna hybrydowa będzie niczym innym jak konfliktem toczonym poniżej progu wojny, noszącym te same cechy i prowadzonym w tym samym celu.

Analizując pojęcia *wojny hybrydowej* i *konfliktu poniżej progu wojny* nie sposób pominąć wypowiedzi szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej gen. W. Gierasimowa, którą zawarł w artykule pt. *Znaczenie nauki w przewidywaniu*[11]. Przedstawione w nim rozważania

OBECNIE ZACIERAJĄ SIĘ RÓŻNICE MIĘDZY STRATEGICZNYM, OPERACYJNYM ORAZ TAKTYCZNYM POZIOMEM DZIAŁAŃ

określono mianem *Doktryny Gierasimowa*.

Analizując przywołany artykuł, należy stwierdzić, że autor nie posługuje się pojęciami *wojna hybrydowa* ani *konflikt poniżej progu wojny*, jednak zawarte treści mogą wskazywać jednoznacznie, iż odnosi się on do elementów, które są właśnie charakterystyczne dla tego zjawiska. W jego opinii wojny

WOJNY XXI WIEKU NIE BĘDĄ POPRZEDZANE FORMALNYMI AKTAMI JEJ WYPOWIEDZENIA, CO BĘDZIE POWODOWAĆ CHARAKTERYSTYCZNY ZANIK GRANIC MIĘDZY STANEM WOJNY I POKOJU

MINISTRY OF DEFENCE OF THE RUSSIAN FEDERATION

XXI wieku nie będą poprzedzane formalnymi aktami jej wypowiedzenia, co będzie powodować charakterystyczny zanik granic między stanem wojny i pokoju, a więc większość działań będzie prowadzonych w sposób charakterystyczny dla kryzysu. Zmiany zachodzące w społeczeństwach, środowisku operacyjnym czy sztuce wojennej w XXI wieku będą powodować nasilenie się takiej formy prowadzenia działań. Zanik granic między stanem wojny i pokoju nie jest nowym zjawiskiem, a kryzys powstały wskutek tych zmian będzie się nasilał ze względu na zwiększone możliwości wykorzystania i stosowania działań podprogowych.

W ocenie gen. W. Gierasimowa głównym zmianom poddano same zasady prowadzenia wojen, a co za tym idzie, dużo większego znaczenia nabrały niemilitarne środki prowadzenia działań wojennych. Niezwykle istotne jest umiejętne wykorzystanie różnorodnych instrumentów ekonomicznych, politycznych oraz humanitarnych, co powinno się odbywać w połączeniu z manipulowaniem nastrojami ludności zamieszkującej obszar konfliktu. Wszystkie działania będą wspierane środkami militarnymi, ze szczególnym uwzględnieniem wojny informacyjnej oraz działań wojsk specjalnych. Autor stwierdza również, że otwarte wykorzystanie oddziałów wojskowych jest dopuszczalne dopiero w późniejszej fazie konfliktu i to pod pretekstem prowadzenia działań humanitarnych czy pokojowych. Jednocześnie wskazuje, że rozwój technologii informacyjnych pozwolił nie tylko na znaczne usprawnienie procesu komunikacji między walczącymi pododdziałami a ich dowództwami, lecz także na wykorzystanie przestrzeni informacyjnej do niwelowania potencjału bojowego przeciwnika. Podaje tutaj przykład państw Afryki Północnej, w których internetowe sieci społecznościowe posłużyły do mobilizowania miejscowej ludności oraz wpływania na organy władzy.

W opracowaniu autor dużą wagę przywiązuje do działań asymetrycznych, zwłaszcza do wykorzystania wojsk specjalnych oraz do funkcjonowania wewnętrznej opozycji politycznej, zmierzających do objęcia konfliktem całego obszaru działań. Szczególną rolę mają do odegrania mobilne mieszane oddziały bojowe, które nie będą się angażowały w otwarte walki z przeciwnikiem. Uważa, że obecnie zacierają się różnice między strategicznym, operacyjnym oraz taktycznym poziomem działań, a także między operacjami zaczepnymi i obronnymi[12].

Jednak mimo że próby samego zdefiniowania pojęcia *wojny hybrydowej* pojawiły się dopiero w ostatnich latach, to działania tego typu możemy zauważyć dużo wcześniej. Od starożytności już bowiem jednym z głównych wyznaczników prowadzenia działań militarnych było prawidłowe rozpoznanie bieżącej sytuacji i dostosowanie do niej swoich działań[13]. Merle Maigre[14] w artykule dla „German Marshall Fund"[15] głosi, że wojna hybrydowa nie jest nowym zjawiskiem, a samo pojęcie sięga daleko, co najmniej dekadę wstecz. Według niej historia daje wiele przykładów łączenia działań regularnych i nieregularnych, gdzie już w starożytności Sun Tzu określał wojnę sztuką przebiegłości. W 1920 roku radziecki wojskowy opracował koncepcję „maskowania walki" (maskirowka), która obejmowała różne środki aktywne i pasywne tak zaprojektowane, by oszukać przeciwnika i wpływać na proces opiniotwórczy oraz podejmowania decyzji. Także radziecka inwazja na Afganistan w 1979 roku była prowadzona poniżej progu wojny, gdy około 700 żołnierzy radzieckich przebranych w mundury armii afgańskiej zajęło kluczowe budynki administracyjne w Kabulu.

Innym przykładem stosowania działań poniżej progu wojny były działania V kolumny, czyli agentur wywiadowczych III Rzeszy. Współdziałały one z wojskami regularnymi oraz grupami dywersantów rekrutowanych spośród nacjonalistycznych środowisk mniejszości niemieckiej podczas agresji na Czechosłowację. Jej działania polegały między innymi na wysuwaniu żądań, prowokowaniu zamieszek, w wyniku których mieli ginąć Niemcy. Miało to służyć oskarżaniu o te tragedie władz państwowych, a przez to wywrzeć na nie silną presję. W tym samym czasie Niemcy prowadzili działania propagandowe, które miały za zadanie podsycać ruchy narodowościowe w celu doprowadzenia do zbrojnego powstania mniejszości niemieckiej[16].

Wtedy też działania poniżej progu wojny prowadzili także Polacy na Zaolziu. Pod pretekstem ochrony mniejszości polskiej dążono do oderwania części tych ziem i włączenia ich do macierzy. Organizowano i prowadzono działalność dywersyjno-wywiadowczą rozwijając organizację „A" i „B". Celem pierwszej było sterowanie nastrojami panującymi wśród zaolziańskich Polaków. Organizacja „B" natomiast miała odpowiadać za dywersję i działania o charakterze terrorystycznym. Celem obu w perspektywie było przygotowanie rozruchów, które mogły się przerodzić w antyczeskie powstanie. Z aktywnością zaolziańskich organizacji skoordynowano działalność Polskiego Radia oraz gazet rządowych. Dodatkowo

[12] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia.* „Przegląd Bezpieczeństwa Wewnętrznego" – Wydanie specjalne. ABW, Warszawa 2015, s. 39–50.

[13] *Sun Tzu: Sztuka wojny.* Gliwice 2004.

[14] Była doradczyni ds. polityki bezpieczeństwa prezydenta Estonii, obecnie dyrektor Centrum Doskonalenia Obrony Cybernetycznej NATO.

[15] M. Maigre: *Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO, The German Marshall Fund of the United States*, 12 February 2015, http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato/. 12.12.2017.

[16] M. Przeperski: *Nieznośny ciężar braterstwa*. Warszawa 2016, s. 264–277.

Sztab Generalny Wojska Polskiego opracował plany interwencji zbrojnej na terytorium Republiki Czechosłowacji, w ramach których przewidywano zorganizowanie bojówek[17] wspierających przyłączenie Zaolzia, Spiszu, a także Orawy do Polski. Przewidywano również możliwość utworzenia korpusu ochotniczego, który miał stanowić wsparcie dla ewentualnego powstania na Zaolziu. Ponadto zaplanowano, jak co roku, wielkie manewry wojskowe na Wołyniu, których celem był między innymi pokaz siły[18].

Można zatem wyciągnąć wniosek, że działania hybrydowe nie są nowym zjawiskiem, jedynie sam termin *hybrydowości* pasuje bardziej do dzisiejszych czasów i odnosi się do prowadzenia działań poniżej progu wojny. Jego stosowanie można by powiązać z zakończeniem zimnej wojny. Ponadto wraz z zanikiem rywalizacji między Wschodem i Zachodem zmniejszyła się liczba konfliktów zastępczych (tzw. proxy wars) oraz wojen peryferyjnych inspirowanych przez oba obozy. Jednak oba te bloki czy bieguny były jakby stabilizatorem, który przyczyniał się do opanowania sytuacji wewnątrz danego bloku, a zatem do umocnienia systemu międzynarodowego, jednocześnie zmniejszając ryzyko wystąpienia wewnętrznych konfliktów na tle narodowościowym, religijnym czy etnicznym[19]. Jak jednak pokazuje teraźniejszość i niedaleka przeszłość, początek XXI wieku charakteryzuje się coraz to nowszymi wyzwaniami rzucanymi państwom w dziedzinie bezpieczeństwa. Już teraz, po kilkudziesięciu latach od rozpadu tzw. dwubiegunowego podziału świata, można stwierdzić, że zakończenie zimnej wojny nie oznaczało wcale wyeliminowania wewnętrznych lub regionalnych źródeł konfliktów i nie zapewniło trwałego pokoju na świecie[20].

Obecnie każdy kraj musi być gotowy na to, by sprostać całkowicie nowym zagrożeniom w sferze bezpieczeństwa. Jednak to zimna wojna przyzwyczaiła wszystkich do tego, iż o konflikcie międzypaństwowym myślano głównie kategoriami tradycyjnych wojen. Natomiast wydarzenia na Ukrainie czy działania tzw. Państwa Islamskiego pokazują, że należy być w gotowości do walki z przeciwnikiem nieokreślonym, pozbawionym jasnych struktur organizacyjnych i niestosującym standardowej taktyki.

Zatem wojna hybrydowa jest niczym innym jak konfliktem poniżej progu wojny, czyli staje się elementem wojny, która może być toczona między: państwami, państwem a organizacją (organizacjami) niepaństwową oraz państwem i organizacją (organizacjami) niepaństwową, które mogą być wspierane przez inne państwa)[21].

Federacja Rosyjska prowadząc tzw. wojnę hybrydową (tzw. ponieważ według Rosjan w ich działaniach nie ma żadnej hybrydowości, lecz stosują „czystą sztukę wojenną"), wykorzystuje na dużą skalę działania asymetryczne, które pozwalają skutecznie niwelować przewagę przeciwnika w walce. W ramach tych działań intensywnie używają wojsk specjalnych i wewnętrznej opozycji oponenta, prowadzą na dużą skalę działania informacyjne, a także stosują inne formy walki adekwatne do miejsca i czasu w celu oddziaływania na całe terytorium przeciwnika[22]. Zatem termin *wojny hybrydowej* jest nowym pojęciem określającym działania, które wcześniej były już stosowane i wpisują się w ramy konfliktu zbrojnego, jednak mogą być prowadzone bez wypowiedzenia aktu agresji innemu państwu czy organizacji, a więc stają się działaniami prowadzonymi poniżej progu wojny. W wyniku braku jasnej klasyfikacji oraz populizmu panującego w mediach częściej jest stosowany termin *wojny hybrydowej* niż *konflikt poniżej progu wojny*. Co więcej, termin *konflikt poniżej progu wojny* jest sformułowaniem trafniejszym.

W EUROPIE I NA BLISKIM WSCHODZIE

Analizując sposoby prowadzenia działań hybrydowych, często można spotkać pogląd, iż działania podprogowe rozpatruje się w dwóch kontekstach: w kontekście konfliktu na Bliskim Wschodzie oraz na Ukrainie, gdyż przedstawiają one dwa modele ich prowadzenia. W wypadku Ukrainy działania podprogowe są prowadzone przez Federację Rosyjską, a na terenie Syrii oraz Iraku przez organizację terrorystyczną tzw. Państwa Islamskiego[23]. Jednak działania tzw. Państwa Islamskiego bardziej odpowiadają działaniom terrorystycznym czy nieregularnym niż poniżej progu wojny. Państwo to jest organizacją terrorystyczną, która sama ustanowiła się państwem, niezaakceptowanym przez jakikolwiek inny kraj czy organizację rządową. Dlatego nawet media, gdy podają jego nazwę, stosują przedimek „tak zwane", aby zastosować wyróżnienie od innych pełnoprawnych krajów.

Jednak konflikt na Ukrainie jest *modelowym przykładem, gdzie państwo, jako strona silniejsza, prowadzi wojnę hybrydową z przeciwnikiem słabszym. W wojnie hybrydowej na Ukrainie można wyodrębnić 4 etapy: dywersję polityczną, budowanie pozycji społecznej i politycznej separatystów, interwencję zbrojną oraz odstraszanie, poprzez demonstrację potencjału sił niekonwencjonalnych. Charakterystyczne dla tego konfliktu jest to, że ww. etapy zachodzą często na siebie i charakteryzują się różną intensywnością.*

[17] Bojówki miały zostać przeszkolone i wyposażone w Polsce – przyp. autora.

[18] R. Parafianowicz, M. Banasiak: *Teoria i praktyka*..., op.cit.

[19] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie przyszłości?*..., op.cit., s. 39–50.

[20] R. Parafianowicz, M. Banasik: *Teoria i praktyka*..., op.cit.

[21] H. Króliowski: *Działania specjalne w strategii wojskowej III RP.* Białystok 2005, s. 118.

[22] R. Jakubczak, R.M. Martowski: *Powszechna Obrona Terytorialna w cyberobronie i agresji hybrydowej*. Warszawa 2017, s. 174.

[23] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie przyszłości?*..., op.cit., s. 45.

Niezwykle istotne jest umiejętne wykorzystanie różnorodnych instrumentów ekonomicznych, politycznych oraz humanitarnych, co powinno się odbywać w połączeniu

Mimo wyraźnych oznak udziału regularnych sił zbrojnych, władze rosyjskie oficjalnie zaprzeczają udziałowi w konflikcie[24]. W tych działaniach chodzi o zdestabilizowanie państwa bez jednoczesnego wszczynania otwartej wojny po to, by w perspektywie długofalowej zablokować integrację Ukrainy z UE oraz NATO. *Wydarzenia na Ukrainie uświadomiły, że wojna hybrydowa może zostać wykorzystana przez jedną ze stron konfliktu do celowego ograniczania skali prowadzonych operacji zbrojnych po to, aby uniemożliwić określenie w sposób jednoznaczny stanu wojny oraz agresora, a tym samym zapobiec reakcji społeczności międzynarodowej*[25]. W działaniach poniżej progu wojny prowadzonych na Ukrainie uwagę należy zwrócić na działania informacyjne, które były niejako symptomem przyszłych działań. Już w latach poprzedzających konflikt Federacja Rosyjska prowadziła medialną ofensywę na Ukrainie, wykorzystując do tego rosyjskie koncerny medialne. Dzięki wykupieniu udziałów w ukraińskich mediach mogła bezpośrednio wpływać na społeczeństwo Ukrainy. Taka sytuacja stwarzała możliwości integracji prorosyjskich środowisk i aktywację rosyjskiej agentury[26].

Wynika z tego, że *w nowoczesnym świecie obok bezpieczeństwa lądowego, powietrznego, wodnego i przestrzeni kosmicznej bezpieczeństwo przestrzeni wirtualnej odgrywa coraz większą rolę. W dobie superszybkich komputerów, „chmur" przechowujących dane, wielofunkcyjnych smartfonów, duża część zadań administracji państwowej przenoszona jest do przestrzeni wirtualnej. Naraża to państwa na nowe niebezpieczeństwa oraz ataki, które mogą poważnie*

[24] R.Parafianowicz, M. Banasik: *Teoria i praktyka*..., op.cit.

[25] Ł. Skoneczny: *Wojna hybrydowa – wyzwanie*..., op.cit., s. 45.

[26] R. Parafianowicz, M. Banasik: *Teoria i praktyka*..., op.cit.

PIXABAY

z manipulowaniem nastrojami ludności zamieszkującej obszar konfliktu.

zdestabilizować ich funkcjonowanie[27]. Oprócz działań typowo informacyjnych niezwykle groźny i niebezpieczny staje się tzw. cyberterroryzm. Według Departamentu Obrony USA *cyberterroryzm to bezprawny atak lub groźba takiego ataku przeciwko komputerom, sieciom komputerowym lub informacjom przechowanym na nich, mający na celu zastraszenie lub wymuszenie na społeczeństwie lub rządzie danego kraju spełnienia określonych celów politycznych*[28]. W ostatnich czasach można zauważyć niebezpieczne zjawisko, jakim jest wykorzystywanie hakerów działających na zlecenie jednych państw przeciwko drugim. Działania te są bardzo często elementem działań podprogowych.

W systemach administracji rządowej Ukrainy znaleziono wirusa o nazwie Snake, służącego prawdopodobnie do szpiegowania i zaburzania systemów informatycznych, który zaatakował 84 strony administracji publicznej[29]. Miesiąc wcześniej, w dniu wyborów prezydenckich, Rosjanie dokonali cybersabotażu na strony Centralnej Komisji Wyborczej. Celem ataku, za którym stał „CyberBerkut", było usunięcie rezultatu wyborów w dniu wyborów prezydenckich. O tym, że cyberprzestrzeń na dobre wchodzi w skład działań podprogowych, może świadczyć fakt, iż Rosjanie rekrutują i ćwiczą „nową armię trolli internetowych", którzy mają za zadanie zmienić postrzeganie inwazji na Ukrainę. Ich zadaniem jest pisanie opinii, komentarzy, blogów przychylnych FR, a oczerniających Ukrainę czy jej sojuszników. Kolejnym przykładem takiego działania może być platforma medialna „Sputnik". Serwis ten zarządzany przez rosyjską agencję „Rossija Siegodnia" (dawniej „RIA Novosti") działa już w 14 krajach, w tym od niedawna i w naszym, *ukazując wielobiegunowy świat, w którym każde państwo ma swoje narodowe interesy, kulturę i tradycję*[30]. Według niego konflikt na Ukrainie jest *wynikiem polsko-amerykańskiego spisku sił wywiadowczych, który wymknął się spod kontroli po zorganizowaniu zamachu stanu na administrację Wiktora Janukowycza*[31].

JAKA PRZYSZŁOŚĆ?

Przytoczone przykłady jasno pokazują, że działania w ramach konfliktu poniżej progu wojny są niezwykle skuteczne. Prowadzone w sposób zaplanowany, przemyślany i dobrany do zdefiniowanego środowiska oddziaływania są doskonałą alternatywą dla działań konwencjonalnych. Ich zastosowanie daje możliwość nie tylko destabilizacji danego kraju czy regionu, lecz także umożliwia jego całkowity paraliż czy zajęcie jego części bądź całego terytorium. Jednocześnie możliwości te osiąga się bez wypowiadania wojny, co, jak wiadomo, wiąże się z o wiele poważniejszymi konsekwencjami, takimi jak: sankcje międzynarodowe, wyobcowanie na arenie międzynarodowej czy podjęcie działań militarnych przez społeczność międzynarodową. Biorąc pod uwagę dynamiczny rozwój cywilizacyjny, należy się liczyć z tym, iż działania poniżej progu wojny wpiszą się na stałe w kanony sztuki wojennej. ■

[27] P. Renn: *Wojna hybrydowa jako nowe zjawisko w sztuce wojennej XXI wieku.* Poznań 2016. http://refleksje.edu.pl/wp-content/uploads/2017/03/nr_13_Przemys%C5%82aw-Renn.pdf/. 1.01.2018.

[28] G. Weimann: *Cyberterrorism, How Real is the Threat? United States Institute for Peace.* Waszyngton 2004. http://www.usip.org/sites/default/files/sr119.pdf/. 23.03.2018.

[29] P. Górecki: *Cyberatak na Ukrainę. Trudno będzie udowodnić, że to Rosja.* „Gazeta Wyborcza", 13.03.2014. http://wyborcza.pl/1,76842,15614511,Cyberatak_ na_Ukraine__Trudno_bedzie_udowodnic__ze.html/. 1.01.2018.

[30] https://pl.sputniknews.com/. 26.12.2017.

[31] P. Renn: *Wojna hybrydowa...*, op.cit.

Współdziałanie zgrupowań aeromobilnych z jednostkami OT

WYKONYWANIE WSPÓLNIE ZADAŃ PRZEZ KOMPONENTY RÓŻNYCH RODZAJÓW SIŁ ZBROJNYCH WYMAGA JASNYCH I PRECYZYJNYCH USTALEŃ, BY OSIĄGNĄĆ EFEKT SYNERGII.

mjr dypl. SZRP Dariusz Dziuba

Autor jest zastępcą dowódcy – szefem Sztabu 18 Batalionu Powietrznodesantowego.

Wojska aeromobilne, w skład których wchodzą pododdziały kawalerii powietrznej, często wykorzystują manewr (w tym pionowy), by zaangażować się w walkę w wyznaczonym rejonie lub opanowanym obiekcie. Zdolności manewrowe zapewniają im śmigłowce, wspierając ich ogniem w trakcie działań prowadzonych na lądzie. Największym atutem tych pododdziałów jest możliwość tworzenia ognisk walki w ugrupowaniu przeciwnika. Z kolei wojska obrony terytorialnej to oddziały (pododdziały) formowane głównie z miejscowych sił, których cechą wyróżniającą jest przede wszystkim doskonała znajomość terenu w ich stałych rejonach odpowiedzialności.

ISTOTA

By zapewnić sukces wspólnej walki tych dwóch komponentów, oprócz jasno postawionego zadania bojowego musi zostać uzgodnione i zsynchronizowane współdziałanie pododdziału kawalerii powietrznej i pododdziału OT, w którego rejonie odpowiedzialności będzie ono wykonywane. W *Regulaminie działań wojsk lądowych* jeden z rozdziałów jest poświęcony temu zagadnieniu. Samo współdziałanie definiowane

Współdziałanie szwadronowej grupy bojowej z siłami OT znacznie wzmocni obronę obiektu, a tym samym zwiększy żywotność walczących pododdziałów.

ARKADIUSZ DWULATEK/COMBAT CAMERA DORSZ

jest jako *zamierzenia polegające na dokonywaniu ustaleń między jednostką walczącą a sąsiadem lub sąsiadami wykonującymi zadania z boku lub z przodu (poza pasem (rejonem) działań). Istota współdziałania sprowadza się do wspólnego działania przy zachowaniu autonomii wykonawców*[1]. Regulaminowe zapisy określają również warunki, jakie muszą zostać spełnione (rys.1), czyli:

– współdziałanie powinno dotyczyć minimum dwóch samodzielnych zgrupowań,

– musi być określony cel wspólnego działania,

– dowódcy zgrupowań powinni wyrazić zgodę na udział w osiągnięciu zdefiniowanego wspólnego celu,

– minimum jedna z jednostek musi wspierać działania drugiej.

Współdziałanie definiowane w doktrynie *Planowanie działań na szczeblu taktycznym w wojskach lądowych* to *uzgodnione działanie na korzyść jednego kooperanta bez bezpośredniego udziału przełożonego (przełożonych) dla realizacji wspólnego celu. Istota – działanie wspólne przy zachowaniu autonomii wykonawców*[2]. Biorąc pod uwagę obie przytoczone definicje, należy stwierdzić, że koniecznym atrybutem współdziałania jest obecność minimum dwóch podmiotów, a jego wyznacznikiem podjęcie dobrowolnej współpracy dla osiągnięcia celu działania. Podpułkownik doktor inżynier Artur Michalak w swojej monografii *Teoretyczne aspekty organizacji współdziałania wojsk lądowych i wojsk specjalnych w operacji* stwierdza, że *nadrzędnym atrybutem realizacji współpracy jest cel, który wyznacza wspólny kierunek i w pewien sposób – przez dążenie do jego osiągnięcia – jednoczy uczestników. Jednocześnie, wraz z chwilą jego osiągnięcia, powoduje zaniknięcie potrzeby współdziałania*[3].

W DZIAŁANIACH BEZPOŚREDNICH

Do zasadniczych zadań zgrupowań aeromobilnych należy zaliczyć:

– wspieranie nacierających zgrupowań w rozwijaniu powodzenia i zwiększaniu tempa działań;

– ubezpieczenie sił głównych w czasie przemieszczania, a także podczas prowadzenia działań opóźniających;

– wzbronienie zajęcia przez przeciwnika dogodnych rubieży i rejonów do wykonania kontrataków i przeciwuderzeń;

– osłona otwartych skrzydeł i luk w ugrupowaniu obronnym;

– blokowanie kierunków lub dróg przemieszczania się zgrupowań przeciwnika;

– wprowadzenie przeciwnika w błąd przez prowadzenie działań pozornych i demonstracyjnych;

– wzmocnienie sił na kierunku zagrożenia;

– paraliżowanie (naruszanie) systemu dowodzenia przeciwnika;

– utrzymywanie kontaktu z przeciwnikiem, przy jednoczesnym wykonywaniu niespodziewanych ataków na jego skrzydła i tyły;

– wzmocnienie wojsk walczących w okrążeniu lub wsparcie podczas ich planowanego wyjścia z okrążenia;

– obsadzenie pozycji ryglowych z jednoczesnym szturmem powietrznym na nacierającego przeciwnika;

– wykonywanie zadań jako odwód przeciwpancerny;

– ubezpieczenie i nadzorowanie obszaru rozmieszczenia[4].

Z kolei pododdziały wojsk obrony terytorialnej mogą realizować takie zadania, jak:

– obrona ważnych obiektów terenowych w ich stałych rejonach odpowiedzialności;

– prowadzenie rozpoznania patrolowego, w tym namierzanie i wskazywanie celów.

W trakcie walki obronnej może powstać sytuacja, gdy przeciwnik uzyska powodzenie i jedno ze skrzydeł związku taktycznego będzie zagrożone okrążeniem. Szwadronowej grupie bojowej może zatem zostać postawione zadanie blokowania i opóźniania natarcia przeciwnika do chwili podejścia w zagrożony rejon odwodu w sile wzmocnionej kompanii czołgów i przejścia do obrony. Na czas wykonania zadania zostanie ona wzmocniona grupą rozpoznawczą, drużyną przeciwlotniczą, czterema wyrzutniami pocisków Spike i drużyną saperów. Z informacji uzyskanych od przełożonego wynika, że w rejonie, w którym ma prowadzić działania szwadronowa grupa bojowa, walczy kompania lekkiej piechoty OT. Znajduje się ona w stałym rejonie odpowiedzialności (SRO) i jest w gotowości do wprowadzenia pododdziałów kawalerii powietrznej w rejon obiektu oraz do podjęcia wspólnej walki. Otrzymane zadanie i ocena terenu wskazują, że należy bronić miejscowości z węzłem dróg oraz nie dopuścić do uchwycenia przez przeciwnika przepraw stałych na pobliskiej przeszkodzie wodnej. Rejon przyszłych działań jest otoczony terenem lesistym z miejscami dogodnymi do lądowania od strony południowo-wschodniej oraz południowo-zachodniej. W przyjętym wariancie działania dowódca szwadronowej grupy bojowej we współdziałaniu z kompanią lekkiej piechoty opanowuje obiekt ALFA i organizuje jego obronę na zagrożonych kierunkach (rys. 2). W celu dezorganizowania działań przeciwnika przygotowuje na jego przedpolach zasadzki ogniowe, a także niszczy infrastrukturę drogową, utrzymując obiekt do czasu zluzowania grupy przez siły odwodu. Zatwierdzony sposób działania dzieli na trzy etapy.

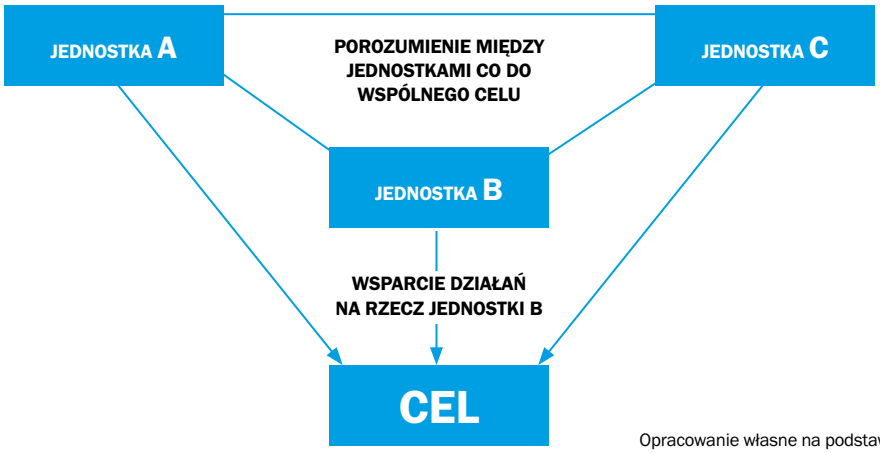
[1] *Regulamin działań wojsk lądowych.* DWLąd, Warszawa 2009, s. 267.

[2] *Planowanie działań na szczeblu taktycznym w wojskach lądowych. DD/3.2.5.* DWLąd, Warszawa 2006, s. 15.

[3] A. Michalak: *Teoretyczne aspekty organizacji współdziałania wojsk lądowych i wojsk specjalnych w operacji.* AON, Warszawa 2016, s. 65.

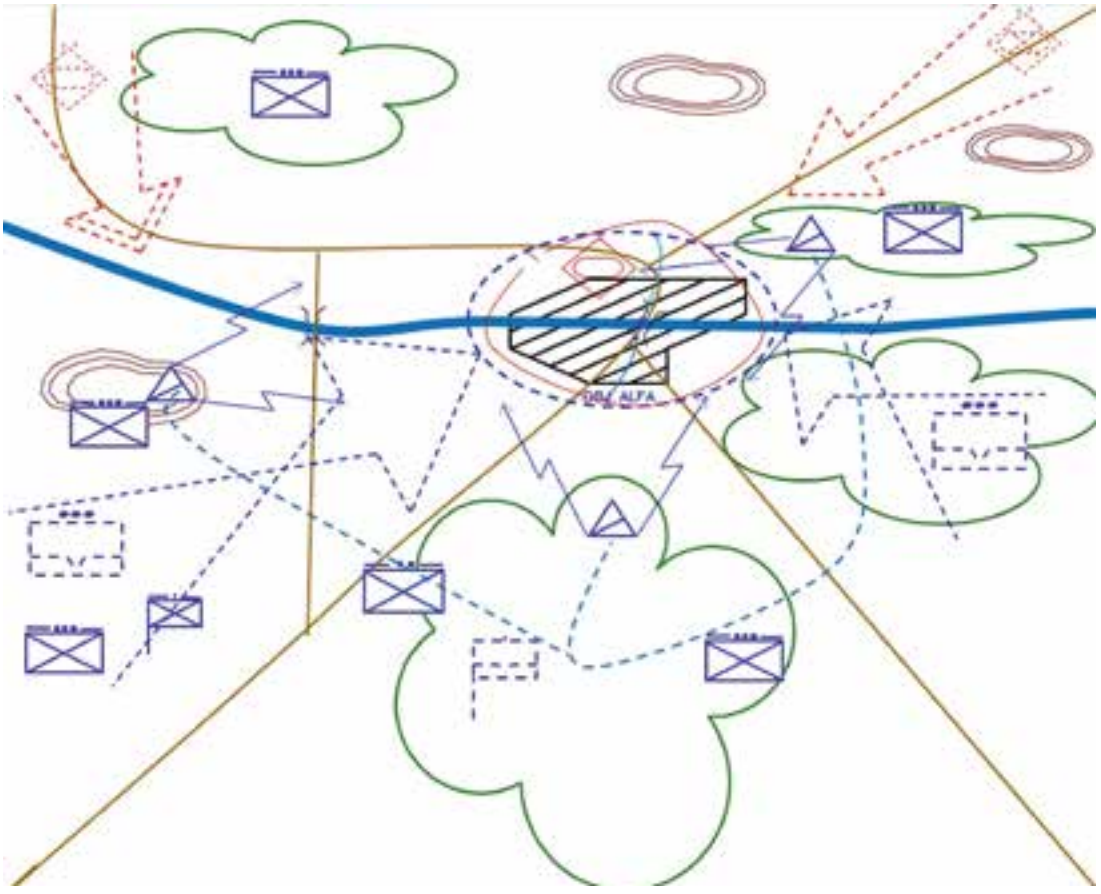
[4] J. Joniak: *Zasadnicze zadania zgrupowań aeromobilnych w operacji.* AON, Warszawa 2003, s. 26.

RYS. 1. SCHEMAT WSPÓŁDZIAŁANIA



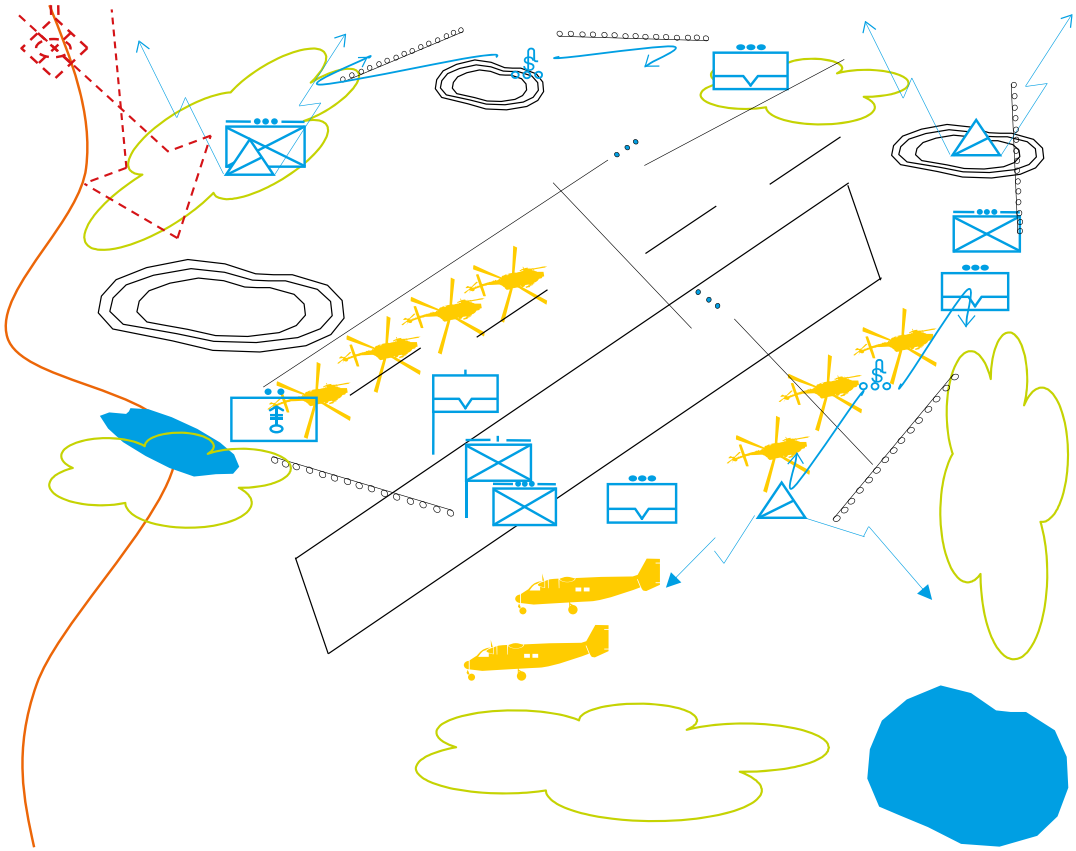
Opracowanie własne na podstawie: *Regulamin działań wojsk lądowych*. DWLąd, Warszawa 2009.

RYS. 2. WSPÓŁDZIAŁANIE SZWADRONOWEJ GRUPY BOJOWEJ Z KOMPANIĄ LEKKIEJ PIECHOTY W OBRONIE OBIEKTU (WARIANT)



Opracowanie własne.

RYS. 3. WARIANT WSPÓŁDZIAŁANIA SZWADRONOWEJ GRUPY BOJOWEJ Z KOMPANIĄ LEKKIEJ PIECHOTY



Opracowanie własne.

Pierwszy to wysłanie elementów rozpoznawczych i nawiązanie kontaktu z dowódcą kompanii lekkiej piechoty, a także zapoznanie go z otrzymanym zadaniem i sposobem jego wykonania. Ponadto ustalenie możliwości wsparcia szwadronowych elementów rozpoznawczych oraz wybór dogodnych miejsc na rozmieszczenie posterunków obserwacyjnych. Kolejny etap to zajęcie obiektu i zorganizowanie obrony, a także określenie obiektów, których mogą bronić elementy ugrupowania bojowego kompanii lekkiej piechoty. Ponadto przygotowanie zasadzek ogniowych na kierunkach przemieszczania się przeciwnika. Ostatni etap to współdziałanie z elementami kompanii lekkiej piechoty podczas obrony obiektu do chwili zluzowania.

W każdym z etapów walki główny wysiłek zostaje skupiony na drodze podejścia zgrupowań przeciwnika. Ponadto część kompanii OT jest zaangażowana w wykonanie zasadzek ogniowych. Przyjęte ugrupowanie bojowe to jeden rzut z odwodem. W pierwszym rzucie przewidziano dwa plutony szturmowe z dwiema wyrzutniami pocisków Spike, a także dwoma saperami w każdym plutonie. Natomiast w odwodzie – pluton szturmowy, drużynę przeciwlotniczą oraz dwóch saperów. Punkt dowódczo-obserwacyjny rozmieszczono na skraju lasu. Na każdym etapie walki działanie szwadronowej grupy bojowej jest wspierane zarówno informacyjnie, jak i ogniowo przez pododdziały lekkiej piechoty. Za korzystne w tym wariancie należy uznać:

– wykonanie manewru pionowego i zajęcie obiektu ALFA,

– równoczesne z organizacją obrony przygotowanie zasadzek na zagrożonym kierunku,

– stworzenie możliwości zorganizowania obrony przez siły odwodu.

Współdziałanie będzie polegało w tym przypadku przede wszystkim na ustaleniu:

– możliwości zbierania przez siły OT informacji o przeciwniku na zagrożonym kierunku;

– liczby zasadzek organizowanych siłami OT oraz szwadronowej grupy bojowej na drogach podejścia;

– możliwości wskazywania celów przez kompanię OT dla artylerii lub przekazywania ich współrzędnych dowódcy szwadronowej grupy bojowej;

– obiektów, których będą bronić siły OT;

– relacji łączności z dowódcą kompanii lekkiej piechoty i określonych sygnałów rozpoznawczych, jak też relacji dowodzenia pododdziałami OT, które będą się bronić w obiekcie ALFA.

Podsumowując, należy stwierdzić, że obecność żołnierzy OT w rejonie działania usprawni zajęcie rejonu przez szwadronową grupę bojową, jak również zapewni dodatkowe wsparcie w trakcie przygotowania obrony i walki z przeciwnikiem.

W TYLNYM PASIE OBRONY

Główne zadania zgrupowań aeromobilnych w tym rejonie obrony to:

– ochrona i obrona obiektów o szczególnym znaczeniu;

– przeciwdziałanie rozpoznaniu przeciwnika;

– osłona przemieszczania elementów ugrupowania bojowego (operacyjnego);

– realizacja zadań jako odwód przeciwpancerny dowódcy dywizji (korpusu);

– zwalczanie desantów bądź grup partyzanckich przeciwnika (odwód przeciwdesantowy);

– likwidacja akcji zbrojnych i sabotażowych[5].

Z kolei wojska obrony terytorialnej zajmujące stałe rejony odpowiedzialności mogą na korzyść wojsk operacyjnych realizować takie zadania, jak:

– ochrona i obrona obiektów oraz infrastruktury krytycznej państwa,

– prowadzenie działań informacyjnych – namierzanie i izolowanie grup dywersyjno-rozpoznawczych oraz aeromobilnych grup rozpoznawczych,

– wykonywanie zadań przeciwdywersyjnych,

– podejmowanie działań przeciwdesantowych.

Jednym z zadań szwadronowej grupy bojowej będzie ochrona i obrona lotniska, które – jak wynika z oceny przeciwnika – będzie chciał opanować w nienaruszonym stanie. W tym wariancie grupa wzmocniona drużyną przeciwlotniczą, czterema wyrzutniami pocisków Spike, drużyną saperów i plutonem moździerzy M-98 otrzyma zadanie ochrony i obrony lotniska. Zdobyte dodatkowe informacje wskazują, że lotnisko znajduje się w stałym rejonie odpowiedzialności (SRO) kompanii lekkiej piechoty. Na podstawie zaś analizy zadania oraz oceny terenu przyszłych działań stwierdzono, że jest ono położone w lesie, z miejscami dogodnymi do lądowania zgrupowań desantowych przeciwnika od strony północno-zachodniej i wschodniej oraz północno-wschodniej. Ponadto przeciwnik prawdopodobnie będzie chciał je opanować, lądując bezpośrednio na nim lub w jego pobliżu. Z decyzji podjętej przez dowódcę szwadronowej grupy bojowej wynika, że zamierza on bronić obiektu wspólnie z kompanią OT oraz pododdziałami, które znajdują się na lotnisku. Główny wysiłek zostanie skupiony na utrudnianiu działania naziemnym zgrupowaniom przeciwnika dążącym do jego zajęcia, a we współdziałaniu z pododdziałami ochrony lotniska – na niedopuszczeniu do jego opanowania z powietrza. Przyjęte ugrupowanie bojowe to jeden rzut z odwodami (rys. 3). W pierwszym rzucie będą dwa plutony szturmowe z dwiema wyrzutniami pocisków Spike, a także dwoma saperami w każdym plutonie. Odwód będą stanowić pluton szturmowy, drużyna przeciwlotnicza oraz dwóch saperów. Punkt dowódczo-obserwacyjny zostanie rozmieszczony na skraju lasu od strony południowej. Główny wysiłek będzie skupiony na lewym skrzydle, gdzie znajdują się dogodne drogi podejścia dla pojazdów pancernych i opancerzonych przeciwnika.

Istotą podjętej decyzji jest wykorzystanie potencjału kompanii lekkiej piechoty w ochronie i obronie lotniska przed siłami naziemnymi przeciwnika. Działania podzielono na trzy etapy. Pierwszy to zorganizowanie sytemu ochrony i obrony we współdziałaniu z siłami OT. Kolejny to obrona przed atakami zgrupowań lądowych przeciwnika. Ostatni etap to odzyskanie lotniska w razie wysadzenia na nim desantu powietrznego. Na każdym etapie walki działanie szwadronowej grupy bojowej będzie wspierane informacyjnie przez elementy rozpoznawcze kompanii lekkiej piechoty.

Zorganizowanie współdziałania będzie polegało przede wszystkim na:

– ustaleniu sposobów przekazywania informacji z posterunków obserwacyjnych utworzonych siłami wojsk obrony terytorialnej;

– określeniu zadań, jakie mogą być wykonywane przez kompanię lekkiej piechoty na drogach podejścia do obiektu;

– uzgodnieniu sygnałów porozumiewania się z elementami ochrony lotniska w sytuacji lądowania desantu przeciwnika;

– ustaleniu sposobów wsparcia przez siły OT walki z desantem przeciwnika;

– określeniu relacji dowodzenia między dowódcą szwadronowej grupy bojowej i dowódcą kompanii lekkiej piechoty.

Z rozważań tych można wyciągnąć wniosek, że współdziałanie szwadronowej grupy bojowej z siłami OT znacznie wzmocni obronę obiektu, a tym samym zwiększy żywotność walczących pododdziałów. Podsumowując, należy stwierdzić, że współdziałanie kawalerii powietrznej i wojsk obrony terytorialnej to przede wszystkim realizacja wspólnego celu. By go osiągnąć, dowódcy poszczególnych szczebli dowodzenia w jasno określony sposób realizują wspólnie otrzymane zadanie. Aby ich skuteczność była faktycznie efektywniejsza, należałoby w procesie szkolenia zwracać więcej uwagi na organizowanie współdziałania zgrupowań aeromobilnych z jednostkami OT. ■

[5] Ibidem, s. 31.

Urządzanie i utrzymanie **przepraw – dowodzenie**

PROWADZENIE DZIAŁAŃ TAKTYCZNYCH W REJONIE CIEKU WODNEGO WYMUSZA KONIECZNOŚĆ REALIZACJI WIELU OKREŚLONYCH PRZEDSIĘWZIĘĆ INŻYNIERYJNYCH PRZEZ WOJSKA POKONUJĄCE PRZESZKODĘ WODNĄ.

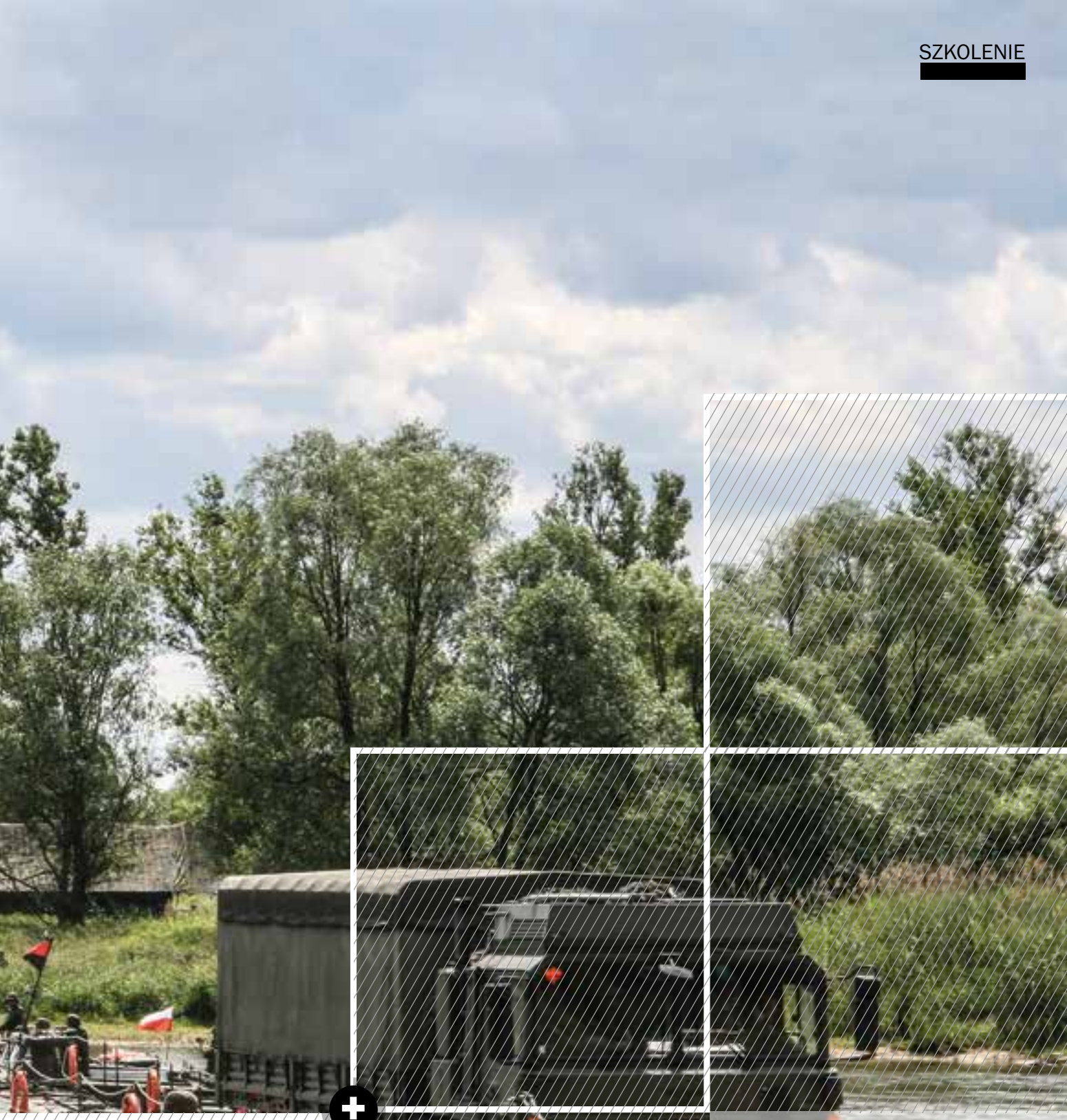
ppłk dr inż. Krzysztof Wysocki

Autor jest kierownikiem Zakładu Inżynierii Wojskowej, Maskowania i Ochrony Wojsk Instytutu Wsparcia i Zabezpieczenia Działań Wydziału Wojskowego ASzWoj.

Specyfika kierowania działaniami inżynieryjnymi w czasie pokonywania przeszkody wodnej warunkuje określone aspekty dowodzenia wojskami. Opracowanie koncepcji, planów i dokumentów rozkazodawczych wymaga od specjalistów wojsk inżynieryjnych rozległej wiedzy taktyczno-operacyjnej, technicznej i specjalistycznej, a także obiektywizmu i realizmu w ocenie sytuacji. Wykonując wszelkie czynności z tym związane, muszą uwzględniać konkretne determinanty środowiskowe wpływające na urządzanie i utrzymania tymczasowych przepraw przez przeszkody wodne, przede wszystkim zaś umiejętnie wykorzystywać ich właściwości taktyczno-operacyjne sprzyjające prowadzeniu działań taktycznych przez wojska własne.

OGNIWA KIEROWANIA DZIAŁANIAMI INŻYNIERYJNYMI

Należy tu wymienić dowództwa jednostek ogólnowojskowych oraz dowództwa oddziałów (pododdziałów) wojsk inżynieryjnych (WInż). Ich zadania są uwarunkowane umiejscowieniem i rolą organów



Kierowanie działaniami inżynieryjnymi przez dowództwo ZT (oddziału) w czasie urządzania i utrzymania przepraw należy do poszczególnych osób funkcyjnych SD w zależności od posiadanych przez nie uprawnień oraz zakresu ich odpowiedzialności.

BOGUSŁAW PILITOWSKI

dowodzenia wojsk inżynieryjnych poszczególnych szczebli. Planowanie przepraw[1] i dowodzenie nimi należy do obowiązku *dowódcy związku taktycznego (oddziału)*, którego elementy ugrupowania bojowego prowadzą działania w rejonie (pasie), w którym urządza się przeprawę[2]. W zależności od otrzymanego zadania, rodzaju prowadzonych działań, sytuacji operacyjno-taktycznej, właściwości przeszkody wodnej i przyległego terenu, a także posiadanych sił i środków oraz charakteru działań przeciwnika – określa on ugrupowanie bojowe oraz kolejność przekraczania przeszkody i wymagania, jakie muszą spełniać punkty przeprawy. W zorganizowaniu wymienionych czynności jego bezpośrednim doradcą jest specjalista wojsk inżynieryjnych – *szef sekcji wojsk inżynieryjnych* związku taktycznego (oddziału).

W wojskach lądowych struktura organizacyjna dowództw ZT, oddziału i pododdziału (do szczebla batalionu) jest następująca: dowódca, zastępca dowódcy, sekcja dowódcy, sekcja ochrony informacji niejawnych[3], szef sztabu (wraz z podległymi pionami) oraz komenda stanowiska dowodzenia (SD). Szefowi sztabu podlegają bezpośrednio szefowie pionów: operacyjnego, wsparcia bojowego i wsparcia, z kolei w skład komendy SD wchodzą węzeł łączności i grupa zabezpieczenia.

Kierowanie działaniami inżynieryjnymi przez dowództwo ZT (oddziału) w czasie urządzania i utrzymania przepraw należy do poszczególnych osób funkcyjnych SD w zależności od posiadanych przez nie uprawnień oraz zakresu ich odpowiedzialności. Jednym z ważniejszych elementów SD, który odpowiada za kierowanie tymi działaniami, jest sekcja wojsk inżynieryjnych. Powinna ona w sposób ciągły monitorować sytuację, planować i koordynować realizację bieżących i przyszłych zadań inżynieryjnych, precyzować zadania dla oddziałów (pododdziałów) w terenie oraz uczestniczyć w odprawach i rekonesansach organizowanych w procesie dowodzenia. Analiza literatury przedmiotu oraz dokumentów normatywnych[4] obowiązujących w SZRP wskazuje, że obsadzenie specjalistami WInż poszczególnych SD jest uzależnione od wielkości struktur organizacyjnych określonego szczebla dowodzenia. Na poziomie taktycznym w dowództwie ZT (oddziału) w pionie wsparcia bojowego występuje szef sekcji WInż oraz dwóch–trzech specjalistów wojsk inżynieryjnych. W zależności od przyjętych rozwiązań w danym ZT (oddziale) sekcja WInż realizuje zadania wraz z pozostałymi specjalistami wojsk inżynieryjnych[5], a miejscem ich pracy jest pion operacyjny oraz pion wsparcia działań – struktury organów dowodzenia SD związku taktycznego (oddziału) ogólnowojskowego. W dowództwie batalionu zmechanizowanego (czołgów) szczegółowymi zagadnieniami inżynieryjnymi zajmuje się najczęściej podoficer – specjalista WInż (tab. 1).

Szefowie sekcji wojsk inżynieryjnych ZT (oddziałów) odpowiadają bezpośrednio za planowanie zadań w ramach wsparcia inżynieryjnego działań taktycznych oraz za organizowanie działań inżynieryjnych, w tym za[6]:

– wypracowanie rozwiązań w tym zakresie w ramach procesu decyzyjnego dowódców ZT (oddziałów) ogólnowojskowych oraz oddziałów pozostałych rodzajów wojsk;

– opracowanie wstawek i załączników do dokumentów dowodzenia;

– koordynację działań inżynieryjnych.

Oprócz tego sekcja odpowiada za[7]:

– doradzanie dowódcy i innym elementom stanowiska dowodzenia oraz dowódcom podległych oddziałów we wszystkich kwestiach dotyczących zagadnień inżynieryjnych;

– ciągłe monitorowanie i ocenę sytuacji inżynieryjnej oraz stopnia realizacji zadań inżynieryjnych, a także aktualnego położenia i możliwości bojowych sił wykonujących te zadania;

– planowanie oraz koordynację realizacji wszystkich zadań inżynieryjnych w pasie (rejonie) odpowiedzialności;

– opracowanie dokumentów bojowych: planów działań inżynieryjnych, załączników i meldunków o sytuacji i realizowanych zadaniach inżynieryjnych;

– przygotowanie i organizowanie współdziałania między pododdziałami wojsk inżynieryjnych i elementami ugrupowania bojowego oraz siłami wspierającymi;

– kontrolowanie (z upoważnienia dowódcy) podwładnych i udzielanie im pomocy w organizowaniu zadań inżynieryjnych.

Ponadto w ramach organizowania wsparcia i zabezpieczenia inżynieryjnego urządzania i utrzymania przepraw sekcja WInż jest odpowiedzialna za:

---

[1] Przeprawa – zorganizowane przemieszczenie wojsk przez trudny teren, zwykle przez naturalną lub sztuczną przeszkodę wodną. Zob. *Instrukcja – pokonywanie przeszkód wodnych przez pododdziały wojsk lądowych.* DWLąd, Warszawa 2013, s. 320.

[2] Dowódca ten odpowiada również za zagwarantowanie swobody ruchu wojskom przekraczającym rejon jego ugrupowania. Ibidem, s. 11.

[3] Sekcja dowódcy i sekcja ochrony informacji niejawnych występują w strukturze organu dowodzenia SD batalionu w zależności od struktury organizacyjnej danego pododdziału.

[4] Zob. S. Kowalkowski (red. nauk.), W. Kawka: *Rola i zadania organów dowodzenia wojsk inżynieryjnych w procesie decyzyjnym. „DOWODZENIE-INŻ"*. AON, Warszawa 2005; *Instrukcja wojennego systemu dowodzenia Sił Zbrojnych RP*. SG WP, sygn. 1667/2014.

[5] W zależności od struktury organizacyjnej danego ZT (oddziału) w pionie operacyjnym oraz pionie wsparcia działań występują etaty dla oficerów – specjalistów WInż (np. w G(S)-2, G(S)-3, G(S)-4).

[6] Por. *Regulamin działań wojsk inżynieryjnych wojsk lądowych (tymczasowy).* DWLąd, Warszawa 2011, s. 105.

[7] Zob. P. Cieślar (red. nauk.), W. Kawka, S. Kowalkowski: *Wykorzystanie wojsk inżynieryjnych w działaniach taktycznych*. AON, Warszawa 2008, s. 285.

TABELA 1. INŻYNIERYJNE ELEMENTY STANOWISK DOWODZENIA ZT (ODDZIAŁÓW, PODODDZIAŁÓW) WOJSK LĄDOWYCH (WARIANT)

Nazwa komórki inżynieryjnej	Nazwa funkcji	Stopnie etatowe i liczba osób	Razem osób
Związek taktyczny			
Sekcja WInż pion wsparcia bojowego	szef sekcji WInż	podpułkownik – 1	4
	specjalista	major/kapitan – 1/1	
	podoficer	chorąży – 1	
Oddział			
Sekcja WInż pion wsparcia bojowego	szef sekcji WInż	major – 1	2–3
	specjalista*	kapitan – 1*	
	podoficer	chorąży – 1	
Pododdział			
Pion operacyjny	instruktor ds. inżynieryjnych	chorąży – 1	1

* w zależności od etatu obsady stanu osobowego danego oddziału

Opracowanie własne na podstawie materiałów pozyskanych z Zarządu Inżynierii Wojskowej Inspektoratu Rodzajów Wojsk Dowództwa Generalnego Rodzajów Sił Zbrojnych.

• ustalenie położenia w rejonie kierowania działaniami inżynieryjnymi;
• przeprowadzenie rozpoznania studyjnego przeszkody wodnej;
• zorganizowanie rozpoznania inżynieryjnego przeszkody wodnej i dróg prowadzących do niej;
• dokonanie analizy i oceny inżynieryjnej przeciwnika oraz środowiska walki pod kątem ich wpływu na działania wojsk własnych, w tym przede wszystkim danych uzyskanych z rozpoznania przeszkody wodnej, przepraw i obiektów hydrotechnicznych;
• określenie na podstawie przeprowadzonej oceny wojsk własnych i wariantów działania:
– priorytetów wsparcia inżynieryjnego,
– zadań, terminów i miejsc ich wykonywania przez pododdziały wojsk inżynieryjnych, czyli ugrupowanie wojsk inżynieryjnych,
– zakresu zadań przewidzianych do realizacji przez inne rodzaje wojsk,
– niezbędnych zmian w podporządkowaniu sił inżynieryjnych;
• skoordynowanie z pozostałymi komórkami strukturalno-funkcjonalnymi SD zakresu planowanych zadań, sporządzenie kalkulacji dotyczącej przeprawy (odcinka przeprawy) ZT (oddziału) oraz opracowanie grafiku (harmonogramu) jej wykonania;
• współudział w synchronizacji działań przewidzianych do realizacji przez pozostałe rodzaje wojsk oraz zadań zabezpieczających działanie pododdziałów WInż;
• opracowanie planu działań inżynieryjnych, załącznika inżynieryjnego do rozkazu bojowego oraz informacji inżynieryjnych do pozostałych dokumentów dowodzenia;
• uczestniczenie w stawianiu zadań przez dowódcę ZT (oddziału) podległym dowódcom (oddziałów, pododdziałów).

W ramach kierowania działaniami inżynieryjnymi specjaliści wojsk inżynieryjnych mogą współpracować ze specjalistami z różnych komórek funkcjonalnych SD lub bezpośrednio z dowódcą ZT (oddziału). Kontakt z nim oznacza zwykle sprawowanie funkcji doradczej. Natomiast wymiana informacji i współpraca między poszczególnymi komórkami odbywa się dzięki funkcjonowaniu powiązań wewnątrz stanowisk dowodzenia. Umożliwiają one dokonywanie wielu uzgodnień przez specjalistów wojsk inżynieryjnych z innymi elementami strukturalno-funkcjonalnymi SD[8] oraz zapewniają przepływ informacji wykorzystywanych przez różne komórki SD.

Dowódcy oddziałów (pododdziałów) inżynieryjnych dowodzą podległymi im elementami oraz ponoszą odpowiedzialność za realizację zadań wsparcia inżynieryjnego. Ponadto zapewniają podległym dowódcom warunki do planowania, organizowania i wykonania zadań inżynieryjnych.

Odpowiadają oni za:
– planowanie działań podległych wojsk w ramach wsparcia inżynieryjnego działań;
– opracowanie dokumentów dowodzenia;

[8] *Struktura organizacyjno-funkcjonalna dotyczy zbioru stosunków organizacyjnych, których wyrazem są określone więzi organizacyjne. Mianem więzi organizacyjnych można określić utrwalone drogi przepływu informacji między elementami danej organizacji (więzi wewnętrzne) bądź między organizacją a systemem wyższego przełożonego, podwładnych i pozostałymi ogniwami otoczenia (więzi zewnętrzne).* Zob. S. Kowalkowski: *Planowanie zadań inżynieryjnych.* AON, Warszawa 2010, s. 109.

– realizację zadań wsparcia inżynieryjnego w trakcie działań bojowych;

– organizację współdziałania między oddziałami i pododdziałami wojsk inżynieryjnych oraz z elementami pozamilitarnymi biorącymi udział w wykonywaniu zadań wsparcia inżynieryjnego.

Współdziałanie dowódców oddziałów i pododdziałów wojsk inżynieryjnych z oddziałami (pododdziałami) ogólnowojskowymi oraz pozostałych rodzajów wojsk obejmuje:

– wymianę informacji o przeciwniku, jego możliwościach i zamiarach działania;

– opracowanie i przygotowanie danych do dokumentów bojowych;

– organizowanie wykonywania zadań przez wojska inżynieryjne na korzyść danego rodzaju wojsk;

– realizowanie zadań wsparcia inżynieryjnego;

– osłonę oddziałów (pododdziałów) wojsk inżynieryjnych podczas działania;

– osłonę i obronę obiektów inżynieryjnych (np. mostów, jazów itp.);

– organizowanie dowozu technicznych środków bojowych i materiałowych wojsk inżynieryjnych oraz remontu sprzętu inżynieryjnego.

Podczas pokonywania przeszkody wodnej wojskami dowodzi się ze stanowisk dowodzenia z uwzględnieniem specyfiki działań prowadzonych w rejonie przeszkody wodnej.

W wojskach lądowych na szczeblu związku taktycznego, oddziału i pododdziału organizuje się następujące rodzaje stanowisk dowodzenia[9]:

– w związku taktycznym: stanowisko dowodzenia (SD), zapasowe stanowisko dowodzenia (ZSD) oraz doraźnie – wysunięte stanowisko dowodzenia (WSD) i powietrzny punkt dowodzenia (PPD);

– w oddziałach wojsk (zmechanizowanych, pancernych): stanowisko dowodzenia (SD), zapasowe stanowisko dowodzenia (ZSD) oraz doraźnie – punkt dowódczo-obserwacyjny (PDO);

– w oddziałach wojsk inżynieryjnych i w batalionach wojsk lądowych: stanowisko dowodzenia (SD) oraz doraźnie – punkt dowódczo-obserwacyjny (PDO);

– w pododdziałach inżynieryjnych (szczebel kompanii): najczęściej punkt dowodzenia (PD).

Wysunięte stanowisko dowodzenia dywizji oraz stanowiska dowodzenia brygad rozwija się na brzegu wyjściowym w rejonie umożliwiającym dowódcy dywizji śledzenie przebiegu przeprawy sił głównych, a dowódcy brygady – obserwowanie pokonywania przeszkody wodnej przez pododdziały przynajmniej na głównym kierunku.

Stanowiska dowodzenia podczas pokonywania przeszkody wodnej przesuwa się tak, by można było skutecznie dowodzić wojskami oraz zachować łączność ze współdziałającymi związkami taktycznymi (oddziałami, pododdziałami) i nadrzędnym dowództwem w czasie podchodzenia do niej oraz jej forsowania, a także działania na przeciwległym brzegu.

W sytuacji pokonywania przeszkód wodnych szczególne znaczenie ma właściwa organizacja podchodzenia do niej kolejnych rzutów bojowych oraz poszczególnych pododdziałów. Dotyczy to zarówno okresu przed rozpoczęciem działań na przeszkodzie wodnej, jak i samej przeprawy, i ma na celu zapewnienie właściwego narastania sił i środków na przeciwległym brzegu. Dla zapewnienia właściwego przebiegu zadań związanych z urządzaniem i utrzymaniem przepraw wyznacza się osoby funkcyjne oraz służbę porządkowo-ochronną.

Analiza literatury oraz dokumentów normatywnych[10] pozwoliła na identyfikację poszczególnych ogniw kierowania działaniami inżynieryjnymi na potrzeby urządzania i utrzymania przepraw. Do osób i zespołów funkcyjnych odpowiedzialnych za urządzenie i utrzymanie przepraw należy zaliczyć[11]:

– dowódcę przeprawy (forsowania) – DP,

– dowódcę odcinka przeprawy (forsowania) – DOP,

– komendanta odcinka przeprawy (forsowania) – KOP,

– 1–2 pomocników komendanta odcinka przeprawy (forsowania) – PKOP,

– dowódcę punktu przeprawy – DPP,

– 1–2 pomocników dowódcy punktu przeprawy – PDPP,

– 1–2 inżynieryjne posterunki kierowania ruchem (regulacji ruchu) – IPKR,

– inżynieryjny posterunek obserwacyjny – IPO,

– dowódców środków przeprawowych – DŚP,

– grupę ratunkowo-ewakuacyjną – GRE,

– pododdziały dyżurne, warty i patrole,

– punkt medyczny.

Dowódcą przeprawy (forsowania) jest dowódca oddziału (związku taktycznego). Jest on odpowiedzialny za terminowe urządzenie przeprawy oraz za utrzymanie jej w pełnej sprawności w czasie przeprawiania wojsk. W celu zapewnienia pełnienia funkcji dowodzenia w rejonie przeszkody wodnej dowódca ten wydziela z podległego sztabu określone osoby funkcyjne, które w ramach grupy operacyjnej realizują zadania na wysuniętym stanowisku dowodzenia lub w punkcie dowódczo-obserwacyjnym. Do składu doraźnie funkcjonującego stanowiska dowodzenia celowe jest wyznaczenie *specjalistów do spraw*: operacyj-

[9] Zob. J. Posobiec, S. Wronka, W. Łydka: *Identyfikacja rodzajów, typów, a także struktury organizacyjnej stanowisk i punktów dowodzenia oraz ich przeznaczenie i główne zadania.* AON, Warszawa 2010, s. 39–40.

[10] Opracowano na podstawie analizy dostępnej literatury: *Instrukcja – pokonywanie przeszkód wodnych*...,op.cit.; J. Parzewski: *Zabezpieczenie inżynieryjne forsowania przeszkód wodnych przez oddział (związek taktyczny).* AON, Warszawa 1996; S. Lang: *Przeprawy (podręcznik).* MON, Warszawa 1979.

[11] Por. *Instrukcja – pokonywanie przeszkód wodnych*..., op.cit., s. 243.

SYLWIA GUZOWSKA

DOWÓDCA ODCINKA PRZEPRAWY (FORSOWANIA) DO PEŁNIENIA FUNKCJI DOWODZENIA W REJONIE PRZESZKODY WODNEJ WYDZIELA Z PODLEGŁEGO SZTABU OKREŚLONE OSOBY FUNKCYJNE.

nych (ochrony wojsk), kierowania ruchem wojsk, inżynieryjnych, zabezpieczenia działań bojowych, łączności oraz rozpoznania i walki elektronicznej. Na osobach tych spoczywa odpowiedzialność za kierowanie ochroną i obroną rejonu przeprawy, za kontrolę ruchu wojsk oraz sprawdzenie terenu przyległego do przeszkody wodnej. Ponadto odpowiadają one za monitorowanie realizacji zadań planowanych do wykonania przez podległe wojska. Na WSD (PDO) powinni zostać skierowani *łącznicy* z przeprawianych jednostek wojskowych. Ich zadaniem jest przekazywanie informacji swoim dowódcom o zmianach wprowadzanych do przyjętego planu (harmonogramu) forsowania (przeprawy) ze względu na zakłócenia systemu dowodzenia i łączności.

Dowódca przeprawy (forsowania) wyznacza *dowódcę* (dowódców) *jej odcinka*. W sytuacji pokonywania przeszkody wodnej przez pododdział bojowy na środkach innych niż inżynieryjne może nim być jego dowódca[12]. Natomiast jeżeli przeprawa jest urządzana z wykorzystaniem środków inżynieryjnych, jest nim dowódca pododdziału (oddziału) przeprawowego wydzielonego do tego zadania.

Dowódca odcinka przeprawy (forsowania) jest odpowiedzialny za techniczne jej aspekty, czyli[13]:

– urządzenie i utrzymanie przeprawy (wjazdów i wyjazdów),

– utrzymanie w stałej gotowości mostów, promów i środków desantowo-przeprawowych,

– kierowanie wojsk na przeprawę,

– dowodzenie służbą porządkowo-ochronną,

– dowodzenie grupą ratunkowo-ewakuacyjną,

– monitorowanie sytuacji technicznej i samej przeprawy.

Dowódca ten do pełnienia funkcji dowodzenia w rejonie przeszkody wodnej wydziela z podległego sztabu określone osoby funkcyjne, które w ramach grupy operacyjnej wykonują zadania w punkcie do-

[12] Na przeprawach w bród i przeprawach czołgów pod wodą oraz na desantowych przeprawach pododdziałów wyposażonych w pływające transportery opancerzone dowódców przepraw wyznacza się z grona oficerów (dowódców lub zastępców) przeprawiających się pododdziałów.

[13] Zob. *Instrukcja – pokonywanie przeszkód wodnych...,* op.cit., s. 38.

wódczo-obserwacyjnym (PDO).W punkcie tym powinni działać oficerowie odpowiedzialni za: urządzenie przepraw, kierowanie ruchem wojsk i ich ochronę oraz elementy zabezpieczenia działań bojowych.

Do zadań zaś *grupy operacyjnej* w PDO należy zorganizowanie[14]:

– ubezpieczenia dróg, rejonów wyczekiwania i wyjściowych do natarcia, które wyznaczono na obu brzegach przeszkody wodnej, oraz terenu przyległego do przeszkody wodnej od rubieży wyjściowej do rubieży wyrównania;

– kierowania ruchem wojsk, czyli utrzymanie ustalonego tempa na przeprawach oraz zapewnienie elastyczności i płynności ruchu, unikanie zatorów, kontrolowanie przemieszczania pododdziałów oraz sprzętu zgodnie z grafikiem (harmonogramem) przepraw;

– kontroli terenu, tzn. koordynowanie wykorzystania terenu przez pododdziały znajdujące się w pobliżu przeszkody wodnej, w rejonach wyczekiwania, ześrodkowania i zbiórek, a także sprawdzenie rozmieszczenia środków przeprawowych i elementów wspierających przeprawy;

– wsparcia przepraw, to jest wsparcia: inżynieryjnego (środki przeprawowe i ich załogi oraz obsługi), technicznego, medycznego i logistycznego oraz innych jego rodzajów, co będzie wynikać z sytuacji bojowej w rejonie przeprawiania się wojsk.

W sytuacji gdy główny wysiłek został przeniesiony z przeprawy na inne zadania, dowodzenie odcinkiem przeprawy – kierowanie ruchem wojsk może być przekazane innej jednostce, w tym wojskom inżynieryjnym utrzymującym przeprawy.

Komendant przeprawy (forsowania) znajduje się bezpośrednio przy przeprawie i podlega dowódcy jej odcinka. Zazwyczaj jest nim dowódca lub oficer pododdziału wojsk inżynieryjnych wydzielony do urządzenia przeprawy. W ramach pełnionej funkcji do jego zadań należy zorganizowanie:

– kierowania ruchem wojsk, obejmującego utrzymanie ustalonego tempa na przeprawach oraz zapewnienie elastyczności i płynności ruchu, unikanie zatorów, kontrolowanie przemieszczania pododdziałów oraz sprzętu zgodnie z grafikiem;

– wsparcia przepraw, czyli wsparcia: inżynieryjnego (środki przeprawowe i ich załogi oraz obsługi), technicznego, medycznego i logistycznego oraz innych jego rodzajów, które mogą wynikać z sytuacji bojowej w danym rejonie.

Powinien on zorganizować odpowiednią służbę w celu utrzymania porządku na przeprawie oraz zapewnić łączność, by we właściwym czasie wywoływać do jej przekroczenia pododdziały następnej fali, a także zagwarantować szybką i sprawną budowę oraz odtworzenie uszkodzonych środków przeprawowych. Ponadto meldować dowódcy odcinka forsowania o jego przebiegu oraz realizować przedsięwzięcia zabezpieczające przeprawę przed zniszczeniem przez przeciwnika. Do pomocy w kierowaniu nią komendant wyznacza ze składu pododdziału urządzającego ją 1–2 pomocników oraz dowódcę punktu przeprawy.

Na *dowódcę punktu przeprawy* wyznacza się przedstawiciela wojsk inżynieryjnych – dowódcę lub oficera z pododdziału przeprawowego, który ją urządza. Do koordynacji działań na brzegu przeciwległym i wyjściowym, w miarę potrzeb, wydziela się pomocników dowódcy.

Do obowiązków dowódcy punktu przeprawy należy:

– przygotowanie i utrzymanie tego punktu, w tym wjazdów na ten punkt i wyjazdów z niego;

– wyznaczenie osi przeprawy dla środków desantowo-przeprawowych i promów;

– techniczne urządzenie przeprawy oraz utrzymanie środków przeprawowych w gotowości do użycia;

– przeprawianie sił i środków materiałowych przez przeszkodę wodną w podległym punkcie przeprawy, w tym wydawanie rozkazów dla przeprawianych pododdziałów, które wynikają ze spraw organizacyjno-technicznych i bezpieczeństwa;

– informowanie kierującego ruchem wojsk w rejonie wyczekiwania o gotowości punktu przeprawy do przeprawienia kolejnych pododdziałów;

– techniczne utrzymanie przeprawy i zapewnienie nieprzerwanego ruchu w jej punkcie.

Pomocnik dowódcy punktu przeprawy na przeciwległym brzegu kieruje rozładowaniem środków desantowych i promów. Nie dopuszcza do zatrzymania się żołnierzy i sprzętu przy brzegu lub w rejonie przeprawy powrotnej, wysyłając ich natychmiast na przejścia w polach minowych lub na wyznaczone drogi. Na przeprawy mostowe i w bród przemieszcza niezbędne środki do zapewnienia ciągłości ruchu pojazdów na przeprawie. Obowiązki swoje wykonuje przy pomocy podległej mu służby porządkowo-ochronnej, przebywającej stale na przeciwległym brzegu. Ponadto podlega mu obsługa środków desantowych i promów w czasie przebywania na przeciwległym brzegu. Przestrzega szybkiego powrotu na brzeg wyjściowy środków desantowych i promów, a w razie potrzeby organizuje prowizoryczną naprawę środków przeprawowych, aby umożliwić ich powrót. Utrzymuje stałą łączność z dowódcą punktu przeprawy i po uzgodnieniu z nim organizuje ewakuację rannych na powracających środkach przeprawowych.

Pomocnik dowódcy punktu przeprawy na brzegu wyjściowym kieruje załadowaniem żołnierzy i sprzętu na środki przeprawowe oraz przestrzega ich prawidłowego wykorzystania. Na przeprawie mostowej występuje jako dyżurny mostu (oficer, podoficer) odpowiedzialny za jego właściwe utrzymanie i eksploatację. W razie uszkodzenia mostu przerywa ruch oraz z użyciem wszelkich możliwych środków dąży do usunię-

[14] Por. Ibidem, s. 244.

cia uszkodzenia siłami obsługi mostu. Zgłaszającemu się do niego dowódcy lub przedstawicielowi sztabu kolejnej przybyłej kolumny (pododdziału, oddziału) wydaje zezwolenie na rozpoczęcie przeprawy. Dowódca przeprawianej kolumny powinien udzielać dyżurnemu mostu wszelkiej pomocy w utrzymaniu porządku i dyscypliny oraz w obronie i ochronie mostu w czasie przeprawy, aż do jej zakończenia. Na przeprawach desantowych i promowych pomocnik dowódcy punktu przeprawy spotyka na linii wyjściowej kolejno przybywające pododdziały (fale) i organizuje ich ładowanie osobiście lub z pomocą inżynieryjnych posterunków regulacji ruchu.

Pomocnikowi dowódcy punktu przeprawy (dyżurnemu mostu) podlega służba porządkowo-ochronna przeprawy na brzegu wyjściowym, obsługa środków przeprawowych (mostu) oraz grupa ewakuacyjno-ratunkowa. Utrzymuje on stałą łączność z dowódcą punktu przeprawy, prowadzi dziennik (ewidencję) przeprawy oraz likwiduje natychmiast wszelkie objawy naruszenia porządku na brzegu wyjściowym, nie dopuszczając do skupienia na nim żołnierzy i sprzętu oraz przebywania w miejscach odkrytych na brzegu itp. Dowódcy wszystkich przepraw ponoszą odpowiedzialność za utrzymanie własnymi siłami porządku oraz za regulację ruchu przeprawianych pododdziałów (kolumn) w rejonie samej przeprawy. Dowódcy odcinków forsowania wyznaczają *komendanta i obsługę posterunków kontroli*, którym podlega dana przeprawa. Do pełnienia służby regulacji ruchu wykorzystuje się zwykle etatowe pododdziały ochrony i regulacji ruchu. Od rubieży i rejonów wyjściowych przeprawianych pododdziałów i oddziałów organizuje się *służbę regulacji ruchu* oraz rozmieszcza w terenie sieć *posterunków kontrolnych*, zwłaszcza w miejscach lub w pobliżu skrzyżowania dróg dofrontowych z rokadami.

Inżynieryjny posterunek kierowania ruchem (regulacji ruchu) odpowiada za przepuszczanie pododdziałów na przeprawę. Utrzymuje stałą łączność z komendantem przeprawy oraz współpracuje z komendantem posterunku kontroli, wyznaczonym przez dowódcę odcinka przeprawy, oraz z przedstawicielem przeprawiającego się aktualnie oddziału (związku taktycznego). Pilnie śledzi, by na przeprawę nie został skierowany sprzęt, którego ciężar lub wymiary wykluczają możliwość jej pokonania na danych środkach przeprawowych.

Żołnierze inżynieryjnego posterunku kierowania ruchem na rozkaz komendanta przeprawy kierują kolejne pododdziały na przeprawę lub wstrzymują ruch. Wspólnie z komendantem posterunku kontroli oraz z przedstawicielem przeprawiającego się oddziału (związku taktycznego) sprawdza on i przepuszcza na przeprawę pododdziały zgodnie z grafikiem (harmonogramem), nie dopuszczając do naruszenia ustalonego porządku. Jeśli nie przydzielono wcześniej pododdziałów do poszczególnych środków przeprawowych (np. w trakcie przygotowania w rejonie wyjściowym), wykonuje on tę czynność oraz instruuje dowódców o zasadach przeprawiania się i przestrzegania porządku.

Na *służbę regulacji ruchu* nakłada się następujące obowiązki:

– regulowanie ruchem wojsk w czasie podchodzenia do przeszkody wodnej oraz przestrzeganie ustalonej przez dowódcę dywizji (brygady) kolejności przeprawy wojsk i porządku ruchu na drogach;

– niedopuszczenie do naruszenia ustalonych odległości i przerw w marszu między oddziałami i pododdziałami;

– zapobieganie nadmiernemu skupianiu się wojsk i środków transportowych na ostrych wzniesieniach i spadkach oraz na trudno przejezdnych odcinkach dróg prowadzących do przeszkody wodnej;

– niedopuszczenie do nadmiernej prędkości ruchu oraz niepotrzebnego wyprzedzania;

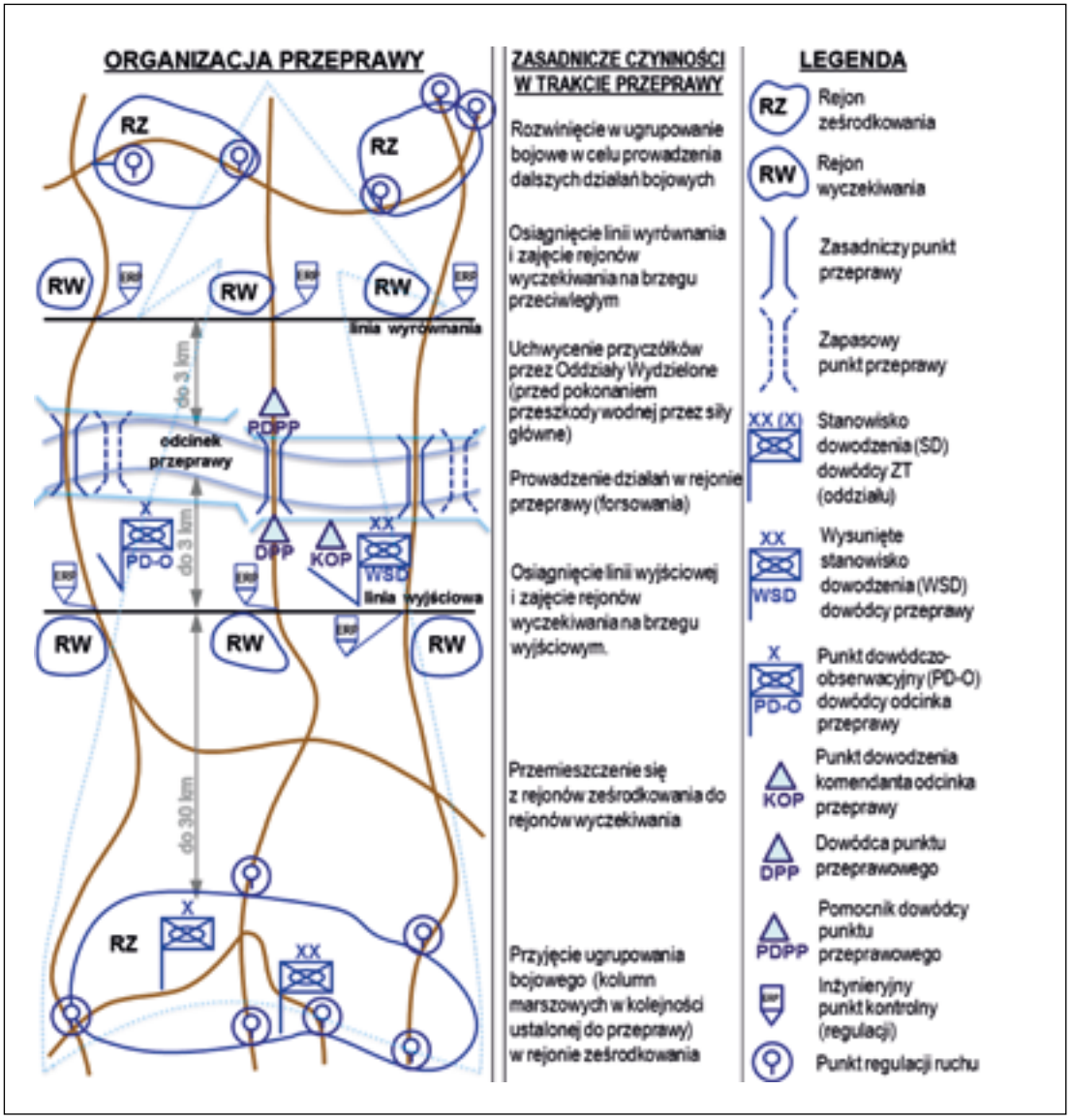
– zapewnienie usuwania z korony drogi uszkodzonego sprzętu bojowego i środków transportowych;

– kontrolowanie przestrzegania zasad maskowania na drogach marszu prowadzących do przeszkody wodnej, przed liniami wyjściowymi i liniami wyrównania, a także w rejonach wyjściowych do forsowania, w rejonach uszczelniania (hermetyzacji) czołgów, w miejscach załadowania sił i środków bojowych na desantowe środki przeprawowe oraz na brzegach przeszkody wodnej i na przeprawach.

Inżynieryjny posterunek obserwacyjny (IPO) organizuje się zazwyczaj niedaleko stanowiska dowodzenia dowódcy punktu przeprawy, w miejscu dogodnym do obserwacji samego przebiegu przeprawy, jak i przeszkody wodnej od strony górnego biegu rzeki. W miarę możliwości miejsce na posterunek powinno nadawać się również do prowadzenia obserwacji przestrzeni powietrznej i monitorowania wystąpienia skażeń. W razie braku możliwości prowadzenia z jednego miejsca obserwacji, wyznacza się kolejne posterunki obserwacyjne. W skład posterunku wchodzi jeden do kilku żołnierzy z pododdziału przeznaczonego do urządzenia przeprawy. Większy skład inżynieryjnego posterunku obserwacyjnego jest niezbędny na przeprawach utrzymywanych dłużej niż 3–4 godziny w celu prowadzenia obserwacji na zmianę (głównie przeprawy mostowe). Prowadzi ją jeden, a w razie potrzeby dwóch obserwatorów jednocześnie w różnych sektorach obserwacji.

W trakcie organizowania forsowania IPO obserwuje przebieg prac inżynieryjnych przeciwnika, zwłaszcza tych związanych z umocnieniem brzegu, oraz wahania poziomu wody. W trakcie przeprawy kontroluje jej przebieg oraz odbiera sygnały od pomocników dowódcy punktu przeprawy i sygnały od czat wodnych, jak również na rozkaz dowódcy punktu przeprawy przekazuje sygnały służbie porządkowo-ochronnej. Śledzi pojawienie się na przeszkodzie wodnej min pływających i innych środków napadu przeciwnika, dokonywanego zarówno z wody, jak i z lądu oraz powietrza. W przypadku zmiany poziomu wody mierzy

RYS. 1. SCHEMAT ORGANIZACJI PRZEPRAWY (FORSOWANIA) PRZESZKODY WODNEJ (WARIANT)



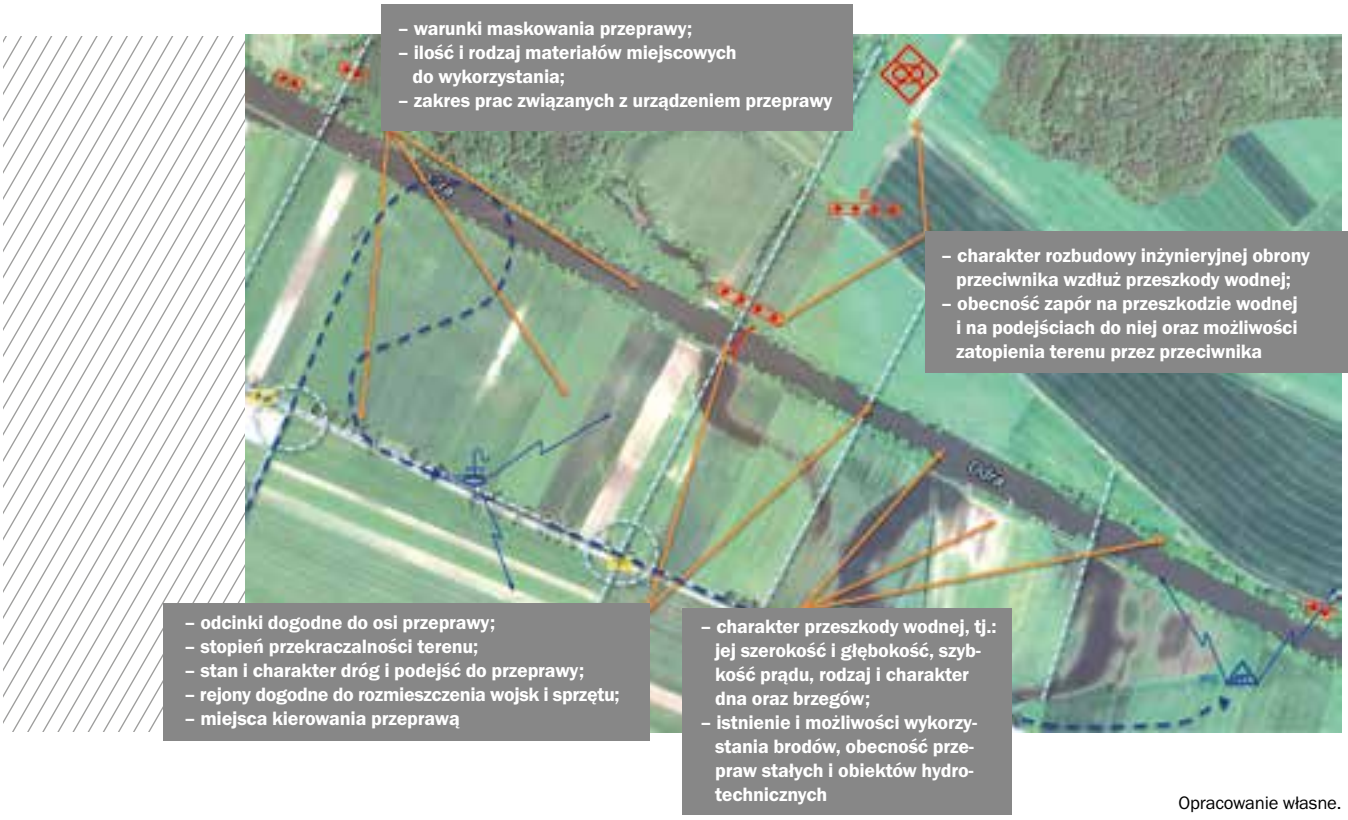
Opracowanie własne na podstawie: STANAG 2395 *Deliberate water crossing procedures*, appendix 1 to annex B, b-1-1.

ją wodowskazem. O spostrzeżeniach melduje natychmiast komendantowi.

Dowódca środka przeprawowego (PTS, łódź, prom) jest przełożonym wszystkich przeprawianych żołnierzy bez względu na ich stopień wojskowy. Odpowiada za właściwe przygotowanie środka przeprawowego oraz za bezpieczeństwo obsługi i desantu.

Służba ratunkowo-ewakuacyjna jest przeznaczona do ratowania żołnierzy oraz ewakuacji uszkodzonego sprzętu z miejsca przeprawy. Grupy ratunkowe udzielają żołnierzom pomocy polegającej na wyławianiu ich z wody, wydobyciu z zatopionych pojazdów (sprzętu), opatrzeniu ran oraz transporcie z miejsca przeprawy do punktów medycznych. Zadaniem *grupy ratunkowo-ewakuacyjnej* jest ratowanie załóg oraz ewakuacja czołgów i wozów bojowych uszkodzonych lub zatopionych w czasie pokonywania przeszkody wodnej. Grupę tę organizuje się na czas forsowania i przeprawiania przez przeszkody wodne, wykorzystując siły i środki, które wydziela dowódca oddziału lub związku taktycznego. Podlega ona bezpośrednio dowódcy odcinka przeprawy. Na jej dowódcę wyznacza się oficera lub podoficera wojsk inżynieryjnych. Jest on odpowiedzialny za stałą jej gotowość do działania. Grupa ratunkowo-ewakuacyjna składa się z drużyny ewakuacji załóg oraz drużyny ewakuacji czołgów i wozów bojowych.

RYS. 2. ZADANIA ROZPOZNANIA INŻYNIERYJNEGO PRZESZKODY WODNEJ



Opracowanie własne.

Przy przeszkodach wodnych organizuje się *przeprawowe punkty medyczne*, które udzielają pierwszej pomocy medycznej oraz ewakuują żołnierzy do punktów wyspecjalizowanej pomocy lekarskiej. Punkt medyczny przeprawy rozmieszcza się na brzegu wyjściowym w pobliżu stanowiska komendanta przeprawy, w miejscu umożliwiającym ukrycie i osłonę rannych oraz wyratowanych z wody przed ogniem i odłamkami pocisków. Organizuje go *dowódca punktu przeprawy* własnymi siłami, a jeśli nie ma takich możliwości, to siłami i środkami otrzymanymi od dowódcy lub komendanta odcinka forsowania oraz od przeprawianych oddziałów. W pierwszym rzędzie wojska inżynieryjne powinny własnymi siłami organizować punkty medyczne przy wszystkich przeprawach mostowych. Punkt medyczny przeprawy podlega dowódcy punktu przeprawy. Wariant organizacji przeprawy (forsowania) przeszkody wodnej zaprezentowano na rysunku 1.

ISTOTA ROZPOZNANIA INŻYNIERYJNEGO

Najważniejszą rolę w zdobywaniu danych potrzebnych do planowania działań inżynieryjnych odgrywają komórki (sekcje) planowania i rozpoznania pionu operacyjnego stanowisk dowodzenia szczebla taktycznego (związek taktyczny, oddział). Prowadząc ocenę inżynieryjną przeciwnika i środowiska, specjalista sekcji WInż wykorzystuje informacje pozyskane od oficerów rozpoznania, którzy opracowują możliwe warianty działania przeciwnika w aktualnych uwarunkowaniach terenowych i atmosferycznych.

Jednym z niełatwych, zarazem bardzo ważnych zadań realizowanych w czasie planowania działań, jest pozyskanie danych z *rozpoznania inżynieryjnego przeszkody wodnej i przeciwnika*. Pozwalają one bowiem na podjęcie właściwej decyzji co do organizacji forsowania i wykorzystania możliwości przeprawowych. Rozpoznanie inżynieryjne powinno określić[15] (rys. 2):

– charakter przeszkody wodnej, czyli: jej szerokość i głębokość, szybkość prądu, rodzaj i charakter dna oraz brzegów, istnienie i możliwości wykorzystania brodów, obecność przepraw stałych i obiektów hydrotechnicznych;

– odcinki dogodne do zastosowania jako zasadnicze i pomocnicze osie przeprawy;

– ogólną charakterystykę właściwości ochronnych, odcinki (rejony) terenu, które mogą być wykorzystane

[15] J. Parzewski: *Zabezpieczenie inżynieryjne forsowania...,* op.cit., s. 17.

jako rejony: wyjściowe przed forsowaniem, uszczelniania czołgów i ześrodkowania sprzętu przeprawowego, a także ustalić warunki skrytego podejścia do przeszkody wodnej;

– stan i charakter dróg i obiektów drogowych, dróg dojazdowych, dróg na przełaj i podejść do przeprawy;

– obecność zapór na przeszkodzie wodnej i na podejściach do niej oraz możliwości zatopienia terenu przez przeciwnika;

– ilość i rodzaj materiałów miejscowych przydatnych do urządzenia przeprawy;

– stopień przekraczalności terenu na podejściach do przeszkody wodnej;

– miejsca na rozwinięcie stanowisk dowodzenia dowódcy odcinka przeprawy, komendanta przeprawy i dowódcy grupy ratunkowo-ewakuacyjnej;

– warunki maskowania przeprawy;

– ogólny charakter i zakres robót związanych z jej urządzeniem;

– charakter rozbudowy inżynieryjnej obrony przeciwnika wzdłuż przeszkody wodnej.

Rozpoznanie inżynieryjne tych przeszkód jest prowadzone w formie rozpoznania studyjnego (działania analityczno-informacyjne) oraz bezpośredniego (działania patrolowe i obserwacja z posterunków).

Rozpoznanie studyjne przeszkód wodnych prowadzą dowództwa jednostek ogólnowojskowych i inżynieryjnych, w tym komórki rozpoznawcze i inżynieryjne poszczególnych stanowisk dowodzenia. Polega ono na systematycznym zbieraniu i gromadzeniu oraz analizowaniu wszelkich dostępnych informacji o: wojskach inżynieryjnych przeciwnika; jego doktrynalnych wzorcach prowadzenia działań bojowych z wykorzystaniem przeszkód wodnych; możliwościach zabezpieczenia i wsparcia inżynieryjnego tych działań; wyposażeniu w techniczne i materiałowe środki inżynieryjne; a także o terenie i warunkach klimatycznych panujących na odcinkach forsowania przeszkody wodnej. Rozpoznanie studyjne przeszkód wodnych prowadzi się w sposób ciągły w czasie pokoju[16], a także we wszystkich okresach (na etapach) prowadzenia działań metodą analizy i syntezy.

Do zasadniczych materiałów źródłowych należą[17]:

– wydawnictwa i publikacje (cyfrowe opracowania) właściwych urzędów administrujących danymi terenami i obiektami (informatory hydrologiczne, opisy terenu, roczniki statystyczne, projekty techniczne itp.),

– mapy analogowe,

– zdjęcia satelitarne, lotnicze i naziemne,

– meldunki i sprawozdania opracowane przez komórki rozpoznawcze, a także biuletyny oraz komunikaty rozpoznawcze nadrzędnych sztabów i sąsiadów.

Do oceny pod kątem inżynieryjnym przeszkody wodnej i przyległego terenu specjaliści WInż mogą wykorzystać również narzędzia informatyczne, w tym przede wszystkim możliwości oferowane przez pakiety grafiki operacyjnej (PGO), cyfrowe produkty geograficzne dostępne w sieci wojskowej oraz komputerowe bazy danych (operacyjne, statystyczne i relacyjne).

Oprócz rozpoznania studyjnego przeszkody wodnej i przyległego terenu jest prowadzone *rozpoznanie bezpośrednie*. Jest to zadanie inżynieryjnych elementów rozpoznawczych, wykonywane w formie działań patrolowych, obserwacji obiektów i rejonów oraz nasłuchu dźwięków z przestrzeni zajmowanej przez przeciwnika[18].

Uzyskane różnymi sposobami informacje o przeszkodzie wodnej i przyległym terenie ewidencjonuje się w zbiorach danych. Zbiory te mogą mieć różną postać zobrazowania informacji (analogową i cyfrową). Są opracowywane jako np.: mapy robocze – topograficzne mapy analogowe i numeryczne (cyfrowe produkty geograficzne), szkice, tabele, meldunki, projekty techniczne, schematy organizacyjne, komputerowe bazy danych oraz inne dokumenty pomocnicze.

Niezwykle istotną kwestią jest posiadanie przez specjalistów wojsk inżynieryjnych bazy danych umożliwiającej pozyskanie informacji o terenie i wojskach inżynieryjnych innych państw czy też modeli symulacyjnych działania wojsk przeciwnika (w tym możliwości i sposobów realizacji przez niego zadań inżynieryjnych). W znaczący sposób przyspieszyłoby to ocenę inżynieryjną środowiska i potencjalnego przeciwnika, pozwalając tym samym na skrócenie czasu planowania, co jest niezwykle istotne w warunkach ograniczonego czasu lub niewystarczającej liczby osób funkcyjnych w sekcji wojsk inżynieryjnych.

Dokonując *inżynieryjnej oceny terenu*: rzek, kanałów i zbiorników retencyjnych, należy rozpatrywać te obiekty jako przeszkody wodne oraz rubieże o znaczeniu taktyczno-operacyjnym. Natomiast organizując forsowanie, szczegółowo powinien być oceniany teren zarówno na brzegu wyjściowym, jak i przeciwległym. Zazwyczaj podczas tej oceny ustala się:

– elementy terenowe mające zasadniczy wpływ na wykonanie zadania (podejście do przeszkody wodnej, forsowanie, natarcie na przeciwległym brzegu);

– charakter rzeźby terenu pod względem pocięcia wąwozami, jarami, rzekami, jeziorami i innymi przeszkodami naturalnymi; warunki obserwacji i maskowania; warunki przejezdności na odcinkach lub kierunkach forsowania zarówno na podejściach

[16] Określone jednostki inżynieryjne corocznie w okresie pokoju prowadzą w ramach szkolenia wojsk rozpoznanie osi przeprawowych na głównych rzekach w Polsce. Ma to na celu uaktualnienie prowadzonej przez organy transportu i ruchu wojsk dokumentacji dotyczącej przygotowania wyznaczonych osi przeprawowych na potrzeby obronne oraz zamierzeń centralnego planu studiów operacyjnych TZS SZ.

[17] *Rozpoznanie inżynieryjne – instrukcja*. DWLąd/SWInż, Warszawa 1998, s. 93.

[18] Do bezpośrednich sposobów rozpoznania inżynieryjnego przeszkody wodnej należą: obserwacja, fotografowanie, wypad, oględziny bezpośrednie (połączone z pomiarami technicznymi). Ibidem, s. 11.

do przeszkody wodnej, jak również na przeciwległym jej brzegu;

– ogólną charakterystykę właściwości ochronnych, warunki skrytego podejścia do przeszkody wodnej, odcinki (rejony) terenu, które mogą być wykorzystane jako rejony wyjściowe przed forsowaniem, rejony uszczelniania czołgów (punkty przeprawy czołgów pod wodą) czy też rejony ześrodkowania sprzętu przeprawowego;

– najdogodniejsze kierunki podejścia do wybranych odcinków forsowania lub przeprawy wojsk;

– podstawowe parametry przeszkody wodnej, czyli: jej szerokość i głębokość, prędkość prądu, grunt dna i brzegów, charakter brzegów, warunki dojazdu, liczba i szerokość odcinków (miejsc) dogodnych do organizowania przepraw.

Oceny terenu na odcinku forsowania dokonuje się bardzo szczegółowo zarówno pod względem jego właściwości taktycznych, jak i hydrologicznych z uwzględnieniem charakteru działań bojowych wojsk własnych i przeciwnika oraz parametrów taktyczno-technicznych sprzętu bojowego, przeprawowego i środków transportowych. Ustalenie ogólnej charakterystyki terenu na odcinku forsowania obejmuje określenie: rodzaju i właściwości terenu, odcinków niedostępnych, dróg lub kierunków dojścia do przeszkody wodnej, dominujących wzniesień na brzegu wyjściowym i przeciwległym, ogólnego charakteru przeszkody, istniejących przepraw i obiektów hydrotechnicznych, właściwości doliny, terenów zalewowych i brzegów oraz prawdopodobnych miejsc przepraw. Oceniając teren przyległy do przeszkody wodnej na przeciwległym brzegu, ustala się: dominujące wzniesienia oraz warunki prowadzenia obserwacji z przeciwległego brzegu; prawdopodobne miejsca rozmieszczenia punktów dowodzenia i obserwacyjnych oraz stanowisk ogniowych artylerii, moździerzy i PPK; rubieże dogodne do organizowania obrony; rejony rozmieszczenia odwodów przeciwnika, możliwe kierunki ich przemieszczania i rubieże rozwijania do kontrataków; charakter i stan dróg; położenie wąwozów, jarów, odcinków zabagnionych i masywów leśnych oraz możliwości ich pokonania lub obejścia przez nacierające pododdziały; warunki przejezdności doliny rzecznej i stromość jej zboczy; miejscowości i charakter ich zabudowy. Obiekty hydrotechniczne (budowle), które znajdują się w rejonie forsowania, ocenia się pod kątem ich znaczenia jako elementów infrastruktury krytycznej, jak również możliwego wpływu na zmianę warunków terenowych w razie ich zniszczenia lub uszkodzenia. W czasie działań bojowych spowodowanie zmian konstrukcyjnych tych obiektów może wywołać m.in.: zatopienie przyległego terenu, utworzenie nowych przeszkód wodnych oraz zmianę szerokości, głębokości i prędkości prądu rzek. Oceniając obiekty hydrotechniczne, zwraca się również uwagę na warunki ich ochrony, możliwości opanowania, zdobycia i utrzymania bądź też zniszczenia lub innego wykorzystania przez własne wojska.

Istotą *oceny inżynieryjnej przeciwnika* jest określenie prawdopodobieństwa realizacji przez niego przedsięwzięć inżynieryjnych mogących mieć wpływ na działania taktyczne w rejonie przeszkody wodnej oraz zakresu zadań inżynieryjnych wykonywanych przez wojska własne. W czasie tej oceny rozpatruje się[19]:

– skład i rodzaj jego wojsk inżynieryjnych;

– możliwości wykonania przez nie prac inżynieryjnych w konkretnych warunkach terenowych, czasowych i meteorologicznych;

– dotychczasowy charakter i zakres realizowanych przedsięwzięć inżynieryjnych;

– aspekty organizacyjno-techniczne dotyczące nie tylko stanu liczbowego oddziałów, lecz także ilości i jakości stosowanych środków i materiałów inżynieryjnych oraz sposobów wykonywania zadań.

Wyniki oceny inżynieryjnej przeciwnika powinny służyć sprecyzowaniu wniosków dotyczących[20]:

– prawdopodobnego ugrupowania jego wojsk inżynieryjnych,

– możliwości wykonywania poszczególnych zadań,

– przedsięwzięć inżynieryjnych, na których przeciwnik prawdopodobnie skupi główny wysiłek;

– potrzebnych dodatkowych informacji o sytuacji inżynieryjnej przeciwnika.

WYBRANE ELEMENTY CYKLU DECYZYJNEGO

W procesie dowodzenia ważna jest *ocena możliwości wykonawczych wojsk własnych, w tym wojsk inżynieryjnych*. Polega ona na analizowaniu zdolności do realizacji zadań w konkretnej sytuacji taktycznej i inżynieryjnej. W ocenie tej uwzględnia się[21]:

– aktualne położenie pododdziałów wojsk inżynieryjnych i jego wpływ na ich możliwości wykonawcze (np. na termin podjęcia zadań);

– ukompletowanie w ludzi i sprzęt organicznych oraz przydzielonych pododdziałów innych rodzajów wojsk[22], a także poziom ich wyszkolenia i przygotowania do wykonywania zadań zabezpieczenia inżynieryjnego;

– skład, ukompletowanie i poziom wyszkolenia organicznych pododdziałów wojsk inżynieryjnych, ich doświadczenie bojowe oraz zdolności organizacyjne dowódców;

– skład, ukompletowanie, czas wzmocnienia i zdolność bojową przydzielonych pododdziałów wojsk in-

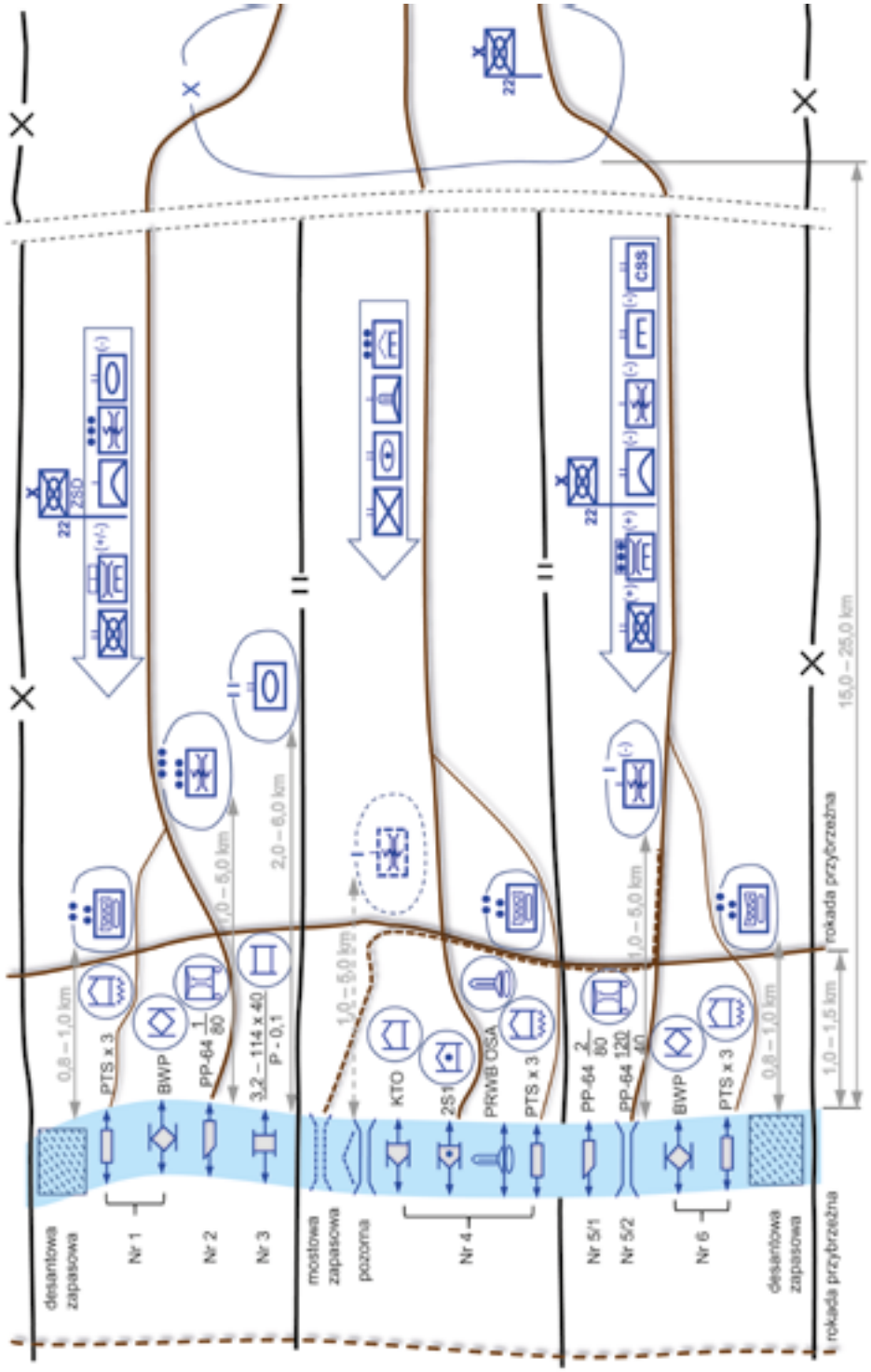
[19] Zob. P. Cieślar (red. nauk.), W. Kawka, S. Kowalkowski: *Wykorzystanie wojsk inżynieryjnych...,* op.cit., s. 298.

[20] *Wojska inżynieryjne w okresie pokoju i zagrożenia wojennego*. AON, Warszawa 2004, s. 80.

[21] Por. S. Kowalkowski: *Planowanie rozbudowy fortyfikacyjnej...*, op.cit., s. 99.

[22] Przez pojęcie *inne rodzaje wojsk* należy rozumieć wszystkie rodzaje wojsk z wyłączeniem wojsk inżynieryjnych.

RYS. 3. PRZYKŁAD SZKICU TYMCZASOWYCH PRZEPRAW PRZEZ PRZESZKODĘ WODNĄ



Źródło: W. Kawka, K. Wysocki: *Inżynieryjne dokumenty dowodzenia*. AON, Warszawa 2014, s. 301.

żynieryjnych wyższego szczebla dowodzenia, zakres zadań realizowanych na korzyść oddziału przez przełożonego, a także zakres uprawnień dowódcy[23] w stosunku do tych pododdziałów;

– możliwości rozpoznania inżynieryjnego;

– możliwości zabezpieczenia logistycznego;

– wyszkolenie i doświadczenie dowódców pododdziałów inżynieryjnych.

We wnioskach z oceny możliwości wykonawczych wojsk powinno się określić[24]:

– zdolność bojową wojsk do realizacji zadań inżynieryjnych,

– podział zadań między etatowe pododdziały inżynieryjne oraz przydzielone i wspierające,

– ograniczenia czasowe związane z możliwością wykorzystania wojsk przydzielonych i wspierających,

– możliwości użycia pododdziałów rodzajów wojsk do wykonywania zadań inżynieryjnych,

– potrzeby dotyczące zmian w podporządkowaniu pododdziałów inżynieryjnych,

– wstępne potrzeby zabezpieczenia logistycznego działań taktycznych pod względem inżynieryjnym.

W wyniku oceny sytuacji (w tym inżynieryjnej) powstają warianty działania wojsk własnych. Następnie są one szczegółowo rozważane i porównywane w celu stworzenia dowódcy możliwie najlepszych warunków do podjęcia decyzji. W ramach planowania jest podejmowana także decyzja oraz zostaje sformułowany i wygłoszony (przez dowódcę) zamiar działania.

Po dokonaniu przez dowódcę wyboru jednego z przedstawionych mu przez sztab wariantów działania i ogłoszeniu go jako decyzji dowódcy wszystkie komórki funkcyjne stanowiska dowodzenia przystępują do opracowania planu działania. Stanowi on podstawę do przygotowania rozkazu bojowego i uzupełniających go załączników oraz planu synchronizacji działań. W aspekcie urządzania i utrzymania przepraw *plan działania w rejonie przeszkody wodnej* powinien zawierać następujące elementy[25]:

• aktualną sytuację i zamiar działania przełożonego;

• zamiar dowódcy oraz wytyczne i ustalenia dotyczące:

– obrony i ochrony,

– kierowania ruchem,

– kontrolowania terenu,

– wsparcia przeprawy;

• główne i zapasowe punkty przepraw oraz drogi dojazdu do nich i wyjazdu z tych punktów (łącznie z drogami inżynieryjnymi, specjalnymi, obejściami i objazdami, jeśli zostały określone);

• ugrupowanie pododdziałów inżynieryjnych oraz ich zadania;

• harmonogram pokonywania przeszkody przez oddziały (pododdziały) lub elementy ugrupowania bojowego, zawierający ich rozmieszczenie lub kolejność podchodzenia do punktów przepraw i przeprawiania się;

• organizację ruchu określającą:

– drogi prowadzące do punktów przepraw,

– drogi za przeszkodą wyprowadzające do rejonów wyczekiwania (ześrodkowania),

– drogi rokadowe,

– posterunki kierowania ruchem,

– rejony ześrodkowania,

– rejony wyczekiwania (zbiórek),

– ustalone terminy przekraczania punktów kontrolnych i rubieży;

• ograniczenia (nośność, prędkość i wojskowa klasyfikacja obciążenia);

• kryptonimy i oznakowania identyfikacyjne dla każdego punktu przeprawy;

• rozmieszczenie sił i środków broniących przeprawy oraz elementów wsparcia medycznego, technicznego i zaopatrzenia;

• schematy sieci łączności;

• organizację ochrony i obrony punktów przeprawy.

Przykład przepraw przez przeszkodę wodną przedstawiono na rysunku 3.

Plan powinien określać wykonawców oraz rodzaj, zakres i terminy wykonania wszystkich zadań inżynieryjnych[26]. Natomiast zakres prac planistycznych zależy od stopnia szczegółowości wcześniej sporządzonych kalkulacji taktycznych i inżynieryjnych, wykonanych dokumentów pomocniczych oraz dokonanych uzgodnień z poszczególnymi zespołami funkcjonalnymi stanowiska dowodzenia. Plan zazwyczaj składa się z dwóch części: opisowej, która jest załącznikiem do rozkazu bojowego i stanowi dokument rozkazodawczy dla wykonawców, oraz graficznej, będącej uzupełnieniem załącznika. Głównym celem opracowania załącznika inżynieryjnego jest sformułowanie i przekazanie zadań poszczególnym wykonawcom. Istotą zaś jego przygotowania jest: dokonanie podziału zadań inżynieryjnych między oddziały i pododdziały inżynieryjne podporządkowane danemu szczeblowi dowodzenia; poinformowanie wszystkich uczestników działań o zadaniach inżynieryjnych podejmowanych przez wojska inżynieryjne w poszczególnych pasach (w rejonach, na kierunkach) działania; określenie i postawienie rodzajom wojsk głównych zadań do wykonania; podanie do wiadomości wytycznych koordynujących wspólną realizację zadań inżynieryjnych przez różnych wykonawców; przekazanie informacji o przedsięwzięciach logistycznych podejmowanych na rzecz

[23] Zob. *Regulamin działań wojsk lądowych*. DWLąd, Warszawa 2008, s. 286–288; *Land Operations. ATP-3.2, s. 2–46; Instrukcja wojennego systemu dowodzenia Sił Zbrojnych RP...*, op.cit.

[24] Por. *Wojska inżynieryjne w okresie pokoju...,* op.cit., s. 85.

[25] Zob. *Instrukcja – pokonywanie przeszkód...,* op.cit., s. 42.

[26] Zob. *Regulamin działań wojsk inżynieryjnych wojsk lądowych...,* op.cit., s. 116.

realizacji zadań inżynieryjnych; poinformowanie podwładnych o wymaganiach w sferze dowodzenia i łączności.

Załącznik inżynieryjny jest głównym dokumentem planistycznym odnoszącym się do działań inżynieryjnych. Ma układ dokumentu sformalizowanego. Składa się z pięciu punktów dotyczących: położenia oddziałów i pododdziałów inżynieryjnych, ogólnego zadania, zadań do realizacji przez poszczególnych wykonawców, wsparcia logistycznego oraz dowodzenia i łączności. Do załącznika można dołączyć wszelkie uzupełnienia w formie pisemnej lub graficznej.

Na potrzeby urządzania i utrzymania przepraw przez związek taktyczny (oddział) będzie to kolejne uzupełnienie do załącznika C (plan działania) rozkazu bojowego bądź też może być dodatkowym załącznikiem – grafik (harmonogram) przeprawy lub grafik (harmonogram) forsowania do wstępnego zarządzenia bojowego lub rozkazu bojowego[27].

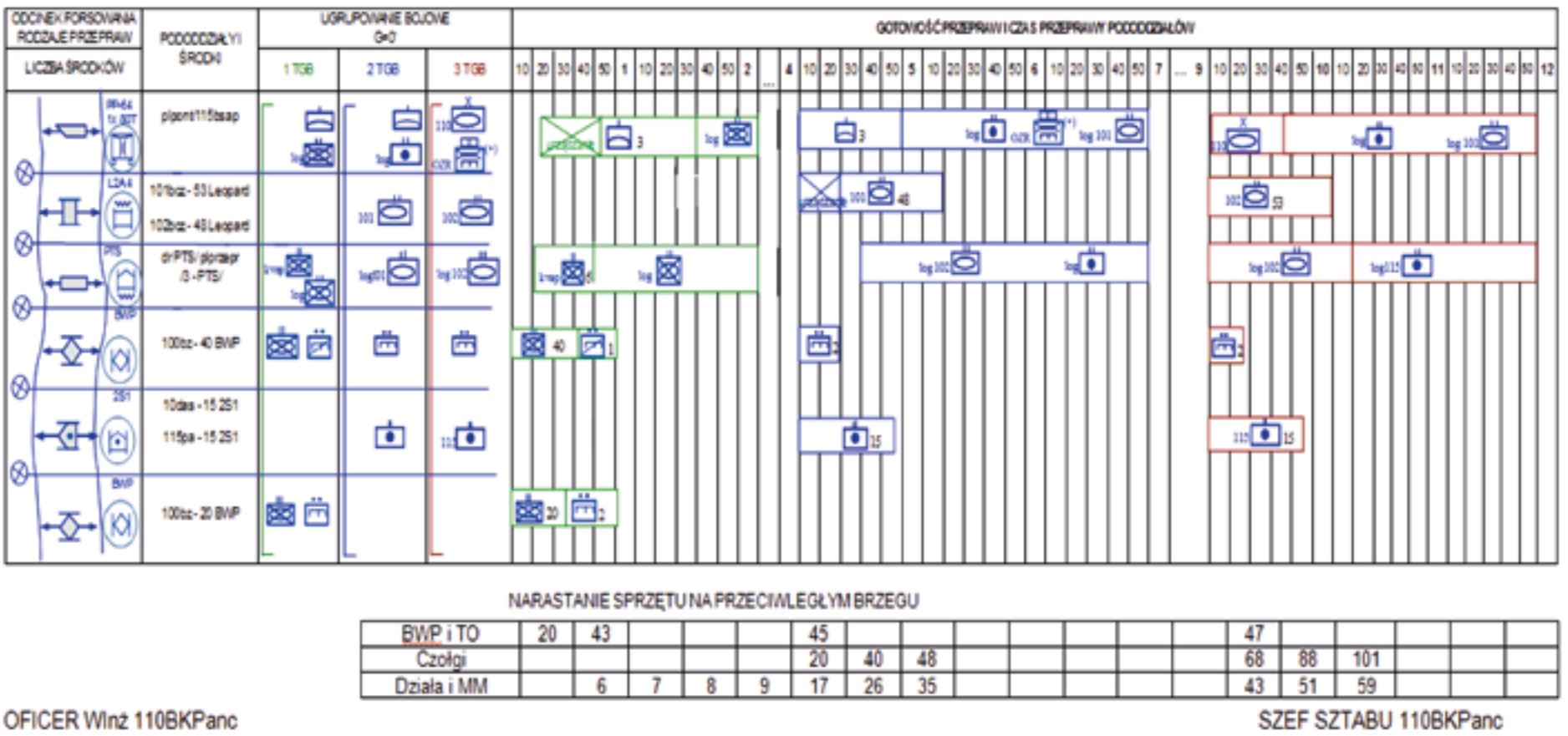
Oceny terenu na odcinku forsowania dokonuje się bardzo szczegółowo zarówno pod względem jego właściwości taktycznych, jak i hydrologicznych z uwzględnieniem charakteru działań bojowych wojsk własnych i przeciwnika oraz parametrów taktyczno-technicznych sprzętu bojowego, przeprawowego. i środków transportowych.

WALDEMAR MŁYNARCZYK
COMBAT CAMERA DORSZ

Grafik (harmonogram) przeprawy lub forsowania (rys. 4) jest dokumentem określającym kolejność i czas przeprawy wojsk. Podpisuje go szef sztabu związku taktycznego (oddziału) oraz szef sekcji wojsk inżynieryjnych, a zatwierdza dowódca. Podaje się w nim: odcinki przeprawy (forsowania) dywizji i brygad (batalionów); kolejność wyjścia oddziałów (pododdziałów) do przeszkody wodnej; miejsca i rodzaje przepraw; trasy (osie) przeprawy czołgów pod wodą; pododdziały wyznaczone do urządzenia i utrzymania przepraw; środki przeprawowe i ich podział; czas gotowości przepraw oraz czas przeprawy wojsk. W brygadzie forsowanie i przeprawę wojsk planuje się poszczególnymi falami[28].

[27] Por. W. Kawka, K. Wysocki: *Inżynieryjne dokumenty dowodzenia*. AON, Warszawa 2014, s. 54.

RYS. 4. GRAFIK (HARMONOGRAM) PRZEPRAWY ODDZIAŁU PRZEZ PRZESZKODĘ WODNĄ (WARIANT)



Źródło: W. Kawka, K. Wysocki: *Inżynieryjne dokumenty dowodzenia*. AON, Warszawa 2014, s. 227.

Opracowanie załącznika jest końcowym rezultatem pracy planistycznej specjalistów wojsk inżynieryjnych. Stanowi połączenie rezultatów wszystkich wymienionych etapów i czynności w postaci dokumentów planistycznych i rozkazodawczych dla podwładnych.

Kolejną fazą jest *stawianie zdań*. Jej celem jest przekazanie zadań bojowych wykonawcom. Zadania te mogą być postawione w formie: rozkazu bojowego, wstępnego zarządzenia bojowego, zarządzenia bojowego lub zarządzenia przygotowawczego[29]. Zwykle proces ten rozpoczyna się po zakończeniu opracowania rozkazu bojowego wraz z niezbędnymi załącznikami i uzupełnieniami.

Etap stawiania zadań dotyczących działań inżynieryjnych traktuje się jako zespół czynności organizatorskich mających na celu przekazanie zadań inżynieryjnych wykonawcom wszystkich rodzajów wojsk oraz spowodowanie utworzenia ugrupowania wojsk inżynieryjnych stosownie do zadań wsparcia inżynieryjnego. Zadania podległym pododdziałom mogą być postawione osobiście przez dowódcę określonego szczebla dowodzenia lub przekazane przez jego zastępcę albo przez oficerów łącznikowych, a także z wykorzystaniem technicznych środków łączności[30].

Praktyka wskazuje, że wykonawcą czynności organizatorskich wsparcia inżynieryjnego jest oficer wojsk inżynieryjnych. Podstawę jego działalności stanowi rozkaz dowódcy wraz z załącznikiem inżynieryjnym i wytycznymi oraz informacje szczegółowe zawarte w planie działań inżynieryjnych. Koordynatorem czynności organizatorskich realizowanych wspólnie przez oficera wojsk inżynieryjnych i specjalistów pozostałych rodzajów wojsk jest szef sztabu ZT (oddziału). Sytuacja taka pozwala na precyzyjne przekazanie zadań oraz umożliwia wyjaśnienie niejasności dotyczących użycia pododdziałów inżynieryjnych.

Ostatnią fazą procesu dowodzenia jest *kontrola*. Jej rezultaty stanowią podstawę do uaktualnienia posiadanych danych o sytuacji (ustalenie położenia) i realizacji kolejnych faz cyklu decyzyjnego. Celem kontroli jest porównanie stanu rzeczywistego realizacji zadań z zadaniami planowanymi do wykonania przez podległe wojska. Za proces kontroli odpowiada dowódca ZT (oddziału, pododdziału), który do tego przedsięwzięcia może zaangażować oficerów sztabu.

WNIOSKI

Na podstawie przedstawionych treści, które stanowią najistotniejszą część pracy specjalistów wojsk inżynieryjnych funkcjonujących na stanowiskach dowodzenia ZT i oddziałów, należy stwierdzić, że kierowanie działaniami inżynieryjnymi na przeszkodzie wodnej i w rejonie do niej przyległym jest realizowane przez dowództwa jednostek ogólnowojskowych oraz dowództwa oddziałów (pododdziałów) wojsk inżynieryjnych. Planowanie przepraw i dowodzenie nimi należy do obowiązków dowódcy związku taktycznego (oddziału), który prowadzi działania bojowe w pasie, w którym urządza się przeprawę. W zależności od otrzymanego zadania, rodzaju prowadzonych działań, sytuacji operacyjno-taktycznej, właściwości przeszkody wodnej i przyległego terenu, posiadanych sił i środków oraz charakteru działań przeciwnika – określa on ugrupowanie bojowe oraz kolejność przekraczania przeszkody i wymagania dla punktów przeprawy. W kwestiach organizacji wykonania tych czynności bezpośrednim doradcą dowódcy jest specjalista wojsk inżynieryjnych – szef sekcji wojsk inżynieryjnych związku taktycznego (oddziału). Do zasadniczych ogniw kierowania działaniami inżynieryjnymi na potrzeby urządzania i utrzymania przeprawy przez przeszkodę wodną należy zaliczyć: dowódcę przeprawy (forsowania), dowódcę odcinka przeprawy (forsowania), komendanta odcinka przeprawy (forsowania), pomocników komendanta odcinka przeprawy (forsowania), dowódcę punktu przeprawy, pomocników dowódcy punktu przeprawy oraz inne osoby związane z zabezpieczeniem przedmiotowego kierowania. Najistotniejszym etapem w pracy szefa sekcji WInż w aspekcie urządzania i utrzymania przepraw jest sporządzenie kalkulacji dotyczącej przeprawy oddziału (związku taktycznego) – zarówno w całości za związek taktyczny (ZT), jak i dla poszczególnych elementów ugrupowania bojowego w kolejności forsowania wynikającej z opracowywanych wariantów działania. Na potrzeby urządzania i utrzymania przepraw przez związek taktyczny (oddział) jest przygotowywany dokument rozkazodawczy – grafik (harmonogram) przeprawy lub grafik (harmonogram) forsowania. Jest on dokumentem określającym kolejność i czas przeprawiania się wojsk. W grafiku (harmonogramie) tym podaje się: odcinki przeprawy (forsowania) dywizji i brygad (batalionów), kolejność wyjścia oddziałów (pododdziałów) do przeszkody wodnej, miejsca i rodzaje przepraw, trasy (osie) przeprawy czołgów pod wodą, pododdziały wyznaczone do urządzenia i utrzymania przepraw, środki przeprawowe i ich podział, czas gotowości przepraw i czas przeprawy wojsk. ■

[28] *Falą nazywamy obrót środków przeprawowych (desantowych lub promowych) podczas przeprawy wojsk, a więc ich załadowanie, pokonanie przeszkody, wyładowanie i powrót na brzeg wyjściowy. Czas potrzebny na wykonanie jednej fali nazywa się czasem obrotu. Zob.* S. Lang: *Przeprawy (podręcznik)...,* op.cit., s. 51.

[29] Zob. *Planowanie działań na szczeblu taktycznym w wojskach lądowych. DD/3.2.5.* DWLąd, Warszawa 2007, s. 53.

[30] Zadania postawione lub przekazane ustnie przez dowódcę (osobę upoważnioną) oraz przez techniczne środki łączności muszą być potwierdzone pisemnym dokumentem dowodzenia, dostarczonym tak szybko jak jest to możliwe. Por. J. Michniak (red. nauk.): *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych (główne problemy).* AON, Warszawa 2000, s. 88.

Nowoczesne mosty **pontonowe typu wstęga**

Marcin Dejewski jest inżynierem w Zakładzie Taktyki i Techniki Wojsk Inżynieryjnych w Instytucie Budowy Maszyn Wydziału Mechanicznego WAT.

Dariusz Kalinko jest inżynierem w Zakładzie Taktyki i Techniki Wojsk Inżynieryjnych w Instytucie Budowy Maszyn Wydziału Mechanicznego WAT.

Marian Janusz Łopatka jest kierownikiem Zakładu Maszyn Inżynieryjnych i Robotów w Instytucie Budowy Maszyn Wydziału Mechanicznego WAT.

WSPÓŁCZESNE POLE WALKI NARZUCA POTRZEBĘ POSIADANIA ŚRODKÓW PRZEPRAWOWYCH ZAPEWNIAJĄCYCH SWOBODĘ MANEWRU WOJSK.

por. mgr inż. Marcin Dejewski, por. mgr inż. Dariusz Kalinko, dr inż. Marian Janusz Łopatka

Niezmiennie od 1964 roku etatowym mostem pontonowym znajdującym się w wyposażeniu Wojska Polskiego jest park pontonowy PP-64. W czasach gdy wprowadzano go do użytku, była to konstrukcja nowoczesna, odpowiadająca stawianym wymaganiom. Dzisiaj jednak jest już wyeksploatowana i nie spełnia warunków współczesnego pola walki.

NOŚNOŚĆ MOSTÓW PONTONOWYCH

W wypadku mostów pontonowych typu wstęga zagadnieniem problematycznym jest ich nośność, ponieważ zmienia się ona w zależności od konkretnych warunków, w jakich pracuje konstrukcja. Wpływają na nią takie parametry, jak: prędkość nurtu i głębokość przeszkody wodnej, typ pojazdu, prędkość jazdy czy mimośrodowość obciążeń (zboczenie pojazdu od osi jezdni). Narażają one most na utratę stateczności na skutek zjawisk hydrodynamicznych.

Jeżeli nałożą się na siebie: mała głębokość wody (efekt jest pomijalny przy głębokości powyżej 6 m[1]), duża prędkość nurtu i nierównomierne obciążenie przeprawy (np. zjechanie pojazdu z osi jezdni), siły hydrodynamiczne mogą wywołać działanie ssące pod dziobową częścią mostu[2]. Może to doprowadzić do destabilizacji mostu i obsunięcia się pojazdu z przeprawy. Z tego powodu nośność mostów pontonowych przy niekorzystnych wartościach prędkości nurtu i głębokości jest ograniczona.

Mając na uwadze wymienione czynniki, zdefiniowano trzy klasy nośności mostów pontonowych[3]:

– nominalną (normal crossing) – określoną dla normalnych warunków eksploatacji: mimośrodowość obciążenia do 0,5 m, dopuszczalna odległość między pojazdami 30 m, dopuszczalna prędkość jazdy 25 km/h dla klasy MLC 30 i 15 km/h dla pojazdów powyżej MLC 30;

– warunkową (caution crossing) – możliwą do wykorzystania przy zaostrzonych warunkach bezpieczeństwa: mimośrodowość obciążenia jest niedopuszczalna, konieczne jest prowadzenie pojazdu przez przewodnika, odległość między pojazdami określona przez producenta wynosząca zwykle około 50 m i dopuszczalna prędkość jazdy 5 km/h;

– maksymalną (risk crossing) – pozwalającą na przekroczenie mostu w warunkach dużego ryzyka: mimośrodowość obciążenia jest niedopuszczalna, konieczne jest prowadzenie pojazdu przez przewodnika, na moście może przebywać tylko jeden pojazd, maksymalna prędkość jazdy to 5 km/h.

Uwzględniając przedstawione uwarunkowania, nośność mostu zależnie od warunków eksploatacyjnych i przyjętych wymagań może się zmieniać dwu–trzykrotnie. Z punktu widzenia taktyki najistotniejsza jest nośność nominalna dla wymaganej prędkości

[1] J. Łopatka *Assessment of river crossing possibility with existing pontoon bridge.* Materiały konferencyjne ITMS 2018.

[2] Z. Bursztynowski: *Mosty wojskowe. Cz. 3. Mosty pływające.* Wojskowa Akademia Techniczna. Warszawa 1970, s. 259–260.

[3] *Umowa standaryzacyjna NATO STANAG 2021.*

nurtu i głębokości przeszkody wodnej, ponieważ jest zdefiniowana dla warunków, w których możliwa jest sprawna przeprawa sprzętu. Dlatego ocena przydatności mostu wymaga analizy przeszkód wodnych.

CHARAKTERYSTYKA PRZESZKÓD WODNYCH

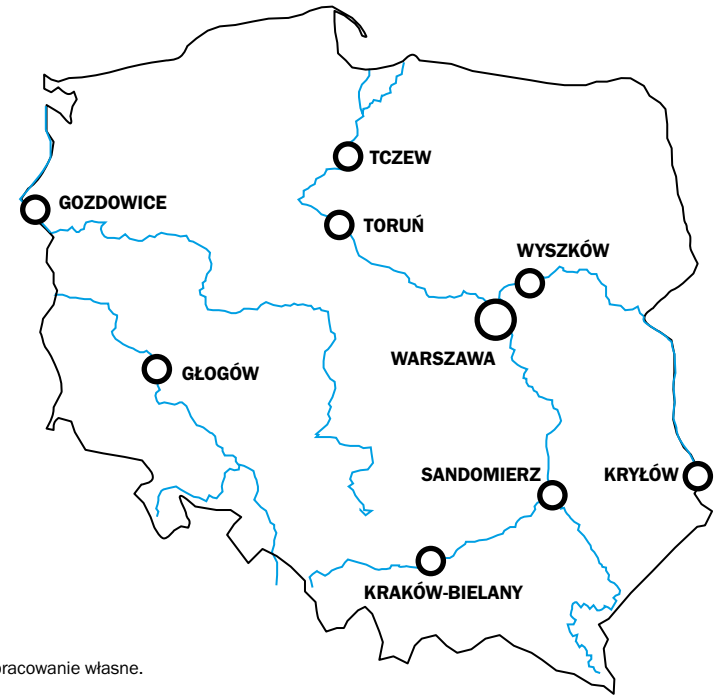
Podstawowym zadaniem Sił Zbrojnych RP jest gotowość do obrony własnego terytorium[4], dlatego też analizę ograniczono do przeszkód wodnych znajdujących się na terenie naszego kraju. Śródlądowe przeszkody wodne można podzielić na występujące na rzekach, kanałach i jeziorach. Jeziora są obiektami łatwymi do ominięcia, kanały natomiast nie występują zbyt często i stwarzają prostsze warunki do wykonania przeprawy pontonowej niż rzeki. W związku z tym najwięcej problemów przysparzają przeprawy rzeczne. Do analizy wytypowano główne przeszkody ograniczające manewr, czyli: Wisłę, Odrę i Bug. Rzeki te ze względu na występujące przepływy i szerokość są najtrudniejsze do pokonania. Ich koryta przebiegają w ważnych taktycznie i operacyjnie rejonach i są ulokowane w pobliżu dużych miast i granic kraju. Parametry rzek na całej ich długości analizuje się w wytypowanych punktach pomiarowych (rys. 1).

Wymagania odnoszące się do długości przeprawy wynikają bezpośrednio z szerokości przeszkody wodnej. Dane dotyczące szerokości rzek w branych pod uwagę miejscach pomiarowych zestawiono na rysunku 2.

Z pomiarów wynika, że w przeważającej liczbie punktów pomiarowych szerokość rzek mieści się w przedziale 70–120 m. Ponadto można zauważyć, że Odra za dopływem Warty na długości około 150 km osiąga szerokość około 200 m, Wisła za dopływem Sanu, na długości około 600 km – szerokość 250–350 m, natomiast Bug poniżej Muchawca przekracza 90 m. Należy jednocześnie zauważyć, że szerokość rzeki może się zwielokrotnić przy podwyższonych stanach wód. Wartości średnie i maksymalne prędkości nurtu analizowanych przeszkód wodnych przedstawiono na rysunku 3.

Średnie prędkości nurtu rzek rzadko przekraczają 1 m/s. Dostępne pomiary prędkości maksymalnych wskazują jednak, że mogą one być trzykrotnie większe w stosunku do prędkości średnich. Dlatego też można oszacować, że prędkości maksymalne w branych pod uwagę punktach pomiarowych osiągają wartość około 2–3 m/s. Potwierdzają to przeprowadzone badania, według których przy podwyższonych stanach wody prędkość nurtu w Wiśle na wysokości Warszawy osiąga 3,5 m/s[5]. Średnie i maksymalne głębokości wody w wybranych punktach pomiarowych przedstawiono na rysunku 4.

RYS. 1. POŁOŻENIE PUNKTÓW POMIAROWYCH NA MAPIE POLSKI



Opracowanie własne.

Z wykresu można odczytać, że średnia głębokość rzek wynosi zazwyczaj 2–4 m, natomiast głębokość maksymalna utrzymuje się w przedziale 3–6 m. Głębokość 6 m jest przekraczana tylko w najgłębszych miejscach, przy podwyższonych stanach wody. Oznacza to, że przy pokonywaniu przeszkód wodnych nie można pominąć destabilizującego działania zjawisk hydrodynamicznych. Maksymalne prędkości nurtu występują w miejscach najgłębszych, a maksymalne prędkości wody (około 3 m/s) przy głębokości od 3 do 5 m.

Przy organizacji przeprawy bardzo istotnym uwarunkowaniem jest również charakter brzegu. W Polsce rzeki na ogół nie są uregulowane. Występują na nich mielizny, a dno przy brzegu jest muliste. Są one też podatne na podmywanie spowodowane falowaniem mostu pontonowego.

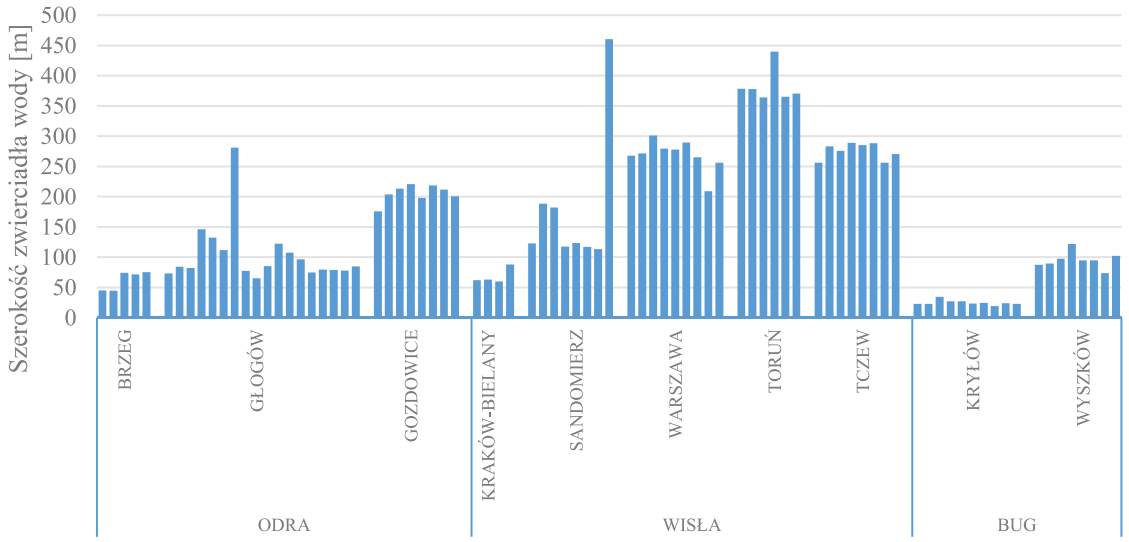
SPECYFIKACJA PRZEPRAWIANEGO SPRZĘTU

Podstawą klasyfikacji obciążenia obiektów mostowych jest STANAG 2021. Norma ta pozwala na

[4] *Koncepcja obronna Rzeczypospolitej Polskiej. MON 2017, s. 6.*

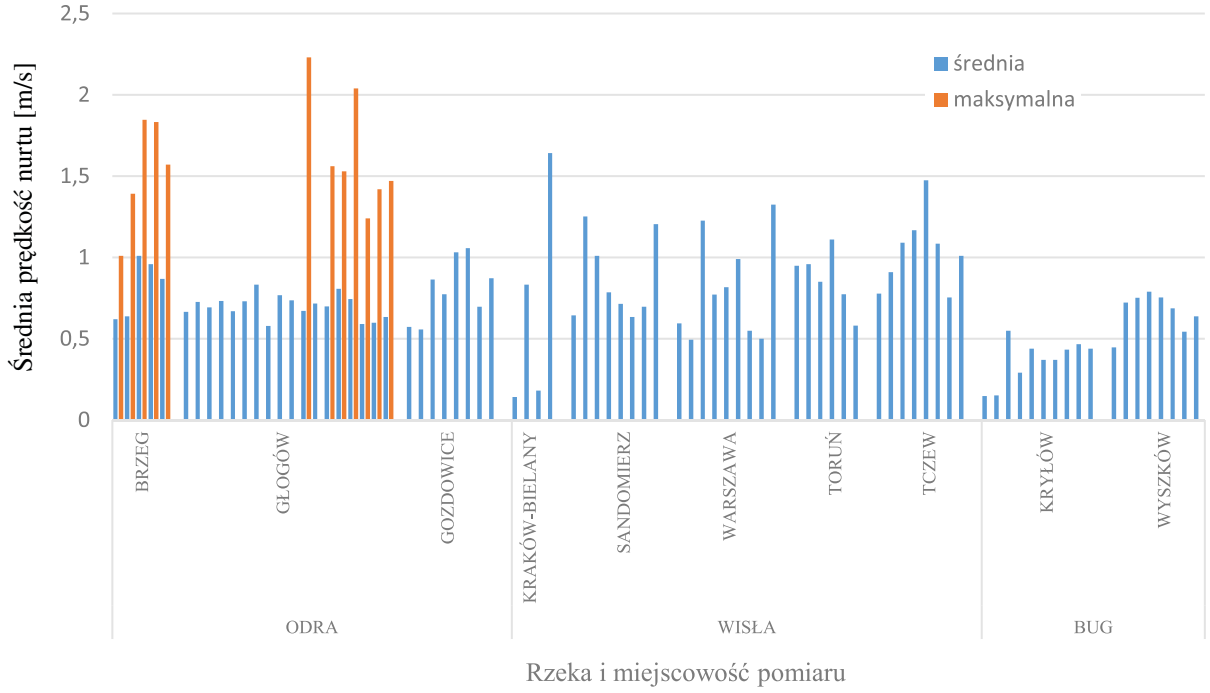
[5] A. Magnuszewski, M. Gutry-Korycka: *Przepływ wielkich wód Wisły we współczesnym korycie*. „Prace i Studia Geograficzne" 2009, T. 43, s. 153–162.

RYS. 2. SZEROKOŚĆ ZWIERCIADŁA WODY W PUNKTACH POMIAROWYCH W LATACH 2016–2017



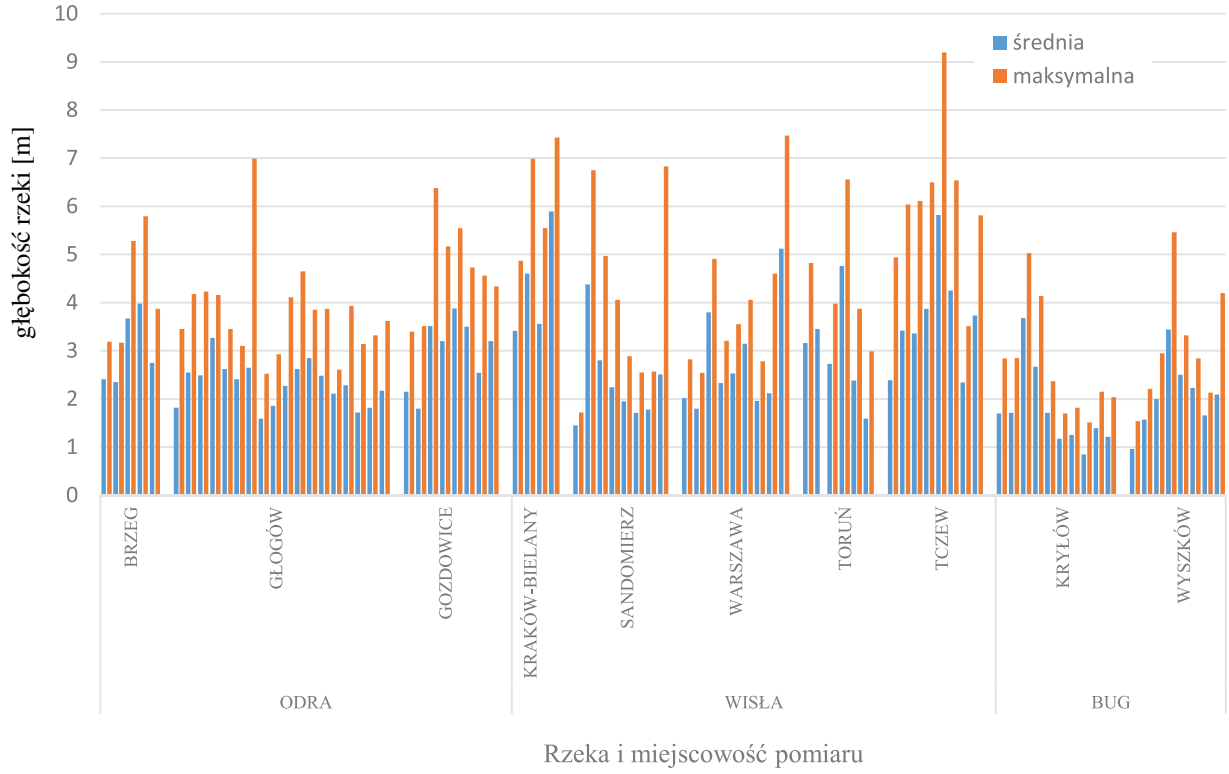
Opracowanie własne na podstawie danych Instytutu Meteorologii i Gospodarki Wodnej.

RYS. 3. PRĘDKOŚĆ NURTU WYBRANYCH PRZEKROJÓW W LATACH 2016–2017



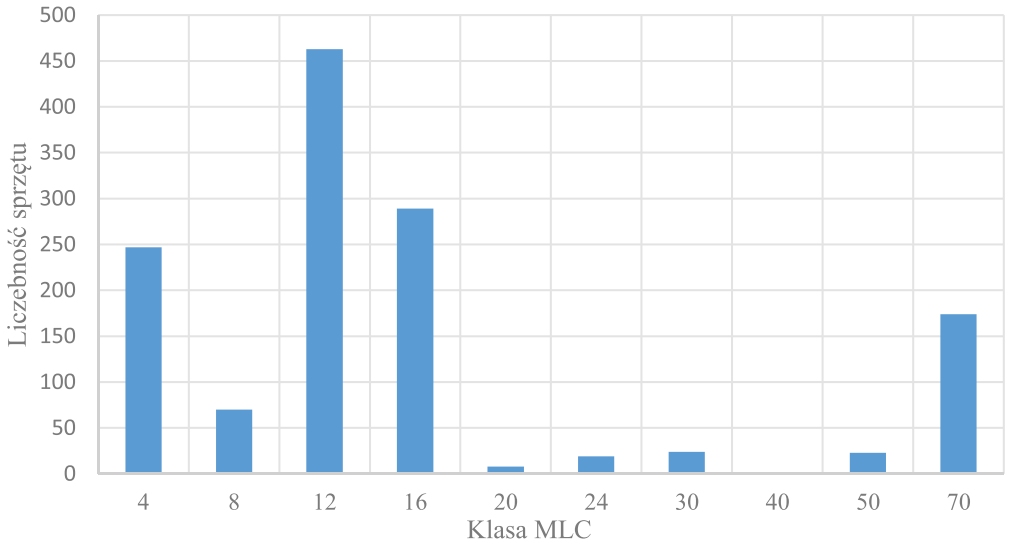
Opracowanie własne na podstawie danych Instytutu Meteorologii i Gospodarki Wodnej.

RYS. 4. ŚREDNIA I MAKSYMALNA GŁĘBOKOŚĆ WODY W PUNKTACH POMIAROWYCH W LATACH 2016–2017



Opracowanie własne na podstawie danych Instytutu Meteorologii i Gospodarki Wodnej.

RYS. 5. LICZEBNOŚĆ SPRZĘTU W BKPANC Z UWZGLĘDNIENIEM PODZIAŁU NA KLASĘ MLC



Opracowanie własne na podstawie: *Kompendium logistyka wojskowego*. SGWP, Zarząd Planowania Logistyki – P4, Warszawa 2014, s. 91.

1. **Park pontonowy PP-64 to konstrukcja wprowadzona do użytku w 1964 roku. W konfiguracji wstęgi podwójnej umożliwia przeprawę pojazdów o klasie MLC 80.**

BOGUSŁAW POLITOWSKI

W POLSCE RZEKI NIE SĄ UREGULOWANE. PRZY BRZEGU JEST MULISTE. SĄ ONE

przypisanie każdego pojazdu do określonej klasy (Military Load Class – MLC) i jednocześnie określa dla każdego obiektu mostowego najwyższą klasę pojazdu, który może być po nim przeprawiony. Umożliwia też szybką ocenę możliwości przeprawienia danego sprzętu po konkretnym moście.

W celu oszacowania obciążenia mostu różnymi klasami pojazdów przyjęto hipotetyczną organizację przeprawy przez most pontonowy Brygady Kawalerii Pancernej. Na rysunku 5 przedstawiono zestawienie liczebności pojazdów przeprawy w poszczególnych grupach MLC.

Sprzęt brygady kawalerii pancernej stanowią głównie pojazdy o klasie MLC 16 i niższych. Liczba tych, które nie przekraczają MLC 16, wynosi 1069, z kolei liczba o klasie większej od MLC 16 to 250, czyli jest ponadczterokrotnie mniejsza. Dysproporcja ta może być wykorzystana do zoptymalizowania konstrukcji mostu pontonowego pod kątem ograniczenia jego kosztów, masy i wielkości, przy zacho-

2. W armii USA użytkuje się most IRB. Konstrukcja bloku pontonowego jest wzorowana na radzieckim PMP. Inaczej niż w konstrukcji rosyjskiej, bloki pontonowe są przewożone na samochodach wyposażonych w uniwersalny system samoładowczy PLS.

3. Elementy rosyjskiego mostu pontonowego PP-2005

MO FEDERACJI ROSYJSKIEJ

WYSTĘPUJĄ NA NICH MIELIZNY, A DNO TEŻ PODATNE NA PODMYWANIE

waniu jak największej przepustowości. Zakładając, że most pontonowy będzie umożliwiał przeprawę dwujezdniową sprzętu o MLC 16 lub mniejszej, to wytrzymałościowo nie przekroczy to możliwości mostu mającego przeprawić pojazdy o MLC 70, pozwoli też dwukrotnie przyspieszyć przeprawę około 80% jednostek sprzętowych. Teoretycznie przekłada się to na szybsze o 40% zrealizowanie przeprawy w porównaniu do przeprawy jednojezdniowej.

Należy jednak zwrócić uwagę na tendencje rozwojowe sprzętu w naszych siłach zbrojnych. Do tej pory podstawowym samochodem transportowym był w nich Star 266 (MLC 12), jednak obecnie wprowadza się większe pojazdy logistyczne MLC 30[6]. W związku z tym można się spodziewać, że na przestrzeni lat rozkład masowy sprzętu przedstawiony na

[6] *Zakupy średnich i ciężkich ciężarówek przez siły zbrojne RP w 2011 roku.* „Nowa Technika Wojskowa" 2012 nr 6, s. 42–46.

TABELA. PODSTAWOWE PARAMETRY BLOKÓW PONTONOWYCH I JEDNOSTEK TRANSPORTOWYCH WYBRANYCH MOSTÓW PONTONOWYCH TYPU WSTĘGA

	PP-64 (Polska)	PFM (Francja)	IRB (USA)	PP-2005 (Rosja)	
				wstęga podwójna	wstęga pojedyncza
Rok opracowania	1964	1984	2002	2005	
Nominalna nośność MLC	80W/80T	80W/70T	96W/80T	66T	130W
Dopuszczalna prędkość nurtu [m/s]	2,9	2,0	2,1	3,0	3,5
Szerokość wstęgi [m]	2x6,25	9,8	8,4	8,28	15,5
Długość pontonu/bloku [m]	1,84/3,7	10,2	6,71	7,36	
Wysokość bloku [m]	0,90	0,73	0,75	0,75	
Masa bloku pontonowego [kg]	3600	10 500	6350	8550	17 100
Szerokość pasa ruchu [m]	4,35	4,0	4,50	4,50	2x4,50
Prędkość jazdy pojazdów gąsienicowych [km/h]	15	15	15	30	
Prędkość jazdy pojazdów kołowych [km/h]	40	25	20	brak ograniczeń	
Nośność dwóch pasów ruchu [W]	2x40	–	2x20	2x30	2x66T
Liczba kutrów/bloków z napędem	6	–	6	2/4	4/8
Liczba samochodów	60	11	21	20	40
Liczba żołnierzy	126	42	65	62	124

Opracowanie własne na podstawie: J. Łopatka: *Assessment of river crossing possibility with existing pontoon bridge*. Materiały konferencyjne ITMS 2018.

rysunku 5 zmieni się w kierunku zwiększenia liczebności klas MLC 20, 24 i 30. Dlatego też dobierając nowy sprzęt przeprawowy, należałoby wziąć pod uwagę perspektywiczne umożliwienie przeprawy dwujezdniowej sprzętu klasy MLC 30.

Do wykorzystania potencjału przepustowości przeprawy dwujezdniowej niezbędne jest odpowiednie przygotowanie dróg dojazdowych. Wiąże się to z wykonaniem dodatkowych prac w rejonie przeprawy. Dlatego kwestia konieczności przystosowania mostu do tego typu przepraw jest dyskusyjna. Niepodważalna natomiast jest potrzeba przeprawiania pojazdów gąsienicowych klasy MLC 70.

MOSTY PONTONOWE

Analiza dostępnych konstrukcji pozwoli na ocenę możliwości istniejących parków pontonowych i wyłonienie rozwiązań odpowiadających potrzebom naszych sił zbrojnych. Park pontonowy PP-64 (fot. 1) to konstrukcja polska wprowadzona do użytku w 1964 roku. W konfiguracji wstęgi podwójnej park umożliwia przeprawę pojazdów o klasie MLC 80 przy prędkości nurtu 2,9 m/s oraz dwujezdniową przeprawę pojazdów o MLC 40[7], co całkowicie spełnia wymagania przekraczania przeszkód wodnych w warunkach dużego ryzyka. Zasadniczym ograniczeniem konstrukcji jest długość pojedynczego bloku pontonowego, która wynosi zaledwie 3,6 m. Konsekwencją tego jest konieczność użycia dużej liczby bloków pontonowych, co tym samym wydłuża czas budowy przeprawy. Do budowy 100-metrowego odcinka mostu w konfiguracji wstęgi podwójnej, zdolnej do przeprawienia czołgu klasy MLC 70, potrzeba 60 pojazdów, 126 żołnierzy (tab.) i czasu wynoszącego około 60 min. Małe wymiary pojedynczego bloku pontonowego wynikają z ograniczonych możliwości pojazdu nośnika, jakim w momencie projektowania mostu był Star 660.

Kolejne ograniczenia stwarzają pontony brzegowe, które na skutek falowania mostu powodują intensywne podmywanie brzegów. Z tego względu konieczne jest wcześniejsze wzmocnienie brzegów faszynami, lekkimi pokryciami drogowymi itp. Podmywanie brzegów prowadzi także do okresowej zmiany miejsca przeprawy, co znacznie ogranicza jej przepustowość. Manewrowanie blokami pontonowymi na wodzie odbywa się z wykorzystaniem kutrów holowniczych o dużym zanurzeniu napędzanych śrubą napędową, co uniemożliwia pracę w zbiornikach płytkich.

Park pontonowy PP-2005 jest użytkowany w armii rosyjskiej. Konstrukcja ta jest kolejnym ulepszeniem mostu PMP z 1962 roku. W porównaniu do PP-64 ce-

[7] *Park pontonowy PP-64 opis i użytkowanie*. MON, Szefostwo Wojsk Inżynieryjnych. Warszawa, 1986, s. 230.

chuje się ona znacznie większą długością bloku pontonowego wynoszącą 6,7 m w wypadku PMP i aż 7,2 m w wypadku PP-2005. 100-metrowy odcinek mostu PP-2005 wykonuje się z użyciem 20 pojazdów. Most w wersji zmodernizowanej umożliwia przejazd pojazdów gąsienicowych z prędkością 30 km/h, co jest najlepszą wartością spośród występujących konstrukcji. Daje również możliwość dwujezdniowego przeprawiania pojazdów w konfiguracji wstęgi podwójnej. Istotną cechą jest zastosowanie płóz hydrodynamicznych, które przeciwdziałają destabilizacji mostu przy silnym nurcie. Pozwalają one na przeprawianie sprzętu z nominalnym obciążeniem przy prędkości nurtu do 3,5 m/s. Mostem na wodzie manewruje się z użyciem specjalistycznych bloków silnikowych, które stanowią jego integralną część, lub kutrów holowniczych.

W armii USA użytkuje się most IRB (fot. 2). Konstrukcja bloku pontonowego jest wzorowana na radzieckim PMP (fot. 3). Inaczej niż w konstrukcji rosyjskiej, bloki pontonowe są przewożone na samochodach wyposażonych w uniwersalny system samozaładowczy PLS. Dlatego też ich transport może być realizowany z użyciem standardowych samochodów wyposażonych w ten system.

Do budowy 100-metrowego odcinka mostu IRB potrzeba 21 pojazdów, 65 żołnierzy i czasu wynoszącego 30 min. Blok pontonowy jest wykonany ze stopów metali lekkich. Ułatwia to jego wykorzystanie w trudnym terenie, a także umożliwia transport śmigłowcem. Nominalna nośność MLC mostu przy małych prędkościach nurtu wynosi 96 dla pojazdów gąsienicowych i 80 dla kołowych, jednak dla prędkości nurtu 3 m/s nośność nie przekracza MLC 50. Jest to poważne ograniczenie taktyczne, gdyż w tych warunkach nie ma możliwości przeprawy czołgów. Ponadto most nie pozwala na dwutorowe przeprawianie sprzętu. Manewrowanie blokami na wodzie odbywa się z użyciem płaskodennych kutrów holujących napędzanych pędnikami strugowodnymi. Konstrukcja kutrów i małe zanurzenie bloków pontonowych pozwalają na użycie mostu na płytkich akwenach.

W armii francuskiej jest użytkowany *most PFM* (fot. 4). Ma on największą długość bloku pontonowego (10 m). Pozwala to na znaczne ograniczenie liczby obsługujących go żołnierzy i czasu potrzebnego na budowę przeprawy. Do powstania 100-metrowego odcinka mostu potrzeba zaledwie dziesięciu pojazdów, 42 żołnierzy i czasu wynoszącego około 30 min. Bloki pontonowe łączy się bez stosowania przegubów, a zamiast pontonów brzegowych wykorzystuje się rampy najazdowe. Przekłada się to na ograniczenie zjawiska podmywania brzegów. Manewrowanie blokami odbywa się z użyciem silników zaburtowych. Brak kutrów holowniczych oznacza też mniejszą liczbę pojazdów transportowych w zestawie. Park jest przewożony na specjalistycznych naczepach przy użyciu ciągników siodłowych. Nośność nominalna mostu przy prędkości nurtu 2 m/s wynosi MLC 70 dla pojazdów gąsienicowych i MLC 80 dla kołowych.

AD MESKENS

4.

MOST PFM

W armii francuskiej jest użytkowany most PFM. Ma on największą długość bloku pontonowego (10 m). Pozwala to na znaczne ograniczenie liczby obsługujących go żołnierzy i czasu potrzebnego na budowę przeprawy.

BYĆ ŚWIADOMYM

Analizując konstrukcje mostów pontonowych wykorzystywanych w innych armiach, można wyciągnąć następujące wnioski:

– z punktu widzenia zdolności przeprawowych most PP-64 jest bardzo dobry, konstrukcje PFM i IRB mu nie dorównują;

– największą wadą polskiego mostu jest duża liczba żołnierzy potrzebnych do wykonania przeprawy, pod tym względem najlepszy jest most PFM;

– z uwagi na dopuszczalną prędkość nurtu mosty PFM i IRB znacznie ograniczają dobór miejsca przeprawy.

Biorąc pod uwagę przedstawioną charakterystykę przeszkód wodnych w Polsce i dobierając parametry nowego mostu dla naszej armii, należy uwzględnić:

– przeprawianie pojazdów klasy MLC 70 przy prędkości nurtu około 3 m/s;

– rozważenie dwujezdniowego przeprawiania pojazdów o klasie do MLC 30;

– zastosowanie płóz hydrodynamicznych;

– wprowadzenie silników zaburtowych do manewrowania blokami;

– użytkowanie ramp najazdowych lub odpowiednio długich pontonów brzegowych;

– zastosowanie w konstrukcji stopów metali lekkich. ■

Integracja **sieci LAN**

ZAUTOMATYZOWANA I NIEZAWODNA WYMIANA DANYCH MIĘDZY ODDALONYMI NA ZNACZNĄ ODLEGŁOŚĆ STANOWISKAMI DOWODZENIA W RAZIE BRAKU DOSTĘPU DO SYSTEMU ŁĄCZNOŚCI SATELITARNEJ JEST ZAPEWNIANA PRZEZ PODSYSTEM ŁĄCZNOŚCI RADIOWEJ HF.

kmdr por. mgr inż. Wiesław Jabłoński

Autor jest szefem Wydziału Monitoringu Centrum Wsparcia Systemów Dowodzenia Dowództwa Generalnego Rodzajów Sił Zbrojnych.

Pod koniec zimnej wojny US NAVY poszukiwała niezawodnego systemu komunikacji z rozmieszczonymi na morzach i oceanach całego globu grupami uderzeniowymi, których podstawowym elementem były lotniskowce. Zasadniczym zadaniem stawianym łączności była możliwość zapewnienia komunikacji w sytuacji prowadzenia przez przeciwnika efektywnej walki radioelektronicznej, wykorzystania impulsów elektromagnetycznych lub detonacji ładunków jądrowych w wyższych warstwach atmosfery w celu obezwładnienia urządzeń łączności satelitarnej. W celu budowy systemu spełniającego stawiane wymagania w latach osiemdziesiątych XX wieku rozpoczęto prace badawcze nad opracowaniem rozwiązań całkowicie cyfrowych systemów łączności radiowej HF.

POTRZEBY

Zasadniczym czynnikiem warunkującym wybór medium transmisyjnego w postaci fal radiowych HF były ich właściwości propagacji w atmosferze oraz fakt, że nawet po uderzeniu jądrowym w górnych warstwach atmosfery stan jonosfery już po upływie kilku godzin od wybuchu zapewniał wystarczające warunki do nawiązania łączności w tym paśmie. Natomiast odtworzenie systemu łączności satelitarnej wymagało umieszczenia na orbicie nowych satelitów. Operacja taka wymagałaby sporo czasu na przygotowanie i start rakiet nośnych z nowymi satelitami, co z pewnością jest nie do przyjęcia z powodów operacyjnych i ekonomicznych w sytuacji pełnoskalowego konfliktu zbrojnego lub lokalnego o dużej intensywności, w którym uczestniczą przeciwnicy o podobnym potencjalnie militarnym. Rzeczywisty bowiem koszt odtworzenia systemu łączności satelitarnej wielokrotnie przewyższy koszt eksploatacji cyfrowych systemów łączności radiowej HF. Tak duże szacunkowe koszty nie będą do zaakceptowania przez żadną ze stron potencjalnego konfliktu. Ponadto bardzo korzystne warunki propagacji radiowej fali powierzchniowej HF nad powierzchnią morza, przy odpowiedniej mocy emisji, umożliwią zastosowanie łączy radiowych na odległość do kilku tysięcy kilometrów.

Dodatkowym czynnikiem mającym wpływ na prowadzone w Stanach Zjednoczonych badania był fakt, że systemy radiokomunikacji HF mają swoją ugruntowaną pozycję w wojskowych systemach łączności na wszystkich poziomach dowodzenia oraz w radiokomunikacji cywilnej. Opracowano więc rozwiązania w postaci niezawodnych, cyfrowych systemów transmisji danych w paśmie częstotliwości radiowych HF. Były one podstawą budowy pierwszych mobilnych systemów klasy C2 (Command and Control – dowodzenie i kontrola) na szczeblu taktycznym oraz klasy C4I (Command, Control, Communications, Computers and Intelligence – dowodzenie, kontrola, łączność, przetwarzanie danych i rozpoznanie) na szczeblu operacyjno-strategicznym.

W następnych latach rozwój technik cyfrowego przetwarzania sygnałów oraz nowe wyrafinowane metody

Zasadniczym czynnikiem warunkującym wybór medium transmisyjnego w postaci fal radiowych HF były ich właściwości propagacji w atmosferze oraz fakt, że nawet po uderzeniu jądrowym w górnych warstwach atmosfery stan jonosfery już po upływie kilku godzin od wybuchu zapewniał wystarczające warunki do nawiązania łączności w tym paśmie.

JAROSŁAW WIŚNIEWSKI

modulacji sygnałów radiowych wraz z postępem technologicznym w dziedzinie podzespołów i elementów elektronicznych wykorzystywanych do budowy nowoczesnych środków krótkofalowej (HF) łączności radiowej pozwoliły implementować w konstrukcjach radiostacji:

• modulacje modemowe zgodnie ze: STANAG-iem 4285, STANAG-iem 4529, STANAG-iem 4415, STANAG-iem 4539 i normą MIL-STD-188-110C;

• funkcje automatycznego zestawienia połączenia [ALE (automatic link establishment) 2G MIL-STD-188-141B App. A lub 3G według STANAG-u 4538 oraz MIL-STD-188-141B App. C];

• interfejsy i protokoły zdalnego sterowania środków radiowych.

Nowe rozwiązania techniczne przyczyniły się do dalszej ewolucji stacji radiowych w radiowe węzły HF, udostępniające usługę wymiany poczty elektronicznej (e-mail) oraz wymiany danych z wykorzystaniem pakietów protokołu IP[1] między znajdującymi się w znacznej odległości mobilnymi lub stacjonarnymi stanowiskami komputerowymi oraz sieciami LAN na platformach lub stanowiskach dowodzenia (SD). Jest oczywiste, że stanowiska komputerowe wraz z sieciami LAN stanowią infrastrukturę teleinformatyczną niezbędną do budowy i eksploatacji systemów klasy C2 i C4I.

Wymienione systemy wymagają wydajnej, niezawodnej, bezpiecznej i bezprzewodowej transmisji danych. W celu spełnienia tych wymagań stosuje się radiowe węzły HF, które zapewniają transmisję danych w rozległych sieciach radiowych HF (określanych mianem HF WAN). Są one eksploatowane w warunkach stacjonarnych w centrach (węzłach) nadawczo-odbiorczych i stacjonarno-mobilnych w ramach polowych węzłów łączności oraz mobilnych na pokładzie okrętów i statków powietrznych, w wozach dowodzenia i aparatowniach wojsk lądowych. We wszystkich wymienionych lokalizacjach węzły HF pozwalają na wymianę danych między sieciami LAN, która integruje terminale i konsole systemów klasy C2 oraz C4I z wykorzystywanymi na ich potrzeby serwerami oraz systemami łączności radiowej lub satelitarnej (rys. 1).

RADIOWY WĘZEŁ HF

Zasadniczym dokumentem mającym praktyczne znaczenie przy projektowaniu i budowaniu radiowych węzłów HF jest opracowany przez Agencję Standaryzacyjną NATO (NSA – NATO Standardization Agency) uzgodnienie standaryzacyjne STANAG 5066 *Profile for high frequency (HF) radio data communications*.

Definiuje ono wymagania dotyczące transmisji danych z wykorzystaniem węzłów HF. Ich spełnienie ma na celu zapewnienie interoperacyjności i niezawodności systemu łączności HF. Służą temu dwa interfejsy: Common Air Interface i Non-HF Interface. Pierwszy odpowiada za wymianę informacji (transmisję danych) w kanale krótkofalowym (HF), drugi zaś za współdziałanie węzła HF z użytkownikami zewnętrznymi żądającymi dostępu do kanału HF przez ten węzeł. STANAG 5066 definiuje użytkowników zewnętrznych jako aplikacje realizujące funkcje serwera lub klienta dla usług udostępnianych przez węzeł HF oraz następujące pojęcia:

• węzeł HF – zespół urządzeń, w skład którego wchodzi: radiostacja HF, modem HF oraz urządzenie kryptograficzne (w nowoczesnych rozwiązaniach radiostacji HF są one integrowane w ramach jednego urządzenia, tzw. transceivera; ponieważ resurs eksploatacji sprzętu radiowego może wynosić do 20 lat, w STANAG-u wskazano na możliwość wykorzystania starszego sprzętu, który nie integruje modemów radiowych i modułów kryptograficznych);

• podsieć HF – podsieć składająca się z węzłów HF, zapewniająca usługi transmisji danych dla zewnętrznych użytkowników lub klientów aplikacji;

• protokół ARQ (Auto Repeat Request) – należący do rodziny protokołów warstwy transmisji danych (Data Link Protocol), działający na zasadzie potwierdzeń poprawnie odebranego każdego wysłanego pakietu danych PDU[2]. Często nazywany protokołem drugiej generacji (2G);

• funkcja ADR (Adaptive Data Rate) – funkcja polegająca na zmianie prędkości transmisji w zależności od jakości kanału HF.

Transmisja danych w kanale HF zgodnie z wymienioną umową standaryzacyjną wymaga posiadania modemu HF spełniającego wymagania zawarte w uzgodnieniach STANAG 4285 i STANAG 4529, którym można zdalnie sterować za pomocą aplikacji lub sprzętu (odpowiadającego warunkom podanym w STANAG-u 5066).

Możliwe jest także użycie modemu HF o charakterystyce podanej w standardzie MIL-STD-188-110C lub gwarantującego nowoczesną modulację oraz techniki detekcji i korekty błędów podczas transmisji danych.

Transmisja danych w kanale HF zgodnie ze STANAG-iem 5066 wymaga posiadania radiostacji pracującej z modulacją SSB[3], spełniającej wymagania zawarte w uzgodnieniach STANAG 4203[4]. Zakłada się, że nie steruje się zdalnie parametrami tej radiostacji.

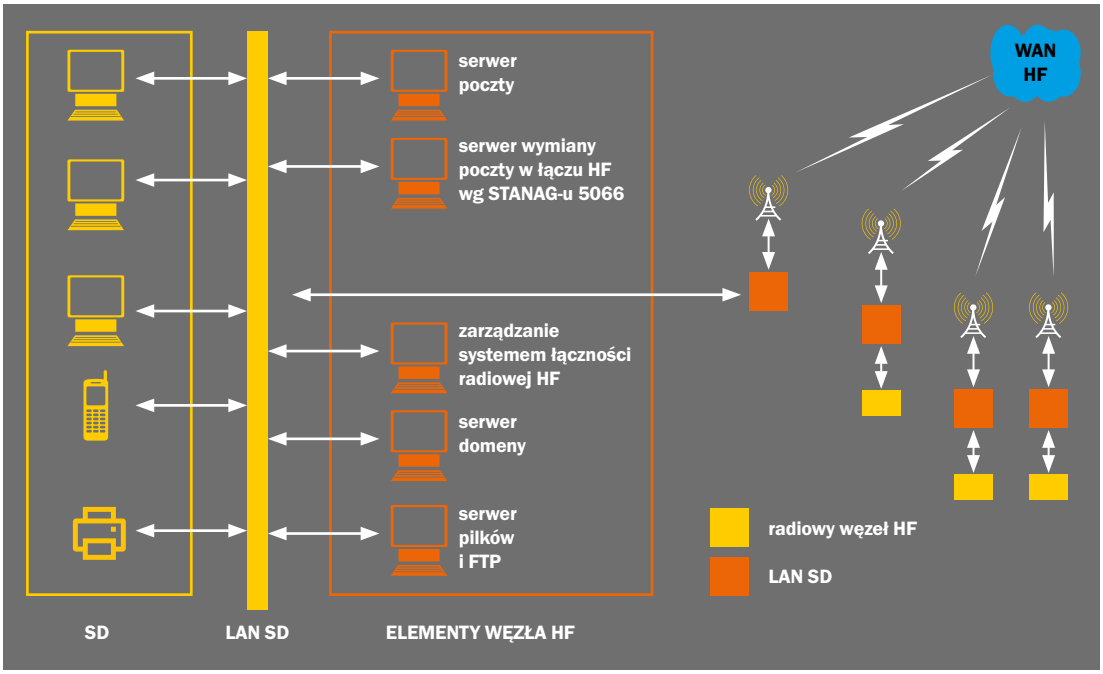
[1] IP (Internet Protocol) – protokół sieciowy wykorzystywany do transmisji danych przez lokalne sieci komputerowe i Internet.

[2] PDU (Protocol Data Unit – jednostka danych protokołu) – struktura danych zdefiniowana w STANAG-u 5066, służąca do przesyłania pakietów danych między dwoma lub więcej stacjami.

[3] SSB (Single Side Band) – rodzaj radiowej emisji, w czasie której emitowana jest tylko jedna wstęga boczna bez fali nośnej; LSB (Lower Side Band) – rodzaj radiowej emisji SSB, w czasie której emitowana jest tylko dolna wstęga boczna bez fali nośnej; USB (Upper Side Band) – rodzaj radiowej emisji SSB, w czasie której emitowana jest tylko górna wstęga boczna bez fali nośnej.

[4] STANAG 4203 *Technical standards for single channel HF radio equipment*.

RYS. 1. OGÓLNA KONCEPCJA BUDOWY SIECI RADIOWEJ HF



Opracowanie własne na podstawie: MIL-STD-188-110C i STANAG-u 5066.

Bezpieczną transmisję danych w kanale HF zgodnie ze STANAG-iem 5066 zapewnia zastosowanie następujących typów urządzeń kryptograficznych wskazanych przez NATO, czyli BID-950 i KG-84C.

Do najważniejszych funkcji węzła HF należy zaliczyć:

• wymianę wiadomości pocztowych zgodnie z protokołem HMTP (High Frequency Mail Transfer Protocol – wysokiej częstotliwości protokół transferu poczty). Jest to protokół SMTP (Simple Mail Transfer Protocol – prosty protokół transferu poczty określony w RFC-821) zmodyfikowany na potrzeby transmisji wiadomości pocztowych w kanale HF;

• wymianę wiadomości pocztowych zgodnie z protokołem CFTP (Compressed File Transfer Protocol – protokół transferu skompresowanych plików). Dokonuje on kompresji wiadomości przed jej wysłaniem drogą radiową oraz dekompresji przed jej wysłaniem do skrzynki pocztowej;

• przesyłanie danych przenoszonych przez pakiety IP zgodnie z wymaganiami określonymi w Aneksie F (STANAG 5066).

NIEZAWODNA WYMIANA DANYCH

Ta funkcja łącza radiowego HF jest zapewniona dzięki użyciu protokołu ARQ w warstwie łącza danych z zastosowaniem nowej generacji jednotonowego modemu radiowego HF oraz innych modemów z nowoczesną modulacją i technikami kodowania przenoszonych danych użytkownika.

Protokół ten odpowiada za nadzór nad poprawnością przesyłanych pakietów danych PDU. Każdy z nich ma dołączoną sumę kontrolną CRC (Cyclic Redundancy Check – cykliczna kontrola nadmiarowości). Po odebraniu pakietu danych następuje analizowanie jego poprawności. Jeżeli zostanie wykryty błąd, wysyłane jest żądanie ponownego jego przesłania.

STANAG 5066 definiuje dwa zasadnicze tryby transmisji:

– ARQ, w którym następuje potwierdzenie pakietu (przez pakiet odpowiedzi ACK informuje o istotności pola „numer potwierdzenia") oraz stosuje się technikę przesuwnego okna. Komunikujące się aplikacje mogą również wymagać potwierdzenia każdego wysłanego pakietu. Jest to konieczne dla wymiany typu punkt–punkt. Ten tryb można porównać do funkcjonowania protokołu TCP[5];

– NON-ARQ jest trybem transmisji, w którym węzeł odbiorczy nie potwierdza poprawnego odbioru pakietów. Aplikacja odbierająca próbuje odtworzyć uszkodzoną część pakietu z kolejnych odbieranych. Tryb ten zapewnia transmisję typu punkt–punkt, punkt–grupa

[5] TCP (Transmission Control Protocol – protokół kontroli transmisji) – protokół sieciowy używany do transmisji danych przez lokalną sieć komputerową i Internet.

TABELA 1.
KATEGORIE KLIENTÓW APLIKACJI ZEWNĘTRZNYCH

Lp.	Typ klienta / aplikacji	SAP ID
1	Subnet management client	0
2	Character-Oriented Serial Stream (COSS) Client	1
3	STANAG 4406 Annex E – Tactical Military Message Handling System (T-MMHS) Client	2
4	HMTP (HF Mail Transfer Protocol)	3
5	HFPOP (HF Post-Office Protocol)	4
6	HF CHAT*	5
7	Reliable Connection-Oriented Protocol (RCOP) / Extended Client	6
8	Unreliable Datagram Oriented Protocol (UDOP) / Extended Client	7
9	Ether client	8
10	IP client	9
11	Reserved – for future assignment – zarezerwowane do wykorzystania w przyszłości	10–11
12	Compressed File Transfer Protocol (CFTP)	12
13	Unassigned – available for arbitrary use – dostępne do wykorzystania	13–15

*CHAT – pogawędka, rodzaj rozmowy między dwoma lub wieloma użytkownikami komputerów za pośrednictwem Internetu lub innej sieci komputerowej, polegającej na naprzemiennym przesyłaniu wiadomości tekstowych.

Opracowanie własne na podstawie STANAG-u 5066.

Legenda:
• COSS – Character-Oriented Serial Stream – zorientowany znakowo strumień danych szeregowych;
• COSS Client – usługa, która przesyła dane z portu szeregowego przez łącze HF. Zachowuje się jak agent między aplikacją używającą portu szeregowego do komunikacji i stosem protokołu STANAG 5066, który faktycznie przesyła pakiety przez łącze radiowe HF, używając dołączonych modemów i transceiverów;
• HMTP – HF Mail Transfer Protocol – protokół służący do transmisji e-maili w kanale HF. Opiera się na protokole SMTP (Simple Mail Transfer Protocol), ale jest szybszy dzięki zmniejszonemu narzutowi na potwierdzanie. Powinien być używany tylko wtedy, gdy jedna ze stacji partnerskich nie obsługuje protokołu CFTP dla transmisji e-maili;
• HMTP Client – usługa, która przesyła e-maile za pomocą protokołu HMTP. Zachowuje się jak agent między klientem e-mail w sieci a stosem protokołu STANAG 5066, który faktycznie przesyła pakiety danych przez łącze radiowe HF z zastosowaniem dołączonych modemów i transceiverów;
• HFPOP – HF Post-Office Protocol – protokół służący do odbioru e-maili w kanale HF, oparty na protokole POP (Post-Office Protocol);
• CFTP – Compressed File Transfer Protocol – skompresowany protokół transferu plików, służący do transmisji e-maili za pomocą HF, używający kompresji danych. Wyjątkowo przydatny do przesyłania dużych objętościowo e-maili;
• CFTP Client – usługa, która przesyła e-maile, używając protokołu CFTP. Zachowuje się jak agent między klientem e-mail w sieci a stosem protokołu STANAG 5066, który faktycznie przesyła pakiety danych przez łącze radiowe HF za pomocą dołączonych modemów i transceiverów;
• IP – Internet Protocol – protokół sieciowy wykorzystywany do transmisji danych przez lokalne sieci komputerowe i Internet;
• IP client – usługa, która przesyła datagramy IP przez łącze HF. Zachowuje się jak agent między aplikacją wykorzystującą IP do komunikacji a stosem protokołu STANAG 5066, który faktycznie przesyła pakiety danych przez łącze radiowe HF Z zastosowaniem dołączonych modemów i transceiverów.

i broadcast[6]. Można go porównać do protokołu UDP (User Datagram Protocol – protokół datagramów użytkownika).

W STANAG-u tym zdefiniowano także maksymalny rozmiar pakietu wymienianego między SIS–SIS (Subnetwork Interface Sublayer – podwarstwa interfejsu podsieci), który wynosi 2048 bajtów, gdy jest używany tryb transmisji punkt–punkt (ARQ lub NON-ARQ), oraz 4096 bitów podczas transmisji typu broadcast (NON-ARQ).

Funkcja ADR zapewnia zmianę prędkości transmisji w razie zmiany jakości kanału HF. Pogorszenie tej jakości przejawia się w zwiększeniu powtórzeń w przesyłaniu ramek. Liczbę powtórzeń w zależności od prędkości transmisji definiuje STANAG 5066. W sytuacji gdy dana ramka jest powtarzana maksymalną ilość razy, dochodzi do automatycznej zmiany prędkości transmisji. Zmiana ta jest możliwa wówczas, gdy zastosowany modem HF wspiera implementację uzgodnień zawartych w wymienionym dokumencie standaryzacyjnym. Oznacza to, że dany modem HF ma zaimplementowaną obsługę poleceń zmiany prędkości i przeplotu. Polecenia te są przekazywanych przez interfejs, np. RS-232, do modemu HF z dołączonego terminalu, na którym jest uruchomiona aplikacja z implementacją uzgodnień według wskazanego STANAG-u.

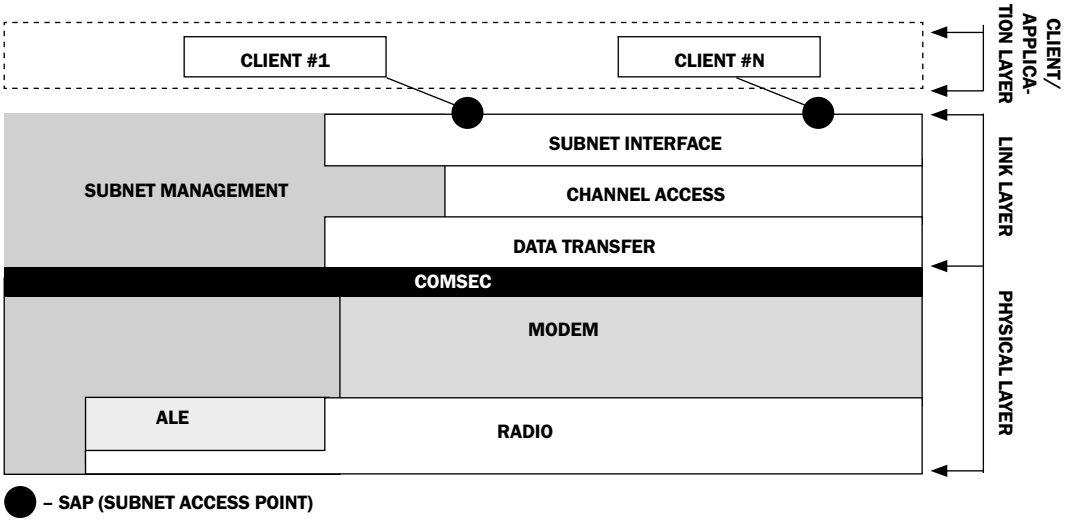
Non-HF Interface odpowiada za współdziałanie węzła HF z klientami aplikacji zewnętrznych żądającymi dostępu do kanału krótkofalowego przez ten węzeł. Uzgodnienie standaryzacyjne rozróżnia maksymalnie 16 różnych klientów aplikacji zewnętrznych. Każdy z nich ma przydzielony charakterystyczny identyfikator, tzw. SAP ID (Subnet Access Point Identifier) – patrz tabela 1.

MODEL OSIRM

W celu ułatwienia poprawnej implementacji poszczególnych funkcji zdefiniowanych przez STANAG

[6] Broadcast rozsiewczy (rozgłoszeniowy) – tryb transmisji danych polegający na wysyłaniu przez jeden port (kanał informacyjny) pakietów, które powinny być odebrane przez wszystkie pozostałe porty przyłączone do danej sieci.

RYS. 2. PODWARSTWY W SYSTEMIE INFORMATYCZNYM WEDŁUG MODELU OSIRM



Opracowanie własne na podstawie STANAG-u 5066.

5066 przypisano je do określonych podwarstw (rys. 2). Te zawierające funkcje modelu OSIRM (ISO OSI RM – ISO Open Systems Interconnection Reference Model – model odniesienia łączenia systemów otwartych) powinny być umieszczone w warstwie fizycznej oraz łącza danych. Na rysunku 2 przedstawiono również warstwę klientów (aplikacji), która nie jest definiowana przez wskazany STANAG.

Elementy systemu informatycznego według modelu OSIRM są następujące:

• **Subnetwork Interface Sublayer** – podwarstwa SIS inicjuje, ustanawia połączenie i realizuje zakończenie połączenia sesji wymiany danych z innym węzłem HF. Nadzoruje przebieg wymiany danych między klientami i aplikacjami zewnętrznymi a węzłem HF oraz między równorzędną warstwą innego węzła HF. Podwarstwa występuje jako implementacja programowa STANAG-u 5066.

• **Channel Access Sublayer** – podwarstwa CAS obsługuje żądania warstwy SIS dotyczące utworzenia lub przerwania fizycznego połączenia. Informuje warstwę SIS o zmianach stanów fizycznego połączenia. Występuje jako implementacja programowa.

• **Data Transfer Sublayer** – podwarstwa DTS obsługuje protokół transmisji danych ARQ oraz funkcję automatycznej zmiany prędkości transmisji danych w odpowiedzi na zmianę jakości kanału krótkofalowego (ADR). Występuje jako implementacja programowa.

• **Communications Security Sublayer** – podwarstwa COMSEC zabezpiecza łączność HF przez wykorzystanie do tego celu urządzeń kryptograficznych zatwierdzonych przez NATO. Występuje jako implementacja sprzętowa.

• **Modem Sublayer** – podwarstwa MS zapewnia cyfrową transmisję danych w kanale HF według STANAG-u 4285, STANAG-u 4529 i standardu MIL-STD-188-110A. Występuje jako implementacja sprzętowa.

• **Automatic Link Establishment Sublayer** – podwarstwa ALES zapewnia automatyzację procesu zestawiania połączenia w radiowym kanale HF. Występuje zazwyczaj jako implementacja sprzętowa w radiostacji HF.

• **Radio Equipment Sublayer** – podwarstwa RES obejmuje wyposażenie wymagane do zapewnienia łączności HF między dwoma węzłami. Występuje jako implementacja sprzętowa. Powinna spełniać wymagania zawarte w STANAG-u 4203.

• **Subnet Management Sublayer** – podwarstwa SMS dysponuje interfejsami do każdej podwarstwy. W rozumieniu uzgodnień STANAG-u 5066 główna jej funkcja to Automatic Link Maintenance (ALM) w postaci automatycznego sterowania parametrami modemu HF (funkcja ADR) oraz zgłoszenia żądania zmiany częstotliwości do podwarstwy ALES. Występuje jako implementacja programowa.

Obecnie w Siłach Zbrojnych RP są eksploatowane następujące implementacje STANAG-u 5066:

– oprogramowanie RDC-9000WMS opracowane przez OBR CTM SA;

– oprogramowanie R&S STANAG 5066 firmy Rohde & Schwarz;

– bezprzewodowy terminal wiadomości RF-6760W skonstruowany przez firmę Harris;

– bezprzewodowa brama RF-6750W firmy Harris.

OPROGRAMOWANIE RDC-9000WMS

Oprogramowanie Radio Data Communications 9000 Wireless Messaging System firmy OBR CTM SA jest implementacją uzgodnień STANAG-u 5066 w systemie informatycznym dla transmisji danych w kanale HF.

Jako transmisyjne oprogramowanie specjalistyczne spełnia wymagania tego dokumentu standaryzacyjnego (v.1.2) oraz stanowi integralną część węzła HF i może funkcjonować tylko w otoczeniu jego elementów.

W skład ukompletowania węzła HF powinny wchodzić następujące elementy:

– radiostacja HF z funkcją automatycznego nawiązywania połączenia (ALE) oraz spełniająca wymagania STANAG-u 4203 oraz STANAG-u 5066 Aneks E;

– modem radiowy o nowoczesnych technikach kodowania, spełniający wymagania: STANAG-u 4285, STANAG-u 4529, MIL-STD-188-110A, MIL-STD-188-110B oraz STANAG-u 5066 Aneks E (np. modem PSK-1001AM produkcji OBR CTM SA);

– urządzenie kryptograficzne typu BID-950 lub KG-84C;

– konwerter transmisji asynchronicznej na synchroniczną, spełniający wymagania STANAG-u 5066 Aneks D (konwerter KIS-4010 produkcji OBR CTM SA);

– komputer węzłowy z zainstalowanym oprogramowaniem, np. RDC-9000WMS;

– serwer pocztowy z zainstalowanym dowolnym oprogramowaniem, obsługujący protokoły SMTP i POP3[7] (do pracy w środowisku Windows można zastosować serwer pocztowy MailEnable oraz serwer Domain Name System – system nazw domen).

Oprogramowane RDC-9000WMS zapewnia prawidłową komunikację między użytkownikami lokalnego węzła HF i innych węzłów HF bądź też użytkownikami sieci LAN dołączonymi do węzłów HF. W zależności od konfiguracji oprogramowanie zainstalowane w komputerze węzłowym może pełnić funkcję autonomicznego terminalu odbierającego i wysyłającego dane oraz wiadomości tylko do podsieci HF (rys. 3) lub do bramy umożliwiającej przesyłanie danych i wiadomości między podsiecią HF i siecią LAN/WAN (rys. 4).

Oprogramowanie RDC-9000WMS może być zarządzane lokalnie z komputera węzłowego lub zdalnie z dowolnego komputera połączonego z nim przez sieć TCP/IP. Może współpracować z własnym serwerem pocztowym lub być dowiązane do innego standardowego serwera pocztowego.

W skład oprogramowania RDC-9000WMS wchodzą następujące moduły:

• graficzny interfejs użytkownika (Graphical User Interface – GUI), który umożliwia użytkownikowi komputera węzłowego (lokalnie lub zdalnie) zarządzanie pozostałymi modułami składającymi się na system RDC-9000WMS (konfiguruje ich parametry oraz steruje ich pracą);

• stos 5066 – moduł transmisyjny, który realizuje transmisje danych zgodnie z protokołem opisanym w STANAG-u 5066 v.1.2;

• kolejka wiadomości – moduł, którego zadaniem jest przetwarzanie wiadomości pocztowej odbieranej i wysyłanej przez węzeł HF. Kolejka filtruje, szereguje oraz decyduje, gdzie wiadomości pocztowe mają zostać przesłane w celu dalszej obróbki;

• tablica translacji adresów (Address Translation Table – ATT) – zmienia przyjazne dla użytkownika adresy internetowe na adresy w formacie podanym w STANAG-u 5066, uzgodnionym na podstawie bazy danych zawierającej wszystkie adresy węzłów HF znajdujących się w podsieci HF;

• oprogramowanie transmisyjne typu klient HMTP – moduł realizujący transmisje wiadomości pocztowych zgodnie z protokołem HMTP;

• oprogramowanie transmisyjne typu klient CFTP – moduł realizujący transmisje wiadomości pocztowych zgodnie z protokołem CFTP;

• oprogramowanie transmisyjne typu RDC-9000IP – zewnętrzny moduł (nie jest zarządzany z poziomu GUI), który spełnia wymagania podane w punkcie 10 Aneksu F (F.10) STANAG-u 5066. Klient IP umożliwia transmisję zgodnie z protokołem IP przez radiową sieć HF;

• oprogramowanie transmisyjne typu Aps – moduł zapewniający komunikację przez sieci TCP/IP między graficznym interfejsem użytkownika i pozostałymi modułami składowymi systemu RDC-9000WMS;

• oprogramowanie transmisyjne typu Control Proxy – moduł umożliwiający współpracę (przez port RS-232C lub TCP) między modemem radiowym i radiostacją a stosem 5066 i kolejką wiadomości;

• oprogramowanie konfiguracyjne typu RDC-9000DEV – zewnętrzna aplikacja pozwalająca na określenie typów urządzeń radiowych (modemu i radiostacji) wchodzących w skład węzła HF oraz skonfigurowanie połączenia między komputerem węzłowym i tymi urządzeniami (definicje portów zdalnego sterowania);

• oprogramowanie konfiguracyjne typu *guipass* – zewnętrzna aplikacja umożliwiająca zmianę hasła administratora RDC-9000WMS.

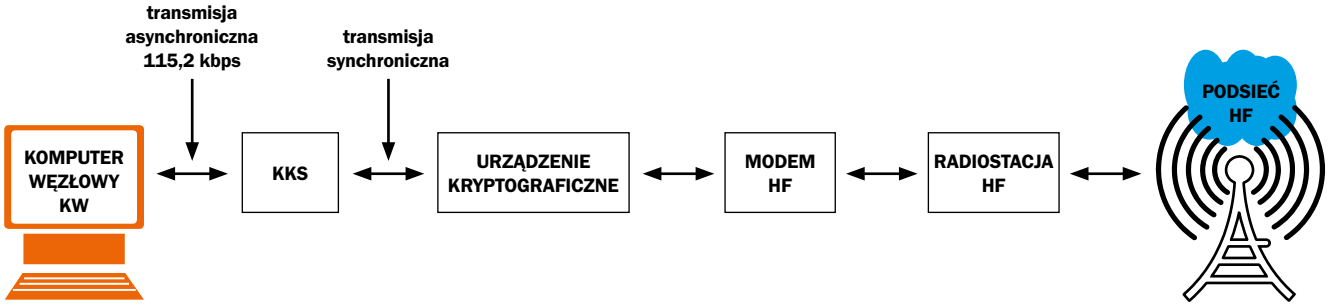
OPROGRAMOWANIE R&S STANAG 5066

Po zainstalowaniu w standardowym PC podłączonym do radiostacji spełniających wymagania określone w STANAG-u 5066 tworzy w pełni funkcjonalny system R&S STANAG 5066, który może zapewnić pracę pojedynczych terminali lub sieci LAN (rys. 5).

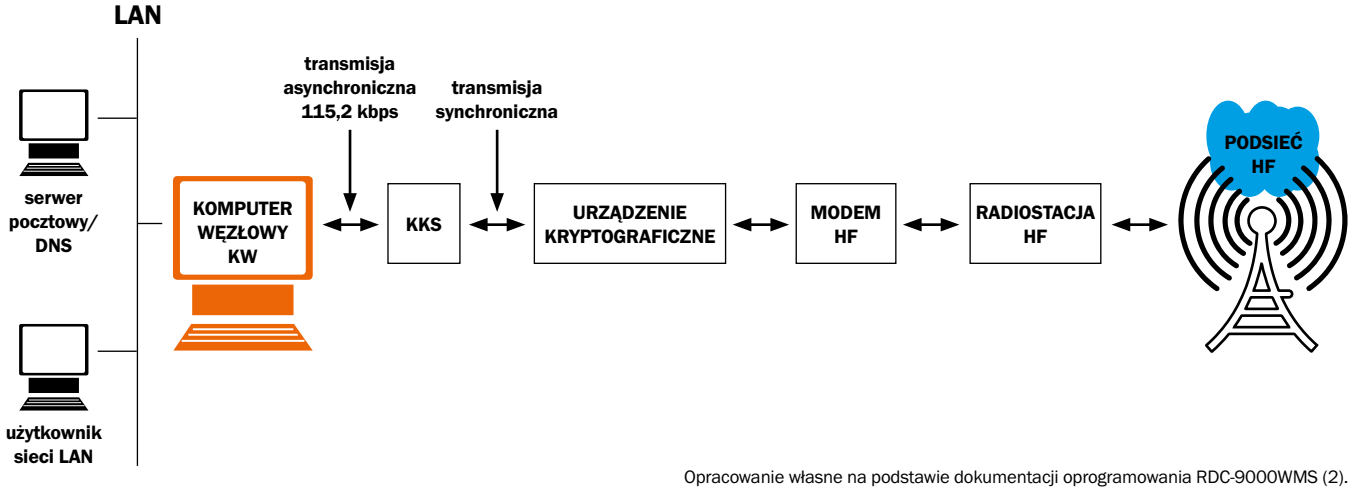
Oprogramowanie R&S STANAG 5066 jest rozwiązaniem komunikacyjnym przeznaczonym do solidnej i bezpiecznej wymiany danych z zastosowaniem sieci radiowych HF zgodnie ze standardem STANAG 5066. Obsługuje ono wymianę danych za pomocą poczty elektronicznej (e-mail), chatów i aplikacji wykorzystujących protokół IP. Oprogramowanie steruje radiostacją i modemami HF firmy Rohde & Schwarz oraz innych

[7] POP3 (Post Office Protocol v. 3) – protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej przesyłanej ze zdalnego serwera do lokalnego komputera przez połączenie TCP/IP. Ogromna większość współczesnych internautów korzysta z POP3 do odbioru poczty.

RYS. 3. KOMPUTER WĘZŁOWY W FUNKCJI TERMINALU

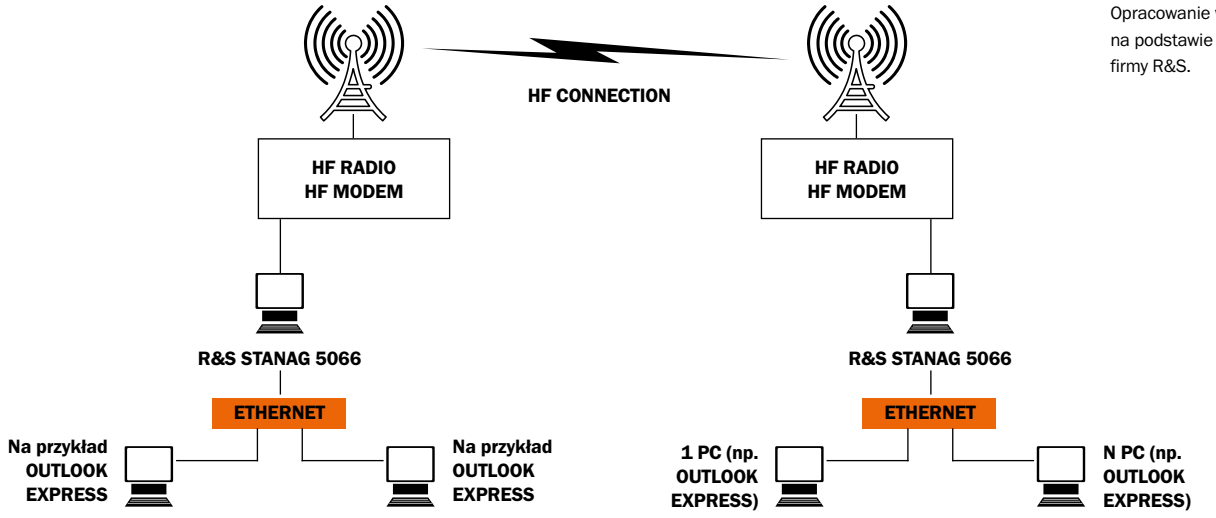


RYS. 4. KOMPUTER WĘZŁOWY W FUNKCJI BRAMY



Opracowanie własne na podstawie dokumentacji oprogramowania RDC-9000WMS (2).

RYS. 5. STRUKTURA SYSTEMU R&S STANAG 5066



Opracowanie własne na podstawie materiałów firmy R&S.

producentów sprzętu radiowego. Z powszechnie stosowanym starszym systemem obsługi wiadomości ACP 127[8] współdziała za pomocą bramy.

R&S STANAG 5066 jest w pełni zintegrowany z systemem sterowania i zarządzania łącznością radiową R&S SIMCOS II (SIgnals Management and COntrol System). Ponadto jest ważnym elementem wojskowego systemu obsługi wiadomości R&S MMHS (Military Message Handling System). W ramach systemu R&S SIMCOS II cały sprzęt łączności radiowej jest sterowany zdalnie za pomocą aplikacji DEVCON (Device Control)[9].

Aplikacja R&S STANAG 5066 składa się z wielu luźno powiązanych elementów. Poszczególne komponenty stanowią osobny proces. Konfiguracja i monitorowanie każdego z nich oraz sterowanie nimi jest udostępniane przez graficzny interfejs użytkownika (GUI). Wspomniana aplikacja ma stos protokołu STANAG 5066, w którym występuje pewna liczba zdefiniowanych punktów dostępu do usługi (Service Access Point – SAP). Do każdego punktu można podłączyć jednego klienta. SAP zapewnia specjalistyczne usługi przesyłania danych przez łącze radiowe HF. Działanie aplikacji zależy od ustawień podłączonego modemu lub radiostacji. Podstawowe parametry robocze, takie jak tryb pracy (ALE/ALE3G/stała częstotliwość) lub profil warstwy łącza danych, mogą wynikać z parametrów urządzeń fizycznych. Zmiany podstawowych parametrów konfiguracyjnych wymagają ponownego uruchomienia stosu. Także dowolne ich zmiany w czasie pracy aplikacji wymuszają ponowne automatyczne jego uruchomienie. Podczas takiej operacji wszyscy klienci przestają być powiązani. Automatyczne ich powiązanie następuje po zakończeniu powtórnego uruchomienia stosu. Przeobrażenia konfiguracji adresowej na ogół nie wymagają ponownego jego uruchomienia. Oprogramowanie R&S STANAG 5066, by pracowało poprawnie, wymaga sieci LAN/WAN, które mają dedykowane lub dzierżawione łącze z pracującym protokołem TCP/IP. Do podłączenia stacji roboczej do serwera potrzebne jest łącze o przepustowości 1 Mbps. Stos protokołu R&S STANAG 5066 wprowadza algorytmy i procedury typu Data Rate Change (DRC) w celu uzyskania optymalnego przepływu danych w kanałach HF w różnych, zmieniających się warunkach transmisji.

Procedura DRC opisuje, w jaki sposób połączone stacje przełączają się na nową szybkość przesyłania danych. Stos protokołu obsługuje dwie takie procedury. Procedura Standard DRC jest zdefiniowana w standardzie STANAG 5066. Może być używana zarówno dla profilów autobodowych[10] (np. STANAG 4539, MIL-STD 188-110B), jak i nieautobodowych (np. STANAG 4285). Natomiast procedura Quick DRC jest ulepszona i może być używana tylko dla profilów autobodowych. Algorytm DRC próbuje określić optymalną szybkość przesyłania danych dla bieżącego kanału HF. Użyte algorytmy opierają się na informacji ARQ i SNR. Wartość szybkości przesyłania danych z algorytmem DRC jest uaktywniana za pomocą procedury DRC, która jest zdefiniowana w dodatku C sekcji 6.4 standardu STANAG 5066. Jest ona wymagana dla profilów modemowych bez właściwości autobodowych (np. STANAG 4285). Może być używana także z profilami autobodowymi. Procedura ta jest dobrze zdefiniowana i odporna, jednak powolna, ponieważ potrzebuje transmisji pięciu zarządzających PDU. Co więcej, nie działa wówczas, gdy kanał HF staje się zbyt słaby do wymiany zarządzających PDU.

Procedura Quick DRC zaś jest preferowana dla profilów modemowych z właściwościami autobodowymi (np. STANAG 4539, MIL-STD 188-110B). Stacja wysyłająca po prostu zmienia prędkość wysyłania danych (TX – nadawanie) modemu wtedy, gdy algorytm DRC to zasugeruje. Największą zaletą jest krótki czas przełączania. Nie jest wymagana transmisja zarządzających PDU ze stałą szybkością. Procedura Quick DRC działa tylko dla trybu autobodowego. W celu poprawienia ARQ opartego na algorytmie DRC stos protokołu R&S STANAG 5066 może obsługiwać informacje jakościowe o transmisji z modemu odbierającego. Modem musi zapewnić dane o jakości transmisji w postaci współczynnika sygnał/szum (SNR). Algorytm DRC oparty na SNR oblicza średnią jego wartość dla kompletnego odbioru. Dla tego uśrednionego współczynnika z tabeli przekształceń jest wybierana optymalna szybkość przesyłania danych.

BEZPRZEWODOWY TERMINAL WIADOMOŚCI

Terminal ten o symbolu RF-6760W (RF-6760W Wireless Message Terminal) firmy Harris zapewnia transparentne dostarczanie e-maili, plików i zdjęć przez dowolne medium transmisyjne, takie jak: łącza radiowe HF/VHF/UHF, mikrofalowe i satelitarne, a także przewodowe linie oraz LAN (rys. 6). Podstawą budowy terminalu jest oprogramowanie RF-6760W wraz z akcesoriami (np. karta rozszerzeń dla PC w standardzie PCMCIA – Personal Computer Memory Card International Association lub dedykowane okablowanie w zależności od wykorzystywanego PC), które może pracować na standardowym PC,

[8] ACP 127 – standardowy format radiogramów obowiązujący w wojskowych systemach łączności radiowej w państwach członkowskich NATO, zdefiniowany w publikacji *Communications Instructions Tape Relay Procedures ACP127 (G).*

[9] Device Control – składnik oprogramowania w ramach SIMCOS II, służący do sterowania urządzeniami i konfigurowania ich, włącznie z urządzeniem R&S STANAG 5066.

[10] Profile autobodowe (na przykład MIL-188-110A, STANAG 4539) – automatycznie wykrywają szybkość bitową przychodzącego strumienia danych. W rezultacie nadawca nie musi czekać, aż odbiorca potwierdzi zmianę szybkości bitowej podczas procedury jej zmiany. W wyniku tego można przyspieszyć procedurę przesyłania danych.

laptopie lub sprzęcie dostarczonym przez firmę Harris. Oprogramowanie RF-6760W w zależności od edycji do prawidłowej pracy wymaga systemu operacyjnego z rodziny Windows firmy MS Microsoft. Zestaw oprogramowania terminalu integruje rozwijane przez firmę Harris niezawodne techniki transmisji danych z komercyjnym oprogramowaniem dla szybkiej i niezawodnej wymiany informacji. Terminal może być podłączony również do LAN wykorzystującego protokoły Ethernet oraz TCP/IP i pracować jako bezprzewodowa brama wiadomości.

Użytkownik terminalu RF-6760W do redagowania e-maili wykorzystuje standardowych klientów pocztowych zgodnych z protokołami SMTP/POP3, takich jak: Microsoft Outlook lub Outlook Express. Oprogramowanie terminalu automatycznie kieruje wiadomości przez odpowiednią radiostację lub linie przewodowe, wysyłając je do końcowego miejsca przeznaczenia przez adaptacyjną selekcję najlepszego dostępnego kanału transmisyjnego. Terminal również automatycznie przekazuje wiadomość z wykorzystaniem alternatywnej trasy, jeżeli pierwsza trasa jest zablokowana lub z innych przyczyn niedostępna.

W celu zabezpieczenia kanałów radiowych HF oprogramowanie terminalu pozwala używać jednego z dwóch zestawów protokołów zdefiniowanych w STANAG-u 5066 lub STANAG-u 4538. Pierwszy z nich jest standardem interoperacyjności NATO drugiej generacji. Korzystanie z niego zapewnia koalicyjną interoperacyjność oraz kompatybilność z globalnym systemem komunikacji HF (HF Global Communications System – HFGCS), którym zarządzają siły powietrzne Stanów Zjednoczonych (US Air Force). STANAG-4538 natomiast jest standardem interoperacyjności trzeciej generacji, który zapewnia doskonałe parametry oferowane przez funkcję ALE oraz możliwość wykorzystania protokołów łącza danych używanych przez radiostacje HF Harris serii Falcon II i III.

W sytuacji gdy łącze jest zrywane lub rozłączane w czasie transferu wiadomości, oprogramowanie RF-6760W będzie ponownie wysyłać wiadomości od miejsca wystąpienia błędu po przywróceniu możliwości transferu. Jego funkcjonalność jest szczególnie użyteczna w sytuacji wysyłania dużych wiadomości w czasie zmiany właściwości kanału transmisyjnego. Wysyłane i odbierane wiadomości e-mail, a także konfiguracja i parametry pracy radiostacji oraz modemów są archiwizowane. Oprogramowanie terminalu zapewnia automatyczne ponowne wysłanie wiadomości przez alternatywną ścieżkę dostępu i medium transmisyjne, konfigurowalny czas transmisji, przypadkowy okres ponownego wysłania wiadomości i łączenia wiadomości do tej samej lokalizacji. Klient IP STANAG-u 5066 bazujący na Windowsie zapewnia transmisję danych IP z użyciem radiostacji, która nie ma możliwości wymiany danych IP. Jest on w pełni zintegrowany z bezprzewodowym terminalem wiadomości (Wireless Message Terminal) dla zapewnienia prostej konfiguracji i jego efektywnego wykorzystania.

Używając nowego narzędzia ściągania wiadomości (pull messaging), użytkownicy zyskują zdolność podejrzenia nagłówka wiadomości e-mail przed jej przesłaniem. Funkcja ta oferuje kontrolę nad tym, jakie wiadomości są ściągane do lokalnego terminalu i zapobiega transmisji wiadomości nieistotnych lub o niższym w danym momencie priorytecie.

Oprogramowanie RF-6760W zawiera również aplikację do cyfrowego przetwarzania grafiki Imager, która dostarcza wszystkich niezbędnych narzędzi do przetwarzania, do czego należy zaliczyć powiększanie, grupowanie, obracanie, dostosowanie koloru (jasności), wyrównanie histogramu, opis obrazu i nałożenie symboli graficznych. Przetwarzana przez aplikację grafika może być kompresowana zgodnie z standardami: wavelet firmy Harris, JPG, BMP, MAC, TIF, PNG. Terminal współpracuje z następującymi urządzeniami kryptograficznymi: KG-84A, KG-84C, KY- 99, KY-57, KIV-7, KY-58, KY-68 oraz urządzeniami wbudowanymi w radiostacje.

Do zasadniczych jego właściwości należy zaliczyć:

- jednorodną transmisję i odbiór e-maili przez kanały HF/VHF/UHF, mikrofalowy i satelitarny lub linie przewodowe oraz LAN;
- wsparcie dla zestawu protokołów zdefiniowanych w STANAG-u 5066 i STANAG-u 4538;
- klienta IP, który umożliwia wymianę danych z pakietów IP z użyciem radiostacji niewspierających protokołu IP (np. radiostacje cyfrowe starszej generacji lub całkowicie analogowe);
- przystosowanie do współpracy z dużą liczbą różnorodnych wbudowanych oraz zewnętrznych urządzeń kryptograficznych dla zapewnienia wysokiego poziomu bezpieczeństwa;
- w pełni zautomatyzowaną konfigurację i oddzielenie od funkcji automatycznego zestawiania połączenia (ALE) łączy używających radiostacji rodziny Falcon II i III zgodnie z wymaganiami MIL-STD-188-141B i STANAG-u 4538;
- możliwość podejrzenia nagłówka wiadomości dzięki funkcji *pull messaging*.

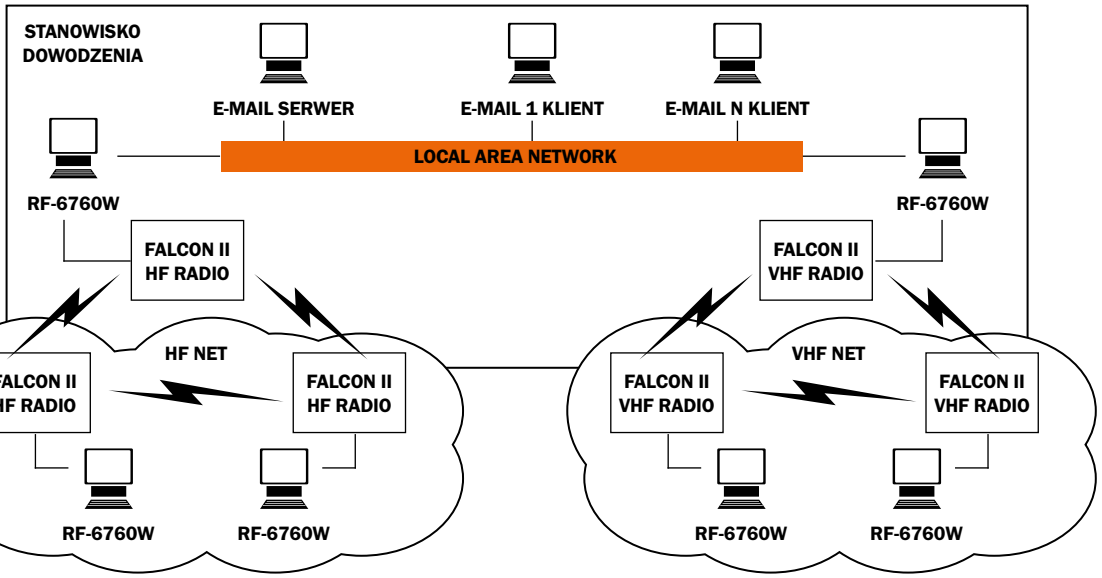
Terminal ma możliwość współpracy z takimi radiostacjami firmy Harris, jak: RF-5800H, PRC-150C, RF-5800V, RF-5800V-HH, AN/PRC-117F, RF-5800M/U, RF-5800M/U-HH, AN/PRC-138, RF-3200E, RF-5022E, RF-5022, RF-7210, z modemami radiowymi tej firmy RF-5710 i RF-5710A oraz z hubem dostępowym sieci taktycznej RF-6010 (Tactical Network Access Hub).

Standardy implementowane w terminalu RF-6760W to:

- Local Area Networking: TCP/IP;
- Automatic Link Establishment: MIL-STD-188-141A, STANAG 4538;
- modem radiowy HF: MIL-STD-188-110B, MIL-STD-188-110A, STANAG 4539, STANAG 4538;
- łącze danych HF: STANAG 5066, STANAG 4538;

KOSZT BUDOWY I EKSPLOATACJI RADIOWYCH WĘZŁÓW HF JEST BARDZO KORZYSTNY W STOSUNKU DO CENY ZAKUPU USŁUGI ŁĄCZNOŚCI I TERMINALI SATELITARNYCH.

RYS. 6. ZASTOSOWANIE BEZPRZEWODOWEGO TERMINALU WIADOMOŚCI RF-6760W



Opracowanie własne na podstawie materiałów firmy Harris.

• e-mail klient/serwer – obsługa protokołów: SMTP, POP3;
• protokół sieciowy: IPv4;
• technologie programowe: ActiveX[11], COM[12], MFC[13].

BEZPRZEWODOWA BRAMA

Zestaw oprogramowania bezprzewodowej bramy RF-6750W (Wireless Gateway) po zainstalowaniu w standardowym PC podłączonym do radiostacji serii Falcon II lub III tworzy w pełni funkcjonalną bezprzewodową bramę, która może zabezpieczyć pracę pojedynczych terminali lub sieci LAN. Zapewnia automatyczne wysyłanie wiadomości e-mail przez łącza radiowe oraz LAN z użyciem protokołów zdefiniowanych w STANAG-ach 5066 i 4538.

Zestaw oprogramowania bramy jest optymalizowany do pracy w sieci LAN wykorzystującej protokoły Ethernet – TCP/IP i działa jako „radio" – serwer poczty. Brama zapewnia transparentną usługę wymiany wiadomości e-mail i plików danych przez dowolne medium transmisyjne, takie jak: łącza radiowe HF/VHF/UHF, przewodowe sieci LAN, linie przewodowe, łącza mikrofalowe lub satelitarne, i jest kompatybilna z oprogramowaniem pocztowym pracującym na różnych platformach. Oprogramowanie bramy integruje rozwiązania niezawodnych technik transmisji danych opracowanych przez firmę Harris z oprogramowaniem komercyjnym na potrzeby szybkiej i niezawodnej wymiany informacji.

Po zainstalowaniu w PC spełniającym minimalne wymagania zestawu oprogramowania RF-6750W tworzy wraz ze sprzętem radiowym multimedialną bramę komunikacji do transparentnego przekazywania e-maili oraz plików przez media, które są skłonne wprowadzać błędy do transmitowanych danych. Brama przekazuje również automatycznie wiadomości, jeżeli pierwsza marszruta (kanał transmisyjny) jest zablokowana.

W razie używania kanału radiowego HF oprogramowanie bramy bezprzewodowej pozwala zastosować jeden z trzech protokołów (protokół warstwy fizycznej).

STANAG 5066, o czym już wspomniano, jest standardem interoperacyjności NATO drugiej generacji.

[11] ActiveX – rodzaj komponentów i kontrolek możliwych do użycia w programach pisanych za pomocą takich narzędzi, jak Delphi, Visual Basic C++, Java, Power Builder i wielu innych. Technologia ActiveX pozwala na przekazywanie danych między różnymi aplikacjami działającymi pod kontrolą systemów operacyjnych Windows. Technologia ta jest ułatwieniem dla programisty – pozwala zaoszczędzić czas, który trzeba by poświęcić na pisanie własnych sposobów komunikacji między programami.

[12] COM (Component Object Model) – standard definiowania i tworzenia interfejsów programistycznych na poziomie binarnym dla komponentów oprogramowania, wprowadzony przez firmę Microsoft wraz z bibliotekami zapewniającymi podstawowe ramy i usługi dla współdziałania komponentów COM i aplikacji.

[13] MFC (Microsoft Foundation Class Library) – biblioteka Visual C++, której klasy stanowią szkielet aplikacji dla programów pracujących w systemie Windows. Jest to biblioteka programistyczna napisana w języku C++, która stanowi obiektową (i uproszczoną) wersję Microsoft Windows API.

Zapewnia zatem koalicyjną interoperacyjność oraz pozwala na kompatybilność z globalnym systemem komunikacji HF.

Natomiast STANAG 4538 jest trzeciej generacji standardem współdziałania oraz FED-STD-1052 (Federal Standard). Jest stosowany w celu zapewnienia współpracy z wcześniejszymi produktami służącymi do łączności bezprzewodowej, oferowanymi przez firmę Harris.

Wiadomości są redagowane i odbierane przez terminale, które są podłączone do sieci LAN lub WAN albo są ulokowane w zdalnej lokalizacji bez możliwości łatwej komunikacji z wykorzystaniem łączy przewodowych.

Nadawca wysyła standardowy e-mail lub dane, a oprogramowanie RF-6750W automatycznie wybiera trasę dla wiadomości przez właściwą radiostację lub łącze przewodowe i wysyła wiadomość do końcowego miejsca przeznaczenia, adaptacyjnie wybierając najlepszy dostępny kanał transmisyjny. Wysyłane i odbierane wiadomości e-mail oraz konfiguracja i parametry pracy radiostacji modemów są archiwizowane. Brama zapewnia automatycznie ponowne wysłanie wiadomości przez alternatywną ścieżkę dostępu i medium transmisyjne, konfigurowalny czas transmisji oraz przypadkowy okres ponownego wysłania wiadomości i łączenia jej do tej samej lokalizacji.

Bezprzewodowa brama implementuje, opartego na systemie operacyjnym Windows, klienta IP zgodnego ze STANAG-iem 5066, który był pierwszym tego typu rozwiązaniem na rynku. Klient IP jest zintegrowany z oprogramowaniem RF-6750W (które nie wspiera protokołu IP) i zapewnia zdolność do transmisji danych IP przez kanał radiowy.

Brama zawiera również narzędzie – Imager firmy Harris, które oferuje duże możliwości przemysłowego standardu, czyli uniwersalne oprogramowanie przesyłania grafiki Harrisa (Harris Universal Imaging Transmission Software – HUITS). Narzędzie to przetwarza grafikę bezpośrednio z aplikacji i pozwala na transmisję cyfrowego obrazu wysokiej rozdzielczości, używając bezprzewodowego systemu e-mail. Imager realizuje również konwersję między plikami w kilku formatach oraz zawiera kompresję *wavelet* (falki), która zapewnia ich zmniejszenie do formatu grafiki typu JPG. Przetwarzana przez aplikację grafika może być kompresowana zgodnie z standardami: wavelet firmy Harris, JPG, BMP, MAC, TIF i PNG.

Do zasadniczych właściwości bezprzewodowej bramy RF-6750W należy zaliczyć:

• jednorodną transmisję i odbiór e-maili przez kanały HF/VHF/UHF, mikrofalowy i satelitarny lub linie przewodowe oraz LAN;

• wsparcie dla zestawu protokołów zdefiniowanych w STANAG-ach 5066 i 4538;

• klienta IP, który umożliwia wymianę danych z pakietów IP z użyciem radiostacji niewspierającej protokołu IP (np. radiostacje cyfrowe starszej generacji lub całkowicie analogowe);

• przystosowanie do współpracy z dużą liczbą różnorodnych wbudowanych i zewnętrznych urządzeń kryptograficznych dla zapewnienia wysokiego poziomu bezpieczeństwa;

• w pełni zautomatyzowaną konfigurację oraz oddzielenie od funkcji automatycznego zestawiania połączenia (ALE) łączy używających radiostacji rodziny Falcon II i III zgodnie z wymaganiami MIL-STD-188-141B i STANAG-u 4538.

Brama współpracuje z następującymi urządzeniami kryptograficznymi: KG-84A, KG-84C, KY- 99, KY-57, KIV-7, KY-58 i KY-68 oraz urządzeniami wbudowanymi w radiostacje.

Ma możliwość współpracy z takimi radiostacjami firmy Harris, jak: RF-5800H, PRC-150C, RF-5800V, RF-5800V-HH, AN/PRC-117F, RF-5800M/U, RF-5800M/U-HH, AN/PRC-138, RF-3200E, RF-5022E, RF-5022 i RF-7210 oraz modemami radiowymi: RF-5710, RF-5710A, a także z hubem dostępowym sieci taktycznej RF-6010 (Tactical Network Access Hub).

Implementowane standardy w bramie bezprzewodowej terminalu RF-6750W to:

• Local Area Networking: TCP/IP;

• Automatic Link Establishment: MIL-STD-188--141A, STANAG 4538;

• modem radiowy HF: MIL-STD-188-110B, MIL-STD-188-110A, STANAG 4539, STANAG 4538;

• łącze danych HF: STANAG 5066, STANAG 4538;

• e-mail klient/serwer – obsługa protokołów: SMTP, POP3;

• protokół sieciwy: IPv4;

• technologie programowe: ActiveX, COM, MFC.

PODSUMOWANIE

Przedstawione implementacje wymagań zdefiniowanych w STANAG-u 5066 pozwalają na budowę i eksploatację nowoczesnych radiowych węzłów HF, które mogą pełnić funkcję: bezprzewodowej bramy radiowej HF udostępniającej usługi wymiany poczty elektronicznej (e-mail) wraz z załącznikami; wymiany plików danych (ftp), wiadomości tekstowych (np. HFCHAT, ACP-127) i grafiki cyfrowej (np. zdjęcia, grafika operacyjna). Są one niezbędne do zapewnienia działalności oddalonych na znaczną odległość mobilnych lub stacjonarnych stanowisk dowodzenia (SD) oraz mobilnych platform (np.: okręty, samoloty, wozy dowodzenia), na których są eksploatowane stanowiska komputerowe oraz terminale systemów klasy C2. Dodatkową zaletą implementacji STANAG-u 5066 jest możliwość automatycznej i niezawodnej integracji sieci LAN SD w sytuacji braku dostępu do systemu łączności satelitarnej lub gdy koszt tego rodzaju łączności jest zbyt wysoki. Również koszt budowy i eksploatacji radiowych węzłów HF jest bardzo korzystny w stosunku do ceny zakupu usługi łączności oraz terminali satelitarnych. ■

Budowanie efektywnych **zespołów ludzkich**

WYKREOWANIE ODPOWIEDNIO ZAANGAŻOWANEGO ZESPOŁU NIE JEST CZYNNOŚCIĄ ŁATWĄ. KAŻDY DOWÓDCA MUSI SOBIE UŚWIADOMIĆ, W JAKIM MOMENCIE ŻYCIA JEST JEGO GRUPA ORAZ JAKIE KROKI MUSI PODJĄĆ, BY STWORZYĆ ZESPÓŁ.

płk mgr inż. Piotr Rupa, ppor. Dariusz Wasilewski

Piotr Rupa jest szefem Wojewódzkiego Sztabu Wojskowego we Wrocławiu.

Dariusz Wasilewski jest dowódcą plutonu w 12 Brygadzie Zmechanizowanej.

Dla żołnierzy Wojska Polskiego wiek XXI przyniósł wiele zmian, na przykład przejście na służbę zawodową czy udział w operacjach poza granicami kraju. Nowa rzeczywistość generuje przed siłami zbrojnymi nowe wyzwania. Warto także zwrócić uwagę na zmiany pokoleniowe wśród społeczeństwa. Na rynku pracy najczęściej możemy się spotkać teraz z pokoleniem „Y". Są to ludzie urodzeni w latach 1982–2001, dorastający na przełomie wieków i od najmłodszych lat korzystający z nowinek technicznych, takich jak komputery, GSM czy Internet[1]. Osoby te są szczególnie nastawione na pracę w grupie. To właśnie dobra atmosfera w pracy jest czynnikiem, dzięki któremu pozostają oni związani dłużej z jednym pracodawcą. Dlatego też w związku z coraz większą konkurencyjnością na rynku pracy oraz zmianą pokoleniową przedsiębiorcy muszą zacząć dbać o pracowników oraz stosunki interpersonalne[2]. Stawia to przed dowódcami trudne zadanie. Jak właściwie zarządzać? Co zrobić, aby zbudować zaangażowanie oraz przywiązanie do jednostki? Zapewne niejeden decydent stawia sobie te pytania.

Analizując współczesne uwarunkowania zarówno w armii, jak i w biznesie, należy zwrócić uwagę, iż coraz częściej to właśnie małe zespoły ludzkie wykonują zadania najbardziej istotne, np. wojska specjalne w siłach zbrojnych czy zespoły funkcjonalne w biznesie. Teraz należy sobie zadać pytanie, czy jednak każda grupa ludzi może się nazywać zespołem. Otóż niestety nie.

ASPEKTY TEORETYCZNE

Definiując grupę, trzeba się zwrócić do nauk związanych z socjologią lub też psychologią. Według specjalistów w tych dziedzinach, *grupa to zbiorowość zaczynająca się od dwóch osób, członkowie grup współdziałają ze sobą na zasadzie odrębności od innych w celu zaspokajania własnych potrzeb, charakteryzują się trwałą strukturą i względnie jednolitym systemem norm i wartości*[3]. Analizując pojęcie grupy pod względem kategorii, jaką jest cel, zauważamy znaczącą różnicę między grupą a zespołem, ponieważ to właśnie zespoły mają wspólny cel i skupiają się na zaspokajaniu potrzeb całej organizacji. Jednak jest to tylko jedna z korzyści efektywnych zespołów. Pozostałe ich cechy przedstawiono na rysunku 1.

Zapewne po przeczytaniu przedstawionych informacji oraz przeanalizowaniu rysunku zastanawiamy się,

[1] D. Berreby: *The Hunter-Gatherers of the Knowledge Economy: The Anthropology of Today's Cyberforagers.* Booz & Company, New York 1999, s. 52–64.

[2] Raport HR 2018, *Zarządzanie multigeneracyjne*, s. 5.

[3] http://www.mojasocjologia.pl/grupa-spoleczna/.

W PROFESJONALNYM ZESPOLE WIĘKSZOŚĆ CZŁONKÓW ZNA I AKCEPTUJE ZARÓWNO USTANOWIONE NORMY, JAK I ROLE, KTÓRE ZOSTAŁY IM PRZYDZIELONE.

CZY LEPIEJ BYĆ LUBIANYM, CZY WZBUDZAĆ STRACH?

GRUPA
to zbiorowość zaczynająca się od dwóch osób, członkowie grup współdziałają ze sobą na zasadzie odrębności od innych w celu zaspokajania własnych potrzeb, charakteryzują się trwałą strukturą i względnie jednolitym systemem norm i wartości.

W celu zbudowania stabilnej oraz pewnej pozycji dowódca musi w sposób właściwy oddziaływać na swoich podwładnych.

SKEEZE / PIXABAY

w jaki sposób buduje się zespół. Przyjmuje się, że dla większości z nich istnieje pięć etapów wspólnych. Pięcioetapowy model jest najbardziej popularny i najczęściej występuje w literaturze naukowej. Jako jego autorów wskazuje się B.W. Tuckmana i M.A.C. Jensena.

Wyróżnia się następujące etapy powstawania zespołów[4]:

Etap 1. Formowanie (forming) – następuje, gdy członkowie zespołu spotykają się po raz pierwszy. To, co najbardziej określa zespół w tej chwili, to: ostrożność, niepewność, szukanie kierunku oraz widoczne unikanie konfliktu. Interakcje między członkami zespołu są przypadkowe. Członkowie w tej fazie polegają w głównej mierze na przywódcy i to do niego trafia większość komunikatów, które dotyczą przede wszystkim spraw ogólnych. Zapoznają się z zadaniami, zbierają odpowiednie informacje i środki. Członkowie zespołu dążą do poznania siebie nawzajem oraz ustalenia początkowych zasad współdziałania. Efektywność chwilowo zostaje zepchnięta na drugi plan, ponieważ priorytetem jest zaangażowanie członków, osiągnięcie spójności oraz poskromienie strachu przed nieznanym. Bardzo ważne w tym etapie jest przejście z myślenia typu „ja" na „my". Kiedy członkowie zespołu odczuwają, że ich los jest wspólny, etap się kończy.

Etap 2. Docieranie się (storming) – charakteryzuje wszechobecny konflikt, który przejawia się we wszystkich aspektach funkcjonowania zespołu. Członkowie zaczynają opierać się emocjonalnie przed wykonywaniem zadań, jednocześnie wątpią w sukces zespołu. Okazują zniecierpliwienie, nie ukrywają swoich osobistych celów i tego, co pragną osiągnąć przez uczestnictwo w zespole. Uczestnicy krytykują siebie nawzajem, a czasem wyrażają wzajemną wrogość. Dochodzi do walk o władzę oraz kwestionuje się wcześniejsze decyzje. Wyraża się sprzeciw wobec kontroli. Etap ten to czas burzliwych rozmów i sporów. W jego trakcie należy się skupić na pozytywnych wynikach i zaakceptować nieprzychylne opinie na temat postępów. Konstruktywne zarządzanie konfliktem może się okazać sprawą kluczową. Narastająca wrogość, której nie uda się zniwelować, może bowiem doprowadzić do rozpadu zespołu.

Etap 3. Normalizacja (norming) – członkowie zespołu przechodzą od konfliktów do rzeczowych rozmów. Otwierają się na wymianę poglądów i okazują sobie wzajemne wsparcie. Dzielą się swoimi poglądami, są gotowi do rozważania alternatyw. Zacieśniają się relacje i uwidacznia się tzw. duch zespołu. Na tym etapie większość członków zna i akceptuje zarówno ustanowione normy, jak i role w zespole, które zostały im przydzielone. Zadania zostają wydelegowane, a struktura komunikacji określona. Rola lidera opiera się w głównej mierze na obserwowaniu. Zakończeniem etapu jest moment, gdy członkowie mają wspólne oczekiwania wobec celowości zespołu.

Etap 4. Wykonanie (performing) – czas najefektywniejszej pracy zespołu. Wdraża się nowe, kreatywne rozwiązania. Klimat panujący w nim sprzyja osiąganiu celów. Pojawia się energia nieodzowna efektywnemu działaniu. Członkowie dążą do konstruktywnego rozwiązywania problemów, niejednokrotnie przekładają cele zespołu ponad własne. Dominują ciepłe relacje, akceptacja i dobrowolna współpraca. Przywództwo jest w pełni zaaprobowane. Jeśli zespół nie przeszedł z powodzeniem poprzednich etapów, może mieć problem z dotarciem do tego miejsca.

Etap 5. Zamknięcie (adjourning) – ostatni z etapów rozwoju zespołu. Dotyczy jedynie niektórych zespołów, np. projektowych. Współpraca zostaje zakończona ze względu na osiągnięcie celów lub wtedy, gdy wszyscy członkowie opuścili zespół. Relacje rozluźniają się, a członkowie podejmują inne wyzwania. Towarzyszy im gorycz porażki bądź radość ze wspólnych osiągnięć. Jeśli zespół odniósł sukces, może być to najtrudniejszy z dotychczasowych etapów. Jest to dobry czas na podsumowanie pracy i wyciągnięcie wniosków na przyszłość. Zamknięcie grupy może odbyć się nagle lub być rozciągnięte w czasie.

Jak widzimy proces formowania zespołu jest zjawiskiem bardzo złożonym, wymagającym wiedzy dotyczącej zarządzania zasobami ludzkimi, jednak dowódca może w czasie każdego z etapów odpowiednio wpłynąć na grupę (rys. 2).

Praca w dobrze zorganizowanym i zaangażowanym zespole niesie ze sobą także bardzo dużo pozytywnych efektów, aczkolwiek również pewne zagrożenia (rys. 3).

Reasumując, stworzenie efektywnego zespołu nie jest procesem, który można zrealizować w ciągu kilku dni, potrzeba tutaj czasu oraz zaangażowania zarówno żołnierzy, jak i dowódcy. Dodatkowo efektywne zespoły cechują się większą wydajnością oraz kreatywnością. Dlatego też warto dołożyć wszelkich starań, by grupy ludzi stawały się zespołami. Niezmiernie ważna jednak jest tutaj rola przełożonego, gdyż to właśnie on musi odpowiednio reagować na procesy w grupie, co więcej, swoim postępowaniem musi osiągnąć czynne zaangażowanie oraz wypracować sobie autorytet.

BUDOWANIE AUTORYTETU

Analizując literaturę związaną z budowaniem autorytetu, można dojść do wniosku, że w celu zbudowania stabilnej oraz pewnej pozycji dowódca musi w sposób właściwy oddziaływać na swoich podwładnych. Aby robić to właściwie, niezbędne jest utrzymanie równowagi między demonstrowaniem kompetencji zawodowych a podejściem zorientowanym na człowieka. Czy lepiej być lubianym, czy wzbudzać strach? Podwładni od samego początku oceniają swoich przełożonych. Zaskakujące jest, że badania dowodzą, iż w pierwszej kolejności podczas oceny przyglą-

[4] B. Tuckman: *Developmental sequence in small groups*. „Psychological Bulletin" 1965, 63 (6), s. 384–399.

RYS. 1. CECHY EFEKTYWNEGO ZESPOŁU

Opracowanie własne na podstawie: S.P. Robbins, D.A. DeCenzo: *Podstawy zarządzania.* Warszawa 2002.

RYS. 2. CYKL ŻYCIA ZESPOŁU

KOLEJNE ETAPY	JAK MOŻE JE WYKORZYSTAĆ PRZYWÓDCA GRUPY
ETAP I formowanie grupy	nadanie ról członkom zespołu (czyli przydzielenie obowiązków i przywilejów) zgodnie z wizją kierownika skorygowaną o oczekiwania pozostałych pracowników
ETAP II ścieranie się różnych opinii, postaw	wykorzystanie wstępnej informacji i zdobytej wiedzy o osobowościach, dominujących cechach charakteru członków grupy do zorganizowania współpracy poszczególnych osób, w sposób przynoszący najwyższą efektywność i sprawność działania
ETAP III normowanie zachowań	uczestniczenie w tworzeniu norm grupowych, kreowanie spójności grupy, częściowo przez działania formalne, częściowo przez nieformalny wpływ własną postawą, zachowaniem dawaniem odpowiedniego przykładu
ETAP IV efektywne działanie	wspieranie, służenie własną wiedzą i doświadczeniem

Opracowanie własne na podstawie: M. Romanowska: *Podstawy organizacji i zarządzania.* Warszawa 2001.

KORZYŚCI ORAZ ZAGROŻENIA PRACY GRUPOWEJ

KORZYŚCI

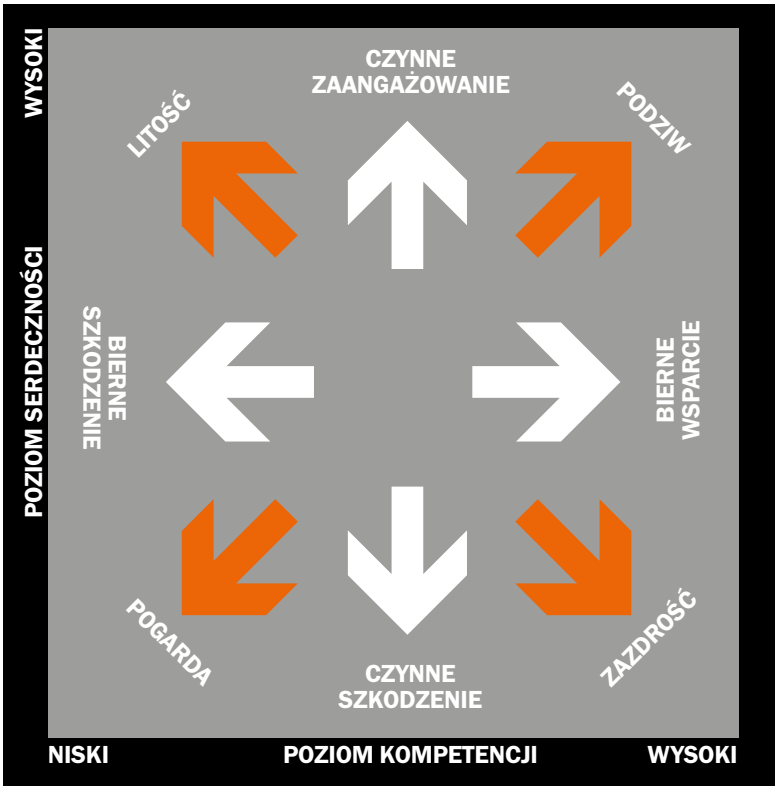
- **większa wiedza, doświadczenie i umiejętności**
- **większa ilość informacji**
- **uwolnienie się od negatywnych efektów indywidualnej percepcji i atrybucji**
- **większa motywacja (facylitacja społeczna)**
- **wyższy stopień akceptacji (zrozumienia) ostatecznej decyzji i łatwiejsze jej wdrożenie**
- **mniejszy stres, co uwalnia kreatywność**
- **człowiek to istota społeczna, więc działanie w grupie daje jednostkom przynależność, identyfikację, wsparcie emocjonalne, pomoc, opiekę**

ZAGROŻENIA

- **dłuższy czas podejmowania decyzji i większe koszty**
- **rozmycie odpowiedzialności za decyzje**
- **potencjalne konflikty mające charakter destrukcyjny**
- **większa skłonność do ryzyka**
- **dominacja jednostki**
- **niezdecydowanie grupy może prowadzić do decyzji kompromisowych**
- **dążenie do zachowania własnej odrębności**
- **zjawisko tłumienia mniejszości**
- **może się pojawić „syndrom grupowego myślenia”**

Opracowanie własne na podstawie: J.M. Lichtarski: *Budowanie skutecznego zespołu pracowniczego.* Uniwersytet Ekonomiczny, Wrocław 2009.

RYS. 4. AUTORYTET A ZAANGAŻOWANIE DOWÓDCY



Opracowanie własne na podstawie: *Budowanie autorytetu*. Raport „Harvard Business Review Polska" nr 185–186, Warszawa 2018.

dają się oni dwóm cechom: czy są mili (czy okazują życzliwość), czy może jednak wzbudzają strach. Badania prowadzone przez Amy Cuddy pokazują, że ludzie oceniani jako kompetentni, jednakże mało życzliwi, często wzbudzają zazdrość i niechęć współpracowników. Z drugiej strony osoby bardzo życzliwe, ale o niskim stopniu kompetencji wzbudzają litość prowadzącą do braku szacunku. Co zatem jest bardziej opłacalne? Bycie sympatycznym przywódcą czy może silnym, stanowczym dowódcą? Otóż odpowiedzi na to pytanie można odszukać w badaniach Jacka Zengera, którymi objęto aż 51 tysięcy przywódców. Wykazało ono, iż jedynie 27 osób z przebadanych wykazywało małą życzliwość w stosunku do swoich podwładnych, osiągając przy tym wysokie wyniki ogólnej skuteczności przywódczej. Nauki behawioralne coraz częściej podczas swych badań wykazują, że aby skutecznie przewodzić, trzeba pokazać swoją ludzką stronę. Nawet mały gest, skinienie głową czy też uśmiech pozytywnie wpłyną na budowanie autorytetu przywódcy.

Teraz przeanalizujmy drugą stronę medalu. Co właściwie się dzieje, gdy najpierw pokazujemy naszą siłę oraz kompetencje? – rys. 4.

Analizując treści przedstawione na nim, należy zwrócić szczególną uwagę na sytuację, kiedy przywódcę wyróżnia średni stopień kompetencji oraz bardzo niski poziom serdeczności. Występuje tutaj czynne szkodzenie! Sytuacja ta jest szczególnie niebezpieczna w wojsku, gdyż nie ma tutaj miejsca na czynne szkodzenie, zarówno jeśli chodzi o sprzęt, jak i o stosunki interpersonalne. Zwróćmy jednak uwagę na sytuację, kiedy lider cieszy się wysoką serdecznością oraz ma średnie kompetencje. Występuje tutaj to, czego naprawdę oczekuje każdy przywódca – czynne zaangażowanie. Dogłębnie analizując wykres, można rozważać także czynniki związane z wypaleniem zawodowym, indywidualizmem oraz profesjonalizmem. Zgodnie z badaniami prowadzonymi w norweskich siłach zbrojnych, osoby wykazujące niski stopień zaangażowania oraz mające cechy przypisane dla indywidualistów bardzo często ulegają wypaleniu zawodowemu. Mówiąc o zaangażowaniu, należy je jednak najpierw zdefiniować. Wiliam Schaufeli i współautorzy zauważają, iż zaangażowanie w pracę to pozytywny stan umysłu pracownika, który jest charakteryzowany przez doświadczanie w pracy wigoru, poziom zaabsorbowania się nią i oddania się jej. Wigor dotyczy doświadczania podczas pracy uczucia przypływu energii oraz odporności na zmęczenie fizyczne i psychiczne. Oddanie się pracy odnosi się do przekonania, że ma ona znaczenie, a jej wykonywanie jest ważne i może napawać dumą. Zaabsorbowanie pracą świadczy o doświadczaniu w jej trakcie pełnej koncentracji na wykonywanych zadaniach, czemu towarzyszyć może poczucie szybkiego upływu czasu[5]. Czy jednak można porównywać zaangażowanie w pracę z zaangażowaniem w służbę ? Otóż tak! Jednostka wojskowa jest specyficzną formą organizacji, która nie jest nastawiona na zysk, a na ukształtowanie człowieka oraz wyszkolenie go w ten sposób, by w czasie zagrożenia był gotów walczyć o wolność własnego kraju. Postarajmy się jednak zdefiniować, czym właściwie jest zaangażowanie w służbę. Przez pojęcie to rozumie się wykonywanie zadań związanych ze służbą wojskową w sposób ukazujący duży entuzjazm oraz własną inicjatywę, dodatkowo żołnierz utożsamia się z celami oraz zadaniami jednostki wojskowej (organizacji). Jest w stanie przekładać dobro służby ponad swoje własne.

Czym właściwie przejawia się zaangażowanie? W literaturze można odszukać wiele cech, jednakże

[5] W. Schaufeli, M. Salanova, V. Gonzalez-Roma, A. Bakker: *The Measurement of Engagement and Burnout: A Two Sample Confirmatory Factor Analytic Approach*. „Journal of Happiness Stadies" 2002 nr 3, s. 71–92.

na potrzeby artykułu przyjęto te najbliższe sercu każdego dowódcy, czyli[6]:

– gotowość do obrony firmy i jej produktów w sytuacji kryzysowej i konfliktowej;

– dumę z pracy w danej organizacji, identyfikację wyrażaną stwierdzeniem „moja firma", „u nas" itp.;

– wykazywanie dużej aktywności i inicjatywy;

– długookresowe zatrudnienie i brak zainteresowania zmianą miejsca pracy;

– dyspozycyjność oraz zgoda na pracę w godzinach ponadwymiarowych, gdy wymaga tego sytuacja;

– zrozumienie dla dodatkowych obowiązków, chęć przyjmowania odpowiedzialności;

– lojalność;

– zaufanie względem przełożonych i współpracowników.

Jednak aby zaangażowanie było autentyczne, nie może się składać tylko z wykazywanych zachowań. Jak podkreśla M. Bugdol, musi ono wynikać z przekonania, że warto coś robić, z wiedzy o mechanizmach integracyjnych oraz z troski o przyszłość organizacji. W jaki sposób budować zaangażowanie? Jakie cechy przywódcy je tworzą? Według badań 4Results, najważniejsze cechy lidera są związane ze swobodą działania oraz szeroko pojętymi stosunkami interpersonalnymi. Co więcej, ważnym elementem jest pomoc zarówno w czasie realizacji zadania, jak i w codziennych sprawach służbowych. Reasumując, budując autorytet przywódca musi zachować równowagę między kompetencjami a życzliwością. Zbyt niski stopień kompetencji na stanowisku, nawet połączony z dużą życzliwością, nie przynosi oczekiwanych skutków. Wynikową odpowiedniego zbalansowania kompetencji oraz zarządzania zasobami ludzkimi, nastawionymi na człowieka, jest czynne zaangażowanie żołnierzy. Analizując doktryny armii sojuszniczych, można odszukać informacje mówiące, że żaden sprzęt nie jest w stanie zastąpić żołnierza zaangażowanego oraz chętnego do działania. To właśnie czynne zaangażowanie jest tym, co chciałby osiągnąć każdy prawdziwy przywódca. Jak właściwie przedstawia się kwestia zaangażowania oraz czynników wzbudzających zaangażowanie wśród pracowników organizacji? Zaprezentowano to w przeprowadzonym ustrukturyzowanym wywiadzie.

BADANIA

Po analizie literatury dotyczącej zaangażowania oraz budowania autorytetu należy ją skonfrontować z rzeczywistością. W związku z tym przeprowadzono wywiad ustrukturyzowany, mający na celu zidentyfikowanie czynników oraz postaw osób zarządzających, wzbudzających zaangażowanie. Podmiotem badań były osoby zatrudnione w różnego rodzaju przedsiębiorstwach N=77 (z racji tego, iż definicja jednostki wojskowej zawiera przesłanki do utożsamiania jej z organizacją cywilną, na potrzeby badań przyjęto: jednostka wojskowa = organizacja). W celu weryfikacji rzetelności opracowanego kwestionariusza przeprowadzono badania metodą sędziów kompetentnych. Wykorzystano technikę prowadzenia badań w postaci wywiadu ustrukturyzowanego. Respondenci zostali poproszeni, by z zaproponowanej im listy czynników wskazali te, które najbardziej wpływają na ich zaangażowanie. Mogli także wpisywać własne odpowiedzi. Ich zadaniem było również dokonanie oceny wpływu każdego czynnika w pięciostopniowej skali Likerta, gdzie 1 oznacza „bez wpływu", a 5 – „bardzo duży wpływ".

KWESTIONARIUSZ OCENY ZAANGAŻOWANIA

1. Z wymienionych czynników przy każdym dopisz w skali od 1–5, w jakim stopniu angażuje Cię on do działania.

a) Realizacja nowego zagadnienia.

b) Duże zaangażowanie zespołu w realizację zadania.

c) Osobiste zaangażowanie Twojego bezpośredniego przełożonego w realizację zagadnienia.

d) Jasno postawiony cel działania.

e) Wprowadzenie w sytuację. Omówienie, po co właściwie wykonuje się dane zadanie.

f) Dobra atmosfera w zespole. Dobry kontakt z przełożonym.

g) Stosowanie przez przełożonego omówienia i wsparcia w realizacji zagadnienia.

h) Odpowiednie wynagrodzenie starań przez przełożonego.

g) Stosowanie ciągłej kontroli.

h) Instrukcje, które ograniczają swobodę wykonania zadania.

i) Atmosfera typowo „wojskowa", ścisłe trzymanie się regulaminu.

2. Oceń swój stopień zaangażowania w wykonywanie zadań w poniższej sytuacji (skala 1–5).

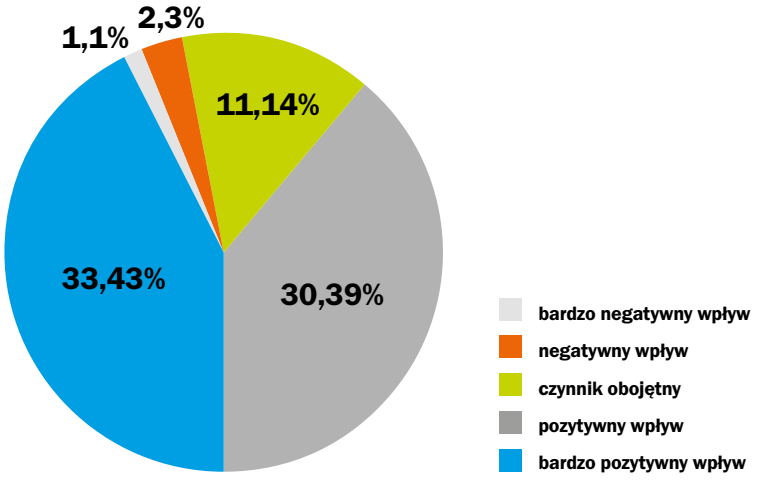
a) Firma ma strukturę zhierarchizowaną, mimo to relacje między pracownikiem a kierownikiem są oparte na wzajemnym szacunku oraz zrozumieniu.

b) Przełożony wymaga bardzo dużo od siebie, ale także od pracowników, ciągle wprowadzając innowacje oraz nowe zagadnienia. Daje sprecyzowane zadania, jednak, oczekując na wynik końcowy, pozostawia dużą swobodę w ich wykonywaniu.

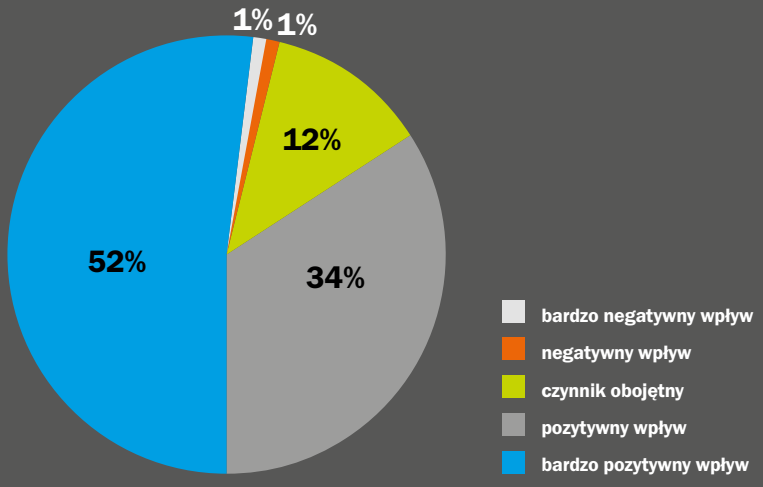
c) W czasie realizacji zagadnienia interesuje się tym, czy podwładny czegoś nie potrzebuje do prawidłowego wykonania zadania, bardzo rzadko kontroluje postępy pracy, licząc na samodzielność. Często stosuje zwroty typu: dziękuję ci za wykonaną pracę, dobrze się spisałeś.

[6] M. Juchnowicz: *Zarządzanie przez zaangażowanie*. Warszawa 2010, s. 37.

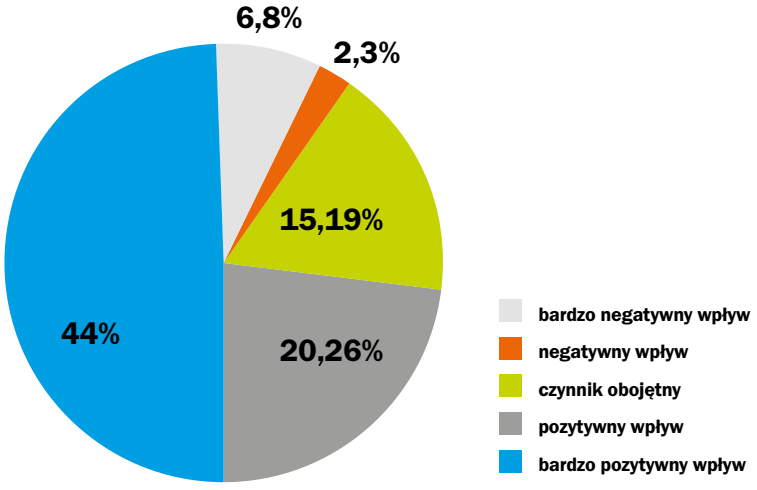
RYS. 5. REALIZACJA NOWEGO ZADANIA



RYS. 6. DUŻE ZAANGAŻOWANIE ZESPOŁU W REALIZACJĘ ZADANIA



RYS. 7. OSOBISTE ZAANGAŻOWANIE TWOJEGO BEZPOŚREDNIEGO PRZEŁOŻONEGO W REALIZACJĘ ZADANIA



Opracowanie własne (3).

d) W firmie organizowane są także spotkania pozasłużbowe między pracownikami i kierownikami mające na celu prawidłowe zbudowanie relacji.

3. Oceń swój stopień zaangażowania w wykonywanie zadań w poniższej sytuacji (skala 1–5).

a) Firma ma strukturę zhierarchizowaną, opartą na regulaminach i ustaleniach. Występuje atmosfera typowo służbowa. Zwracanie się do siebie na pan.

b) Przełożony wymaga bardzo dużo od pracowników, jednakże daje bardzo mizerny przykład osobisty. Daje sprecyzowane zadanie uniemożliwiające indywidualne podejście do zagadnienia czy problemu.

W czasie realizacji zagadnienia nie interesuje się tym, czy podwładny czegoś potrzebuje do prawidłowego wykonania zadania – liczy się tylko i wyłącznie efekt końcowy, bardzo często kontroluje postępy pracy.

Często stosuje zwroty typu: jeśli tego nie wykonasz, zostaniesz ukarany.

4. Jakie cechy Twojego bezpośredniego przełożonego zwiększają Twoje zaangażowanie?

5. Co chciałbyś zmienić w swoim miejscu pracy? Jakie czynniki zmniejszają Twoje zaangażowanie?

6. Jakie cechy Twojego przełożonego wpływają negatywnie na Twoje zaangażowanie?

Po przeanalizowaniu wyników otrzymano następujące odpowiedzi dotyczące punktu pierwszego ankiety:

– realizacja nowego zadania aż w 67% wpływa pozytywnie na zaangażowanie pracowników (rys. 5). W związku z tym jest to bardzo ważny czynnik. Mając to na uwadze, osoby zajmujące się planowaniem muszą się starać wprowadzać innowacje. Zaledwie 2% osób odczuwa duży spadek zaangażowania, kiedy stawia się ich przed nowymi wyzwaniami.

– Kolejnym rozpatrywanym czynnikiem było duże zaangażowanie zespołu w czasie realizacji zadania. Jego członkowie zarażają się nawzajem pozytywną energią, co działa na zespół bardzo pozytywnie. Patrząc na rys. 6, można zauważyć, że aż 86% osób uznało, że duże zaangażowanie zespołu koreluje dodatnio z zaangażowaniem indywidualnym, w związku z czym można śmiało stwierdzić, że przez pryzmat zaangażowania wzajemne „nakręcanie się pozytywną energią" jest nawet ważniejsze niż ciągłe wprowadzanie nowych zadań.

Następny determinant jest związany z osobistym zaangażowaniem przełożonego w realizację zadania (rys. 7). Już na pierwszy rzut oka można zauważyć, że nie ma tutaj aż tak wysokiego wyniku, jak w wypadku zaangażowania całego zespołu, jednak jest to czynnik, który istotnie dodatnio wpływa na zaangażowanie pracownika, w związku z czym to, czy przełożony sam angażuje się w dane zadanie, jest także bardzo ważne. Przy budowaniu zaangażowania należy też zwrócić uwagę na to, w jaki sposób wydajemy polecenia. Aż 78% badanych stwierdziło, iż ten czynnik znacząco działa na ich zaangażowanie. Przy formułowaniu celu należy się kierować zasadą SMART, tak by wydawane polecenia, czy też stawiane zadania były odpowiednio zrozumiane. Jednak czym byłoby stawianie zadań bez wprowadzenia w sytuację oraz omówienia, po co właściwie wykonujemy daną czynność. 74% osób biorących udział w wywiadzie ustrukturyzowanym stwierdziło, iż jest to istotny element.

Kolejny badany czynnik to wpływ dobrej atmosfery oraz właściwego kontaktu z przełożonym. Porównując go z pozostałymi wymienionymi dotychczas, stwierdzono, że aż 74% badanych uważa, że właśnie taka atmosfera wpływa bardzo istotnie na ich zaangażowanie, dodatkowo dla 10% jest to czynnik oddziałujący pozytywnie. Po podsumowaniu mamy aż 84% wyników pozytywnych. Dlatego też można stwierdzić, iż jest to czynnik niezmiernie ważny. Stosowanie omówienia oraz wspieranie podwładnego w czasie realizacji zadań jest także bardzo istotne. Aż 80% osób stwierdziło, że jest to element bardzo ważny lub ważny w budowaniu zaangażowania. Pogłębiając wiedzę na temat zaangażowania, należy też zwrócić uwagę na odpowiednie zachowanie przełożonego w związku z odpowiednim wynagrodzeniem. Aż dla 73% ankietowanych odpowiednie wynagrodzenie jest czynnikiem budującym zaangażowanie.

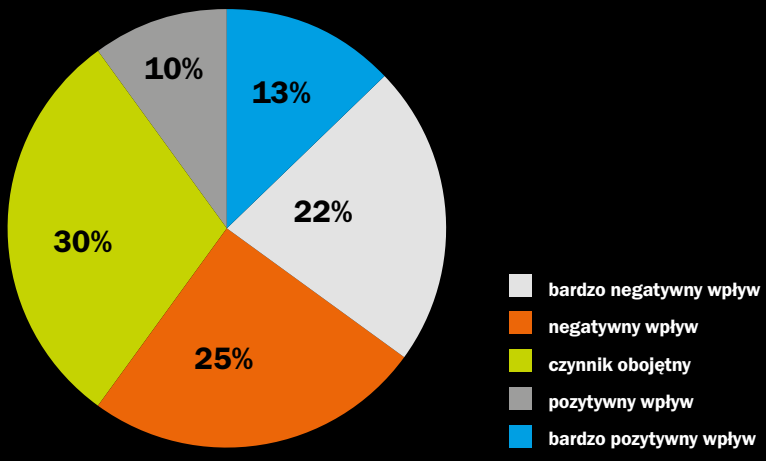
Po przeanalizowaniu czynników wzbudzających zaangażowanie w świetle literatury przedmiotu przyszedł czas na skonfrontowanie z rzeczywistością determinantów zmniejszających zaangażowanie. W czasie badań wynikło, że ciągła kontrola nie jest zjawiskiem pożądanym, co więcej, częste kontrolowanie podwładnego ogranicza ilość czasu przełożonego na realizację innych przedsięwzięć (rys. 8).

Z kolei atmosfera oparta na regulaminach oraz autorytecie formalnym nie wpływa pozytywnie na zaangażowanie (rys. 9).

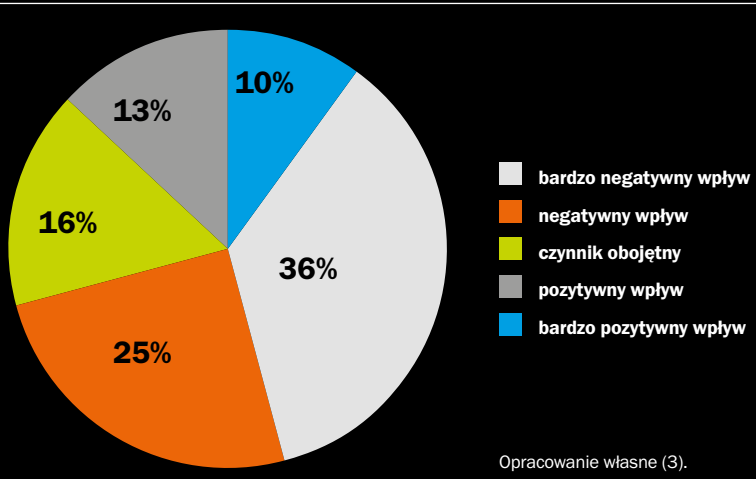
Struktura przeprowadzonego wywiadu miała na celu przedstawienie dwóch typów organizacji. Pierwsza z nich to organizacja nowego typu, nastawiona na człowieka, druga to firmy ukierunkowane wyłącznie na cel, z niską dbałością o stosunki interpersonalne. Ankietowani oceniali ich stopień zaangażowania w pracę podczas różnych sytuacji. Z wyników badań wynika, że hierarchizacja nie jest czynnikiem zmniejszającym zaangażowanie, jeśli w firmie występuje „zdrowa" atmosfera. Aż 90% ankietowanych stwierdziło, że to właśnie takie firmy wzbudzają ich zaangażowanie. Aż 81% osób uznało, że przykład osobisty oraz swoboda działania wpływają pozytywnie na zaangażowanie, nawet jeśli idą w parze z dużymi wymaganiami.

Jak wynika z badań, przełożony po postawieniu zadania powinien się zainteresować, czy podwładny ma odpowiednie narzędzia do jego wykonania. Bardzo pożądanym zjawiskiem jest także powiedzenie zwykłego dziękuję. Z kolei spotkania pozasłużbowe nie są aż tak istotnym czynnikiem, aczkolwiek też pozytywnie wpływają na zaangażowanie w pracę. Po przeanalizowaniu organizacji nastawionej na stosunki interpersonalne nastąpił czas, aby przyjrzeć się „przedsię-

RYS. 8.
STOSOWANIE CIĄGŁEJ KONTROLI



RYS. 9.
PRZESTRZEGANIE REGULAMINU



Opracowanie własne (3).

CZEŚĆ PRZEŁOŻONYCH ZUPEŁNIE NIE WIE, JAK CO PROWADZI DO CZYNNEGO SZKODZENIA ORAZ

biorstwu" starego typu. Typowo służbowa atmosfera w pracy również nie służy budowaniu zaangażowania. Aż dla 51% osób czynnik ten działa demotywująco. Brak przykładu osobistego oraz ograniczanie możliwości działania także wpływają negatywnie na zaangażowanie. Aż dla 79% osób postawienie zadania bez zainteresowania się, czy podwładny czegoś potrzebuje do jego wykonania, wpływa bardzo negatywnie na zaangażowanie. Ostatnim czynnikiem analizowanym podczas wywiadu ustrukturyzowanego był strach związany z niewykonaniem danego zadania. Okazuje się, iż dla 80% tzw. strach wpływa negatywnie na ich zaangażowanie. W czasie wywiadu respondenci mieli także możliwość odpowiedzi na pytania otwarte. W związku z czym uzyskano następujące wyniki:

Jakie cechy Twojego bezpośredniego przełożonego zwiększają Twoje zaangażowanie?

Respondenci zwrócili uwagę na takie cechy, jak: przykład osobisty, jasno określone oczekiwania, merytoryczna pomoc w trakcie realizacji zadania, sprawiedliwość, charyzma, szacunek dla ludzi, otwartość, decyzyjność, uczciwość, mentoring, empatia, pracowitość, zaangażowanie. Jednak pojawiają się także opinie negatywne, aż 11 uczestników wywiadu stwierdziło, że żadna cecha ich bezpośredniego przełożonego nie angażuje ich do działania.

Co chciałbyś zmienić w swoim miejscu pracy? Jakie czynniki zmniejszają Twoje zaangażowanie?

Były to takie uwagi, jak: zbyt duży natłok pracy, asekuranctwo przełożonych w czasie przydzielania zadań (osoby niekompetentne otrzymują mniej zadań ze względu na strach przełożonego przed słabą jakością wykonania zadania), bardzo niska frekwencja, wakaty, zbyt częsta kontrola, skupianie się na rzeczach mało istotnych, brak perspektyw rozwoju, brak feedbacku, niekompetencja dowódców, hipokryzja, ciągły strach

RAWPIXEL/PIXABAY

POSTĘPOWAĆ Z CZŁOWIEKIEM, ZMNIEJSZENIA ZAANGAŻOWANIA

przed karą, brak wsparcia. Co więcej, niektórzy respondenci stwierdzili, że jedyne co chcą zmienić w miejscu swojej pracy to przełożonego, ponieważ to właśnie on wpływa negatywnie na zaangażowanie.

Jakie cechy Twojego przełożonego wpływają negatywnie na Twoje zaangażowanie?

Respondenci zaliczyli do nich: brak kompetencji na stanowisku, brak dostosowania do potrzeb podwładnych, egoizm, wywyższanie się, nerwowość, brak autorytetu, stronniczość, brak zrozumienia, pychę, bycie przełożonym a nie dowódcą, brak przykładu osobistego, niedocenianie podwładnych, nadmierne delegowanie obowiązków, brak kultury osobistej, niskie zaangażowanie. Dodatkowo aż dziesięciu respondentów wskazało na lenistwo przełożonych.

Po przeanalizowaniu wyników badań można śmiało stwierdzić, iż determinanty zaangażowania przedstawione w literaturze są zbieżne z odpowiedziami ankietowanych. Jednak bardzo niepokojący jest fakt, iż cześć przełożonych zupełnie nie wie, jak postępować z człowiekiem, co prowadzi do czynnego szkodzenia oraz zmniejszenia zaangażowania.

Dodatkowo trzeba zauważyć, że brak zaangażowania może prowadzić do wypalenia zawodowego, a w efekcie do zmiany pracy. W związku z tym, czy nie warto zainteresować się obowiązkowymi szkoleniami z zakresu mentoringu, coachingu lub też szeroko pojętego zarządzania zasobami ludzkimi dla osób zarządzających grupami ludzi? To właśnie takie szkolenia będą w stanie zmienić perspektywę osób zarządzających, a w efekcie doprowadzić do zmniejszenia liczby wakatów czy też do czynnego zaangażowania pracowników. I co najważniejsze, zwiększą poczucie przywiązania pracownika (żołnierza) do miejsca pracy (służby). ■

Zużycie i uszkodzenie **łożysk tocznych**

DBAŁOŚĆ O WŁAŚCIWY STAN TECHNICZNY SPRZĘTU TO NIE TYLKO OBSŁUGA CODZIENNA I OKRESOWA. TO TAKŻE ZWRACANIE UWAGI NA WSZELKIE ODSTĘPSTWA W DZIAŁANIU POJAZDU PODCZAS JEGO EKSPLOATACJI.

st. chor. sztab. mgr inż. Dariusz Woźniak

Autor jest p.o. szefem Służby Czołgowo-Samochodowej w 17 Wojskowym Oddziale Gospodarczym.

W sprzęcie technicznym występują one powszechnie i wbrew pozorom ich rola jest dość duża. Wymagają od użytkowników oraz pracowników nadzoru technicznego wiele uwagi i to ciągłej, by nie dopuścić między innymi do uszkodzeń samochodu (pojazdu), wypadku (kolizji) oraz strat ekonomicznych. Zasadniczym wymaganiem technicznym, jakie stawia się łożyskom tocznym, jest zdolność przenoszenia obciążeń przy danej liczbie obrotów. Typ łożyska określają głównie następujące parametry[1]:

• zdolność przenoszenia przez nie obciążeń w różnych kierunkach, przy czym w zależności od kierunku obciążenia można je podzielić na trzy zasadnicze grupy:

– poprzeczne – przystosowane do przenoszenia obciążeń w kierunku prostopadłym do osi (niektóre konstrukcje łożysk poprzecznych mogą przenosić również obciążenia wzdłużne),

– wzdłużne – przystosowane do przenoszenia obciążeń wzdłużnych w kierunku osi łożyska; do tej grupy zalicza się również te przypadki obciążenia, przy których obciążenie wzdłużne odgrywa główną rolę,

– skośne – przystosowane do obciążeń złożonych (poprzeczne i wzdłużne);

• kształt części tocznych; w zależności od niego łożyska dzielą się na: kulkowe, wałeczkowe i igiełkowe; wałeczki występują jako: walcowe, stożkowe, kręte, baryłkowe itp.[2];

• zdolność do samoustawiania się lub nieustawiania pod wpływem zmiany położenia wału; rozróżnia się w tej grupie:

– łożyska wahliwe (samoustawne),

– łożyska niewahliwe.

Bardzo ważnym zagadnieniem jest normalizacja łożysk tocznych pod względem rodzajów, wymiarów i znakowania[3].

ZASTOSOWANIE

Spośród różnych rodzajów łożysk tocznych[4] w pojazdach samochodowych najczęściej są stosowane łożyska kulkowe. Analizując rozwiązania konstrukcyjne, można zauważyć, że zazwyczaj występują w różnych połączeniach i podzespołach samochodów, np. w układzie zawieszenia. Łożyska toczne są używane w wahaczach, i razem z nimi podlegają wymianie. Innymi składowymi zawieszenia, gdzie są wykorzystywane, są amortyzatory. Również w układach kierowniczych występują łożyska toczne kulkowe lub igiełkowe, głównie w kolumnach i przekładniach kierowniczych. Kon-

[1] K. Witkowski, H. Brudnicki: *Łożyska toczne w pojazdach mechanicznych*. MON, Warszawa 1955.

[2] *Łożyska toczne*. Katalog-informator. Warszawa 1982.

[3] Ibidem.

[4] Z. Jaśkiewicz: *Łożyskowanie toczne w pojazdach mechanicznych*. Warszawa 1971.

ARCH. AUTORA (2)

1. Elementy toczne łożyska z ubytkami

2. Bieżnia wewnętrzna łożyska z ubytkami

strukcyjnie (w zależności od przeznaczenia samochodu) najwięcej łożysk tocznych jest zabudowanych w układach przeniesienia napędu (tab.).

Układy kół zębatych skrzyń biegów, skrzyń rozdzielczych i skrzyń pośrednich są łożyskowane na różnego rodzaju łożyskach igiełkowych, a wałki pośrednie i zdawcze – na łożyskach kulkowych, igiełkowych lub walcowych. W mechanizmach różnicowych mostów przednich, tylnych i pośrednich są stosowane głównie łożyska stożkowe. W skład półosi napędowych wchodzą najczęściej łożyska kulkowe typu zakrytego.

W mostach napędowych znajdują zastosowanie m.in. łożyska: stożkowe, walcowe, rzadziej kulkowe i igiełkowe. W rozwiązaniach konstrukcyjnych różnych typów silników spalinowych stosuje się również łożyska toczne. Należy tu wskazać pompy układów chłodzenia, wspomagania i zasilania, gdzie przewidziano łożyska kulkowe lub walcowe albo typu igiełkowego. W wentylatorach, prądnicach i alternatorach wykorzystuje się przede wszystkim układy łożysk kulkowych. Dobór, montaż i smarowanie łożyska to podstawowe czynniki wpływające na jego prawidłową i długotrwałą pracę. Temperatura odpowiednio zamontowanego i smarowanego nie powinna przekraczać 70°C, a w czasie eksploatacji pozostawać na niższym poziomie. Pracujące łożyska powinny wydawać regularny, niski dźwięk (pomruk). Jakiekolwiek gwizdy i piski mogą świadczyć o zbyt małych luzach roboczych lub niedostatecznym smarowaniu. Z kolei grzechotanie, nierównomierny szum czy dudnienie mogą oznaczać zbyt duży luz lub uszkodzenie bieżni i elementów tocznych. Uszkodzenie łożyska może nastąpić na skutek zbyt dużego obciążenia, nieskutecznych uszczelnień lub za ciasnych pasowań, powodujących zbyt mały luz, oraz długiego okresu eksploatacji (pracy).

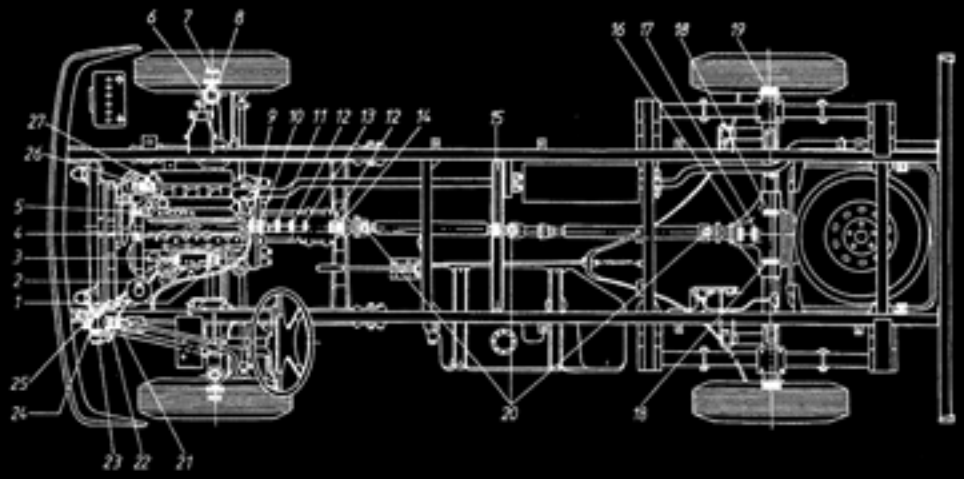
Pozostają wówczas na nim charakterystyczne ślady. Poddając takie łożysko analizie technicznej i szczegółowym oględzinom, można wyciągnąć wnioski dotyczące przyczyny uszkodzenia (niekiedy zużycia) oraz podjąć właściwe działania obsługowo-naprawcze[5].

DEFEKTY I USZKODZENIA

Mają postać ubytku lub zniekształcenia, najczęściej elementów konstrukcyjnych, co często prowadzi do całkowitego zniszczenia łożyska[6]. Do uszkodzeń i defektów należy zaliczyć m.in.: korozję bieżni lub elementów tocznych, zatarcia, złuszczenia czy nierówność

[5] D. Woźniak, J. Kubicki, Z. Ciekot: *Obsługiwania techniczne i naprawy sprzętu wojskowego z uwzględnieniem jego tendencji rozwojowych w odniesieniu do wybranych aspektów technicznych.* W: *Tendencje rozwojowe środków transportowych w Siłach Zbrojnych RP.* Warszawa-Sulejówek 2015.

[6] J. Janecki, S. Gołąbek: *Zużycie części i zespołów pojazdów samochodowych*. Warszawa 1974.



(1) – skrzynia pięciobiegowa TS5-21
(2)– skrzynia czterobiegowa A13.3
(3)– przekładnia kierownicza ze wspomaganiem
(4)– przekładnia kierownicza bez wspomagania

TABELA. ZESTAWIENIE ŁOŻYSK TOCZNYCH W SAMOCHODZIE LUBLIN

Pozycja na rysunku	Oznaczenie łożyska	Numer normy	Nazwa łożyska i zastosowanie	Liczba sztuk
1	6200-2RS	CSN 02 4640	łożysko kulkowe regulacji prędkości obrotowej	1
2	6403A	CSN 02 4630	łożysko stożkowe pompy wtryskowej	1
3	6303A	CSN 02 4630	łożysko stożkowe pompy wtryskowej	1
4	6206-2RS	PN-85/M-86100	łożysko kulkowe napinacza paska zębatego	2
5	11.26.100.2	PLC75-2-9	wałek w komplecie z łożyskiem cieczy chłodzącej	1
6	512Z25.1V	PN-86/M-86260	łożysko kulkowe wzdłużne zwrotnicy	2
7	30207A	PN-86/M-86220	łożysko stożkowe piasty kół (wewnętrzne)	2
8	30305A	PN-86/M-86220	łożysko stożkowe piasty kół (zewnętrzne)	2
9	6203-2RS	PN-85/M-86100	łożysko kulkowe wałka sprzęgłowego	1
10	114-791-2Z	–	łożysko kulkowe wyciskowe sprzęgła (1)	1
10	17-1601072	CBK-197	łożysko kulkowe wyciskowe sprzęgła (2)	1
11	32008XA-FAG	–	łożysko stożkowe wałka napędowego skrzynki biegów (1)	1
11	20-1701032	–	łożysko kulkowe wałka sprzęgłowego skrzynki biegów (2)	1
12	30206A-FAG	–	łożysko stożkowe wałka pośredniego (1)	2
12	M-7118/M-7121	–	łożysko wałeczkowe wałka pośredniego krótkie/długie (2)	2
13	32004X-FAG	–	łożysko stożkowe wałka głównego bez pierścienia zewnętrznego (1)	1
13	K20x26x17	PN-81/M-86310	łożysko igiełkowe skrzyni biegów (2)	1
14	32008XA-FAG	–	łożysko stożkowe wałka głównego (1)	1
14	A13.1-1701190	–	łożysko kulkowe skośne wałka głównego (2)	1
15	62205-2RS	PN-85/M-86100	łożysko kulkowe podpory wału napędowego	1
16	33207A	PN-86/M-86220	łożysko stożkowe zewnętrzne wałka napędzającego	1
17	32308A	PN-86/M-86220	łożysko stożkowe wewnętrzne wałka napędzającego	1
18	3202-2403050	–	łożysko stożkowe mechanizmu różnicowego	2
19	U499-U460L	–	łożysko stożkowe półosi kpl.	2
20	12.431.0.030	–	krzyżak z łożyskami kpl.	3
21	03.880.0	–	złożenie igiełkowe (3)	1
21	62.315.0.702	–	złożenie kulkowego łożyska ślimaka (4)	2
22	03-888.0	–	złożenie kulkowe (3)	1
22	62.113.0.702	–	pierścień złożenia kulkowego łożyska ślimaka (4)	2
23	03.822.0	–	łożysko (3)	2
23	RHNA 354220	PN-84/M-86295	łożysko igiełkowe przekładni kierowniczej (4)	3
24	03.821.0	–	łożysko (3)	1
25	03.879.0	–	złożenie igiełkowe (3)	1
26	6302A-2Z	PN-85/M-86100	łożysko kulkowe alternatora (przednie)	1
27	6201A-2Z	PN-85/M-86100	łożysko kulkowe alternatora (tylne)	1

Opracowanie własne na podstawie: J. Zagaja, A. Grabowski: *Naprawa samochodów Lublin*. Warszawa 1997.

3. Zużycie łożyska w węźle

4. Zmatowienie elementów tocznych

ARCH. AUTORA (2)

powierzchni tocznej. Mogą one powstawać nie tylko na skutek nadmiernego obciążenia łożysk czy starzenia się ich elementów, lecz także w wyniku niewłaściwego montażu lub smarowania. Dlatego tak ważne jest sprawowanie nadzoru eksploatacyjno-diagnostycznego przez użytkownika. Powinien on rozpoznawać zmiany stanu dynamicznego łożysk pod względem m.in.: jakości pracy, stopnia hałasu, postępującego zużycia i zwiększania się luzów oraz rodzaju i poziomu ewentualnych uszkodzeń po to, by zapobiec ich skutkom i wcześniej podjąć odpowiednie działania techniczne.

Do istotnych uszkodzeń łożysk samochodowych można zaliczyć: złuszczenia (łuszczenie), pełzanie, blokowanie, uszkodzenie koszyka, koliste ślady wytarcia, zacieranie się (fretting), korozję (w tym elektrolityczną), wgniecenia, zmatowienie oraz pitting (wykruszenia). Uszkodzenia te wywierają wpływ na bezpieczeństwo i ergonomię eksploatacji (jazdy), a także na własności trakcyjne pojazdu. W razie ich wystąpienia i zweryfikowania konieczna jest natychmiastowa wymiana uszkodzonych łożysk. Ważne jest więc wczesne wykrycie uszkodzeń. Wymaga to, o czym już wspomniano, monitorowania pracy łożysk głównie przez użytkownika, także podczas wykonywania obsług bieżących (OB) i okresowych obsług technicznych zalecanych przez producenta lub wojskowy organ normalizacyjny, oraz doskonalenia metod diagnostycznych.

Na fotografii 1 przedstawiono łożysko stożkowe wymontowane z piasty koła. Wykazuje ono zmiany zmęczeniowe typu pitting. W środkowej części bieżni (fot. 2) widoczne są ślady nadmiernego zużycia (ubytek materiału). Wyniki analizy technicznej pozwoliły na stwierdzenie, że uszkodzona powierzchnia nie jest gładka – występują na niej liczne jamki o zróżnicowanej wielkości i różnym kształcie. Podczas dalszej weryfikacji zauważono zjawisko pittingu oraz nadmierne zużycie materiału, które występowało również na elementach tocznych przedstawionego łożyska (fot. 1).

Powierzchnie wykazujące nadmierne zużycie i zmiany wywołane przez pitting na bieżni wewnętrznej świadczą o nierównomiernym jej obciążeniu na obwodzie. Przyczyną może być przekoszenie bieżni wewnętrznej w stosunku do elementów tocznych oraz bieżni zewnętrznej, spowodowane niewłaściwym montażem łożyska lub zbyt dużym jego luzem. Nadmierne zużycie występuje w obszarze największego nacisku. W czasie pracy łożyska z takim uszkodzeniem powstają duże obciążenia dynamiczne skutkujące rozprzestrzenianiem się pęknięć oraz drganiami elementów węzła łożyskowego, które przenoszą się na inne podzespoły układu jezdnego. Może to wywierać niekorzystny wpływ na ich trwałość. Oprócz tego drgania tego rodzaju są źródłem hałasu. W samochodach osobowych taki hałas często sygnalizuje kierowcy, że doszło do uszkodzenia łożyska i konieczna jest jego naprawa. W samochodach ciężarowych, ze względu na duży hałas powodowany przez silnik oraz wytłumienie kabiny, kierowca na ogół nie ma możliwości usłyszenia niekorzystnych symptomów akustycznych towarzyszących uszkodzeniu łożysk tocznych kół jezdnych. W takiej sytuacji pozostaje głównie weryfikacja warsztatowa.

Innym uszkodzeniem łożysk tocznych kół jezdnych samochodów, występującym często w procesie eksploatacji, jest ich przegrzanie. Jego efektem jest zmatowienie i zmiana barwy powierzchni bieżni i elementów tocznych. Ponadto w wyniku weryfikacji powierzchni bieżni zewnętrznej przegrzanego łożyska stwierdza się często występowanie znacznych nierówności. Współpraca toczna takich powierzchni prowadzi do powstawania obciążeń dynamicznych mogących być przyczyną innych uszkodzeń.

Przegrzanie łożysk może być skutkiem zbyt małego luzu między elementami tocznymi a bieżniami. Niekiedy również jest spowodowane brakiem środka smarnego lub utratą jego własności użytkowych w związku z procesami starzenia.

Nieco inną odmianą uszkodzenia łożysk tocznych, często występującą w procesie eksploatacji, jest klasyczne ich zużycie (fot. 3), połączone ze zmianą chropowatości powierzchni. Wywołane jest długotrwałą pracą. Objawia się zwiększonym luzem oraz zmatowieniem i częściową zmianą barwy powierzchni bieżni i elementów tocznych, często ze smugami na obwodzie (fot. 4). Łożyska takie są kwalifikowane zazwyczaj do wymiany jako niesprawne, faktycznie jednak spełniają warunki techniczne i mogą być dalej używane. Podobnie mylna może być ocena dokonywana podczas ich weryfikacji na podstawie tylko wyglądu zewnętrznego bezpo-

5. Montaż łożyska w piaście

6. Uszkodzone pierścienie

7. Uszkodzenia i braki elementów bieżnych

ARCH. AUTORA (3)

średnio po ich demontażu z podzespołów samochodowych, np. z piast kół czy półosi napędowych. Często po starannym umyciu, osuszeniu i wymianie smaru nadają się do dalszej eksploatacji.

IDENTYFIKACJA USZKODZEŃ

W praktyce warsztatowej uszkodzenia spowodowane *niewłaściwym montażem* można rozpoznać, stosując typowe metody organoleptyczne, najczęściej na podstawie występujących rys, defektów o charakterze mechanicznym oraz wgłębień na bieżni łożyska. Najczęstsze przyczyny uszkodzeń bieżni wynikają z:

– przenoszenia sił osiowych podczas montażu, powodujących wgniecenia na bieżniach łożysk kulkowych;

– przekoszenia pierścienia wewnętrznego w stosunku do pierścienia zewnętrznego z wałeczkami (przekoszenie wałka w stosunku do oprawy), powodujące powstawanie zatarć na powierzchniach pracujących łożysk walcowych;

– bezpośredniego uderzenia młotka w czasie montażu, czego następstwem są na przykład wykruszenia obrzeża jednego z pierścieni łożyska.

Nienormalny ślad na bieżni łożyska może wynikać ze zbyt ciasnych pasowań, z nadmiernego zacisku wzdłużnego, z błędów kształtu czopa, z niewspółosiowości czopów lub zbyt ciasnego osadzenia łożyska ruchomego.

Jednym z możliwych rodzajów likwidacji tego rodzaju uszkodzeń jest wciskanie łożysk do podzespołów samochodowych, na przykład piast kół przednich, za pomocą pras mechanicznych czy hydraulicznych (fot. 5) z wykorzystaniem odpowiednich elementów oporowych o różnych kształtach i średnicach. Zachowuje się wówczas wymagany nacisk.

Właściwy montaż i pewne osadzenie pierścieni łożyska na wale napędowym i w obudowie na przykład skrzyni biegów w zależności od rodzaju pasowania i wymaganych luzów montażowych ma istotne znaczenie dla prawidłowego działania węzła łożyskowego i jego trwałości[7]. Sporadycznie występują *błędy konstrukcyjne*, często wynikające z niedopracowania technicznego, niedokładności obróbki, braku lub niezachowania wymaganych pasowań (tolerancji wymiarowych). Niekiedy są one korygowane przez producenta (wykonawcę) w ramach organizowanych kampanii. Z kolei *korozja i zanieczyszczenie łożysk* jest stosunkowo częstą przyczyną wywołującą przyspieszone ich zużycie (lub uszkodzenie), wynikające m.in. z:

– niewłaściwego przechowywania i złej konserwacji łożysk w magazynach lub zestawach naprawczych;

– nieodpowiedniego uszczelnienia łożyska, czego następstwem może być przedostanie się wody lub oparów kwasów, a także zakwaszenie środków smarnych wewnątrz niego;

[7] Z. Jaśkiewicz: *Łożyskowanie toczne*..., op.cit.

– uszkodzenia lub utraty szczelności przez osłony blaszane i pierścienie gumowe w łożyskach tocznych typu zakrytego (fot. 6), wynikiem czego jest ich uszkodzenie i częściowe wypadnięcie z nich kulek tocznych (fot. 7).

Zanieczyszczenia łożysk najczęściej mają związek z:

– montażem zabrudzonych części lub niewłaściwym ich rozkonserwowaniem,

– przedostaniem się na przykład cząsteczek stałych (piasku) do obudowy,

– niewłaściwym uszczelnieniem węzłów łożyskowych,

– występowaniem metalowych opiłków z kół zębatych (lub innych cząsteczek), wprowadzonych do łożyska razem z olejem,

– zanieczyszczeniem smaru lub jego zestarzeniem.

W sytuacji oddziaływania bardzo dużych wymuszeń dynamicznych powodowanych przez pracę sąsiadujących układów w podzespołach, wałach i półosiach elementy toczne łożyska będącego w spoczynku mogą odcisnąć się na jego bieżniach. Z praktycznego punktu widzenia *przegrzania i uszkodzenia termiczne* są najczęstszymi przyczynami pracy łożyska w podwyższonej temperaturze, do czego może doprowadzić:

– zbyt ciasne pasowanie na zasadzie stałego wałka lub stałego otworu,

– mały luz łożyska na skutek jego nagrzewania się od wału (fot. 8), co najczęściej powoduje dość rozległe uszkodzenia,

– nieodpowiedni dobór smaru plastycznego lub oleju do danych warunków pracy węzła łożyskowego,

– zbyt niski poziom oleju spowodowany na przykład jego wyciekiem z obudowy lub mała ilość smaru w węźle,

– zbyt wysoki poziom oleju,

– odkształcenie otworów obudowy, nierówna powierzchnia podparcia,

– zbyt mały luz łożyska ze względu na wydłużanie się wału,

– ocieranie się uszczelnienia lub odrzutników oleju o nieruchome elementy,

– zatkane kanały powrotne oleju,

– zbyt silnie dokręcona nakrętka tulei,

– niewyważenie elementów wirujących,

– niewspółosiowe ustawienie na przykład wałów napędowych samochodu,

– niewłaściwie umiejscowiony (przeciwnie do kierunku obrotu łożyska) regulator poziomu oleju,

– zbyt luźne pasowanie, niekiedy zbyt duży otwór w obudowie, potocznie określany jako rozkalibrowanie (fot. 9 – przykład uszkodzenia łożyska wału w otworze obudowy skrzyni rozdzielczej samochodu średniej ładowności wysokiej mobilności typu Star 266).

Uszkodzenie łożyska tocznego kulkowego spowodowane przez zestarzały smar i długotrwałą pracę w podwyższonej temperaturze pokazano na fotografii 10. Powierzchnie zewnętrzne i układ bieżny łożyska są mocno oklejone zgorzeliną, na której pojawia się

Uszkodzenia mechaniczno-termiczne łożyska

Rozkalibrowanie obudowy

ARCH. AUTORA (3)

Podzespół z zastosowanym niewłaściwym olejem

11.

Łożysko podpory

12.

13. Części koszyczka i kulek

ARCH. AUTORA (3)

ZBYT UPROSZCZONE ANALIZY DOTYCZĄCE STANU PRZEDWCZESNĄ WYMIANĘ ORAZ GENEROWANIE

następnie korozja. Łożysko jest w dużym stopniu zmatowiałe, o zmienionej barwie powierzchni bieżni i elementów tocznych. Niekiedy podczas weryfikacji uszkodzenia po spuszczeniu oleju z podzespołu okazuje się, na przykład, że skrzynia biegów została zalana niewłaściwym jego rodzajem (fot. 11). W tym przypadku stosowano rozrzedzony olej, przypominający konsystencją bardziej hydrauliczny niż przekładniowy. Miało to określone znaczenie dla czasu i jakości pracy łożysk w podzespole.

Powodem uszkodzeń łożysk tocznych mogą być drgania. Do ich źródeł zalicza się m.in.[8]:

– zmianę liczby elementów tocznych przenoszących obciążenie wpływające na zmianę sztywności układu i generujące drgania parametryczne (gasnące lub niegasnące);

– błędy wynikające z technologii wykonania elementów łożyska (niedokładność kształtu bieżni pierścienia i elementów tocznych), na przykład odchylenia od kształtu okrągłego, baryłkowego (owalność, falistość) względem gładkości powierzchni (niekiedy chropowatości);

– niewyważenie koszyka na przykład na skutek częściowej deformacji;

– mimośrodowość bieżni w stosunku do osi obrotu wału, luz promieniowy lub osiowy powiększający się w sposób przyspieszony podczas eksploatacji (pracy);

– drgania własne poszczególnych elementów łożyska o charakterze gasnącym, przy czym poziom drgań uszkodzonych łożysk podnosi się wraz z ich zużyciem i często ma przebieg niegasnący.

Defekt często występujący w połączeniach wałów napędowych za pomocą tzw. łożyska pośredniego pokazano na fotografii 12. Łożysko po przekroczeniu określonego luzu uległo zużyciu. Bezpośrednim objawem było tzw. bicie wału i intensywny wyciek smaru z gumowej obsady łożyska wzmocnionej stalową obejmą. Stosunkowo często w wyniku eksploatacji łożysk dochodzi do ich zniszczenia w postaci uszkodzenia koszyczka (fot. 13), którego zadaniem jest między innymi podtrzymanie elementów bieżnych i zapewnienie równomiernej ich pracy. Taka awaria kwalifikuje łożysko do wymiany. Do analizy technicznej przyjęto łożysko wałka napędowego skrzyni rozdzielczej samochodu dużej ładowności zwiększonej mobilności typu Jelcz 662. Podczas jazdy skrzynia uległa awarii. Reakcja kierowcy z powodu warunków drogowych i hałasu była dość spóźniona, gdyż skrzynia uległa zablokowaniu i uszkodzeniu, między innymi pękła żeliwna pokrywa obudowy (fot. 14).

Zablokowany został wałek główny, łożysko zaś całkowicie zniszczone. Zdefragmentowaniu uległa jego bieżnia zewnętrzna. Uszkodzone zostały również elementy toczne, na powierzchniach których widać wy-

[8] J. Janecki, S. Gołąbek: *Zużycie części...*, op.cit.

Uszkodzona pokrywa uszczelniająca

14.

15. Miejsce uszkodzenia

ARCH. AUTORA (2)

TECHNICZNEGO ŁOŻYSK POWODUJĄ CZĘSTO ICH KOSZTÓW Z TYM ZWIĄZANYCH

raźne odkształcenia mechaniczne w postaci nieregularnych wyżłobień oraz zniekształceń kształtu wywołanych naciskami i tarciem. Ich charakter wskazuje na oddziaływanie bardzo dużych obciążeń dynamicznych.

Inny przykład uszkodzenia eksploatacyjnego łożyska to pęknięcie tylnej półosi napędowej samochodu ciężarowo-osobowego dużej mobilności typu Tarpan Honker. Podczas jazdy nastąpiła awaria w układzie przeniesienia napędu i słyszalny był wyraźny chrobot połączony z piskami, prawidłowo zidentyfikowany przez kierowcę. Po demontażu piasty tylnego koła samochodu za pomocą wyciągacza oraz wyjęciu części półosi z pochwy tylnego mostu napędowego ustalono przyczynę awarii (fot. 15). Pośrednio było nią uszkodzenie łożyska kulkowego typu zakrytego, które pracowało nadal, powodując coraz większe drgania i opory w przekazywaniu napędu przez elementy i półoś na koło. Efektem końcowym było ukręcenie półosi i pęknięcie jej na wskroś.

METODY DIAGNOZOWANIA

W wojskowej praktyce warsztatowej stosuje się najczęściej metody organoleptyczne, takie jak: obserwacja wzrokowa, osłuchiwanie łożyska oraz kontrola jego temperatury. Właściwie pracujące łożysko wywołuje miękki, czysty szum. Nietypowe dźwięki o charakterze mielenia, gwizdania lub innym wskazują najczęściej na pogorszenie jego stanu. Metaliczne dźwięki mogą świadczyć o zbyt małym luzie na łożysku. Nierównomierny czysty ton może być wynikiem wgłębień na jego bieżni. Z kolei niewystarczająca ilość smaru będzie słyszana jako gwizd. Następujące okresowo hałasy mogą wskazywać na uszkodzenie elementu tocznego. Zanieczyszczone łożysko powoduje hałas jak przy mieleniu. Na znaczne jego uszkodzenie wskazuje nieregularny i wysoki poziom hałasu. Jednak najprostszą metodą diagnozowania są okresowe lub ciągłe pomiary szerokopasmowych poziomów drgań. Zarejestrowane poziomy drgań węzłów łożyskowych są porównywane z wartościami granicznymi, podanymi na przykład w międzynarodowych normach ISO 10816.

* * *

Przedstawiona w artykule problematyka przybliża niektóre aspekty techniczne związane z eksploatacją, stanem technicznym i zasadnością wymiany łożysk tocznych w pojazdach samochodowych. Autor odniósł ją bezpośrednio do swojej praktyki zawodowej w służbie czołgowo-samochodowej i wybrał niektóre przykłady w ujęciu praktycznym. Zbyt uproszczone analizy stanu technicznego łożysk powodują często ich przedwczesną wymianę oraz generowanie kosztów z tym związanych. Natomiast nieprzestrzeganie określonych warunków eksploatacji i obsług technicznych oraz brak reakcji użytkownika na ich niewłaściwą pracę często jest przyczyną znacznych uszkodzeń podzespołów i połączeń w węzłach łożyskowych w samochodach. ■

Bałtycki **tygrys**

LITWA BARDZO POWAŻNIE POTRAKTOWAŁA KWESTIĘ WZMOCNIENIA SWOJEJ ARMII I W KRÓTKIM CZASIE WYKONAŁA KILKA ISTOTNYCH KROKÓW W TEJ DZIEDZINIE, KONTYNUUJĄC DZIAŁANIA ZMIERZAJĄCE DO JEJ DALSZEJ MODERNIZACJI.

płk rez. Tomasz Lewczak

Autor jest starszym specjalistą w Oddziale Szkolenia Międzynarodowego Inspektoratu Szkolenia DGRSZ.

W marcu 2015 roku litewska Rada Obrony Państwa jednogłośnie zaakceptowała założenia *Koncepcji obronności kraju* na kolejne siedem lat (2015–2021). Przyjęto kierunki rozwoju sił zbrojnych Litwy i zdefiniowano szczegółowe priorytety. Zdecydowano m.in. o przywróceniu w trybie natychmiastowym zasadniczej służby wojskowej, zapowiedziano też utworzenie nowych jednostek oraz zmodernizowanie uzbrojenia i wyposażenia we wszystkich rodzajach sił zbrojnych, szczególnie w wojskach lądowych. W tych ostatnich w pierwszej kolejności założono pozyskanie: kołowych bojowych wozów piechoty, śmigłowców bojowych, artyleryjskich środków ogniowych oraz środków obrony przeciwlotniczej. W parlamencie Litwy przyjęto ustawy o systematycznym, skokowym (tzw. tygrysie skoki) wzroście budżetu Ministerstwa Obrony Narodowej (MON), co umożliwi szybką realizację przyjętych założeń *Koncepcji…* W związku z tym siły zbrojne Litwy weszły w 2018 rok ze zwiększonym o 300 mln euro budżetem, który w 2017 roku wyniósł około 725 mln euro. Planowane kolejne zakupy uzbrojenia i sprzętu wojskowego opierają się na założeniu dalszego wzrostu budżetu obronnego do poziomu 2,00% PKB w 2020 roku.

WOJSKA LĄDOWE

Do końca 2015 roku najważniejszą jednostką litewskich wojsk lądowych była Brygada Piechoty Zmotoryzowanej o nazwie Żelazny Wilk (lit. Geležinis Vilkas), która w swojej strukturze miała trzy bataliony piechoty i dywizjon artylerii. Ponadto w skład wojsk lądowych wchodziły: trzy samodzielne bataliony zmotoryzowane, batalion inżynieryjny, Centrum Szkolenia Wojsk Lądowych oraz Ochotnicze Siły Obrony Narodowej (OSON) liczące sześć batalionów piechoty. OSON to nic innego jak bataliony obrony terytorialnej. Szkolenie w nich trwa średnio około 20 dni w roku.

Realizując ustalenia litewskiego parlamentu, w styczniu 2016 roku utworzono Brygadę Piechoty Zmotoryzowanej o nazwie Gryf (lit. Žemaitija). Jej głównym zadaniem będzie wykonywanie zadań w ramach artykułu 5 *Traktatu Północnoatlantyckiego*, czyli obrona terytorium Litwy ze szczególnym uwzględnieniem wybrzeża morskiego. Miejscem stałej dyslokacji dowództwa brygady jest Kłajpeda.

W strukturze organizacyjno-etatowej Brygady znajduje się batalion Dragonów im. Wielkiego Księcia Butigeidisa z Kłajpedy (wcześniej był on podporządkowany dowódcy wojsk lądowych) oraz batalion piechoty zmotoryzowanej im. Wielkiego Księcia Kęstutisa z Taurogów (z brygady Żelazny Wilk). Następnie pojawiły się w niej kompanie: zabezpieczenia logistycznego, rozpoznawcza i łączności. Z kolei w 2017 roku rozwinięto batalion piechoty i dywizjon artylerii samobieżnej. Proces tworzenia Brygady i osiągnięcie przez nią gotowości bojowej ma nastąpić do końca 2021 roku.

Brygada Piechoty Zmotoryzowanej Żelazny Wilk w 2016 roku przeszła gruntowną restrukturyzację

Żelazny Wilk

Brygada Piechoty Zmotoryzowanej Żelazny Wilk (lit. Geležinis Vilkas) w 2016 roku przeszła gruntowną restrukturyzację i obecnie dysponuje czterema batalionami zmotoryzowanymi, dywizjonem artylerii samobieżnej oraz batalionem zabezpieczenia logistycznego.

U.S. ARMY/ANDREW MCNEIL

SIŁY ZBROJNE LITWY WESZŁY W 2018 ROK ZE ZWIĘKSZONYM O 300 MLN EURO BUDŻETEM, KTÓRY W 2017 ROKU WYNIÓSŁ OKOŁO 725 MLN EURO

i obecnie dysponuje czterema batalionami zmotoryzowanymi, dywizjonem artylerii samobieżnej oraz batalionem zabezpieczenia logistycznego. Ponadto wojska lądowe mają w swoim składzie skadrowaną brygadą zmechanizowaną z dowództwem w Wilnie. Będzie ona rozwinięta w razie zagrożenia wybuchem wojny.

W wyniku przywrócenia zasadniczej służby wojskowej (trwa dziewięć miesięcy, z czego trzy są przeznaczone na szkolenie podstawowe i specjalistyczne, a sześć miesięcy na szkolenie zgrywające pododdział: drużyna-pluton – kompania-batalion) liczebność litewskich sił zbrojnych na koniec 2017 roku (tab.) wyniosła około 16,5 tys. (około 14,7 tys. – wojska lądowe, około 0,7 tys. – marynarka wojenna i około 1,1 tys. – siły powietrzne).

W grudniu 2015 roku litewskie Ministerstwo Obrony Narodowej podjęło decyzję o wyborze dla wojsk lądowych nowego kołowego bojowego wozu piechoty. Zdecydowano się na niemiecki pojazd Boxer. Jest on wyposażony w wieżę z armatą kalibru 30 mm i przeciwpancerny pocisk kierowany Spike. Boxer został wybrany spośród 12 nadesłanych zagranicznych ofert. Wśród nich znalazły się m.in.: KTO Rosomak, Pirania oraz Stryker. Kontrakt na zakup 88 sztuk (dla dwóch batalionów zmechanizowanych) tego typu pojazdów został podpisany w czerwcu 2016 roku. Pierwsze dostawy rozpoczęły się w roku 2017, a zakończą w 2021. Litwa stała się trzecim użytkownikiem tych pojazdów po wojskach lądowych RFN i Holandii.

Jeszcze w 2015 roku Litwa zakupiła od Bundeswehry 21 haubic PzH 2000 (za 16,2 mln euro) oraz nabyła polskie zestawy przeciwlotnicze Grom i amerykańskie przeciwpancerne pociski kierowane Javelin (174 wyrzutni i 220 pocisków za 28 mln USD). Pod koniec 2016 roku litewskie MON podpisało także kontrakt na dostawę 340 pięciotonowych pojazdów ciężarowych typu Unimog (za 60 mln euro). Ich dostawa ma się zakończyć w 2021 roku. Litwa kupiła również pakiet kilkuset używanych pojazdów różnych typów od holenderskich sił zbrojnych. W 2016 roku zakupiono od Norwegów dwie baterie obrony powietrznej NASAMS za 100 mln euro oraz 168 pojazdów wsparcia M577 od Niemców za 1,6 mln euro. W 2016 roku Litwa przeznaczyła na zakup uzbrojenia i sprzętu wojskowego około 28% budżetu obronnego, co pod względem procentowym uplasowało ją na pierwszym miejscu w NATO. Natomiast w roku 2017 wydano jeszcze więcej, bo aż 32% budżetu wojskowego, co jest jednym z trzech najlepszych wyników w Sojuszu.

Litwa od początku istnienia (1991 rok), mimo niezbyt licznej armii, była dość aktywna na arenie międzynarodowej (NATO, ONZ, Unia Europejska). W przeszłości wysyłała swoich żołnierzy w ramach kontyngentów wojskowych do: Bośni i Hercegowiny, Chorwacji, Kosowa, Iraku, Afganistanu, Mali i na Somalię.

Obecnie Litwini uczestniczą w takich przedsięwzięciach NATO i Unii Europejskiej, jak:

– Siły Odpowiedzi NATO (NATO Response Force – NRF),

– Grupa Bojowa Unii Europejskiej (European Union Battle Group – EU BG),

– Połączone Siły Bardzo Wysokiej Gotowości (Very High Readiness Joint Task Forces – VJTF);

– Połączona Międzynarodowa Grupa Szkoleniowa na Ukrainie (Joint Multinational Training Group-Ukraine – JMTG-U),

– Misja Operacyjnego Zdecydowanego Wsparcia (Operation Resolute Support Mission – ORSM),

– Wzmocniona Wysunięta Obecność NATO (Enchanced Forward Presence – eFP).

Ponad 700 litewskich żołnierzy będzie w 2019 roku pełnić dyżur w ramach struktur Sił Odpowiedzi NATO i grup bojowych Unii Europejskiej.

W ramach Wzmocnionej Wysuniętej Obecności NATO od czerwca 2017 roku na terytorium Litwy przebywa Batalionowa Grupa Bojowa (BGB) NATO, która jest podporządkowana dowódcy brygady Żelazny Wilk. W jej skład wchodzą:

– dowództwo BGB (około 50 żołnierzy);

– niemiecka kompania zmechanizowana wzmocniona pododdziałami rodzajów wojsk (20 bojowych gąsienicowych wozów piechoty Marder, pięć czołgów Leopard 2A6, sześć haubicoarmat PzH 2000, około 30 innych pojazdów i około 450 żołnierzy);

– holenderska wzmocniona kompania zmechanizowana (czołgi Leopard 2A5, bojowe kołowe wozy piechoty Boxer, bojowe gąsienicowe wozy piechoty CV90, bojowe kołowe wozy rozpoznawcze Fennek, około 30 innych pojazdów i około 270 żołnierzy);

– norweska kompania zmechanizowana (dziewięć czołgów Leopard 2A5, dziewięć bojowych gąsienicowych wozów piechoty CV90 i około 250 żołnierzy);

– francuska kompania zmechanizowana (czołgi Leclerc, bojowe wozy piechoty i około 300 żołnierzy);

– czeska kompania zmechanizowana (bojowe wozy piechoty i około 250 żołnierzy);

– chorwacka kompania zmechanizowana (bojowe wozy piechoty i około 220 żołnierzy);

– belgijska kompania logistyczna (pojazdy zabezpieczenia logistycznego i medycznego oraz około 120 żołnierzy);

– pododdział logistyczny z Luksemburga (pojazdy zabezpieczenia logistycznego i medycznego oraz około 30 żołnierzy). Pododdział ten funkcjonuje w składzie kompanii belgijskiej.

Litwa stale zabiega o sukcesywne zwiększanie natowskiej obecności na swoim terytorium i o pozyskiwanie jak największej ilości środków finansowych z amerykańskiego programu o nazwie European Reassurance Initiative (ERI). Jej siły zbrojne aktywnie uczestniczą również w litewsko-polsko-ukraińskiej brygadzie (LITPOLUKRBRIG). Składa się ona

TABELA. LICZBA ŻOŁNIERZY W LITEWSKICH WOJSKACH LĄDOWYCH W LATACH 2014–2019

Żołnierze	2014	2015	2016	2017	2019
Służby zasadniczej	0	około 2400	około 2400	około 3000	około 4000
Zawodowi	około 3650	około 3700	około 4900	około 6100	około 7200
Czynna rezerwa (obrona terytorialna)	około 5950	około 5600	około 5600	około 5600	około 6500
Razem	**około 9600**	**około 11 700**	**około 12 400**	**około 14 700**	**około 18 200**

Opracowanie własne.

US ARMY

W 2018 roku żołnierze państw bałtyckich (w tym Litwy) wzięli udział w następujących ćwiczeniach prowadzonych na terytorium naszego kraju: dowódczo-sztabowych wspomaganych komputerowo „Bóbr" oraz taktycznych z wojskami: „Borsuk, „Karakal", „Puma" i „Saber Strike".

z Dowództwa Wielonarodowej Brygady rozmieszczonego w Lublinie i afiliowanych pododdziałów z trzech państw członkowskich. Działania ich służą osiągnięciu następujących celów: wspieranie starań Ukrainy w jej integracji z Sojuszem Północnoatlantyckim; zacieśnianie trójstronnej współpracy wojskowej; stworzenie podstaw do utworzenia w nieodległej przyszłości na bazie międzynarodowej brygady kolejnej grupy bojowej Unii Europejskiej.

Litewskie wojska lądowe bardzo aktywnie uczestniczą również w ćwiczeniach międzynarodowych i to zarówno w tych prowadzonych na terytorium swojego kraju, jak i poza jego granicami. Do najważniejszych przeprowadzonych na terytorium Litwy w 2017 roku należy zaliczyć: „Iron Wolf", „Saber Strike", „Flaming Thunder" i „Hunter". Brali w nich udział również żołnierze z: USA, Wielkiej Brytanii, Kanady, RFN, Łotwy, Czech, Danii, Polski, Gruzji, Estonii, Luksemburga, Francji, Armenii, Azerbejdżanu, Rumunii, Bułgarii i Norwegii. Do najważniejszych ćwiczeń, w których uczestniczyli litewscy żołnierze za granicą swojego państwa w 2017 roku, można zaliczyć: „Trident Jaguar" (Wielka Brytania); „Arcade Fusion" (Wielka Brytania); „Gungnir" (Łotwa); SIL-17 (Estonia); „Yellow Knight" (Dania); „Red Knight" (Dania); „Saber Junction" (amerykański poligon Hohenfels na terytorium RFN). W 2019 roku pakiet ćwiczeń będzie większy. Litewscy żołnierze byli również obecni na ćwiczeniach „Anakonda '18". Wydzielili do nich kompanię piechoty zmotoryzowanej, pluton do rozbrajania ładunków wybuchowych (Explosive Ordnance Disposal – EOD) i pododdział obrony przeciwchemicznej.

MARYNARKA WOJENNA

Jej główne zadania to: kontrola, ochrona i obrona wód terytorialnych i wyłącznej strefy ekonomicznej Litwy; zapewnienie bezpiecznej nawigacji litewskim statkom handlowym i okrętom wojennym; kontrola i ochrona podejścia do portu w Kłajpedzie oraz udział w misjach poszukiwawczo-ratowniczych. W skład litewskiej marynarki wojennej wchodzą trzy eskadry okrętów: niszczycieli min (pięć jednostek), okrętów patrolowych (pięć jednostek) i okrętów pomocniczych (cztery jednostki).

Eskadra niszczycieli min to:

– dwa niszczyciele min (typ 331) M51, M52 SULDUVIS zakupione w RFN;

– dwa niszczyciele min klasy Hunt: M53 Skalvis i M54 Kursis zakupione od Wielkiej Brytanii;

– okręt dowodzenia N42 Jotvingis (typ Vidar) zakupiony w Norwegii.

W skład *eskadry okrętów patrolowych* wchodzą:

– dwie łodzie patrolowe klasy Storm: P32 Selis, P33 Skalvis pozyskane od Norwegów;

– trzy łodzie patrolowe typu Flyvefisken: P11 Zemaitis, P12 Dzukas, P14 Aukstaitis, kupione w Danii.

Eskadra okrętów pomocniczych składa się z okrętu poszukiwawczo-ratowniczego (produkcji radzieckiej) i trzech kutrów portowych: H21, H22, H23.

W drugiej połowie 2016 roku do dyżuru bojowego w NRF wydzielono niszczyciel min Skalvis.

SIŁY POWIETRZNE I SIŁY SPECJALNE

Do ich głównych zadań należy: prowadzenie obserwacji oraz ochrona i obrona przestrzeni powietrznej państwa; wspieranie litewskich wojsk lądowych i marynarki wojennej; prowadzenie operacji poszukiwawczo-ratowniczych oraz specjalnych; przewożenie ładunków i personelu. Litewskie lotnictwo zapewnia też wsparcie dla jednostek NATO i UE w trakcie trwania misji NATO Baltic Air Policing.

Litwini mają bazę lotnictwa w Szawlach i tu właśnie stacjonują kontyngenty misji NATO Baltic Air Policing. Do tego dochodzą jeszcze dwie bazy ratownictwa w Kownie i w Nemirseta (okolice Kłajpedy). W skład litewskiego lotnictwa wchodzi także Dywizjon Obrony Powietrznej oraz Centrum Kontroli i Nadzoru Przestrzeni Powietrznej. Litwini nie mają, niestety, własnego lotnictwa bojowego, dlatego ich przestrzeń powietrzną chronią sojusznicy z państw NATO. Trzon ich lotnictwa stanowią samoloty transportowe i śmigłowce (Mi-8). Aby chociaż częściowo poprawić ten stan rzeczy, w 2015 roku Litwini zdecydowali się na zakup trzech śmigłowców Eurocopter AS365 Dauphin. Zastąpią one wysłużone już Mi-8.

W WYNIKU PRZYWRÓCENIA ZASADNICZEJ SŁUŻBY WOJSKOWEJ LICZEBNOŚĆ LITEWSKICH SIŁ ZBROJNYCH NA KONIEC 2017 ROKU WYNIOSŁA OKOŁO 16,5 TYS.

Wojska specjalne składają się z Batalionu Jegrów, jednostek antyterrorystycznych oraz morskich jednostek specjalnych. Wszystkie podlegają bezpośrednio ministrowi obrony narodowej.

DALSZA MODERNIZACJA

W kolejnych latach (2022–2028) planuje się położyć większy nacisk przede wszystkim na modernizację techniczną marynarki wojennej i sił powietrznych. Daje się zauważyć, że pod względem zakupów uzbrojenia i sprzętu wojskowego strategicznym partnerem dla Litwy w Europie jest Republika Federalna Niemiec, która jednocześnie jest uznawana przez litewskich polityków za politycznego lidera w Europie i gwaranta pokojowej stabilności. Według Litwinów takie postrzeganie RFN wynika przede wszystkim z ich potencjału gospodarczego oraz odgrywania dominującej roli w relacjach zarówno z państwami NATO, Unii Europejskiej, jak i Federacją Rosyjską. Mimo jasnego określenia partnera strategicznego, Litwini uznali, że nie zwalnia to ich z inwestycji w armię, nawet jeśli atak przeciwnika powstrzymaliby jedynie na kilkadziesiąt godzin, może kilka dni. Te dni (godziny) dadzą czas innym państwom NATO na skierowanie w ten region swoich sił. Litwini doskonale zdają sobie z tego sprawę i stąd ich plany zwiększenia wydatków na obronność.

WSPÓŁPRACA

Wspólne przedsięwzięcia szkoleniowe naszych sił zbrojnych z jednostkami sił zbrojnych Litwy trwają już kilka lat. Nasze pododdziały wojsk lądowych w 2016 roku były obecne na ćwiczeniach taktycznych z wojskami „Saber Strike" (Litwa, Łotwa, Estonia), „Strong Hussar" (Litwa) czy „Iron Sword" (Litwa). W 2017 roku w państwach bałtyckich prowadziliśmy rotacyjną obecność pododdziałów w ramach państw Grupy Wyszehradzkiej V4 (Polska, Węgry, Czechy, Słowacja). Od połowy 2017 roku 15 Brygada Zmechanizowana współpracuje z litewską brygadą Żelazny Wilk, głównie w ramach Wzmocnionej Wysuniętej Obecności NATO (Enhanced Forward Presence – eFP). Pododdziały rozpoznawcze i walki elektronicznej cyklicznie uczestniczą w takich przedsięwzięciach szkoleniowych, jak: zawody drużyn rozpoznawczych Admiral Pitka Recon Challenge i Utria Assault oraz ćwiczeniach taktycznych „Spring Storm".

Pododdziały inżynieryjne współpracują ze swoimi odpowiednikami z państw bałtyckich (w tym z Litwą), głównie w ramach Transatlantyckiej Inicjatywy Wzmocnienia Zdolności i Szkolenia (Transatlantic Capability Enhancement and Training Initiative – TACET). Inicjatywa ta jest pochodną ustaleń ze szczytu NATO w Newport i stanowi jedną z form aktywności Sojuszu w ramach *Planu podniesienia poziomu gotowości Sojuszu* (Readiness Action Plan – RAP). Działalność ta jest ukierunkowana przede wszystkim na: koordynację szkolenia wojsk inżynieryjnych; udział w narodowych i międzynarodowych ćwiczeniach taktycznych z wojskami; wymianę doświadczeń szkoleniowych oraz zwiększenie interoperacyjności i zdolności wojsk inżynieryjnych.

W ramach przedsięwzięć szkoleniowych zrealizowanych w 2017 roku litewska grupa do rozbrajania ładunków wybuchowych (Explosive Ordnance Disposal – EOD) uczestniczyła w ćwiczeniach taktycznych z wojskami „Dragon", gdzie razem z polską EOD (z 1 psap) utworzyła na potrzeby ćwiczeń zespół CBRN EOD (Chemical, Biological, Radiological & Nuclear Explosive Ordnance Disposal).

Utrzymywane są też doraźne kontakty służbowe z przedstawicielami wojsk inżynieryjnych państw bałtyckich w ramach grup roboczych funkcjonujących w obszarze inżynierii wojskowej organizowanych przez NATO.

W 2018 roku żołnierze państw bałtyckich (w tym Litwy) wzięli udział w następujących ćwiczeniach prowadzonych na terytorium naszego kraju: dowódczo-sztabowych wspomaganych komputerowo „Bóbr" oraz taktycznych z wojskami: „Borsuk, „Karakal", „Puma" i „Saber Strike".

Z kolei nasze pododdziały wojsk lądowych brały udział w następujących ćwiczeniach na Litwie: „Flaming Thunder" i „Maple Arch", a siły powietrzne w ćwiczeniach taktycznych „Hedgehog" oraz „Baltops". Wydzielone siły morskie państw bałtyckich, w tym i Litwy, uczestniczyły w ćwiczeniach „Open Spirit". Jest to międzynarodowe przedsięwzięcie szkoleniowe polegające na oczyszczaniu akwenów wodnych z przedmiotów wybuchowych i niebezpiecznych pochodzących najczęściej z okresu II wojny światowej (Historical Ordnance Disposal Operation – HODO). Ćwiczenia odbywają się cyklicznie na wodach przybrzeżnych Litwy, Łotwy i Estonii, i biorą w nich udział siły przeciwminowe. Państwa bałtyckie uczestniczą również w ćwiczeniach międzynarodowych, takich jak: „Baltops", „Saber Strike" czy „Northern Coasts".

Przedstawiciele Marynarki Wojennej RP i marynarek wojennych państw bałtyckich biorą udział

w cyklicznych spotkaniach w ramach europejskich konferencji oficerów odpowiedzialnych za planowanie działań różnych elementów europejskiej floty (European Fleet Programmers Meetings – EFMP) oraz w inicjatywie zawiązanej przez dowódców sił morskich akwenu Morza Bałtyckiego w zakresie planowania i organizowania ćwiczeń oraz szkolenia (Baltic Commanders Conference Exercise and Training Working Group – BCC WG 2).

Wymieniane są również informacje o sytuacji operacyjnej w obszarach morskich w ramach systemów:

– współpracy w zakresie nadzoru morskiego Morza Bałtyckiego (Sea Surveillance Co-operation Baltic Sea – SUCBAS). W przedsięwzięciu tym uczestniczy osiem krajów akwenu Morza Bałtyckiego, w tym Polska, państwa bałtyckie oraz Wielka Brytania;

– morskiej sieci wymiany informacji w zakresie bezpieczeństwa i ochrony (Maritime Surveillance Networking – MARSUR).

MWRP wzięła również udział w ćwiczeniach taktycznych „Open Spirit' 18". Zostały one zorganizowane w granicach wód terytorialnych państw bałtyckich.

W związku z uzyskaniem w 2014 roku statusu państwa ramowego w zakresie dowodzenia sojuszniczymi operacjami specjalnymi do dowodzenia operacjami specjalnymi Sojuszu w konflikcie o małej skali (Special Operations Forces Special Operations Component Command Smaller Joint Operations – SOF-SOCC-SJO) nasz kraj, mający tego typu zdolności, stał się naturalnym liderem w regionie państw bałtyckich.

Jesteśmy postrzegani jako ci, którzy są zdolni koordynować wysiłki państw regionu i tym samym osiągnąć efekt synergii w obszarze działania wojsk specjalnych na wschodniej flance NATO. Wyrazem takiego podejścia jest zapraszanie naszego dowódcy Komponentu Wojsk Specjalnych do udziału w organizowanym cyklicznie dwa razy do roku przez dowódców SOF Litwy, Łotwy i Estonii przedsięwzięciu 3B + POL SOF Commanders' Meeting. Ostatnie spotkania odbywały się od 30 maja do 1 czerwca 2017 roku na Łotwie oraz od 22 do 25 października tegoż roku w Estonii.

PROPOZYCJE

Ze względu na specyfikę środowiska bezpieczeństwa regionu Europy Środkowo-Wschodniej oraz różne inicjatywy rozwoju wspólnych projektów obronnych należy dążyć do zacieśniania współpracy regionalnej w każdym aspekcie militarnym. Zwiększenie przez Litwę aktywności w międzynarodowych przedsięwzięciach szkoleniowych i w ćwiczeniach organizowanych zarówno na terenie własnego kraju, jak i poza jego granicami, pozwala z optymizmem patrzeć na najbliższą przyszłość. Inicjatywy, zarówno Rotacyjnej Obecności Szkoleniowej w ramach NATO Assurance Measures, jak i zaznaczenie swojej obecności sił zbrojnych państw Grupy Wyszehradzkiej V4 w państwach bałtyckich, połączone z udziałem w ćwiczeniach taktycznych z wojskami, pokazały zdolność kolektywnego działania naszego kraju i V4 na rzecz bezpieczeństwa w regionie. Inicjatywy te wyprzedziły nawet natowską obecność w państwach bałtyckich w ramach Wysuniętej Wzmocnionej Obecności NATO (eFP) w państwach bałtyckich.

Zagrożenia wystąpieniem incydentu CBRN powodują, że nawiązanie i zacieśnienie współpracy w obszarze obrony przed bronią masowego rażenia (OPBMR) z państwami bałtyckimi (w tym z Litwą) byłoby jak najbardziej zasadne. Szczególnie pożądana byłaby współpraca związana z wymianą informacji o zagrożeniach CBRN w regionach transgranicznych w ramach systemu wykrywania skażeń.

Chcąc podnieść rangę naszego kraju jako państwa wiodącego w obszarze OPBMR w Europie Środkowo-Wschodniej, wskazane byłoby zaproszenie państw bałtyckich (w tym Litwy) do udziału w Inicjatywie Smart Defence (SD) Tier 1.29 – *Wspólne zdolności OPBMR* (Pooling CBRN Capabilities). Projekt ten jest platformą do rozwijania współpracy międzynarodowej państw regionu Europy Środkowo-Wschodniej. Obecne zagrożenia powodują, że jej nawiązanie i zacieśnienie z państwami bałtyckimi (w tym i z Litwą) w obszarze inżynierii wojskowej, w tym szczególnie w zakresie EOD oraz C-IED, byłoby zasadne.

Litwa i Estonia mają rozwinięte elementy rozpoznawcze, które mogą dostarczać wiarygodnych informacji, np. na temat aktywności wojsk Federacji Rosyjskiej w rejonie Kaliningradu i Białorusi, dlatego też współdziałanie w tej dziedzinie jest bardzo pożądane. Dodatkowo należy kontynuować współpracę szkoleniową z litewskimi wojskami specjalnymi, ukierunkowaną na prowadzenie działań głębokich (Deep Actions DA), ze szczególnym uwzględnieniem terenów przygranicznych oraz zagrożeń z rejonu obwodu kaliningradzkiego. Trzeba też w dalszym ciągu rozwijać współpracę odnoszącą się do ćwiczeń skupionych na niekonwencjonalnej walce (Unconventional Warfare – UW), wykorzystując do tego doświadczenia litewskie i łotewskie oraz możliwości szkolenia pododdziałów naszych wojsk specjalnych na terenie Litwy i Łotwy.

Czynnikami spowalniającymi tempo i zakres współdziałania z państwami bałtyckimi są przede wszystkim ograniczenia infrastrukturalne i logistyczne (ograniczona pojemność koszarowa, żywieniowa, mps, remontowa itp.) oraz zbyt mała baza szkoleniowa (zarówno garnizonowa, jak i poligonowa). Trzeba jednak obiektywnie powiedzieć, że państwom bałtyckim zależy na stałym rozszerzaniu współpracy i zostały w nich uruchomione środki finansowe na rozbudowę infrastruktury i to zarówno tej socjalnej, jak i szkoleniowej. ■

Nowy standard w nawigacji

NOWOCZESNE, TO ZNACZY PRECYZYJNE OKREŚLANIE POŁOŻENIA STATKÓW (OKRĘTÓW) NA MORZU POLEGA DZISIAJ NIE TYLKO NA UŻYCIU NIEZAWODNYCH ELEKTRONICZNYCH URZĄDZEŃ DO TEGO SŁUŻĄCYCH CZY BARDZO DOKŁADNYCH MAP, LECZ RÓWNIEŻ SPECJALISTYCZNEGO OPROGRAMOWANIA KOMPUTEROWEGO.

Przemysław Miller

Autor jest członkiem General News Service Network Association Inc. European News Agency/ General News Service.

Niezwykle dynamiczny rozwój technologiczny przełomu XX i XXI wieku nie ominął również morskich i śródlądowych systemów przeznaczonych do określania położenia obiektów pływających. Klasyczna nawigacja oparta na systemach skomplikowanych namierników, przenośników, trójkątów, cyrkli i wiecznie łamiących się ołówków przechodzi do lamusa. Przysłowiowego konia z rzędem temu nawigatorowi, który dziś posługuje się sekstansem i przy specjalnym stoliku kreśli kurs statku. Elektronika nawigacyjna w postaci konsoli GPS, radaru ARPA i innych tego typu urządzeń bezpowrotnie wyparła wymienione przedmioty. Każde z tych elektronicznych urządzeń oferuje operatorowi kompleksowe dane ułatwiające bezpieczną żeglugę oraz planowanie operacji morskich w dowolnym miejscu naszej planety. Standardem wyposażenia elektronicznego nie tylko dużych okrętów, lecz również i małych jednostek stały się plotery nawigacyjne wyświetlające zagregowane dane na zaimplementowanej mapie nawigacyjnej.

Sprzęgnięcie narzędzi nawigacyjnych w jeden system umożliwia specjalistyczne oprogramowanie pozwalające na wyświetlenie położenia jednostki pływającej na mapie elektronicznej. Ułatwia ono podejmo-

ESA/DAVID DUCROS

GPS NAVSTAR

System obejmuje swoim zasięgiem całą kulę ziemską. Jest jednym z najważniejszych elementów zapewniających precyzję odczytu pozycji przez współpracującego z nim nawigatora.

wanie decyzji związanych z bezpieczeństwem żeglugi dzięki prezentacji nie tylko podstawowych danych o nautycznej sytuacji własnej, takich jak: kierunek wiatru, kurs, prędkość i pozycja, lecz także o ruchu innych jednostek znajdujących się w sąsiedztwie. Wszystkie dane są wyświetlane na tle głównej mapy nawigacyjnej. Dzisiejsze programy komputerowe zapewniają użytkownikowi możliwość zobrazowania elektronicznych map nautycznych zbudowanych w formacie: C-Map, S-57, QV Navigator, Maptech, GeoTIFF oraz rastrowych BSB. Aby zaprezentować w czasie rzeczywistym pełną sytuację wokół danej jednostki, programy te zostały przystosowane do obsługi wszystkich podstawowych elektronicznych urządzeń nawigacyjnych, które pracują według standardu NMEA0183, takich jak: GPS NAVSTAR, AIS, radar ARPA, echosonda, żyroskop i wiatromierz.

Dzisiejsza popularność komputerów, w szczególności laptopów i tabletów, sprawiła, że wykonanie klasycznych zadań i czynności nawigacyjnych w połączeniu z szeroko rozumianą ochroną okrętu przed kolizjami może stać się jeszcze łatwiejsze. Ogromna moc obliczeniowa, prawie nieograniczona dostępność zasobów pamięci, mobilność, energooszczędność oraz wyjątkowa prostota instalacji stawia komputery na czele dzisiejszych pomocy nawigacyjnych. Niemniej w celu pełnego wykorzystania posiadanego sprzętu, należy bezwzględnie zaopatrzyć go w specjalistyczne oprogramowanie pozwalające na właściwe zarządzanie wszystkimi pokładowymi urządzeniami nawigacyjnymi oraz prezentujące ich wskazania na zintegrowanym stanowisku dowodzenia okrętem. Do wsparcia pracy tego typu systemów zalecana jest najczęściej standardowa przeglądarka internetowa. Potrzebne jest także minimum 128 MB pamięci operacyjnej RAM, około 100 MB wolnej przestrzeni na dysku oraz kolorowy monitor przystosowany do wyświetlania kolorów w trybie 16 bitów z rozdzielczością minimum 800x600 pikseli. Ponadto systemy takie muszą mieć jeszcze zaimplementowane środowisko NET Framework, a jeżeli program instalacyjny nie wykryje go, automatycznie dokona jego instalacji. Wynika z tego, że programy takie nie należą do specjalnie wymagających i mogą dzięki temu pracować praktycznie na każdym pececie.

ZASADA DZIAŁANIA

Programy komputerowe nie zawierają map, ponieważ służą użytkownikom do obrazowania oficjalnych informacji nawigacyjnych (Electronic Chart Display and Information System – ECDIS) oraz nieoficjalnych map morskich różnych producentów, a także do prowadzenia nawigacji za ich pomocą. Większość tego typu programów bez najmniejszych problemów współpracuje ze wszystkimi najpopularniejszymi formatami map morskich – zarówno rastrowymi, jak i wektorowymi. Systemowo i domyślnie wiele z nich opiera się na przykład na mapach C-MAP Jeppesen. Ponadto mogą korzystać z następujących map morskich: Maptech, SoftChart, ETopo i GeoTIFF. Użytkowanie najnowszych technologii informatycznych zaowocowało także bardzo dobrą formą wyświetlania obrazów oraz zarządzania zasobami map zastosowanymi w tego typu oprogramowaniu, które pozwala nawigatorowi na płynne skalowanie i przesuwanie obrazu na ekranie komputera. Programy wyświetlają i interpretują mapy opracowane według najpopularniejszego systemu odniesienia WGS-84, który jest używany między innymi w GPS NAVSTAR. Płynne skalowanie map oraz ich widoczność zapewnia zazwyczaj mechanizm *scroll*. Kompleksowa obsługa map elektronicznych może odbywać się na przykład z zastosowaniem zarówno plików map zainstalowanych bezpośrednio na dysku stałym komputera, jak i za pomocą czytnika. Oprócz tego systemy takie mają wbudowany mechanizm rozpoznawania obecności map morskich oraz mechanizm poszukiwania i importu wielu innych map na dysk komputera. W odniesieniu do map wektorowych programy potrafią zwiększyć ich przejrzystość dzięki przeprowadzonej przez nawigatora parametryzacji wyświetlania informacji nawigacyjnych, które są nieistotne dla użytkownika w danej chwili.

Jednym z wielu produktów przeznaczonych dla użytkowników jest program Chart Updater, który służy do szybkiego pobierania z Internetu dostępnych map morskich pochodzących z dowolnego źródła, np. NOAA Army Corp. Program ten łączy się ze wskazanym źródłem map i sprawdza ich dostępność. Wyszukiwanie interesującej mapy odbywa się za pomocą wyszukiwarki, która lokalizuje poszukiwaną na podstawie dowolnej frazy z jej nazwy lub przez zaznaczenie na mapie podkładowej obszaru, dla którego chcemy pobrać mapy szczegółowe. W celu ułatwienia procedury program na podstawie już zainstalowanych w komputerze map sprawdza jednocześnie ich aktualizację. Gdy tylko na serwerze ich producenta pojawią się zweryfikowane pliki z naniesionymi poprawkami, system informuje o tym

OGROMNA MOC OBLICZENIOWA I PRAWIE ZASOBÓW PAMIĘCI STAWIA KOMPUTERY NA

i umożliwia automatyczne pobranie map oraz ich zainstalowanie w komputerze.

OSPRZĘT NAWIGACYJNY

W tym konkretnym rozwiązaniu technologicznym osprzęt ten nie będzie już potrzebny. W związku z tym nie trzeba zaopatrywać się w ponadstandardowy zestaw urządzeń nawigacyjnych. Za pomocą wspomnianych programów można samodzielnie prowadzić na ekranie komputera pełną klasyczną nawigację na podstawie pomiarów standardowych namierników, logów i sond oraz odczytów kompasu. Elastyczność i wszechstronność tego typu programów sprawia, że potrafią one obsługiwać każde urządzenie, które komunikuje się z otoczeniem przez port NMEA0183 (GPS NAVSTAR/DGPS, radar ARPA, AIS, echosonda, autopilot, anemometr i żyrokompas). Urządzenia te mogą być podłączone do dowolnego portu komunikacyjnego (USB, port IP lub COM) w komputerze. W celu ułatwienia właściwego przyporządkowania portu do konkretnego urządzenia system został dodatkowo wyposażony w kreator urządzeń. Umożliwia on błyskawiczne sprawdzenie wszystkich portów dostępnych w komputerze, przeprowadzenie tzw. ich nasłuchu oraz określenie możliwej prędkości transmisji z danym urządzeniem.

Jednym z najważniejszych elementów zapewniających precyzję odczytu pozycji przez nawigatora jest *współpraca z GPS NAVSTAR*. Dlatego też programy takie, oprócz wyświetlania informacji na temat: pozycji, kursu i prędkości, mają całą gamę innych dostępnych dla użytkownika parametrów, pozwalających określić między innymi poziom nadawanego z satelity sygnału (PDOP, HDOP i VDOP) oraz precyzyjnie podać jego umiejscowienie względem danej jednostki, a także – co się z tym wiąże – szacować aktualną dokładność pomiaru pozycji. W takiej sytuacji można z powodzeniem osiągnąć dokładność do 1 m. Praca programu z GPS-em jest niezwykle intuicyjna, ponieważ raz włączony odbiornik działa w systemie automatycznie. W razie wystąpienia awarii program zgłasza ten fakt po 10 s użytkownikowi w formie alarmu. Obsługa systemu GPS NAVSTAR w programach komputerowych służy do określania aktualnej pozycji, rejestracji przebytej drogi na mapie nawigacyjnej, ustalania rzeczywistej prędkości jachtu i rzeczywistego kursu, wywoływania alarmu zejścia z kursu, mierzenia tempa wykonywanego zwrotu oraz obrazowania na mapie aktualnej i prognozowanej lokalizacji jednostki.

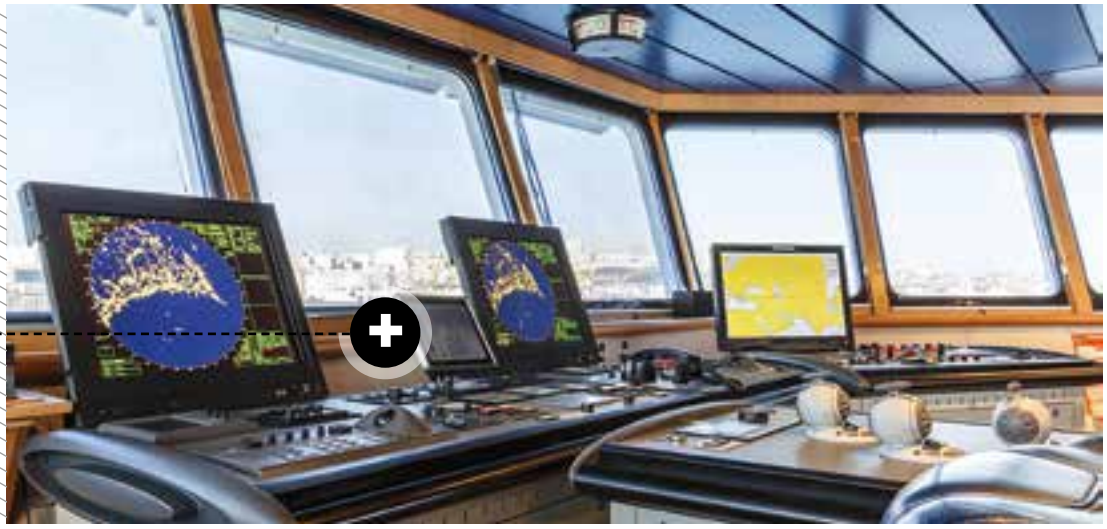
Drugim po GPS-ie podstawowym systemem, który został zintegrowany z oprogramowaniem, jest *system automatycznej identyfikacji* (Automatic Identification System – AIS). Zawiera funkcjonalność GPS NAVSTAR, a dołączony do programów typu *cruiser* dodatkowo umożliwia obrazowanie sytuacji nawigacyjnej przestrzeni wokół okrętu. Zastosowanie takiego oprogramowania pozwala nawigatorowi na obserwowanie na ekranie monitora w zaznaczonym uprzednio obszarze wokół jednostki ruchów innych statków wyposażonych w system AIS. Zapewnia to wykrycie potencjalnych kolizji z innymi jednostkami na morzu.

Każdy z programów wyświetla na ekranie monitora sylwetki innych jednostek w zróżnicowanych kolorach, oznaczając je jako bezpieczne, stanowiące potencjalne zagrożenie lub realne zagrożenie kolizją.

Uzupełnieniem AIS jest bez wątpienia możliwość wyświetlania na ekranie komputera obrazu generowanego przez *radar ARPA* (Automatic Radar Plotting – Aid). Radary te mają wbudowany komputer, który odpowiada za automatyczne prowadzenie zakresów radarowych. Urządzenia te potrafią śledzić od kilku do kilkudziesięciu obiektów, obliczając przy tym ich dokładne parametry ruchu. Wszystkie nowoczesne programy mają już wbudowane mechanizmy przystosowane do odczytu parametrów ruchu śledzonych przez radar obiektów i jednoczesnego wyświetlania ich na tle mapy nawigacyjnej. Programy te mają również wbudowane mechanizmy indeksowania równoległego.

Praca z sonarem (echosondą) polega na rzetelnym zobrazowaniu dna oraz na dokładnym pomiarze głębokości. W programie obraz zarejestrowany przez echosondę zostaje zapisany również jako dodatek do przebytej przez aparat sonarowy drogi. Istnieje zatem możliwość późniejszej analizy dna pod przebytą drogą jednostki. Dodatkowo pomiar sonarowy służy do uruchamiania alarmu płytkiej wody. Jedną z najważniejszych funkcji takiego oprogramowania jest możliwość wprowadzenia dogodnej personalizacji wyglądu ekranu roboczego. Dzięki temu nie ma żadnych ograniczeń w tworzeniu wyglądu ekranu tak, by był on zgodny z preferencjami każdego nawigatora. Specjalnie wbudowane interfejsy typu: Basic, Planning, Quad i Sail-On Water są gwarantem najwyższej jakości pracy. Każdy ekran jest zdefiniowany jako zakładka widoku, na której można w dowolny sposób

NIEOGRANICZONA DOSTĘPNOŚĆ
CZELE DZISIEJSZYCH POMOCY NAWIGACYJNYCH



Każdy z programów wyświetla na ekranie monitora sylwetki innych jednostek w zróżnicowanych kolorach, oznaczając je jako bezpieczne, stanowiące potencjalne zagrożenie lub realne zagrożenie kolizją.

ALEXMU/STOCK.ADOBE.COM

rozplanować wszystkie elementy niezbędne dla bezpiecznej żeglugi.

KONTEKSTOWE MENU

Kolejnym *novum* jest menu, które pozwala na korzystanie z różnorodnych narzędzi wyłącznie za pomocą prawego przycisku myszki. W zależności od wybranego na ekranie przez nawigatora obiektu (strefa, marker, trasa, mapa) wciśnięcie prawego jej klawisza powoduje wyświetlenie listy zawierającej wszystkie niezbędne narzędzia, które będą potrzebne w pracy z danym obiektem.

Głównym miejscem zarządzania danymi każdego z wymienionych programów jest tzw. manager, który odgrywa rolę kontrolera wszystkich zebranych i zmagazynowanych przez program informacji. Za jego pomocą można łatwo odszukać wszystkie mapy zaimplementowane do programu i zarządzać nimi oraz tymi stworzonymi przez nawigatora w trakcie jego pracy. Narzędzie to w prosty sposób umożliwia dotarcie do szukanego obiektu i ustawienie mapy w jego rejonie, dzięki czemu można również dokonać pełnej modyfikacji każdego z obiektów oraz ukrywać, ale nie usuwać, te, które w danej chwili są niepotrzebne.

W trakcie żeglugi istnieje często konieczność zaznaczenia na mapie jakiegoś ważnego punktu i opisania go. W programach komputerowych służą do tego celu tzw. markery, które znajdują się w pasku narzędzi nawigacyjnych. Dzieli się je na markery swobodne i markery pozycji jednostki.

Użycie *markera swobodnego* powoduje zmianę wyglądu kursora – zamiast strzałki pokazuje się wtedy ikonka markera wraz z jego tymczasową nazwą. Natomiast wybór narzędzia *marker pozycji jednostki* powoduje ustawienie nowego markera w miejscu aktualnej pozycji danej jednostki. Każdy marker ma domyślnie ustawioną nazwę oraz przypisane mu współrzędne geograficzne. Wszystkie programy komputerowe zostały wyposażone także w specjalny marker MOB, dzięki któremu podczas alarmu „człowiek za burtą" nawigator może skorzystać ze specjalnego przycisku. Wtedy na mapie nawigacyjnej zostaje ustawiony specjalny marker, którego nie można przesunąć, zmienić ani skasować. Od momentu jego ustawienia do czasu zakończenia alarmu program będzie automatycznie podawał namiar na pozycję rozbitka oraz dokładną odległość do niego.

Ostatnim ważnym rodzajem markera specjalnego jest *marker dowolnej pozycji* o charakterze stricte pozycyjnym. Ustawia się go wówczas, gdy nawigator chce odnaleźć i oznaczyć pozycję na przykład proszącego o pomoc innego statku o znanych współrzędnych geograficznych.

Kreator stref – to kolejne niezwykle przydatne narzędzie w pracy nawigatora. Służy do wykreślania na morskiej mapie stref użytkownika. Mogą to być strefa specjalnych akwenów zamkniętych lub strefa zasięgu kotwicy. Do ich wyznaczania służy przyjazne i wygodne narzędzie, które znajduje się w pasku narzędzi nawigacyjnych. Przekroczenie wyznaczonych granic stref spowoduje natychmiastowe uaktywnienie alarmu dźwiękowego, gdy jednostka znajdzie się na ich krawędzi, wejdzie w ich obszar lub opuści je.

PARAMETRYZACJA

Programy komputerowe zostały zaprojektowane tak, by każdy z ich użytkowników mógł ustawić prezentację wyświetlanych wartości zgodnie z poziomem swojej wiedzy, przyzwyczajeniami i znanym systemem miar. Nawigator może dzięki temu dostosować do swoich potrzeb praktycznie wszystkie parametry prezentacji danych. Do dyspozycji użytkownika oddano nie tylko ustawienia kolorystyczne, jednostki miar, parametry jednostki, precyzję i dokładność pomiarów czy ustawienia alarmów, lecz także zasięgi radarów i filtry AIS. ■

BEZPIECZEŃSTWO

O SUWERENNOŚCI POWIETRZNEJ

JEŚLI BEZPIECZEŃSTWO NARODOWE ROZUMIEMY JAKO STAN OSIĄGNIĘTY W REZULTACIE ODPOWIEDNIO ZORGANIZOWANEJ OBRONY I OCHRONY PRZED WSZELKIMI ZAGROŻENIAMI MILITARNYMI I POZAMILITARNYMI Z UŻYCIEM SIŁ I ŚRODKÓW POCHODZĄCYCH Z RÓŻNYCH SFER DZIAŁALNOŚCI PAŃSTWA, TO MUSIMY RÓWNIEŻ UWZGLĘDNIĆ PRZESTRZEŃ POWIETRZNĄ NAD NASZYM KRAJEM.

Współcześnie bezpieczeństwo coraz częściej jest porównywane do kostek domina, gdy przewrócenie jednej powoduje lawinowy upadek innych. Publikacja, którą chcę zarekomendować, dotyczy bezpieczeństwa w przestrzeni powietrznej i kosmicznej. W pierwszej części zamieszczono artykuły omawiające funkcjonowanie misji Baltic Air Policing pod kątem przygotowania sekcji bezpieczeństwa lotów do wykonywania zadań poza granicami kraju. O ruchu lotniczym w siłach zbrojnych traktuje kolejny materiał, którego autor przedstawił organizację, zadania i strukturę nowo powstałego pionu służb ruchu lotniczego. Dzięki rozwiązaniom systemowym przestrzeń powietrzna nie jest już traktowana jako cywilna lub wojskowa, lecz jako dobro narodowe. W kontekście bezpieczeństwa w lotnictwie cywilnym scharakteryzowano zagrożenia mogące doprowadzić do sytuacji kryzysowej zarówno w portach lotniczych, jak i na pokładach statków powietrznych. Warto przy tym rozważyć przeniesienie na grunt wojskowy części zaproponowanych zmian mających zapewnić bezpieczne funkcjonowanie portów lotniczych. Jak słusznie zauważono, najsłabszym ogniwem systemów bezpieczeństwa jest człowiek. Przedstawiono również zagrożenia, których źródłem są bezzałogowe systemy powietrzne. Wskazano na ich coraz częstsze stosowanie w działaniach militarnych oraz na możliwości przeciwdziałania tego rodzaju platformom użytym przez potencjalnego przeciwnika. Zamieszczone w publikacji opracowania traktują również o wpływie postępu naukowo-technicznego na współczesne konstrukcje lotnicze. Nowoczesne technologie klejenia nie tylko przyspieszają proces montażu i pozwalają na uzyskanie odpowiedniej wytrzymałości połączeń, lecz zwiększają także stopień ich szczelności, co jest szczególnie ważne dla zapewnienia bezpiecznego wykonywania lotów.

Część drugą publikacji, poświęconą bezpieczeństwu kosmicznemu, otwiera materiał dotyczący norm prawnych odnoszących się do korzystania z kosmosu przez zainteresowane państwa. Organizacja Narodów Zjednoczonych usiłuje zapobiec jego przekształceniu w arenę wyścigu zbrojeń. Jednak wiele państw niechętnie podpisuje zobowiązanie do wykorzystywania tej przestrzeni tylko w celach pokojowych. Należy jednak mieć nadzieję, że zdroworozsądkowe podejście większości z nich wymusi podporządkowanie się tych, które chcą militaryzować kosmos. By kształtować wiedzę o sytuacji w tej przestrzeni i o obiektach kosmicznych, powstały systemy śledzące, niwelujące niebezpieczeństwo ich zderzenia z Ziemią. Badane są również zjawiska związane z pogodą kosmiczną, która ma olbrzymi wpływ na życie człowieka i gospodarkę. Istotne jest także ryzyko uderzenia w powierzchnię naszej planety dużych meteoroidów lub komet, co mogłoby przynieść niewyobrażalne skutki. Właśnie w te działania międzynarodowej społeczności, zwłaszcza UE, wpisuje się aktywność naszego kraju, o czym traktuje jeden z materiałów.

Jako społeczeństwo informacyjne korzystamy z satelitów komunikacyjnych i nawigacyjnych. Jednak istnieje ryzyko ich zaatakowania. W związku z tym są opracowywane rozwiązania systemowe służące zapewnianiu ich bezpieczeństwa. Warto zapoznać się zatem z pracami na temat bezpieczeństwa globalnych systemów nawigacyjnych oraz możliwości ich zakłócania, co w dzisiejszej dobie jest bardzo istotne i nie dotyczy tylko sfery militarnej. Podsumowując, należy stwierdzić, że polecane opracowanie, mimo że zawiera wiele wątków z dziedziny bezpieczeństwa w obszarze lotniczym i kosmicznym, może stanowić przyczynek do szczegółowego zainteresowania się prezentowaną problematyką.

Życzę przyjemnej lektury. ■

Opracował JB

Bezpieczeństwo w środowisku lotniczym i kosmicznym. Red. nauk. R. Bielawski, B. Grenda. Wyd. Semper, Warszawa 2018.

Dear Readers,

for some time now, the military and academic environment have been facing the challenge to find solutions to many questions related to a growing phenomenon called a hybrid war. The main dilemmas relate mainly to the very core of such war, and the issues of what it is, how it is conducted, what is different about it, as well as what is the potential of such war, how to counteract it, etc. The key issue seems however answering a question whether or not it is a new problem, and if it is, why?

All these questions are discussed by our authors who make attempts to define the mechanisms of conduct in a hybrid war, and effective counteracting activities. There is a dominating opinion that in case of a hybrid conflict, we have to deal with a permanent and simultaneous attack within multiple areas of social functioning, which is expanding with escalation of a conflict. In their deliberations on the subjects, the authors point to two crucial stages of a hybrid war, i.e. activity below the threshold of war and open war activity. Many claim that this new kind of war is an aftermath of a developing civilization, particularly the increase in capability and activity of a human being in cyberspace.

Cyberspace affects human communication not only in the informational and propaganda aspect, but also in the economic one. It omits traditional territorial limitations, offering to its participants unlimited range of activity. Today, all essential relations between social life entities are reflected in cyberspace relationships, or they even come from there and have their source there. Therefore, ruling the infosphere gives the potential to not only create images, but also affect an actual state of things in a given area. The authors, using examples of conflicts in Georgia or Ukraine, show mechanisms applied by both parties of the conflict to achieve assumed objectives.

In this edition of The Armed Forces Review (Przegląd Sił Zbrojnych), we present the articles by the War Studies University graduates who write about hybrid activities, and the way to counteract them with the use, e.g. air-mobile and territorial defense forces.

There is also a material about organizational activities that must be undertaken by fighting troops to overcome water obstacles. The author presents the tasks of engineering forces' elements on command post of a tactical unit or a squad tasked to overcome such obstacles. He explains how important it is for the specialist of engineering forces to cooperate with other units of command posts in order for this task to be smoothly carried out.

The other two articles are on: how technological progress affects the methods of radio signal modulation and the building of modern high-frequency radio communication systems; and on the significance of the rolling bearing in the designs of mechanical vehicles – exploitation, technical condition, and the grounds for replacement of rolling bearings in vehicles.

Last but not least, there are also other articles which can be equally interesting for the Readers.

Enjoy reading!
Editorial Staff

WARUNKI ZAMIESZCZANIA PRAC

Materiały (w wersji elektronicznej) do „Przeglądu Sił Zbrojnych" prosimy przesyłać na adres: Wojskowy Instytut Wydawniczy, Aleje Jerozolimskie 97, 00-909 Warszawa lub e-mail: psz@zbrojni.pl. Opracowanie musi być podpisane imieniem i nazwiskiem z podaniem stopnia wojskowego i tytułu naukowego, a także adresu służbowego z numerem telefonu. Ponadto należy dołączyć zdjęcie z aktualnym stopniem wojskowym. Rysunki i szkice powinny być przygotowane zgodnie z wymaganiami poligrafii (najlepiej w programie Ilustrator lub Corel), zdjęcia w formacie TIFF lub JPEG w rozdzielczości 300 dpi. Autor powinien podać źródła, z których korzystał przy opracowywaniu materiału. Niezamówionych artykułów Instytut nie zwraca. Zastrzega sobie przy tym prawo do dokonywania poprawek stylistycznych oraz skracania i uzupełniania artykułów bez naruszania myśli autora. Autorzy opublikowanych prac otrzymają honoraria według obowiązujących stawek. Z chwilą wpłynięcia artykułu WIW wysyła do autora drogą elektroniczną kwestionariusz do wypełnienia. Pochodzące z niego informacje są niezbędne do wypłacenia honorarium.

W celu wywiązania się z obowiązków informacyjnych dotyczących przetwarzania danych osobowych oraz w związku ze zmianami przepisów normujących postępowanie z danymi osobowymi, w tym z obowiązku stosowania Ogólnego Rozporządzenia o Ochronie Danych Osobowych (tzw. RODO), informujemy, że ich administratorem jest Wojskowy Instytut Wydawniczy. Dane autora nie będą przetwarzane w sposób zautomatyzowany, nie będą też profilowane. Natomiast będą przechowywane przez okres niezbędny do realizacji celów związanych z przekazaniem artykułu do druku.

We wszystkich sprawach dotyczących danych osobowych Autor może się skontaktować listownie na adres: Wojskowy Instytut Wydawniczy w Warszawie, 00-909 Warszawa, Aleje Jerozolimskie 97 lub e-mail: rodo@zbrojni.pl.

POLSKA ZBROJNA

Sprawdzony tytuł. Nowa odsłona