System teleinformatyczny PMN 2.0 w służbie NATO

Bezpieczeństwo w cyberprzestrzeni

Łączność troposferyczna

PRZEGLĄD SIŁ ZBROJNYCH

Cena 14,99 zł (w tym 8% VAT)

nr 5 / 2022

wrzesień–październik

WOJSKOWY INSTYTUT WYDAWNICZY

ISSN 2353-1975

ISSN 2353-1975 05 9 772353 197201

Zamów

PRENUMERATĘ

NA 12 MIESIĘCY

roczna prenumerata „Przeglądu Sił Zbrojnych”
6 wydań za 80 zł

Prenumeratę można zamówić na

sklep.polska-zbrojna.pl

Szanowni Państwo!

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.: 261 849 007, 261 849 008
faks: 261 849 459

Redaktor naczelny:
IZABELA BORAŃSKA-CHMIELEWSKA
tel.: 261 849 212
e-mail: ibc@zbrojni.pl

Redaktor wydawniczy:
KRZYSZTOF WILEWSKI
tel.: 261 849 186

Redaktor prowadzący:
płk w st. spocz. dr JAN BRZOZOWSKI
tel.: 261 849 186

Opracowanie redakcyjne:
MARYLA JANOWSKA,
KATARZYNA KOCOŃ

Opracowanie graficzne:
WYDZIAŁ SKŁADU
KOMPUTEROWEGO I GRAFIKI WIW

Kolportaż i reklamacje:
Punkt Pocztowy Włocławek
ul. Duninowska 9a
87-823 Włocławek
elzbieta.kurlapska@poczta-polska.pl
tel. 885 870 509, kom. 502 012 187

Druk: DRUKARNIA KOLUMB
ul. Kaliny 7
41-506 Chorzów

Zdjęcie na okładce:
WB ELECTRONICS

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

Krzysztof Wilewski

Analiza konfliktów zbrojnych w XX i XXI wieku potwierdza, że sprawny system dowodzenia, niezależnie od rozpatrywanego poziomu działań, nie funkcjonuje bez niezakłócanych systemów łączności. Wraz z postępem technologicznym zwiększa się zapotrzebowanie na takie systemy przekazywania zadań w czasie zbliżonym do rzeczywistego, by można je było wykonać w określonym czasie. W ramy łączności wprzęgnięto zatem informatykę, bez której żadne stanowisko dowodzenia obecnie nie jest w stanie wypełniać swoich funkcji w zakładanych reżimach czasowych. Dlatego mamy dziś do czynienia z wojskami łączności i informatyki. To właśnie specjaliści tego rodzaju wojsk zapewniają rozwijanie systemów teleinformatycznych, które w połączeniu ze środkami łączności radiowej i radioliniowej umożliwiają dowódcom przekazywanie zarządzeń do utworzonych elementów ugrupowania bojowego oraz kierowanie środkami walki.

W kolejnym numerze „Przeglądu Sił Zbrojnych" zamieściliśmy dział poświęcony wyzwaniom, które niesie współczesna łączność wojskowa. Z pewnością nie powstałby on bez osobistego zaangażowania szefa Zarządu Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ oraz kierownika Zakładu Cyberbezpieczeństwa Wydziału Wojskowego ASzWoj, którym w tym miejscu wyrażam podziękowanie. W dziale tym opublikowaliśmy opracowanie ppłk. dr. inż. Bartłomieja Terebińskiego, w którym zaprezentował on kierunki rozwoju łączności wojskowej. Natomiast wspólnie z mjr. dypl. SZRP Piotrem Kamieńskim omówili zagrożenia systemu łączności, jakie mogą wystąpić na polu walki. Z kolei płk dr inż. Maciej Nowak określił rolę użytkownika operacyjnego w eksploatacji i rozwoju systemów informatycznych, a płk dr inż. Marcin Marek i ppłk Zbigniew Ćwik scharakteryzowali właściwości systemu informatycznego PMN 2,0. Kmdr por. Paweł Kamiński przedstawił systemy kryptograficzne w taktycznych systemach łączności. Natomiast ppłk mgr inż. Robert Kozłowski omówił wnioski z organizacji łączności radiowej KF w związku taktycznym. Jakie usługi funkcjonalne oferuje system NATO FAS to temat opracowania mjr. dr. inż. Andrzeja Bogdańskiego, sposób zaś wykorzystania taktycznych systemów transmisji danych Link wskazał ppłk. Dariusz Łuczak. O systemie monitorowania położenia wojsk własnych i przeciwnika napisał mjr Marcin Nalberczyński. Poza tym o zaletach łączności troposferycznej przekonuje w swoim artykule mjr Marek Mirowski, a radiostacji AN/PRC-150C – plut. Kamil Nowakowski.

Oprócz tego w dwumiesięczniku zamieściliśmy opracowania absolwentów Podyplomowych Studiów Operacyjno-Taktycznych Wydziału Wojskowego ASzWoj. Polecamy też artykuł płk. rez. prof. dr. hab. Marka Wrzoska o rosyjskiej wojskowej operacji specjalnej. Jestem przekonany, że opracowania, które nie zostały tutaj wymienione, również będą z uwagą przeczytane, co pogłębi znajomość wielu aspektów sztuki wojowania.

Zachęcam do lektury!

nr 5 / 2022

Spis treści

TEMAT NUMERU – WSPÓŁCZESNA ŁĄCZNOŚĆ

NAJLEPSZY ARTYKUŁ

WSPÓŁCZESNE ARMIE

DOŚWIADCZENIA

WYBITNI DOWÓDCY

UMOŻLIWIA DOWÓDCY ORAZ ORGANOM DOWODZENIA DYWIZJI WYMIANĘ DANYCH I FONU CYFROWEGO Z PRZEŁOŻONYM, JAK RÓWNIEŻ Z JEDNOSTKAMI PODLEGŁYMI I WSPÓŁDZIAŁAJĄCYMI W PASIE ODPOWIEDZIALNOŚCI OBRONNEJ TEGO ZWIĄZKU TAKTYCZNEGO. ZAPEWNIA ZDOLNOŚĆ DYWIZJI DO ROZWIJANIA I EKSPLOATOWANIA:
– SYSTEMU ŁĄCZNOŚCI BEZPRZEWODOWEJ W ZAKRESIE FAL HF/VHF/UHF W RAMACH OSIĄGANIA INTEROPERACYJNOŚCI Z SYSTEMAMI ŁĄCZNOŚCI BEZPRZEWODOWEJ EKSPLOATOWANYMI W ARMIACH INNYCH PAŃSTW NATO;
– POLOWEGO SYSTEMU TELEINFORMATYCZNEGO URUCHAMIANEGO NA STANOWISKACH DOWODZENIA.

WÓZ DOWODZENIA

NA PLATFORMIE KTO ROSOMAK

WIESŁAW JABŁOŃSKI

Łączność wojskowa – **teraźniejszość i kierunki rozwoju**

WSPÓŁCZEŚNIE INFORMACJA JEST ZASOBEM STRATEGICZNYM NIEZBĘDNYM DO PODEJMOWANIA OPTYMALNYCH DECYZJI, A DĄŻENIE DO PRZEWAGI INFORMACYJNEJ JEST WARUNKIEM POWODZENIA OPERACJI MILITARNYCH.

ppłk dr inż. Bartłomiej Terebiński

Autor jest kierownikiem Zakładu Cyberbezpieczeństwa w Wydziale Wojskowym Akademii Sztuki Wojennej.

Dowodzenie ugrupowaniem bojowym jest uzależnione od niezakłóconej wymiany informacji. Zatem już na wstępie nietrudno dojść do wniosku, że każda próba zakłócenia dowodzenia, a więc i zaburzenia właściwego funkcjonowania kanałów informacyjnych (w tym wykorzystujących techniczne środkach łączności), spowoduje reakcję łańcuchową inicjującą destabilizację procesu dowodzenia, w konsekwencji utrudniającą prowadzenie działań lub wręcz pozbawiającą możliwości ich podjęcia. Chociaż obecnie można podejmować próby eksploracji wojskowego systemu łączności w celu dokonania diagnozy jego skuteczności, trudno jednak postawić tezę dotyczącą dalszego jego rozwoju. Przede wszystkim w odniesieniu do nowych sposobów porozumiewania się ludzi na odległość w codziennym funkcjonowaniu na płaszczyźnie cywilnej, jak również w kwestii skrytej, wiernej i terminowej wymiany informacji.

ŁĄCZNOŚĆ CYWILNA A WOJSKOWA

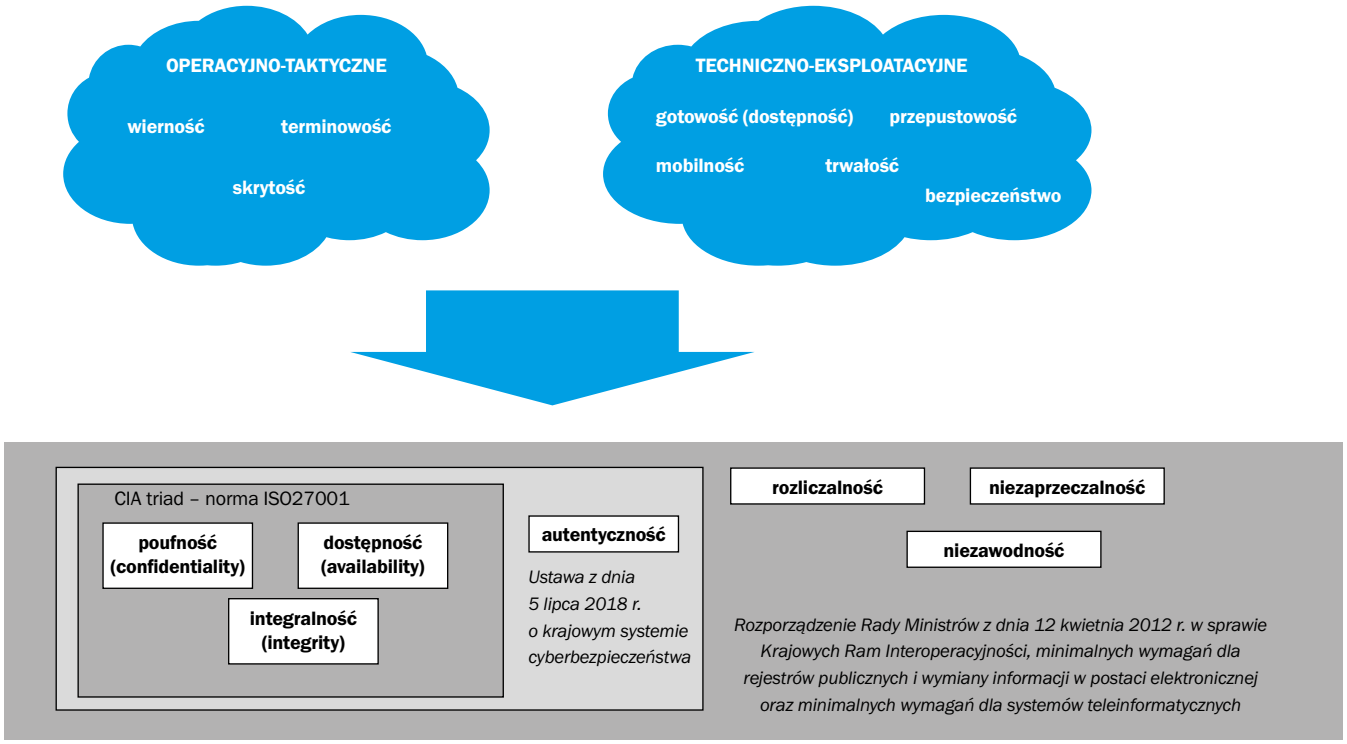
Na wstępie warto wskazać pewne fakty i zjawiska związane z łącznością w ogólnym znaczeniu, w tym z łącznością wojskową. Pojawia się zatem pytanie, czym jest łączność wojskowa i co ją odróżnia od łączności cywilnej. Łączność cywilną cechuje, oprócz wielu funkcjonalności na rzecz organizacji, instytucji, służb, urzędów itd., przede wszystkim użytek prywatny. Uogólniając, należy zauważyć, że prywatność oznacza głównie dowolność w dostępie do usług telekomunikacyjnych niezależnie od miejsca i czasu.

W dużej mierze, o czym traktuje literatura przedmiotu, skutkiem tej dowolności jest wygenerowanie od początku posługiwania się danymi w formie cyfrowej około 10 jottabajtów danych. Natomiast jeśli wziąć pod uwagę wyłącznie rok kalendarzowy, to do jego końca zostaną wytworzone w sumie 94 zettabajty danych. Można zadać pytanie, czy to dużo. Tak naprawdę odpowiedź jest niejednoznaczna.

Z jednej bowiem strony po powołaniu się na wyniki badań ekspertów[1] oraz rozpatrując to zagadnienie przez pryzmat masy elektronów, które są nośnikami informacji, można oszacować, że łączna masa wszystkich informacji zgromadzonych w wirtualnym świecie to „zaledwie" od 40 do 80 kg. Te dane szacunkowe kontrastują często z liczbą nośników danych. I tak

1 Piotr Prajsnar, ekspert ds. analityki *big data*, absolwent SGH i PJWSTK w Warszawie, CEO Cloud technologies. Źródło: https://www.forbes.pl/autorzy/piotr-prajsnar/. 20.01.2022.

RYS. 1. WYMAGANIA DOTYCZĄCE ŁĄCZNOŚCI



Opracowano na podstawie: *Regulamin działań wojsk lądowych*, DWLąd, sygn. Wewn. 115/1008. Warszawa 2008.

w przypadku, gdyby spróbować skopiować całą zawartość sieci Internet na płyty Blu-ray, okazałoby się, że po położeniu jednej na drugą zajęłyby drogę z Ziemi na Księżyc i z powrotem. Jeśli zaś spojrzeć na tę kwestią w ujęciu czasu, to znaczy ile trwałoby to kopiowanie, wskazuje się na setki milionów lat. Ten ogrom danych będzie wzrastał z roku na rok i chyba jako wojskowi nie mamy na to wpływu. Tutaj rządzą zasady komercji.

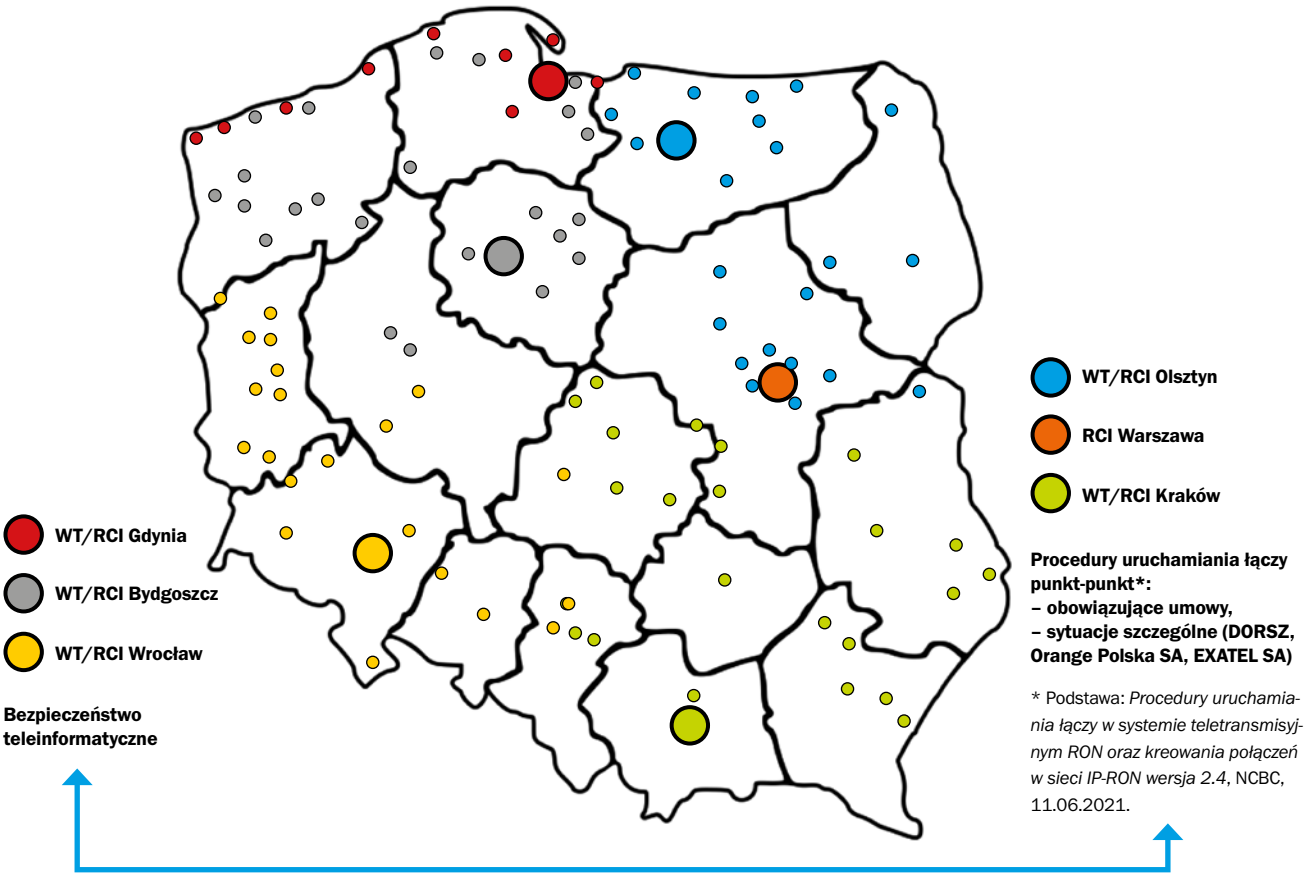
Łączność wojskowa natomiast to skuteczna wymiana informacji na potrzeby kierowania i dowodzenia siłami i środkami militarnymi. Zawężenie świadczonych usług do obszaru militarnego wyklucza przypadkowość obserwowaną u prywatnych użytkowników. Co więcej, użycie wojskowej łączności powinno mieć miejsce wyłącznie w przypadkach, gdy jest to konieczne. Tak naprawdę jednak, czy te ograniczenia powodują, że personel wojskowy przesyła wyłącznie niezbędne dane w ramach swojej działalności?

SPEŁNIĆ WYMAGANIA

Na pytanie, jaka ma być łączność w siłach zbrojnych, odpowiada się w sposób naturalny, wskazując na wymagania stawiane łączności, w domyśle mając na względzie szersze pojęcia, jakimi są *sieć łączności* czy *system łączności*. W literaturze przedmiotu można znaleźć zapisy wskazujące, że przy próbie dokonania oceny dowolnego wojskowego systemu łączności zawsze należy określić stopień zgodności jego cech charakteryzujących przedmiotowy system (i jego funkcje) z wymaganiami. Jest ich całkiem sporo (rys. 1). Jeśli dodatkowo zostaną wzięte pod uwagę atrybuty związane z bezpieczeństwem wymiany i przetwarzania informacji, to uwarunkowań i cech związanych z łącznością, w tym łącznością wojskową, jest imponująca liczba.

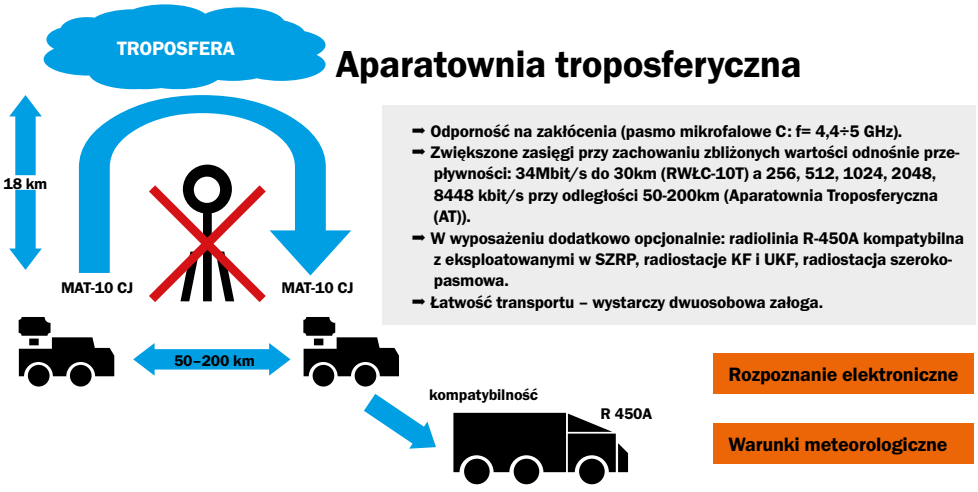
Kolejną kwestią jest fakt, że na wojskowy system łączności, który zdecydowanie można zaliczyć do systemu typu otwartego, oddziałuje jego otoczenie. Zatem tak jak działania prowadzone przez zgrupowania zadaniowe zawsze są konfrontowane z potencjalnym przeciwnikiem, tak samo funkcjonowanie wojskowego systemu łączności warto zestawiać przede wszystkim z destrukcyjnym oddziaływaniem strony przeciwnej, w tym środków walki elektronicznej, jak również z niekorzystnymi warunkami propagacyjnymi, klimatycznymi czy ukształtowaniem terenu. W związku z tym sposób organizacji wojskowej łączności zawsze będzie kształtowany przez wskazane czynniki. W odniesieniu do wyma-

RYS. 2. WOJSKOWY STACJONARNY SYSTEM ŁĄCZNOŚCI



Opracowanie własne.

RYS. 3. ŁĄCZNOŚĆ TROPOSFERYCZNA



Źródło: B. Terebiński, *Stanowisko dowodzenia poziomu taktycznego* [w:] *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*, red. B. Biernacik, G. Pilarski, L. Kalman, ASzWoj, Warszawa 2018, s. 43; http://www.zdz.krakow.pl/index.php/produkcja-krakow/mobilna-aparatownia-troposferyczna/. 20.01.2022.

gań regulaminowych z jednej strony wskazuje się na te dotyczące skrytości łączności. Biorąc jednak pod uwagę wzrastające nasycenie środkami emitującymi falę elektromagnetyczną nie tylko na stanowiskach dowodzenia, można dojść do wniosku, że ukrycie wojsk staje się po prostu niemożliwe. Powstaje zatem pytanie, czy naprawdę potrzebujemy tak dużo urządzeń łączności.

ŁĄCZNOŚĆ STACJONARNA

Na terenie naszego kraju jest około stu zasadniczych wojskowych punktów dostępowych do usług świadczonych przez Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni[2] (rys. 2). Można pokusić się o stwierdzenie, że stanowią one elementy zintegrowanej infrastruktury teleinformatycznej segmentu stacjonarnego resortu obrony narodowej. Co więcej, prowadzone analizy wskazują na fakt, że ich liczba jest wystarczająca w czasie bieżącej działalności naszych sił zbrojnych oraz podczas ćwiczeń. Powstaje natomiast zasadnicze pytanie, co w zamian za wojskowy system telekomunikacyjny w przypadku jego obezwładnienia czy zniszczenia. Warto przy tym zaznaczyć, że lokalizacje poszczególnych węzłów teleinformatycznych lub regionalnych centrów informatyki można odnaleźć w sieci Internet w ramach białego wywiadu.

Wojskowy system telekomunikacyjny może być na mocy obowiązującego w naszym kraju prawa wzmacniany elementami infrastruktury przedsiębiorców telekomunikacyjnych. W tym względzie szczególne znaczenie mają zasady organizowania zadań na rzecz obronności państwa realizowanych przez przedsiębiorców wykonujących działalność gospodarczą na terytorium RP oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym. Wskazanych przedsiębiorców charakteryzuje to, że teren ich działania musi obejmować więcej niż jedno województwo, a przedmiotem działalności są obiekty i sektory ważne dla bezpieczeństwa państwa (np.: lotniska, porty morskie, kolportaż, media, produkty naftowe, uzbrojenie i sprzęt wojskowy, obrót specjalny, transport, poczta, telekomunikacja, gaz ziemny, paliwa, energia elektryczna). Wykaz przedsiębiorców telekomunikacyjnych o szczególnym znaczeniu gospodarczo-obronnym, których przedmiotem wykonywanej działalności gospodarczej jest telekomunikacja, obejmuje w sumie 12 przedsiębiorstw nadzorowanych przez ministrów właściwych do spraw informatyzacji, łączności, aktywów państwowych i transportu oraz przez ministra obrony narodowej[3].

Niemniej powstaje podobne do zadanego wcześniej pytanie, czym zastąpić łącza stacjonarne uruchamiane na podstawie podpisanych umów z przedsiębiorcami telekomunikacyjnymi. Tym bardziej że należy zdawać sobie sprawę z faktu, iż nie trzeba niszczyć wszystkich punktów dostępowych do cywilnych łączy w naszym kraju, co zresztą mogłoby być kłopotliwe, ponieważ takich punktów, powołując się na raporty Urzędu Komunikacji Elektronicznej, jest już prawie 50 mln. Wystarczy skoncentrować wysiłek na elementach zarządzających. Każda sieć czy to operatora publicznego, czy innego ma właśnie takie słabe punkty.

ŁĄCZNOŚĆ RADIOLINIOWA I RADIOWA

Wydaje się, że najsilniejszymi mobilnymi łączami wykorzystującymi falę elektromagnetyczną, którymi dysponują siły zbrojne, są łącza radioliniowe. Niestety choć ich przepływność wciąż wzrasta, aktualnie eksploatowane łącza 34 Mbit/s stają się wąskim gardłem. Trzeba przy tym założyć, że wchodzące do użytkowania aparatownie (100 Mbit/s) z pewnością również będą wymagały wymiany za jakiś czas.

Warto jednak pokusić się o określenie minimalnej liczby takich urządzeń, która wystarczy do pokrycia terytorium całego kraju, by w 100% procentach zastąpić system stacjonarny. Mowa tu o budowie redundantnego[4] systemu typu krata, by utrudnić obezwładnienie całego systemu nawet w przypadku zniszczenia (obezwładnienia) jego pojedynczych elementów. Zakładając, że zasięg praktyczny radiolinii HCLOS pracujących w paśmie III+ znajdujących się w wyposażeniu RWŁC-10T wynosi od 25 do 30 km (przy założeniach producenta w warunkach laboratoryjnych 50 km), oraz uwzględniając powierzchnię naszego kraju (312 697 km^2), można oszacować liczbę takich aparatowni mobilnych, która będzie wynosić od 440 do 640.

Jak wyglądałaby sytuacja, gdyby w podobny sposób pokryć teren naszego kraju radiostacjami z rodziny PR4G typu F@stnet? Każda z nich może stanowić punkt retlansacyjny, co zdecydowanie zwiększy zasięg ich pracy. Przy założeniu zasięgu praktycznego od 20 do 25 km dla radiostacji RRC 9311 o mocy 50W szacunkowo należałoby ich uruchomić od 640 do 1000.

ŁĄCZNOŚĆ TROPOSFERYCZNA I SATELITARNA

W ciągu ostatnich lat można zaobserwować zdecydowane zwiększenie wielkości pasów (rejonów) odpowiedzialności przydzielanych dowódcom po-

2 Od początku 2022 roku występujące jako Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni [przyp. autora].

3 Według stanu prawnego na dzień 21.05.2021 r. są to przedsiębiorstwa: Naukowa i Akademicka Sieć Komputerowa (NASK) – Państwowy Instytut Badawczy, EMITEL S.A., Multimedia Polska S.A., NETIA S.A., Orange Polska S.A., POLKOMTEL Sp. z o.o., T-Mobile Polska S.A., TTComm S.A., EXATEL S.A., Poczta Polska S.A., ENERGO-TEL S.A., PKP TELKOL Sp. z o.o.

4 Redundancja – tutaj: nadmiarowość osiągana przez zapewnienie możliwości elektronicznej wymiany informacji różnorodnymi sposobami, zwiększająca żywotność wojskowego systemu łączności [przyp. autora].

szczególnych szczebli dowodzenia. W praktyce, przykładowo, dywizja broni się już nawet w pasie 100 na 100 km. Wiąże się to również ze zwiększaniem odległości między elementami dowodzenia w ugrupowaniu bojowym.

Odpowiedzią na nowe warunki prowadzenia działań wydaje się powrót do łączności troposferycznej jako bardziej odpornej na zakłócenia stosowane przez przeciwnika w porównaniu z innymi bezprzewodowymi środkami łączności. Co ważne, aparatownie MAT-10 CJ (rys. 3) ze względu na doposażenie w radiolinie horyzontowe są w pełni kompatybilne z używanymi RWŁC-10T. Przy wielu ich zaletach należy wskazać istotną cechę łączności troposferycznej, a mianowicie duży wpływ niekorzystnych warunków meteorologicznych na zmniejszenie przepływności łączy.

Na świecie jest użytkowanych kilka tysięcy satelitów. Typowo na potrzeby wojskowe jest stosowanych ich prawie 13%. W naszym kraju już kilka razy pojawiały się plany umieszczenia w kosmosie własnych, opracowanych przez rodzimych naukowców, satelitów, jednak zwykle na realizację tych zamierzeń brakowało środków. Udało się nam jedynie umieścić na orbicie mikrosatelity PW-Sat w 2012 roku, a później Lem i Heweliusz.

Trzeba podkreślić, że w praktyce już trzy satelity umieszczone na orbicie geostacjonarnej co 120° pokryją niemal całe terytorium globu (z wyłączeniem obszarów podbiegunowych poza około 70° szerokości geograficznej). Dla naszych sił zbrojnych, biorąc nawet pod uwagę udział w operacjach poza granicami kraju, byłoby to wystarczające. Ostatecznie zaledwie jeden satelita geostacjonarny mógłby w pełni zaspokoić potrzeby na terenie Polski. Tymczasem korzystamy z usług innych państw. Wskazać ponadto należy, że sygnał transmitowany przez satelitę umieszczonego na wspomnianej orbicie może być przechwycony przez nieruchome anteny ustawione gdziekolwiek w zasięgu pokrywanego obszaru, a ten z kolei może mieć wielkość regionu, kraju, a nawet całego kontynentu. Każdy odbiorca umieszczony w zasięgu nadawania satelity jest w stanie odebrać nadawany sygnał, posługując się niewielką anteną, zazwyczaj o średnicy 40–50 cm.

SKALOWALNY SYSTEM ŁĄCZNOŚCI

Jeśli uwzględnimy zaprezentowane treści, możemy pokusić się o próbę wskazania możliwości wojskowego systemu łączności transmisji danych w ugrupowaniu bojowym (rys. 4). W podstawowym rozwiązaniu zakłada się łączność opartą na transmisji danych, a więc odchodzenie od pracy fonem na rzecz ustandaryzowanych wiadomości przesyłanych w ramach obowiązującego systemu meldunkowego, szczególnie w odniesieniu do najniższych szczebli dowodzenia. Dlaczego właśnie tak? Chodzi przede wszystkim o czas – przekazanie informacji fonem trwa zdecydowanie dłużej niż przesłanie wiadomości (meldunku) w postaci pliku, komunikatu itd. Natomiast równoczesna praca fonem oraz transmisja danych powodują znaczne ograniczenie przepływności łączy radiowych.

W tym miejscu warto wskazać system wspomagania dowodzenia C3IS HMS Jaśmin jako element spinający różne systemy użytkowane w siłach zbrojnych w jedną całość. Na podstawie przeprowadzonych w Akademii Sztuki Wojennej badań[5] można stwierdzić, że i na najniższych szczeblach dowodzenia wymiana informacji w tym systemie może odbywać się w sposób zbliżony do rzeczywistego, nawet z wykorzystaniem radiostacji KF czy też UKF. Warunek jest jednak jeden: przed rozpoczęciem działań należy zaktualizować lokalne bazy danych. Dzięki temu wymienia się później przez łącza radiowe po prostu mniej informacji.

REDUKCJA BARIER

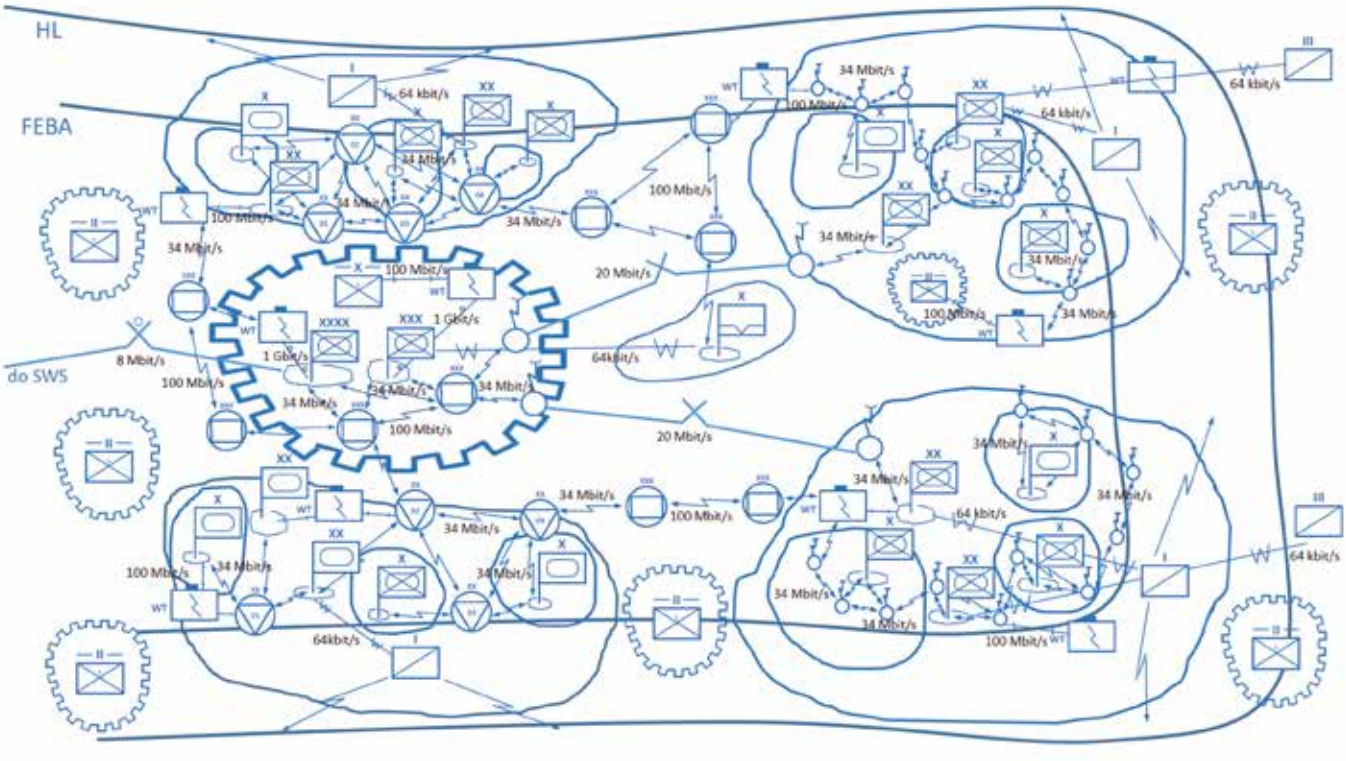
Wojskowy system łączności funkcjonuje w dynamicznie zmieniającym się otoczeniu. Wymiana w nim informacji wymaga dokonywania zmian, które ograniczą bądź wyeliminują bariery stanowiące przeszkody w jej sprawnym przebiegu. Redukcja barier w wojskowym systemie łączności będzie następować wraz z osiąganiem kolejnych zdolności w odniesieniu do systemu funkcjonalnego wsparcia dowodzenia.

W ostatnim czasie można zaobserwować z jednej strony znaczne zwiększanie pasów (rejonów) działania (odpowiedzialności) na poszczególnych szczeblach dowodzenia. Z drugiej natomiast wprowadzane rozwiązania techniczno-organizacyjne mają na celu ostateczne włączenie wszystkich elementów ugrupowania w jeden zintegrowany system teleinformatyczny, co jest nazywane w literaturze *integracją platform bojowych z rozległymi sieciami teleinformatycznymi*. Chodzi tutaj w pierwszej kolejności o integrację stanowisk dowodzenia z wozami dowodzenia z wykorzystaniem różnorakich środków transmisyjnych, jak również samych stanowisk dowodzenia (rys. 5). W drugiej – trudniejszej do osiągnięcia – o wymianę informacji (budowanie takich zdolności), aby uzyskać dostęp do wspólnego obrazu sytuacji w ramach systemu teleinformatycznego (ST) PMN 2.0, a więc nie tylko między stanowiskami dowodzenia.

Usprawnienie wymiany informacji w wojskowym systemie łączności będzie wymagać zbudowania dwóch niezależnych systemów: operacyjnego ST, utworzonego ze zintegrowanych elementów systemu stacjonarnego, i polowego PMN oraz taktycznego ST, który będą stanowić wozy dowodzenia i wozy bojowe. W konsekwencji takie rozwiązania umożliwią integrację międzysystemową, powszechność

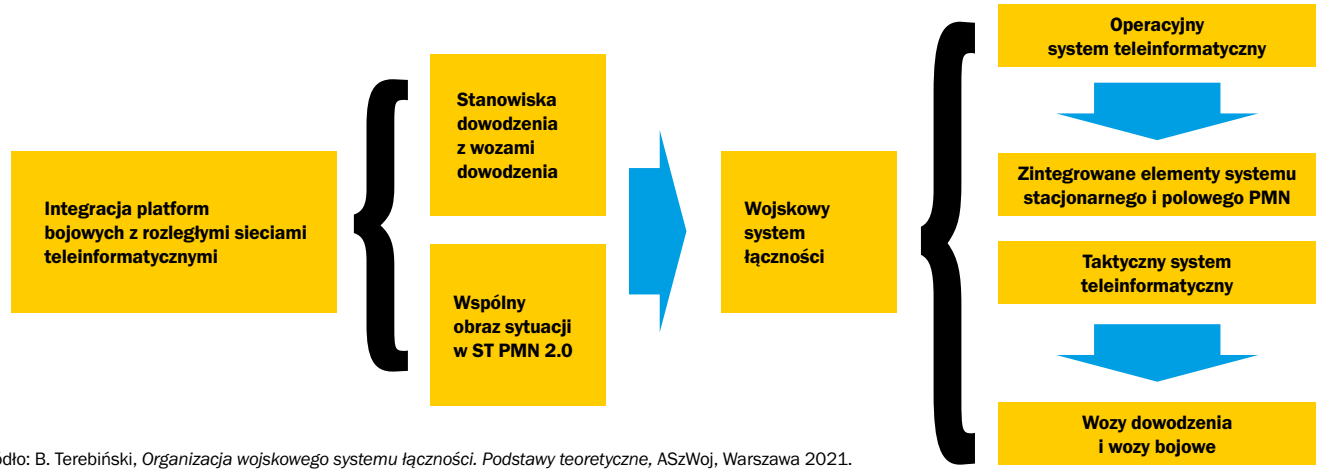
5 B. Biernacik, *Ćwiczenie studyjne BRAMA-21*, Zakład Teleinformatyki, AszWoj, Warszawa 2021.

RYS. 4. TRANSMISJA DANYCH W UGRUPOWANIU BOJOWYM (PRZYKŁAD)



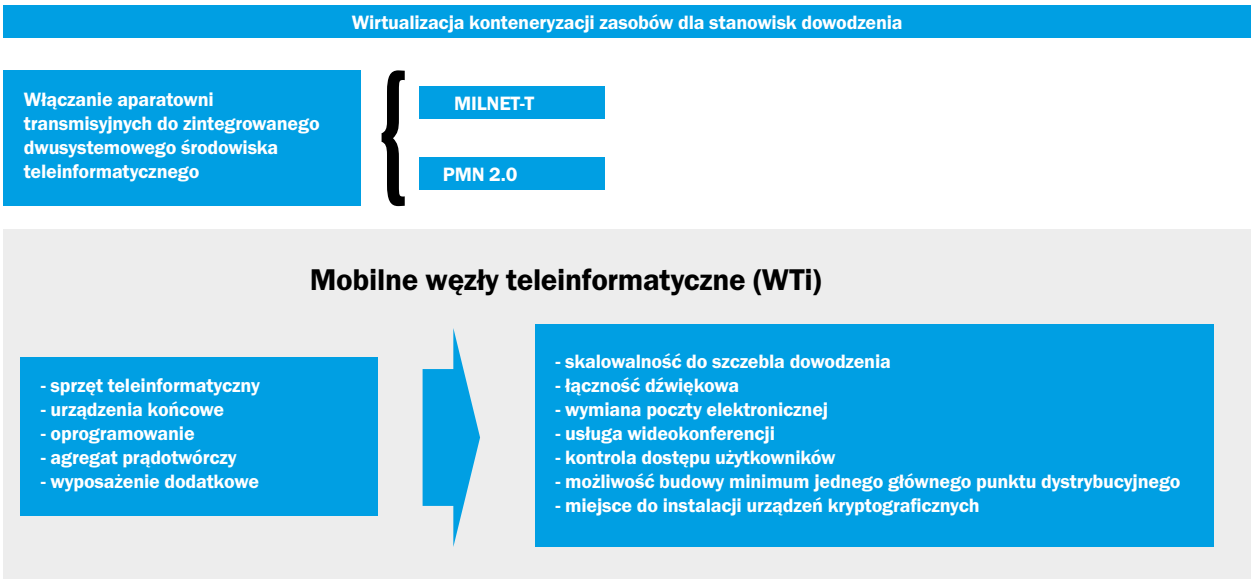
Źródło: B. Terebiński, S. Fabicki, *Transmisja danych w cyberprzestrzeni SZ RP – analiza porównawcza* [w:] *Bezpieczeństwo działań w cyberprzestrzeni – wybrane aspekty*, t. 2. *Techniczne aspekty cyberprzestrzeni,* red. M. Marczyk, M. Stolarz, B. Terebiński, ASzWoj, Warszawa 2022.

RYS. 5. DUALNOŚĆ WOJSKOWEGO SYSTEMU ŁĄCZNOŚCI



Źródło: B. Terebiński, *Organizacja wojskowego systemu łączności. Podstawy teoretyczne,* ASzWoj, Warszawa 2021.

RYS. 6. DWUSYSTEMOWOŚĆ ŚRODOWISKA TELEINFORMATYCZNEGO



Źródło: B. Terebiński, *Organizacja wojskowego systemu łączności. Podstawy teoretyczne,* ASzWoj, Warszawa 2021.

wymiany danych oraz nadmiarowość (redundancję) systemową. Integracja systemu stacjonarnego i polowego zapewni efektywniejsze wykorzystanie posiadanych zasobów oraz umożliwi zbudowanie systemu teleinformatycznego przygotowanego zawczasu. Wiązać się to będzie z wykorzystaniem serwerowni stacjonarnych oraz udostępnieniem jak największej liczby usług dostarczanych centralnie. Natomiast na stanowiskach dowodzenia będą lokalnie utrzymywane najważniejsze usługi. Ostatecznie transmisja danych będzie się opierać przede wszystkim na systemie stacjonarnym, jak również na systemach stacjonarno-radioliniowych, stacjonarno-satelitarnych, radioliniowo-satelitarnych oraz łączności KF. Rodzi to także implikacje związane z opracowaniem uniwersalnych modułów dla transmisji oraz budowy sieci LAN (MAN) stanowisk dowodzenia z wykorzystaniem węzłów teleinformatycznych (WT) oraz wozów kablowych wzmocnionych dodatkową radiolinią. Na każdym stanowisku dowodzenia niezbędny będzie element zarządzania odpowiedzialny za uruchomienie i nadzorowanie pracy domen informacyjnych, stanowiący pierwszą linię wsparcia użytkowników.

Istotne jest przy tym uzyskanie możliwości przetwarzania w chmurze (wirtualizacja konteneryzacji zasobów) dla stanowisk dowodzenia oraz wdrażanie aparatowni transmisyjnych i włączanie ich do zintegrowanego dwusystemowego środowiska teleinformatycznego (rys. 6). Dwusystemowość dotyczy połączenia systemów teleinformatycznych: funkcjonującego w czasie pokoju MILNET-T oraz już wskazanego PMN. Natomiast w ST PMN, który ma umożliwić przetwarzanie informacji o klauzuli *tajne* i *NATO SECRET* na stanowiskach dowodzenia wszystkich szczebli, będą wykorzystywane głównie mobilne węzły teleinformatyczne (WTi). Zestaw WTi będzie się składał ze*: sprzętu teleinformatycznego, urządzeń końcowych, oprogramowania, agregatu prądotwórczego i wyposażenia dodatkowego*. [Zestawy te zapewnią]: *skalowalność do szczebla, na jakim będą zastosowane transmisje danych, łączność dźwiękową, wymianę poczty elektronicznej i dystrybucję plików, usługę wideokonferencji oraz kontrolę dostępu użytkowników do systemu teleinformatycznego, możliwość budowy minimum jednego głównego punktu dystrybucyjnego (np. serwery, firewall, routery, urządzenia szkieletowe sieci), a także miejsce do instalacji urządzeń kryptograficznych (Polowe Kancelarie Kryptograficzne dla WP, 2018-07-08)*[6].

Procedura pozyskania sprzętu i oprogramowania do budowy ST MILNET-T została zainicjowana w lipcu 2019 roku przez Centrum Zasobów Informa-

6 Źródło: https://www.milmag.pl/news/view?news_id=1755/. 20.01.2022.

tycznych Inspektoratu Informatyki, przekształconego (31.12.2019) w Centrum Zasobów Cyberprzestrzeni Sił Zbrojnych Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. Węzły teleinformatyczne mają stanowić uzupełnienie funkcjonujących już zintegrowanych węzłów teleinformatycznych (ZWT) Komputerowo-Telefonicznego Systemu Alarmowania wersji polowej (KTSAwp) Jaśmin, podlegających ciągłym modernizacjom do kolejnych standardów. W następnym kroku niezbędne będzie pozyskanie zdolności elementów mobilnych do wymiany informacji w ST PMN z wykorzystaniem łączności radiowej w ramach szerokopasmowych i wąskopasmowych *waveformów* zgodnie ze specyfikacją obowiązujących standardów Spiral FMN[7].

Rozwój infrastruktury teleinformatycznej, zarazem wdrożenie usprawnień związanych z przepustowością łączy oraz terminowością wymiany informacji będą uwarunkowane możliwością wykorzystania technologii LTE oraz 5G. Z kolei w ramach zintegrowanych sieci przewodowych, radioliniowych, radiowych oraz taktycznych systemów transmisji danych jest wskazywana technologia AI (Artificial Intelligence – sztuczna inteligencja) do wyboru optymalnego kanału transmisyjnego, technologia hybrydowych łączy optyczno-radiowych oraz technologia Wi-Fi do budowy bezpiecznych sieci lokalnych stanowisk dowodzenia. Na potrzeby stanowisk dowodzenia, jak również ćwiczeń niezbędne są zdolności do uruchamiania usług teleinformatycznych w sieciach komputerowych organizowanych w trybie *ad hoc*. Ważna jest przy tym konieczność budowania operacyjnej bazy danych na potrzeby planowania i prowadzenia operacji obronnej oraz zintegrowanie specjalistycznych usług dziedzinowych z bazami HNS (Host Nation Support – wsparcie przez państwo gospodarza). W celu usprawnienia funkcjonowania sieci radiowych warto, po uzyskaniu uprawnień przez personel po przeszkoleniu w Wojskowym Biurze Zarządzania Częstotliwościami, posługiwać się narzędziem, którym jest system zarządzania widmem częstotliwości Spectrum XXI.

Rozwiązaniem problemu współdziałania ze służbami spoza układu militarnego, co jest bolączką najnowszego rodzaju sił zbrojnych, którym są wojska obrony terytorialnej, jest wdrożenie do działalności służbowej systemu TETRA[8]. Współcześnie około 60% jego użytkowników na świecie stanowią różnego rodzaju służby publiczne czy ratownicze. Coraz częściej system ten znajduje zastosowanie do komunikacji krytycznej w innych sektorach, takich jak transport czy energetyka. W naszym kraju około 47% stacji bazowych należy do systemu TETRA, a więc jest to system o największym krajowym zasięgu. Umożliwia współpracę z sieciami zewnętrznymi, takimi jak: publiczna telefoniczna sieć stała, sieci ISDN, sieci pakietowej transmisji danych itp.

Mobilne stacje bazowe wyposażone w radiolinie powszechnie wykorzystywane w siłach zbrojnych (np. R-450) umożliwiają współpracę urządzeń w odległości do 40 km od stacjonarnych węzłów teleinformatycznych. Kolejne mobilne stacje mogą pełnić rolę elementów osi radioliniowej[9].

DĄŻYĆ DO KOMPATYBILNOŚCI

Podsumowując rozważania prowadzone w obszarze militarnego wykorzystania środków łączności i informatyki, warto wskazać, że obecnie próby wyznaczania trendów rozwoju technologicznego w perspektywie długoterminowej mogą być trudne lub wręcz niemożliwe. Dlatego w opinii autora ważne jest uwypuklenie tego, co należy zrealizować w najbliższej przyszłości. Stąd priorytetowe wydaje się w dalszym ciągu dążenie do kompatybilności etatowych środków łączności pododdziałów wsparcia dowodzenia nie tylko pod względem *hardware*, lecz również *software*. Wiąże się to z koniecznością utworzenia repozytorium ustandaryzowanego oprogramowania, którego próżno szukać na witrynach wojskowych systemów teleinformatycznych. Częściowym rozwiązaniem tego problemu (czy wręcz koniecznością) są warsztaty łączności (zgrupowania wojsk łączności) przed każdymi ćwiczeniami. Powstaje jednak pytanie, czy wystarczy na to czasu w warunkach bojowych. Podobnie istotne wydaje się zastanowienie nad miejscem, gdzie można łączyć różne platformy (rozwiązania) i ustalać zasady interoperacyjności. I tutaj z pomocą przychodzą ćwiczenia CWIX corocznie organizowane przez Centrum Szkolenia Sił Połączonych NATO[10], do udziału w których swoje rozwiązania mogą zgłaszać zarówno siły zbrojne państw sojuszniczych, jak i prywatne przedsiębiorstwa.

Natomiast niekwestionowany jest fakt, że organizację łączności kształtuje przyjęty system dowodzenia, a więc również struktura organizacyjna elementów dowodzenia w ugrupowaniu bojowym. Zatem czy sposób rozwijania (umiejscowienia) elementów dowodzenia zgodnie z obowiązującymi normatywami jest tym, czego potrzebuje pole walki, w szczególności na poziomie taktycznym? Odpowiedź na to pytanie wymaga przeprowadzenia osobnej diagnozy wykraczającej poza niniejszą publikację. ■

7 Por. https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_ Bundle.pdf/. 20.01.2022.

8 Por. B. Terebiński, S. Fabicki, *Łączność radiotelefoniczna w brygadzie obrony terytorialnej – możliwości i wyzwania,* „Przegląd Sił Zbrojnych" 2021 nr 6.

9 Por. B. Terebiński, *Teleinformatyka wojskowa,* ASzWoj, Warszawa 2022.

10 Joint Force Trainning Centre – ośrodek szkoleniowy NATO podległy Dowództwu ds. Transformacji w Norfolk, https://www.jftc.nato.int/. 20.01.2022.

Rola użytkownika operacyjnego w eksploatacji **i rozwoju systemów (usług) informatycznych**

ZARZĄDZANIE INFORMACJĄ TO DOMENA PRZEDSTAWICIELI PIONÓW OPERACYJNYCH STANOWISK DOWODZENIA WSPIERANA ŚRODKAMI TELEINFORMATYKI.

płk dr inż. Maciej Nowak

Autor jest głównym specjalistą w Zarządzie Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ.

Zdający egzamin ze sprawności fizycznej żołnierze, w tym także autor artykułu, będący w VII grupie wiekowej (i wyższych), zapewne pamiętają czasy, gdy już byli żołnierzami, a nie było nie tylko smartfonów, lecz w ogóle telefonów komórkowych. Nawet posiadanie zwykłego aparatu stacjonarnego nie było powszechne. Tymczasem już wtedy prężnie rozwijała się informatyka. Absolwenci Wydziału Cybernetyki WAT znajdowali zatrudnienie w filiach Wojskowego Instytutu Informatyki (WII) czy ośrodkach przetwarzania informacji (OPI). Projektowali bazy danych i systemy przetwarzania informacji, oparte na dużych komputerach typu Mainframe (w tym polskiej produkcji, np. Odra).

Społeczność operacyjna (autor używa tego pojęcia, aby określić wszystkich nieinformatyków) odgrywała w tych czasach rolę *dostawcy* danych wejściowych i *konsumenta* danych wyjściowych – wyników przetwarzania, najczęściej w postaci zestawień i analiz ilościowych. To, jak odbywało się przetwarzanie, pozostawało w obszarze *wiedzy tajemnej*, magii, która działała w *czarnym pudełku* informatyków.

EWOLUCJA

Początek lat dziewięćdziesiątych ubiegłego wieku to już czas rewolucji, jaką było wprowadzanie do użycia komputerów osobistych (autor na pierwszym roku studiów w WAT korzystał w laboratorium z komputera klasy XT, niedługo kupił sobie AT – z dyskiem twardym 40 MB!), na trzecim roku miał już 386, by piąty ukończyć z 486 DX2/66, choć niektórzy koledzy *szarpnęli się* już na pierwsze Pentium).

Rewolucja była tak szybka, że pomysły na wykorzystanie coraz szybszych komputerów osobistych przez społeczność operacyjną nie nadążały za rozwojem technologii. Efektem było to, że pojawiło się zjawisko *komputeryzacji*, tzn. prostego zastępowania komputerami tradycyjnych maszyn do pisania. Przy czym już korzystanie z nich nastręczało niektórym

dinozaurom sporych problemów, dlatego też utarło się, że najlepiej, jakby obsługiwał je jakiś młody absolwent kierunku informatycznego. W ćwiczeniach wykorzystywano siły i środki informatyki, często w postaci złożonych z informatyków tzw. grup automatyzacji dowodzenia (GAD). To z tamtych czasów wywodzi się funkcjonujące niestety do dziś przekonanie, że informatyzacja[1] to dziedzina informatyków.

Tymczasem rolą systemów informatycznych czy też – wobec powszechnego wykorzystania MILNET-Z, MILNET-I, PMN 2.0 – i innych usług oferowanych w systemach teleinformatycznych jest wsparcie procesów informacyjnych zachodzących w organizacji o bardzo złożonej strukturze, jaką są siły zbrojne i resort obrony narodowej. *Właścicielami* tych procesów nie są informatycy, lecz społeczność operacyjna. Stanowią ją tradycyjnie: logistycy, finansowcy i kadrowcy, a także komórki rozpoznania, planowania, *stricte* operacyjne (tzw. trójki), a wreszcie żołnierze korzystający z zautomatyzowanych systemów kierowania środkami walki. Czy ktoś jeszcze ma dzisiaj wątpliwości, czy system wsparcia artylerii Topaz, wspierający chociażby dywizjony samobieżnych haubic Krab i moździerzy Rak, powinien być obsługiwany przez artylerzystów. To oni powinni mieć głos decydujący w sprawie kierunków jego rozwoju – rozbudowy funkcjonalności o nowe elementy.

A jednak rozumienie podziału ról: informatyk – dostawca usługi teleinformatycznej (odpowiedzialny też za jej utrzymanie), użytkownik operacyjny – odbiorca i użytkownik usługi, przedstawiciel społeczności będącej *właścicielem* danego systemu informacyjnego wspieranego usługą – nie jest jeszcze powszechne. Weźmy przykład FAS-ów (Functional Area Services – zbioru usług (systemów informatycznych) powszechnie wykorzystywanych w NATO do wsparcia wielu różnych obszarów funkcjonalnych. Jeszcze do niedawna regułą podczas organizowania ćwiczeń, zwłaszcza dowódczo-sztabowych, było wymaganie, by w rozwijanym na potrzeby ćwiczeń systemie teleinformatycznym były uruchomione wszystkie FAS-y. Oczywiście jednostki wsparcia dowodzenia, nakładem dużych sił, środków (m.in. serwerów usług, w tym osadzanych na maszynach wirtualnych) i czasu, instalowały i utrzymywały te usługi, zakładały i konfigurowały konta użytkowników. Po ćwiczeniach okazywało się, że niektórzy użytkownicy nawet nie zalogowali się do swoich usług, a wykorzystanie niektórych było symboliczne i nie odnosiło się do *meritum* ćwiczeń (np. tylko krótkie powitania w J-Chat). Wynikało to z tego, że użytkownik operacyjny, zmuszony idącymi z góry poleceniami, wymagał uruchomienia usługi, ale już nie miał pomysłu, jak ją wykorzystać. System nakazowy, tak popularny w siłach zbrojnych na całym świecie, nie sprawdza się w odniesieniu do wdrażanych rozwiązań informatycznych.

JAROSŁAW WIŚNIEWSKI

Na szczęście ta sytuacja – z punktu widzenia jednostek łączności i wsparcia dowodzenia – już korzystnie się zmieniła. Po pierwsze, wprowadzono nowe zasady udostępniania FAS-ów. Na potrzeby ćwiczeń (ma to też zastosowanie do każdej operacji) tworzy się tzw. matrycę usług. Jej kolumny stanowią uruchamiane usługi, wiersze zaś – odbiorcy (użytkownicy) usług. Jeśli w którejś kolumnie nie ma zdefiniowanych użytkowników, dana usługa po prostu nie jest uruchamiana i utrzymywana. Ale kto ma taką usługę zgłosić? I tu pojawia się druga i kluczowa kwestia: *wymagania na wymianę informacji* (Information Exchange Requirements IER). W NATO już dawno wzięto na warsztat zagadnienie odpowiedzialności za obszary (systemy) informacyjne, tworząc wskazane pojęcie. Zgodnie ze STANAG-iem 2519, wprowadzającym natowski standard APP-15 *NATO Information Exchange Requirement Specification Process*, za użytkowników operacyjnych są uznawane dowództwa na wszystkich poziomach (natowskie dowództwa strategiczne, operacyjne lub taktyczne, inne odpowiednie organizacje NATO oraz dowództwa narodowe), które mają potrzebę wysyłania i odbierania informacji w celu realizacji swoich zadań. Użytkownik operacyjny odpowiada za identyfikację swoich potrzeb informacyjnych i dostarczenie szczegółów niezbędnych do specyfikacji właściwych wymagań na wymianę informacji (IER).

Za całościowe kierowanie procesem opracowania IER (w swoim obszarze zainteresowania) odpowiada władza operacyjna, którą w NATO jest jedna z Rad Standaryzacyjnych Komitetu Wojskowego (Military Commitee Standarization Boards – MCSB), pod którą podlegają sponsorzy operacyjni (Operational Sponsors). Z kolei ci są odpowiedzialni za opracowanie

1 Autor sugeruje przyjęcie definicji informatyzacji jako ciągłego procesu wdrażania i doskonalenia systemów informatycznych (usług w systemach teleinformatycznych) wspierających funkcjonowanie systemów informacyjnych.

i rozwój wymagań na wymianę informacji[2]. Każdemu ze środowisk operacyjnych: lądowemu, powietrznemu, morskiemu i połączonemu MCSB ustanowiło wyższy panel IER (Senior IER Panel – SIERP) dla harmonizacji i koordynacji IER.

Jedną z grup roboczych NATO jest Information Exchange Requirement Harmonization Working Group (IERHWG), która odpowiada za rozwój i utrzymanie publikacji, określających przede wszystkim procedury operacyjne, strukturę i formę wiadomości, ich adresatów, zawartość czy operacyjne wykorzystanie wiadomości. Dlatego też w skład grupy wchodzą przedstawiciele pionów operacyjnych, których sferą działalności jest identyfikowanie określonych potrzeb w zakresie wymiany informacji między wojskami lub dowództwami. Przedmiotowy STANAG został formalnie ratyfikowany przez stronę polską 14 kwietnia 2015 roku.

Wyrazem praktycznego przełożenia reguł określonych natowskim STANAG-iem na nasz resort obrony jest m.in. *Instrukcja organizacji i funkcjonowania systemu łączności w ramach wojennego systemu dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej*. Stanowi ona, że planowanie systemu łączności na potrzeby konkretnej operacji obejmuje: po pierwsze – analizę posiadanych i pozyskiwanych informacji, po drugie – pozyskanie wymagań na wymianę informacji (IER). Wymagania te opracowują komórki operacyjne lub odpowiedzialne za zarządzanie wymianą informacji danego stanowiska dowodzenia (Information Knowledge Management – IKM) komórki etatowe, lub wskazane przez dowódcę/komendanta/dyrektora/szefa. Dzięki temu na trzecim poziomie procesu planowania systemu łączności, zgodnym z architekturą systemu funkcjonalnego wsparcia dowodzenia SZRP (kolejnym po poziomach: operacyjnym i widoków systemowych), możliwe jest określenie organizacji usług i systemów teleinformatycznych. Przyjmuje ona postać m.in. tzw. matrycy PACE (PACE MATRIX)[3] oraz wynikającej z niej – wspominanej już – matrycy usług teleinformatycznych (CIS Service MATRIX). IER-y opracowuje się na podstawie potrzeb informacyjnych poszczególnych komórek sztabowych (Community of Interest – COI) i procesów operacyjnych realizowanych na stanowisku dowodzenia.

W przedmiotowych IER-ach powinno się określać m.in.: schematy wymiany informacji między poszczególnymi poziomami kierowania i dowodzenia oraz szczeblami organizacyjnymi, rodzaj i format dokumentów wytwarzanych na danych stanowiskach funkcyjnych, sposób przekazywania i wytwarzania poszczególnych informacji (która usługa w systemie teleinformatycznym ma być do tego wykorzystana). Na podstawie powyższych matryc i schematów komórki i pododdziały odpowiedzialne za rozwijanie systemu łączności opracowują matrycę sprzętu teleinformatycznego i usług oraz globalną listę adresową (Global Address List – GAL).

WŁAŚCIWE PODEJŚCIE

Społeczność operacyjna coraz bardziej jest świadoma spoczywającej na niej odpowiedzialności i roli, jaką powinna odgrywać w relacjach ze społecznością (tele)informatyki. Jako przykład można podać zadanie postawione przez dowódcę generalnego RSZ w wyniku konferencji pionów operacyjnych sił zbrojnych „Operator-21", przeprowadzonej przez Zarząd Planowania Użycia Sił Zbrojnych i Szkolenia – P3/P7 Sztabu Generalnego WP w 2021 roku. W zadaniu tym szef sztabu DGRSZ jest wskazany jako odpowiedzialny za sprawowanie nadzoru nad wyznaczeniem właściwych komórek odpowiedzialnych za opracowanie i utrzymanie w aktualności wymagań na wymianę informacji w ramach wojennego systemu dowodzenia (WSyD) – zgodnie z zapisem przywołanej wcześniej *Instrukcji organizacji …* przez dowódców jednostek bezpośrednio podporządkowanych dowódcy generalnemu RSZ. Warto podkreślić, że wyraźnie wskazano tu, iż zasadniczą rolę w tym zakresie odgrywają komórki operacyjne. Zwieńczeniem procesu formalnego usankcjonowania tych zasad jest *Rozkaz Nr Z-32/ZKiD-P6 Szefa Sztabu Generalnego WP z dnia 03 czerwca 2022 r. w sprawie wprowadzenia do użytku wymagań na wymianę informacji (Information Exchange Requirements – IER's) w ramach Wojennego Systemu Dowodzenia Sił Zbrojnych RP (WSyD SZ RP).*

Kolejne ćwiczenia i treningi sztabowe, np. trening Dowództwa Generalnego RSZ „Model-22", są już realizowane zgodnie z tą koncepcją. Przełożenie zapisów dokumentów formalnych, szczegółowo opisujących podział kompetencji i odpowiedzialności na praktyczne działanie w procesach przygotowania, rozwijania i funkcjonowania stanowisk dowodzenia w obszarze teleinformatyki, zdecydowanie zwiększa ich efektywność, pozwalając w rezultacie na zwiększenie efektywności systemów informacyjnych warunkujących sprawne funkcjonowanie stanowiska dowodzenia.

Jak widać, istnieją już formalne podstawy uporządkowania relacji między użytkownikami operacyjnymi systemów informatycznych (usług w systemach teleinformatycznych) a ich dostawcami. Są też już pierwsze przykłady, które wskazują na praktyczne korzyści z ich stosowania. Jedyne co zostało, to ostatecznie przeciąć wynikającą z historii pępowinę w sferze przyzwyczajeń, łączącą użytkownika z informatykiem tak, by ten pierwszy mógł się wreszcie usamodzielnić. Większa odpowiedzialność po jego stronie to wymierne korzyści dla całego systemu kierowania i dowodzenia, który współcześnie bez wsparcia usługami systemów teleinformatycznych nie ma racji bytu. ■

2 *An Operational Sponsor is a body that assumes responsibility for the development and maintenance of an IER*, NATO Standardization Office, Bruksela 9.06. 2017.

3 Od: Primary, Alternate, Contingency, Emergency.


GRUPA WB
Nasza rzeczywistość
to wasza przyszłość
www.wbgroup.pl

System teleinformatyczny PMN 2.0 w służbie NATO

DĄŻENIE DO INTEROPERACYJNOŚCI ORAZ USPRAWNIENIA WYMIANY INFORMACJI W ARMIACH CZŁONKOWSKICH SOJUSZU POLEGA MIĘDZY INNYMI NA TWORZENIU SIECI MISJI.

Marcin Marek jest szefem Oddziału Wsparcia Teleinformatycznego w Zarządzie Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ.

Zbigniew Ćwik jest starszym specjalistą w Zarządzie Wsparcia Dowodzenia i Łączności IRW DGRSZ.

płk dr inż. Marcin Marek, ppłk Zbigniew Ćwik

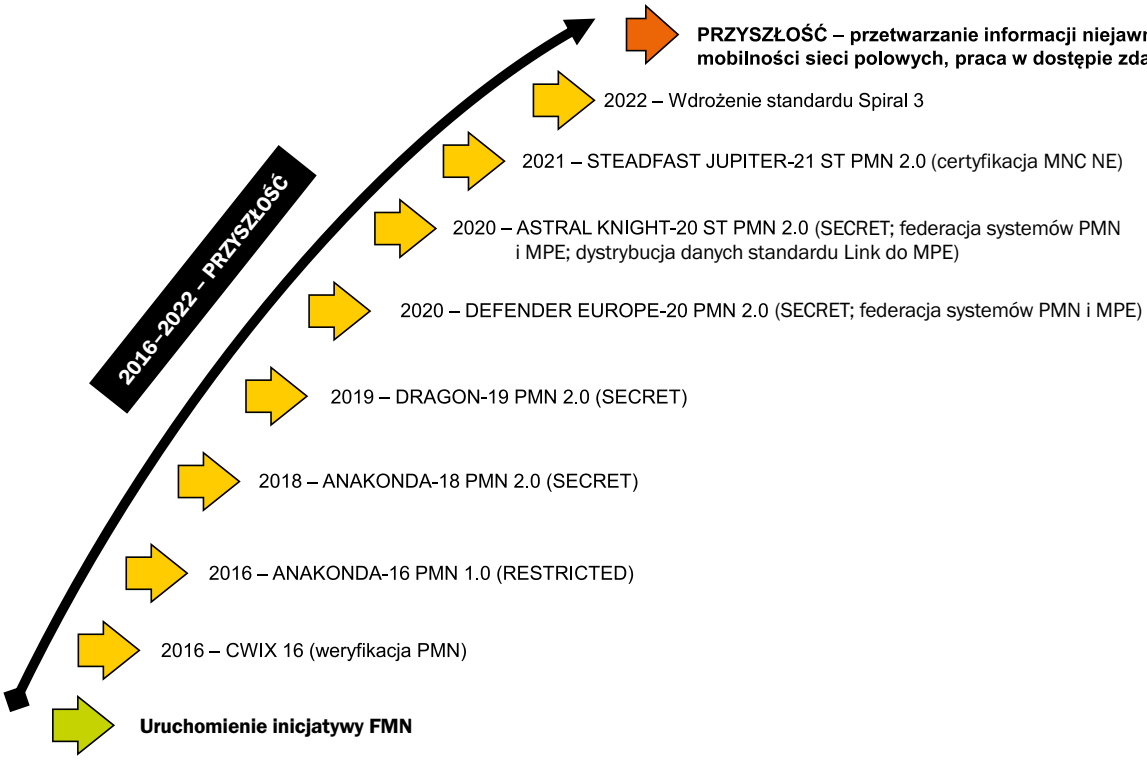
Doświadczenia z Afganistanu uwidoczniły zaangażowanym w prowadzoną w tym kraju operację kontyngentom wojskowym wielu państw wykorzystującym rodzime systemy wsparcia dowodzenia, jak ważne jest osiągnięcie interoperacyjności. Po początkowych poszukiwaniach doraźnych rozwiązań mających zapewnić współdzielenie połączonego obrazu operacyjnego oraz sprawne funkcjonowanie w międzynarodowym środowisku teleinformatycznym wdrożono i rozwijano Afghanistan Mission Network, czyli sieć federacyjną łączącą odrębne komponenty połączone wspólną modułową filozofią działania. Na podstawie doświadczeń z jej funkcjonowania stwierdzono, że konieczne są ustandaryzowane podejście, wspólne procedury i jednolite wymagania techniczne, które umożliwią państwom NATO przygotowanie wspólnych federacyjnych sieci teleinformatycznych zapewniających wsparcie dowodzenia w przyszłych sojuszniczych operacjach połączonych. Wymogiem niezbędnym do wdrożenia tego projektu okazało się zbudowanie stałej struktury koordynującej sterowanej przez centralne instytucje Sojuszu. Nazwano ją Federated Mission Networking (FMN).

Polska od początku uczestniczyła w pracach z tym związanych. Wspierała jej rozwój oraz przygotowywała się do stworzenia polskiej implementacji – Polish Mission Networking (PMN). W założeniu zaspokaja ona zarówno narodowe potrzeby w dziedzinie wsparcia operacji i ćwiczeń, jak i umożliwia udział komponentów naszych sił zbrojnych w międzynarodowych zamierzeniach.

INICJATYWA FMN

Została uruchomiona przez North Atlantic Council w 2015 roku. Jej głównym zadaniem było skonsolidowanie wysiłków instytucji NATO oraz państw członkowskich związanych z definiowaniem procedur operacyjnych i technicznych w celu zarządzania połączeniami międzysystemowymi wsparcia dowodzenia w układzie sojuszniczym. Wdrożenie inicjatywy zapoczątkowało opracowanie w 2014 roku NATO FMN Implementation Plan (NFIP), w czym uczestniczyły połączone siły Allied Command Transformation (ACT), Allied Command Operations (ACO) i NATO Communication and Information Agency (NCIA). Według założeń NFIP w ramach NATO powołano strukturę pod kierownictwem NATO Military Committee, która odpowiada za wdrażanie podstawowych założeń FMN, czyli współdziałanie ludzi, procesów i technologii w celu wymiany informacji i usług między jej uczestnikami. Kluczową rolę, choć niewyczerpującą wszystkich zagadnień, odgrywa

RYS. ROZWÓJ NARODOWEGO SYSTEMU TELEINFORMATYCZNEGO



Opracowanie własne.

zbiór połączonych operacyjnie, przy tym autonomicznych w zarządzaniu, sieci komputerowych. Dodatkowym zadaniem struktur FMN jest przywództwo w opracowywaniu wizji i wytycznych do jej dalszego rozwoju w NATO.

Dla zapewnienia doskonalenia przyjętych rozwiązań bez utraty ciągłej dostępności dotychczasowych przyjęto podejście spiralne, tzn. każdy kolejny poziom stanowi rozwinięcie i kontynuację poprzedniego. Poziom wymagań dla każdej kolejnej spirali jest uzgadniany i definiowany ze znacznym wyprzedzeniem czasowym w stosunku do terminu wdrożenia, co umożliwia wieloletnie planowanie technologiczne i budżetowe dalszego rozwoju sieci oraz osiąganie poziomu dojrzałości w tempie dostosowanym do potrzeb i możliwości poszczególnych państw. Obecnie zdefiniowano wymagania dla *spirali 5*, które dotyczą głównie wdrażania standaryzowanych usług funkcjonalnych w systemach FMN, czyli Functional Area Services (FAS). Do uprawnień struktur FMN należy weryfikowanie, którego poziomu spirali spełniają wymagania poszczególne państwa członkowskie i instytucje NATO. Jest to realizowane w trakcie ćwiczeń NATO, takich jak na przykład „Coalition Warrior Interoperability eXercise" (CWIX).

ROZWÓJ PMN

Pierwsza wersja narodowego systemu teleinformatycznego spełniającego założenia FMN pod nazwą ST PMN 1.0 została z sukcesem zweryfikowana podczas ćwiczeń CWIX 2016. W tym samym roku system PMN 1.0 został praktycznie wykorzystany podczas ćwiczeń międzynarodowych „Anakonda-16" do wymiany informacji niejawnych do klauzuli NATO RESTRICTED włącznie. Następnym krokiem był ST PMN 2.0, którego poziom zabezpieczeń umożliwiał bezpieczną wymianę informacji niejawnych do klauzuli NATO SECRET i został w tym charakterze wykorzystany podczas kolejnych ćwiczeń z udziałem komponentów z innych państw NATO: „Anakonda-18" i „Dragon-19".

Wypróbowano również zdolności PMN do federacji. W 2020 roku dokonano udanego połączenia ST PMN 2.0 z Mission Partnership Environment (MPE), czyli z siecią misyjną USA. Federacja ta została sprawdzona pod kątem operacyjnego wykorzy-

stania podczas ćwiczeń sił powietrznych USA w Europie „Astral Knight-20", znacząco podnosząc poziom sojuszniczej świadomości sytuacyjnej.

Obecnie ST PMN 2.0 spełnia wszystkie wymagania *spirali 2* FMN. Pakiet FAS dostępny w tym systemie, poza takimi podstawowymi, jak: e-mail, komunikacja głosowa i wideo oraz SharePoint, obejmuje również usługi specjalistyczne, do których można zaliczyć np.: JChat, JOCWatch czy ICC. Usługi ST PMN 2.0 umożliwiają wsparcie dowodzenia w następujących obszarach: planowanie operacyjne, zarządzanie kryzysowe i rozpoznanie. Oprócz zastosowań krajowych zapewniają interoperacyjność w układzie sojuszniczym. Potrzeby generowane podczas realizacji tego rodzaju przedsięwzięć są motorem napędowym dalszego rozwoju PMN w zakresie połączeń międzysystemowych oraz korzystania z wachlarza usług. Plany dalszego rozwoju przewidują osiąganie kolejnych poziomów spiral, zwiększając dostępne dla użytkowników systemu zdolności, w tym mobilności i mediów transmisyjnych, jak również umożliwiając przetwarzanie informacji niejawnych UE (rys.).

KONIECZNE SĄ WSPÓLNE PROCEDURY I JEDNOLITE WYMAGANIA TECHNICZNE, KTÓRE UMOŻLIWIĄ PAŃSTWOM NATO PRZYGOTOWANIE WSPÓLNYCH FEDERACYJNYCH SIECI TELEINFORMATYCZNYCH

WYKORZYSTANIE

Jednym z ustaleń szczytu NATO w Warszawie w 2016 roku było zapewnienie rotacyjnej obecności sił NATO w regionie bałtyckim w ramach tzw. enhanced Force Presence (eFP). Militarna aktywność wojsk Federacji Rosyjskiej i kontrolowanych przez Rosję podmiotów na terytorium Ukrainy zmusiła NATO do wzmocnienia efektu odstraszania. Zadanie koordynowania wysiłków z tym związanych zostało powierzone Wielonarodowemu Korpusowi Północno-Wschodniemu (MNC NE). Zdecydowano również o utworzeniu kolejnego międzynarodowego związku taktycznego w regionie – Wielonarodowej Dywizji Północny Wschód (MND NE). Jednym z zobowiązań naszego kraju było zapewnienie funkcjonowania systemów C2 na ich stanowiskach dowodzenia. Została w tym celu utworzona nowa instancja systemu – POL eFP, przeznaczona do sfederowania dowództwa MND NE z afiliowanymi polskimi jednostkami. Podczas kolejnych przedsięwzięć szkoleniowych wypróbowano nowe rozwiązania federacyjne. Przykładowo, w fazie przygotowania ćwiczeń „Defender Europe-20" wykorzystano federację między systemami eFP MN i MPE. Zbudowano stałe połączenie międzysystemowe między eFP MN i NATO Secret Wide Area Network (NS-WAN) zapewniające efektywną komunikację między MNC NE i strukturami Sojuszu. Umożliwiono w ten sposób NATO Joint Force Command (JFC) Brunssum zdalny dostęp do lokalizacji w eFP MN, jak również komunikację głosową (wideo) między systemami.

Takie rozwiązania teleinformatyczne skróciły czas wymagany na realizację procesu planowania i podejmowania decyzji zarówno na poziomie operacyjnym, jak i taktycznym podczas działań MNC NE oraz podległych jemu jednostek. Wykorzystanie systemu eFP MN podczas ćwiczeń „Steadfast Jupiter", w czasie których MNC NE uzyskał certyfikację, po raz kolejny dowiodło możliwości rozwiązań federacyjnych.

WNIOSKI

Wyzwania oraz dodatkowe wymagania stawiane narodowym systemom teleinformatycznym, związane z międzynarodową współpracą oraz osiąganiem wysokiego poziomu interoperacyjności podczas wspólnych zamierzeń, stanowią potężny impuls prorozwojowy. Zdobyte doświadczenia przynoszą dodatkową korzyść umożliwiającą pozyskanie nowych zdolności również w krajowych rozwiązaniach. Nawet po osiągnięciu przez struktury międzynarodowe w regionie bałtyckim dojrzałości umożliwiającej wdrożenie własnych przyszłościowych rozwiązań teleinformatycznych, wkład rodzimych specjalistów FMN w osiągnięcie dotychczasowego ich poziomu powinien zostać doceniony. Korzyść z tej współpracy jest obopólna. Konieczność zapewnienia wysokiego poziomu interoperacyjności usług C2 między strukturami NATO i Siłami Zbrojnymi RP pozostanie również w przyszłości motorem pozytywnych zmian, a podejście federacyjne, dzięki przestrzeganiu puli wspólnych standardów, pozwoli na wykorzystywanie w coraz większym stopniu możliwości jednolitego, skoordynowanego i efektywnego działania dużej liczby niejednolitych sił. ■

Bezpieczeństwo w cyberprzestrzeni

NALEŻY MIEĆ ŚWIADOMOŚĆ, ŻE SPEKTRUM NIEBEZPIECZEŃSTW, Z KTÓRYMI MOŻNA SIĘ ZETKNĄĆ W TRAKCIE UŻYTKOWANIA SYSTEMÓW TELEINFORMATYCZNYCH, JEST O WIELE WIĘKSZE.

mjr mgr Grzegorz Kaśkiewicz, kpt. mgr Marek Błachut

Technologia informacyjna (Information Technology – IT) towarzyszy nam dzisiaj w każdej dziedzinie życia. Jednak jej rozwój niesie też zwiększające się spektrum zagrożeń, w tym tych w cyberprzestrzeni. Jak wynika z raportu CERT Polska (Computer Emergency Response Team) w 2020 roku odnotowano 10 420 incydentów dotyczących cyberbezpieczeństwa, co stanowiło wzrost o ponad 60% w stosunku do roku poprzedniego. Warto zaznaczyć, że 32 incydenty zostały sklasyfikowane jako poważne, czyli takie, które istotnie wpływają na kluczowe aspekty funkcjonowania podmiotów, w tym krajowych instytucji publicznych[1]. Jak widać tendencja jest wzrostowa, dlatego też nie powinno dziwić, że w miarę zwiększającego się zagrożenia opracowuje się coraz to nowe technologie, które chronią systemy przed zakłóceniem ich funkcjonowania czy penetracją. Należy dodać, że cyberprzestrzeń ma postać przestrzeni wirtualnej, która służy komunikowaniu się, a jej byt jako obszar wymiany informacji jest uzależniony od istnienia urządzeń i systemów teleinformatycznych[2].

APARAT POJĘCIOWY

Aby przybliżyć problematykę bezpieczeństwa w cyberprzestrzeni, należy wyjaśnić kilka podstawowych pojęć z tej dziedziny. W literaturze występuje wiele definicji systemu teleinformatycznego. W rozumieniu *Ustawy z dnia 21 lipca 2000 roku – Prawo telekomunikacyjne* jest to *zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego*.

Z kolei bezpieczeństwo teleinformatyczne (Electronic Information Security – INFOSEC) można zdefiniować jako *całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemom i sieciom teleinformatycznym oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach*[3]. Zapewnia się je, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed[4]: utratą poufności, dostępności i integralności. Należy dodać, że system lub sieć teleinformatyczna są w pełni chronione, jeżeli każdy zbiór miejsc wrażliwych na atak jest zabezpieczony.

Bezpieczeństwo teleinformatyczne jest rozumiane także w kategoriach uzasadnionego poziomu zaufa-

Grzegorz Kaśkiewicz jest szefem Sekcji Wsparcia Dowodzenia i Łączności w Pułku Wsparcia Dowodzenia Wielonarodowej Dywizji Północny Wschód.

Marek Błachut jest kierownikiem Zespołu Sytemów Łączności w Instytucie Dowodzenia Akademii Wojsk Lądowych.

1 *Raport roczny z działalności CERT Polska*, NASK PIB/CERT Polska 2020, s. 13.
2 M. Czyżak, *Prawna ochrona cyberprzestrzeni państwa*, „Horyzonty Bezpieczeństwa" 2017 nr 8, s. 7, 9.
3 *Doktryna systemów łączności i informatyki Sił Zbrojnych RP D/6*, Bydgoszcz 2013, s. 22.
4 T. Malinowski, *Wykłady: Technologie w sieciach teleinformatycznych,* WAT, Warszawa 2021.

nia, że podmiot nie poniesie strat wynikających z niepożądanego ujawnienia, zmiany bądź zniszczenia informacji[5]. Składa się ono z wielu procesów zorientowanych na osiągnięcie oraz utrzymanie atrybutów bezpieczeństwa w systemach teleinformatycznych. A to z kolei gwarantuje odpowiednie zachowanie planowanego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności[6].

Jako cyberprzestrzeń należy uznać globalną domenę, w skład której wchodzą systemy i technologie informacyjne, systemy i sieci informatyczne oraz inne systemy elektroniczne wraz z pakietami danych w nich przechowywanych i przetwarzanych. Składniki te mogą być ze sobą powiązane lub mogą funkcjonować niezależnie. Jest to rozległy obszar, który trudno zamknąć w fizycznej przestrzeni.

Zagrożenia, które funkcjonują w wirtualnej przestrzeni, określane mianem *cyberzagrożeń* lub *cyberataków*, M. Marczyk interpretuje jako możliwość negatywnego wpływu na działanie podmiotów w cyberprzestrzeni[7]. W zasadzie każde nieuprawnione i celowe działanie, mające na celu pozyskanie lub zniszczenie informacji, a także zakłócenie sprawnego funkcjonowania systemu teleinformatycznego, powinno się rozpatrywać w kategoriach cyberataku.

ZAGROŻENIA I MECHANIZMY OCHRONY

Atak sieciowy polega na kradzieży poufnych lub prywatnych informacji. W wyniku tego dochodzi do dowolnej zmiany lub usunięcia danych, zmiany ustawień konfiguracyjnych lub zablokowania usługi[8]. Ataki sieciowe ze względu na źródło możemy podzielić na[9]:

– wewnętrzny (lokalny), polega na tym, że jest przeprowadzany z systemu znajdującego się w sieci lub z wykorzystaniem fizycznego dostępu do urządzenia;

– zewnętrzny (zdalny), przeprowadzany z systemów znajdujących się poza atakowaną siecią. Ataki te kwalifikuje się dzięki przypisaniu do poszczególnych warstw modelu TCP/IP;

– pośredni, polegający na tym, że ataki są przeprowadzane za pomocą systemów i urządzeń pośredniczących. Ma to służyć ukryciu właściwego jego źródła[10];

– bezpośredni, czyli ukierunkowany atak na system, przeprowadzany (zdalnie lub lokalnie) bez wykorzystywania żadnych innych systemów i urządzeń pośredniczących. Jest to atak przez wykryte luki, których specyfika nie wymagała wykorzystania pośredników do przekazania strumienia ataku[11].

Przykładowe ataki sieciowe to:

– DoS (Denial of Service) – powoduje, że atakowany system w wyniku zapełnienia portu serwera nieprawidłowymi pakietami przestaje prawidłowo działać. Przykład usterki, usługi internetowej (np. www) lub całego serwera;

– DDoS (Distributed Denial of Service) – ulepszona odmiana ataku DoS. Polega na jednoczesnym atakowaniu ofiary (użytkownika) z wielu miejsc za pomocą kontrolowanego oprogramowania (tzn. botów i trojanów) przejętych komputerów. Komputery na dany sygnał zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora), co przy bardzo dużej ilości żądań prowadzi do wyczerpania jego dostępnych zasobów. Efektem tego jest przerwa w działaniu lub nawet zawieszenie systemu. Typowy atak DDoS wymaga obecności czterech elementów[12]: atakującego (Client), węzłów głównych (Handler), agentów (Agent) i ofiary (Client, użytkownik);

– Email Bombing – efekt wysyłania komuś dużej liczby e-maili, co prowadzi do przeładowania jego skrzynki pocztowej lub sieciowego połączenia. Skrzynka może w wyniku tego przepełnienia zablokować się;

– Teardrop IP Attack – polega na wykorzystaniu błędu protokołu IP. Wymaga on zbyt dużego pakietu danych, który nie może być przesłany przez następny router, dlatego też jest dzielony na części. Fragment pakietu rozpoznaje miejsce, w którym zaczyna się pierwsza część pakietu i uruchamia proces łączenia wszystkich fragmentów w całość. Osoba atakująca zmienia fragment odpowiedzialny za odnalezienie początku pakietu i rozpoczęcie procesu scalania, przez co system ma problemy z poskładaniem pakietu w całość i przesłaniem go dalej. To najczęściej doprowadza do zawieszenia systemu;

– SQL Injection – to nieuprawniony dostęp do bazy danych dzięki odpowiedniej manipulacji aplikacją, która komunikuje się z ową bazą danych. Polega to na spreparowaniu specjalnego ciągu i wprowadzeniu go do aplikacji przez pasek URL lub formularz on-line. Spreparowanym ciągiem może być czyste wyrażenie SQL lub charakterystyczny dla danej platformy język komunikacji z nią. Podatna aplikacja pobiera dane od

5 K. Liderman, *System bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" 2002 nr 17, s. 82.

6 Ibidem, s. 480–481.

7 M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018 nr 1–2, s. 67.

8 http://dlmas2k17.prv.pl/. 9.01.2022.

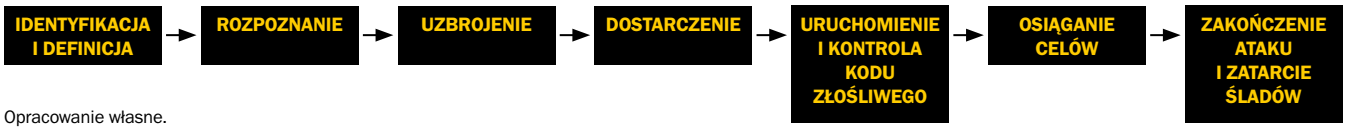
9 Ibidem.

10 A. Chojnowski, *Bezpieczeństwo komputerowe, Prawo a bezpieczeństwo,* t. I, Warszawa 2021, s. 85.

11 Ibidem.

12 https://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g6/Ela/DoS.html/. 10.01.2022.
https://www.komputerswiat.pl/zapora-ogniowa/. 10.01.2022.

RYS. 1. ETAPY OGÓLNEGO PROCESU CYBERATAKU



Opracowanie własne.

atakującego i wykonuje zapytania SQL, bez wcześniejszego sprawdzenia, czy dane te są poprawnym czystym tekstem. Dzięki temu włamywacz otrzymuje możliwość modyfikacji oraz usuwania czy dodawania nowych wpisów w bazie danych;

– DNS Spoofing – atak na serwer DNS, który ma bazę danych przechowującą numery IP dla poszczególnych adresów mnemonicznych. Atak tego typu polega na ingerencji w tablicę DNS i modyfikacji poszczególnych wpisów tak, by klient zamiast do komputera docelowego był kierowany do komputera atakującego;

– atak Man-in-the-Middle (MITM) – dochodzi w nim do kradzieży danych przesyłanych między dwoma obiektami, np. z wykorzystaniem punktów dostępowych Wi-Fi. Agresor może podszyć się pod jedną ze stron w celu przechwycenia informacji. Warunkiem powodzenia ataku jest niezauważalność napastnika zarówno przez ofiarę, jak i zasób, pod który podszywa się atakujący;

– wyłudzanie informacji – to jeden z najprostszych ataków, który nie wymaga od napastnika ani specjalistycznej wiedzy, ani zaawansowanego sprzętu. Bazuje na nieświadomości i łatwowierności ofiary. Zwykle ma postać wiadomości e-mail, która stwarza wrażenie bezpiecznej i nie budzi żadnych podejrzeń. Tym samym użytkownik bez jakichkolwiek podejrzeń otwiera wiadomość i wykonuje czynności w niej opisane, udostępniając napastnikowi dane wrażliwe.

Do zabezpieczenia sieci używane są takie narzędzia i aplikacje (mechanizmy), jak:

– zapora ogniowa (firewall) – jest to sprzętowy lub programowy mechanizm bezpieczeństwa, który blokuje dostęp osób niepowołanych do sieci lub systemu czy urządzenia. Chroni przed próbami włamania bezpośrednio na komputer. Dodatkowo połączenia wychodzące i wchodzące są filtrowane, a działania uznane za niebezpieczne blokowane, dzięki czemu dane są bezpieczne[13];

– broker spamu – jest oprogramowaniem zainstalowanym na serwerze lub komputerze, które identyfikuje i usuwa niechciane wiadomości[14];

– Malware Hunter Pro – zapewnia kompleksową ochronę w czasie rzeczywistym przed wszystkimi rodzajami zagrożeń, zabezpiecza dane i chroni prywatność. Jest dobrym uzupełnieniem podstawowego antywirusa[15];

– ochrona przed Spyware – oprogramowanie służące do wykrywania i usuwania spyware[16] i adware[17];

– bloker wyskakujących okienek – służy do zabezpieczenia wyskakujących niechcianych okienek z reklamami[18];

– ochrona przed wirusami – oprogramowanie wspomaga użytkownika lub serwer, wykrywając i usuwając: wirusy, robaki czy konie trojańskie z plików oraz wiadomości e- mail[19].

ETAPY ATAKU CYBERNETYCZNEGO

Wielu ludzi odbiera cyberatak jako pojedyncze zdarzenie. Jednak rzeczywistość pokazuje, że jest to cykl wieloetapowy, w którym poszczególne czynności mają swoją określoną kolejność, czas i miejsce. Są one połączone w fazy i tworzą swojego rodzaju proces, którego poznanie może pomóc w lepszym przygotowaniu się do potencjalnego zagrożenia, zidentyfikowania zaczynającego się ataku czy zmniejszenia potencjalnych efektów jego oddziaływania.

W literaturze przedmiotu istnieje wiele przykładów cyberataku. Uogólniony cykl, łączący wiele innych koncepcji, przedstawia Romuald Hoffman w swoim artykule. Dzieli on ten cykl na siedem faz (rys. 1)[20]:

13 https://www.komputerswiat.pl/zapora-ogniowa/. 10.01.2022.

14 D. Chaładyniak, *Podstawy bezpieczeństwa sieciowego,* Warszawa 2009, s. 12.

15 https://www.komputerswiat.pl/poradniki/programy/malware-hunter-pro-za-darmo-dla-czytelnikow-komputer-swiata/b0g9qvl/. 10.01.2022.

16 Spyware to złośliwe oprogramowanie szpiegujące, które atakuje komputer, przenika przez zabezpieczenia i infekuje system. Oprogramowanie instaluje się zazwyczaj bez naszej zgody i wiedzy, następnie działa cichutko w tle i zbiera cenne informacje na nasz temat. Monitoruje nasze kroki, kradnie poufne dane osobowe lub hasła dostępu, w efekcie może powodować poważne szkody.

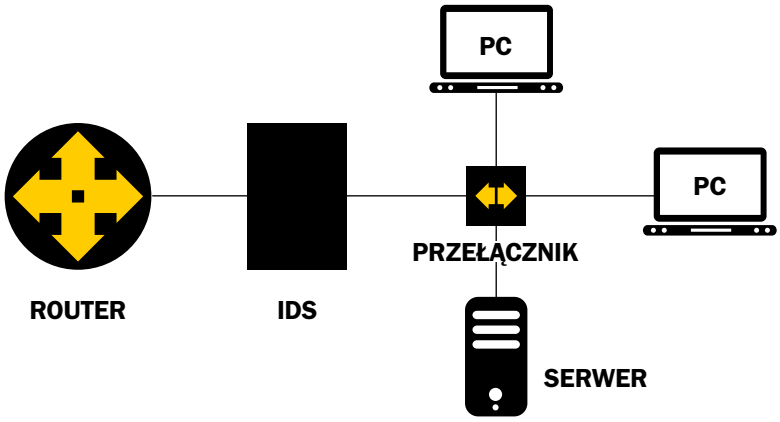
17 Adware to typ złośliwego oprogramowania malware, które wyświetla w nachalny sposób niechciane reklamy, zwykle w formie bannerów, wyskakujących okien lub paska narzędzi w przeglądarce, zwanego toolbarem.

18 D. Chaładyniak, *Podstawy bezpieczeństwa...,* op.cit. s. 12.

19 Ibidem, s. 12–13.

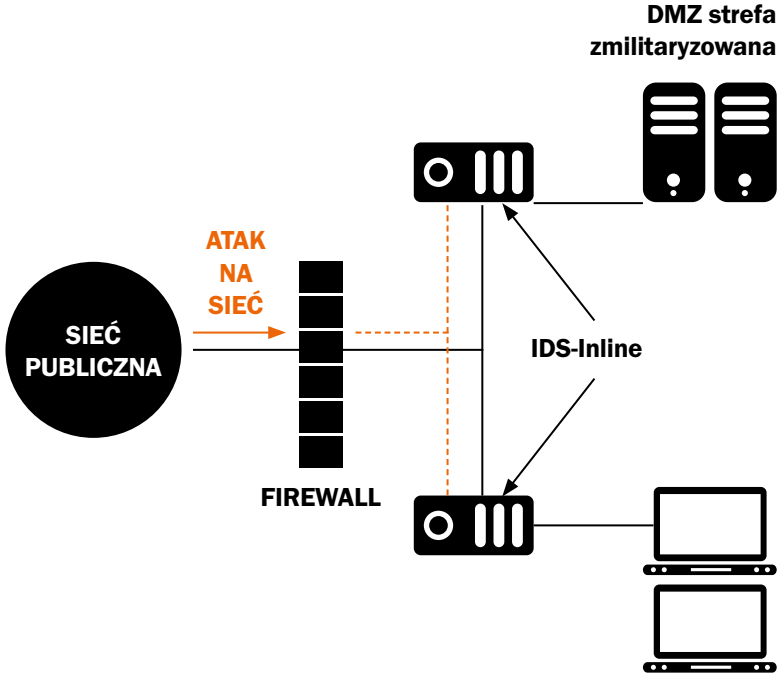
20 R. Hofmann, *Ogólny cykl życia ataku cybernetycznego i jego markowski model,* „Ekonomiczne Problemy Usług" 2018 nr 2, s. 124.

RYS. 2. SCHEMAT SYSTEMU WYKRYWANIA INTRUZÓW IDS



Opracowano na podstawie: https://sieci.infopl.info/index.php/bezpieczenstwo/ids/. 11.01.2022.

RYS. 3. SCHEMAT SYSTEMU WYKRYWANIA ATAKÓW IDS-INLINE



Opracowano na podstawie: https://sieci.infopl.info/index.php/bezpieczenstwo/ids/. 12.01.2022.

– identyfikacja i definicja – w tej fazie napastnik określa podmiot ataku oraz cel, jaki chce osiągnąć. Następuje tu również wstępne planowanie czasu oraz narzędzi;

– rozpoznanie – polega na wnikliwej analizie środowiska, w którym odbędzie się atak pod kątem potencjalnych luk lub podatności ułatwiających działanie. Wyciągnięte wnioski przyczyniają się do skonkretyzowania czasu oraz użytych narzędzi;

– uzbrojenie – tu następuje przygotowanie cyberbroni (np. wirusów) oraz narzędzi służących do ich dostarczenia (tzw. weaponizer);

– dostarczenie – czyli dystrybucja narzędzia z cyberbronią do środowiska docelowego;

– uruchomienie i kontrola kodu złośliwego – faza polegająca na aktywacji cyberbroni oraz na sterowaniu jej działaniem. W zależności od zakładanych celów oraz poziomu technicznego agresora aktywacja może być realizowana automatycznie lub w sposób zdalny. W tej fazie może też nastąpić rozszerzenie złośliwego kodu źródłowego, jego modyfikacja lub wprowadzenie dodatkowego narzędzia ataku;

– realizacja celów – tu atakujący podejmuje określone czynności ukierunkowane na osiągnięcie zakładanych celów. Faza ta może się wiązać z jedną czynnością (np. skopiowanie danych) lub składać się z wielu złożonych działań (np. przejęcie konta pocztowego i wykorzystywanie go do rozprzestrzeniania ataku w szerszym środowisku). Może tu również dojść do częściowego lub całkowitego zniszczenia infrastruktury systemu;

– zakończenie ataku i zatarcie śladów – faza ma charakter opcjonalny. Często zdarza się, że nie występuje. Napastnik, gdy osiągnie oczekiwane efekty, nie zadaje sobie trudu, aby ukryć swoje działanie. Jednak w niektórych sytuacjach, jeśli agresor planuje ponowienie ataku, w sposób kontrolowany dezaktywuje złośliwy kod oraz usuwa lub maskuje pozostawione ślady.

WYBRANE SYSTEMY I NARZĘDZIA WYKRYWANIA WŁAMAŃ

System wykrywania intruzów (Intrusion Detection Systems – IDS) zajmuje się wykrywaniem (identyfikacją) prób uzyskania dostępu do systemu (rys. 2). Jego zadanie polega na wykryciu takiego zdarzenia i poinformowaniu o tym odpowiednich osób. Podstawowe zadania IDS to monitorowanie systemu, detekcja ataków i podejmowanie stosownych działań w zależności od zagrożeń, takich jak[21]: wylogowanie użytkowników czy zablokowanie konta lub wykonanie odpowiednich skryptów.

Najczęściej informacja o ataku jest natychmiast przesyłana do upoważnionych osób, np. e-mailem. Celem stosowania IDS-ów jest[22]: wykrywanie ataków,

21 https://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html /. 11.01.2022.

22 https://sieci.infopl.info/index.php/bezpieczenstwo/ids/. 12.01.2022.

zapobieganie nim, gromadzenie dowodów i monitorowanie strategii.

Rodzaje systemów wykrywania intruzów[23]:

– serwerowy SIDS (Server Intrusion Detection System) – jest zainstalowany na wybranym serwerze i jego zadaniem jest identyfikowanie ataków na ten konkretny serwer;

– wykrywania komputera HIDS (Host Intrusion Detection System) – działa na niezależnych hostach i urządzaniach sieciowych, monitorując wychodzące pakiety z konkretnych urządzeń;

– sieciowy NIDS (Network Intrusion Detection System) – znajduje się na dedykowanym urządzeniu i obserwuje cały ruch w swojej sieci. Identyfikuje wszystkie ataki skierowane przeciwko elementom;

– protokolarny PIDS (Protocol-based Intrusion Detection System) – monitoruje konkretny ruch sieciowy między serwerem a klientem;

– protokół aplikacji APIDS (Application Protocol-based Intrusion Detection System) – identyfikuje włamania do konkretnych aplikacji, np. zdalne ataki na SQL.

Sieciowe systemy wykrywania intruzów (IDS-Inline) z reguły mają dwie karty sieciowe: zewnętrzną i wewnętrzną. Jedna służy do wykrywania zagrożeń, druga zaś do zastosowań standardowych. Cały monitorowany ruch sieciowy przechodzi przez urządzenie. Przypomina to budowę firewalla, jednak w środku działa silnik IDS, który wykrywa ataki i umie je blokować. Urządzenie pełni podobne funkcje jak firewall, jednak działa w inny sposób. Istotą działania IDS jest wykrywanie prób ataku, dlatego też IDS-Inline, chociaż jest umieszczony w tym samym miejscu co firewall, to działa w ten sposób, że przepuszcza cały ruch oprócz tego, co uzna za próbę ataku (rys. 3).

Systemy IDS wykrywają takie zagrożenia, jak[24]:

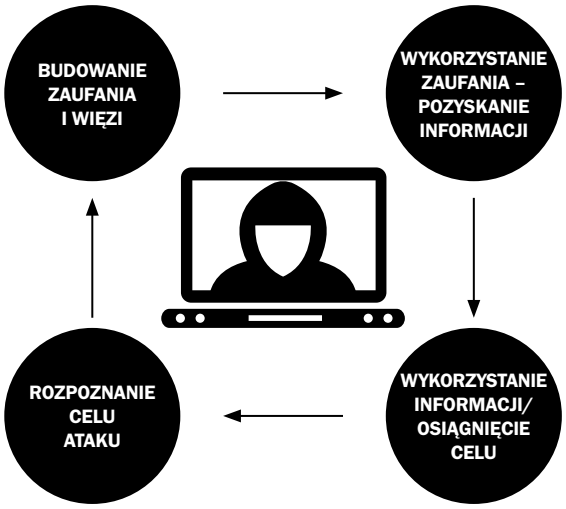
– skalowanie sieci – polega na tym, że każdy atak rozpoczyna się rozpoznaniem sieciowym, przez poznawanie topologii hostów i otwartych portów;

– ataki na konkretnych protokołach, takich jak: z wykorzystaniem PING, LDAP, za pośrednictwem DNS, exploitacja SMB;

– rozprzestrzeniania ransomware[25], które próbuje rozprzestrzenić się na innych komputerach w sieci, szyfrując jak największą liczbę plików, np. atak WannaCry[26];

– ataki DDoS, czyli zwiększenie ilości w sieci połączeń przychodzących do konkretnego hosta bądź usługi;

RYS. 2. CYKL ATAKU SOCJOTECHNICZNEGO



Opracowanie własne.

– błędy konfiguracji sieci, np. asymetryczny routing czy otwarte porty, które mogą być wykorzystane przez hakerów.

System IDS potrafi wykryć niemal każde zagrożenie, które polega na specyficznej komunikacji sieciowej. Jednak nie zatrzymuje złośliwego oprogramowania (np. malware). Program, który działa lokalnie, zaszywa się w pamięci hosta, następnie nierozprzestrzenia się na zewnątrz, a IDS go nie wykrywa. Mimo to technologia IDS nadal powinna mieć swoje miejsce w każdej większej sieci teleinformatycznej.

Ze względu na wykorzystywane techniki analizy systemy IDS dzielimy na[27]:

- systemy wykrywania nadużyć (misuse) – wykrywające znane ataki z użyciem określonych, specyficznych dla nich cech–sygnatur. Podstawowe ich zalety i wady to[28]:

– wykrywanie nadużyć jest niezwykle skuteczną metodą wykrywania włamań, wolną od generowania ogromnej liczby fałszywych alarmów;

– możliwe jest szybkie i trafne wykrycie zastosowanej metody lub narzędzia ataku, co pozwala osobie odpowiedzialnej za bezpieczeństwo podjąć odpowiednie środki zaradcze;

23 Ibidem.

24 Ibidem.

25 Oprogramowanie wymuszające okup, złośliwe oprogramowanie, blokuje użytkownikom dostęp do ich systemów lub plików osobistych, następnie żąda uiszczenia opłaty w zamian za jego przywrócenie.

26 Program, który atakuje sieci korzystające z protokołu SMBv1 ułatwiającego komunikację między komputerami a drukarkami i innymi urządzeniami w sieci.

27 P. Kukiełka, Z. Kotulski, *Systemy wykrywania intruzów wykorzystujące metody sztucznej inteligencji*, „Przegląd Telekomunikacyjny" 2011 nr 4, s. 114.

28 https://edu.pjwstk.edu.pl/wyklady/bsi/scb/main86.html /. 8.02.2022.

– umożliwiają łatwe wyśledzenie problemów związanych z bezpieczeństwem nawet mniej zaawansowanym administratorom;

– metoda wykrywania nadużyć pozwala wykryć tylko znane wcześniej typy ataków. Ważne jest, aby dbać o aktualność naszej bazy wzorców ataków (bazy sygnatur);

– porównuje sygnatury w celu wykrycia włamania, przez co czasami powoduje niemożność detekcji nieco zmodyfikowanej wersji ataku na system;

• systemy wykrywania anomalii (anomaly) – wykrywające niezwyczajne zachowania na komputerze lub w sieci, które mogą świadczyć o działaniu intruza. System IDS, opierający się na wykorzystywaniu anomalii, jest bardziej skuteczny od systemu wykrywania nadużyć przy stosowaniu nieznanych, nowych typów ataków. Do jego zalet i wad możemy zaliczyć[29]:

– system potrafi wykryć dziwne zachowania. Dzięki temu ma możliwość wykrycia symptomów ataku bez specyficznej wiedzy o nim samym;

– detektory anomalii mogą generować dane wykorzystywane później do definiowania sygnatur dla detektorów nadużyć;

– detektory anomalii zwykle generują dużą liczbę fałszywych alarmów, co powoduje, że nie zawsze możliwe są do przewidzenia zachowania użytkowników bądź sieci;

– metoda systemu często wymaga rozległych zbiorów treningowych wydarzeń systemowych w celu zdefiniowania normalnego jego zachowania.

Ze względu na źródła wykorzystywanych informacji systemy IDS dzielimy na:

• lokalne IDS – HIDS (Host Based IDS) – to najwcześniej zaimplementowane systemy wykrywania intruzów. Biorą one pod uwagę informacje, jakie można pobrać bezpośrednio z chronionego komputera (hosta). Mogą to być, np. logi systemowe, logi aplikacji korzystających z sieci IP lub informacje zawarte w plikach audytu systemu operacyjnego;

• sieciowe IDS – NIDS (Network Based IDS) – analizują informacje w sieci przepływające między hostami, które są połączone za pomocą różnych mediów z wykorzystaniem różnych protokołów transmisji. Polega to na sprawdzaniu pakietów poruszających się po sieci, które są analizowane, następnie określane jako prawidłowe bądź złośliwe. System ten dobrze sobie radzi z nieautoryzowanym dostępem spoza systemu oraz z atakiem typu Denial of Service (zauważając pakiety zaczynające taki atak).

Przedstawione podejścia do systemów wykrywania intruzów różnią się znacznie, ale zastosowane jednocześnie doskonale się uzupełniają. Ciekawym pomysłem jest wprowadzenie rozproszonej sieci agentów, z których każdy działa tak, jakby był gospodarzem systemu i wymienia się informacjami z innymi agentami. Właściwa implementacja systemu IDS powinna integrować cały system wykrywania intruzów w takim stopniu, aby jej efekty nie były odróżnialne od pracy Host-Based IDS, umieszczonego w jednym, centralnym punkcie, zachowując się jak System Real-Time[30]. Zachowanie to polega na równoległym prowadzonym obliczaniu z przebiegiem zewnętrznego procesu. Celem tego jest nadzorowanie, sterowanie oraz reagowanie na zachodzące w tym procesie zdarzenia[31].

ŚWIADOMOŚĆ UŻYTKOWNIKA A OCHRONA INFORMACJI

Mimo zastosowania bardzo skomplikowanych zabezpieczeń hardware'owych[32] oraz software'owych[33], a także mnóstwa systemów wykrywających potencjalne zagrożenia, nie zawsze udaje się uniknąć ataków cybernetycznych na systemy teleinformatyczne. Wynika to często z osłabienia czujności użytkowników, którzy ślepo ufają zastosowanym technologiom bezpieczeństwa. W takiej sytuacji czynnik ludzki staje się najsłabszym ogniwem, gdyż złamanie bariery ludzkiej jest łatwiejsze niż pokonanie zaawansowanych technologii. Taki użytkownik będzie wówczas głównym celem ataku socjotechnicznego, który na każdym etapie może pozostać niezauważony (rys. 4).

Często atak na system bezpieczeństwa rozpoczyna się od pozyskania potencjalnie jawnej, nic nie znaczącej i ogólnie dostępnej informacji, która w rękach socjotechnika hakera jest cennym narzędziem do przeprowadzenia dalszych kroków. Może to polegać na analizie informacji pozyskanych ze stron internetowych organizacji, artykułów z prasy czy telewizji, z zawartości śmietników (!) lub z bezpośredniej rozmowy z pracownikiem. Etap rozpoznania jest niezwykle ważnym elementem ataku, pozwalającym na znalezienie luk w systemie bezpieczeństwa, określenie ilości i kolejności kroków potrzebnych do uzyskania celu oraz na wskazanie potencjalnej ofiary, na którą atak będzie stosunkowo prosty i zapewniający największe prawdopodobieństwo sukcesu.

Przy bezpośrednim ataku na użytkownika socjotechnik może się podać za pracownika tej samej organizacji lub za inną osobę z nią współpracującą. Będzie zdawał sobie sprawę, że w czasie rozmowy może napotkać na problemy. Będzie też przewidywał, że z pewnością pojawią się trudne pytania ze strony ofiary, wynikające z jej podejrzliwości. Dlate-

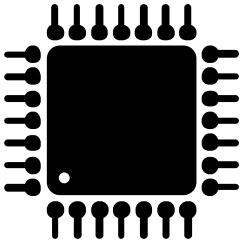
29 Ibidem.

30 https://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html/. 12.01.2022.

31 J. Ułasiewicz, *Wykład: komputerowe systemy sterowania, systemy czasu rzeczywistego – wstęp,* Instytut Cybernetyki Technicznej Politechniki Wrocławskiej, Wrocław 2019, s. 5.

32 Hardware – fizyczna, materialna część komputera, ogólnie cały sprzęt informatyczny.

33 Software – oprogramowanie implementowane na sprzęcie informatycznym lub w systemie teleinformatycznym.



RYS. 5. CYKL ŻYCIA SYSTEMU TELEINFORMATYCZNEGO

Opracowanie własne.

go będzie dokładnie planował swój atak. Jedną z najskuteczniejszych technik jest zbudowanie zaufania z atakowanym. W tym przypadku zasada jest prosta – im bardziej rozmowa dotyczy spraw codziennych, z pojawiającymi się nazwiskami czy imionami osób z otoczenia ofiary, tym mniejsza szansa na podejrzenia. Człowiek zaczyna ufać rozmówcy, który zna okoliczne środowisko.

Kolejną techniką pomagającą zbudować silne więzi z użytkownikiem jest zaoferowanie przez napastnika potencjalnej pomocy. Zdaje sobie on sprawę, że każdy człowiek czuje się wdzięczny i zobowiązany za okazaną pomoc w rozwiązaniu problemu. Oczywiście problem nie występuje realnie, lecz jest zaaranżowany przez socjotechnika lub odnosi się do problemów z przeszłości.

Odwrócenie ról, czyli prośba atakującego o pomoc, stanowi trzecią technikę budowania więzi z ofiarą. W tym wypadku socjotechnik wykorzystuje współczucie – jako główną słabość ofiary.

Opisane techniki mogą występować niezależnie, ale mogą również być skorelowane i stanowić kolejne kroki w procesie budowania zaufania i więzi z atakowanym użytkownikiem.

Następnym etapem ataku socjotechnicznego jest wykorzystanie pozyskanego zaufania. Wtedy to uzyskanie potrzebnych informacji (np. kodów, haseł, loginów) czy określonych czynności (np. odbiór poczty ze złośliwym oprogramowaniem, udostępnienie konta e-mail) jest kwestią czasu. Ofiara jest tak długo manipulowana, aż informacje czy działania będą zadowalające dla socjotechnika.

Następnie napastnik wykorzystuje informację lub działanie do osiągnięcia zakładanego celu. W tym momencie atak socjotechniczny może zostać zakończony lub, jeśli ostateczny efekt nie został osiągnięty, proces jest powtarzany, aż do uzyskania pełnego sukcesu.

UŚWIADAMIANIE UŻYTKOWNIKA

Tak naprawdę nie istnieje taka technologia czy procedura, która w pełni ochroni przed atakiem socjotechnicznym. Ale wykorzystując pewne narzędzia, możemy zminimalizować zagrożenie.

Pierwszym i zasadniczym krokiem jest uświadomienie użytkowników, że w wirtualnej przestrzeni funkcjonują ludzie, którzy za pomocą manipulacji i socjotechnik będą próbować zaatakować. Członkowie organizacji muszą wiedzieć, jakie informacje (również te potencjalnie nieistotne) powinny być strzeżone i jak to robić na co dzień. Powinni również znać sposoby manipulacji – wówczas łatwiej im będzie rozpoznać potencjalny atak i zerwać kontakt z napastnikiem.

Narzędziem do osiągnięcia tego celu może być prowadzenie cyklicznych i obowiązkowych szkoleń z użytkownikami. Niezwykle ważne jest, by szkoleniem objąć wszystkich pracowników korzystających z systemu. Nie powinno ono ograniczyć się jedynie do przedstawienia informacji dotyczących bezpieczeństwa systemu. Powinno wzbudzić w członkach organizacji chęć współpracy oraz niwelować skłonność do omijania lub całkowitego deprecjonowania zaleceń. Program szkolenia powinien być również zróżnicowany i dostosowany do określonych grup pracowników. Szkolenie powinno być ukierunkowane na:

– zapoznanie z polityką bezpieczeństwa i procedurami bezpiecznej eksploatacji systemu w kontekście specyfiki codziennych obowiązków szkolonej grupy;

– zmotywowanie członków organizacji do stosowania założonych procedur bezpieczeństwa dzięki opisaniu korzyści płynących dla organizacji oraz ich samych lub zagrożeń związanych ze skutkami ataków – łącznie z rozwiązaniem organizacji, a tym samym utratą posady przez pracowników;

– podkreślenie roli, jaką odgrywają w systemie bezpieczeństwa pojedynczy pracownicy;

– uświadomienie, że ochrona informacji to jeden z podstawowych obowiązków każdego członka organizacji;

– przedstawienie przykładów technik i metod stosowanych podczas ataków socjotechnicznych oraz sposobów ich udaremnienia;

– sprawdzenie poziomu wiedzy opanowanej podczas szkolenia.

OCHRONA INFORMACJI W WOJSKOWYM SYSTEMIE TELEINFORMATYCZNYM

Proces powoływania do życia systemu teleinformatycznego jest kilkustopniowy i wymaga od jego organizatora spełnienia określonych warunków, związanych z bezpieczeństwem użytkowania systemu oraz bezpieczeństwem przetwarzanych w nim informacji (rys. 5). Każdy system teleinformatyczny przetwarzający informacje niejawne musi mieć opracowaną dokumentację bezpieczeństwa teleinformatycznego. W jej skład wchodzą[34]:

– szczególne wymagania bezpieczeństwa – zawierają efekty procesu szacowania ryzyka dla przetwarzanych w systemie informacji oraz sposoby uzyskania akceptowalnego poziomu bezpieczeństwa systemu;

– procedury bezpiecznej eksploatacji – obejmują sposoby postępowania i algorytmy działania użytkowników w celu zachowania bezpieczeństwa informacji, opisują zakres odpowiedzialności poszczególnych osób, które mają dostęp do systemu, określają sposób implementacji oraz wykorzystania zastosowanych w systemie zasad oraz narzędzi bezpieczeństwa.

Podczas szacowania ryzyka dla bezpieczeństwa informacji należy pamiętać, że odpowiedzialność za zaakceptowanie poziomu ryzyka w systemie spada na jego organizatora. On też sprawuje nadzór nad organizacją bezpieczeństwa teleinformatycznego systemu.

W wypadku rozległych systemów teleinformatycznych, czyli funkcjonujących w więcej niż jednej jednostce organizacyjnej, opracowuje się ogólnosystemową dokumentację bezpieczeństwa, w której określa się minimalne wymagania bezpieczeństwa stawiane komponentom lokalnym, oraz opisuje sposób i zakres wykonania załączników do dokumentacji bezpieczeństwa. Poszczególne lokalizacje dołącza się do systemu na podstawie przedmiotowych załączników, za opracowanie których odpowiedzialność biorą kierownicy jednostek organizacyjnych uruchamiających komponent lokalny.

Kolejnym krokiem, niezbędnym do uruchomienia systemu, jest jego akredytacja, czyli dopuszczenie systemu do jego wykorzystania. Organem właściwym do jej udzielenia jest[35]:

– organizator systemu – dla systemów teleinformatycznych przetwarzających informacje klauzuli „zastrzeżone";

– Służba Kontrwywiadu Wojskowego – dla systemów przeznaczonych do przetwarzania informacji o klauzuli „poufne" lub wyższej oraz niejawnych informacji międzynarodowych.

Warunkiem dopuszczenia do rozpoczęcia przetwarzania informacji niejawnych w systemie jest zatwierdzenie dokumentacji bezpieczeństwa przez organizatora systemu (w odniesieniu do informacji o klauzuli „zastrzeżone") lub pisemna zgoda uzyskana od Służby Kontrwywiadu Wojskowego (w wypadku informacji „poufnych" i wyższych oraz informacji niejawnych międzynarodowych).

Dopiero po uzyskaniu akredytacji system może zostać uruchomiony w określonej komórce organizacyjnej. Informację o tym ujmuje się w rozkazie lub w decyzji kierownika jednostki organizacyjnej. W rozkazie lub w decyzji kierownika jednostki organizacyjnej musi zostać ujęte również wyłączenie systemu. Ponadto w razie wycofania z eksploatacji systemu przetwarzającego wiadomości o klauzuli „poufne" lub wyższe organizator systemu jest zobowiązany do zwrócenia świadectwa akredytacji do organu, który je wydał.

Zakres zadań w aspekcie bezpieczeństwa systemów teleinformatycznych w jednostce organizacyjnej podporządkowanej ministrowi obrony narodowej został opisany w zarządzeniu nr 7/MON. Uwzględnia się w nim wszystkie osoby funkcyjne biorące udział w tworzeniu bezpieczeństwa systemu teleinformatycznego. Ze względu na ich udział w tym procesie oraz funkcje pełnione w jednostce organizacyjnej możemy ich podzielić na:

– personel kierowniczy: kierownik jednostki organizacyjnej lub komórki organizacyjnej;

– personel bezpieczeństwa: pełnomocnik ochrony, inspektor bezpieczeństwa teleinformatycznego, administrator systemu, oficer bezpieczeństwa systemów łączności i informatyki.

Kierownik jednostki organizacyjnej jest głównym odpowiedzialnym za właściwą eksploatację systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej, w tym za ich bezpieczeństwo. W zakresie dokumentacji bezpieczeństwa nadzoruje proces ich powstawania oraz akceptuje efekty procesu szacowania ryzyka dla informacji przetwarzanych w organizowanych systemach. To on wyznacza osoby funkcyjne dla systemów wymagane przez dokumentację bezpieczeństwa. Dla systemów organizowanych w podległych jednostkach organizacyjnych przetwarzających informacje o klauzuli „zastrzeżone" kierownik jednostki organizacyjnej jest władzą akredytacyjną – udziela zgody na eksploatację systemu. Ponadto jest odpowiedzialny za kontakt ze Służbą Kontrwywiadu Wojskowego w zakresie:

– weryfikacji poprawności zakredytowanych przez siebie systemów;

– przeprowadzenia niebędącej w jego zakresie kompetencji akredytacji pozostałych systemów (w tym przetwarzających informacje niejawne międzynarodowe);

– przeprowadzania badań laboratoryjnych sprzętu pod kątem klasy urządzenia lub technicznego pozio-

34 *Decyzja Nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej,* Dz.Urz. MON 2012.8 z dnia 09.02.2012, s. 3.

35 Ibidem.

mu zabezpieczenia urządzenia, a także wyznaczenia poziomu zabezpieczenia miejsc rozwinięcia systemu;

– dopuszczenia do eksploatacji w systemie urządzeń kryptograficznych oraz certyfikowania środków ochrony elektromagnetycznej.

Kierownik komórki organizacyjnej – adekwatnie do zajmowanego stanowiska – odpowiada za bezpieczne funkcjonowanie systemów teleinformatycznych w komórce organizacyjnej. Zakres jego odpowiedzialności może być większy w wypadku wyznaczenia go przez kierownika jednostki organizacyjnej na organizatora systemu. Wówczas zadania ciążące na kierowniku komórki organizacyjnej są takie same jak kierownika jednostki organizacyjnej.

Pełnomocnik ochrony to osoba funkcyjna, która odpowiada za całe spektrum zadań związanych z zapewnieniem ochrony systemów teleinformatycznych z pominięciem ochrony kryptograficznej. Zadania te można pogrupować ze względu na przedmiot zainteresowania:

– procedury, przepisy, dokumenty – czuwanie nad zapewnieniem przestrzegania przepisów ochrony informacji niejawnych przetwarzanych w systemach, przeprowadzenie szacowania ryzyka dla bezpieczeństwa informacji niejawnych, współtworzenie projektów planowanych do budowy systemów teleinformatycznych, współuczestniczenie oraz uzgadnianie dokumentacji bezpieczeństwa dla systemów;

– techniczne aspekty funkcjonowania – ewidencja systemów teleinformatycznych użytkowanych w jednostce organizacyjnej oraz środków ochrony elektromagnetycznej, a także nadzór nad zmianami rekonfiguracyjnymi systemów;

– fizyczna ochrona – organizacja fizycznych zabezpieczeń miejsc rozwinięcia komponentów lokalnych. Ważnym aspektem tego zadania jest ścisła współpraca pełnomocnika z komendantem ochrony jednostki organizacyjnej w zakresie bezpieczeństwa fizycznego;

– przygotowanie użytkowników – przeprowadzanie cyklicznych szkoleń dla użytkowników końcowych systemów podnoszące ich wiedzę na temat zasad bezpieczeństwa oraz świadomości w kwestii potencjalnych zagrożeń dla użytkowanych systemów.

Odpowiedzialność *inspektora bezpieczeństwa teleinformatycznego* (IBT) obejmuje sprawdzanie systemu wraz z jego wszystkimi elementami (oprogramowanie, elementy serwerowe, elementy strukturalne, urządzenia końcowe, środki bezpieczeństwa fizycznego i ochrony elektromagnetycznej) pod kątem zgodności z dokumentacją bezpieczeństwa. Weryfikacja odnosi się także do poprawności czynności wykonywanych przez administratorów systemu z uwzględnieniem prawidłowości archiwizowania rejestrów zdarzeń, zakładania kont użytkownikom oraz zakresu nadawanych im uprawnień, a także przestrzegania przez użytkowników procedur bezpieczeństwa. W razie stwierdzenia jakichkolwiek nieprawidłowości czy zdarzeń mogących mieć wpływ na bezpieczeństwo systemu IBT, przekazuje te informacje pełnomocnikowi. Ponadto inspektor bezpieczeństwa teleinformatycznego uczestniczy w opracowywaniu projektów planów rozbudowy systemów.

Administrator to osoba funkcyjna, która opracowuje i aktualizuje dokumentację bezpieczeństwa systemu (bierze również udział w szacowaniu ryzyka), konfiguruje i na bieżąco sprawdza mechanizmy bezpieczeństwa oraz działanie systemu, wdraża procedury bezpiecznej eksploatacji. Wykryte naruszenia bezpieczeństwa przekazuje pełnomocnikowi ochrony. Odpowiada również za nadanie dostępu wyłącznie użytkownikom posiadającym wymagane uprawnienia oraz za prowadzenie z nimi szkoleń z zapisów procedur bezpiecznej eksploatacji. Sporządza i aktualizuje wykaz osób z dostępem do odpowiedniego systemu. Dodatkowo czuwa nad serwisowaniem i aktualnością certyfikatów urządzeń ochrony elektromagnetycznej – w razie wystąpienia konieczności ich serwisu czy przedłużenia certyfikacji informuje o tym pełnomocnika.

Ostatnią osobą funkcyjną odpowiadającą za bezpieczeństwo teleinformatyczne w jednostce organizacyjnej jest *oficer bezpieczeństwa systemów łączności i informatyki* (OBSŁiI). Bierze on odpowiedzialność za nadzór nad bezpieczeństwem kryptograficznym systemu. W związku z tym uczestniczy w opracowywaniu dokumentacji bezpieczeństwa w zakresie użycia urządzeń oraz dokumentów kryptograficznych oraz kontroluje prawidłowość wykorzystania urządzeń kryptograficznych użytych w systemie.

ATAK SIECIOWY POLEGA NA KRADZIEŻY POUFNYCH LUB PRYWATNYCH INFORMACJI. W WYNIKU TEGO DOCHODZI DO DOWOLNEJ ZMIANY LUB USUNIĘCIA DANYCH, ZMIANY USTAWIEŃ KONFIGURACYJNYCH LUB ZABLOKOWANIA USŁUGI.

PODSUMOWANIE

Cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa, co pociąga za sobą konieczność dokonania licznych zmian w obszarze odpowiedzialności użytkownika. Korzystając z systemów i technologii teleinformatycznych, jesteśmy narażeni na zagrożenia płynące z przestrzeni wirtualnej. W zapobieżeniu potencjalnym atakom mogą pomóc odpowiednie narzędzia i aplikacje (mechanizmy) do zabezpieczenia sieci oraz systemy wykrywania intruzów. Niebagatelne znaczenie ma również właściwe wykonywanie zadań przez personel sprawujący ochronę informacji w systemach. Jednak nie możemy zapomnieć o niezwykle ważnej kwestii, jaką jest świadomość każdego użytkownika systemu. Czynnik ludzki wciąż pozostaje piętą achillesową każdego systemu zabezpieczeń. Dlatego też wyszkolony i świadomy użytkownik to jedno z ogniw łańcucha bezpieczeństwa systemu, który jest tak silny, jak najsłabszy jest jego element.

Opisane zagrożenia stanowią konsekwencję niewłaściwego korzystania użytkownika z wirtualnej cyberprzestrzeni, bezpośrednio godzą w rzeczywiste naruszenia w sposób konwencjonalny oraz strefę środowiska fizycznego. Zatem ochrona sieci teleinformatycznych jest nieporównywalnie trudniejsza i wymaga odpowiednich, a zarazem poważniejszych przedsięwzięć organizacyjnych, skłaniających do zwiększenia intensywności zmian w zakresie zastosowania odpowiednich rozwiązań technologicznych. ■

Modernizacja kryptograficzna w taktycznych systemach łączności

POPRAWNIE FUNKCJONUJĄCE ZABEZPIECZENIE KRYPTOGRAFICZNE ODGRYWA ISTOTNĄ ROLĘ W ZAPEWNIANIU POUFNOŚCI, INTEGRALNOŚCI I AUTENTYCZNOŚCI PRZEKAZYWANYCH INFORMACJI.

ROBERT SUCHY/COMBAT CAMERA DORSZ

Procedury kryptograficzne poddano standaryzacji zarówno dla wąsko-, jak i szerokopasmowych transmisji.

kmdr por. Paweł Kamiński

Autor jest starszym specjalistą w Wydziale Bezpieczeństwa Kryptograficznego Zarządu Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ.

Większość państw posiada lub tworzy instytucje, które mają za zadanie zapewnienie niezbędnych atrybutów przekazywanych informacji. Powstają programy mające na celu zapewnienie wysokiego poziomu bezpieczeństwa kryptograficznego wewnątrz własnych sił zbrojnych, jak również w ramach współpracy koalicyjnej czy też międzynarodowej. Zapewnienie kryptograficznej interoperacyjności między nowymi urządzeniami kryptograficznymi a wycofywanymi jest dużym wyzwaniem. Dlatego też są opracowywane standaryzowane protokoły kryptograficzne, takie jak NINE[1] czy SCIP[2], umożliwiające państwom członkowskim NATO produkowanie urządzeń zapewniających interoperacyjność kryptograficzną tworzonych systemów informacyjnych na poziomie narodowym i koalicyjnym. W celu zapewnienia kompatybilności wstecznej są opracowywane dokumenty standaryzacyjne narzucające pewne rozwiązania i funkcjonalności, jednocześnie usprawniające procesy wymiany informacji, takie jak amerykański TSVCIS (Tactical Secure Voice Cryptographic Interoperability Specification). By zapewnić kompatybilność między urządzeniami kryptograficznymi opartymi na standaryzowanym natowskim protokole kryptograficznym SCIP a amerykańskimi urządzeniami kryptograficznymi implementującymi specyfikację TSVCIS, dokumenty standaryzacyjne zostały uzupełnione o rozwiązania implementowane przez TSVCIS jako dodatkowa specyfikacja STaC-IS.

POTRZEBY

W tym kontekście należy zwrócić uwagę na trwający obecnie konflikt rosyjsko-ukraiński. Zgodnie z posiadanymi informacjami obie jego strony w celu wymiany informacji na najniższych szczeblach dowodzenia wykorzystują komercyjne radiotelefony, na przykład chińskiej firmy Boafeng. Cechują się one dużą bezawaryjnością, jak również niską ceną. Duży popyt na tego rodzaju sprzęt jednoznacznie wskazuje na jego zapotrzebowanie na polu walki, na którym coraz większego znaczenia zaczyna nabierać żołnierz wyposażony w narzędzia umożliwiające mu zwalczanie środków walki przeciwnika. Jednym z podstawowych elementów zapewniających współdziałanie w drużynie (zespole) jest sprawnie działająca łączność służąca do przekazywania rozkazów, wskazywania celów, jak również zapewniająca wsparcie innych środków walki. Wynika z tego, że komunikacja na tym podstawowym szczeblu jest niezbędna do zwalczania przeciwnika dysponującego lepszymi środkami walki. Kupowane przez siły ukraińskie urządzenia łączności w większości są pozbawione funkcji zapewniających bezpieczną łącz-

1 NINE – Network and Information Infrastructure Internet Protocol Network Encryption standard.

2 SCIP – Secure Communications Interoperability Protocol Standart.

ność, takich jak COMSEC (Communications Security) czy TRANSEC (Transmission Security). Brak zabezpieczenia łączności pod kątem transmisji danych (TRANSEC) może skutkować tym, że bardzo łatwo jest ją zakłócić. Natomiast brak wbudowanych w radiostacje funkcji COMSEC uniemożliwia zachowanie poufności korespondencji, jej integralności oraz autentyczności przekazywanej informacji, co może spowodować w przypadku prowadzonej przez przeciwnika walki radioelektronicznej utratę wszystkich korzyści oferowanych przez poprawnie funkcjonującą łączność radiową oraz powoduje podatność na dezorganizację działań oraz zniszczenie sił i środków. Wniosek z pobieżnej analizy przebiegu konfliktu na Ukrainie pod kątem jednego z aspektów C4ISR[3] wydaje się oczywisty: łączność na szczeblu drużyny oraz poszczególnych żołnierzy jest niezbędna, ale bez zapewnionych funkcji COMSEC i TRANSEC wydaje się być podatna na oddziaływanie drugiej strony, zapewniając jej olbrzymią przewagę w prowadzeniu działań.

Jeżeli uwzględnimy pobieżne wnioski na temat łączności na szczeblu drużyny, możemy wykazać, że nie mniej istotne, jeśli nie ważniejsze jest utrzymanie bezpiecznej łączności z elementami ugrupowania bojowego brygady, w tym także innych rodzajów wojsk. Ponadto w ramach reorganizacji naszych sił zbrojnych oraz ich modernizacji również w zakresie C4ISR niezwykle istotna jest kompatybilność wsteczna nowo wprowadzanego sprzętu łączności, jak również jego interoperacyjność w różnych rodzajach wojsk.

W ARMII AMERYKAŃSKIEJ

W Stanach Zjednoczonych działa wiele instytucji mających na celu usystematyzowanie z wykorzystaniem odpowiednich programów problemów interoperacyjności kryptograficznej i ich ostateczne rozwiązanie. W ramach dostępnych materiałów do instytucji zarządzających oraz wpływających na kształt kryptografii w USA, tym samym w dużej części świata, zalicza się:

– NSA (National Security Agency) – odpowiedzialną za zapewnienie szeroko rozumianego bezpieczeństwa informacyjnego (przetwarzania informacji polegającego na bezpiecznym jej przechowywaniu, przetwarzaniu i przesyłaniu);

– Cryptographic Modernization Branch (CMB) [element składowy Communications-Electronics Research Development and Engineering Center (CERDEC)] – wydział zajmujący się testowaniem rozwiązań kryptograficznych przed wdrożeniem ich do sił zbrojnych. Weryfikuje rozwiązania kryptograficzne dostępne na rynku pod kątem ich interoperacyjności z funkcjonującymi już w siłach zbrojnych rozwiązaniami oraz przydatności zapewniających przez nie funkcjonalności;

– National Cryptographic Solutions Management Office (NCSMO) – biuro odpowiadające za wdrażanie algorytmów Suite B (komercyjnych rozwiązań umożliwiających przetwarzanie informacji niejawnych) oraz innych rozwiązań kryptograficznych;

– Committee on National Security Systems (CNSS) – instytucja zajmująca się między innymi tworzeniem polityk, dyrektyw, instrukcji i procedur operacyjnych odnoszących się do wykorzystania materiałów kryptograficznych.

Z całą pewnością są jeszcze inne instytucje zaangażowane w realizację przedsięwzięć zabezpieczenia kryptograficznego sił zbrojnych USA. Wskazuje to, jak bardzo złożony i istotny jest to proces, wymagający koordynacji wielu podmiotów w celu prawidłowego zabezpieczenia pod względem poufności przetwarzanych informacji niejawnych w państwie. Należy przy tym podkreślić, że Stany Zjednoczone są jednym z liderów w tej dziedzinie. Duża część państw korzysta z opracowanych przez Amerykanów algorytmów, urządzeń czy też procedur.

Warto również wspomnieć o programach modernizacji kryptograficznej realizowanych w tym kraju. Zaliczamy do nich *Cryptographic Modernization Program*, który ma zapewnić odpowiednie zdolności kryptograficzne stosownie do wymagań operacyjnych, jak również uwarunkowań pola walki. W szczególności ma za zadanie wymianę sprzętu kryptograficznego, którego okres użyteczności pod względem technologicznym się zakończył lub zbliża ku końcowi (20–30 lat), oraz transformację systemów wymieniających informacje punkt–punkt do systemów sieciocentrycznych. Obecnie Ministry of Defense (DoD) oraz National Security Agency opracowują program *Cryptographic Modernization Program 2*, którego zadaniem będzie usuwanie podatności istniejących systemów kryptograficznych na nowe zagrożenia w postaci komputerów kwantowych z ich unikalnymi algorytmami oraz mocami obliczeniowymi[4].

Program modernizacyjny radiostacji ARC-210 amerykańskiej marynarki wojennej ma na celu pozyskanie radiostacji piątej generacji. Rodzina radiostacji AN/ARC-210 była także w wyposażeniu jednostek lotniczych USA. Zapewniała łączność foniczną oraz wymianę danych w zakresie częstotliwości UHF i VHF z modulacją amplitudy oraz częstotliwości AM i FM, jak również łączność satelitarną SATCOM. Radiostacje te mają wbudowane funkcje umożliwiające przeciwdziałanie aktywności przeciwnika polegającej na zagłuszaniu częstotliwości, takie jak HaveQuick I, HaveQuick II oraz Saturn. Poza tym zapewniają przesyłanie danych oraz głosu.

3 C4ISR – Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR).

4 *DoD Digital Modernization Strategy*, 12.07.2019, Department of Defence https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF/. 15.03.2022.

Piąta ich generacja w postaci RT-1939 jest rodziną radiostacji z kryptografią zapisaną w niej programowo zgodnie z założeniami NSA w ramach modernizacji kryptograficznej (Cryptographic Modernization Initiative).

Kolejny program modernizacyjny był realizowany przez firmę Raytheon. W 2016 roku firma ta zdobyła kontrakt na dostarczenie amerykańskiej armii urządzeń kryptograficznych przeznaczonych dla sił powietrznych, gwarantujących bezpieczną łączność foniczną oraz wymianę danych. W ramach kontraktu miała ona dostarczyć do 15 grudnia 2021 roku zmodernizowane urządzenia kryptograficzne VINSON oraz ANDVT (Advanced Narrowband Digital Voice Terminal). Urządzenia VINSON bazują na algorytmie kryptograficznym Saville zaliczającym się do algorytmów typu Suite A, czyli certyfikowanych przez NSA, nieudostępnianych poza kraje koalicyjne, umożliwiających przetwarzanie informacji niejawnych. Według dostępnych w Internecie informacji algorytm ten wykorzystuje klucze o długości 128 bitów, z czego 120 służy do szyfrowania wiadomości, natomiast pozostałe 8 to suma kontrolna. Algorytm ten został opracowany pod koniec lat sześćdziesiątych ubiegłego stulecia i jest powszechnie stosowany w wielu urządzeniach kryptograficznych mających za zadanie szyfrowanie komunikacji fonicznej. Wykorzystują go między innymi urządzenia kryptograficzne Elcrodat produkowane przez firmę Rohde & Schwarz, a także wchodzące w skład VINSON (np. KY 68) oraz ANDVT (np. KY-99).

Zgodnie z informacjami zawartymi w publikacji opisującej modernizację marynarki wojennej wstępną gotowość operacyjną zmodernizowane urządzenia kryptograficzne VINSON/ANDVT osiągnęły w 2016 roku. W ramach programu Information Systems Security Program prowadzi się prace nad systemami uniemożliwiającymi ingerencję we własne systemy łączności (telekomunikacyjne). Program ten, oprócz zapewnienia możliwości obrony sieci informatycznych (Computer Network Defense – CND) oraz rozwijania systemów kształtujących świadomość operacyjną w cyberprzestrzeni, koncentruje się na zagwarantowaniu bezpieczeństwa komunikacji w postaci kryptografii oraz modernizacji elementów zarządzania materiałami kryptograficznymi (Key Management Infrastructure – KMI), jak również infrastruktury klucza publicznego (Public Key Infrastructure). Jednym z zasadniczych celów programu jest zapewnienie bezpieczeństwa przetwarzanych informacji pod kątem poufności, integralności, dostępności oraz niezaprzeczalności.

Amerykańskie Ministerstwo Obrony we współpracy z NSA na początku obecnego stulecia podjęło działania mające na celu opracowanie standardu kryptograficznego pozwalającego na wymianę fonicznych informacji niejawnych. Założono wprowadzenie aparatów telefonicznych STU III umożliwiających prowadzenie niejawnej korespondencji. Koncepcja ta została udostępniona NATO i przekształcona w projekt o nazwie Secure Communication Interoperability Protocol. W jego ramach ustalono standaryzowane wymagania oraz protokół dla urządzeń kryptograficznych *end to end* (E2E), co oznacza możliwość montowania ich w urządzeniach końcowych w celu zapewnienia bezpiecznej wymiany informacji niejawnych. Do najważniejszych cech protokołu SCIP można zaliczyć jego niezależność od warstwy transportowej, ponieważ kryptografia skupia się na warstwie aplikacji w modelu OSI, czyli pozwala na stosowanie tego protokołu w dowolnych urządzeniach, które zapewnią zestawianie połączeń na poziomie warstwy transportowej[5].

ISTOTNY PROTOKÓŁ

Realizacja różnorodnych projektów w siłach zbrojnych USA oraz posiadanie dużej ilości sprzętu łączności starszej generacji spowodowały konieczność opracowania standardu, który zapewniałby kompatybilność wsteczną ze starszą generacją urządzeń wykorzystujących moduły kryptograficzne. W tym celu w 2008 roku powołano w NSA grupę o nazwie Tactical Secure Voice Working Group[6] w celu takiej modernizacji urządzeń fonicznych, aby zagwarantować interoperacyjność między nowymi i starymi urządzeniami. Głównym zadaniem powołanego zespołu było opracowanie specyfikacji zapewniającej wspomnianą interoperacyjność. W 2009 roku po sześciu miesiącach pracy powstał dokument Tactical Secure Voice Cryptographic Interoperability Specification (TSVCIS), w którym opisano wymagania i protokoły umożliwiające osiągnięcie założonego celu. Składa się on z dwóch części: jawnej i niejawnej, określających zasady kodowania fonii, kryptografii i synchronizacji oraz zawartość przesyłanych ramek, sposób zarządzania dokumentami kryptograficznymi, a także wiele innych funkcji dla uzyskania bezpiecznej komunikacji fonicznej i przesyłania danych.

W tym czasie trwały również prace związane z modernizacją urządzeń z rodziny VINSON/ANDVT użytkowanych przez siły powietrzne oraz opracowywano w marynarce wojennej radiostacje piątej generacji ARC-210. Głównym więc celem przygotowanej dokumentacji było zwiększenie możliwości operacyjnych nowego sprzętu z uwzględnieniem wymogu kompatybilności wstecznej z urządzeniami starszej generacji, których modernizacja nie była możliwa.

TSVCIS jest specyfikacją bazującą na warstwie aplikacji w modelu odniesienia łączenia systemów

5 P. Kamiński, *Protokół kryptograficzny SCIP Secure Communication Interoperability Protocol*, „Przegląd Sił Zbrojnych" 2021 nr 4.

6 Th. Moran, D. Heide, S. Shah, *An Overview of the Tactical Secure Voice Cryptographic Interoperability Specification*, U.S. Naval Research Laboratory, The 2010 Military Communication Conference.

otwartych OSI. Jej opracowanie miało służyć zapewnieniu bezpiecznej fonicznej łączności taktycznej, na przykład z wykorzystaniem wojskowej łączności radiowej.

Głównymi problemami, które powodowały brak interoperacyjności urządzeń radiowych, były różna prędkość transmisji danych (przepływność), odmienne metody kompresji dźwięku, kryptografii i synchronizacji oraz struktury przesyłanych ramek. Brak jednakowych standardów uniemożliwiał tworzenie wydajnych i efektywnych sieci radiowych zapewniających łączność taktyczną. TSVCIS zawiera bowiem tylko podstawowe wymagania, które powinny zostać spełnione dla osiągnięcia interoperacyjności, natomiast sama interoperacyjność zależy od zaimplementowanych systemów oraz konkretnych modułów.

Specyfikacja ta została już wdrożona w radiostacjach na przykład firmy L3 HARRIS, takich jak: L3Harris Falcon IV AN/PRC-158 (fot.), AN/PRC-152 oraz AN/PRC-117G(V)1(C), a także w urządzeniach firmy BAE Systems: AN/ARC-231A RT-1987.

Niejako przy okazji poprawiono istniejące standardy odnoszące się do technologii zapewniających taktyczną bezpieczną łączność foniczną. Modernizacji poddano takie elementy, jak wspomniana kryptografia, synchronizacja i funkcja dystrybucji dokumentów kryptograficznych drogą radiową (OTAR). W jej wyniku uzyskano większą prędkość transmisji danych oraz zwiększoną odporność na zakłócenia. Przy tym urządzenia implementujące specyfikację TSVCIS powinny mieć zdolność do współpracy we wszystkich trybach fonicznych w czasie przesyłania zaszyfrowanych informacji.

Główne korzyści wynikające z implementacji tej specyfikacji to:

- Interoperacyjność uzyskana między urządzeniami pracującymi w trybach szeroko- i wąskopasmowych, wynikająca z zastosowania tego samego kodeka głosu, takiej samej synchronizacji oraz standardu przechodzenia z przesyłania fonii na przesyłanie danych, jak również wykorzystania tych samych trybów kryptograficznych.

Przyjęty w specyfikacji kodek głosu to enhanced Mixed-Excitation Linear Prediction (MELPe), który w 2002 roku po intensywnych testach oraz rywalizacji z innymi kodekami został poddany procedurze standaryzacyjnej w NATO i opisany dokumentem STANAG 4591. Jest on wykorzystywany przy przepływnościach 2400 bit/s. W przypadku większej prędkości transmisji danych są przesyłane dodatkowe informacje poprawiające jakość fonii. Nie wymaga to zastosowania kolejnych procesów dekodowania i przetwarzania sygnału, żeby przesyłać informacje z inną prędkością ze względu na ich modułowość. Owocuje to poprawą jakości przesyłanego dźwięku przy większych przepływnościach, a przy mniejszych prędkościach wiąże się jedynie z odrzuceniem modułów poprawiających jakość fonii.

Ponadto dokonano standaryzacji takich elementów synchronizacji transmisji danych, jak: Mode Control Word (MCW) służący do przełączania trybów pracy między transmisją foniczną i danych; pola identyfikujące oraz pola oznaczające koniec transmisji; jak również w kryptografii wektor inicjujący (Initialization Vector).

Procedury kryptograficzne również poddano standaryzacji zarówno dla wąsko-, jak i szerokopasmowych transmisji. Opisano algorytmy zamieszczane w ramkach, przesyłane informacje oraz tryb pracy, co eliminuje konieczność rozszyfrowania i ponownego zaszyfrowania danych w razie przejścia na inny tryb transmisji (wąsko- lub szerokopasmowej).

- Poprawa jakości głosu (jakości transmisji fonicznej), co jest jedną z prerogatyw protokołu TSVCIS i polega na neutralizacji zakłóceń losowych na częstotliwościach radiowych powodujących błędy w przesyłanych bitach oraz na niwelowaniu wpływu hałasu generowanego przez platformy (np. śmigłowce). W tym celu w przypadku trybów pracy umożliwiających szybszą transmisję danych wprowadzono dodatkowe zabezpieczenia w postaci Forward Error Correction (FEC).
- Osiągnięcie interoperacyjności kryptograficznej polegającej na wykorzystaniu zatwierdzonych przez NSA algorytmów Suite A i Suite B do szyfrowania danych, jak również przesyłania drogą radiową dokumentów kryptograficznych (OTAD), co jest spójne z programem modernizacji kryptograficznej pilotowanym przez agencję. Najważniejszą jednak cechą specyfikacji protokołu TSVCIS pod kątem kryptografii jest to, że w największym możliwym stopniu bazuje ona na protokole kryptograficznym SCIP będącym standardem w NATO (STANAG 5068). Specyfikacja ta wykorzystuje standardowe zasady synchronizacji kryptograficznej, jak również zasady tworzenia ramek ujęte w SCIP. Tym samym urządzenia z zaimplementowanym protokołem TSVCIS powinny być interoperacyjne z urządzeniami implementującymi standard NATO SCIP, co jest ogromną zaletą specyfikacji, ponieważ w przypadku powszechnego wdrożenia protokołu SCIP w państwach NATO oraz w państwach aspirujących do kooperacji z siłami Sojuszu urządzenia armii amerykańskiej będą z nimi interoperacyjne pod względem kryptograficznym.

Ponadto specyfikacja TSVCIS skupia się na wprowadzeniu jak najmniejszego opóźnienia w nawiązywaniu łączności powodowanego niezbędną synchronizacją kryptograficzną. W związku z tym, że synchronizacja musi mieć miejsce za każdym razem, gdy jest realizowana transmisja w półdupleksie, ma ona wpływ na nawiązanie łączności w czasie rzeczywistym.

- Zarządzanie dokumentami kryptograficznymi z wykorzystaniem systemu Over The Air (Key) Distribution (OTAD) przez zastosowanie algorytmów Suite A i Suite B w celu szyfrowania przesyła-

HARRIS

Radiostacja L3Harris AN/PRC-158 implementująca specyfikację TSVCIS

nych kluczy, które są następnie deszyfrowane w urządzeniach za pomocą uprzednio wgranych kluczy. Ponadto, zgodnie z udostępnionymi informacjami, system ten ma ulepszoną ochronę przesyłanych kluczy dzięki zastosowaniu wielopoziomowej ochrony w porównaniu z poprzednimi generacjami systemu OTAD. Dodatkowo dostarczane klucze mają opisujące je metadane, które upraszczają ich identyfikację. W związku z tym nie wymagają ingerencji operatora w celu ich implementacji do realizacji zadań polegających na nawiązywaniu konkretnego bezpiecznego połączenia. Przekazywane drogą radiową klucze mogą być następnie przesyłane w postaci zaszyfrowanej do urządzeń służących do dystrybucji dokumentów kryptograficznych w celu dalszego ich manualnego kolportażu. Przesyłanie drogą radiową dokumentów kryptograficznych jest zabezpieczone metodą Forward Error Correction (FEC) oraz Majority Voting Logic (MVL). Informacje są przekazywane z małą prędkością 2400 bit/s, co nie wpływa ujemnie na wszystkie wymienione zalety.

Dzięki wprowadzeniu specyfikacji TSVCIS możliwe jest zastosowanie wielu usprawnień wykorzystujących głównie modułową elastyczną strukturę przesyłanego sygnału, który w zależności od prędkości przekazywania danych – szerokości dostępnego kanału – można rozbudowywać bądź też odbierać dodatkowe informacje foniczne poprawiające jego jakość względem podstawowego standardu opartego na kodeku eMELP.

Ponadto taka struktura przesyłanych informacji pozwala na tworzenie sieci radiowych z użyciem różnego rodzaju sprzętu przez zastosowanie odpowiednich bram sprzętowych dopasowujących zawartość informacyjną sygnału do możliwości przesyłowych oraz generacji radiostacji. Wszystkie operacje dostosowujące przesyłany sygnał do możliwości kanału nie wymagają rozszyfrowywania oraz ponownego zaszyfrowywania przekazywanych informacji ze względu na modułową jego strukturę. W związku z tym wszystkie operacje modyfikujące strukturę sygnału mogą być realizowane na zaszyfrowanej postaci informacji, co zmniejsza czasochłonność procesu oraz upraszcza go. Zapewnia to bezpieczną interoperacyjność urządzeń, jak również bezpieczną łączność *end to end* (E2E) między urządzeniami. Właściwa informacja w postaci zaszyfrowanej przez cały okres jest przesyłana zarówno w sieciach homogenicznych, jak i heterogenicznych (jeden z filarów protokołu SCIP).

Przy przesyłaniu sygnału w trybie szerokopasmowym istnieje możliwość wykorzystania systemu FEC nie tylko do korekty przesyłanej informacji, lecz również do oceny poziomu zakłóceń w danym kanale, co umożliwia ustalenie stosunku: sygnał szum/zakłócenia generowane przez otoczenie oraz zniekształcające przekazywaną informację foniczną. Analizując te współczynniki, urządzenie może podjąć decyzję o wykorzystaniu FEC z naciskiem na korektę błędów w przesyłanych bitach lub też zastoso-

wać dodatkowe elementy spektralne w celu eliminacji szumów/zakłóceń otoczenia. Może być to okresowo zmieniane w zależności od warunków otoczenia, jak również od zmian kanału i warunków na nim panujących.

WAŻNY DOKUMENT

W celu zapewnienia interoperacyjności kryptograficznej między implementowaną w amerykańskich radiostacjach specyfikacją TSVCIS a wdrażanym w krajach NATO protokołem kryptograficznym SCIP w roku 2017 została powołana grupa specjalistów z państw członkowskich z zadaniem opracowania dokumentu wchodzącego w skład dokumentacji standaryzującej SCIP, wypełniającego lukę między protokołem i specyfikacją. W jej skład weszli specjaliści z Francji, USA, Wielkiej Brytanii, RFN, Włoch, Norwegii, Hiszpanii i Turcji. Pierwsza wersja dokumentu Secure Tactical Communications Interoperability Specification (STaC-IS) została dołączona do dokumentacji SCIP w październiku 2018 roku. Prace uaktualniające trwały przez 2019 rok. Finalna wersja 1.1 powstała 14 września 2020 roku jako tryb interoperacyjności STaC-IS między protokołem SCIP i specyfikacją TSVCIS. Odpowiedzialność za kolejne modyfikacje protokołu SCIP przejęła natowska instytucja: Communication and Information Systems Secure Standards – Communication and Information Partnership (CIS3 C&IP). Opracowany moduł STaC-IS nie powoduje zmian w istniejącym już i zatwierdzonym dokumencie AComP 5068 opisującym protokół SCIP[7]. Zawiera on wymagania zapewniające interoperacyjność między środkami komunikacji wąsko- i szerokopasmowej, trybami pracy w pasmach KF (HF) oraz zasadami zarządzania dokumentami kryptograficznymi i wykorzystywanymi mechanizmami kryptograficznymi. Ponadto opisuje specyfikacje bramy między wąskopasmowymi lub starymi szerokopasmowymi urządzeniami a nowo projektowanymi środkami komunikacji umożliwiającej ich łączność przez zapewnienie interoperacyjności.

W ramach standaryzacji kryptograficznej między SCIP oraz TSVCIS przyjęto, na przykład, tryb działania Electronic Code Book (ECB) jako metodę szyfrowania bloków informacji wykorzystującą klucze symetryczne. Jest to metoda bezpośrednia polegająca na szyfrowaniu każdego bloku danych osobno za pomocą ustalonego klucza szyfrującego. Różni się ona od innych trybów szyfrowania, takich jak np. Cipher Block Chaining Mode (CBC) czy też Cipher Feedback Mode (CFB), tym, że uprzednio szyfrowane bloki danych nie mają wpływu na wynik kolejnych szyfrowanych bloków. Rozwiązanie to ma zarówno zalety, jak i wady. Jedną z największych zalet jest to, że utrata przesyłanego bloku danych bądź też odebranie go z błędami nie skutkuje brakiem możliwości odszyfrowania kolejnych bloków. Wszystkie bowiem są niezależne od siebie. W przypadku komunikacji radiowej, w której prawdopodobieństwo utraty przesyłanych danych lub też odebrania ich z błędami jest bardzo duże czy to z powodów naturalnych, czy też celowych działań przeciwnika, rozwiązanie to wydaje się być jedyną rozsądną propozycją do zastosowania. Ponadto pozwala na przyspieszenie procesu szyfrowania i deszyfrowania danych, umożliwiając równoczesne realizowanie procesów z różnymi blokami danych, by na końcu zestawić je we właściwej kolejności[8]. Do głównych wad można zaliczyć deterministyczne wyniki szyfrowania, które powodują to, że w przypadku braku zmiany klucza szyfrującego otrzymane wyniki dla takich samych bloków danych będą również identyczne, co ułatwia ingerencję w ich integralność, czyli zamianę zaszyfrowanych bloków danych. Osoba podsłuchująca wymianę informacji może dokonać jej analizy, wyodrębnić takie same elementy, przypisać im możliwe znaczenie, następnie przez przemyślaną ich zamianę wpłynąć na zmianę treści przesyłanych informacji.

Aby zapobiec takiej sytuacji, należy wciąż zmieniać klucz szyfrujący bloki danych. W związku z tym, że jest on symetryczny, a zatem znany obu korespondentom, należy go albo w sposób niejawny przesyłać, albo też generować w sposób wiadomy dla obu stron wymiany informacji, bazując na niejawnym stałym komponencie i wciąż zmieniającym się składniku, którego niejawność nie jest już wymagana. Jest to możliwe dzięki zastosowaniu wektora stanu, którego jedną z części składowych jest licznik kolejnych przesyłanych bloków danych. Wektor stanu jest wykorzystywany do generowania klucza szyfrującego konkretnego bloku danych. W związku z tym, że wektor stanu zmienia się wraz z kolejno szyfrowanym blokiem danych, finalny klucz szyfrowania bloku danych jest zawsze inny. W celu wygenerowania klucza szyfrowania bloku danych jest używany wektor stanu, który jest następnie szyfrowany kluczem symetrycznym sesji za pomocą wskazanego algorytmu szyfrowania w ramach procesu uzgadniania warunków połączenia kryptograficznego (synchronizacji połączenia). Otrzymany klucz jest następnie dodawany binarnie modulo 2 (operacje XOR) do szyfrowanego bloku zarówno w procesie szyfrowania, jak i odszyfrowywania.

Pozornie wydawać by się mogło, że mała zmiana wektora stanu polegająca na przyroście licznika zaszyfrowanych (przesłanych) bloków danych nie wpłynie znacząco na cykliczną całkowitą zmianę generowanych kluczy szyfrowania. Jednakże aktualnie wykorzystywane algorytmy szyfrowania w ramach

7 AC/322-N(2020)0085 SCIP *Extension for Interoperability with TSVCIS Release* 1.1, 14.09.2020, C3B.

8 Ch. Paar, J. Pelzl, *Understanding Cryptography,* Springer 2010.

algorytmów Suite B, przykładowo Advance Encryption Specification (AES), mają zaimplementowane mechanizmy dyfuzji, które gwarantują, że drobna zmiana szyfrowanego bloku danych (wektora stanu) powoduje kompletnie inny wynik szyfrowania.

Dodatkowo w ramach ujednolicania wymagań kryptograficznych dla taktycznych systemów łączności radiowej między TSVCIS oraz SCIP (STaC-IS) określono wymagania dotyczące dokumentów kryptograficznych, które muszą być spełnione w celu zapewnienia bezpieczeństwa przesyłanych informacji. Należą do nich:

- Traffic Encrytpion Key (TEK) – symetryczny klucz szyfrujący transmisje danych wprowadzany do urządzenia kryptograficznego w ramach przygotowania go do pracy w trybie niejawnym, na przykład w ramach systemu Over The Air (Key) Distribution (OTAD) – dystrybucji dokumentów kryptograficznych drogą radiową[9];
- OTAD Key Encryption Key (KEK) – symetryczny klucz szyfrujący transmisje danych z wykorzystaniem systemu OTAD, wprowadzany do urządzenia na przykład w bezpiecznej sieci, do której są wpinane urządzenia radiowe w celu aktualizacji między innymi dokumentów kryptograficznych;
- End Cryptographic Unit Key Encryption Key (ECU KEK) – klucz deszyfrujący klucze wprowadzane do urządzenia w formie zaszyfrowanej.

WNIOSKI

Niezaprzeczalnie kryptografia pełni jedną z kluczowych ról w zapewnianiu bezpiecznego przepływu informacji. Niemniej zabezpieczenie kryptograficzne boryka się z problemami wynikającymi z realizacji przeciwstawnych celów: z jednej strony ograniczony dostęp do produktów kryptograficznych dla zapewnienia im jak największego bezpieczeństwa, z drugiej zaś konieczność zapewnienia powszechnego bezpieczeństwa informacji dla jak największej liczby użytkowników. Powszechność wymaga skoordynowanych działań na poziomie państwa. Natomiast ze względu na coraz częstszą współpracę koalicyjną czy też międzynarodową wymaga również współpracy na tym poziomie. W pierwszym przypadku państwa radzą sobie, powołując rozbudowane instytucje mające na celu planowanie, modernizowanie i zarządzanie kryptografią. W drugim przypadku zarządzanie kryptografią jest przekazywane do instytucji międzynarodowych bądź koalicyjnych, np. NATO. Taka sytuacja ma miejsce w przypadku tworzenia wspólnych projektów kryptograficznych mających zapewnić interoperacyjność państw członkowskich w tej dziedzinie. Charakterystyczny jest proces proponowania rozwiązań gwarantujących międzynarodową interoperacyjność, kiedy to strona amerykańska wskazuje na rozwiązanie kryptograficzne, np. protokół SCIP, początkowo projektowany i rozwijany na potrzeby narodowe, następnie przekazany międzynarodowym koalicjantom do dalszego rozwoju w ramach współpracy. Umożliwia to uzyskanie kryptograficznej interoperacyjności między siłami zbrojnymi w ramach operacji połączonych angażujących kraje Sojuszu, pozwalając jednocześnie na wykorzystanie narodowego przemysłu do produkcji własnych rozwiązań kryptograficznych zgodnie ze standaryzowanymi protokołami. Działania te z jednej strony zapewniają interoperacyjność, z drugiej zaś pozwalają na dowolność wyboru producenta, rozwój rodzimych technologii i przemysłu oraz, co jest równie istotne, krążenie środków finansowych w obrębie własnego kraju. Strona amerykańska, dążąc do zapewnienia kompatybilności wstecznej swoich rozwiązań modernizacyjnych w ramach tworzonych nowych produktów gwarantujących bezpieczną łączność taktyczną, udostępnia opracowane specyfikacje w celu ich adaptacji na poziomie międzynarodowym dla umożliwienia szeroko rozumianej interoperacyjności z koalicjantami w ramach NATO. Powoduje to aktualizację dokumentacji standaryzacyjnej, na przykład protokołu kryptograficznego SCIP do wersji STaC-IS, który wydaje się być kolejnym wyznacznikiem kierunku rozwoju produktów mających zapewnić bezpieczną łączność na poziomie taktycznym.

Na amerykańskim przykładzie zarządzania rozwojem kryptografii można wykazać, jak trudny i skomplikowany jest to proces, wymagający dużego nakładu sił i środków oraz planowania i realizacji długofalowych programów modernizacyjnych, cyklicznie modyfikowanych i unowocześnianych w celu zagwarantowania ich aktualności oraz zabezpieczenia informacji w warunkach dynamicznie zmieniającej się rzeczywistości. Obecnie konieczność zapewnienia bezpieczeństwa kryptograficznego wszystkim użytkownikom pola walki, począwszy od naczelnego dowódcy, skończywszy na poszczególnych żołnierzach, jak również sprostania postępowi technologii, na przykład rozwojowi komputerów kwantowych zwiększających wymagania stawiane algorytmom kryptograficznym, powoduje, że modernizacja kryptografii będzie w dalszym ciągu ewoluowała, co wiąże się z coraz trudniejszymi zadaniami dla instytucji zarządzających.

Wydaje się, że standaryzowane podejście do implementacji rozwiązań kryptograficznych (NINE, SCIP) jest słuszną drogą, a ich modyfikacje zapewniające między innymi kompatybilność wsteczną oraz przyszłościowo rozumianą modułowość sygnału w postaci rozwiązań narodowych (TSVCIS) czy też ich międzynarodowych implementacji (STaC-IS) będą dominowały na polu walki w sferze zabezpieczenia kryptograficznego. ■

9 Należy jednak mieć na uwadze, że ta funkcja nie została opisana i poddana standaryzacji w ramach projektu SCIP. Planowane jest jej dodanie w kolejnych aktualizacjach dokumentacji.

Zagrożenia dla systemu **łączności na polu walki**

PRIORYTETOWYMI ZADANIAMI PRZECIWNIKA PODCZAS PROWADZENIA DZIAŁAŃ BOJOWYCH SĄ IDENTYFIKACJA I WSKAZYWANIE MIEJSC ROZWINIĘCIA ELEMENTÓW DOWODZENIA DRUGIEJ STRONY, ZBIERANIE INFORMACJI O JEJ OBIEKTACH I ŹRÓDŁACH ELEKTRONICZNYCH ORAZ ICH ZAKŁÓCANIE I NISZCZENIE.

Bartłomiej Terebiński jest kierownikiem Zakładu Cyberbezpieczeństwa w Akademii Sztuki Wojennej.

Piotr Kamieński jest zastępcą dowódcy Batalionu Dowodzenia Wojsk Lądowych.

ppłk dr inż. Bartłomiej Terebiński, mjr dypl. SZRP Piotr Kamieński

Rozwój środków walki, nowe domeny prowadzenia działań (cyberprzestrzeń), jak i postępująca automatyzacja uzbrojenia czy tworzenie zintegrowanego obrazu sytuacji taktycznej powodują pojawianie się nowych zagrożeń mogących oddziaływać na stanowiska dowodzenia, w tym na rozwinięty system łączności polowej. Wskazanie owych zagrożeń implikuje konieczność szukania rozwiązań mających na celu zastosowanie właściwych środków zapobiegających takiemu oddziaływaniu. Współczesne konflikty zbrojne wskazują na zmianę podejścia do prowadzenia wojny. Obecnie można zaobserwować połączenie działań konwencjonalnych z dominującymi precyzyjnymi uderzeniami artylerii i środków napadu powietrznego wraz z oddziaływaniem w przestrzeni informacyjnej oraz wpływem czynników pozamilitarnych na prowadzenie działań (aspekt polityczny, gospodarczy, finansowy).

ZE STRONY ELEMENTÓW ROZPOZNAWCZYCH

Do efektywnego rażenia przez przeciwnika elementów dowodzenia, do których zalicza się przede wszystkim środki łączności, niezbędny jest odpowiednio zorganizowany i sprawnie funkcjonujący systemu rozpoznania. Możliwości jego oddziaływania na stanowiska dowodzenia (SD) i powiązane z nimi rozwinięte elementy sieci łączności są dwojakie. Po pierwsze będzie prowadzone rozpoznanie na korzyść wspomagania procesu decyzyjnego. Na podstawie bowiem informacji o aktualnym położeniu wojsk są opracowywane plany użycia ich zgrupowań lub są wyznaczane środki rażenia do obezwładnienia albo niszczenia stanowisk dowodzenia. Po drugie rozpoznanie celów będzie prowadzone na korzyść rażenia ogniowego. Zatem określenie miejsca rozmieszczenia stanowiska dowodzenia lub elementu systemu łączności pozwoli przeciwnikowi na wybór środka ogniowego, który je obezwładni lub zniszczy (tzw. key target).

Głównym zagrożeniem dla systemu łączności są siły i środki przeciwnika prowadzące rozpoznanie dalekie i patrolowe.

Dzięki *rozpoznaniu dalekiemu* zdobywa on informacje o obiektach terenowych w strefie działań głębokich, a więc tam, gdzie należy się spodziewać rejonów rozwinięcia węzłów łączności oraz stacji nadawczo-odbiorczych. Wykorzystując grupy dywersyjno-rozpoznawcze (GDR) oraz etatowe elementy oddziałów i pododdziałów rozpoznawczych, będzie on wykrywał i pozycjonował elementy dowodzenia rozmieszczone w głębi. Rozpoznanie może być wsparte misjami bezzałogowych statków powietrznych (BSP), w które będą wyposażone GDR.

Z kolei *rozpoznanie patrolowe* należy do oddziałów i pododdziałów rozpoznawczych działających na rzecz procesu decyzyjnego w celu zdobycia informacji o obrońcy i środowisku na głębokość dywizji pierwszego rzutu. Najbardziej narażone będą elementy systemu łączności i informatyki, jak również stanowiska dowodzenia rozmieszczone w małej odległości od linii styczności wojsk.

Kolejnym zagrożeniem ze strony przeciwnika jest *rozpoznanie obrazowe* prowadzone metodą teledetek-

Ochrona i obrona stanowiska dowodzenia może być wzmocniona pododdziałem wyznaczonym z ugrupowania bojowego.

SEBASTIAN BRZEZINA/6 BPD

cji. Sensory mogą być umieszczone na platformach satelitarnych, powietrznych lub lądowych. Dzięki takiemu działaniu przeciwnik ma możliwość dokładnego określenia położenia stanowisk dowodzenia, zwłaszcza jeśli będzie używał pasma podczerwieni. Pozwoli to na wykrycie emisji ciepła związanej na przykład z pracującymi zespołami prądotwórczymi. W zakresie widzialnym w największym stopniu narażone na rozpoznanie będą maszty antenowe, zwłaszcza aparatowni radioliniowych (o wysokości do 24 m), oraz anteny rozwiniętych systemów satelitarnych.

Radarowe rozpoznanie obrazowe pozwoli na lokalizowanie węzłów łączności SD. Ponadto umożliwi przeciwnikowi wykrywanie przemieszczających się kolumn tych stanowisk.

Rozpoznanie radioelektroniczne natomiast pozyskuje dane i informacje o obiektach wypromieniowujących energię elektromagnetyczną. Dzięki niemu można określić lokalizację nadawanego sygnału. W celu jego uszczegółowienia oraz potwierdzenia stosuje się inne rodzaje rozpoznania identyfikujące źródło i przekazujące dane do systemu rażenia.

Innym zagrożeniem dla eksploatowanego systemu łączności jest *rozpoznanie pomiarowo-badawcze*. Informacje są pozyskiwane na podstawie ilościowych i jakościowych analiz danych (dane metryczne, kąty, dane przestrzenne, długość fal, pomiar czasu, modulacja itp.) uzyskiwanych z przyrządów technicznych. Ma ono na celu identyfikowanie cech źródeł, nadajników i urządzeń wypromieniowujących energię elektromagnetyczną, co pozwala na ich ostateczną identyfikację. W największym stopniu narażone na rozpoznanie będą zespoły prądotwórcze generujące w sposób ciągły głośne dźwięki.

Do pozyskania informacji o ważnych obiektach (w tym SD) może być stosowane również *rozpoznanie osobowe,* czyli zdobywanie informacji o rozwiniętych stanowiskach dowodzenia od uprowadzonych żołnierzy. Istotne jest także korzystanie z wiadomości z portali społecznościowych (Internetu), na których żołnierze lub ludność cywilna mogą zamieszczać zdjęcia pozwalające na identyfikację miejsca rozwinięcia SD, jak również z opisów postów wskazujących ich lokalizację (tzw. biały wywiad). Ponadto informacje przekazywane w radiu, telewizji i prasie mogą wskazywać przeciwnikowi rejon, w którym prawdopodobnie są rozwinięte elementy dowodzenia.

WALKA RADIOELEKTRONICZNA

Prowadzenie tego rodzaju walki (WRE) przez przeciwnika będzie wiązało się z zakłócaniem pracy środków łączności. Będzie on mieć możliwość zdobycia o nich informacji oraz użycia do ich niszczenia środków precyzyjnego rażenia[1]. Celem WRE jest zmniejszenie efektywności działania systemów rozpoznania, łączności i nawigacji oraz sterowania środkami walki.

Walka radioelektroniczna obejmuje działania ofensywne i defensywne. Pierwsze z nich będą polegały na celowym wypromieniowaniu lub odbiciu energii elektromagnetycznej ukierunkowanej na systemy radioelektroniczne strony przeciwnej. Działania te będą szczególnie istotne z punktu widzenia funkcjonowania węzłów łączności stanowisk dowodzenia, jak również węzłów pomocniczych oraz węzłów bazowych sieci łączności przestrzennej[2]. W związku z tym można założyć, że przeciwnik będzie dążył do przejęcia kontroli nad spektrum elektromagnetycznym przez odmowę dostępu, unieszkodliwianie informacyjne, jak i niszczenie urządzeń elektronicznych[3]. Działania te będą:

– *uniemożliwiać dostęp* zarówno w wymiarze fizycznym (wykorzystanie wybranych zakresów spektrum elektromagnetycznego), jak i informacyjnym (zdobywanie danych i informacji oraz ich przesyłanie przy użyciu fal EM);

– *dezorganizować*, czyli celowo wprowadzać stronę przeciwną w stan niepewności, co spowoduje opóźnienia w reakcji na zaistniałe fakty. W ramach dezorganizacji są stosowane zakłócenia radioelektroniczne powiązane z pozorowaniem radioelektronicznym;

– *obezwładniać*, czyli pozbawiać systemy elektroniczne strony przeciwnej zdolności do wykonywania zasadniczych zadań. Ma to na celu spowodowanie redundancji informacyjnej w systemach rozpoznania i dowodzenia, co będzie skutkować niepewnością co do przebiegu zdarzeń oraz opóźnieniami w procesie podejmowania decyzji;

– *neutralizować*, czyli celowo stosować energię elektromagnetyczną do czasowego uniemożliwienia wykorzystania urządzeń strony przeciwnej, których działanie jest uzależnione od dostępu do spektrum elektromagnetycznego.

Współczesne technologie pozwalają na wytworzenie generatorów niszczących promieniowanie EM o zasięgu do kilkunastu kilometrów (typowo do 1 km), a w przypadku prostszych rozwiązań o mniejszej mocy (generatorów przenośnych) – o zasięgu do kilkudziesięciu metrów. Oddziaływanie silnych pól elektromagnetycznych może powodować zaburzenia pracy monitora i urządzeń do wprowadzania danych (myszki, klawiatury) oraz przypadkowe kopiowanie i kasowanie plików znajdujących się na dysku[4]. Oddziaływanie na stanowisko dowodzenia przy użyciu energii mikrofalowej na większą skalę wydaje się

1 S. Markiewicz, *Proces oceny zagrożenia radioelektronicznego z wykorzystaniem metody scenariuszy* [w:] *Proces oceny zagrożenia militarnego z wykorzystaniem metody scenariuszy*, red. M. Wrzosek, ASzWoj, Warszawa 2020, s. 131–132.

2 Przykładowo taktycznej sieci łączności dywizji [przyp. autorów].

3 S. Markiewicz, *Zagrożenia w przestrzeni elektromagnetycznej* [w:] *Organizacja systemu rozpoznania zagrożeń państwa*, red. M. Wrzosek, ASzWoj, Warszawa 2020, s. 83–84.

4 S. Markiewicz: *Proces oceny zagrożenia*..., op.cit., s. 140.

RYS. 1. ZASIĘG ODDZIAŁYWANIA ŚRODKÓW WALKI RADIOELEKTRONICZNEJ

Opracowanie własne.

*** rlin. – radioliniowe**

być jeszcze odległą przyszłością ze względu na jej krótki zasięg. Obecnie bardziej prawdopodobne jest użycie generatorów przenośnych w aktach dywersji dokonywanych na stanowisku dowodzenia.

Zastosowanie przez przeciwnika zautomatyzowanych systemów walki radioelektronicznej pozwoli na skuteczne zakłócanie funkcjonowania łączności radiowej, radioliniowej i satelitarnej, jednocześnie zapewniając swobodę działań w spektrum elektromagnetycznym (rys. 1).

Przykładem może być w pełni autonomiczny system WRE Borisoglebsk-2. Składa się on z mobilnego systemu kierowania R-300KMw oraz do ośmiu pojazdów wyposażonych w różne systemy zakłóceń (P-378BMW, P-330BMW, P-934BMW i P-325UMW). Charakteryzuje się dużą mobilnością i może być rozwinięty do pracy z położenia marszowego w ciągu 15 min. Działający w jego ramach zestaw rozpoznania radioelektronicznego przekazuje dane do stanowiska analizy i kierowania, które ocenia znaczenie namierzonych źródeł sygnałów i nakierowuje na nie odpowiedni rodzaj zakłóceń radioelektronicznych. System pozwala w zautomatyzowany sposób zakłócać maksymalnie do 30 źródeł promieniowania elektromagnetycznego. Celem jego działania jest przeciwdziałanie systemom łączności radiowej (w tym satelitarnej). Według Rosjan jest on w stanie rozpoznać i zakłócać radiostacje o skokowo zmienianej częstotliwości nośnej (z hoppingiem) – do 300 skoków na sekundę. Dodatkowo jest wyposażony w stację typu R-378 do aktywnych zakłóceń radiowych pasma KF. Jest ona przeznaczona do zagłuszania urządzeń łączności radiowej KF poziomu taktycznego, które pracują zarówno na stałych częstotliwościach, jak i z adaptacyjną lub programowalną zmianą częstotliwości. Nadajnik zestawu pracuje w pasmie od 1,5 do 30 MHz. Zestaw R-378 może zakłócić trzy radiostacje pracujące na stałej częstotliwości lub jedną pracującą z hoppingiem. Jest to system dookólny z dokładnością około 3° namierzania się na źródło promieniowania[5].

Ponadto rosyjskie pododdziały WRE mają możliwość zakłócania łączności telefonii komórkowej oraz telefonicznej łączności satelitarnej. Ponadto dysponują zestawami (np. Lieer) pozwalającymi na wysyłanie wiadomości SMS do wybranych telefonów[6].

Przeciwnik będzie prowadził również działania w cyberprzestrzeni[7]. Może oddziaływać na platformy bojowe wyposażone w dające się programować układy scalone, które można zakłócać bądź infekować mylącym lub destrukcyjnym oprogramowaniem umożliwiającym zdalne sterowanie nimi oraz przeprowadzenie ataku na system łączności i informatyki[8].

Działania w cyberprzestrzeni mogą być prowadzone w dowolnym momencie przez jakikolwiek podmiot oraz w dowolnym celu. Dzięki nim przeciwnik osiągnie następujące cele:

– zmniejszenie funkcjonalności usług przetwarzania/transmisji danych albo ograniczenie ich zdolności do działania na optymalnym poziomie;

5 https://defence24.pl/moskwa-demonstruje-systemy-walki-elektronicznej/. 22.01.2022.

6 Ibidem.

7 W *Doktrynie cyberbezpieczeństwa RP* zdefiniowano pojęcie cyberprzestrzeń jako *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz użytkownikami. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s. 7.

8 B. Terebiński, M. Woźniak, *Zagrożenia stanowisk dowodzenia dywizji*, „Przegląd Sił Zbrojnych" 2018 nr 4, s. 62–63.

TABELA. ZESTAWIENIE MOŻLIWOŚCI WYBRANYCH ŚRODKÓW ARTYLERYJSKICH FEDERACJI ROSYJSKIEJ

Oznaczenie	Nazwa	Kaliber [mm]	Zasięg pocisku [km]
Zmodernizowany taktyczny kompleks rakietowy			
SS-21	Toczka	–	70
Wieloprowadnicowe wyrzutnie rakiet			
BM-21	Grad	122,4	20,4
BM-27	Uragan	220	35
BM-30	Smiercz	300	20–70(90)
Armaty samobieżne			
2S5	Hiacynt-S	152,4	28
2S7	Pion	203	47,5
Haubice samobieżne			
2S1	Gwozdika	122	15
2S3	Akacja	152,4	24
2S19	MSTA-S	152	29

Opracowano na podstawie: https://obserwator-polityczny.pl/wojska-rakietowe-artyleria-sil-zbrojnych-federacji-rosyjskiej/. 27.12.2021.

– ograniczenie dostępności usług na określony czas;

– zniszczenie lub uszkodzenie zasobów (baz danych) tak, aby stały się trwale niedostępne.

W trakcie prowadzenia działań istotnymi zagrożeniami będą:

– możliwość wprowadzenia złośliwego oprogramowania do sieci teleinformatycznych, na skutek czego ich użycie będzie utrudnione;

– ataki DoS[9] i DDoS[10] ograniczające funkcjonalności usług sieciowych, jak również zmniejszające redundancję sieci teleinformatycznych;

– ataki typu *insider*, czyli monitorowanie pracy w sieci teleinformatycznej, przechwytywanie danych, blokowanie usług i dezinformacja.

Mimo że większość sieci teleinformatycznych używanych na stanowisku dowodzenia jest odseparowana od ogólnodostępnej sieci, przeciwnik wykorzystując błędy ludzkie, może doprowadzić do wprowadzenia złośliwego oprogramowania do nich. Może również prowadzić celowe działania w postaci akcji sabotażowych dla obezwładnienia sieci teleinformatycznych. Zakłócenie funkcjonowania Internetu utrudni natomiast komunikację z podmiotami spoza struktur dowodzenia, a także prowadzenie rozpoznania z otwartych źródeł. Przeciwnik może użyć Internetu również do dezinformacji, w tym z zastosowaniem technik *deepfake*[11] urealniających fałszywy przekaz. Dzięki takim działaniom może wpłynąć na morale wojsk, na przykład publikować fałszywe informacje wsparte zdjęciami odnośnie do sytuacji ich rodzin lub ukazywać negatywny wizerunek dowódcy. Dla funkcjonowania stanowiska dowodzenia istotne będzie wykorzystanie zewnętrznej sieci energetycznej oraz punktów dostępu do stacjonarnej sieci teleinformatycznej.

UŻYCIE WOJSK RAKIETOWYCH I ARTYLERII

Do rażenia celów położonych w głębi przeciwnik użyje tych wojsk. Natomiast lotnictwo, w szczególności załogowe, będzie działać głównie tam, gdzie zasięg środków ogniowych jest niewystarczający lub gdy będzie ich za mało do jednoczesnego wykonania uderzenia ogniowego na kilku kierunkach[12]. Wykorzysta zatem artylerię do rażenia rozpoznanych i z ustaloną pozycją stanowisk dowodzenia znajdujących się w jej zasięgu lub zakłóci ich przemieszczanie

9 Atak typu DoS oznacza odmowę dostępu. Realizowany jest przez wysyłanie ogromnej liczby szkodliwych zapytań bądź generowanie dużej ilości ruchu, co prowadzi do przeładowania określonego zasobu. Źródło: https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/. 18.01.2022.

10 Odmiana ataku DoS polegająca na atakowaniu z wielu miejsc jednocześnie. Źródło: https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/. 18.01.2022.

11 Technika obróbki obrazu polegająca na łączeniu obrazów twarzy ludzi przy użyciu technik sztucznej inteligencji. Źródło: https://scroll.morele.net/technologia/technika-deepfake-co-to-jest-i-dlaczego-moze-byc-niebezpieczna/. 18.01.2022.

12 D. Żyłka, *Scenariusz zagrożenia powietrznego* [w:] *Organizacja systemu rozpoznania...*, op.cit., s. 109.

się do rejonu rozmieszczenia. Środki artyleryjskie przeciwnika cechuje duża siła ognia oraz stosowanie różnego rodzaju amunicji. Przykładowo armatohaubica 2S19 MSTA-S ma możliwość strzelania amunicją termobaryczną[13]. Obecnie coraz większe znaczenie w arsenale środków rażenia mają lądowe pociski balistyczne, takie jak np. 9M723 Iskander, które mogą zostać użyte do wykonania uderzeń (tab.).

ŚRODKI NAPADU POWIETRZNEGO

Ciągły dynamiczny rozwój technologiczny środków walki oraz doświadczenia wynikające z konfliktów zbrojnych pozwalają stwierdzić, że na polu walki możliwe są dwa sposoby oddziaływania lotnictwa na stanowiska dowodzenia – z dużej wysokości poza zasięgiem środków ogniowych wyposażonych w optyczne urządzenia celownicze lub z małej i bardzo małej wysokości, gdy ukształtowanie terenu pozwala zbliżyć się do celu i dokonać niespodziewanego ataku[14]. Najgroźniejszymi środkami napadu powietrznego mogącymi oddziaływać na stanowisko dowodzenia są:

– załogowe statki powietrzne (Manned Aircraft – MA), do których zalicza się samoloty oraz śmigłowce sił powietrznych, lądowych i morskich. W tej grupie środków następuje szybki rozwój przenoszonego przez nie uzbrojenia rakietowego klasy powietrze–ziemia. Coraz częściej samolot czy śmigłowiec stają się nosicielem i zarazem systemem kierowania – zasięg odpalania rakiet wciąż się zwiększa, co oznacza, że załogowy statek powietrzny może wystrzelić pociski przed zbliżeniem się do zasięgu środków obrony powietrznej[15];

– bezzałogowe statki powietrzne (BSP), których wielofunkcyjne i masowe wykorzystanie będzie powodowało stopniowe przejmowanie zadań wykonywanych dotychczas przez lotnictwo załogowe[16]. W tym zakresie BSP mogą oddziaływać na stanowisko dowodzenia nie tylko w celu jego rozpoznania, lecz również rażenia jego elementów amunicją krążącą;

– rakiety skrzydlate (Cruise Missiles – CMs) oraz taktyczne rakiety balistyczne (Tactical Ballistic Missiles – TBMs) pozostające wciąż jednym z głównych rodzajów zagrożenia powietrznego[17]. Ze względu na możliwość niszczenia obiektów znajdujących się w dużej odległości, a także dokonywanie precyzyjnych uderzeń mogą być użyte do niszczenia elementów stanowiska dowodzenia, głównie systemu łączności;

– pociski moździerzowe (Rocket and Artillery Mortar's – RAM), które ze względu na ich stosowanie na dużą skalę mogą być użyte przez przeciwnika w działaniach sabotażowych lub rebelianckich do obezwładniania lub niszczenia stanowiska dowodzenia.

Kolejnym środkiem napadu powietrznego, który może być użyty do oddziaływania na SD, są śmigłowce. Mogą one wykonywać wiele różnych zadań. Te najistotniejsze ze względu na oddziaływanie na stanowisko dowodzenia to zadania ogniowe, rozpoznawcze i walki radioelektronicznej. Mogą być używane również do transportu zgrupowań aeromobilnych mogących niszczyć te stanowiska w odległości do 70 km od linii styczności wojsk. Śmigłowce bojowe są zdolne także do samodzielnego poszukiwania i zwalczania obiektów położonych w głębi obrony.

Współcześnie – oprócz samolotów i śmigłowców – coraz większe zagrożenie stanowią BSP, które poza zadaniami o charakterze rozpoznawczym będą angażowane do misji uderzeniowych na elementy ugrupowania bojowego. Obecnie stanowią jeden z najbardziej zaawansowanych technologicznie środków walki i są postrzegane jako przyszłość lotnictwa, ponieważ oprócz wsparcia informacyjnego samolotów załogowych wykonują zadania ogniowe[18]. Trudności w zwalczaniu tego typu środków napadu powietrznego oraz ich duże możliwości sprawią, że oprócz rozpoznania i pozycjonowania stanowisk dowodzenia oraz prowadzenia walki radioelektronicznej będą niszczyły elementy rozwiniętego SD (głównie priorytetowe środki łączności), jak również dezorganizowały ich przemieszczanie się.

W dzisiejszej dobie rakiety skrzydlate są samonaprowadzającymi się środkami rażenia, które mogą być odpalane z samolotów bombowych, okrętów nawodnych i podwodnych oraz z wyrzutni naziemnych. Podczas lotu są trudne do wykrycia i zniszczenia, a ich atak może nastąpić z każdego kierunku.

Ze względu na przenoszony duży ładunek bojowy, a także odporność na rażenie przez systemy OPL rakiety skrzydlate będą zagrożeniem dla rozwiniętych SD. Ich uderzenie będzie w stanie porazić całość rozwiniętego stanowiska dowodzenia.

Następnym zagrożeniem będą rakiety balistyczne, które mogą przenosić konwencjonalne głowice do rażenia tych stanowisk i systemów łączności. Bardzo duży ich zasięg oraz względnie mała podatność na oddziaływanie systemów obrony powietrznej umożliwi przeciwnikowi rażenie SD w rejonach ześrodkowania wojsk w miejscach stałej dyslokacji jeszcze przed ich rozwinięciem się do prowadzenia

13 https://defence24.pl/sily-zbrojne/rosyjska-amunicja-termobaryczna-w-donbasie/. 12.01.2022.

14 A. Radomyski, K. Dobija, *Podręcznik przeciwlotnika (wydanie drugie poprawione i rozszerzone)*, AON, Warszawa 2014, s. 59.

15 Ibidem, s. 65.

16 M. Adamski, T. Compa, *Bezpilotowe środki napadu powietrznego jako element współczesnego pola walki* [w:] *Systemy przeciwlotnicze i obrony przeciwlotniczej*, zbiór prac z V Międzynarodowej Konferencji Naukowo-Technicznej „CRAAS 2003", Tarnów–Zakopane 2003, s. 286–288.

17 *Joint Warfare Publication 3-63,* Joint Air Defence, July 2003, s. 3-3–3-4.

18 Ibidem, s. 133.

działań. Ponadto potencjalny przeciwnik może wykorzystywać do rażenia stanowisk dowodzenia wyrzutnie Toczka oraz Elbrus.

UŻYCIE BRONI MASOWEGO RAŻENIA

Mimo że jej stosowanie jest zabronione dzięki odpowiednim traktatom i normom prawa międzynarodowego, należy liczyć się z możliwością jej użycia.

Bojowe środki trujące mogą zostać wykorzystane do spowodowania dużych strat w ludziach oraz do długotrwałego skażenia terenu, obiektów i sprzętu bojowego[19]. Ponadto późniejsze zabiegi związane z likwidacją skażeń stanów osobowych i sprzętu wojskowego spowodują duże opóźnienia w funkcjonowaniu stanowiska dowodzenia.

Środki biologiczne mogą być bardzo skuteczne. Przy tym będą wymagać specyficznego sposobu ich wykrywania i identyfikacji oraz likwidacji, a także leczenia porażonych[20]. Ze względu na właściwości środków biologicznych ich użycie przez przeciwnika do porażenia stanów osobowych stanowiska dowodzenia wydaje się mało prawdopodobne.

Zagrożenie użyciem *broni radiologicznej* można rozpatrywać jako atak dywersji/terroryzmu w przypadku prowadzenia działań poniżej progu wojny. Charakter i skala skutków wybuchu jądrowego zależą od rodzaju użytej broni, mocy ładunku, środowiska fizycznego, w którym nastąpił wybuch, oraz charakterystyki obiektu będącego celem uderzenia[21]. Jej uaktywnienie do zniszczenia stanowiska dowodzenia nie będzie celem przeciwnika. Jednak ze względu na zasięg oddziaływania może skutkować zakłóceniem funkcjonowania SD i jego przemieszczania.

Toksyczne *środki przemysłowe* to ogólne pojęcie odnoszące się do chemicznych, biologicznych i radioaktywnych substancji występujących w postaci stałej, ciekłej, aerozoli lub gazowej, wykorzystywanych w przemyśle, handlu lub medycynie. Siły zbrojne mogą być narażone na ich oddziaływanie w wyniku zamierzonego lub przypadkowego ich uwolnienia będącego skutkiem celowego działania przeciwnika lub wystąpienia awarii technicznych.

ZE STRONY ZGRUPOWAŃ LĄDOWYCH

W ugrupowanie obronne naszych zgrupowań przeciwnik będzie wysyłał oddziały wydzielone i rajdowe, grupy desantowo-szturmowe oraz taktyczne desanty powietrzne[22]. Należy podkreślić, że zasięg działania oddziałów wydzielonych, a także rajdowych będzie wynikał z możliwości wsparcia ich ogniem, czyli będzie wynosił około 70–90 km. Również działanie zgrupowań wojsk aeromobilnych jest uzależnione od wywalczenia przewagi w powietrzu, jak również od zdolności do tworzenia przez nie punktów bazowania (Forward Arming And Refuelling Point – FARP), które pozwolą na zwiększenie zasięgu ich oddziaływania na elementy ugrupowania bojowego (operacyjnego) broniącego się.

Z kolei taktyczne desanty powietrzne będą wysadzane na kierunkach największego powodzenia dla uchwycenia newralgicznych obiektów zapewniających utrzymanie szybkiego tempa natarcia lub w celu zamknięcia pierścienia okrążenia i niedopuszczenia do dopływu świeżych sił w rejon prowadzonych walk.

Użycie taktycznych zgrupowań bojowych i okrążanie sił głównych spowoduje, że również stanowiska dowodzenia znajdą się w tym rejonie, co ograniczy ich możliwości manewrowe i narazi je na zniszczenie.

Z kolei wojska specjalne prowadzące działania rozpoznawczo-dywersyjne i sabotażowe na zapleczu przeciwnika mogą potwierdzać rozmieszczenie stanowisk dowodzenia i ich elementów łączności oraz dokonać dywersji i przeprowadzić akcje sabotażowe przeciwko rozwiniętemu systemowi łączności.

MOŻLIWE SPOSOBY PRZECIWDZIAŁANIA

Podstawowym będzie skuteczne maskowanie elementów stanowiska dowodzenia. Powinno ono być aktywne, ciągłe, wiarygodne i różnorodne. Aktywność maskowania to nieustanne wprowadzanie przeciwnika w błąd co do położenia poszczególnych obiektów przez ich zakrycie i imitację. Z kolei ciągłość będzie polegać na realizowaniu przedsięwzięć maskujących w każdej sytuacji we wszystkich etapach walki. Wiarygodność sprowadza się do przedsięwzięć urealniających, które powinny być prawdopodobne i naturalne oraz odpowiadać warunkom terenowym, porze roku i konkretnej sytuacji.

Jednym ze sposobów maskowania sprzętu łączności jest zastosowanie siatek maskujących i wielozakresowych pokryć maskujących (np. Berberys). Charakterystyki widmowe siatki[23] zapewniają to, że sprzęt i obiekty zamaskowane przy ich użyciu nie są w warunkach terenowych rozpoznawane okiem nieuzbrojonym podczas prowadzenia obserwacji naziemnej i z powietrza z odległości lub na wysokości 1000 m i większej oraz na zdjęciach fotograficznych wykonanych w skali 1:5000 i mniejszej przy rozdzielczości liniowej zdjęć 20 linii/mm. Ich zastosowanie zmniejsza efektywność rozpoznania termalnego dzięki deformacji zobrazowania termalnego obiektu, zmianie przestrzennych charakterystyk promieniowania oraz ograniczeniu kontrastu termalnego między maskowanym obiektem a tłem do wartości k = 0,01 przy różnicy temperatury ± 4 K w odległości 1000 m. Ponadto

19 *Obrona przed bronią masowego rażenia w operacjach połączonych DD/3.8(A)*, CDiSSZ, Bydgoszcz 2013, s. 17.

20 Ibidem, s. 20.

21 Ibidem, s. 25.

22 B. Terebiński, M. Woźniak, *Zagrożenia stanowisk...,* op.cit., s. 62.

23 https://miranda.pl/oferta/miranda-military/. 10.01.2022.

zmniejszają one współczynnik odbicia promieniowania od sprzętu w takim stopniu, by techniczną odległość jego rozpoznania przez stacje radiolokacyjne ograniczyć co najmniej o 50% przy tłumieniu maksymalnych odbić fal elektromagnetycznych od maskowanego sprzętu na poziomie co najmniej 12 dB.

Niestety w naszych siłach zbrojnych ich niedostateczna liczba umożliwia zamaskowanie na stanowisku dowodzenia tylko aparatowni, węzłowych wozów kablowych, wozów dowodzenia i mobilnych modułów stanowiska dowodzenia. Nie jest natomiast możliwe zamaskowanie wozów dowodzenia z rozwiniętym w pełni systemem antenowym, takich jak ZWD-3, ZWDSz i ZWD-1.

Kolejnym elementem utrudniającym rozpoznanie powinny być zestawy maskowania radiolokacyjnego (np. Miraż białoruskiej firmy Oboronnyje Iniciatiwy).

Podczas funkcjonowania stanowisk dowodzenia należy pamiętać również o:

– ich przemieszczaniu w warunkach ograniczonej widoczności w ugrupowaniu mieszanym;

– płynności przemieszczania oraz zajmowania rejonu rozwinięcia stanowisk dowodzenia;

– budowaniu obiektów pozornych;

– stosowaniu kryterium wiedzy niezbędnej dla osób funkcyjnych obsady SD, jak i pododdziałów ochrony oraz pododdziałów łączności i informatyki;

– odpowiednim rozplanowaniu dalekosiężnych linii kablowych i ich maskowaniu;

– zmianie tras wojskowej poczty polowej;

– wykrywaniu oraz przeciwdziałaniu bezzałogowym systemom powietrznym realizującym rozpoznanie w obrębie rejonu rozwinięcia stanowiska dowodzenia;

– używaniu agregatów w obniżeniach terenowych, tak by stłumić hałas ich pracy, oraz o wykorzystaniu stacjonarnej sieci energetycznej;

– stosowaniu punktów dostępowych do stacjonarnej sieci teleinformatycznej;

– wyborze rejonu rozmieszczenia zapewniającym naturalne właściwości maskujące w przypadku rozwijania stanowiska dowodzenia w terenie lesisto-jeziornym;

– wykorzystaniu obiektów położonych z dala od dużych skupisk ludzkich, umożliwiających zamaskowanie rozwijanych elementów łączności w przypadku organizowania stanowiska dowodzenia w terenie zurbanizowanym;

– realizowaniu przedsięwzięć obrony elektronicznej przez obsługi elementów łączności;

– stworzeniu zewnętrznego pierścienia obrony i ochrony pozwalającego na wykrycie elementów rozpoznawczych przeciwnika.

Zastosowanie środków maskowania oraz zrealizowanie przedsięwzięć maskujących utrudni przeciwnikowi zlokalizowanie miejsca rozwinięcia stanowisk dowodzenia i elementów systemu łączności oraz uniemożliwi mu ich rażenie ogniowe.

PRZECIWDZIAŁANIE ZAGROŻENIOM KINETYCZNYM

Związane jest z wykonywaniem zadań zabezpieczenia bojowego przez obsady stanowisk dowodzenia oraz z zastosowaniem specjalistycznych środków.

Głównym jego elementem realizowanym na stanowisku dowodzenia zarówno podczas przemieszczania, jak i funkcjonowania w rejonie będzie ubezpieczenie. Organizuje się je w celu niedopuszczenia do przeniknięcia elementów rozpoznawczych przeciwnika oraz zapewnienia warunków do funkcjonowania SD. Do zadań ubezpieczenia należy[24]:

– umożliwienie ubezpieczanym elementom stanowiska dowodzenia wyznaczeniu odpowiednich rubieży ochrony;

– bezpośrednia ochrona SD w rejonie rozwinięcia.

Za ubezpieczenie bezpośrednie odpowiadają dowódcy wszystkich elementów stanowiska dowodzenia. Organizuje się je w każdych warunkach. W ramach ubezpieczania rozwiniętego stanowiska dowodzenia tworzy się:

– posterunek obserwacyjny na głównym kierunku spodziewanego ataku przeciwnika;

– patrole piesze wokół pierścieni wewnętrznych i zewnętrznych;

– posterunki ochronne przy: bramach wjazdowych, wejściach do stref ochronnych, elementach łączności i elementach zabezpieczenia logistycznego;

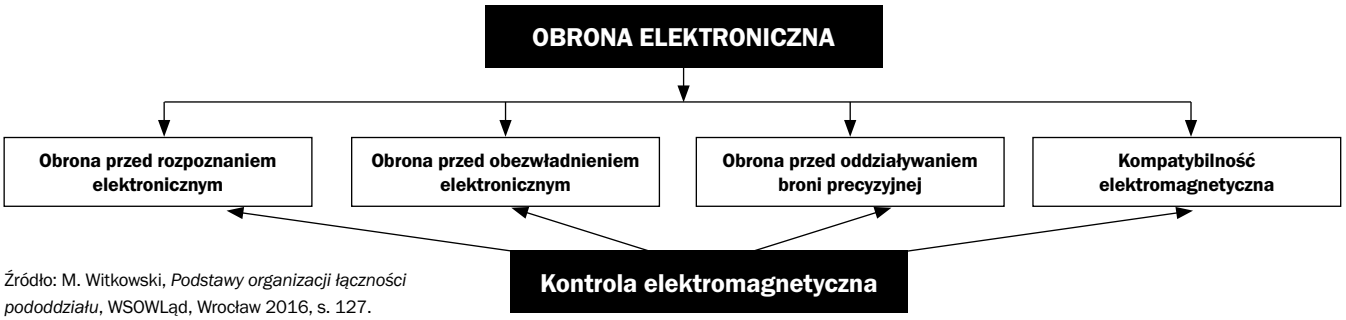
– rubieże obrony zajmowane w przypadku ataku na stanowisko dowodzenia na rozkaz komendanta SD.

Ochrona i obrona stanowiska dowodzenia może być wzmocniona pododdziałem wyznaczonym z ugrupowania bojowego. Przydzielenie do stanowiska dowodzenia plutonu zmechanizowanego/zmotoryzowanego pozwoliłoby zwiększyć możliwości ogniowe w celu przeciwdziałania aktywności grup dywersyjno-rozpoznawczych czy aktom dywersji. Dodatkowo posiadanie wzmocnienia zapewniłoby zabezpieczenie bojowe przemieszczanych kolumn SD. Dobrym pomysłem byłoby docieranie na SD łączników z utworzonych elementów ugrupowania bojowego własnymi wozami bojowymi, których załogi stanowiłyby wzmocnienie jego ochrony i obrony w czasie trwania odprawy.

Pododdziały dowodzenia szczebla brygady i dywizji mają w swoich strukturach plutony oraz kompanie ochrony i regulacji ruchu. Ich wyposażenie pozwala na ubezpieczenie stanowisk pracy obsady operacyjnej (warta wewnętrzna) oraz utworzenie odwodu komendanta SD. Jest jednak niewystarczające do pełnego ubezpieczenia rejonu rozwinięcia stanowiska dowodzenia, w przypadku zaś dywizji również elementów sieci łączności – bazowych węzłów łączności. Utrzymywanie w pobliżu SD kompanii

24 *Regulamin działań wojsk lądowych,* DWLąd, Warszawa 2008, s. 343.

RYS. 2. ZAKRES PRZEDSIĘWZIĘĆ OBRONY ELEKTRONICZNEJ



Źródło: M. Witkowski, *Podstawy organizacji łączności pododdziału*, WSOWLąd, Wrocław 2016, s. 127.

lub batalionu zapasowego umożliwi wykonywanie zadań na posterunkach ochronnych.

Kolejnym przedsięwzięciem jest powszechna obrona przeciwlotnicza (POPL). Jej organizatorami są dowódcy wszystkich szczebli dowodzenia. Obejmuje ona[25]:

– rozpoznanie przeciwnika powietrznego, które na stanowisku dowodzenia należy do żołnierzy z posterunku obserwacyjnego, a w trakcie przemieszczania do obserwatorów z załogi każdego pojazdu;

– alarmowanie pododdziałów o zagrożeniu z powietrza;

– prowadzenie zorganizowanego ognia do celów powietrznych z użyciem niespecjalistycznych środków (1/3 stanu osobowego stanowiska dowodzenia);

– maskowanie przed rozpoznaniem z powietrza;

– rozśrodkowanie wojsk [rozmieszczenie sił i środków stanowiska dowodzenia w odstępach i odległościach określonych normami w celu zmniejszenia skutków uderzeń środków napadu powietrznego (ŚNP)];

– przygotowanie schronów i ukryć (szczelin) przeciwlotniczych (1/3 stanu osobowego stanowiska dowodzenia w schronach);

– likwidację skutków uderzeń ŚNP (występowanie przy SD zastępu straży pożarnej, możliwość udzielania pomocy medycznej przez grupy/zespoły zabezpieczenia medycznego).

Stanowisko dowodzenia może być jednym z obiektów osłony pododdziałów OPL, co pozwoli zwalczać ŚNP za pomocą specjalistycznego uzbrojenia. Do SD mogą zostać przydzieleni strzelcy przeciwlotnicy z PPZR Grom lub samobieżne przeciwlotnicze zestawy rakietowe Poprad.

Rozbudowa fortyfikacyjna stanowiska dowodzenia będzie wiązała się z realizacją zabezpieczenia inżynieryjnego polegającego na przystosowaniu terenu do specyfiki jego rozmieszczenia. Będzie ono polegało na zwiększeniu efektywności obrony przed środkami rażenia, czyli na: wykonywaniu ukryć dla stanu osobowego i na sprzęt, utrudnianiu dostępu przez tworzenie zawał i niszczeń; użyciu środków minerskich na kierunku prawdopodobnego działania przeciwnika[26]. Dodatkowo należy przeszukać teren i drogi w celu wykrycia min lub improwizowanych urządzeń wybuchowych w rejonie rozwinięcia, jak i na drodze marszu kolumn stanowiska dowodzenia. Obrona przed bronią masowego rażenia (OPBMR) to zespół przedsięwzięć, których celem jest ograniczenie skutków jej użycia przez przeciwnika, w tym również toksycznych środków przemysłowych. Urządzenia filtrowentylacyjne umieszczone na mobilnych modułach stanowiska dowodzenia są w stanie zapewnić ciągłą pracę obsady operacyjnej. Ponadto urządzenia te zamontowane w wozach dowodzenia typu ZWD-1, ZWDSz-1 oraz aparatowniach pozwalają na pracę w środowisku skażonym.

OBRONA ELEKTRONICZNA

Ma na celu zapewnienie swobody funkcjonowania wojsk własnych w widmie elektromagnetycznym, czyli uodpornienie systemów radioelektronicznych przed skutkami oddziaływania przeciwnika (rys. 2). Obejmuje wiele przedsięwzięć uniemożliwiających lub utrudniających przeciwnikowi prowadzenie rozpoznania elektronicznego systemu łączności, zakłócania elektronicznego oraz informacyjnego[27].

Należy tu wymienić przedsięwzięcia techniczne i organizacyjne zabezpieczające obiekty radioelektroniczne przed porażeniem ogniowym, zakłóceniami radioelektronicznymi i dywersją radiową[28]. Elementy łączności występujące na stanowisku do-

25 Ibidem, s. 345–348.

26 *Regulamin działań wojsk...,* op.cit., s. 343.

27 M. Witkowski, *Podstawy organizacji łączności pododdziału*, WSOWLąd, Wrocław 2014, s. 38.

28 Ibidem, s. 39.

wodzenia są zobowiązane chronić swoje systemy radioelektroniczne przed[29]:

– rozpoznaniem radioelektronicznym;

– rażeniem ogniowym, w tym także środkami naprowadzanymi na źródła promieniowania energii EM;

– zakłóceniami radiowymi i próbami dywersji radiowej;

– zakłóceniami wzajemnymi.

Podstawowym sposobem obrony elektronicznej jest emisja radiowa tylko w konkretnych przypadkach. W razie braku konieczności wykorzystania radiostacji środki radiowe powinny pracować w odbiorze dyżurnym. Do kolejnych przedsięwzięć obrony elektronicznej należą:

– krótki czas pracy radiostacji na nadawanie;

– praca radiostacji z minimalną mocą umożliwiającą zachowanie wierności transmisji;

– gdy to możliwe, wykorzystywanie anten kierunkowych;

– przestrzeganie przepisów korespondencji radiowej;

– ścisłe zarachowanie dokumentów łączności (również plików) związanych z konfiguracją systemów łączności radiowej.

Zniwelowaniu skutków walki radioelektronicznej przez przeciwnika może służyć wybranie odpowiedniego trybu pracy środków radiowych.

Rozwiązaniem, które może chronić własne systemy łączności przed celowymi i przypadkowymi zakłóceniami oraz częściowo przed podsłuchem i przechwyceniem transmitowanych danych, jest wykorzystanie urządzeń radiowych, radioliniowych i satelitarnych pracujących w technice skaczącej częstotliwości nośnej (Frequency Hopping – FH) oraz ochrona tajemnicy środków radiowych. Technika FH pozwala na jednoczesną pracę wielu stacji radiowych w tym samym przedziale dostępnego pasma częstotliwości. Zapewnia równomierne rozłożenie obciążenia wykorzystywanego dostępnego pasma emisji radiowych. Elektroniczne środki zabezpieczenia (Electronic Protective Measure – EPM) to większy obszar działań, w ramach którego zapewnia się utajnianie transmisji (Transmission Security – TRANSEC) oraz ochronę tajemnicy środków łączności (Communications Security – COMSEC)[30].

Tryb FH chroni taktyczny system łączności radiowej przed podsłuchem dzięki stosowaniu na kierunku radiowym technikę pseudolosowej zmiany częstotliwości. Cyfrowe szyfrowanie transmitowanych danych zabezpiecza je przez zastosowanie unikatowego algorytmu, którego odpowiednio dobrana moc kryptograficzna gwarantuje bezpieczeństwo. Skoki odbywają się na stosunkowo dużej liczbie wybranych oraz niezakłóconych częstotliwości. W przypadku stosowania odbiorników szerokopasmowych istnieje możliwość wykrycia i przechwycenia części lub wszystkich transmitowanych fragmentów. Poprawne wytypowanie i wybranie tych fragmentów ze zbioru innych pochodzących od naturalnych i sztucznych źródeł zakłócających jest jednak zadaniem bardzo trudnym i czasochłonnym. Wykorzystanie technik FH zapobiega[31]:

– wykryciu transmitowanych sygnałów radiowych,

– zagłuszeniu transmisji w wykorzystywanych relacjach radiowych,

– zmniejszeniu redundancji łącza radiowego.

Zdolność do pracy w trybie FH mają radiostacje rodziny PR4G (w tym F@stNet) firmy Radmor oraz KF firmy Harris.

Radiostacje rodziny PR4G mają też tryb pracy FCS (poszukiwanie wolnego kanału). Za każdym przełączeniem radiostacji na nadawanie wybiera ona niezakłóconą częstotliwość roboczą w granicach podpasm zdefiniowanych podczas wstępnego przygotowania radiostacji do pracy. Radiostacje KF firmy Harris pracują w trybach ALE, 3G i 3G+ pozwalających na automatyczne zestawianie połączeń (na kanale cechującym się najlepszymi warunkami transmisji – niezakłóconym). Radiostacje szerokopasmowe firmy Harris mają zabezpieczenie przed przeciwdziałaniem radioelektronicznym dzięki pracy na częstotliwości skokowej oraz lepszemu szyfrowaniu danych z wykorzystaniem szyfrowania Type-1. Na bezpieczeństwo ich pracy wpływają także możliwości programowania za pomocą urządzeń do wprowadzania danych radiowych lub oprogramowania, które pozwala po podłączeniu radiostacji do komputera na konfigurowanie sieci łączności radiowej.

Dodatkowo elementami zwiększającymi bezpieczeństwo łączności jest rozwijanie pozornych sieci radiowych, kontrola emisji elektromagnetycznej wojsk własnych oraz wykorzystanie właściwości terenu umożliwiających maskowanie pracy środków radiowych przed rozpoznaniem radioelektronicznym przeciwnika.

WIELE DO ZROBIENIA

Poszukując sposobów przeciwdziałania oddziaływaniu przeciwnika na stanowiska dowodzenia, autorzy skłaniają się do konkluzji, że oprócz realizacji przedsięwzięć zabezpieczenia bojowego w celu skutecznej ich ochrony potrzebny jest wysiłek innych rodzajów wojsk (dodatkowe siły do ochrony i obrony). Ponadto, by skutecznie przeciwdziałać w wymiarze spektrum elektromagnetycznego, proponowana jest realizacja pasywnej obrony elektronicznej przez załogi elementów łączności na stanowisku dowodzenia.

Rozważania podjęte na łamach artykułu nie wyczerpują w pełni problematyki związanej z możliwościami oddziaływania przeciwnika na system łączności oraz ze sposobami przeciwdziałania jego działaniom mającym na celu zniszczenie lub zakłócenie pracy elementów stanowiska dowodzenia. Przedstawione problemy mogą być zatem podstawą do dalszych poszukiwań. ■

29 W. Scheffs, *Batalion walki radioelektronicznej w działaniach operacyjnych*, AON, Warszawa 2002, s. 126.

30 W. Jabłoński, *Utajnianie transmisji w systemach radiowych HF*, „Przegląd Sił Zbrojnych" 2018 nr 4, s. 52.

31 Ibidem, s. 52–53.

Nowy wymiar **łączności radiowej KF**

CYFROWA ŁĄCZNOŚĆ RADIOWA NA FALACH KRÓTKICH (KF) TO PRZEDE WSZYSTKIM ZAAWANSOWANE TECHNOLOGIE INFORMATYCZNE NIEMAJĄCE NIC WSPÓLNEGO Z TRADYCYJNYM WYKORZYSTANIEM RADIOSTACJI ERY ANALOGOWEJ.

ppłk mgr inż. Robert Kozłowski

Autor jest szefem Wydziału Mobilnych Sieci Bezprzewodowych w Centrum Wsparcia Systemów Dowodzenia Sił Zbrojnych.

W artykule przybliżono praktyczne wykorzystanie łączności radiowej KF walczących pododdziałów. Zamieszczone rozważania opierają się na możliwościach, jakie oferuje użytkowany w siłach zbrojnych sprzęt radiowy i oprogramowanie firmy Harris.

Od kilku lat w 12 Szczecińskiej Dywizji Zmechanizowanej trwają prace nad wypracowaniem optymalnego systemu krótkofalowej łączności radiowej ugrupowania bojowego dywizji spełniającego wymogi pola walki. Nasze działania zdominowały czynniki determinujące prostotę konfiguracji i możliwość elastycznego tworzenia ugrupowania bojowego stosownie do otrzymanych zadań. Centralnie zaplanowany i wdrożony system łączności radiowej KF znacznie ułatwia funkcjonowanie ugrupowania bojowego każdego szczebla dowodzenia. Ujednolica poziom zaawansowania technicznego planistów i operatorów, co przy dużych brakach kadrowych i mało optymalnym systemie podnoszenia poziomu wiedzy i kwalifikacji stwarza idealne możliwości wykorzystania go w dywizji. Podstawowy warunek, który musi zostać spełniony, to dysponowanie jednolitym cyfrowym sprzętem łączności radiowej KF w całej organizacji. Wówczas z powodzeniem można zastosować prezentowane rozwiązania.

ZAŁOŻENIA

Opierając się na możliwościach sprzętu radiowego, wdrożonych innych systemach teletransmisyjnych, uwarunkowaniach obiegu informacji oraz specyficznych potrzebach osób funkcyjnych, udało się wyodrębnić kilka kluczowych zagadnień wymagających uwagi przy projektowaniu systemu.

Naturalnym bezprzewodowym rozszerzeniem domeny informacyjnej (sieci komputerowej) funkcjonującej na stanowiskach dowodzenia jest sieć radiowa. Zapewnia ona możliwość dostarczenia wiadomości w pierwotnym obiegu informacji do elementów mobilnych oraz do tych, które nie mają możliwości być włączone w przewodowy system teletransmisyjny. Wyższość transmisji danych nad łącznością foniczną wynika z uwarunkowań, jakie dostarcza nam sprzęt i wykorzystana w nim technologia. Nie bez znaczenia jest także ukompletowanie peryferyjne, które daje możliwość wyniesienia usług poza pojazd z radiostacją czy wóz dowodzenia. Nadrzędnym celem było uniezależnienie dowódców od *odległości od mikrotelefonu* oraz wkomponowanie możliwości oferowanych przez środki radiowe w miejsca pracy osób funkcyjnych na stanowisku dowodzenia. Obecnie dostarczenie usług radiowych, głównie fonicznych, *na biurko* jest w większości wypadków trudne do zrealizowania.

Należy podkreślić brak użyteczności pracy fonem, zwłaszcza w pracy sztabowej. Zaimplementowane mechanizmy obsługi ruchu radiowego nie pozwalają już chwycić za mikrotelefon i rozmawiać. Wcześniej należy wykonać wiele czynności, które wymagają bezpośredniego dostępu do radiostacji i obsługi panelu klawiatury. Połączenie foniczne z abonentem, z którym chcemy prowadzić wymianę informacji, jest zestawiane manualnie. Inicjalizacja radiostacji KF do pracy z wybranym abonentem sie-

BOGUSŁAW POLITOWSKI

Wydanie rozkazu brygadowego powoduje dystrybucję objętościowo dużych plików i problem przesyłania tego samego dokumentu bojowego kolejno do każdego z podległych elementów.

ci jest unikatowa. Zawiera mechanizmy sondowania jakości sygnału do aktualnych warunków propagacji fal i doboru optymalnej częstotliwości na kierunku wybranego abonenta. Właśnie z tego powodu rozmowa na okólnik w fonicznej sieci KF jest całkowicie bezzasadna. Pomija wszystkie mechanizmy optymalizacji kanału radiowego i wraca do czasów, kiedy komunikacja była zdana tylko na zadowalające warunki propagacyjne. Możliwości transmisji danych w kanale radiowym KF wybiegają o wiele dalej niż praca fonem. W najnowszych i bezpieczniejszych trybach funkcjonowania radiostacji KF praca fonem jest już niemożliwa.

Wymogiem koniecznym, wynikającym z obranego systemu obiegu informacji i dostosowanego do niego systemu meldunkowego, są konsekwencje ujednolicenia klauzuli tajności sieci radiowej z przewodową. Wymusi to, ewentualnie, stosowanie bardziej skomplikowanych rozwiązań, takich jak wprowadzenie praktyk integrujących różne klauzule bezpieczeństwa systemów przewodowych i radiowych wraz z markerami gradacji poufności przesyłanych informacji.

Integrując system radiowy, niezbędne staje się dostosowanie obowiązujących procedur bezpieczeństwa. Muszą one być wynikiem kompromisu między rozwiniętym systemem zabezpieczeń przewodowych systemów informatycznych a zagrożeniami wynikającymi z wykorzystania łączności bezprzewodowej. W 12 Dywizji Zmechanizowanej przyjęto, że optymalnym trybem wymiany danych w sieciach radiowych KF pod względem cyberbezpieczeństwa oraz oddziaływania elektromagnetycznego będzie usługa poczty elektronicznej. Jest ona stosunkowo łatwa do zabezpieczenia oraz elastyczna w integracji z systemem przewodowym. Jednym z ważniejszych aspektów wyboru usługi poczty elektronicznej w kanale radiowym jest to, że transmisja w kanale nie jest *czystą* transmisją IP. Kanał radiowy nie jest widoczny dla całości ruchu sieciowego w systemie teleinformatycznym. Dzięki temu nie istnieje możliwość *zapchania* i tak już bardzo wąskiego kanału KF danymi pochodzącymi z innych usług sieci teleinformatycznej.

Specyfika łączności KF wynika z bardzo ograniczonego kanału przepływu informacji. Wykorzystując tę formę, należy się liczyć z tym, że wiadomości dotrą z opóźnieniem i nie mogą być zbyt obszerne. Ponadto trzeba brać pod uwagę dużą zmienność warunków propagacji fal radiowych. Utrzymanie kanału do świadczenia usług jest bardzo trudne. Przerwy w łączności radiowej KF są nieprzewidywalne i nieuniknione. Mimo tych niedogodności, spoglądając na łączność radiową KF z innej perspektywy, na przykład wad wymiany informacji za pomocą poczty polowej, można się pokusić o stwierdzenie, że ten rodzaj łączności bezprzewodowej jest bardziej przystępny i pożądany w każdym z bojowych aspektów jej wykorzystania.

Optymalizacja ruchu w kanale radiowym jest najważniejszym celem naszych działań. Temu zagadnieniu poświęciliśmy najwięcej czasu. Wytypowaliśmy najodpowiedniejsze tryby pracy dostępne w radiostacjach. Gwarantują one z jednej strony po-

żądaną jakość połączenia, a z drugiej – zapewniają transmisję danych z zadowalającą prędkością. Maksymalne wykorzystanie mechanizmów bezpieczeństwa ochrony informacji i transmisji było naszym priorytetem. Odpowiednie zarządzanie częstotliwościami pozwoliło zredukować ilość wykorzystywanych nominałów do absolutnego minimum, zapewniając jednocześnie szerokie spektrum doboru częstotliwości roboczych stosownie do warunków propagacyjnych. Plan radiowy obejmuje kilka nominałów częstotliwości dobranych odpowiednio do warunków propagacji fal KF. Samowystarczalność w doborze właściwych częstotliwości do planów radiowych KF dywizji, włączając w to jednostki podległe, nie byłaby możliwa bez współpracy z Wojskowym Biurem Zarządzania Częstotliwościami. Wykorzystanie środków cyfrowych i zrozumienie odmienności przyjętych rozwiązań od obowiązujących standardów w doborze częstotliwości KF pozwoliło zredukować prawie o jedną trzecią ilość używanych częstotliwości w porównaniu do innych związków taktycznych wojsk lądowych.

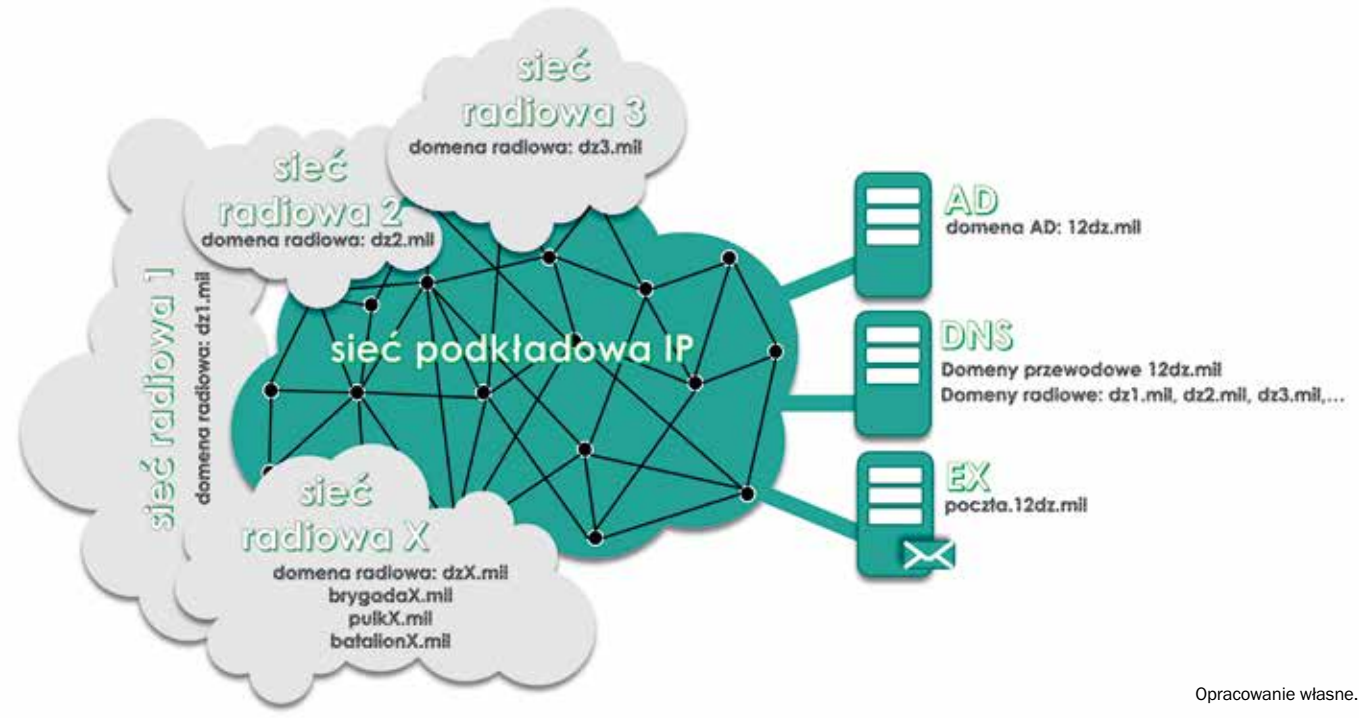
Brak nadzoru nad zajętością kanału radiowego jest elementem, który determinuje sposób pracy w sieci radiowej. Niestety, wykorzystując transmisję danych, nie mamy kontroli nad momentem wykorzystania kanału radiowego. Radiostacja automatycznie inicjuje nadawanie z chwilą otrzymania zadania wysłania poczty elektronicznej. Zagwarantowanie dostępności kanału radiowego oraz redukcja kolizji są realizowane m.in. dzięki zwielokrotnieniu częstotliwości. Newralgicznym aspektem jest wykorzystanie trybu pracy z aktywnym mechanizmem automatycznego zestawiania połączenia między dwoma abonentami (Automatic Link Establishment – ALE). Mechanizm ALE przed nadawaniem sonduje fale eteru podczas stale zmieniających się warunków propagacji jonosferycznej, zakłóceń odbioru oraz współdzielenia widma, wybierając optymalny nominał częstotliwości. Jest on gwarantem automatycznego wyboru częstotliwości roboczej o najwyższej jakości z puli tych zakłóconych i już zajętych. Umożliwia to realizację większych przepływności, a zatem skraca czas nadawania.

Jeszcze większą efektywność transmisji radiowych zapewnia redukcja odległości między miejscem nadawania i odbioru. W naszym systemie, dzięki integracji systemu radiowego z siecią WAN, lokalizacja nadajnika i odbiornika nie musi być tożsama z lokalizacją adresata i nadawcy. Ta funkcjonalność zostanie opisana bardziej szczegółowo w dalszej części artykułu. Zmniejszenie odległości zapewnia dodatkową korzyść, jaką jest redukcja mocy nadawania. Niższa moc nadawania pozwala na użycie tych samych częstotliwości w innej lokalizacji między inną parą nadawcy i odbiorcy. System radiowy w wypadku kolizji lub braku obecności abonenta w sieci automatycznie powtarza wysyłanie wiadomości o założoną ilość razy. Może automatycznie przekazać wiadomość, niekoniecznie drogą radiową, do innych wyznaczonych korespondentów sieci, którzy z założenia będą świadczyć usługę przekazywania wiadomości. Rozwiązanie takie zwiększa dostępność abonentów radiowych, zwłaszcza dostępność radiostacji przełożonego, która zwyczajowo generowała największy ruch w sieci radiowej.

Ochrona elektromagnetyczna oraz kontrola emisji są równie ważnymi czynnikami, choć po lekturze poprzedniego akapitu można odnieść przeciwne wrażenie. To właśnie dzięki wykorzystaniu technologii IP oraz integracji radiostacji z przewodowym systemem teletransmisyjnym uzyskaliśmy możliwość ustalania priorytetów sposobu wysyłania wiadomości. Oprogramowanie systemowe radiostacji (Wireless Messaging Terminal – WMT) potrafi dynamicznie wykorzystywać dostępne media transmisyjne. W pierwszej kolejności WMT dokona próby nawiązania połączenia IP między abonentami z pominięciem środków radiowych KF. Natomiast kiedy nastąpi wykorzystanie kanału radiowego, odpowiednio konfigurując sposób zestawiania połączeń radiowych, można uzyskać zdolność wysyłania wiadomości z minimalną mocą do najbliżej położonej radiostacji i co do zasady optymalizacji – połączonej z siecią IP WAN. Wiadomość jest przekazywana automatycznie, transparentnie i prawie niezauważalnie dla operatora pośredniczącej radiostacji. Użycie zmniejszonej mocy i skrócenie czasu nadawania obniża możliwość wykrycia. Maskuje system radiowy, używając połączeń w sieci IP WAN kanału radiowego tylko wtedy, kiedy jest to absolutnie konieczne. W wypadku namierzenia wykrycie ugrupowania bojowego jest utrudnione z powodu nietożsamych lokalizacji nadajników z topologią i hierarchią sieci radiowej. Włączenie trybu kontroli emisji jest tożsame z wyłączeniem nadajnika radiostacji, lecz nie jest jednoznaczne ze zniknięciem radiostacji z sieci. Radiostacja nadal będzie odbierać i wysyłać wiadomości, jeśli ma dostęp do innego medium transmisyjnego.

Pliki konfiguracyjne radiostacji – plany radiowe to cyfrowy zbiór informacji o konfiguracji całej sieci radiowej. Obejmują techniczne, specyficzne dane dla pojedynczych stacji radiowych i sposobu ich dostępu do kanału radiowego KF. Zawierają też informacje o otaczającym tę sieć radiową świecie zewnętrznym i możliwościach dostępu do innych mediów w systemie teletransmisyjnym. Od strony radiowej pliki konfiguracyjne obejmują kilka nominałów częstotliwości w granicach minimalnej i maksymalnej użytecznej wartości częstotliwości wyznaczonych prognozą jonosferyczną. Jonosfera bardzo szybko się zmienia, dlatego wprowadzono w plikach konfiguracyjnych kilka planów radiowych, np.: dzienny, nocny i zapasowy z przydziałem częstotliwości dla warunków dzienno-nocnych. Ten zabieg jeszcze bardziej optymalizuje wykorzystanie częstotliwości, skraca

RYS. 1. SCHEMAT POGLĄDOWY INTEGRACJI SYSTEMU RADIOWEGO KF Z PRZEWODOWYM SYSTEMEM TELETRANSMISYJNYM



Opracowanie własne.

czas sondowania mechanizmu ALE, co przekłada się na minimalizację ryzyka wykrycia emisji. Poprawia też możliwości operacyjne sieci, umożliwiając manewr częstotliwościami. Szybkie przejście na inne nominały częstotliwości, bez przeprogramowywania każdej radiostacji w sieci, pozwala unikać zakłóceń celowych, a także zamaskować rozpoznane lokalizacje nadawania i zmylić co do topologii sieci.

Od strony przewodowej dość ważna z punktu widzenia tego artykułu jest tabela routingu, która informuje radiostacje o innych sposobach komunikacji IP między abonentami. Te ustawienia wpływają na formy planowania i użytkowania sieci radiowych KF jako bezprzewodowego kanału transmisyjnego o statycznych ustawieniach strony przewodowej. Konsekwencje tego poznamy w dalszej części artykułu. Jednak najważniejszą zaletą plików konfiguracyjnych jest ich użyteczność w czasie programowania radiostacji. Manualne programowanie przerasta możliwości operatora, tym bardziej że musi on wprowadzić do swojej stacji dane o wszystkich radiostacjach w sieci. Ustawień jest tak dużo, że zwykle bazuje się na ustawieniach domyślnych. W trybach zaawansowanych z włączonymi mechanizmami bezpieczeństwa kryptograficznego programowanie manualne jest niemożliwe. Niemożliwe jest też śledzenie przez każdego operatora zmian technicznych wprowadzanych przez innych abonentów sieci. Zmiany w konfiguracji jednej radiostacji wymagają powielenia zmian lokalnie u wszystkich innych abonentów sieci radiowej. Dlatego system zapisu całej sieci radiowej w jednym pliku jest niezmiernie funkcjonalny. Ponadto taki sposób programowania nie wymaga od operatorów interpretacji zapisów planistów systemu i umożliwia zróżnicowanie konfiguracji do potrzeb konkretnego abonenta. Stosując plik konfiguracyjny, korzyści wynikające z redukcji błędów, jakie mógłby popełnić każdy z operatorów, są niezaprzeczalne.

PLANOWANIE SYSTEMU RADIOWEGO KF

Instrukcyjne możliwości systemu nigdy nie będą równe jego możliwościom w środowisku docelowym. Jest dużo syntetycznych opracowań dotyczących możliwości systemów łączności i informatyki i niewiele empirycznych publikacji na temat wdro-

żeń w konkretnym ekosystemie procedur i kultury organizacji. Wiele możliwości technicznych nowego systemu zostanie wykluczonych lub bardzo ograniczonych z różnych powodów. Na kształt systemu łączności mają wpływ szczególnie kwestie bezpieczeństwa i kompatybilności wstecznej z użytkowanym już sprzętem różnych generacji.

Poniższe dylematy planistyczne dotyczą zarówno sfery normatywnych rozwiązań proceduralnych, jak i ukompletowania oraz przyjętych wymogów taktycznych. Oto kilka najważniejszych i innowacyjnych, z którymi przyszło nam się zmierzyć. Wymienione zagadnienia mają charakter poglądowy i są zbieżne z tymi, które zapewne zostały wygenerowane przez inne osoby mające doświadczenie w integracji radiostacji rodziny Harris w sieci WAN. Rozważania nie zawierają wrażliwych rozwiązań wdrożonego systemu w 12 Dywizji Zmechanizowanej.

Integracja z domeną informacyjną. Koncepcja adresacji i nazewnictwo komponentu radiowego. Włączenie systemu radiowego KF do systemu transmisyjnego sieci komputerowej używanej na stanowiskach dowodzenia tworzy alternatywny kanał przepływu informacji. Może on współistnieć z szerokopasmowym dostępem LAN/WAN. System radiowy będzie się odwoływał do najlepszych właściwości sieci przewodowej i działał bez wykorzystania medium radiowego zawsze, gdy radiostacje będą dołączone do sieci komputerowej (rys. 1). Z chwilą, gdy jeden z użytkowników radiostacji utraci połączenie przewodowe, stanie się mobilny, system automatycznie wykryje ten stan i udostępni usługę dostarczania wiadomości bezprzewodowo – drogą radiową. Kanały radiowe KF stają się pełnoprawnym (w naszym wariancie celowo ograniczonym tylko do przepływu usługi poczty elektronicznej) medium transmisyjnym. Nie działają już jako środki odwodowe czy zapasowe w wypadku awarii głównego systemu transmisyjnego. Integracja systemów przewodowych i radiowych daje swobodę mobilności i jednocześnie dba o komfort tych użytkowników, którzy nie są świadomi ruchu adresata.

Głównym wyzwaniem jest ustalenie adresacji IP komponentu radiowego. Czynnością bezwzględną jest opracowanie adresacji IP dla każdego stanowiska dowodzenia. Jeżeli warunek ten zostanie spełniony, to jednoznacznie będziemy mogli odpowiedzieć na kluczowe pytanie: jaki jest mój adres radiowy. Adresacja IP i nazewnictwo domen radiowych muszą pozostać niezmienne. Zostanie to potwierdzone w dalszej części artykułu, gdzie szczegóły konfiguracji systemu radiowego unaocznią identyczne wymagania jak dla sieci komputerowych. Dotychczasowy sposób organizacji łączności radiowej stanie się nieaktualny i nieadekwatny do wymaganych czynności konfiguracyjnych. Niezmienna pozostaje możliwość dokonywania zmian puli częstotliwości. Zmiany rzutujące na całą sieć teleinformatyczną są bardzo niewskazane, a nawet niemożliwe. System radiowy musi być zaprojektowany jako zwarta konstrukcja przystająca budową do systemu przewodowego. Nie da się starym zwyczajem poprawnie zaplanować i uruchomić sieci radiowej przy obowiązującym rozdziale kompetencji na osoby funkcyjne segmentu radiowego i informatycznego. Użycie trybu transmisji danych w kanale radiowym będzie przezroczyste dla użytkownika, zarówno radiowego, jak i przewodowego. Zniknie istniejący podział sieci radiowych na sieci służące jednemu celowi, jak sieci dowodzenia lub też współdziałania. Oprócz tego nie będzie można ich charakteryzować ich specjalistycznym przeznaczeniem, na przykład rozpoznania lub logistyki. Każda informacja zostanie przesłana w sieci radiowej, podobnie jak dzieje się to w przewodowej sieci komputerowej, w której, z technicznego punktu widzenia, nie ma znaczenia, czy dana wiadomość dotyczy logistyki, czy dowodzenia.

Planując sieć radiową KF, należy wziąć pod uwagę, na jakich stanowiskach dowodzenia będzie miała ona funkcjonować. Tryb cyfrowy wymusza uwzględnienie w planach radiowych wszystkich możliwych korespondentów, których liczba jest ograniczona. Inaczej niż dotychczas należy przewidzieć unikatowy zestaw konfiguracji dla każdej radiostacji, uwzględniając manewr stanowiskami dowodzenia. Wynikiem tego jest zajęcie kilku pozycji w planie sieci radiowej na radiostacje jednej organizacji, wynikające z modelu funkcjonowania stanowisk dowodzenia. Każda radiostacja jest skonfigurowana unikatowo, uwzględniając adres IP sieci LAN stanowiska dowodzenia. Niemożliwe jest funkcjonowanie radiostacji z jednego stanowiska dowodzenia na innym stanowisku, tak jak nie jest możliwe przenoszenie stacji roboczej między sieciami komputerowymi bez ich rekonfiguracji. Konsekwencją tych zmian jest utracenie możliwości funkcjonowania w poprzednim stanie i uzyskanie kompletnie nowego zestawu ustawień. Mając na uwadze, że zmiany ustawień abonentów radiowych należy powielić u wszystkich abonentów sieci radiowej, dochodzimy do wniosku, że budowa systemu radiowego KF ma charakter statyczny.

Ilość i dostępność sieci (kanałów) radiowych. Na wszystkich szczeblach dowodzenia, projektując sieć radiową, należy przewidzieć nadmiarowość i ująć w planie docelową liczbę zestawów konfiguracyjnych poszczególnych radiostacji. Każda zmiana topologii sieci radiowej będzie wymagała zmian na wszystkich radiostacjach w sieci radiowej oraz ich uwzględnienia w systemie przewodowym informacjami o styku z systemem radiowym. Powiązanie systemu radiowego z systemem przewodowym zapewnia przepływ wiadomości między abonentami różnych sieci radiowych oraz użytkownikami sieci przewodowych. Zwiększenie liczby radiostacji KF na stanowisku dowodzenia prowadzi do zwielokrotnienia możliwości transmisyjnych tylko w wypadku

pracy w oddzielnych sieciach (kanałach). Przypisanie radiostacji do sieci może być przypadkowe, ale spełniające jedynie jedno kryterium, jakim jest przewidywane obciążenie kanału radiowego. Nie ma już bowiem związku abonenta i radiostacji z podmiotem celowości organizacji sieci – kanał radiowy jest medium transmisyjnym dostępnym dla każdego użytkownika poczty.

Bojowe wykorzystanie przedstawionych właściwości systemu radiowego KF sprowadza się do zaplanowania kilku kanałów (sieci) radiowych z przeznaczeniem dla wszystkich elementów ugrupowania bojowego jednego poziomu (nadmiarowo). Nadwyżka możliwości konfiguracji abonentów radiowych w planach radiowych pozwoli na elastyczne dodawanie przydzielonych, wspierających i współpracujących elementów do ugrupowania bez konieczności wprowadzania zmian w całym systemie ZT. System radiowy jest skalowalny i jeśli zaplanowano go w sposób przemyślany, może połączyć wszystkie szczeble dowodzenia. Wówczas tworzenie ugrupowania bojowego oraz roszady podległości pododdziałami nie wywierają żadnego wpływu na system łączności radiowej KF. Mimo zmiany podległości danego elementu nie ma potrzeby zmiany jego systemu łączności radiowej. Pracuje on dalej w swoim kanale radiowym KF, a dowodzenie odbywa się przez wymianę informacji z wykorzystaniem już zorganizowanych relacji radiowych.

Opierając się na przedstawionych tezach, możemy zejść jeszcze niżej w procesie planowania systemu łączności radiowej KF i zdefiniować wiele nowych zależności, które nigdy nie były zauważalne lub ważne, przez co pomijane.

Kryptonim radiostacji KF definiuje stanowisko dowodzenia. Znany wszystkim kryptonim AIR FORCE ONE kryje unikatowe znaczenie. We wdrożonym w 12 Dywizji Zmechanizowanej systemie łączności radiowej KF kryptonimy radiowe nabierają podobnego wymiaru. Nowa funkcjonalność kryptonimu radiowego jest o wiele szersza od obecnie stosowanego. Oprogramowanie firmy Harris wykorzystuje kryptonimy radiostacji do tworzenia nazewnictwa domen radiowych i kont pocztowych. Pomysłów na powstawanie domen radiowych może być mnóstwo, ale naturalne dla każdego żołnierza jest odniesienie ich do kryptonimu stanowiska dowodzenia i jego węzła łączności.

We wczesnej fazie projektowania naszego systemu KF sprawdzaliśmy koncepcję rozdzielenia strony technicznej od części proceduralnej sieci radiowej. Chcieliśmy, aby relacja łączności – sieć radiowa – była zbudowana niezależnie od zabezpieczającej ją strony technicznej. Budowa sposobu wymiany informacji jest niezmienna i ujęta w stałych procedurach operacyjnych. Natomiast od strony technicznej każdy zestaw konfiguracyjny sieci jest w stanie zabezpieczyć powyższą wymianę. Strona techniczna może dowolnie się zmieniać i nie wymusza to zmiany standardów wymiany informacji. Zupełnie inne dane pojawiają się na wyświetlaczu radiostacji, a innymi posługują się osoby funkcyjne, gdy prowadzą wymianę korespondencji. Koncepcja ta została zarzucona ze względu na zbyt gwałtowny przeskok myślowy i odstawanie od obecnego stanu kształcenia operatorów i użytkowników radiostacji. Osoby te miały większą tendencję do stosowania kryptonimów użytych po stronie technicznej niż do wykorzystywania standardowych, ale dalej umownych danych radiowych.

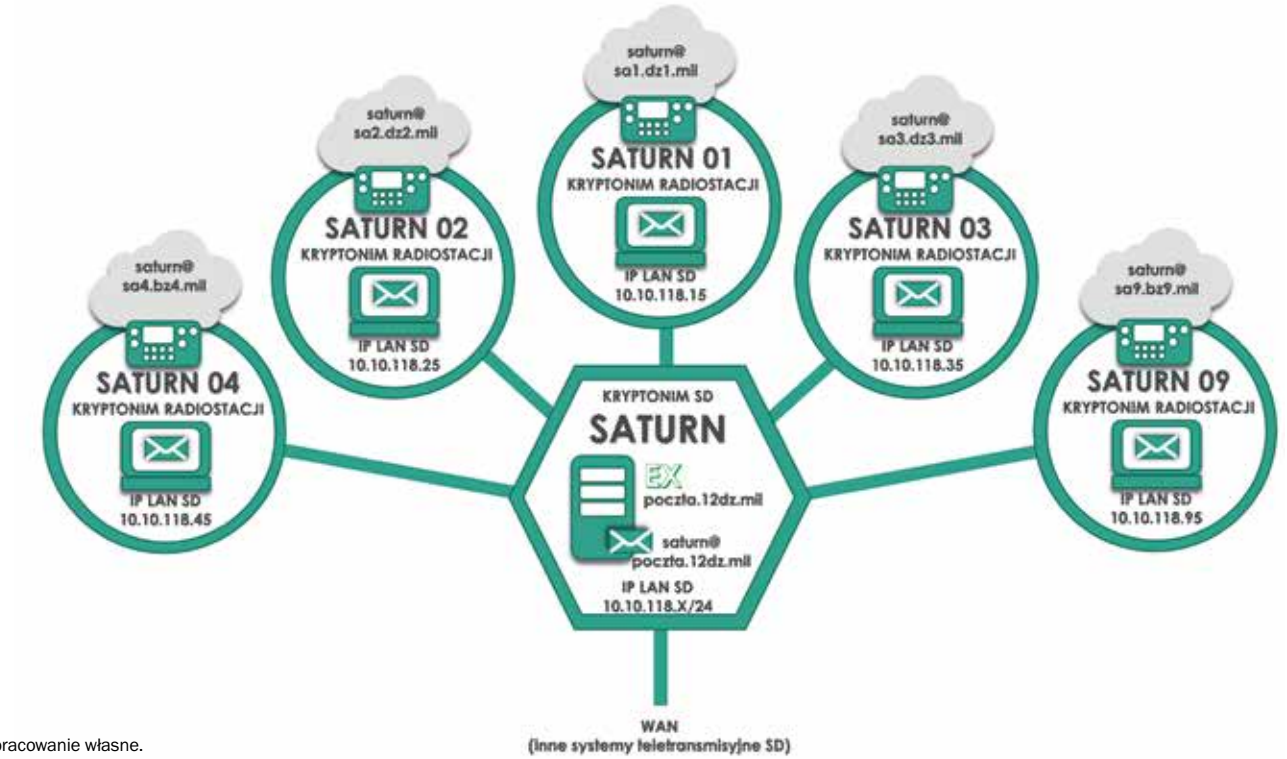
Przypisanie kryptonimu do stanowiska dowodzenia umożliwia nadanie tego samego kryptonimu wszystkim radiostacjom na nim pracującym. Mechanizm utożsamiania kryptonimu ze stanowiskiem dowodzenia jest pomocny dla innych użytkowników systemu pocztowego. Pomaga w zrozumieniu, z jakiego elementu otrzymali wiadomość pocztową lub w jaki sposób wiadomość zaadresować. Każdy może przyznać, że zrozumienie nazewnictwa, a tym samym topologii systemu radiowego, nie przyjdzie łatwo, tym bardziej jeśli system radiowy wychodzi poza jedną organizację. Należy podkreślić, że będzie wiele kryptonimów radiowych określających jedną jednostkę wojskową. Będzie ich tyle, ile stanowisk dowodzenia buduje ta organizacja. Za każdym kryptonimem stanowiska dowodzenia kryją się dane środowiska informatycznego definiowanego unikatowym adresem IP lokalnej sieci komputerowej oraz sposobem zarządzania ruchem sieciowym. Ponadto obowiązującą procedurą jest dodawanie indeksów do kryptonimów: cyfr od 01 do 99. Nie są one niezbędne, zwłaszcza gdy w danej relacji pracuje tylko jeden środek radiowy na danym stanowisku. Mając kilka środków radiowych na stanowisku pracy, wszystkie mogą być rozpoznawane tym samym kryptonimem. Można wykorzystać indeksy radiowe jako numerację funkcjonujących radiostacji w jednej lokalizacji, tym bardziej że domyślnie WMT też w pewien sposób wplata indeks w domenę radiową.

Każde stanowisko dowodzenia musi mieć *unikalny adres IP sieci LAN w systemie transmisyjnym.* Jest to wyznacznik naszych czasów. Deprecjonuje on obecnie stosowany archaiczny schemat adresów radiowych i czyni go nieużytecznym. Adresacja IP może też zastąpić numerację sieci radiowych, która jest już tylko zbiorem cyfr bez żadnego znaczenia. Przyczyni się to do opanowania złożoności koncepcji adresacji i uniknięcia dużych problemów w wypadku powielenia adresów IP.

Koncepcja adresacji IP jest jednym z najpoważniejszych wyzwań i dotyczy zarówno podsieci, jak i poszczególnych urządzeń sieciowych. Comiesięczne treningi łączności przyniosły duży wkład w opracowanie adresacji IP segmentu radiowego dywizji, a to w wyniku zaangażowania żołnierzy wojsk łączności mających różne doświadczenia i odmienny, dzięki specyfice swojej jednostki, punkt widzenia. Mimo szczegółowej fazy planowania,

NIEPRAWIDŁOWO SKONFIGUROWANE REGUŁY ODNAJDYWANIA SERWERÓW WMT W SYSTEMIE IP LUB ZASADY DOSTARCZANIA WIADOMOŚCI POCZTOWYCH MOGĄ ZDESTABILIZOWAĆ CAŁY SYSTEM.

RYS. 2. WARIANT WYKORZYSTANIA RADIOSTACJI KF NA STANOWISKU DOWODZENIA O KRYPTONIMIE SATURN



Opracowanie własne.

dopiero metodą prób i błędów opracowano plan adresacji stanowisk dowodzenia i ich urządzeń sieciowych, który funkcjonuje płynnie i bez zakłóceń.

Każdy komputer obsługujący radiostację KF (serwer poczty – WMT) musi mieć stały i niezmienny adres IP w lokalnej sieci komputerowej stanowiska dowodzenia. Jako że systemy informatyczne nie lubią dynamiki zmian wynikających z mobilności, należy zaplanować unikatową adresację dla wszystkich sieci radiowych i ujętych w nich abonentów. Niezmienność adresacji jest konieczna w razie wykorzystania poczty elektronicznej. Zmiana adresu IP serwera pocztowego zawsze powoduje druzgoczące skutki w systemie dostarczania poczty. Nazwa skrzynki pocztowej nie zawiera jej konkretnego adresu. W sieciach komputerowych serwery DNS (Domain Name System) dbają m.in. o to, by systemy pocztowe odnalazły adres IP serwera pocztowego odbiorcy na podstawie nazwy domeny. Oprogramowanie radiostacji wraz z ogólnym sposobem budowy systemów pocztowych wprowadza następną stałą – domenę radiową.

Domena radiowa w systemie łączności radiowej KF obejmuje adres sieciowy powstały na bazie stałego adresu IP serwera pocztowego WMT ze stałym kryptonimem stanowiska dowodzenia oraz indeksami kryptonimów jako identyfikację kanału radiowego. W ten oto nieunikniony sposób dochodzimy do sytuacji, gdzie wszystko opisane zaczyna się zazębiać i nabierać konkretnego wymiaru. Jego głębię pozwoli nam zrozumieć wiedza o sposobie budowy podobnych rozwiązań domenowych w klasycznych – przewodowych sieciach informatycznych. O ile koncepcja budowy domen przewodowych systemów informatycznych nie wymaga szczegółowych wyjaśnień, o tyle należy się przyjrzeć, w jaki sposób oprogramowanie firmy Harris tworzy domeny radiowe. Dość specyficzne tło stwarza również system przesyłania poczty elektronicznej, który zaprojektowano dla statycznych systemów przewodowych i narzuca on swoje reguły dynamicznemu i mobilnemu systemowi radiowemu.

Domeny to podstawowy składnik tożsamości sieciowej, który współtworzy unikatowy adres organi-

zacji w środowisku komputerowym. Na podstawie domen powstają adresy stron internetowych oraz adresy skrzynek poczty internetowej. Sfera bitowa systemów teleinformatycznych nie rozpoznaje tekstu, jakim są nazwy stron i skrzynek pocztowych. Dlatego kluczową rolę w systemie domenowym i adresacji pocztowej odgrywa serwer DNS. To właśnie on zamienia nazwę mnemoniczną przyjazną dla człowieka z postaci *domena.pl* na adres IP komputera obsługującego tę domenę. Zamiana z formy tekstowej na docelowy adres IP jest realizowana na zapytanie każdego komputera w systemie informatycznym.

Aby lepiej prześledzić proces tworzenia domen zintegrowanego systemu radiowego, należy posłużyć się przykładem. Na rysunku 2 przedstawiono wariant wykorzystania radiostacji KF na stanowisku dowodzenia o kryptonimie Saturn. Obejmuje on pięć radiostacji pracujących w pięciu oddzielnych kanałach KF. Adresacja IP sieci LAN tego stanowiska skupia wszystkie urządzenia peryferyjne, w tym radiostacje KF. Stałe są adresy IP stacji komputerowych WMT, czyli serwerów poczty odpowiadających przypisanym domenom radiowym. Warto zwrócić uwagę, że dla zachowania przejrzystości budowy systemu adresy IP serwerów WMT (ostatni oktet) są odniesieniem do indeksu radiostacji. Pozwala to wielu osobom funkcyjnym, zajmującymi się różnymi zagadnieniami sieciowymi, zrozumieć zasady budowy systemu.

Domena radiowa powstaje z wybranej przez planistów nazwy domeny najwyższego poziomu dla danego kanału radiowego. W wariancie dla stanowiska Saturn zorganizowano następujące domeny kanałów radiowych: dz1.mil, dz2.mil, dz3.mil – odpowiedniki sieci dywizyjnych – oraz domeny dla sieci brygadowych: bz4.mil i bz9.mil. Nazwy domen radiowych muszą być unikatowe. Przeprowadzone testy w 12 DZ potwierdzają zasadność tworzenia domen radiowych o innym nazewnictwie niż domeny systemu przewodowego, co ułatwia zarządzanie przepływem wiadomości pocztowych.

Wszystkie radiostacje pracujące w wybranej domenie (sieci radiowej) posiadają subdomenę utworzoną z wykorzystaniem przedrostka powstałego z pierwszych dwóch liter kryptonimu i ostatniej cyfry indeksu (sa1.dz1.mil, sa2.dz2.mil, sa3.dz3.mil, sa4bz4.mil i sa9.bz9.mil). Jest to domyślny mechanizm budowy domen, zaimplementowany w oprogramowaniu do konfiguracji sieci radiowych KF firmy Harris. Oprogramowanie pozwala na zupełną dowolność w tworzeniu domen radiowych. Stanowisko dowodzenia opisane jest różnymi adresami domen. W 12 DZ przyjęliśmy, że sposobem na optymalne zarządzanie informacją na danym stanowisku jest *wypłaszczenie* architektury systemu radiowego. Ujednolicenie nazw skrzynek pocztowych jest jednym z ważniejszych czynników wpływających na prostotę systemu łączności. Adresem ogólnym wszystkich relacji radiowych dla konkretnego stanowiska jest jego kryptonim. Adresy skrzynek saturn@saX.domenaX.radiowa (@sa1.dz1.mil, @sa2.dz2.mil, @sa3.dz3.mil, @sa4.bz4.mil i @sa9.bz9.mil) są podstawowym adresem pocztowym obsług (operatora) każdej radiostacji. Serwery pocztowe WMT potrafią obsługiwać wiele skrzynek pocztowych i można im nadać dowolne nazwy. Adresując pocztę do korespondenta Saturn w dowolnej domenie radiowej, odbiorcą staje się operator radiostacji lub zgodnie z procedurami zarządzania informacją dowolny użytkownik systemu pocztowego.

Serwer pocztowy (EX) obsługujący użytkowników systemu przewodowego nie musi być zlokalizowany na stanowisku dowodzenia Saturn, lecz musi być dostępny przez sieć IP w lokalizacji zdalnej. Natomiast umiejscowienie serwera pocztowego (EX) lokalnie na stanowisku dowodzenia pozwala na prostsze zarządzanie przepływem poczty między sieciami radiowymi bez dostępu do WAN.

W tak zintegrowanym systemie łączności radiowej KF z systemem przewodowym wymiana wiadomości pocztowych odbywa się między abonentami różnych sieci radiowych oraz między abonentami radiowymi i użytkownikami sieci stacjonarnych. Nie ma znaczenia mobilność abonentów radiowych, gdyż usługa ta jest realizowana zarówno na postoju, jak i w ruchu.

PRZEPŁYW POCZTY – ZARZĄDZANIE RUCHEM

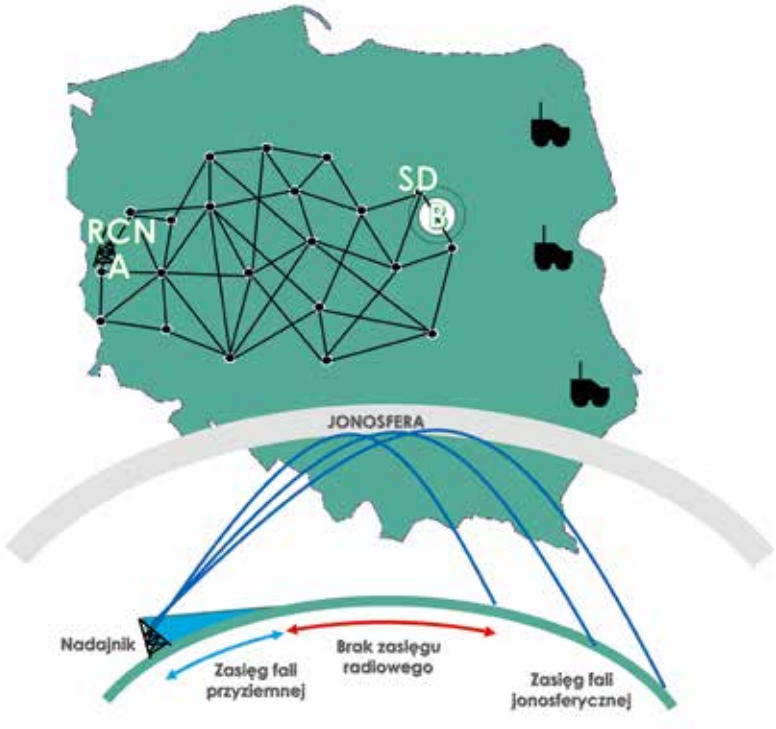
Wdrożony w 12 Dywizji Zmechanizowanej system łączności KF oferuje każdej osobie funkcyjnej posiadającej stację roboczą w lokalnej sieci komputerowej możliwość wysyłania wiadomości pocztowych przez dowolną sieć radiową. Ten przywilej może podlegać reglamentacji, stosownie do potrzeb, na zasadach ustalonych na kontrolerze domeny i serwerze poczty. Nie jest wymagane bezpośrednie połączenie z dedykowaną radiostacją ani też jej lokalne umiejscowienie na stanowisku dowodzenia.

Mówiąc dygresyjnie, jest to ciekawe zjawisko, które umożliwia budowę centrów nadawczych w lokalizacji A i przypisanie ich potencjału dla dowolnej organizacji w lokalizacji B. Innymi słowy, jeśli organizacja nie jest zbyt mobilna (nie potrzebuje łączności radiowej KF w ruchu) i ma stałe połączenie z siecią WAN, może wykorzystywać dowolne środki radiowe KF w systemie IP, by komunikować się z elementami mobilnymi (rys. 3).

Dużym ułatwieniem dla obsad operacyjnych stanowisk dowodzenia jest to, że nadawca nie musi posiadać wiedzy na temat topologii sieci przewodowej i sieci radiowych. Wystarczy jedynie, aby znał adres skrzynki pocztowej, podobnie jak to się dzieje w Internecie.

Przesyłkę dostarcza się na podstawie informacji zawartych w serwerze pocztowym. Ten może być rozmieszczony lokalnie w tej samej sieci LAN stanowiska dowodzenia lub umiejscowiony gdziekol-

RYS. 3. POTENCJAŁ RADIOWY RADIOWEGO CENTRUM NADAWCZEGO (RCN) PRZYPISANY DO STANOWISKA DOWODZENIA (SD), KTÓRE UTRZYMUJE ŁĄCZNOŚĆ RADIOWĄ KF Z ELEMENTAMI MOBILNYMI



Opracowanie własne.

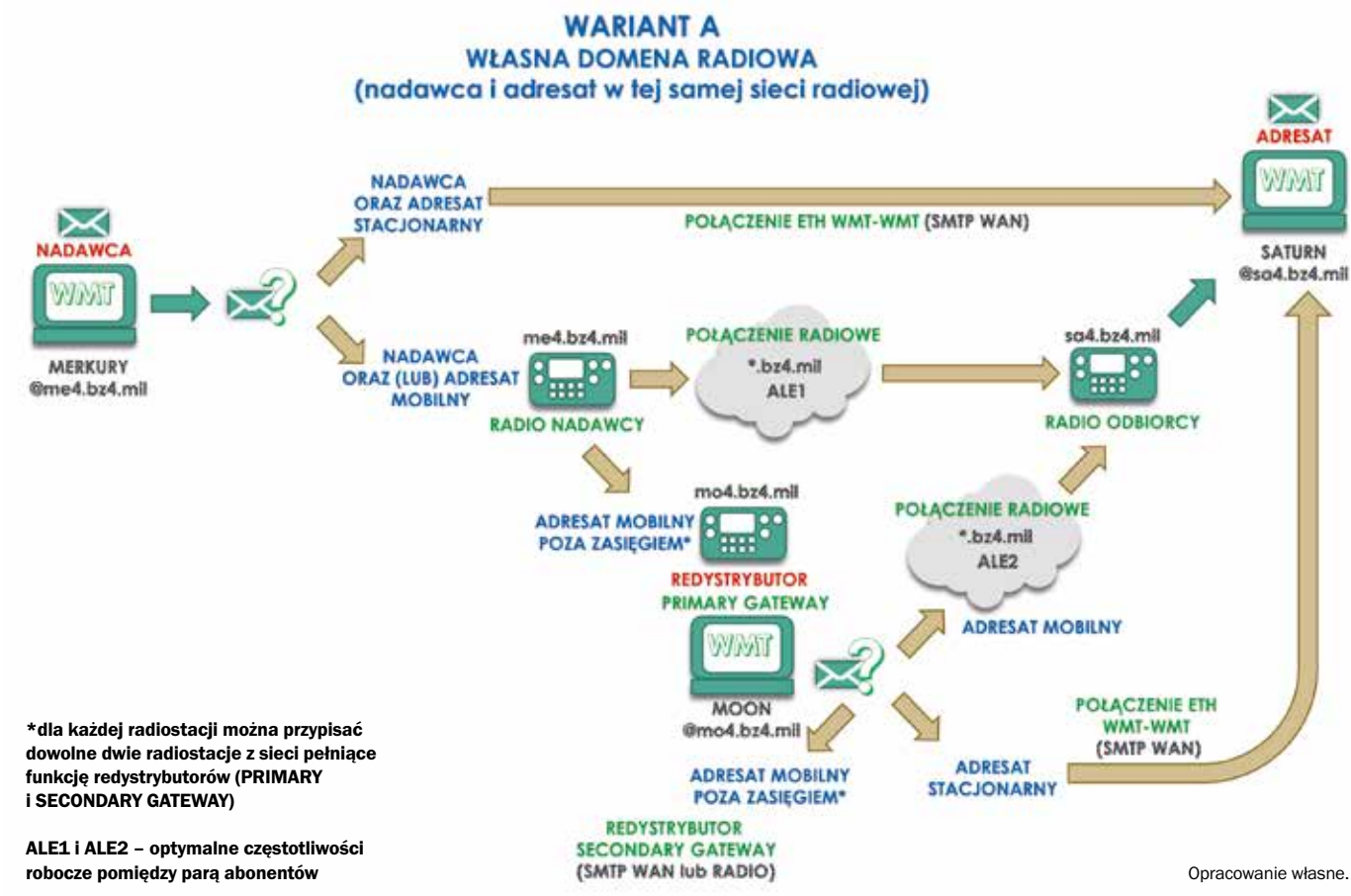
ROZWIĄZANIE NIWELUJE STREFĘ MARTWĄ ZASIĘGU RADIOWEGO MIĘDZY FALĄ PRZYZIEMNĄ A JONOSFERYCZNĄ Z ZASTOSOWANIEM ANTEN KIERUNKOWYCH (NP. DIPOL).

wiek w systemie teletransmisyjnym. Serwer ten zna połączenia z domenami radiowymi i może się posiłkować informacjami z serwera DNS, który rozwiąże adresy skrzynek (domen) i wskaże konkretny adres IP serwera adresata. Wiadomość dotrze do odbiorcy bezpośrednio w systemie przewodowym między serwerami poczty obsługującymi nadawcę i adresata lub pośrednio – w razie jego mobilności. To inne radiostacje w sieci radiowej adresata pomogą dostarczyć wiadomość. Jednak co do zasady optymalizacji przepływu poczty w momencie pośredniczenia powinny posiadać aktywny styk z systemem przewodowym, a ich rola musi zostać uwypuklona na serwerze pocztowym.

Dostarczanie informacji we własnej sieci radiowej odbywa się dwutorowo (rys. 4). Najpierw system radiowy sonduje połączenie przewodowe i dopiero gdy nie znajdzie w systemie przewodowym serwera docelowego, przesyła wiadomość drogą radiową. Dostarczenie wiadomości drogą radiową spełnia wszystkie warunki mobilności zarówno nadawcy, jak i odbiorcy. W wypadku braku dostępności adresata, z różnych powodów, radiostacja próbuje wysłać wiadomość założoną ilość razy. Przy każdej próbie podjęcia wysłania wiadomości radiostacja nadawcy sprawdza, czy nie zmienił się status mobilności odbiorcy. Dalszy brak odpowiedzi odbiorcy w wypadku braku zasięgu radiowego lub zajętości sprawi, że nadawca będzie zmuszony przekazać wiadomość do redystrybutora. Każdy abonent sieci ma indywidualnie sprecyzowane dwie inne radiostacje z sieci, które mogą odgrywać taką rolę. W 12 DZ przyjęliśmy, że jest to parametr definiowany przez operatorów, a nie narzucany w planie radiowym. Tylko operatorzy (lub osoby kierujące lokalnym systemem radiowym) znają aktualne, wynikające z sytuacji taktycznej położenie najbliższych radiostacji mających styk z siecią przewodową. Jeżeli z jakichkolwiek powodów pierwszy redystrybutor (Primary Gateway) nie jest osiągalny, to być może jest szansa, że zadanie wykona drugi redystrybutor (Secondary Gateway). Proces ten jest realizowany na każdej radiostacji, jeśli ma ona zdefiniowane redystrybutory. Jest to akcja wieloetapowa i zapętlona, dlatego procedury użycia redystrybutorów muszą być opracowane bardzo szczegółowo i świadomie wykorzystywane przez operatorów. Ważne jest, aby redystrybutor zawsze był podłączony do sieci LAN. Wówczas wiadomość zostanie dostarczona drogą przewodową, co oszczędzi czas i zmniejszy ryzyko emisji ujawniającej na *drugi skok* wiadomości w kierunku radiowym.

Do domen obcych wiadomości wysyła się na podstawie informacji o środowisku zewnętrznym lub informacji o innych radiostacjach w sieci mających dostęp do sieci WAN. Jednym z najprostszych sposobów dodania informacji o środowisku poza siecią radiową jest zdefiniowanie informacji w WMT o dostępie do zewnętrznego serwera pocztowego. Serwerem zewnętrznym może być inne WMT lub

RYS. 4. PRZEPŁYW WIADOMOŚCI POCZTOWYCH WE WŁASNEJ DOMENIE (SIECI) RADIOWEJ



***dla każdej radiostacji można przypisać dowolne dwie radiostacje z sieci pełniące funkcję redystrybutorów (PRIMARY i SECONDARY GATEWAY)**

ALE1 i ALE2 – optymalne częstotliwości robocze pomiędzy parą abonentów

Opracowanie własne.

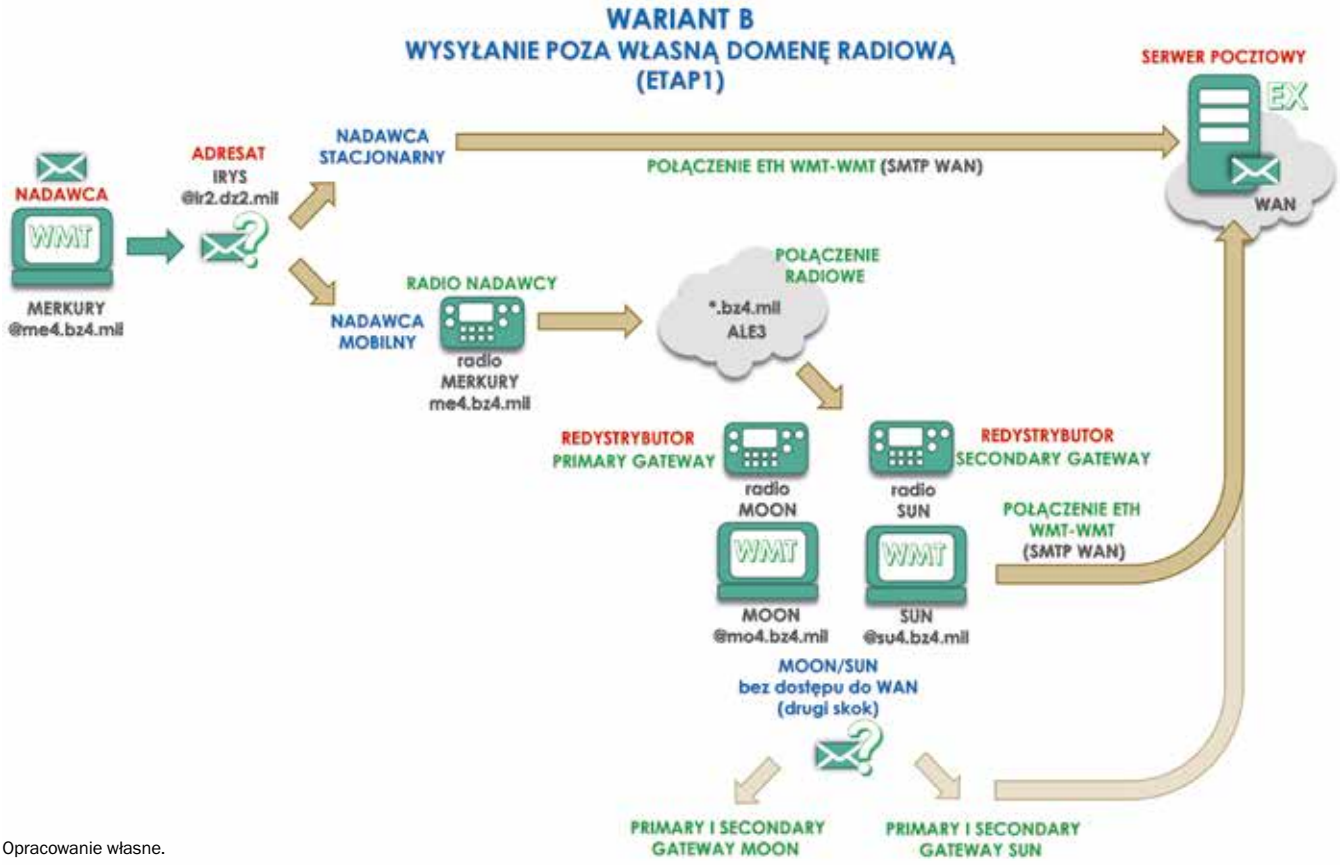
serwer obsługujący system poczty dla użytkowników sieci LAN.

Stacja nadawcy poszukuje zewnętrznego serwera pocztowego i może go zlokalizować w sposób przewodowy, gdy nadawca jest stacjonarny, lub przez wyznaczone radiostacje funkcjonujące jako redystrybutory, kiedy nadawca jest mobilny. Proces można podzielić na dwa etapy. Pierwszy to mechanizm odnajdywania połączenia do serwera zewnętrznego (rys. 5). Drugi to mechanizm przekazywania wiadomości do konkretnych sieci radiowych, oparty na informacjach w konfiguracji serwera pocztowego, wspomaganego informacjami zawartymi w serwerze DNS (rys. 6).

Jeśli przesyłka pocztowa z serwera radiowego WMT dotarła do zewnętrznego serwera poczty (EX), to znaczy, że osiągnęliśmy połowiczny sukces. Standardowa konfiguracja zewnętrznego serwera pocztowego (EX) pozwala na dostarczenie poczty do użytkowników lokalnych sieci komputerowych stanowisk dowodzenia. Użytkownik sieci komputerowej stanowiska dowodzenia, wysyłając do niego wiadomość, nie musi nic wiedzieć o statusie użytkownika radiowego. To specjalna konfiguracja serwera pocztowego umożliwi odszukanie abonentów sieci radiowych. Może być to realizowane z wykorzystaniem mechanizmu DNS na podstawie ujętej tam bazie rekordów MX serwerów pocztowych. Wówczas serwer EX odpytuje serwer DNS o adres IP serwera pocztowego WMT obsługującego domenę IRYS ir2.dz2.mil. Serwer DNS podaje adres IP. Serwer pocztowy wysyła wiadomość bezpośrednio do adresata.

Innym mechanizmem jest wysyłanie wiadomości do pocztowych serwerów pośredniczących (SMART

RYS. 5. PRZEPŁYW WIADOMOŚCI POCZTOWYCH DO INNEJ SIECI (DOMENY) LAN LUB INNEJ DOMENY (SIECI) RADIOWEJ. ETAP PIERWSZY – MECHANIZM ODNAJDYWANIA ZEWNĘTRZNEGO SERWERA POCZTY



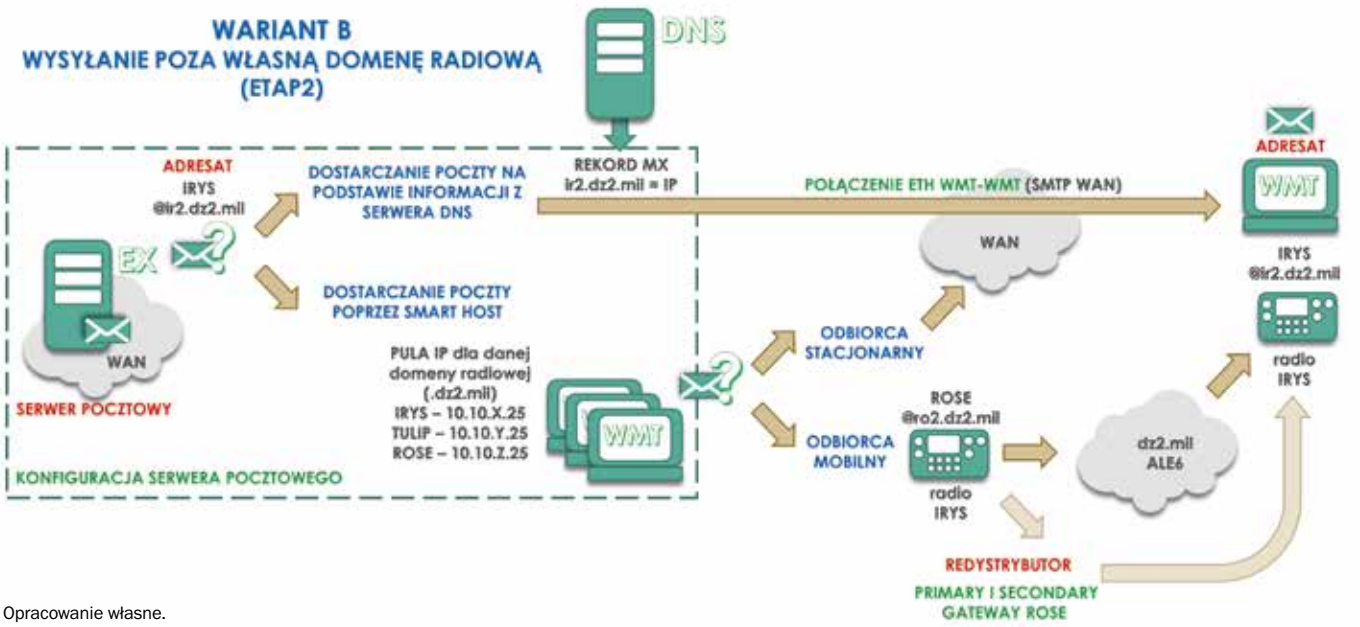
Opracowanie własne.

HOST). W tym wypadku konfiguracja serwera pocztowego mówi, że wszystkie wiadomości dla danej domeny wyższego szczebla (dz2.mil) należy wysyłać pod konkretny adres IP, a wskazany serwer już sobie z tym poradzi. Można definiować pulę serwerów SMART HOST dla konkretnych domen. Przekazanie poczty do serwera pośredniczącego SMART HOST zdejmuje odpowiedzialność za dostarczenie poczty z serwera poczty (EX). Stacja WMT, działająca jako SMART HOST, ma wszelkie informacje na temat konfiguracji całej sieci radiowej, a w szczególności sieci bezprzewodowej i połączeń poszczególnych abonentów do sieci LAN. Jej działanie jest identyczne jak dystrybucja poczty w wariancie A (rys. 4) w ramach tej samej domeny radiowej.

Jeżeli poczta nie może być dostarczona do adresata, to nadawca otrzyma zwrotnie monit informujący o braku możliwości jej dostarczenia.

Wieloszczeblowy przepływ poczty uwypuklił też inną, ważną kwestię dotyczącą budowy systemu radiowego KF. Obecnie wszyscy czujemy, że jeśli jest zdefiniowany poziom dowodzenia, to musi być stworzona odpowiadająca mu sieć radiowa – przynajmniej dowodzenia. Nic bardziej mylnego. Dowódca drużyny nie musi być w sieci z dowódcą plutonu, do-

RYS. 6. PRZEPŁYW WIADOMOŚCI POCZTOWYCH DO INNEJ SIECI (DOMENY) LAN LUB INNEJ SIECI (DOMENY) RADIOWEJ. ETAP DRUGI – MECHANIZM ODNAJDYWANIA ABONENTA RADIOWEGO



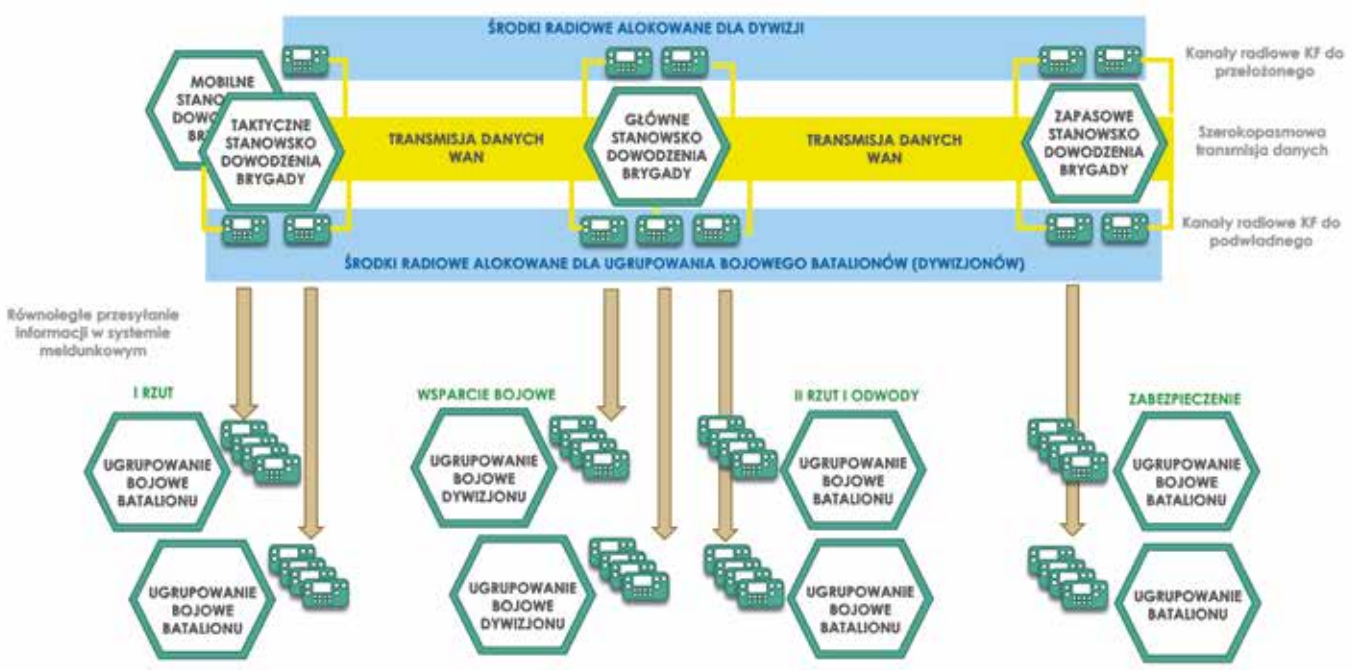
Opracowanie własne.

wódca plutonu z dowódcą kompanii, a ten z dowódcą batalionu i tak dalej. Kluczowe jest odpowiednie wykorzystanie posiadanych na stanowisku dowodzenia środków radiowych oraz stworzenie kanałów radiowych chroniących przepływ informacji. To kryterium zagwarantowania optymalnego przepływu informacji będzie dyktowało architekturę sieci i jej skład. Rozważania budowy systemu radiowego KF *od góry* wykazały inną architekturę systemu radiowego, niż budując system KF *od dołu*. Zdefiniowany wariant budowy zintegrowanego systemu radiowego KF ZT posłuży nam do dalszych rozważań. Nie oznacza to wcale, że budowa systemu od szczebla dywizji w dół jest wariantem preferowanym. Najbardziej optymalne wykorzystanie radia będzie wówczas, gdy na stanowisku dowodzenia dysponujemy dostępem do szerokopasmowego medium łączności (przewodowego, radioliniowego, satelitarnego). Nie jest właściwe, aby *marnować* środki radiowe na poszczególne *skoki radiowe* w hierarchii dowodzenia. Nadrzędnym celem jest dostarczyć radiostację ze stykiem do systemu przewodowego do najniższych szczebli dowodzenia, w ich sieci radiowej KF. Obecnie takie idealne możliwości mają stanowiska dowodzenia brygady (pułku). Aby zrealizować ten wymóg, może się okazać, że sieci radiowe szczebla brygada – batalion staną się zbędne. Z całą pewnością budowa systemu łączności KF brygady (pułku) będzie unikatowa i uzależniona od nasycenia pododdziałów środkami KF.

Aby tę odmienność uwidocznić, należy odpowiedzieć na kilka pytań. Pierwsze z nich dotyczy dostępności środków KF na szczeblach poniżej batalionu włącznie. Według obecnych standardów, uogólniając, jeśli brygada zorganizuje trzy sieci radiowe KF, wówczas wymagana jest alokacja trzech środków na poziomie każdego elementu podległego brygadzie. Drugie pytanie to: jak dostarczyć radiostację włączoną w system przewodowy do najniższych szczebli dowodzenia lub czy jest dopuszczalne, by więcej niż jeden skok radiowy był wymagany do dostarczenia wiadomości do systemu LAN/WAN.

RYS. 7. WARIANT ORGANIZACJI ŁĄCZNOŚCI KF BRYGADY

ALOKACJA ŚRODKÓW RADIOWYCH NA STANOWISKACH DOWODZENIA BRYGADY, DOSTARCZENIE RADIOSTACJI WŁĄCZONEJ DO IP WAN DO ELEMENTÓW UGRUPOWANIA BOJOWEGO BRYGADY (SIECI RADIOWYCH BATALIONÓW/DYWIZJONÓW), RÓWNOLEGŁE PRZESYŁANIE INFORMACJI (ROZKAZÓW, MELDUNKÓW), WYMIANA INFORMACJI MIĘDZY WSZYSTKIMI ELEMENTAMI UGRUPOWANIA BOJOWEGO – KOMPANIA JAKO ODWÓD BRYGADY (DYWIZJI) MOŻE FUNKCJONOWAĆ BEZ REKONFIGURACJI SYSTEMU RADIOWEGO KF



Opracowanie własne.

Należy podkreślić, że skoki radiowe znacznie wydłużają czas dostarczenia wiadomości i stwarzają możliwość wykrycia. Wydaje się, że najbardziej optymalne rozwiązanie to uwzględnienie stanowisk dowodzenia brygady (tylko trzy–cztery pozycje w sieci) w planach radiowych podległych batalionów (dywizjonów). Właściwe jest grupowanie w sieciach radiowych elementów (pododdziałów) kolejnych rzutów, wsparcia bojowego oraz zabezpieczenia, mając na uwadze tylko przepustowość kanału radiowego. Warto też regulować wykorzystanie radiostacji na stanowiskach dowodzenia brygady i dopisywać elementy pierwszego rzutu do stanowiska dowodzącego, a odwody do stanowiska rozwiniętego w rejonie tylnym (rys. 7).

Aby spojrzeć odmiennie na tę hierarchię budowy systemu radiowego KF, należy badać przypadki szczególne. Takim znaczeniem charakteryzuje się np. system meldunkowy i obieg informacji. Jeżeli uzmysłowimy sobie, że wszystkie elementy ugrupowania bojowego brygady nie mają dostępu do systemu przewodowego, dlatego też przesyłają informacje (meldunki) drogą radiową. Analizując ten aspekt, możemy zidentyfikować pewne niedogodności. Zwykle system meldunkowy wymaga przesłania meldunków w tym samym czasie od całości ugrupowania bojowego. Spowoduje to zapchanie tradycyjnej sieci radiowej dowodzenia KF informacjami generowanymi przez wszystkich abonentów i *znokautowanie* radiostacji odbiorcy (brygadowej).

Z drugiej strony wydanie rozkazu brygadowego powoduje dystrybucję objętościowo dużych plików i problem przesyłania tego samego dokumentu bojowego kolejno do każdego z podległych elementów. Umiejscowienie radiostacji brygadowych (pułkowych) w sieciach batalionów (dywizjonów) pozwoli zredukować tę niedogodność i dostarczać oraz otrzymywać dokumenty równolegle, a nie szeregowo.

ZARZĄDZANIE SYSTEMEM

Podsumowując, należy również podkreślić czynności, które są zwykle pomijane przy budowie systemu łączności radiowej. Dystrybucja cyfrowych planów radiowych oraz ich sposób uaktualnienia są równie ważne jak zaprezentowane działania. Krytyczne jest zmienianie parametrów technicznych radiostacji w sieci oraz dystrybucja i uaktualnienie kluczy ochrony kryptograficznej dla wszystkich abonentów w tym samym czasie, mimo dużych odległości między lokalizacjami. Nadrzędną zasadą podczas wprowadzania zmian w sieciach radiowych jest transparentność dla systemu IP. Niezależna od topologii sieci zmiana planów częstotliwości radiowych, kluczy czy niektórych parametrów technicznych ustawień radiostacji jest możliwa. Mechanizm importu selektywnych ustawień z pliku konfiguracyjnego zapewnia duży poziom bezpieczeństwa i wyklucza możliwość popełnienia błędu przez operatora, gwarantując jednocześnie spójność systemu teletransmisyjnego.

Przewartościowania wymaga system meldunkowy dotyczący łączności radiowej KF. Obecnie środek ciężkości raportowania polega na subiektywnej ocenie gotowości systemu radiowego. Natomiast w proponowanym systemie kluczową sprawą jest dzielenie się informacjami o konfiguracji sieci radiowych i ich poszczególnych abonentów. Najważniejsze dla administratorów serwerów są dane uwzględniające konfigurację sieci radiowej na styku z częścią informatyczną systemu przewodowego. Dotychczasowa autonomiczność systemu radiowego sprawiła, że nie ma nawyku współpracy osób funkcyjnych z obszaru informatyki i łączności radiowej. Brak dialogu na temat sposobu planowania i zarządzania, a w tym tak ważnych czynności jak uaktualniania rekordów serwera DNS lub konfiguracji serwera pocztowego, ma duży wpływ na funkcjonowanie zintegrowanego systemu. Istotnym trendem będzie edukacja personelu informatycznego do planowania łączności radiowej, a typowi radiowcy *wyginą*, ewoluując w stronę informatyczną. Dzieje się to już teraz. Przykładem jest każdy z nas, który ma w domu router internetowy emitujący sygnał sieci bezprzewodowej. Z pewną dozą przekory można stwierdzić, że domowy router jest radiostacją, a wojskowa radiostacja jest routerem. Każdy potrafi skonfigurować domowy router bardziej profesjonalnie lub całkiem amatorsko. Obaj, profesjonalista czy amator, niewiele wiedzą (lub nic) o częstotliwości radiowej. Nie jest to informacja niezbędna, by sygnał bezprzewodowy uwolnił nas od kabli i dał swobodę ruchu. Ważnymi kwestiami dla zarządzającego i użytkownika routera są przede wszystkim ustawienia sieciowe: kryptonim (nazwa) sieci bezprzewodowej, bezpieczeństwo sieci (hasło) oraz adres IP (własny i strony zarządzania ruterem). Ta analogia pokazuje, że typowe wojskowe podejście do kwestii planowania i zarządzania z podziałem na obszary informatyczne i radiowe nie ma sensu.

Brak narzędzi do realizacji procedur organizacji systemu radiowego powoduje, że katalog czynności do wykonania przy budowie i zarządzaniu systemem może być realizowany tylko przez osoby o ponadprzeciętnej wiedzy fachowej. Osób o tak wszechstronnej, syntetycznej wiedzy i umiejętnościach w pododdziałach bojowych praktycznie się nie spotyka. Jest to kolejny argument, by system radiowy planowany był równolegle z sieciami przewodowymi w jednodomenowym środowisku. Ponadto w samym zarządzaniu zintegrowaną domeną pojawia się wiele obszarów administracyjnych, których istnienie nie jest zauważane z powodu braku powszechnego użycia zintegrowanej łączności radiowej. Nie ma podziału odpowiedzialności w kwestii korygowania błędów i niespójności w obszarach takich, jak: domeny radiowe, adresy IP oraz trasy routingu. Na pierwszy plan wysuwa się obszar zarządzania ruchem sieciowym. Nieprawidłowo skonfigurowane reguły odnajdywania serwerów WMT w systemie IP lub zasady dostarczania wiadomości pocztowych mogą zdestabilizować cały system.

Konkludując przedstawione rozwiązania, tak zaprojektowany system łączności radiowej KF, według opisanych zasad, uwarunkowań i doświadczeń, gwarantuje dużą elastyczność i ochronę najbardziej skomplikowanych zadań bojowych. Zadań, których wykonanie wymaga od łączności radiowej KF wykorzystania nowatorskich, ale niezbędnych usług. Dzięki takiemu podejściu w 12 DZ w sieciach KF jesteśmy stanie zapewnić monitorowanie położenia i ruchu wojsk. Mamy możliwość wymiany dokumentów bojowych. Zupełnie automatycznie następuje wymiana świadomości operacyjnej w aplikacji wsparcia dowodzenia i jej dystrybucja od najniższych szczebli dowodzenia i do nich.

Wyprzedzając nasuwające się pytania, to twierdząco należy odpowiedzieć na te dotyczące możliwości uzyskania podobnych rezultatów dla łączności ultrakrótkofalowej (UKF). Sposób integracji systemów KF i UKF z zastosowaniem radiostacji tego samego producenta jest banalnie prosty. Radiostacje UKF oferują odmienny od łączności KF wachlarz możliwości. Owa odmienność łączności UKF jest dopełnieniem łączności KF, a wymiana informacji między użytkownikami domeny informacyjnej nabiera kompletnego wymiaru. Ale to już temat do kolejnych rozważań. ■

Podstawowe usługi **funkcjonalne NATO FAS**

IMPLEMENTACJA NOWYCH TECHNOLOGII, SYSTEMÓW I USŁUG TELEINFORMATYCZNYCH SPOWODOWAŁA ZNACZĄCY WZROST ILOŚCI PRZETWARZANYCH I PRZEKAZYWANYCH INFORMACJI.

mjr dr inż. Andrzej Bogdański

Autor jest szefem Sekcji Administrowania Systemami Teleinformatycznymi w Akademii Sztuki Wojennej.

Ostatnie lata obfitowały w wiele ćwiczeń, podczas których polscy żołnierze mieli możliwość korzystania z usług dziedzinowych *NATO – Functional Area Services*. Użytkowanie tych usług pozwoliło zaobserwować ogromny postęp w dziedzinie nowych technologii teleinformatycznych wykorzystywanych do wspomagania dowodzenia. Potencjał technologiczny, którym dysponuje nasza armia w zakresie infrastruktury teleinformatycznej, wciąż się zwiększa i nie ustępuje przy tym obecnym standardom światowym. Nowoczesne sieci to jednak nie wszystko.

DETERMINANTY ZMIAN

Do sprawnego i skutecznego funkcjonowania infrastruktury teleinformatycznej niezbędne jest również nowoczesne i dostosowane do współczesnych wymagań środowiska funkcjonowania sił zbrojnych oprogramowanie, którego użycie jest istotą systemów wspomagania dowodzenia. Niestety, jak można łatwo zauważyć, świadomość w kwestii wykorzystywanych w Siłach Zbrojnych RP usług teleinformatycznych jest niewystarczająca, co wpływa negatywnie na poziom bezpieczeństwa ich eksploatacji. W dobie społeczeństwa informacyjnego i znaczących przewartościowań w obszarze zagrożeń bezpieczeństwo informacyjne jest jednym z najważniejszych składowych bezpieczeństwa państwa.

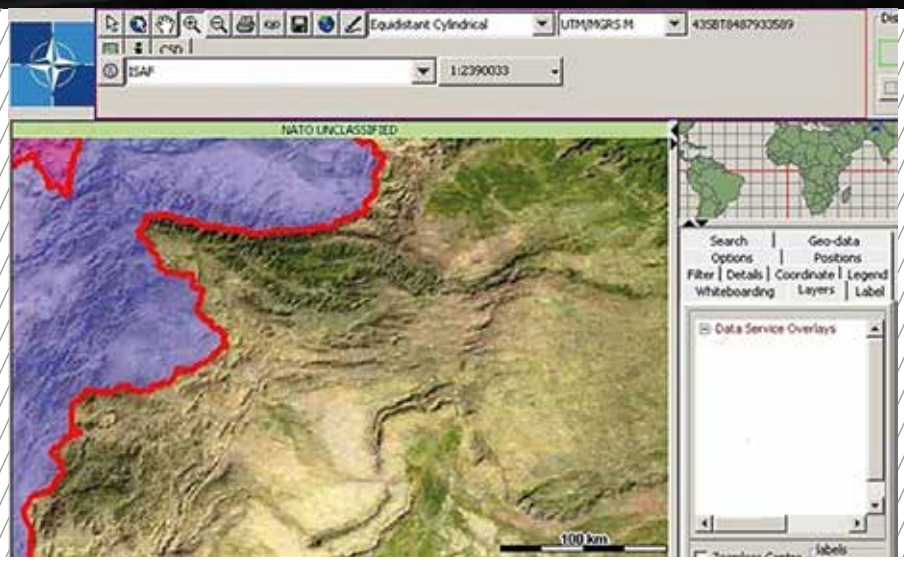
Sieci teleinformatyczne to nic innego jak autostrady, po których podróżują pakiety danych, a nie narzędzie samo w sobie. Usługi funkcjonalne to nie zabawki dla informatyków, lecz narzędzia, które powinny wspierać, usprawniać i przyspieszać proces dowodzenia. To właśnie czas wypracowania decyzji ma wymierny wpływ na skuteczność działań. W warunkach dynamicznych zmian sytuacji na polu walki zdobycie przewagi jest zdeterminowane szybkością pozyskania aktualnych i pewnych informacji oraz wypracowaniem decyzji w krótszym czasie.

WYBRANE USŁUGI

Jedną z podstawowych usług funkcjonalnych jest *Interim Geo-Spatial Intelligence Tool* (IGeoSIT) – fot. Jest to system zobrazowania sytuacji operacyjnej bazujący na wspólnych podkładach map cyfrowych na wszystkich poziomach dowodzenia. Z usługi tej korzystały również eksploatowany dawniej system rozpoznawczy NATO Intelligence Toolbox (NITB) oraz Integrated Command and Control Software for Air Operations (ICC). Kolejną usługą był *Joint Operations Centre Watch* (JOC Watch), która zbierała, przechowywała i przetwarzała informacje o incydentach. W przystępnej formie udostępniała je – dzięki hiperłączom żołnierze mogli obejrzeć zdjęcia i filmy z miejsca zdarzenia oraz pozyskać dodatkowe informacje znajdujące się w innych usługach.

W początkowym etapie eksploatacji usług funkcjonalnych przez naszych żołnierzy przydatnym narzędziem wspomagającym rozpoznanie był *NATO Intelligence Toolbox* (NITB). Usługa ta pozwalała publikować i wyszukiwać dane rozpoznawcze i wywiadowcze. W jej skład wchodził interfejs zarządzania danymi służący do wprowadzania informacji w formie opisów, zdjęć, map i filmów. Integralną, współpracującą usługą był Toolbox – rodzaj wyszu-

JAROSŁAW WIŚNIEWSKI



ARCHIWUM AUTORA

Widok interfejsu użytkownika usługi Interim Geo-Spatial Intelligence Tool

kiwarki funkcjonalnie podobnej do powszechnie używanego Google.

UWZGLĘDNIĆ SPECYFIKĘ

Na podstawie charakterystyki wybranych możliwości i przeznaczenia kluczowych usług funkcjonalnych NATO – Functional Area Services można pokusić się o następujące wnioski:

– mnogość usług informatycznych NATO FAS wymaga gruntownego przeszkolenia żołnierzy zarówno je eksploatujących, jak i zajmujących się ich administrowaniem;

– wymagane kompetencje i obowiązki personelu wsparcia teleinformatycznego powinny wynikać z zakresu usług;

– szkolenie specjalistów wsparcia teleinformatycznego powinno być realizowane systemowo w odniesieniu do konkretnej grupy usług NATO FAS;

– żołnierze wsparcia teleinformatycznego powinni stanowić wyselekcjonowaną grupę specjalistów o odpowiedniej wiedzy i umiejętnościach praktycznych związanych z obszarem ich odpowiedzialności;

– istotnym czynnikiem jest system doboru kandydatów z dużym doświadczeniem zawodowym, jednocześnie zdeterminowanych do zdobywania nowej wiedzy i umiejętności.

Reorganizacja wsparcia teleinformatycznego w celu zwiększenia efektywności realizacji zadań to proces złożony, który powinien być szczegółowo zaplanowany, a jego najważniejsze elementy to:

– dobór, wyszkolenie, a także odpowiednia liczba specjalistów na danym szczeblu umożliwiająca nieprzerwane wsparcie teleinformatyczne w systemie zmianowym w trybie ciągłym: 24 godziny 7 dni w tygodniu;

– wsparcie użytkownika w zakresie usług funkcjonalnych powinno być realizowane przez wydzielone komórki Help Desk, tak by specjaliści wsparcia teleinformatycznego mogli skupić się na wspomaganiu administratorów usług;

– konieczne jest zwiększenie potencjału wyspecjalizowanej instytucji o charakterze eksperckim świadczącej wsparcie trzeciego poziomu administratorom usług NATO – Functional Area Services. ■

Wykorzystanie taktycznych systemów transmisji **danych Link w NATO**

POLE WALKI JEST OBECNIE BARDZO ZŁOŻONE I DYNAMICZNE, PRZEZ CO WYMAGA PODEJMOWANIA SZYBKICH I PRZEJRZYSTYCH DECYZJI NA WSZYSTKICH POZIOMACH DOWODZENIA.

ppłk Dariusz Łuczak

Autor jest szefem Wydziału Taktycznych Systemów Transmisji Danych – zastępcą szefa Oddziału w Zarządzie Wsparcia Dowodzenia i Łączności IRW Dowództwa Generalnego RSZ.

Każda informacja zapewniająca świadomość sytuacyjną, odnoszącą się do położenia wojsk, sprawności technicznej środków walki, poziomu logistycznego zaopatrzenia, zdolności do działań poszczególnych zgrupowań bojowych, jak również do możliwości dowodzenia nimi, musi być dostępna dla dowódców i oficerów sztabu. Aby spełnić wskazane wymagania, wszystkie informacje i dane muszą być przekazywane we właściwym czasie między stanowiskami dowodzenia i platformami bojowymi biorącymi udział w walce.

Jedyne systemy, które odpowiadają wymaganiom związanym z dostarczaniem danych w czasie rzeczywistym lub zbliżonym do rzeczywistego, to wykorzystywane w NATO taktyczne systemy transmisji danych Link (Tactical Data Link – TDL).

POCZĄTKI

Rozwiązania odnoszące się do TDL były już rozwijane kolejno w latach sześćdziesiątych, siedemdziesiątych oraz osiemdziesiątych ubiegłego wieku jako oddzielne, odseparowane od siebie, zapewniające właściwy zasób danych dla realizowanych działań czy też zgrupowań bojowych je wykorzystujących. Ówczesne możliwości techniczne tych systemów sprawiały, że każdy z nich wymieniał dane, wykorzystując unikatowy format wiadomości oraz różnorodne media transmisyjne, pracujące na różnych zakresach częstotliwości fal radiowych. Po przeprowadzeniu wielu analiz stwierdzono, że implementacja odmiennych formatów wiadomości w systemach kierowania i dowodzenia (Command and Control Systems) powoduje opóźnienia w przetwarzaniu danych, co z kolei drastycznie wpływa na efektywność prowadzonych działań.

Wskazano jednoznacznie, że wymiana informacji z wykorzystaniem TDL jest kluczowym elementem odnoszącym się do kierowania i dowodzenia, zarówno na szczeblu operacyjnym, jak i strategicznym. Dokładne i aktualne dane, jakie są wymieniane między systemami TDL funkcjonującymi w NATO a systemami narodowymi, są elementem krytycznym dla uzyskania połączonego obrazu sytuacji operacyjnej, a co za tym idzie – osiągnięcia zwiększonej świadomości sytuacyjnej.

Na poziomie Sojuszu zdecydowano, że zamiast wprowadzać kolejne rozwiązania i zmiany, które mogłyby stać w konflikcie z narodowymi programami rozwoju systemów transmisji danych, ustanowiono ogólną strategię ich migracji, wskazując wszystkim sojusznikom wspólną architekturę taktycznych systemów transmisji danych, zapewniającą pełną

TABELA. PARAMETRY POSZCZEGÓLNYCH STANDARDÓW TDL

LINK	Link-1	ATDL-1	Link-11	Link- 11B	Link-16	Link-22	VMF
Transfer danych b/s	600–2400	50 duplex, 600–2400 simplex	1365/2250	600–2400	25 000–23 8000	do 3600 HF do 16 000 UHF	zmienny
Zasięg radiowy	nie dotyczy	nie dotyczy	HF 500 nm UHF 300 nm GAG GG 30 nm		UHF LOS* 300 nm UHF BLOS** 500 nm	HF do 1000 nm UHF do 300 nm (GAG***) 30 nm (GG****) zwiększany przez relay	LOS 30 nm GAG 300 nm SATCOM
Format wiadomości	wiadomości serii S	wiadomości serii B	wiadomości serii M	wiadomości serii S	wiadomości serii J	wiadomości serii F/FJ	wiadomości serii K
Odporność na zakłócenia	nie	nie	nie	nie	tak	tak dla UHF z EPM***** nie dla UHF i HF przy FF******	tak
Transmisja głosu	nie	nie	nie	nie	tak (2 kanały 2,4 lub 16 kb/s)	nie	tak
Szyfrowanie	nie	tak – tylko MSEC*******	tak – tylko MSEC	tak – tylko MSEC	tak – MSEC i TSEC********	tak – MSEC i TSEC (FF tylko MSEC)	możliwe, w zależności od użytych mediów transmisyjnych
Korekta błędów	nie	nie	tak	tak	tak	tak	tak

*Line of Sight, ** Beyond Line of Sight, *** Ground-Air-Ground, **** Ground-Ground, ***** Electronic Protective Measures, ****** Fixed Frequency, ******* Message Security, ******** Transmission Security.

Opracowanie własne.

interoperacyjność podczas realizacji wspólnych działań. Główne systemy transmisji danych taktycznych, wykorzystywane obecnie w NATO i w krajach należących do Sojuszu, to (tab.):

- Link-1 – standard wymiany danych typu punkt–punkt, zdefiniowany w dokumencie standaryzacyjnym *Allied Tactical Data Publication NATO* (ATDLP-5.01). Używany na stacjonarnych stanowiskach dowodzenia obrony powietrznej i umożliwiający wymianę danych o sytuacji powietrznej;
- Link-11 – standard wymiany danych dystrybuowanych w sieciach radiowych (w paśmie HF i UHF), zdefiniowany w dokumencie standaryzacyjnym NATO – ATDLP-5.11. Umożliwia wymianę danych o obiektach morskich i powietrznych oraz kierowanie i dowodzenie;
- Link-11B – standard wymiany danych typu punkt–punkt, zdefiniowany w dokumencie standaryzacyjnym NATO – ATDLP-5.11. Używany głównie w obszarze obrony powietrznej i umożliwiający wymianę danych między zestawami obrony przeciwlotniczej, systemami rozpoznania sytuacji powietrznej, kierowania i dowodzenia oraz jednostkami wymieniającymi informację w ramach sieci radiowych;
- Army Tactical Data Link (ATDL 1) – standard wymiany danych typu punkt–punkt, zdefiniowany w dokumencie standaryzacyjnym USA – MIL-STD-6013. Używany przede wszystkim w obszarze obrony powietrznej i umożliwiający połączenie między systemami obrony powietrznej w zakresie wymiany danych o obiektach powietrznych oraz dokumentów rozkazodawczych;

PIOTR ŁYSAKOWSKI

• Link-16 – standard wymiany danych dystrybuowanych w sieciach radiowych (w paśmie UHF), zdefiniowany w dokumencie standaryzacyjnym NATO – ATDLP-5.16 i używany w ramach operacji połączonych. Umożliwia transmisję danych o dużej przepływności, odpornych na zakłócenia radioelektroniczne w domenie powietrznej, morskiej, podwodnej, lądowej, kosmicznej, jak również w ramach obrony przed pociskami balistycznymi;

• Link-16 – wymiana danych Link-16 protokołem Joint Range Extension Application Protocol (C JREAP-C) – typu IP przez kanał satelitarny, zdefiniowany w dokumencie standaryzacyjnym NATO – ATDLP-5.18. Używany w ramach operacji połączonych we wszystkich domenach oraz do transmisji danych poza horyzont radiowy (Beyond Line of Sight) przez inne media transmisyjne niż te, dla których Link-16 został zaprojektowany. Wykorzystywany jest tu dedykowany protokół oraz struktura wiadomości (serii X);

• Link-22 – standard wymiany danych dystrybuowanych w sieciach radiowych (w paśmie HF i UHF), zdefiniowany w dokumencie standaryzacyjnym NATO – ATDLP-5.22. Używany głównie w obszarach morskim i powietrznym, umożliwiający wymianę danych między okrętami nawodnymi, podwodnymi, samolotami oraz posterunkami brzegowymi. Został zaprojektowany, aby zastąpić Link-11 oraz uzupełnić zdolności Link-16, zapewniając wymianę danych w pasmach UHF oraz HF. Link-22 wykorzystuje dosyć znaczącą ilość wiadomości i elementów danych, jakie są używane w Link-16 (wiadomości serii J);

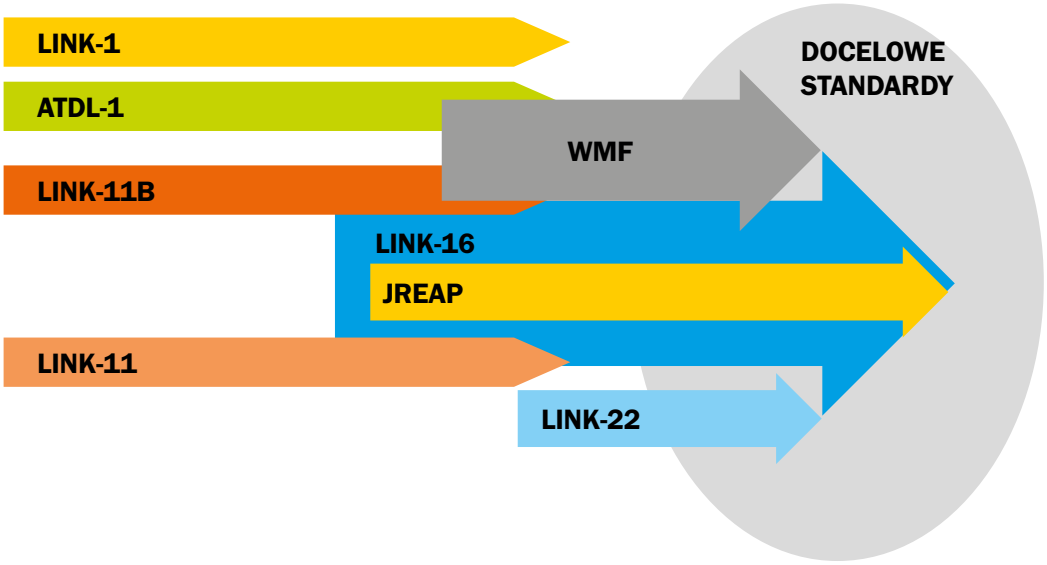
• VMF (Variable Message Standard) – standard wymiany danych zdefiniowany w dokumencie standaryzacyjnym USA – MIL-STD-6017, używany głównie w domenie lądowej, gdzie format wiadomości jest zorientowany bitowo, a wiadomość ma zmienną długość, zapewniając tym samym możliwość wymiany tych danych przez różne media transmisyjne oraz między różnymi platformami bojowymi na różnych poziomach dowodzenia.

NOWE PODEJŚCIE

Systemy NATO oraz narodowe systemy kierowania i dowodzenia stanowią podstawę dla zapewnienia świadomości sytuacyjnej, podejmowania decyzji oraz osiągania celów prowadzonej operacji połączonej. Zgodnie z założeniami NATO Network Enabling Capability (NNEC), w obszarze prowadzonych działań powinna być zapewniona niezakłócona i aktualna informacja w pełnym zakresie, z minimalnym wykorzystaniem interfejsów oraz bram międzysystemowych.

W związku z przyjętym założeniem powstał NATO Tactical Data Link Implementation Plan (NTDLP),

RYS. STRATEGIA NATO W ZAKRESIE WYKORZYSTANIA DOCELOWYCH STANDARDÓW WYMIANY DANYCH TAKTYCZNYCH LINK



Źródło: *The Strategic Commanders' Datal Link Migration Strategy*, wyd. 2016.

który został opracowany przez międzynarodową grupę zrzeszającą przedstawicieli krajów NATO (Tactical Data Link Capability Team) i przez nią jest koordynowany. Odpowiedzialność za zgodność z przyjętymi zapisami NTDLP spoczywa na każdym kraju, który ma w tej grupie swoich przedstawicieli.

Główne cele przyjętego sposobu implementacji systemów transmisji danych to:

– ustanowienie rodziny wiadomości serii J, których przesyłania nie ograniczają media transmisyjne;

– ustanowienie wspólnego formatu wiadomości;

– zredukowanie ilości bram międzysystemowych i interfejsów, zapewniających translację danych/wiadomości między systemami TDL;

– usprawnienie zautomatyzowanego zarządzania wymianą danych między TDL w celu zminimalizowania problemu duplikowania się przekazywanej informacji;

– zminimalizowanie strat informacji w wypadku konieczności przysłania danych między różnymi TDL.

Osiągnięcie standaryzacji odnoszącej się do przesyłanych danych taktycznych w obszarze operacyjnym znacząco poprawi zdolności systemów TDL do wsparcia procesu kierowania i dowodzenia. Dlatego też wszystkie kraje powinny dążyć do przyjęcia wymienionych standardów i zaadaptowania w narodowych systemach (rys.).

Dodatkowo na wskazany w zakresie systemów TDL kierunek działania kluczowy wpływ mają także czynniki, które pojawiły się po wydaniu powyższej strategii. I tak strona amerykańska zdecydowała, że Link-11 po 31 grudnia 2024 roku nie będzie już wspierany. Dlatego też niezbędne jest osiągnięcie zdolności do wymiany danych w standardzie Link-22, który ma go zastąpić.

Naczelne Dowództwo Sił Sojuszniczych w Europie (Supreme Headquarters Allied Power Europe – SHAPE) podjęło decyzję, że w odniesieniu do wymiany danych w ramach NATINAMDS będzie wycofywany obecnie wykorzystywany Link-1, który ma być docelowo zastąpiony przez JREAP-C.

* * *

Strategia NATO odnosząca się do docelowego wykorzystania standardów wymiany danych taktycznych będzie się opierać na systemach wymieniających informacje z wykorzystaniem rodziny wiadomości z serii J, tzn. Link-16, Link-22 oraz VMF. Pozwoli to do minimum zredukować liczbę formatów wiadomości, protokołów wymiany danych oraz mediów transmisyjnych, jakie są obecnie wykorzystywane na polu walki. Osiągnięcie tego celu znacząco poprawi interoperacyjność systemów kierowania i dowodzenia NATO oraz narodowych. ■

Łączność **troposferyczna**

JEST TO JEDEN Z SYSTEMÓW SPEŁNIAJĄCYCH WYMAGANIA WYMIANY INFORMACJI NA ODLEGŁOŚĆ KILKUSET KILOMETRÓW.

Autor jest szefem Sekcji Wsparcia Dowodzenia i Łączności w 10 Pułku Dowodzenia.

mjr mgr Marek Mirowski

Wojskowe systemy łączności i informatyki dynamicznie się zmieniają. Jest to związane z dążeniem do zapewnienia przepływu informacji w czasie rzeczywistym z jednoczesną integracją wielu usług, zarówno telefonicznych, jak i transmisji danych. Dokonujące się zmiany mają doprowadzić do sprostania wymaganiom pola walki, tzn. umożliwić dotarcie z informacją do odbiorcy w czasie rzeczywistym z jednoczesnym zachowaniem jej integralności i bezpieczeństwa. Zdolność do szybkiego przekazywania zadań i zbierania meldunków o sytuacji będzie stanowić zasadnicze uwarunkowanie osiągnięcia powodzenia na polu walki. Będzie to jednak możliwe tylko w wypadku dysponowania skutecznym systemem wspierającym dowodzenie, którego osnową powinny być nowoczesne systemy łączności i informatyki, w tym w szczególności niezawodne i bezpieczne systemy transmisyjne. Możliwość budowy elastycznego i niezawodnego systemu o dużych przepływnościach na duże odległości (50–250 km), niezależnie od systemu łączności satelitarnej (częściowe lub całkowite zastąpienie relacji satelitarnych), zapewniają aparatownie troposferyczne.

POCZĄTKI

Warstwę troposferyczną, jako najniższą i najcieńszą warstwę atmosfery pod względem zastosowania na potrzeby łączności, rozpoczęto wykorzystywać w pierwszej połowie XX wieku. W latach trzydziestych sukcesem zakończyły się pierwsze próby nawiązania łączności radiowej z zastosowaniem zjawiska rozpraszania się fal elektromagnetycznych w warstwie troposfery. Ówczesna technologia pozwalała na skonstruowanie radiostacji troposferycznych, ale ich urządzenia nadawczo-odbiorcze miały olbrzymie rozmiary i bardzo dużą moc, co zasadniczo utrudniało ich militarne zastosowanie.

Badania nad aparatowniami troposferycznymi nabrały jeszcze większego tempa po zakończeniu II wojny światowej, kiedy powstały dwa przeciwstawne bloki polityczno-militarne. W okresie zimnowojennym linie troposferyczne odgrywały rolę łączy zapasowych bądź były przedłużeniem łączy przewodowych i obejmowały znaczny obszar Europy. System zwany ACE High NATO skupiał stacje troposferyczne zlokalizowane od północnej Norwegii, przez zachodnią i południową Europę, aż po wschodnią Turcję. Z kolei Układ Warszawski wykorzystywał linie troposferyczne do budowy sieci łączności strategicznej BARS oddanej do użytku w 1987 roku. W skład systemu wchodziło 26 węzłów na terenie ZSRR, Polski, NRD, Czechosłowacji, Węgier i Bułgarii. Były one w pełni autonomiczne – dysponowały własnymi generatorami prądu oraz zapasami żywności i wody.

Pierwsze radiolinie troposferyczne w naszych siłach zbrojnych wprowadzono do użytku w 1985 roku w ówczesnej 15 Brygadzie Radioliniowo-Kablowej i w 6 Pomorskim Pułku Łączności. Były to aparatownie R-412 zamontowane na nadwoziach samochodów ciężarowych typu Kamaz i Ural 375. Po raz ostatni nasze siły zbrojne operacyjnie zastosowały aparatownie troposferyczne R-412 w systemie łączności i informatyki zorganizowanym na potrzeby Wielonarodowej Dywizji w Iraku w 2003 roku.

Stacje troposferyczne zapewniały polskiemu kontyngentowi wojskowemu w Iraku po cztery analogowe kanały telefoniczne PCM 64 między centralami DGT 3450 w każdym kierunku troposferycznym.

Umożliwiało to przekazywanie wiadomości, jednak nie spełniało wszystkich oczekiwań, które główny nacisk kładły na transmisję danych. Dlatego też konieczne okazało się wykorzystanie pasma satelitarnego. Stacje troposferyczne pozostawały w rezerwie. Rozwinięty na potrzeby PKW w Iraku system łączności stanowił kombinację środków łączności satelitarnej, troposferycznej i horyzontalnej.

Początek XXI wieku to również intensywne prace nad wykorzystaniem systemów łączności troposferycznej. Opracowane w armii amerykańskiej aparatownie AN/TRC-170 zapewniały przepływność 4 Mb/s (w Afganistanie AN/TRC-170 V5 16 Mb/s). Pierwsze ich wersje (V1 i V2) składały się z czteroosobowej załogi, a czas ich rozwinięcia i skonfigurowania wynosił 5 godz. Obecnie dwie radiolinie troposferyczne zainstalowane na pojeździe M1097 Heavy HMMWV obsługuje dwuosobowa załoga, a czas ich rozwinięcia i ustawienia wynosi godzinę.

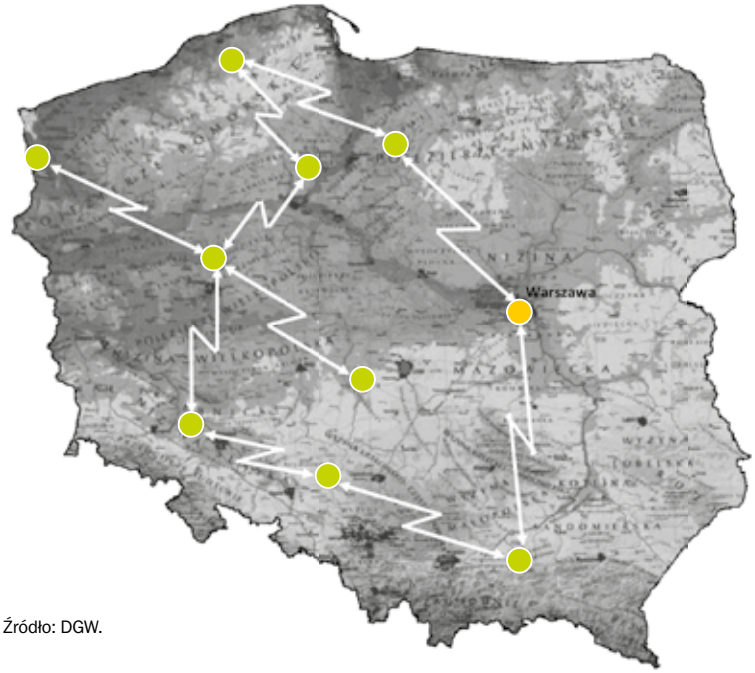
W armii amerykańskiej wykorzystuje się dzisiaj radiolinie troposferyczne AN/TSC-198 o maksymalnej przepływności łącza 50 Mb/s, co stanowi skuteczną alternatywę dla łączności satelitarnej.

NASZE ROZWIĄZANIA

Projekt rodzimej mobilnej aparatowni transmisyjnej troposferyczno-horyzontowej MAT-10TH, opracowanej w Zakładzie Doskonalenia Zawodowego w Krakowie, powstał w 2006 roku. Przeprowadzone testy, m.in. podczas warsztatów łączności „Combined Endavour-09" w Bośni i Hercegowinie w 2009 roku oraz w czasie ćwiczeń „Borsuk-10" w 2010 roku, wykazały duży potencjał opracowanych rozwiązań w zakresie wykorzystania łączności troposferycznej. W kolejnych latach powstały różne wersje tych aparatowni, m.in. MAT-10CT, MAT-10CJ. Umożliwiają one pracę z maksymalną mocą nadajnika do 1000 W i są przeznaczone do zapewnienia łączności między dwoma punktami w odległości 50–250 km z szybkością transmisji 256-8448 kb/s przy wykorzystaniu propagacji troposferycznej. Zastosowane w nich urządzenia zapewniają współpracę z obecnie eksploatowanymi aparatowniami typu RWŁC-10/T, RWŁC-10/K i innymi urządzeniami łączności oraz wozami dowódczo-sztabowymi. Aparatownia może pełnić funkcję małego węzła abonenckiego. Połączenia z innymi węzłami abonenckimi zapewniają dwie radiolinie horyzontowe R-450A.

Głównym elementem aparatowni troposferycznej MAT-10 jest zestaw cyfrowej radiolinii troposferycznej R-450BT firmy Transbit pracującej w paśmie C (4,4–5 GHz) i odpowiedzialnej za realizację łączności dalekosiężnej. Wyposażenie radiolinii troposferycznej w GPS, elektroniczny kompas magnetyczny, układ do zdalnej regulacji automatyki azymutu i kąta elewacji anten (na odległość do 600 m) umożliwia automatyzację procesu nawiązywania łączności, znacząco skracając czas oraz ograniczając liczbę osób do obsługi.

RYS. 1. MOBILNA SIEĆ SZKIELETOWA WYKORZYSTUJĄCA APARATOWNIE TROPOSFERYCZNE (WARIANT I)

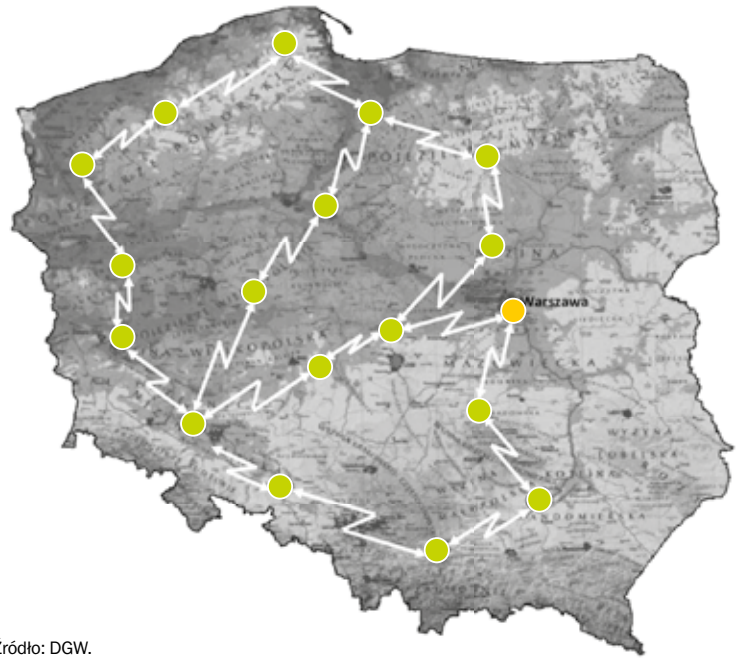


Źródło: DGW.

Nowoczesne aparatownie troposferyczne są w stanie zapewnić budowę mobilnej sieci szkieletowej na duże odległości – do 200–250 km, gwarantując tym samym łączność w razie zniszczenia stacjonarnego systemu łączności (rys. 1 i 2).

Funkcjonalność aparatowni troposferycznych można również wykorzystać do szybkiej odbudowy wybranych relacji stacjonarnych. W trakcie pozyskiwania aparatowni troposferycznych należy koniecznie pamiętać o wyposażeniu ich w odpowiednie interfejsy (złącza), które pozwolą na ich dołączenie do systemów dowodzenia i łączności użytkowanych w siłach zbrojnych. Ponadto aparatownie powinny dysponować półkompletem radiolinii horyzontalnych wraz z systemem antenowym celem przyjęcia bezprzewodowych traktów radioliniowych. Rozwiązania te pozwolą na zapewnienie interoperacyjności aparatowni

RYS. 2. MOBILNA SIEĆ SZKIELETOWA WYKORZYSTUJĄCA APARATOWNIE TROPOSFERYCZNE (WARIANT II)



Źródło: DGW.

troposferycznej z innym sprzętem, m.in. ZWT KTSA Jaśmin czy RWŁC-10/T (rys. 3 i 4). Duże moduły umożliwiają skuteczne wpięcie się do systemu za pomocą kierunku radioliniowego. Wykorzystanie ich pozwala stworzyć niezawodną platformę transmisyjną na bazie aparatowni łączności troposferycznej na obszarze około 250x250 km, a współpraca z większą liczbą aparatowni (z innych rodzajów sił zbrojnych) umożliwi stworzenie rozległej sieci szkieletowej między WŁ.

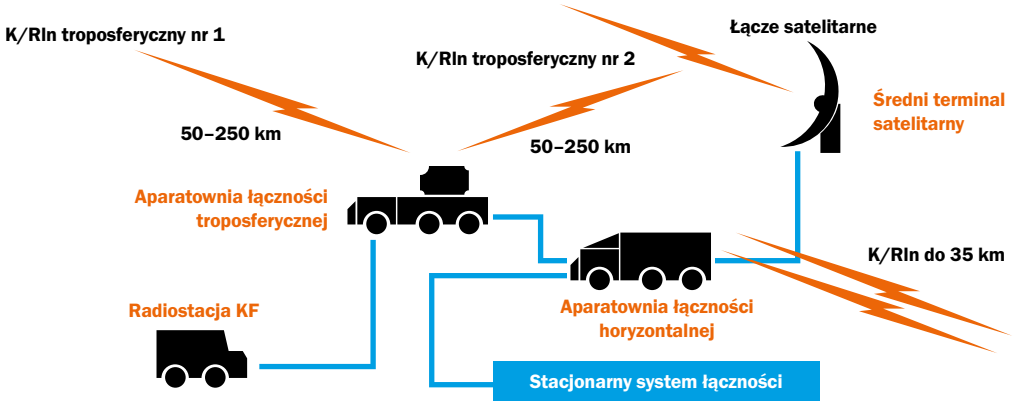
Dodatkowo wyposażenie dużych modułów pozwala również na wykorzystanie terminala satelitarnego, który umożliwia realizację łączności o zasięgu globalnym także w trakcie wykonywania zadań poza granicami kraju. Zadaniem zwykłego modułu będzie jedynie dowiązanie węzłów łączności stanowisk dowodzenia do istniejącej infrastruktury stacjonarnej.

Środki łączności HF wchodzące w skład dużego i zwykłego modułu zapewnią możliwość śledzenia przemieszczających się modułów, łączność służbową do czasu zestawienia traktów troposferycznych lub satelitarnych, następnie punkty retranslacyjne systemu HF (relacje dowodzenia i alarmowania poziomu strategicznego i operacyjnego).

Przewagę zastosowania łączności troposferycznej (pozahoryzontowej) nad łącznością radioliniową (horyzontalną) przedstawiono na rysunku 5. Z zobrazowania tego wynika, że zorganizowanie osi radioliniowej na odległość 140 km wymaga zaangażowania jedynie dwóch aparatowni troposferycznych w stosunku do sześciu aparatowni horyzontalnych przy odpowiednim ich rozmieszczeniu. Kierunki radioliniowe stacji horyzontalnych są uzależnione od tzw. profilu trasy, czyli przesłonięć między antenami. Ze względu na ugięcie Ziemi, wynoszące około 24 m na odległość 35 km, wymagane jest precyzyjne planowanie trasy, aby uzyskać tzw. wolną I strefę Fresnela.

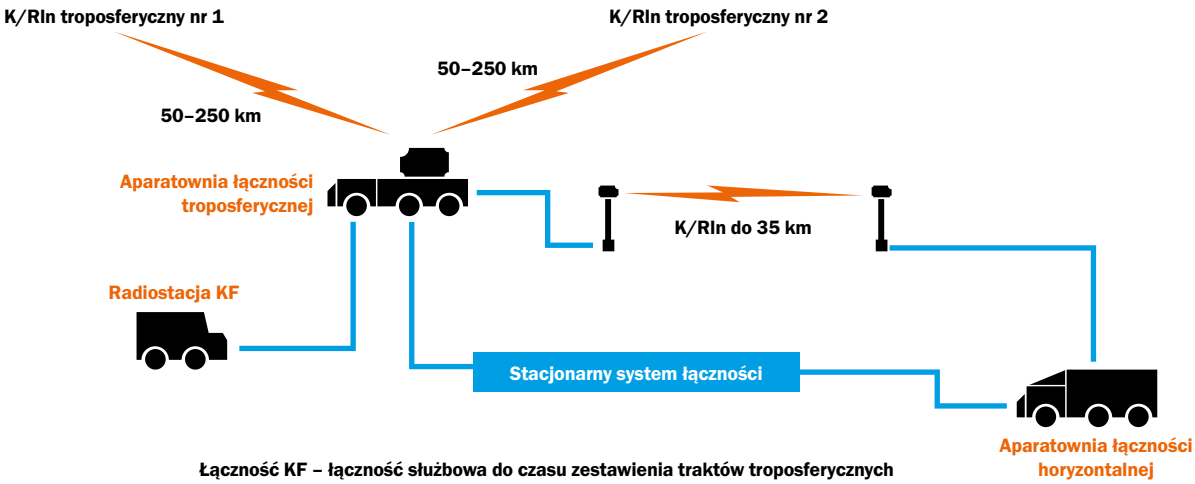
Dodatkowe korzyści, które wynikają z zastosowania łączności troposferycznej, to:

RYS. 3. KONCEPCJA FUNKCJONOWANIA DUŻEGO MODUŁU



Opracowanie własne.

RYS. 4. KONCEPCJA FUNKCJONOWANIA ZWYKŁEGO MODUŁU



Łączność KF – łączność służbowa do czasu zestawienia traktów troposferycznych

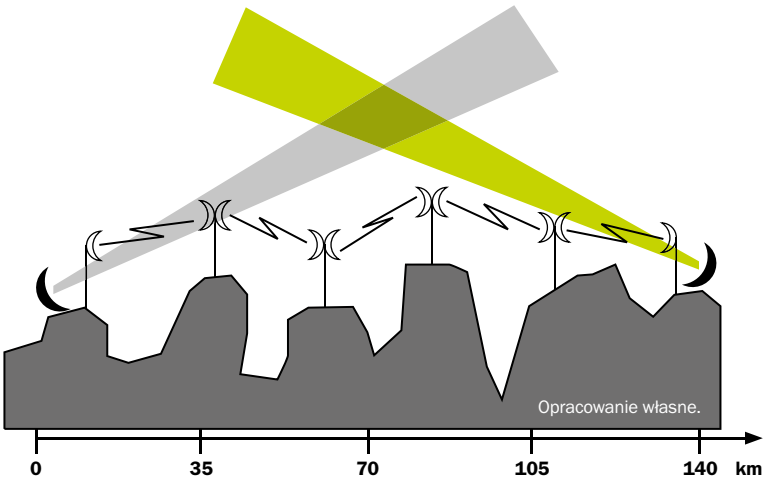
- znacząco niższe koszty operacyjne w stosunku do dzierżawy pasm satelitarnych czy leasingu transponderów satelitarnych;
- brak ryzyka związanego z dostępnością łączy satelitarnych;
- małe opóźnienie dla aplikacji krytycznych (np. dane radarowe);
- możliwość zapewnienia łączności na znacznie większej odległości między stanowiskami dowodzenia;
- brak kosztów transmisji danych;
- autonomiczne rozwiązanie pozwalające na realizowanie niezawodnego systemu łączności w każdych warunkach geopolitycznych;
- niskie koszty utrzymania.

WNIOSKI

Dalekosiężne systemy łączności oparte na łączności pozahoryzontowej powinny być rozwijane oraz produkowane z wykorzystaniem narodowego potencjału naukowego, technologicznego i produkcyjnego. Deklarowane parametry techniczne muszą być zgodne z rzeczywistością i sprawdzone, tym bardziej że ich ewentualny zakup wiąże się z eksploatacją systemu łączności troposferycznej przez najbliższe kilkadziesiąt lat.

Ewolucja systemów troposferycznych dzięki zwiększeniu ich możliwości i zmniejszeniu wymiarów stanowi alternatywę dla systemu łączności satelitarnej. W razie konieczności dzierżawy pasma satelitarnego od podmiotów komercyjnych rozwój systemów łączności troposferycznej wydaje się oczywistą alternatywą i szansą dla naszych sił zbrojnych. ■

RYS. 5. PORÓWNANIE WARIANTU WYKORZYSTANIA APARATOWNI TROPOSFERYCZNYCH I HORYZONTALNYCH



Monitorowanie położenia **wojsk własnych i przeciwnika**

PRECYZYJNE OKREŚLENIE POŁOŻENIA I CECH IDENTYFIKACYJNYCH WŁASNYCH ORAZ SOJUSZNICZYCH PLATFORM BOJOWYCH, A TAKŻE INNYCH ŚRODKÓW WALKI WPŁYWA NA WZROST ŚWIADOMOŚCI OPERACYJNEJ. WSPIERA TYM SAMYM PROCES DECYZYJNY.

mjr Marcin Nalberczyński

Autor jest specjalistą w Zarządzie Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ.

Wymagania pola walki, charakter prowadzonych operacji oraz ich dynamika powodują potrzebę zapewnienia i rozwijania w naszych siłach zbrojnych specjalistycznych systemów dostarczających w czasie rzeczywistym (zbliżonym do rzeczywistego) między innymi danych o wojskach własnych (np.: położenie, kierunek przemieszczania, skład ugrupowania). Jednym z nich jest system monitorowania sił własnych określany w ramach Sojuszu Północnoatlantyckiego (NATO) skrótem FFTS (Friendly Force Tracking System). Stanowi on istotne źródło informacyjne dla zautomatyzowanych systemów wsparcia dowodzenia, rozpoznania, kierowania środkami walki, zabezpieczenia logistycznego działań oraz przetrwania i ochrony wojsk itp.

NARZĘDZIE I JEGO MOŻLIWOŚCI

W skład systemu FFTS wchodzą tylko platformy wojsk lądowych, ponieważ marynarka wojenna i siły powietrzne używają innych, porównywalnych systemów współpracujących na przykład z radarami, systemem IFF (Identification Friend or Foe) czy taktycznymi systemami transmisji danych, które zasilają stanowiska dowodzenia informacjami o platformach powietrznych RAP (Recognized Air Picture) oraz morskich RMP (Recognized Maritime Picture).

Obecnie nasze siły zbrojne wykorzystują System Informatyczny Monitorowania Geograficznego Położenia Obiektów GPS (SI MGPO GPS) bazujący w części związanej z prezentacją położenia sił własnych (i przeciwnika) oraz tła operacyjnego na oprogramowaniu Pakiet Grafiki Operacyjnej 2014 Service Pack 3 (PGO 2014 SP3).

Jest on przeznaczony do monitorowania położenia sił i środków z wykorzystaniem odpowiednich sieci radiowych (VPN GSM) oraz polowych systemów łączności. Archiwizuje trasy przemieszczania się pojazdów wyposażonych w transpondery mobilne SI MGPO GPS (fot.) oraz usprawnia zarządzanie transportem wojsk, wykorzystując w tym celu narzędzia wspomagające. W zakresie funkcjonalnym oraz eksploatacyjno-operacyjnym jest odpowiedni dla poziomu taktycznego, szczególnie w przypadku sieci radiowych o niskiej i bardzo niskiej przepustowości oraz mobilnych relacji radiowych zestawianych bez wcześniejszego przygotowania (*ad hoc*), między innymi dla działań charakteryzujących się dużą manewrowością. W razie zastosowania go jako medium transmisyjne sieci o wysokiej przepustowości [lokalne sieci komputerowe (LAN) lub szybkie sieci radiowe] możliwości systemu będą większe. Aktualna wersja oprogramowania SI MGPO GPS pozwala na:

Widok terminalu SI MGPO GPS umieszczonego w KTO Rosomak

ARCHIWUM AUTORA

– zbieranie danych o położeniu obiektów nadających automatycznie położenie z sieci radiowej fal ultrakrótkich (UKF; Ultra High Frequency – UHF) z wykorzystaniem samej radiostacji lub na stanowisku pracującym również w stanie ciszy radiowej;

– zbieranie danych o położeniu radiostacji nadających automatycznie położenie z sieci radiowej UKF z wykorzystaniem radiostacji „ręcznych" (poszczególnych żołnierzy); łącznie do 32 radiostacji;

– zbieranie danych o położeniu obiektów nadających automatycznie położenie z sieci radiowej fal krótkich (KF; High Frequency – HF); łącznie dziesięć obiektów radiowych pracujących w ramach jednej sieci;

– zarządzanie informacją (np.: agregacja, retranslacja) o położeniu obiektów;

– przesyłanie informacji o położeniu obiektów na inne stanowiska monitorujące drogą radiową w polowych relacjach UKF i KF bardzo niskiej przepustowości, przewodowo i bezprzewodowo z wykorzystaniem łączności o wysokiej przepustowości [LAN, Wireless Fidelity (WiFi), łącze satelitarne, łącze wirtualnej sieci prywatnej globalnego systemu łączności telefonii komórkowej (Virtual Private Network Global System for Mobile Communications – VPN GSM), łącze radioliniowe];

– wspomaganie operatora (z wykorzystaniem PGO 2014 SP3 i map wysokościowych) przy optymalnym rozmieszczeniu radiostacji UKF oraz pracujących na fali przyziemnej radiostacji KF;

– bieżącą orientację w terenie podczas marszu na podstawie podkładów mapowych PGO 2014 SP3 z wykorzystaniem nawigacji lokalnej opierającej się na odbiornikach wojskowych lub komercyjnych GPS dołączonych do komputera i radiostacji lub wbudowanych w radiostacje;

– bieżącą i bardzo szybką orientację w ilości sił i środków (obiektów wybranych typów) zlokalizowanych w zdefiniowanych przez użytkownika obszarach zainteresowania;

– przesyłanie w sieci radiowej UKF i KF między stanowiskami sytuacji operacyjnej (np. zmieniającego się położenia wojsk własnych lub przeciwnika) wytworzonej w oprogramowaniu PGO 2014 SP3 oraz jej automatycznej aktualizacji na stanowisku adresata.

Ponadto oprogramowanie SI MGPO GPS może być wykorzystane do:

– przesyłania krótkich informacji tekstowych w sieci lokalnej i sieci radiowej UKF i KF (Tactical Chat);

– wysyłania i odbierania alarmów w sieci radiowej UKF (m.in. z automatycznym przekazywaniem ich do sieci lokalnej na inne stanowiska);

Zadanie monitorowania elementów własnego ugrupowania powinno być realizowane z wykorzystaniem systemów automatyzacji dowodzenia i kierowania środkami walki.

JACEK SZUSTAKOWSKI

– efektywnego manualnego przesyłania plików (dowolne formaty) w sieci lokalnej oraz sieci radiowej UKF i KF;

– serwowania i synchronizacji czasu w sieci radiowej i sieci lokalnej;

– przesyłania między stanowiskami dowodzenia w sieci radiowej UKF i KF komunikatów o zagrożeniu użyciem broni masowego rażenia (Chemical, Biological, Radiological and Nuclear – CBRN) wytworzonych z wykorzystaniem oprogramowania Kreator Wiadomości CBRN oraz ich automatycznej aktualizacji (jeżeli na stanowisku jest zainstalowane oprogramowanie systemu informatycznego SI Promień);

– nawiązywania komunikacji z wykorzystaniem sieci radiowej ze stanowiskami pracującymi w tzw. ciszy radiowej w zakresie odbierania przez nie wysyłanych z innych stanowisk: alarmów, wiadomości tekstowych, położenia obiektów własnych oraz rozpoznanych obiektów przeciwnika, plików projektów PGO 2014 SP3 oraz plików protokołu NVG (NATO Vector Graphics) na potrzeby automatycznie odświeżanego tła operacyjnego w PGO 2014 SP3, a także plików i zdjęć skompresowanych operacyjnie w innym oprogramowaniu (np. IMAGER);

– wytwarzania i odczytu wiadomości w formacie ADatP-3;

– wytwarzania prostych meldunków bojowych o ewakuacji medycznej (Medical Evacuation – MEDEVAC), próśb o wsparcie sił szybkiego reagowania (Quick Reaction Force Request – QRF REQUEST), raportów o aktywności przeciwnika (Salute Report), o stanie transportu (Salter Report) oraz o incydentach z wykorzystaniem improwizowanych urządzeń wybuchowych lub o niewybuchach (bombach, pociskach, granatach, minach lądowych lub morskich).

Oprogramowanie SI MGPO GPS opierające się na zastosowaniu polowych środków łączności (np. radiostacji) cechuje się małymi wymaganiami w odniesieniu do sprzętu teleinformatycznego używanego bez wcześniejszego przygotowania, szczególnie istotnymi w warunkach polowych, a mianowicie:

– wydajną pracą programu nawet z użyciem starszych typów komputerów;

– możliwością jednoczesnej pracy z kilkoma urządzeniami sieciowymi;

– zdolnością do pracy podczas ruchu naziemnej platformy bojowej lub śmigłowca;

– możliwością sprawnego wykorzystania jednego środka radiowego UKF do pracy (w tym automatycznej) w wielu sieciach radiowych;

– brakiem konieczności posiadania oprogramowania serwerów poczty oraz stosowania sprzętu serwerowego;

– małym poborem energii podczas pracy programu z użyciem sprzętu mobilnego.

Oprogramowanie SI MGPO GPS zostało już praktycznie przetestowane. Współpracuje z wybranym sprzętem łączności, wzmocnionymi i wytrzymałymi komputerami klasy semi rugged lub fully rugged oraz z GPS umożliwiającymi ich implementację na poziomie taktycznym.

REFLEKSJE

Zadanie monitorowania elementów własnego ugrupowania powinno być realizowane z wykorzystaniem systemów automatyzacji dowodzenia i kierowania środkami walki. Możliwość osiągnięcia przewagi informacyjnej i tym samym tworzenia oraz istotnego zwiększenia świadomości sytuacyjnej zgrupowań bojowych, w tym ich bezpieczeństwa, zapewnia na przykład natychmiastowa i skuteczna dystrybucja informacji o zagrożeniach oraz zastosowanie zautomatyzowanego systemu informowania o bieżącym położeniu wojsk własnych. Pozwoli to również na automatyczne tworzenie połączonego obrazu sytuacji operacyjnej (POSO) w czasie zbliżonym do rzeczywistego oraz na współpracę z innymi systemami. Efektem użytkowym wprowadzenia SI MGPO GPS jest uzyskanie rozwiązań zwiększających świadomość sytuacyjną, tym samym zapewniających większą skuteczność działania i precyzję oddziaływania na przeciwnika oraz uniknięcie ognia bratobójczego w trakcie operacji połączonych prowadzonych w czasie kryzysu i wojny. ■

Nośniki **danych**

ŻOŁNIERZE I PODODDZIAŁY W WALCE KORZYSTAJĄ Z ŁĄCZNOŚCI BEZPRZEWODOWEJ, KTÓRA POWINNA BYĆ NIEZAWODNA I ODPORNA NA WSZELKIEGO TYPU ZAKŁÓCENIA.

dr inż. Marek Dąbrowski

Autor jest publicystą zajmującym się tematyką militarną.

W przeciwieństwie do efektów ognia prowadzonego z różnych środków walki pasmo przenoszenia informacji nad rejonami (obszarami) prowadzonych zmagań nie jest widoczne. Jednak stale jest atakowane, czy to w sposób zamierzony, czy też uwarunkowany środowiskiem walki. Widmo elektromagnetyczne dziś jest już mocno zatłoczone, a jego przeciążenie będzie tylko się zwiększało. A do tego trzeba pokonać systemy walki radioelektronicznej (WRE) przeciwnika czy cyberatak na wykorzystywane przez nas oprogramowanie.

Z kolei operacje wielodomenowe wymagają płynnego i szybkiego przekazywania informacji, co obecnie nie do końca jest spełnione. Dlatego wiele armii stoi przed poważnym zadaniem: szukaniem nowych rozwiązań w tej dziedzinie. Niezbędne też jest opracowanie precyzyjnych wymagań i nawiązanie współpracy z przemysłem i ośrodkami naukowymi.

POSZUKIWANIA

Od sieci taktycznej w zastosowaniach militarnych wymaga się wykorzystania kilku różnych technologii (dynamicznie konfigurowalnych i zarządzanych systemów sieciowych) do komunikacji między poszczególnymi węzłami wchodzącymi w jej skład. Również w sytuacji, gdy brakuje wymaganej infrastruktury czy wysokiej mobilności. Dodatkowo w siłach zbrojnych jest niezbędne, aby wzajemne oddziaływanie sieci czy innych systemów na siebie było ograniczone. Uzyskuje się to dobierając odpowiednie protokoły warstwy fizycznej oraz utrzymując łączność przy dynamicznie zmieniającej się jej topologii dzięki wykorzystaniu efektywnych protokołów routingu oraz, co istotne, gwarantując wysoki poziom bezpieczeństwa ich wykorzystania.

Aby to osiągnąć, siły zbrojne mogą wybrać dwie drogi postępowania: zbudować nowe, własne pasma przenoszenia lub skorzystać z komercyjnych rozwiązań dostępnych na rynku cywilnym i zmodyfikowanych pod kątem zastosowań militarnych (Commercial of the Shelf). O ile te pierwsze staną się własnością armii, o tyle rozwiązanie z „półki" należy do wybranej firmy, która jest odpowiedzialna za aktualizację oprogramowania, wprowadzane poprawki czy testy adaptacyjne. Trzeba też zaaprobować rygorystyczne protokoły bezpieczeństwa i pamiętać, że komercyjne rozwiązania nie zawsze spełnią oczekiwania wojsk, lecz są dostępne w zasadzie od ręki.

Wprowadzane rozwiązanie TSM (Tactical Ad Hoc Battlefield Networking – mobilne sieci ad hoc) nie do końca zostało zaakceptowane w siłach zbrojnych. Zmodernizowana siatka przebiegów sieciowych składa się z grupy urządzeń, które działają jako pojedyncze Wi-Fi, sieć obsługująca internetowy protokół danych i głos jednocześnie. TSM może działać w wielu wariantach pasma, umożliwiając użytkownikowi przełączanie częstotliwości i wielokanałowe tryby przepustowości – przełączanie się od 1.2 do 10 MHz z obsługą do 32 grup głosowych.

Choć TSM działa na krótkich dystansach (tzw. zasięgu widzialności wzrokowej), to pozwala każdemu węzłowi na przesyłanie, odbieranie i przekazywanie danych czy lokalizację informacji jednocześnie. Te możliwości zapewniły integralne zdolności

w ramach zintegrowanego zestawu możliwości sieci taktycznej (ITN).

Nie tylko w USA, także i w wielu innych krajach jest użytkowany jednokanałowy naziemny i powietrzny system radiowy (Single Channel Ground and Airborne Radio System – SINCGARS). Radiotelefon typu Combat-net (CNR) jest wykorzystywany w wielu armiach, a sama sieć jest zbudowana wokół trzech systemów: wspomnianego SINCGARS, radia wysokiej częstotliwości (HF) oraz satelity taktycznego SC (TACSAT). Każdy system ma jednak inne możliwości i charakterystykę transmisji.

Podstawową rolą SINCGARS jest transmisja głosu w ramach C2 między naziemnymi i powietrznymi systemami dowodzenia. Może on działać w trybie SC lub przeskoku częstotliwości (FH) i przechowuje zarówno częstotliwości SC, jak i FH. System jest kompatybilny ze wszystkimi radiotelefonami VHF-FM w trybie SC niezabezpieczonym. Działa na dowolnym z 2320 kanałów od 30 do 88 MHz z separacją kanałów co 25 kHz. Akceptuje wejścia cyfrowe lub analogowe i nakłada sygnał na falę nośną o częstotliwości radiowej (RF). W trybie FH zmienia częstotliwość około 100 razy na sekundę w częściach taktycznego zakresu VHF-FM. SINCGARS zapewnia szybkość transmisji danych do 16 000 bit/s.

Jest on obsługiwany przez liczne systemy łączności, m.in. jednokanałowy RT-1523 VHF, który obecnie jest modernizowany do standardu internetowego radia bojowego. Ale mamy tu też nowoczesne, dwukanałowe definiowane programowo systemy AN/PRC-148D i AN/PRC 163 Leader, radiotelefony oraz radiostacje plecakowe AN/PRC-158 i AN/PRC-162. Tu zaletą jest zdolność do wykorzystania SINCGARS na jeden kanał i zmianę w zależności od charakteru wykonywanego zadania. Pasma SINCGARS są obecnie modernizowane, co ma zwiększyć ich efektywność w ochronie przed systemami WRE i poprawić jakość prowadzonych rozmów.

W wypadku transmisji klasyfikowanych jako tajne lub poniżej w siłach zbrojnych USA wykorzystuje się Warrior Robust Enhanced Network (WREN). TSM, która zapewnia żołnierzom opcję uruchamiania zarówno funkcji Sensitive But Unclassified (SBU), jak i Secret oraz Below, przy użyciu krypto NSA typu 1 na różnych kanałach lub pojedynczo, zachowując pełną izolację danych i głosu na dostępnych poziomach klauzuli tajności. Gwarantuje to elastyczność w sytuacjach, gdy komunikacja na poziomie tajnym nie jest potrzebna, a w razie takiej potrzeby WREN może nadal działać w trybie secret i zezwalać na ruch zaszyfrowany przez NSA w tej samej sieci.

Armie, które rozumieją powagę zagrożenia i jako pierwsze podejmą próbę wprowadzenia nowych rozwiązań, zapewniających szybki, nieprzerwany, skalowalny i odporny przepływ informacji w przeciążonym i zakłóconym środowisku elektromagnetycznym, będą się znajdować na uprzywilejowanej pozycji.

US ARMY

Nowe zdolności testowali już żołnierze 1 Brygadowego Zespołu Bojowego 82 Dywizji Powietrznodesantowej w Fort Bragg w 2021 roku. Wykorzystanie WREN TSM, zintegrowane z systemem Android Tactical Assault Kit (ATAK) w ramach taktycznego zestawu Nett Warrior, umożliwiało żołnierzom przekazywanie informacji z utajnionych lokalizacji oraz głosu i dowolnego tekstu na dowolnie sklasyfikowanym poziomie w celu zwiększenia świadomości sytuacyjnej. Sprzęganie Secret-and-Below i SBU (Sensitive But Unclassified) pozwala uzyskać bezpieczną transmisję danych.

Ponadto w ramach tego sprawdzianu jeden węzeł został zintegrowany z platformą Joint Battle Command-Platform (JBC-P), która zapewniała wspólny obraz operacyjny (COP) uwzględniający PLI wszystkich 93 węzłów w sieci.

Nowy wąskopasmowy WREN – WREN-Narrowband (NB) daje już rozszerzoną komunikację (jednoczesne przesyłanie głosu, informacji o położeniu i danych w postaci fali sieci mobilnej ad-hoc skalowalnej do setek węzłów), w tym w obszarze powietrze–ziemia, powietrze–powietrze, oraz efektywniejszą ochronę przed WRE, a także wsparcie przeciwzakłóceniowe i małe prawdopodobieństwo przechwycenia.

Wąskopasmową falę *Katana* zaprojektowano do działania w bardzo spornym środowisku komunikacyjnym, wykorzystującym częstotliwości radiowe. Jest ona odporna na zaawansowane ataki elektroniczne i obsługuje systemy łączności na poziomie bezpieczeństwa SBU z programem wąskopasmowym US Army Program of Record (PoR) Warrior Robust Enhanced Networking (WREN) (WREN NB).

Daje to możliwość rozbudowy radiotelefonów TrellisWare Software Defined Radios (SDR) obecnej generacji do obsługi zarówno kształtu fali TSM, jak i kształtu fali *Katana*. Najnowszy system oferuje funkcje podstawowe, alternatywne i awaryjne (PACE) do pracy zarówno w zatłoczonych, jak i spornych środowiskach.

Największe wyzwania na obecnym etapie prac badawczych są związane z poprawą integracji fal w obszarach: o niskim prawdopodobieństwie wykrycia (LPD), niskim prawdopodobieństwie przechwycenia (LPI) oraz niskim prawdopodobieństwie geolokalizacji (LPG). Istotny jest też rozwój funkcji zapobiegających, które mogą wyprzedzić możliwości zagrożenia przeciwnika. Te ostatnie pozwalają uniknąć zakłóceń dzięki technologii przeskoku częstotliwości lub technologii widma rozproszonego, które zmniejsza skutki zakłóceń. Z kolei LPI i LPD minimalizują widmową obecność kształtu fali, co pozwala uniknąć wykrywania i zakłócania, równoważąc jednocześnie przepustowość i możliwe do uzyskania zasięgi.

W armii amerykańskiej wstępnie oceniono rozwiązania komercyjne pod kątem spełnienia LPI i LPD oraz odporności na WRE w przeciążonym środowisku elektromagnetycznym. Przeprowadzono też konkurs technologiczny xTechSearch dla małych firm, aby zidentyfikować oferowany przez nie sprzęt i oprogramowanie.

Ponadto Manager Waveforms stworzyła sieć radiową o wysokiej skali zdolności do działania w przewidywanym, przyszłym środowisku walki.

SIŁY ZBROJNE MOGĄ WYBRAĆ DWIE DROGI POSTĘPOWANIA: ZBUDOWAĆ NOWE, WŁASNE PASMA PRZENOSZENIA LUB SKORZYSTAĆ Z KOMERCYJNYCH ROZWIĄZAŃ DOSTĘPNYCH NA RYNKU CYWILNYM.

PODSUMOWANIE

Chociaż obecne i przyszłe pole walki zdominują kolejne generacje systemów rażenia, to najbardziej krytycznym jego elementem pozostanie system wymiany danych. To w zasadzie on będzie spinał pozostałe składowe, będąc zarazem w największym stopniu narażony na zamierzone ataki lub środowiskowe utrudnienia. Armie, które rozumieją powagę zagrożenia i jako pierwsze podejmą próbę wprowadzenia nowych rozwiązań, zapewniających szybki, nieprzerwany, skalowalny i odporny przepływ informacji w przeciążonym i zakłóconym środowisku elektromagnetycznym, będą się znajdować na uprzywilejowanej pozycji. Drogi są dwie: opracowanie od podstaw nowych rozwiązań lub dostosowanie tych już istniejących. Zatem już dziś należy szukać wyprzedzających rozwiązań w sferze dystrybucji danych, by znane lub przewidywalne zagrożenia, przed którymi siły zbrojne staną w przyszłości, zostały pokonane. ■

Radiostacja AN/PRC 150C w wojskach obrony terytorialnej

BY ZAPEWNIĆ NIEZAWODNĄ WYMIANĘ INFORMACJI MIĘDZY ELEMENTAMI UGRUPOWANIA BOJOWEGO, NALEŻY DYSPONOWAĆ ODPOWIEDNIM SPRZĘTEM ORAZ PROFESJONALNIE WYSZKOLONYMI OBSŁUGAMI.

plut. mgr Kamil Nowakowski

Autor jest młodszym instruktorem w Centrum Szkolenia Łączności i Informatyki.

Jednym z głównych zadań wojsk obrony terytorialnej jest obrona oraz wspieranie lokalnych społeczności. W czasie pokoju oznacza to między innymi przeciwdziałanie klęskom żywiołowym i zwalczanie ich skutków, a także prowadzenie działań ratowniczych i poszukiwawczych. Natomiast w czasie wojny będzie to prowadzenie działań przeciwdywersyjnych, nieregularnych, ochrona mienia oraz wsparcie elementów układu pozamilitarnego, jak również współdziałanie z wojskami operacyjnymi.

POTRZEBY

By żołnierze WOT mogli być „zawsze gotowi i zawsze blisko" swoich małych ojczyzn, konieczna jest niezawodna łączność zapewniona z zastosowaniem właściwych środków. Jednym z nich jest radiostacja AN/PRC 150C (fot. 1). Spełnia ona kilka ważnych kryteriów, do których należą wszechstronność oraz trudność podsłuchania przekazywanych przez nią informacji. Jej zaletą są również niewielkie rozmiary. Radiostacja umożliwia łączność nie tylko z pododdziałami wojsk lądowych, lecz gwarantuje także współpracę ze statkami powietrznymi zarówno wojskowymi, jak i cywilnymi.

Jest przeznaczona do pracy cyfrowej i analogowej w sieciach i na kierunkach radiowych. Wykorzystywana jest do utrzymywania łączności w dalekosiężnych relacjach radiowych na szczeblu taktycznym w zakresie HF/VHF w przedziale częstotliwości od 1,6 do 59,9999 MHz. Radiostacja pracuje w układzie simpleksowym i duosimpleksowym. Zapewnia pracę fonem oraz transmisję danych w systemie synchronicznym i asynchronicznym, w łączu jawnym i utajnionym.

Jej główne funkcje to:

– realizacja bezpiecznej łączności cyfrowej dzięki trybowi szyfrowania Type I;

– nadawanie głosowe w trybie cyfrowym oraz zapis wiadomości LDV w pamięci radiostacji (Last Ditch Voice);

– automatyczne zestawianie połączenia ALE (Automatic Link Establishment);

– automatyczne sterowanie radiostacją ARCS (Automatic Radio Control System) oraz protokołami ustawień połączeń i przesyłu danych w trybie 3G;

– odbiór i nawiązywanie połączeń w trybie ALE podczas działania w trybie 3G i 3G+;

– udoskonalona funkcja częstotliwości skokowej w paśmie KF – tryb HOP;

– możliwość automatycznej synchronizacji czasu TOD (Time-of-Day) po podłączeniu GPS z precyzyjnym odczytem;

– zdolność do działania sieciowego za pośrednictwem protokołu PPP lub sieci lokalnej Ethernet;

1. Radiostacja AN/PRC 150C

2. Praktyczne wykorzystanie radiostacji w trakcie ćwiczeń

ARCHIWUM AUTORA (2)

– opcjonalnie możliwość zmniejszenia prawdopodobieństwa przechwycenia (Low Probability of Intercept – LPI) i wykrycia (Low Probability of Detection – LPD) za pomocą szybkiego przekazywania wiadomości na niskim poziomie mocy;

– możliwość zdalnego sterowania radiostacją po podłączeniu terminalu zdalnego sterowania przez RS-232/RS-422 lub protokół punkt do punktu (Point-to-Point Protocol – PPP);

– możliwość transmisji danych przy użyciu aplikacji TC (Tactical Chat) i WMT (Wireless Message Terminal)[1].

Jej podstawowe dane to[2]:

- pasmo pracy: 1,6 do 59,9999 MHz
- masa: 4,5 kg bez baterii
- zakres temperatury pracy: od -40 do +70°C
- wodoszczelność: zanurzenie do 0,9 m wody
- moc nadawania: 1, 5 lub 20 W.

SZKOLENIE OBSŁUG

Oprócz sprawnych radiostacji warunkiem zapewnienia skutecznej łączności jest właściwe przygotowanie personelu, który będzie je eksploatował. W WOT nauka posługiwania się AN/PRC 150C odbywa się dwuetapowo. W pierwszym etapie operatorzy radiostacji szkoleni są przez mobilne zespoły szkoleniowe, które tworzą byli żołnierze wojsk specjalnych – fachowcy w dziedzinie łączności. To oni, dzieląc się swoim doświadczeniem, są odpowiedzialni za podstawowe przygotowanie łącznościowców najniższego szczebla. Szkolenia odbywają się w trybie rotacyjnym w wymiarze dwóch dni w miesiącu w weekendy. Są organizowane na terenie funkcjonowania danego batalionu OT.

Etapem doskonalenia umiejętności oraz zdobywania odpowiednich uprawnień do pracy z użyciem radiostacji AN/PRC 150C jest szkolenie specjalistyczne prowadzone w kolebce łącznościowców, jak często jest nazywane zegrzyńskie Centrum Szkolenia Łączności i Informatyki. Są tu prowadzone kursy z eksploatacji radiostacji na dwóch poziomach: podstawowym oraz zaawansowanym.

Kurs podstawowy, przygotowujący żołnierzy do obsługi radiostacji, obejmuje następujące zagadnienia:

– przepisy korespondencji radiowej,

– teoretyczne podstawy oraz zasady walki elektronicznej,

– budowa, ukompletowanie oraz możliwości techniczne radiostacji,

– realizacja łączności w podstawowych trybach pracy oraz przygotowanie do transmisji fonicznej.

Podczas kursu zaawansowanego żołnierze zdobywają dodatkowo wiedzę na temat wykorzystania transmisji danych, technicznych możliwości współpracy z urządzeniami zewnętrznymi (laptopy, urządzenia cyfrowe oraz zdolności Switch LAN), a także współdziałania radiostacji z różnego rodzaju aplikacjami (np.: Tactical Chat, RF-6760W WMT itp.). Uczestnik kursu po ukończeniu szkolenia potrafi:

– prowadzić prawidłową wymianę korespondencji radiowej,

– eksploatować radiostację zgodnie z jej przeznaczeniem,

– zaprogramować ją w sposób ręczny, a także przy użyciu komputera.

Po ukończeniu obu poziomu kursów żołnierze uzyskują uprawienia do użytkowania wyspecjalizowanego sprzętu z rodziny Falcon II. Umiejętności opanowane w CSŁiI żołnierze WOT-u weryfikują podczas treningów radiowych oraz ćwiczeń dowódczo-sztabowych, w tym ćwiczeń z wojskami (fot. 2).

W trakcie tych przedsięwzięć szkoleniowych wykorzystywano łączność dalekosiężną między batalionami lekkiej piechoty. Jednym z celów ćwiczeń jest doskonalenie umiejętności wykorzystania możliwości radiostacji AN/PRC 150C[3]. ■

1 http://szpzl-zegrze.waw.pl/wps/anprc_150/rdst.html; http://wzl2.pl/wp-content/uploads/2021/09/WD_FR_21.pdf/.

2 Ibidem.

3 http://www.szpzl-zegrze.waw.pl/pdf/publikacje/k37/3.pdf/.

Działania **powietrznodesantowe**

PRZENIESIENIE CIĘŻARU WALKI W GŁĄB UGRUPOWANIA PRZECIWNIKA JEST MOŻLIWE DZIĘKI WYKORZYSTANIU PRZESTRZENI POWIETRZNEJ PRZEZ ODPOWIEDNIO PRZYGOTOWANE ODDZIAŁY I PODODDZIAŁY WOJSK LĄDOWYCH.

mjr dypl. SZRP Krzysztof Kałwak

Autor jest komendantem Ośrodka Szkolenia Podstawowego w Centrum Szkolenia Wojsk Inżynieryjnych i Chemicznych.

Ten sposób prowadzenia walki może być stosowany dzięki użyciu środków transportu powietrznego, których szybkość i zasięg będą determinować wybór rejonów i obiektów, które mają zostać uchwycone i utrzymane przez zgrupowania lądujące metodą spadochronową bądź wysadzane ze śmigłowców. Jednak ich powodzenie będzie zależeć od wywalczonej i utrzymywanej przewagi w powietrzu, by można było zapewnić zarówno bezpieczeństwo przelotu, jak i wsparcie po wylądowaniu w trakcie walki z przeciwnikiem naziemnym.

ISTOTA

Analizując literaturę przedmiotu, warto zwrócić uwagę na interpretację pojęcia *działania powietrznodesantowe* przez amerykańskiego generała Billy'ego Mitchella, które są rozumiane jako wykorzystanie potencjału i możliwości transportu powietrznego do nagłego przeniesienia walki w głąb ugrupowania przeciwnika w celu uzyskania zaskoczenia, co w konsekwencji spowoduje lokalne załamanie spójności jego struktury obronnej[1].

Regulamin działań wojsk lądowych wskazuje na wykonanie określonych zadań przez wojska powietrznodesantowe (WPD) po ich wylądowaniu w rejonie wynikającym z celu działania[2]. Z kolei A. Polak i J. Joniak definiują działania powietrznodesantowe jako rodzaj działań bojowych charakteryzujący się dużą dynamiką, elastycznością i precyzją prowadzenia. Obejmują one desantowanie oraz przemieszczanie zgrupowań lądowych drogą powietrzną[3]. Natomiast według *Słownika języka polskiego desant* to, po pierwsze, operacja wojskowa polegająca na przerzuceniu i wysadzeniu wojsk na terytorium zajętym przez przeciwnika. Po drugie, są to oddziały wojskowe biorące udział w tej operacji lub przerzucone na teren przeciwnika[4]. W *Leksykonie wiedzy wojskowej* zaś działania desantowe są definiowane jako lądowanie wojsk z powietrza lub morza na terytorium przeciwnika z jednoczesnym prowadzeniem walk z jego oddziałami znajdującymi się w rejonie desantowania lub zdążającymi do tego rejonu[5].

Można zatem stwierdzić, że siły i środki wojsk powietrznodesantowych przerzucane drogą powietrzną w rejon wykonania zadania stanowią desant. Pozostałe siły i środki, które nie są przewidywane do przerzutu, tworzą inne elementy ugrupowania bojowego desantowanego oddziału. Ponadto wszelkie przedsięwzięcia organizacyjne i techniczne związane z przerzutem pododdziałów w rejon działania me-

1 K. Frącik, G. Plaskota, A. Skrzek, *Rola i miejsce kawalerii powietrznej w systemie wojsk aeromobilnych Sił Zbrojnych Rzeczypospolitej Polskiej,* ASzWoj, Warszawa 2019, s. 121.

2 *Regulamin działań wojsk lądowych,* DWLąd. sygn. Wewn. 115/2008, Warszawa 2008, s. 157.

3 A. Polak, J. Joniak, *Sztuka wojenna,* AON, Warszawa 2014, s. 234.

4 *Słownik języka polskiego,* PWN, Warszawa 1992, s. 384.

5 *Leksykon wiedzy wojskowej,* MON, Warszawa 1979, s. 102.

todą spadochronową nazywa się desantowaniem. Najbardziej trafną definicję oddającą istotę działań powietrznodesantowych zawiera amerykańska instrukcja *Field Manual*. Zgodnie z nią są to działania szturmowe wykonane po lądowaniu sposobem spadochronowym w celu zniszczenia przeciwnika lub zdobycia i utrzymania ważnego obiektu do czasu połączenia się z siłami głównymi. Wszystkie rodzaje aktywności w głębi ugrupowania przeciwnika mogą przyczynić się do zniszczenia i neutralizacji jego sił, jak również do zatrzymania jego natarcia[6].

Niewątpliwie zaprezentowane definicje i pojęcia są zbieżne. Ich wspólną cechą jest wskazanie istoty omawianych działań, którą jest wysadzenie desantu spadochronowego w ugrupowaniu bojowym strony przeciwnej. Biorąc jednak pod uwagę to, że mogą być prowadzone we wszystkich rodzajach działań taktycznych oraz w operacjach pokojowych, możemy je zdefiniować jako wykonanie zadań przez wojska powietrznodesantowe po ich wylądowaniu na terenie kontrolowanym przez przeciwnika. Natomiast próbując określić istotę działań wojsk powietrznodesantowych, niewątpliwie należy stwierdzić, że są to jednostki wojsk lądowych biorące udział w walce lądowej, ale wchodzące do niej dzięki użyciu różnych środków transportu powietrznego.

WARUNKI I OGRANICZENIA

Absolutnie konieczną przesłanką, aby WPD przystąpiły do realizacji stojących przed nimi zadań, jest posiadanie przewagi w powietrzu. Pozwoli ona siłom lądowym, morskim i powietrznym na podjęcie działań w określonym czasie i miejscu bez istotnego przeciwdziałania ze strony sił powietrznych przeciwnika. Ponadto powodzenie tych działań w dużej mierze zależy od zachowania tajemnicy oraz zaskoczenia przeciwnika co do miejsca, czasu i sposobu użycia desantu. Osiągnięcie tego efektu będzie możliwe dzięki skrytemu jego przygotowaniu polegającemu na realizacji całokształtu przedsięwzięć maskujących związanych z przemieszczaniem pododdziałów powietrznodesantowych w rejon lotnisk (lądowisk), jak również lotnictwa transportowego. Nie bez znaczenia jest także pora desantowania, która powinna stanowić moment trudny do oszacowania przez przeciwnika, uniemożliwiając mu ocenę wartości użytego potencjału. Należy zaznaczyć, że żołnierze są przygotowywani do działań, w tym wykonywania skoków spadochronowych, w warunkach ograniczonej widoczności.

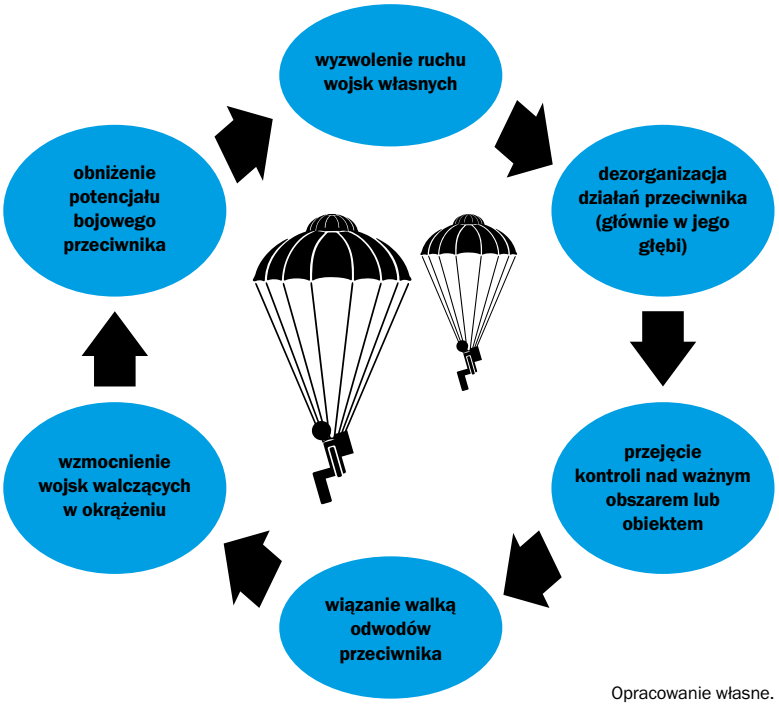
Kolejnym czynnikiem jest rozpoznanie ugrupowania bojowego przeciwnika, tzn. jego możliwości bojowych i prawdopodobnych zamiarów planowanych do zrealizowania blisko stref zrzutu lub lądowania. Istotne staje się również rozpoznanie ugrupowania przeciwnika w danym rejonie bądź w obiekcie, który jest celem ataku.

6 *Field Manual,* No. 90-26, s. 14.

MARIUSZ BIENIEK/6 BPD

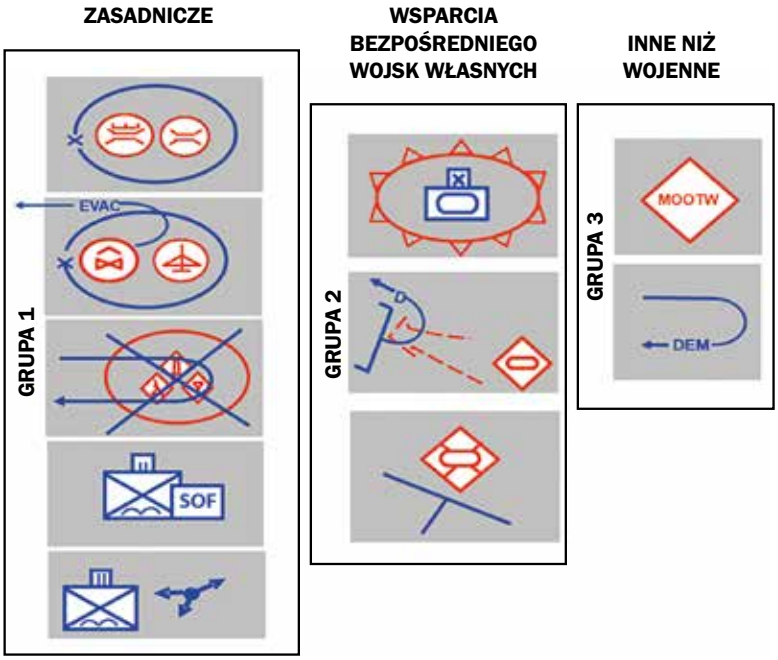
Siły i środki wojsk powietrznodesantowych przerzucane drogą powietrzną w rejon wykonania zadania stanowią desant.

RYS. 1. WYKORZYSTANIE PODODDZIAŁÓW POWIETRZNO-DESANTOWYCH



Opracowanie własne.

RYS. 2. RODZAJE ZADAŃ WYKONYWANYCH PRZEZ PODODDZIAŁY POWIETRZNODESANTOWE



Opracowanie własne.

Oprócz czynników, które muszą zostać uwzględnione, by użycie pododdziałów powietrznodesantowych było realne i skuteczne, należy przeanalizować wszelkie ograniczenia, które będą miały wpływ na wykonanie zadania. Do podstawowych można zaliczyć[7]:

– niekorzystne warunki atmosferyczne determinujące użycie desantu (niski pułap chmur ograniczający widoczność, duża prędkość wiatru, marznące opady deszczu, oblodzenia, silne turbulencje);

– ograniczenia związane z przydzieleniem ilości oraz rodzaju środków transportu powietrznego;

– zdolności ogniowe przeciwnika (w tym środków przeciwlotniczych);

– niepełne rozpoznanie rejonu lądowania desantu i trasy jego przelotu;

– utrudnienia we wsparciu ogniowym walczących pododdziałów;

– kłopoty z zaopatrzeniem w środki bojowe i materiałowe;

– skomplikowane warunki ewakuacji medycznej;

– czas trwania działań powietrznodesantowych.

Liczba statków powietrznych, często dostarczanych poniżej oczekiwanego minimum, wymusza na dowódcach konieczność dokonania korekty podjętej decyzji w odniesieniu do sił i środków przewidzianych do desantowania. Kolejnym aspektem, na który należy zwrócić szczególną uwagę, jest szeroko rozumiana manewrowość pododdziałów powietrznodesantowych po wylądowaniu, w zasadzie ich ograniczona mobilność taktyczna. Spadochroniarz bowiem po wylądowaniu przemieszcza się w celu wykonania powierzonego zadania o własnych siłach. Dlatego też planując użycie pododdziałów powietrznodesantowych, należy wziąć pod uwagę ich żywotność i możliwości bojowe, by nie dopuścić do utraty przez nie zdolności do działania (rys. 1). Należy w związku z tym rozpatrzyć możliwość wzmocnienia ich pododdziałami innych rodzajów wojsk oraz czas połączenia z siłami głównymi. Właściwie zrealizowany proces przygotowawczy z uwzględnieniem wszystkich ograniczeń, jak i czynnika zaskoczenia zniweluje poziom ryzyka do akceptowalnego przez dowódcę, który decyduje o użyciu pododdziałów powietrznodesantowych.

CELE I ZADANIA

Zasadniczym sposobem przerzutu jest metoda powietrzna, czyli zrzut żołnierzy, sprzętu i środków materiałowych niezbędnych do wykonania zadania z wykorzystaniem spadochronów. Jednak siły, sprzęt oraz środki materiałowe mogą być dostarczone w rejon działania na pokładach lądujących statków powietrznych (po wcześniejszym opanowaniu lotnisk lub lądowisk), jak również drogą wodną (jeśli jest taka możliwość). Liczba środków transportu powietrznego oraz sposób przerzutu są związane z otrzymanym zadaniem, warunkami terenowymi w rejonie lądowania oraz składem i wyposażeniem desantowanych pododdziałów.

Zadania wojsk powietrznodesantowych wynikają z ich przeznaczenia oraz możliwości bojowych[8]. Dzielą się na zasadnicze, odwodowe (wsparcia) oraz inne niż wojenne (rys. 2).

Do zadań zasadniczych można zaliczyć takie, jak:

- niszczenie ważnych obiektów (stanowisk dowodzenia, elementów systemów rozpoznawczo-uderzeniowych itp.);
- opanowanie i utrzymanie do czasu podejścia wojsk własnych:

– obiektów/węzłów drogowo-mostowych dogodnych do przepraw,

– odcinków i obiektów dogodnych do przepraw przez szerokie przeszkody wodne,

– przełęczy górskich, cieśnin i innych newralgicznych rejonów,

– lotnisk i lądowisk;

7 L. Elak, *Podstawy działań taktycznych,* AON, Warszawa 2013, s. 565.
8 *Regulamin działań wojsk*..., op.cit., s. 159.

• izolowanie rejonu starcia od dopływu kolejnych sił przeciwnika i dowozu środków materiałowych;

• zamknięcie, wspólnie z wojskami nacierającymi od czoła, pierścienia okrążenia wokół zgrupowania przeciwnika;

• wzmocnienie sił będących w okrążeniu bądź stworzenie warunków do wyjścia z okrążenia i połączenia się z siłami głównymi lub przejścia do działań nieregularnych;

• osłona (obrona) samodzielnych kierunków i rejonów, luk i otwartych skrzydeł wojsk własnych.

Do wsparcia bezpośredniego własnych wojsk, które znalazły się w niekorzystnej sytuacji taktycznej (gdy czas reakcji wyklucza użycie innych rodzajów wojsk), mogą być realizowane takie zadania, jak[9]:

– prowadzenie działań opóźniających;

– blokowanie przeciwnika na skrzydłach nacierającego zgrupowania wojsk własnych;

– wzmocnienie sił znajdujących się w okrążeniu;

– zamykanie otwartych skrzydeł i luk.

Do zadań o charakterze innym niż wojenne, których realizacja wiąże się z koniecznością dostarczenia sił i środków metodą zrzutu spadochronowego, zalicza się:

– ewakuację zagrożonych osób z rejonów, w których wybuchły niepokoje społeczne;

– udzielenie pomocy logistycznej lub medycznej;

– wsparcie innych rodzajów wojsk (np.: inżynieryjnych, chemicznych) podczas prowadzenia przez nie działań humanitarnych;

– demonstrację siły;

– rozdzielenie spornych stron lub prewencyjne rozmieszczenie sił pokojowych.

Biorąc pod uwagę zadania, które mogą wykonywać pododdziały powietrznodesantowe, należy zauważyć, że siły te muszą być tak wyszkolone, by w niekorzystnej sytuacji taktycznej przejść do prowadzenia działań nieregularnych. W tym przypadku zakres ich zadań będzie tylko niewielką cząstką całokształtu podejmowanych przedsięwzięć, których celem będzie utrzymanie ciągłości walki zbrojnej oraz stworzenie warunków do organizowania grup oporu i oddziałów partyzanckich z zadaniem podjęcia przez nie działań.

Kolejnym aspektem jest przygotowanie pododdziałów powietrznodesantowych do walki w okrążeniu. Jest to szczególny rodzaj działań taktycznych, niezwykle wymagający ze względu na swoją specyfikę. Okrążone pododdziały mogą być bowiem atakowane z różnych stron, a wsparcie z zewnątrz będzie ograniczone lub zupełnie niemożliwe. Niewykluczone przy tym, że pododdziały te będą w dużej mierze narażone na zmasowany ogień artylerii oraz ataki z powietrza. Ponadto okrążone zgrupowania mogą utracić zdolność do pozyskiwania aktualnych danych z rozpoznania[10]. Należy przy tym pamiętać, że walka w okrążeniu polega na izolowaniu określonego zgrupowania od bazy zaopatrzenia i pozostałych sił[11]. Wówczas celem okrążonych pododdziałów będzie obrona opanowanego obiektu, a także opóźnianie podejścia kolejnych sił przeciwnika. Dlatego główny wysiłek należy skupić na niedopuszczeniu do rozcięcia ugrupowania oraz na stworzeniu warunków do wyjścia z okrążenia lub utrzymywania pozycji do czasu połączenia się z siłami głównymi.

Rozpatrując czynnik ludzki, należy zauważyć, że to właśnie żołnierze pododdziałów powietrznodesantowych muszą opanować w trakcie szkolenia ponadprzeciętne umiejętności ogniowe, charakteryzować się odpowiednim poziomem sprawności fizycznej (wyższe normy testów sprawnościowych) oraz określonymi predyspozycjami psychicznymi (testy psychologiczne). Ponadto zdolnością do samodzielnego działania oraz przetrwania w warunkach izolacji[12]. Dodatkowo wyszkolenie żołnierzy spadochroniarzy ściśle koreluje z realizacją procesu zabezpieczenia logistycznego. Ich limity amunicji, żywności i innych środków materiałowych zależą od tego, ile są w stanie zabrać i swobodnie oddać skok. Żołnierz musi być zatem tak wyszkolony, by każdy z dysponowanych przez niego środków został użyty zgodnie z przeznaczeniem i adekwatnie do zaistniałej sytuacji.

Podsumowując, należy stwierdzić, że zadania pododdziałów powietrznodesantowych wymagają odmiennego, bardziej szczegółowego planowania z uwzględnieniem czynników, które w innych rodzajach wojsk wydają się nieistotne lub mają znaczenie marginalne.

WNIOSKI

O sukcesie na polu walki stanowi niewątpliwie zdolność do szybkiego ześrodkowania sił i środków tam, gdzie z punktu widzenia własnych celów jest to najbardziej korzystne. Osiągnięcie takiego stanu jest możliwe dzięki odpowiedniej ruchliwości zgrupowań zadaniowych przekształconej w manewr na obszarze prowadzonych działań. Jest to zasadniczy czynnik, który wpływa na sposoby wykorzystania pododdziałów powietrznodesantowych w połączeniu z odpowiednią organizacją oraz wyszkoleniem. Ograniczenia, a także warunki, które muszą zostać spełnione, decydują o tym, czy użycie tych sił jest możliwe. W momencie osiągnięcia pożądanego stanu następuje ich pełna aktywacja oraz zostaje sformułowane zadanie uwzględniające zarówno możliwości przerzutu, jak i prowadzenia walki po wylądowaniu w głębi ugrupowania przeciwnika. Zatem wyszkolenie oraz przygotowanie stanów osobowych, a także odpowiedni proces planistyczny wydają się być właściwą receptą na osiągnięcie sukcesu w walce. ■

9 *SPO 001.00/6BPD/wersja01*, Kraków 2010.

10 L. Elak, *Podstawy działań...*, op.cit., s. 218.

11 *Leksykon wiedzy wojskowej...*, op.cit., s. 274.

12 T. Piekarski, *Wojska powietrznodesantowe wciąż potrzebne*, „Przegląd Wojsk Lądowych" 2013 nr 3, s. 1.

Natarcie pododdziałów czołgów w terenie **zurbanizowanym**

TEREN, POGODA, WARUNKI ATMOSFERYCZNE ORAZ KLIMATYCZNE ISTOTNIE WPŁYWAJĄ NA PROWADZENIE DZIAŁAŃ BOJOWYCH.

mjr dypl. SZRP Grzegorz Schabowski

Autor jest asystentem w Zakładzie Działań Wojsk Lądowych i OT Instytutu Taktyki Wydziału Wojskowego ASzWoj.

Ważnym czynnikiem, zarówno w planowaniu i organizowaniu działań, jak i w trakcie prowadzenia walki, jest ocena warunków środowiska. Uwzględnienie środowiska walki i terenu, w którym będzie ona toczona, jest jednym z czynników, który umożliwi osiągnięcie przewagi. Uwarunkowania te, czyli klimat, teren, pora roku, doby i inne, pozwoliły wyodrębnić specyficzne warunki środowiskowe, które przez swoją odmienność bezpośrednio lub pośrednio wpływają na sposób użycia wojsk[1]. Specyficzne właściwości obszaru zabudowanego oraz jego ciągły rozwój i zmiany, które w nim następują, wpływają na wykreowanie jego charakterystycznych cech. W związku z tym powstają nowe, odmienne czynniki, które oddziałują na prowadzenie w nim działań bojowych.

SPECYFIKA DZIAŁAŃ

Wyodrębnienie specyficznych środowisk walki pozwala dowódcom na wyszkolenie i przygotowanie pododdziałów do prowadzenia przyszłych działań w danym środowisku. Do specyficznych środowisk walki zaliczamy teren[2]: zurbanizowany, lesisty (lesisto-jeziorny), górzysty, pustynny, wybrzeże morskie oraz warunki ograniczonej widoczności, a także ekstremalnie gorące i niskie temperatury.

O czystej postaci specyficznego środowiska walki będziemy mówić rzadko, ponieważ praktycznie żadne z nich nie występuje w jednolitej formie. Zatem istotą specyficznych środowisk walki jest wzajemne przenikanie się, dlatego też działania bojowe będą z reguły odbywały się w warunkach jednoczesnego wpływu kilku środowisk na prowadzoną walkę.

Specyficzne warunki charakteryzują się swoistymi czynnikami środowiskowymi o jednolitych i niezmiennych cechach[3]. W związku z tym prowadzenie w nich działań, a tym bardziej w terenie zurbanizowanym, nie powinno być czymś nowym czy też szczególnym i wyjątkowym dla zgrupowań pododdziałów wojsk lądowych, w tym również pododdziałów czołgów. Należy też zaznaczyć, że walka w specyficznych środowiskach będzie prowadzona z zasady na oddzielnych kierunkach, często od siebie oddalonych. Dlatego też tworzenie zgrupowań taktycznych czy grup zadaniowych powinno być w nich normą.

Jednym ze specyficznych środowisk walki jest teren zurbanizowany. Jego infrastruktura oraz obecność lud-

1 M. Kubiński [red.], *Taktyka wojsk lądowych. Podręcznik,* AON, Warszawa 2010, s. 362.
2 *Regulamin działań wojsk lądowych,* DWLąd, Warszawa 2008, s. 173.
3 M. Kubiński [red.], *Taktyka wojsk...,* op.cit., s. 363.

Powodzenie w walce można uzyskać dzięki właściwemu oraz umiejętnemu wykorzystaniu walorów pododdziałów czołgów. Nie należy przy tym zapominać o ich ubezpieczaniu, by nie stały się łatwym celem dla żołnierzy przeciwnika, wyposażonych w przenośne środki przeciwpancerne.

LESZEK KUJAWSKI

ności cywilnej istotnie będą wpływać na sposób oraz przebieg prowadzonych działań. Ponadto będzie on wymagać szczególnej analizy pod kątem przyszłych działań bojowych. Dotyczy to zwłaszcza pododdziałów czołgów, których działanie może być dość utrudnione przez różne specyficzne czynniki właściwe dla tego terenu. Jednym z czynników jest typ zabudowy, określany przez jej gęstość, charakter budynków i ich konstrukcję. To od niej zależy ilość oraz rodzaj wojsk planowanych do użycia, jak również sposób ich wsparcia i zabezpieczenia, a także sposób zaopatrywania ludności cywilnej w podstawowe środki do życia. W miastach wyróżnia się zabudowę[4]:

– zwartą (budynki są rozstawione bardzo blisko siebie, prawie bez odstępów),

– gęstą (niewielkie odstępy między nimi),

– luźną (budynki znajdują się w pewnym oddaleniu od siebie),

– rozproszoną (znaczna odległość między budynkami).

Stopień zurbanizowania naszego kraju powoduje, że na około 65% jego obszaru prowadzenie skutecznej obserwacji i ognia będzie możliwe na odległość 500–600 m, a w 10–15% do 2 km[5].

Teren zurbanizowany to wycinek obszaru powierzchni ziemi, którego ponad 50% pokrycia stanowią miasta, osiedla typu miejskiego (mają charakter miejski), obiekty przemysłowe oraz występująca w nich infrastruktura[6]. Rozrastając się, zwiększa on swoje znaczenie w sposobie prowadzenia działań, szczególnie w trakcie natarcia. Oprócz tego działania w terenie zurbanizowanym charakteryzują się[7]:

– ograniczonym polem ostrzału i obserwacji;

– korzystnymi warunkami ubezpieczenia, maskowania wojsk i sprzętu, co zwiększa trudności w ocenie sił;

– obniżonymi możliwościami wykonywania manewru, w szczególności przez pododdziały czołgów, zmechanizowane oraz zmotoryzowane;

– większą możliwością przenikania i wykonywania obejść przez wojska obu walczących stron (tym samym zwiększa się czynnik zaskoczenia);

– wymuszoną walką w obszarach o ograniczonych możliwościach pokonywania ich przez środki walki,

4 L. Elak, *Taktyczne aspekty terenu w walce*, AON, Warszawa 2013, s. 134.

5 Ibidem, s. 41.

6 *Regulamin działań wojsk...,* op.cit., s. 173.

7 Ibidem, s. 175–176.

co zdecydowanie wpływa na możliwości wykorzystania czołgów, BWP oraz KTO w bezpośredniej styczności z przeciwnikiem;

– koniecznością prowadzenia walki na trzech poziomach: na poziomie ulicy, ponad ziemią (w budynkach i na dachach budynków) oraz pod ziemią (w piwnicach, ciągach kanalizacyjnych i w systemach podziemnych przejść i tuneli);

– walką prowadzoną w bezpośredniej styczności, co wpływa na większą podatność pojazdów na zwalczanie ich z bliskiej odległości;

– zwiększona wrażliwość pojazdów na atak z bliskiej odległości;

– zdecentralizowane użycie wielu rodzajów wojsk, w tym szczególnie czołgów i artylerii strzelającej na wprost;

– trudności w dowodzeniu i utrzymaniu łączności w związku z decentralizacją dowodzenia;

– wykorzystanie większej liczby spieszonych pododdziałów;

– zwiększone możliwości przenikania i obejścia;

– duże zużycie amunicji i środków bojowych;

PROWADZENIE DZIAŁAŃ BOJOWYCH W TERENIE CZOŁGÓW NALEŻY DO NAJTRUDNIEJSZYCH,

– obecnością ludności cywilnej oraz obiektów chronionych prawem międzynarodowym, co znacznie może ograniczać działania wojsk;

– dużym zużyciem amunicji i innych środków walki;

– trudnościami w dowodzeniu, kierowaniu i łączności, dlatego też dowodzenie musi być zdecentralizowane.

Zasadniczym wyznacznikiem, który odróżnia teren zurbanizowany od pozostałych środowisk walki, jest to, że miasta bezustannie się zmieniają. Stawiane są nowe budynki, powstają centra handlowe, a to powoduje, że teren ten powiększa swoją objętość, co jest istotne w momencie planowania działań w tym specyficznym środowisku[8].

UWARUNKOWANIA

Uwzględniając charakterystykę tego środowiska walki, już w trakcie planowania działań bojowych należy mieć na uwadze jego ograniczenia i umieć je pokonać. W związku z tym skuteczność powodzenia w walce będzie uzależniona od takich czynników, jak:

– posiadanie rzetelnych informacji o układzie topograficznym terenu zurbanizowanego i możliwościach strony przeciwnej;

– ograniczone pole ostrzału i obserwacji;

– odpowiednie warunki do organizowania ubezpieczeń, ukrycia i maskowania sił i środków;

– obniżone możliwości manewru, szczególnie pododdziałów zmechanizowanych i czołgów;

– intensywne stosowanie broni krótkiego zasięgu i granatów ręcznych;

– walka prowadzona w kwartałach o zwartej zabudowie;

– inicjatywa i sprawność działań na najniższych szczeblach dowodzenia;

– walka prowadzona na trzech poziomach: na poziomie ulicy, ponad ziemią na dachach i w budynkach oraz pod ziemią w kanalizacjach i systemach podziemnych przejść i tuneli;

– zaangażowanie w walkach w rejonie zabudowanym z reguły nieproporcjonalnie dużej ilości wojsk;

– obecność ludności cywilnej[9].

Częste zmiany sytuacji, trudności w orientacji w terenie oraz decentralizacja dowodzenia mogą istotnie utrudnić prowadzenie działań bojowych. Podobnie możliwość zaskoczenia stawia bardzo wysokie wymagania przed żołnierzami, a przede wszystkim przed dowódcami. Niejednokrotnie inicjatywa i pomysłowość już na najniższych szczeblach organizacyjnych może się okazać kluczowym wyznacznikiem sukcesu w tym środowisku walki[10].

Odpowiednie wykorzystanie terenu może się przełożyć na zapewnienie ochrony i obrony, obserwacji oraz przeciwdziałania rażeniu ogniowemu. Poza tym może ułatwić wykonywanie manewru sprzętem, w tym czołgami. Szczególne warunki terenu zurbanizowanego powodują, że w trakcie planowania walki należy uwzględnić następujące kwestie[11]:

– stanowiska ogniowe muszą być starannie wybrane, by uniemożliwić przeciwnikowi zaskoczenie w warunkach ograniczonej widoczności i dostępności pól ostrzału;

– nie tylko stanowiska ogniowe, lecz także siły i zamiary przeciwnika są trudne do wykrycia (oceny);

– manewr i ruch będą poważnie ograniczone z uwagi na zniszczone budynki, które zapewnią obrońcy wiele ukryć, a atakujący nie będzie dokładnie znał jego stanowisk oporu. Wolniejsze będzie tempo walki;

– szeroko będą stosowane granaty, mogą wystąpić trudności w prowadzeniu ognia z wozów bojowych;

8 G. Sobolewski, *Działania zgrupowań wojsk lądowych w terenie zabudowanym,* AON, Warszawa 2008, s. 73.

9 M. Huzarski [red.], *Taktyka ogólna wojsk lądowych. Podręcznik,* AON, Warszawa 2000, s. 215–216.

10 Ibidem, s. 112.

11 A. Bujak, *Środowisko a działania bojowe na terytorium Polski,* Toruń 2000, s. 45.

– wsparcie ogniowe będzie trudne do osiągnięcia, gdyż środki ognia pośredniego będą miały ograniczone zastosowanie;

– walka uliczna jest wyczerpująca zarówno fizycznie, jak i psychicznie, powodzenie jest mierzone niewielkimi zdobyczami terenowymi, a utrzymanie efektywności bojowej wymaga częstego luzowania pododdziałów biorących w niej udział.

Niejednokrotnie teren zurbanizowany ze specyfiką prowadzonych w nim działań może wyrównać szanse walczących stron bez względu na różnice w sprzęcie i jego zaawansowaniu technologicznym. Użycie czołgów będzie ograniczone praktycznie do dróg i ulic. Poza tym teren ten powoduje, że prowadzenie działań dużymi, zwartymi pododdziałami jest bezzasadne. Wymusza on na dowódcach tworzenie mniejszych grup zadaniowych lub szturmowych o różnorodnej strukturze. Oprócz tego należy się liczyć z dużymi stratami zarówno wojsk, jak i wśród niewysiedlonej ludności cywilnej oraz znacznymi zniszczeniami w infrastrukturze miejskiej. Duży wpływ na prowadzenie działań będą też miały dobra kultury i obiekty prawnie chronione zapisami międzynarodowego prawa humanitarnego konfliktów zbrojnych. Niekiedy obiekty te mogą być wyłączone z prowadzenia w nich lub w ich obrębie jakichkolwiek działań bojowych, co może utrudnić wykonanie zadania. W związku z tym walka będzie skupiona głównie na pojedynczych, niekiedy bezpośrednich starciach mniejszych grup czy zgrupowań.

NATARCIE

Prowadzenie działań bojowych w terenie zurbanizowanym przez pododdziały czołgów, a przede wszystkim natarcia, należy do jednych z najtrudniejszych, gdyż sprzyja on działaniom obronnym. Cechą charakterystyczną natarcia będzie utrudnione przemieszczanie oraz ograniczenia w manewrze pododdziałami, w tym czołgów. Utrudnione też będzie prowadzenie rozpoznania. Niższa będzie również efektywność użycia środków radiowych.

Pododdziały czołgów mogą służyć przede wszystkim do niszczenia stanowisk ogniowych przeciwnika znajdujących się wewnątrz budynków, niszczenia zapór czy też barykad oraz do blokowania ogniem przeciwnika. Poza tym można ich użyć do ograniczania ogniem manewru przeciwnika, zabezpieczenia skrzydeł wojsk własnych, jak również do wykonywania otworów w budynkach, by umożliwić pododdziałom piechoty wtargnięcie do nich i ich opanowanie.

W związku z tym pododdziały czołgów, będąc w składzie grup szturmowych, są w stanie wykorzystać właściwości terenu zurbanizowanego. Skuteczność natarcia, oprócz rozpoznania terenu oraz wsparcia pododdziałów czołgów przez piechotę, jest uzależniona od: uzyskania zaskoczenia, utrzymania zakładanego tempa działań, spotęgowania uderzenia z różnych stron, prostoty planowania i działania oraz zdecydowanej realizacji postawionego zadania[12].

Czołgi są bardzo mobilnym środkiem walki, który pozwala na szybkie przemieszczenie się, wykonanie rajdu, wypadu czy też szybką zmianę stanowiska ogniowego podczas prowadzenia ognia. Poza tym bezpieczeństwo załóg raczej jest traktowane priorytetowo, a to właśnie czołgi zapewniają najlepszą dla nich ochronę. Ponadto pancerz gwarantuje odporność na większość stosowanych współcześnie środków walki oraz wpływa na bezpieczeństwo załogi.

Z pewnością pododdziały czołgów nie będą wykonywały zadań samodzielnie, będą one elementem grup lub oddziałów szturmowych, by wesprzeć je ogniem w opanowywaniu poszczególnych obiektów.

Użycie czołgów i wykorzystanie ich cech, np. siły ognia czy mobilności, jest gwarantem osiągnięcia sukcesu. Można się zastanawiać nad tym, że być może ich użycie w coraz to bardziej zabudowanych obszarach nie jest zasadne. Zabudowa przecież ogranicza pole widzenia, pozwalając przeciwnikowi podejść dość blisko do czołgu będąc niezauważonym. Konflikty zbrojne, zwłaszcza toczone w XXI wieku, dostarczyły licznych dowodów na przydatność czołgów w analizowanym terenie. Warunkiem koniecznym jest niewątpliwie użycie pododdziałów czołgów do walki ze środkami opancerzonymi przeciwnika bądź jego środkami przeciwpancernymi. Ich zastosowanie wywiera efekt psychologiczny zarówno u wojsk przeciwnika, jak i własnych. Przekłada się to na pożądany efekt, czyli opanowanie obiektu ataku. Wysoka manewrowość czołgów, ich siła ognia, którą wspierają piechotę, pancerz oraz zamontowane w nich systemy dowodzenia i łączności, zapewnią zarówno ciągłość dowodzenia, jak i mniejsze straty wśród spieszonych pododdziałów. Doświadczenia z konfliktów zbrojnych prowadzonych w terenie zurbanizowanym wskazują, że powodzenie w walce można uzyskać dzięki właściwemu oraz umiejętnemu wykorzystaniu walorów pododdziałów czołgów. Nie należy przy tym zapominać o ich ubezpieczaniu, by nie stały się łatwym celem dla żołnierzy przeciwnika wyposażonych w przenośne środki przeciwpancerne. ■

ZURBANIZOWANYM PRZEZ PODODDZIAŁY GDYŻ SPRZYJA ON DZIAŁANIOM OBRONNYM

12 *Urban Operations FM 3-06*, Headquarters Department of the Army, October 2006, s. 129 (par. 1-7).

Czynniki walki zbrojnej a wybrzeże morskie

DO POKONANIA PRZECIWNIKA OPRÓCZ ŚRODKÓW WALKI POTRZEBNA JEST WIEDZA ORAZ UMIEJĘTNOŚĆ SKUTECZNEGO JEJ WYKORZYSTANIA W TRAKCIE DZIAŁAŃ BOJOWYCH.

mjr dypl. SZRP mgr inż. Maciej Trepiak

Autor jest zastępcą dowódcy – szefem sztabu batalionu czołgów w 34 Brygadzie Kawalerii Pancernej.

Analizując współczesne konflikty, można zauważyć, że są prowadzone w różnych środowiskach. Często są one określane jako specyficzne ze względu na dominujący charakter jednego z nich. Dane środowisko w znaczący sposób wpływa na prowadzenie w nim działań, zatem oddziałuje również na czynniki walki zbrojnej. Dlatego też warto przeanalizować to zagadnienie. Znając wady i zalety każdego środowiska, można je wykorzystać w umiejętny sposób, co przyczyni się bezpośrednio do odniesienia sukcesu w walce.

CZYNNIKI WALKI ZBROJNEJ

By je określić, należy w pierwszej kolejności odnieść się do tego, czym jest walka zbrojna. *Regulamin działań wojsk lądowych* definiuje ją następująco: *walka zbrojna to rodzaj walki polegający na prowadzeniu działań, których celem jest zniszczenie (obezwładnienie) przeciwnika przy wykorzystaniu broni*[1]. Kolejną definicję walki zbrojnej zawiera opracowanie pt. *Sztuka wojenna* pod redakcją Andrzeja Polaka i Jacka Joniaka: *walka zbrojna to zjawisko, którego istota sprowadza się do bezpośredniego starcia zgrupowań wojsk, to wzajemne destrukcyjne oddziaływanie za pomocą posiadanych środków rażenia, to przede wszystkim fizyczne niszczenie, a także psychologiczne obezwładnienie przeciwnika jako przeszkody na drodze do celu*[2].

Należy przy tym wspomnieć, że walka zbrojna może być prowadzona na każdym poziomie, to znaczy: strategicznym, operacyjnym i taktycznym.

Odnosząc się do jej celu, należy zauważyć, że jest nim pokonanie przeciwnika. O ile w swojej istocie nie zmienił się on na przestrzeni lat, o tyle sposób prowadzenia walki oraz stosowane środki wciąż ewoluują.

Rozpatrując walkę zbrojną, trzeba rozważyć jej czynniki, gdyż to one decydują o skutkach każdego starcia.

Czynniki walki zbrojnej są *istotnymi elementami mającymi znaczenie w osiąganiu dezintegracji i destrukcji możliwości zaczepnych bądź obronnych przeciwnika*[3] (rys.). W procesie niszczenia rozumiane są jako coś, co wywołuje i warunkuje określony skutek oraz rozstrzyga o jego osiągnięciu. Tym, co powoduje określony skutek, jest informacja. Tym, co warunkuje zamierzony skutek, jest wszelki ruch. Natomiast tym, co rozstrzyga o osiągnięciu oczekiwanego skutku, jest rażenie[4].

W literaturze przedmiotu przedstawiono podział czynników walki zbrojnej na dwa rodzaje: elementarne (podstawowe) i syntetyczne (złożone).

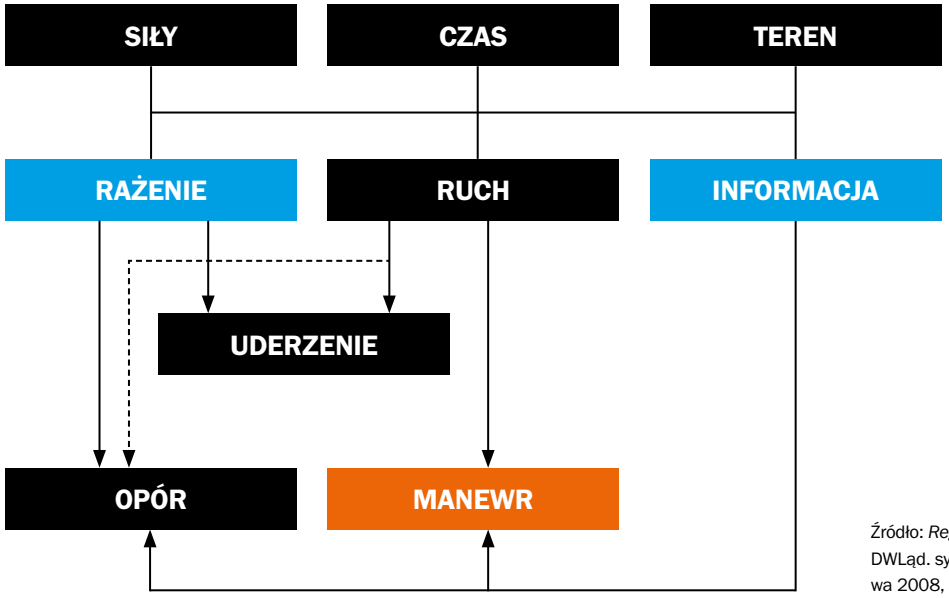
Do podstawowych czynników walki zbrojnej zalicza się: rażenie, ruch i informację. Ich znaczenie sprowadza się do skutecznego zwalczania broniącego się lub nacierającego przeciwnika. Uwidacz-

1 *Regulamin działań wojsk lądowych*, DWLąd. sygn. Wewn. 115/2008, Warszawa 2008, s. 21.
2 *Sztuka wojenna*, red. A. Polak, J. Joniak, AON, Warszawa 2014, s. 201.
3 *Regulamin działań...*, op.cit., s. 22.
4 *Sztuka wojenna...*, op.cit., s. 202.

Działania prowadzone na wybrzeżu morskim dzielą się na dwa rodzaje: obronę wybrzeża oraz działania desantowe podejmowane z morza.

TOMASZ MIELCZAREK/7 BOW

RYS. CZYNNIKI WALKI ZBROJNEJ



Źródło: *Regulamin działań wojsk lądowych*, DWLąd. sygn. Wewn. 115/2008, Warszawa 2008, s. 22.

nia się to w ponoszonych przez niego stratach oraz niezrealizowaniu celu działania[5].

Rażenie, ruch i informacja odnoszą się do czynników operacyjnych, tzn. do terenu (obszaru) podejmowanych działań, użytych sił, a także czasu ich prowadzenia.

Spójne oddziaływanie na przeciwnika podstawowych czynników walki zbrojnej oraz ich synteza (manewr, uderzenie oraz opór) prowadzą do osiągnięcia celu walki.

Rażenie polega na bezpośrednim fizycznym, psychicznym i informacyjnym oddziaływaniu na siły i środki przeciwnika w stopniu koniecznym do osiągnięcia celu. Jest nim obniżenie jego potencjału bojowego i zdolności bojowej oraz zdezorganizowanie działań, tym samym zapewnienie wojskom własnym sprzyjających warunków do wykonania postawionych zadań[6]. Skuteczność rażenia odnosi się do sił, które będą oddziaływać na przeciwnika, oraz do obiektów i czasu oddziaływania, a także do terenu, w którym działania będą prowadzone. Teren może wpłynąć znacząco na efektywność rażenia. Może on ją zwiększać bądź zmniejszać.

W trakcie oddziaływania na przeciwnika należy określić cel do osiągnięcia. Może nim być całkowite zniszczenie jego sił bądź czasowe obezwładnienie przez wyłączenie z walki określonego przez dowódcę elementu ugrupowania bojowego. Trzeba również określić obiekt oddziaływania. Informacja ta pozwoli na dobór odpowiedniej formy rażenia. *Podstawową formą rażenia jest ogień, wyrażający się w oddziaływaniu na przeciwnika różnymi środkami ogniowymi. Szczególnymi formami oddziaływania są inżynieryjne środki rażenia, rażenie elektroniczne i oddziaływanie psychologiczne*[7].

Ruch to wszelkie przesunięcia i zmiany rozmieszczenia sił i środków. Najważniejszymi jego wskaźnikami są odległość i czas przesunięcia oraz ich iloraz, czyli prędkość lub tempo działania[8].

Ruch jest obecny na wszystkich etapach przygotowania i prowadzenia walki. Jest kojarzony z rażeniem lub informacją. Przybiera wówczas formę uderzenia lub manewru i staje się czynnikiem złożonym. Trzeba pamiętać, że inną formą ruchu jest przegrupowanie, które nie jest bezpośrednio związane z rażeniem, zatem i z prowadzeniem walki.

Przegrupowanie to zmiana ugrupowania, realizowana na wszystkich poziomach przygotowania i prowadzenia walki zbrojnej[9]. Do podstawowych jego determinantów należą:

– zmiana ugrupowania w celu przygotowania się do realizacji następnego zadania,

5 *Regulamin działań...*, op.cit., s. 22.
6 Ibidem.
7 Ibidem, s. 22–23.
8 Ibidem, s. 23.
9 A. Czupryński, *Przegrupowanie i manewr*, AON, Warszawa 2002, s. 9.

– brak kontaktu bojowego przeciwstawnych zgrupowań lądowych,

– możliwość stosowania we wszystkich okresach funkcjonowania państwa[10].

Ten czynnik ruchu może służyć pośrednio oraz bezpośrednio do osiągnięcia celu walki. Będzie stosowany w ramach prowadzonej operacji lub samodzielnie. Niejednokrotnie staje się narzędziem, które przyczyni się do zapobieżenia konfliktowi przez przegrupowanie wojsk w obszar prawdopodobnego wystąpienia konfliktu, by uniemożliwić koncentrację wojsk strony przeciwnej.

Informacja należy do niematerialnego elementu zespalającego pozostałe czynniki w zharmonizowaną całość danego rodzaju działań bojowych. W tej funkcji przejawia się ona w dowodzeniu, a także ma swoje znaczenie w rozpoznaniu, maskowaniu i walce elektronicznej[11].

Do prowadzenia działań bojowych niezbędne są odpowiednie informacje zarówno o przeciwniku, jak i o terenie oraz pogodzie. Należy przy tym chronić własną informację, by przeciwnik nie poznał naszych zamiarów. *Znaczenie informacji w dążeniu do osiągnięcia celów militarnych powoduje konieczność prowadzenia działań informacyjnych jako integralnej części operacji. Działania te prowadzone są podczas działań militarnych w czasie pokoju i kryzysu oraz po zakończeniu działań wojennych*[12].

Skuteczność działań informacyjnych, a zatem osiągnięcie przewagi informacyjnej będzie się przejawiać w reakcji na sytuację w otaczającym wojska własne obszarze, w skuteczniejszym oddziaływaniu na przeciwnika oraz zmniejszeniu ryzyka zakłócenia funkcjonowania naszych sił i środków.

O znaczeniu informacji pisali również wybitni teoretycy sztuki wojennej. Jednym z nich był Sun Tzu, który wskazywał: *Poznaj siebie i poznaj wroga, dopiero wtedy Twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy Twoje zwycięstwo będzie całkowite*[13]. Również Clausewitz pisał o informacji jako o *całej wiedzy posiadanej o nieprzyjacielu i jego kraju, o podstawie własnych idei i działań*[14].

Trzeba pamiętać, że odpowiednia informacja użyta we właściwym czasie może odwrócić wynik walki. Należy również zdawać sobie sprawę, że obecnie mamy przesyt informacji, których część może być fałszywa albo niepotrzebna. Dlatego też bardzo ważne jest posiadanie odpowiedniego systemu rozpoznania, który te dane mógłby zweryfikować bądź zdobyć.

CZYNNIKI SYNTETYCZNE

Uderzenie łączy w sobie rażenie oraz ruch. Należy jednak zaznaczyć, że ruch odbywa się w stronę przeciwnika. Natomiast w trakcie uderzenia następuje jednoczesne lub kolejne rozbijanie jego zgrupowań. Sam ruch w kierunku przeciwnika jednak nie wystarczy, dodatkowo *musi on doprowadzić do zmniejszenia dystansu między własnymi siłami uderzeniowymi a przeciwnikiem. Jeśli np. przeciwnik będzie z tą samą albo z większą prędkością odstępował pola, z jaką porusza się nacierający, to do uderzenia nie dojdzie. Będzie to co najwyżej rażenie nieprzyjaciela w ruchu*[15].

Należy jednak wspomnieć, że przed masowym użyciem broni palnej uderzenie odbywało się z zastosowaniem broni białej. Natomiast wraz z rozwojem broni palnej oraz pojawieniem się bojowych wozów piechoty oraz czołgów uderzenie stało się czynnikiem bardziej złożonym. Dalszy rozwój środków rażenia zwiększył możliwość uderzenia na dużą odległość, co wyklucza konieczność bezpośredniej styczności z przeciwnikiem. Nie ma zatem potrzeby, aby wojska walczące nabierały rozpędu jako wypadkowej masy i prędkości[16].

Powstanie środków precyzyjnego rażenia wymusiło natomiast konieczność połączenia posiadanych środków walki zbrojnej w zespolone systemy tej broni – kompleksy uderzeniowe. W skład tych kompleksów wchodzą środki dowodzenia, rozpoznania, zabezpieczenia oraz rażenia[17].

Odnosząc się do celu uderzenia, należy stwierdzić, że przez uderzenie *dąży się do zmiany układu przestrzennego stron*[18].

W podsumowaniu rozważań dotyczących uderzenia należy zauważyć, że mimo rozwoju technologii jest ono związane z ruchem, który odbywa się w stronę przeciwnika i dodatkowo jest połączony z rażeniem. Można więc stwierdzić, że siła oddziaływania uderzenia będzie większa, im większa będzie dynamika własnych pododdziałów (oddziałów) oraz im większa będzie siła ich rażenia.

Opór łączy w sobie czynnik rażenia z „bezruchem" lub z ruchem wymuszonym przez uderzającego przeciwnika. Z tego względu można mówić o oporze statycznym i dynamicznym, pozycyjnym

10 Ibidem.

11 *Regulamin działań...,* op.cit., s. 24.

12 Ibidem.

13 Sun Tzu, *Sztuka wojny, czyli trzynaście rozdziałów,* s. 67.

14 *Sztuka wojenna...*, op.cit., s. 206.

15 S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993, s. 95.

16 S. Owczarek, *Czynniki walki zbrojnej z perspektywy współczesnego pola walki,* AON, Warszawa 2003, s. 51.

17 Ibidem.

18 *Sztuka wojenna...*, op.cit., s. 209.

i manewrowym. Siła oporu i jego efektywność zależą przede wszystkim od skuteczności rażenia i odporności na różnorodne oddziaływanie przeciwnika, w tym zwłaszcza na rażenie ogniowe[19]. Odnosząc się do tego czynnika, można dostrzec, że opór jest antytezą uderzenia. Przez opór dąży się bowiem do przeciwstawienia się uderzeniu i – co się z tym wiąże – uniemożliwienia zmiany układu przestrzennego walczących stron.

Porównując opór i uderzenie, można zauważyć, jak ważny jest ruch wśród złożonych czynników walki zbrojnej. Uderzenie jest silniejsze i efektywniejsze, im ruch i dynamika wojsk są większe. W ramach uderzenia dąży się wręcz do zapewnienia ruchu. Natomiast w oporze nie tylko liczy się odporność wojsk na oddziaływanie przeciwnika, lecz także przeciwstawienie się ruchowi wywołanemu przez stronę przeciwną.

Można więc założyć, że opór ma na celu zatrzymanie strony przeciwnej. Nie oznacza to, że wojska stawiające go mają być statyczne.

W oporze bardzo ważną rolę odgrywa również rzetelna informacja. Dzięki niej jest możliwe przygotowanie i prowadzenie skutecznego oporu. Przejawia się to między innymi w odpowiednim doborze sił oraz w adekwatnym przystosowaniu terenu do prowadzonych działań, co w znaczący sposób może zwiększyć jego efektywność.

Z dotychczasowych rozważań wynika, że uderzenie i opór są to przeciwieństwa. W uderzeniu chodzi o ruch połączony z ogniem, a w oporze – do jego zaniku po stronie przeciwnika. Uderzenie ma na celu zmianę układu przestrzennego walczących stron, natomiast opór – powstrzymanie wszelkich zmian w rejonie (obszarze) prowadzonych działań zbrojnych.

Manewr jest nieodłącznie związany z ruchem. W *Regulaminie działań wojsk lądowych wskazano,* że jest jego najważniejszą formą. Istota manewru polega na zorganizowanym ruchu sił oraz środków. Jest on wykonywany w określonym celu. Między innymi umożliwia przenoszenie punktu ciężkości w czasie i przestrzeni[20].

Wspomniany *Regulamin…* wyróżnia następujące formy manewru: uderzenie czołowe, pokonanie, oskrzydlenie, obejście, przenikanie, manewr mylący, demonstrację i odejście[21].

Rozpatrując formy manewru oraz jego regulaminową definicję, można stwierdzić, że jest realizowany dla poprawy własnej sytuacji względem przeciwnika. By wykonać manewr w określonej jego formie, musi być jasno określony cel do osiągnięcia. Wymienione jego formy umożliwiają zmylenie przeciwnika co do charakteru przyszłych działań własnych sił oraz zaskoczenie go przez wyjście na jego skrzydło lub tyły, co w dalszej konsekwencji może doprowadzić do jego porażki. Manewr może też służyć do poprawienia aktualnej sytuacji. Pozwala bowiem nie tylko atakować, lecz również uniknąć uderzenia przeciwnika i zniwelować niekorzystną dla własnych wojsk sytuację.

Idea manewru będzie więc odnosić się do sprawnego dowodzenia wojskami w trakcie walki z zadaniem realizacji określonego celu i oddziaływania na przeciwnika. Dlatego też podstawowymi determinantami manewru są wykonanie uderzenia lub jego uniknięcie oraz zjawisko relatywne do działania przeciwnika (dwupodmiotowe)[22].

Analizując czynniki walki zbrojnej, można zauważyć, że składową manewru jest nie tylko ruch, lecz również informacja. Dzięki precyzyjnemu obrazowi sytuacji jest możliwa odpowiednia reakcja przez dobranie stosowanej formy manewru.

Czynniki, które wpływają na manewr, A. Czupryński określił jako:

– cel manewru, czyli ustalone oddziaływanie na realnego przeciwnika,

– siły przeciwnika będące podmiotem i przedmiotem walki zbrojnej,

– siły wydzielone do realizacji manewru,

– obszar wykonania manewru,

– czas, w którym działanie nadal jest zasadne[23].

Istotnym elementem manewru jest zaskoczenie. Należy dążyć do narzucenia woli przeciwnikowi oraz postawienia go w niedogodnej dla niego sytuacji. Przez właściwe zastosowanie manewru można nie tylko spotęgować efektywność uderzenia, lecz również wzmocnić siłę oporu. Wymaga to jednak odpowiedniego wykorzystania warunków terenowych oraz mobilności wojsk, a także sprzyjającej sytuacji.

Regulamin działań wojsk lądowych wymienia specjalną formę manewru, czyli manewr ogniem, który dzieli się na ześrodkowanie, przeniesienie oraz podział ognia[24].

Chcąc uzyskać najlepsze efekty manewru, trzeba stosować następujące zasady:

– zapewnić swobodę ruchu – składową manewru,

– używać wojsk cechujących się dużą mobilnością w danym terenie,

– dążyć do dezorganizowania manewru przeciwnika,

– stosować manewr do tworzenia przewagi,

– wykorzystać manewr w celu uchylenia sił od starcia w niekorzystnych warunkach,

19 S. Koziej, *Teoria sztuki wojennej…*, op.cit., s. 95.

20 *Regulamin działań…*, op.cit., s. 23.

21 Ibidem.

22 A. Czupryński, *Przegrupowanie i manewr…*, op.cit., s. 9.

23 Ibidem, s. 55.

24 *Regulamin działań…*, op.cit., s. 24.

– manewr powinien cechować się prostotą, szybkością oraz skrytością[25].

SPECYFICZNE ŚRODOWISKO WALKI

W znaczeniu militarnym *środowisko jest najczęściej kojarzone z zasadniczym przeznaczeniem sił zbrojnych, dlatego też w terminologii wojskowej najczęściej można spotkać pojęcie środowisko pola walki (działań). W rozumieniu ogólnym środowisko pola walki oznacza obszar, na którym pododdziały, oddziały i związki taktyczne prowadzą walkę lub na który przeciwnik oddziałuje uderzeniami ogniowymi*[26].

Za *normalne środowisko walki* uznaje się *teren równinny lub pocięty, w którym wysokość względna wzniesień nie przekracza 50 m, a ich stoki są w miarę dogodne do pokonania przez czołgi, bojowe wozy piechoty i inne wojskowe pojazdy. A również wtedy, gdy pokrycie terenu, tj. zalesienia, wody (bagna) lub zwarta zabudowa, nie przekracza 50% rozpatrywanej powierzchni. Ponadto przyjmuje się, że w warunkach normalnych zasięg widoczności jest nie mniejszy niż 4 km, temperatura otoczenia waha się w granicach od -5 do +30 stopni Celsjusza, natomiast grubość pokrywy śnieżnej nie przekracza 15 cm*[27].

Natomiast *specyficzne środowisko walki* to *obszar i otoczenie, które ze względu na ukształtowanie i pokrycie terenu oraz warunki klimatyczne i pory doby w istotny sposób wpływają na możliwości przygotowania i prowadzenia walki*[28].

Do specyficznych środowisk walki zalicza się teren: zurbanizowany, lesisty, górzysty, wybrzeże morskie, warunki ograniczonej widoczności, teren pustynny i warunki ekstremalnie gorące oraz rejon panowania niskiej temperatury[29].

W artykule zostanie przeanalizowane wybrzeże morskie.

Działania prowadzone na *wybrzeżu morskim* dzielą się na dwa rodzaje: obronę wybrzeża oraz działania desantowe podejmowane z morza.

Obrona wybrzeża i obszarów morskich to zespół przedsięwzięć i działań prowadzonych przez rodzaje sił zbrojnych w celu niedopuszczenia do zbrojnego wtargnięcia na obszary morskie i wybrzeże sił przeciwnika oraz zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów i podmiotów administracji państwowej i gospodarki narodowej, rozmieszczonych na tym obszarze. Obrona wybrzeża i obszarów morskich łączy wysiłki podejmowane w sferze militarnej i pozamilitarnej[30].

Działania desantowe z morza to wydzielone i odpowiednio przygotowane siły i środki wojsk lądowych, marynarki wojennej i sił powietrznych, które wykorzystując transport morski, osłonę z powietrza oraz z morza, lądują na wybrzeżu, prowadząc walkę z przeciwnikiem aż do opanowania przyczółka i rozwinięcia działań w głąb. Prowadzone są połączonym wysiłkiem większości typów okrętów, statków, samolotów i sił desantowych, przeciwko siłom przeciwnika na wybrzeżu. Działania te są najbardziej złożonymi spośród działań połączonych. Wymagają koordynacji na każdym szczeblu między siłami desantowymi i siłami wspierającymi. Złożoność działań implikuje potrzebę szczegółowego rozważenia składu sił desantowych i wspierających oraz struktury dowodzenia tak, by zapewnić jedność dowodzenia[31].

Na podstawie analizy tych definicji można zauważyć, że do prowadzenia działań głównie desantowych potrzebne są odpowiednie jednostki marynarki wojennej, które umożliwią załadowanie sprzętu ciężkiego oraz wyładowanie go na brzeg. Jeżeli chodzi o desantowanie, Siły Zbrojne Rzeczypospolitej Polskiej nie dysponują jednostkami, które realizują *stricte* to przedsięwzięcie. Natomiast do obrony wybrzeża nie potrzeba specjalistycznego sprzętu.

ZNACZENIE CZYNNIKÓW WALKI ZBROJNEJ

W *Regulaminie działań wojsk lądowych* w odniesieniu do wybrzeża morskiego jako specyficznego środowiska walki wyróżnia się obronę wybrzeża oraz działania desantowe z morza.

Rozpatrując pierwszy ich rodzaj, czyli obronę wybrzeża, można zauważyć, że składa się z dwóch etapów:

– Obrony morskiej, która obejmuje *morskie i powietrzne operacje dokonywane w celu przeciwdziałania zagrożeniom desantem morskim przeciwnika. Prowadzona będzie przez siły morskie i powietrzne wsparte artylerią o dużym zasięgu prowadzonego ognia. Najbardziej pożądanym celem jest zniszczenie sił przeciwnika, gdy jest on na morzu. Ograniczenia w przygotowaniu i prowadzeniu działań w obronie wybrzeża to przede wszystkim możliwości prowadzenia rozpoznania. Wiadomości pozyskiwane będą tylko z rozpoznania powietrznego, radioelektronicznego* […].

– Obrony lądowej, która *powinna być skoncentrowana wokół terenu kluczowego i najbardziej prawdopodobnych rejonów desantowania, gdyż wojska organizujące obronę nie będą w stanie umocnić się na całej długości wybrzeża. Pozostałe rejony powinny być patrolowane i obserwowane.*

25 S. Koziej, *Podstawy sztuki wojennej,* AON, Warszawa 1992, s. 143.

26 Ibidem, s. 9.

27 W. Kaczmarek, *Działania taktyczne związku taktycznego (oddziału) w specyficznych środowiskach pola walki,* AON, Warszawa 1995, s. 5.

28 *Regulamin działań…*, op.cit., s. 173.

29 Ibidem.

30 Ibidem, s. 194.

31 Ibidem, s. 197.

Najbardziej pożądanym celem jest zniszczenie przeciwnika na plaży[32].

W obronie morskiej stosowanie poszczególnych czynników walki zbrojnej będzie ograniczone ze względu na środowisko: wodne oraz powietrzne. Główne czynniki, które będą stosowane w jej ramach, to informacja i rażenie.

Zdobycie *informacji* będzie odnosić się do poznania planów działania przeciwnika, określenia składu jego sił, kierunku przemieszczania oraz prawdopodobnych kierunków desantowania. Według cytowanego *Regulaminu…* informacja będzie pozyskiwana przez środki latające, morskie oraz radioelektroniczne.

Odpowiedzią na informację będzie śledzenie przeciwnika oraz jego zwalczanie, czyli rażenie. Stosując efektywnie czynnik walki zbrojnej, którym jest rażenie, uniemożliwi się przeciwnikowi wykonanie desantu morskiego. Głównym sposobem jego prowadzenia będzie rażenie ogniowe oraz elektroniczne.

W obronie lądowej użycie czynników walki zbrojnej zarówno elementarnych, jak i złożonych ma większe zastosowanie.

Informacja również w obronie lądowej odgrywa znaczącą rolę. Odpowiednio szybkie oraz wiarygodne rozpoznanie miejsca desantowania przeciwnika może wpłynąć na przebieg walki. Ważna jest także znajomość jego sprzętu. Pozwoli bowiem na określenie nie tylko miejsc desantowania ze względu na możliwości techniczne, lecz również na łatwość załadunku i przenoszenia siły żywej oraz sprzętu. Pozwoli to na lepsze przygotowanie się do obrony.

Należy jednocześnie pamiętać, że przeciwnik może prowadzić działania pozorne w celu odwrócenia uwagi drugiej strony i skupienia wysiłku w innym rejonie. Zatem w obronie wybrzeża, w szczególności w obronie lądowej, informacja jest kluczowym czynnikiem.

Kolejnym jest *rażenie*. W przypadku ustalenia miejsca desantowania oraz niepowodzenia obrony morskiej należy uniemożliwić przeciwnikowi podejście do plaży. W tym etapie należy zintensyfikować rażenie, głównie ogniowe. W razie jego wyjścia na ląd należy wykorzystywać na dużą skalę przede wszystkim środki przeciwpancerne w celu uniemożliwienia mu uchwycenia przyczółków. W trakcie bowiem walk o przyczółek siły przeciwnika będą wrażliwe na oddziaływanie ogniowe.

W kolejnym etapie, czyli w walce w głębi, odporność przeciwnika na rażenie będzie wzrastać, natomiast skuteczność rażenia przez wojska broniące się będzie się zmniejszać. Ponadto ruch będzie bardzo ograniczony dla strony broniącej się.

Prowadząc działania defensywne, dąży się do uniemożliwienia przeciwnikowi wykonania desantu. W sytuacji uzyskania przez niego powodzenia – do utrzymania bronionego wybrzeża. Ruch wojsk będzie się nasilać w razie przeniesienia walki w głąb lądu. Można stwierdzić, że intensywny ruch będzie w głównej mierze po stronie przeciwnika, który po opanowaniu przyczółków skieruje wysiłek na opanowanie obiektów w głębi lądu. W związku z tym należy skupić się na kontrmobilności.

Manewr jako złożony czynnik walki zbrojnej będzie miał ograniczone znaczenie. Wynika to z celu działania, którym jest utrzymanie nakazanego rejonu (pasa) wybrzeża. Dodatkowy wpływ na manewr mają plaże, które nie są zbyt szerokie, co utrudnia jego wykonanie. Również ten czynnik zyskuje na znaczeniu w trakcie prowadzenia walki w głębi lądu. W przypadku uchwycenia plaż oraz przeniesienia walki w głąb lądu należy wykonywać manewr oskrzydlenia. Przy tym dążyć do odcięcia przeciwnika, który naciera w głąb lądu, od elementów pozostałych na plaży. Działania te uniemożliwią mu wprowadzenie odwodów oraz wsparcie logistyczne.

Opór jest bardzo ważny w trakcie obrony lądowej przez cały okres jej prowadzenia. Obrońca musi mieć dużą odporność na oddziaływanie ogniowe przeciwnika. Ten będzie raził w pierwszym etapie z użyciem własnego lotnictwa oraz sił morskich. Po uzyskaniu powodzenia i uchwyceniu przyczółków dojdzie rażenie lądowe, które będzie w miarę postępów przybierać na znaczeniu. Słabnąć będzie za to przede wszystkim oddziaływanie marynarki wojennej.

Należy pamiętać, że składową oporu są dwa czynniki walki zbrojnej, czyli informacja oraz rażenie. Można stwierdzić, że opór w obronie wybrzeża jest najważniejszym czynnikiem złożonym. Wynika to przede wszystkim z zadania, którym jest niedopuszczenie do lądowania sił przeciwnika oraz uniemożliwienie im uchwycenia przyczółków. Zdobycie informacji odnoszącej się do rejonu desantowania przeciwnika pozwoli w miarę szybko na odpowiednie przygotowanie się do obrony. Znacząco zwiększy to odporność na oddziaływanie przeciwnika, w konsekwencji wzrośnie opór obrońcy.

Ponadto należy dążyć do tego, by opór był największy w pierwszych etapach walki. Jeśli nie uda się pokonać przeciwnika przed opanowaniem przyczółka, trzeba wykonywać uderzenia kosztem oporu.

Przechodząc do prowadzenia działań desantowych z morza, należy rozpatrzeć czynnik walki zbrojnej, który zdaje się być najistotniejszy w tych działaniach, czyli rażenie. Działania desantowe z morza wymagają użycia wojsk lądowych, marynarki wojennej oraz sił powietrznych.

Przed wyładowaniem wojsk lądowych na brzeg należy razić nie tylko marynarkę wojenną i lotnictwo przeciwnika, lecz także wojska lądowe, w szczególności artylerię dalekiego zasięgu. Rażenie będzie prowadzone w dużej mierze ogniem oraz w mniejszym stopniu radioelektronicznie. Bez skutecznego rażenia nie ma możliwości prowadzenia dalszych

32 Ibidem, s. 194.

TOMASZ MIELCZAREK/7 BOW

działań. Rażenie przez cały okres prowadzenia działań desantowych, również po opanowaniu przyczółków, nie będzie tracić na znaczeniu.

Istotnym czynnikiem jest informacja ze szczególnym uwzględnieniem wiadomości o linii brzegowej. Dane te pozwolą na określenie dogodnych miejsc do desantowania oraz sił przeciwnika, których należy się spodziewać zarówno na brzegu, jak i w głębi lądu. Istotną informacją jest położenie wojsk wspierających, głównie artylerii, oraz rejonów zagród i pól minowych.

Nie można zapominać o śledzeniu sytuacji na morzu, zwłaszcza położenia okrętów podwodnych, które stanowią poważne zagrożenie dla jednostek morskich wojsk własnych.

Prowadząc działania desantowe, ważne jest to, by ruch – przemieszczanie własnych wojsk w szczególności w etapie „morskim" – był zamaskowany. Należy dążyć do tego, by przeciwnik jak najpóźniej zorientował się o przemieszczaniu sił drugiej strony w prawdopodobne rejony desantowania.

W czasie prowadzenia działań obronnych zarówno w etapie morskim, jak i lądowym uderzenie również nie będzie traciło na znaczeniu. Wręcz przeciwnie, jego rola będzie coraz większa. Od momentu opanowania przyczółka przez przeciwnika jego znaczenie będzie wzrastać. Po jego uchwyceniu przeciwnik będzie dążył do jak najszybszego przeniesienia walki w głąb lądu. Szybkie przemieszczenie i sprawne rażenie przeciwnika to podstawa sukcesu działań obronnych.

Opór będzie ograniczony ze względu na specyfikę środowiska, w którym są prowadzone działania. Duże znaczenie będą miały możliwości sprzętu. Należy przy tym pamiętać, że obrońca nie tylko musi być odporny na rażenie ogniowe, lecz także radioelektroniczne oraz inżynieryjne. Dodatkowo opór musi być stawiany zarówno w wymiarze obrony powietrznej, jak i morskiej oraz lądowej.

Ostatnim rozpatrywanym czynnikiem jest *manewr*. Z powodu złożoności działań będzie on ograniczony ze względu na teren prowadzonych działań oraz potrzebę posiadania sił w wielu miejscach.

Preferowanymi formami manewru powinny być działania demonstracyjne oraz w mniejszym stopniu manewr mylący. Mają one wprowadzić przeciwnika w błąd odnośnie do głównego kierunku działania obrońcy oraz spowodować przesuwanie jego wysiłku w inny rejon i na inny obiekt. Pozostałe formy manewru będą wykorzystywane w ograniczonym zakresie lub wcale.

Podsumowując, należy stwierdzić, że najważniejsze w tych działaniach będą czynniki związane z rażeniem i – co za tym idzie – z obezwładnieniem przeciwnika ze względu na zaczepny charakter prowadzonych działań.

UMIEĆ WYKORZYSTAĆ

Trzeba pamiętać, że każde działania są umiejscowione w konkretnym terenie – w środowisku, które niejako definiuje sposób jego wykorzystania. W związku z tym nie tylko sama znajomość czynników walki zbrojnej wystarczy. Należy również znać wpływ środowiska na nie. To, jak będzie oddziaływać środowisko walki, czy to w sposób negatywny, czy pozytywny, pozwoli na racjonalne jego wykorzystanie.

Dodatkowo należy ocenić nie tylko teren, lecz również warunki atmosferyczne, które mogą całkowicie zmienić sposób prowadzenia działań.

Po uzyskaniu wiedzy na temat czynników oraz cech środowiska, w którym będą podejmowane działania, należy informacje te zestawić ze sobą, by móc uzyskać rzetelny obraz sytuacji oraz odpowiedź na pytanie, jakie działania mogą być prowadzone, tzn. gdzie są silne, a gdzie słabe strony. W konsekwencji posiadania tak ukierunkowanej wiedzy można zaplanować własne działania, a w trakcie walki skutecznie nimi kierować. ■

Fregaty patrolowe **typu Halifax**

KRÓLEWSKA KANADYJSKA MARYNARKA WOJENNA, CZYLI ROYAL CANADIAN NAVY (RCN) LUB MARINE ROYALE CANADIENNE (FR.), STANOWI ZNACZĄCĄ SIŁĘ W REJONIE PÓŁNOCNYCH RUBIEŻY NASZEGO GLOBU.

Autor jest analitykiem wojskowym oraz redaktorem wydania miesięcznika MW „Bandera”.

Sławomir J. Lipiecki

Trzon floty stanowi 12 zbudowanych w latach 1992–1996 średniej wielkości (około 5000 t) fregat rakietowych typu Halifax klasyfikowanych oficjalnie jako fregaty patrolowe (FFH). Są to obecnie jedyne liczące się uderzeniowe okręty nawodne RCN, gdyż ostatni z niszczycieli rakietowych należący do zmodyfikowanego typu Iroquois – HMCS „Athabaskan” (DDG 282) wycofano z eksploatacji w roku 2017. Budowa tych niezwykłych jednostek przeciągała się w nieskończoność, między innymi ze względu na niezdecydowanie zarówno analityków, jak i decydentów kanadyjskiej marynarki wojennej co do dzielności morskiej (w tym możliwości operowania na akwenach zalodzonych), uzbrojenia, systemów obserwacji technicznej czy też warunków socjalnych załóg. Projekt i budowa pochłonęły około 6,2 mld dolarów kanadyjskich (CAD), co było jednym z najkosztowniejszych programów zbrojeniowych realizowanych po wojnie. Zrezygnowano przy tym całkowicie z budowy mniejszych jednostek, takich jak na przykład korwety rakietowe, uznając je za nieperspektywiczne. Tym samym w skład współczesnej RCN wchodzi aż 12 fregat patrolowych (Halifax), cztery okręty podwodne z napędem konwencjonalnym (Victoria), 12 okrętów patrolowych (Kingston), osiem okrętów szkolnych (Orca) i żaglowiec szkolny HMCS „Oriole”. Do tego dochodzą 24 nieuzbrojone jednostki pomocnicze działające w ramach Canadian Forces Auxiliary Vessel (CFAV).

FREGATY PATROLOWE

W okresie zimnej wojny głównym zadaniem ówczesnego Maritime Command była ochrona rozległych linii komunikacyjnych głównie na Atlantyku

Halifaxy charakteryzują się dużym potencjałem do zwalczania okrętów podwodnych. W zasadzie do tych zadań są najlepiej przystosowane.

US NAVY

(wspomniane CFAV) oraz wsparcie sił morskich NATO w zwalczaniu okrętów podwodnych (ZOP). Stąd siły główne stacjonowały zwykle na wschodnim wybrzeżu Kanady (12 niszczycieli i fregat w dwóch eskadrach plus trzy okręty podwodne brytyjskiego typu Oberon oraz dwa okręty zaopatrzeniowe). Trzon Floty Pacyfiku stanowiło osiem niszczycieli (również zgrupowanych w dwóch eskadrach) należących do typów Iroquois, Annapolis, Mackenzie oraz nieco starszych – Restigouche i St. Laurent, a także okręt zaopatrzeniowy. Do tego dochodziła spora liczba jednostek przeciwminowych i patrolowych (Fort, Bay i Porte).

Po rozpadzie ZSRR strategia wymierzona w radzieckie okręty podwodne patrolujące wody Północnego Atlantyku straciła rację bytu (jak się później okazało tylko teoretycznie). Nowe zadania stawiane przed RCN wiązały się z posiadaniem okrętów wielozadaniowych, co zaowocowało między innymi modernizacją niszczycieli typu Iroquois w ramach programu *TRUMP*. Zdawano sobie również sprawę z faktu, że – mimo mniejszego zagrożenia zewnętrznego – dotychczasowe siły ZOP bardzo się zestarzały i muszą zostać jak najszybciej wyposażone w nowe okręty. W związku z tym opracowano program budowy fregat patrolowych (mimo że miały one realizować różnorodne zadania predysponujące je do miana jednostek wielozadaniowych) – CPF, czyli Canadian Patrol Frigate, w wyniku realizacji którego powstały jednostki typu Halifax (zwane potocznie typem City).

Głównym wykonawcą okrętów została stocznia Saint John Shipbuilding w Saint John (New Brunswick), która zbudowała dziewięć fregat, natomiast konstrukcję pozostałych trzech jednostek powierzono stoczni MIL Davie Shipbuilding w Lauzon (Quebec). Stępkę pod prototypową jednostkę (przyszłą HMCS Halifax FFH 330) położono 19 marca 1987 roku i nieco później, 30 kwietnia 1988 roku, nowy okręt został zwodowany. Pierwsze próby wykazały, że fregata dysponuje zbyt lekkim (w stosunku do wymagań RCN) kadłubem. Ponadto dochodziło do różnego rodzaju awarii na ogół związanych z typową chorobą wieku dziecięcego. Ostatecznie testy i próby morskie ciągnęły się do połowy 1990 roku. W wyniku wprowadzonych zmian w konstrukcji wyporność projektowana (normalna) fregaty wzrosła o około 500 ts [tona standardowa]. Poprawki były na bieżąco wprowadzane w budowanych pozostałych okrętach serii. Ostatni okręt typu Halifax (HMCS „Ottawa" FFH 341) zasilił szeregi RCN 28 września 1996 roku.

KONSTRUKCJA

Fregaty typu Halifax mają solidny, dodatkowo wzmocniony kadłub odporny na uszkodzenia i zarazem doskonale dostosowany do operowania na zalodzonym akwenie (klasa lodowa 5, czyli polarna). Dobrą dzielność morską gwarantuje korzystny stosunek długości do szerokości (1:8,2 m), duże zanurzenie – dobrą stateczność i dużą wartość parametru metacentrum GM, dzięki czemu nie było potrzeby instalowania dodatkowych stabilizatorów bocznych (oprócz standardowych stępek obłowych) i to mimo relatywnie wysokiej wolnej burty (dzięki czemu z kolei okręty dobrze trzymają się na fali, a ich pokłady nie są notorycznie zalewane przez nią). Dodatkowe zwiększenie metacentrum (punkt geometryczny jednostki pływającej) osiągnięto przez rozmieszczenie nadbudówek na jak największej powierzchni, co umożliwiło zmniejszenie ich wysokości. Z tego powodu fregaty patrolowe typu Halifax mają stosunkowo krępe sylwetki. Bardzo dobra dzielność morska oznacza, że kanadyjskie jednostki mogą prowadzić walkę nawet podczas sztormu (rys. 1).

Wraz z wejściem do służby okrętu prototypowego Royal Canadian Navy wzbogaciła się o pierwszą jednostkę zbudowaną według technologii zapewniającej obniżenie skutecznej powierzchni odbicia radiolokacyjnego (SPO). Wszystkie krawędzie (na całej długości okrętów) są zaokrąglone, a powierzchnie boczne odchylone od pionu o 5–7°. Dzięki temu fale elektromagnetyczne odbijając się od burt i nadbudówek, nie powracają do źródła ich emisji. Skuteczność radarów potencjalnego przeciwnika – podobnie jak na francuskich fregatach typu La Fayette – zredukowano również przez znaczne ograniczenie wystających elementów wyposażenia dodatkowego. Długość całkowita kadłuba wynosi 134,1 m, szerokość maksymalna na owrężu –16,4 m, zanurzenie przy wyporności normalnej – 4,9 m (7,1 m z kopułą sonaru podkilowego). Projektowana wyporność normalna 4470 ts zwiększyła się (w wyniku szeregu modernizacji) do 4795 ts. Mimo to kanadyjskie fregaty nadal dysponują pokaźnym zapasem wyporności rezerwowej. Gotowe do walki okręty wypierały początkowo 4850 ts, obecnie ich wyporność bojowa wynosi 5235 ts. Są to więc całkiem spore jednostki jak na swoją klasę, aczkolwiek – z pozoru – niedozbrojone.

Zbudowano je całkowicie ze stali specjalnej (ulepszanej cieplnie) i ciągliwej. Ich kadłuby zaprojektowano w systemie blokowym (nie mylić z typowymi modułami). Tworzy je łącznie 56 zasadniczych bloków, z których większość była już kompletnie wyposażona z chwilą montowania ich w stoczni. Dużo uwagi poświęcono przy tym zagadnieniom związanym z odpornością na uszkodzenia i przetrwaniem na polu walki. Żywotne partie kadłuba (m.in.: BCI, CSS i sekcje siłowni) ochraniane są pasem ze stali HY80. Na burtach i nadbudówkach zastosowano miejscami ochronę balistyczną w postaci płyt stalowych lub poszycia kevlarowego. Kadłub na linii wodnicy został znacznie wzmocniony stalą specjalną calowej grubości. Z kolei w części dziobowej wykorzystano dodatkowe wręgi i zastosowano wzmocnienia wzdłużne, by łatwiej kruszyć lód.

Projektowanie cyfrowe umożliwiło precyzyjne określenie kształtu każdego elementu konstrukcji, w tym między innymi miejsc penetracji kadłuba, grodzi wodoszczelnych czy też wyposażenia każdej sek-

cji. Podwodną część zabezpieczono przed oddziaływaniem fali uderzeniowej powstałej w wyniku bliskich wybuchów głowic torpedowych i min. Wnętrze kadłuba podzielono grodziami na 12 głównych sekcji szczelnych oraz pięć głównych stref przeciwpożarowych (Firezones). Grodzie sekcyjne mają zwiększoną grubość poszycia, co zapewnia także ochronę przeciwodłamkową (cytadele przykrywa od góry wzmocniony pokład górny). Z kolei poszycie grodzi lekkich jest miejscami podwójne, co również wpływa na zwiększenie ochrony biernej jednostek. Fregaty przystosowano do działania w warunkach skażenia bronią jądrową, biologiczną, chemiczną i radiologiczną (Nuclear, Biological, Chemical, Radiological – NBCR). Wszystkie ważne pomieszczenia, w tym socjalne, umieszczono wewnątrz gazoszczelnych cytadel, z których każda wchodzi w skład indywidualnej strefy kontroli uszkodzeń. Cytadele są całkowicie autonomiczne. Dysponują własnym system zasilania i dystrybucji energii (Electrical Distribution Contres – EDC), wentylacji i klimatyzacji oraz nadciśnieniowymi filtrami, a także wewnętrzną siecią łączności i systemem przeciwpożarowym. Wyposażono je ponadto w system zraszaczy zewnętrznych pełniących funkcje gaśnicze oraz utrzymujących opad radioaktywny z dala od okrętu. Poza tym jednostki mają bogate wyposażenie ratunkowe i komunikacyjne, między innymi dwie 7,8-metrowe hybrydowe łodzie motorowe RHIB (ich instalacje znajdują się na śródokręciu) oraz pneumatyczne tratwy mające (łącznie) o 50% więcej miejsc ratunkowych, niż wynosi liczebność załogi.

Napęd w systemie CODOG (COmbined Diesel Or Gas turbine) jest kombinacją turbin gazowych i silników wysokoprężnych o zapłonie samoczynnym. Składają się na niego dwie turbiny gazowe General Electric LM2500+ o mocy nominalnej 17 700 kW [23 750 shp (shaft horse power)] każda z dwustopniowymi przekładniami redukcyjnymi Royal de Schelde i silnik wysokoprężny SEMT-Pielstick 20PA6 V280 BTC (obecnie zmodyfikowany) o mocy nominalnej 6900 kW przy 900/1000 obr./min (pierwotnie 6480 kW). Pełna (trwała) łączna moc napędu wynosi 35 400 kW (47 500 shp). Przekazywana jest na dwie linie wałów zwieńczonych pędnikami w postaci pięciołopatowych śrub nastawnych o stałym skoku Escher Wyss. Prędkość marszowa (ekonomiczna) kanadyjskich okrętów wynosi 15 w. Idąc z taką prędkością, jednostki mogą pokonać aż 9500 Mm (pierwotnie – 7100 Mm) przy zapasie paliwa 480 ts, co jest wartością imponującą. Przy pełnej mocy nominalnej fregaty są w stanie rozpędzić się do prędkości ponad 34 w. (oficjalnie podawana prędkość 28 w. jest prawdopodobnie celowo zaniżona; poza tym przeprowadzone modernizacje znacznie zwiększyły osiągi napędu). Okrętowe zapasy pozwalają na długotrwałe pozostawanie w morzu bez konieczności zawijania do portu i korzystania ze wsparcia jednostek zaopatrzeniowych (autonomiczność wynosi 70 dób).

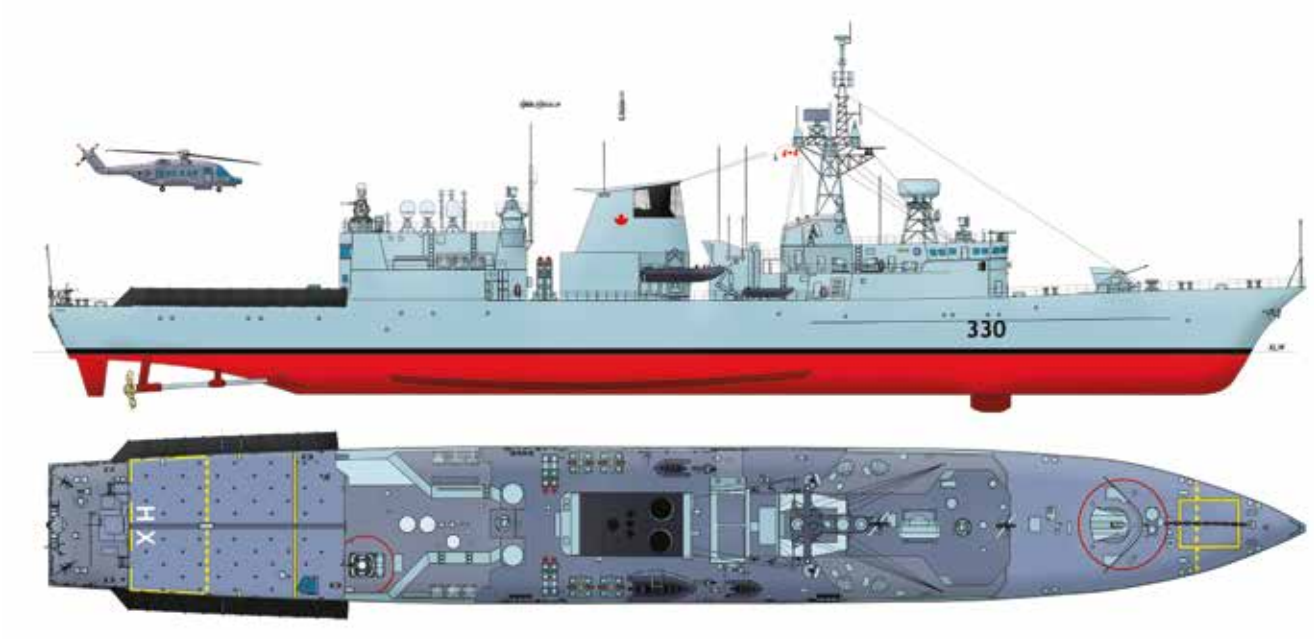
Sterowanie napędem jest całkowicie zautomatyzowane i odbywa się z poziomu centrum sterowania siłownią (CSS). Za kontrolę urządzeń napędowych, zasilania, obrony przeciwawaryjnej (OPA) itd. odpowiada obecnie nowy, w pełni zintegrowany system IPMS (Integrated Platform Management System), który – w ramach modernizacji MLU (Mild-Life Upgrade) – zastąpił oryginalny system CAE Electronics. Wszelkie jego podzespoły (wraz z konsolami i oprogramowaniem) dostarczył Lockheed Martin Canada. Tory kablowe i linie dystrybucji energii elektrycznej są podwójnie zdublowane (2 × lewa i prawa burta), co w połączeniu z niezależnymi rozdzielniami dzieli okręty na pięć całkowicie autonomicznych stref (Direct Current Zonal Electrical Distribution System – DC ZEDS). Chroni to fregaty przed utratą dużej ilości energii elektrycznej w razie awarii lub przypadkowych uszkodzeń w czasie potencjalnej walki. Samą energię dostarczają cztery agregaty trójfazowego prądu przemiennego AEG Telefunken o mocy 1650 kW (pierwotnie 850 kW) każdy (440/600 V i 60 Hz), dwa silniki elektryczne GEC o łącznej mocy nominalnej 5960 kW oraz wysokoprężny agregat awaryjny. Wszystkie elementy napędu zostały odpowiednio wyciszone i zainstalowane na specjalnych fundamentach dysponujących podkładami przeciwwibracyjnymi, a same jednostki zaopatrzono w system wyciszania Prairie-Masker. W celu lepszej kontroli pól fizycznych na GSD (głównym stanowisku dowodzenia) znalazł się system monitoringu pomiaru poziomu wibracji i pola akustycznego (Vibration and Noise Monitoring System – VIMOS Plus) wykorzystujący kombinacje akcelerometrów i hydrofonów rozmieszczonych w newralgicznych miejscach kadłuba.

Dzięki pojemnym kadłubom jednostki kanadyjskie dysponują sporą przestrzenią użytkową i to mimo gęstego zagospodarowania ich wnętrza (typ Halifax ma jeden z najwyższych współczynników wykorzystania powierzchni wewnętrznej). Umożliwiło to zapewnienie załodze dużego komfortu (pozwoliło przy tym rozplanować pomieszczenia tak, że są one niezależne dla służących na okrętach marynarzy różnej płci). Takie podejście dobrze wpływa na morale i ogólną gotowość bojową okrętów, pozwalając załodze realizować zadania podczas długotrwałych rejsów w szczególnie niesprzyjających warunkach atmosferycznych północnego Atlantyku tudzież akwenów arktycznych. Według projektu stała załoga Halifaxów składa się z 225 marynarzy (w tym 23 oficerów). Ze względu jednak na znaczne zwiększenie zakresu zadań wykonywanych przez te okręty (nie mówiąc już o częstym pełnieniu funkcji jednostek flagowych grup bojowych) oraz wzrastającą ilość nowego wyposażenia w rzeczywistości na jednostkach przebywa więcej osób. Fregaty dysponują przy tym możliwością swobodnego zakwaterowania dodatkowych 20 żołnierzy pododdziału wojsk specjalnych.

SKROMNE UZBROJENIE – CZY NA PEWNO?

Przy tak solidnie zaprojektowanych kadłubach i bogatym wyposażeniu oraz wyporności rzędu około 5000 ts koniecznością (siłą rzeczy) było poświę-

RYS. 1. FREGATA PATROLOWA TYPU HALIFAX



Opracowanie własne.

cenie jednego z parametrów technicznych jednostek. W tym wypadku padło na uzbrojenie. Niejako na wstępie zrezygnowano z bloków wyrzutni pionowych Mk 41 VLS, co automatycznie pozbawiło okręty rakiet przeciwlotniczych średniego i dalekiego zasięgu. Ograniczono się (wzorem holenderskich fregat typu Karel Doorman) do dwóch ośmiokontenerowych bloków wyrzutni Mk 48 Mod. 0 GMVLS do 16 rakiet przeciwlotniczych bliskiego zasięgu RIM-7M „Sea Sparrow" (fot. 1). Wyrzutnie ustawiono w dość nietypowy sposób, bo na śródokręciu bezpośrednio na pokładzie górnym za specjalnymi wzmocnionymi osłonami (nadburcia). Broń ta dość szybko okazała się niewystarczająca nawet do obrony własnej. W związku z tym podczas modernizacji rakiety RIM-7M zastąpiono nowoczesnymi pociskami RIM-162 ESSM (Evolved Sea Sparrow Missile), występującymi obecnie w wersji Block 2 o zwiększonym zasięgu skutecznym. ESSM pod względem osiągów pobiły na głowę wcześniej stosowane rakiety RIM-7P [na przykład prędkość odpowiada liczbie Ma równej 4 (lub większej) przy maksymalnym zasięgu około 50 km, jest to więc dystans średni]. Poza tym mają własny system naprowadzania, dzięki czemu nie ma już potrzeby stałego utrzymywania celu w wiązce radiolokacyjnej (podświetlenie celu ciągłą wiązką następuje dopiero w fazie permanentnej). Modyfikacja wyrzutni nie pozwoliła co prawda składować rakiet w quadpackach (jednostka ognia pozostała na poziomie 16 rakiet), ale umożliwiła odpalanie innych, cięższych rakiet przeciwlotniczych. Biorąc pod uwagę to, że zasięg skuteczny ESSM Block 2 znacznie przekracza 50 km, Halifaxy dysponują obecnie zdolnościami zwalczania platform powietrznych (wszystkich klas i typów poza rakietami balistycznymi) na średnim i bliskim dystansie.

Uzbrojenie okrętu uzupełnia zestaw obrony bezpośredniej CIWS kalibru 6x20 mm Mk-15 Phalanx w najnowszej wersji Block 1B Baseline 1 (oryginalnie był to Mk 15 Block 1 lub Block 1A). Block 1B ma większe możliwości „trackowania" szybkich obiektów powietrznych, jak również prowadzenia ognia do celów nawodnych (fot. 2). Jego szybkostrzelność wzrosła do 4500 pocisków na minutę. Zwiększono również zapas amunicji (zarówno w taśmach, jak i magazynie) oraz wzbogacono system kierowania ogniem o dodatkowy kanał (optyczny). Nie jest przy tym wykluczone doposażenie fregat w jeden–dwa wysokoenergetyczne zestawy laserowe, na przykład amerykańskie HELIOS. Oznacza to, że obrona bezpośrednia kanadyjskich fregat będzie spełniała najwyższe standardy światowe.

Poza tym Halifaxy mają jeszcze do dyspozycji uniwersalną armatę morską kalibru 57 mm (2,25") L/70 SAK Mk 3 (pierwotnie była to wersja Mk 2) Bofors / BAE Systems, która jest wyjątkowo skuteczna zarówno na bliskim, jak i bezpośrednim dystansie i to zarówno w niszczeniu środków napadu powietrznego, jak i małych jednostek nawodnych (fot. 3). Zainstalowano ją na dziobie w specjalnie zaprojektowanej wieży, która spełnia normy SPO. Kąt podniesienia armaty mieści się w przedziale od -10 do +77°. Maksymalny zasięg skuteczny przy strzelaniu do celów powietrznych (z użyciem pocisków P3 zaopatrzonych

w zapalniki zbliżeniowe VT) w dużej mierze zależy od ich pułapu i mieści się w przedziale od 5000 do 7600 m. Z kolei zasięg maksymalny przy strzelaniu do celów nawodnych nie przekracza 17 000 m. Przeładowywanie odbywa się automatycznie z magazynu podręcznego znajdującego się w zespole nieruchomym wieży (barbecie), który zawiera 120 pocisków (całkowita pojemność magazynu wynosi tysiąc pocisków). Armata dysponuje poczwórną linią dosyłania amunicji (po dwa dosyłacze znajdują się wewnątrz wieży po obu stronach armaty). Wykorzystywane są cztery rodzaje amunicji: PF/HE, HC/ER (masa całkowita 6,5 kg), HE i zbliżeniowa-programowalna 3P (Programmable, Pre fregmanted, Proximity fuze) o masie całkowitej 6,1 kg. Szybka reakcja, w tym zmiana kąta obrotu (57°/s) i podniesienia (44°/s), w połączeniu z dużą szybkostrzelnością wynoszącą do 220 poc./min, efektywnym systemem kierowania ogniem ze stanowiskami Signaal VM 25 STIR (obecnie Saab CEROS 200) oraz amunicją zbliżeniową jest dużą szansą na zniszczenie celu. Poza tym do armaty kalibru 57 mm będzie wkrótce dostępna nowoczesna amunicja Raytheon MAD-FIRES programu *DARPA*, służąca do zwalczania rakiet przeciwokrętowych (także w przypadku tzw. ataku saturacyjnego) wszystkich klas i typów na bliskim i bezpośrednim dystansie.

Do walki z celami nawodnymi (oprócz armaty) są używane przede wszystkim amerykańskie rakiety RGM-84 Harpoon. Na fregatach umieszczono dwie czteroprowadnicowe wyrzutnie Mk 141 zgrupowane przeciwstawnie na śródokręciu (na spardeku, tuż za przednią nadbudówką), co oznacza jednostkę ognia w liczbie ośmiu rakiet. Pociski rakietowe RGM-84 są udaną bronią przeciwokrętową średniego zasięgu (prędkość około 850 km/h, zasięg powyżej 120 km, głowica bojowa o masie 220–360 kg). Opracowano je w koncernie McDonnell Douglas jeszcze w 1971 roku i są wciąż udoskonalane (obecnie prace z tym związane prowadzi firma Boeing). W ramach modernizacji Halifaxy wyposażono w najnowszą wersję tych pocisków – RGM-84L Block 2 (w miejsce Block 1C), które – poza zwiększonymi parametrami taktyczno-technicznymi – mają także możliwość rażenia celów lądowych. Uzupełnieniem uzbrojenia rakietowego i artyleryjskiego jest sześć stanowisk ogniowych ciężkich karabinów maszynowych kalibru 12,7 mm (0,5") M2 Browning.

Halifaxy charakteryzują się dużym potencjałem do zwalczania okrętów podwodnych. W zasadzie do tych zadań są najlepiej przystosowane. Podstawę własnego uzbrojenia do ZOP stanowią obsługiwane zdalnie z pozycji bojowego centrum informacyjnego (BCI; Combat Information Center – CIC) dwie dwururowe stałe (montowane parami w tylnej nadbudówce) wyrzutnie kalibru 324 mm Mk 32 Block 9 do torped Mk 48 Mod. 5 – fot. 4 (obecnie Mk 54 MAKO LHT) oraz zrzutnie grawitacyjnych bomb głębinowych Mk 11. Magazyn torped jest w stanie pomieścić ich 24. Kanada przez lata wykorzystywała lekkie torpedy serii Mk 46, które dzięki pakietowi modernizacyjnemu występowały w nowoczesnej wersji Mod 5. Kolejny pakiet zamówiony w 2008 roku miał służyć do unowocześnienia torped do standardu najnowszych amerykańskich Mk 54 (zamówiono zarówno pakiety modernizacyjne, jak i gotowe torpedy). Torpedy Mk 54 MAKO, pierwotnie znane jako LHT (Lightweight Hybrid Torpedo), skonstruowano głównie z myślą o stosowaniu ich na płytkich wodach przybrzeżnych (także tych o małym zasoleniu) przeciwko wyjątkowo cichym okrętom podwodnym z napędem klasycznym najnowszej generacji. Wykazują się one odpornością na zakłócenia pochodzące zarówno od środków aktywnych, jak i spowodowane naturalnymi zjawiskami, między innymi odbiciami fal dźwiękowych między płytko leżącym dnem a powierzchnią wody czy też od tzw. warstw zmieszanych oraz szumami przypadkowych jednostek znajdujących się w strefie działania. W wersji hard-kill mogą również odgrywać rolę uzbrojenia przeciwtorpedowego. Ich średnica to 32,4 cm, długość 2,72 m i masa 276 kg. Głowica bojowa zawierająca zmodyfikowany ładunek PBXN-103 ma masę 43,9 kg. Zarówno prędkość biegu torpedy, jak i zasięg skuteczny oraz maksymalna głębokość operacyjna są objęte tajemnicą. Pod względem systemów wykrywania i naprowadzania na cel (Advanced Guidance & Control Section – G&C) broń ta łączy rozwiązania przyjęte w kosztownej torpedzie Mk 50 z zespołem napędowym lekkiej Mk 46. Jej konstrukcja nawiązuje do budowy ciężkiej torpedy Mk 48 ADCAP. Wykorzystano przy okazji sporo rozwiązań ze sfery cywilnej (np. cyfrową obróbkę dźwięku) oraz oprogramowania.

Pod względem ZOP fregaty typu Halifax nie dysponują żadną alternatywą dla torped i bomb głębinowych. Zastosowanie na przykład rakietotorped rodzaju VL-ASROC nie wchodzi w grę, ponieważ komory rakietowe Mk 48 Mod. 0 GMVLS uniemożliwiają użycie tego rodzaju uzbrojenia. Poza tym główną bronią do walki z okrętami podwodnymi są śmigłowce ZOP. Początkowo okręty dysponowały udanym, aczkolwiek podstarzałym już wówczas (pozostającym w służbie od 1963 roku), śmigłowcem ZOP CH-124 Sea King. Z biegiem lat Ministerstwo Obrony Kanady zamówiło 28 śmigłowców CH-148 Cyclone będących wojskowym wariantem S-92/H-92 Superhawk. Dostawa maszyn napotkała wiele trudności i w rezultacie do kwietnia 2021 roku dostarczono 22 śmigłowce. Co gorsza, jeden z nich utracono w tragicznym wypadku (zginęła cała załoga) na Morzu Jońskim (między wybrzeżem Grecji i Włoch). Maszyna pochodziła z fregaty patrolowej HMCS „Fredericton" (FFH 337).

Ponieważ maszyny serii CH-148 są znacznie większe od śmigłowców typu Sea King (masa startowa 11861 kg przy podwieszonych dwóch torpedach Mk 54 MAKO), projektanci Halifaxów (trzeba przyznać – perspektywicznie) przeznaczyli bardzo dużo miejsca na pokład lotniczy i obszerny hangar zamy-

ROYAL CANADIAN NAVY (2).

Blok wyrzutni rakiet przeciwlotniczych RIM 162 ESSM

Zestaw obrony bezpośredniej CIWS Mk-15 Phalanx

kany pojedynczą bramą segmentową. Pokład lotniczy wyposażono w dostarczony przez Indal Technologies of Ontario system ułatwiający obsługę wiropłatów RAST (Recovery, Assist, Securing and Traversing), który umożliwia operowanie śmigłowcem nawet przy stanie morza 6, przy przechyłach bocznych dochodzących do 28° i przegłębieniach dochodzących do 5° (sic!). Kanadyjskie fregaty wykorzystują także bezzałogowe statki powietrzne (BSP), takie jak na przykład AeroVironment RQ-20 Puma LE. Ta niewielka platforma może operować w powietrzu do sześciu godzin nawet w trudnych warunkach pogodowych (od -29 do 49°C, przy wietrze wiejącym z prędkością do 50 km/h i opadach deszczu ze śniegiem). Wyposażony jest m.in.: we własny system nawigacyjny, GPS, kamerę światła dziennego i nocnego oraz system śledzenia dalekiego zasięgu z anteną LRTA.

MAŁE OKRĘTY DOWODZENIA

Fregaty patrolowe typu Halifax od początku były wyposażone nie tylko w rozbudowane, wręcz awangardowe w swoim czasie systemy obserwacji technicznej, lecz także w kompleksowy system dowodzenia i zarządzania walką Lockheed Martin Canada CMS330. Znany jest on jako Saab 9LV Mk 4 lub CanACCS-9LV (przed modernizacją był to oryginalny SHINPADS – SHipboard INtegrated Processing And Display System) wspomagany przez system walki zespołowej CEC (Cooperative Engagement Capability) wraz z systemem wymiany danych taktycznych NTDS (Naval Tactical Data System) i NTCDL (Naval Tactical Common Data Link) z głównymi liniami transmisji danych Link-11 oraz wkrótce także Link-16, Link-22 i Link-1 TDL. W skład wyposażenia służącego do komunikowania się wchodzą ponadto systemy: komunikacji satelitarnej MARSAT/INMARSAT, łączności satelitarnej najnowszej generacji (pasma Ka) AN/WSC6(v) NMT SATCOM (także oryginalne z antenami OE-82) i nawigacji satelitarnej AN/WSC-3 NAVSAT oraz łączności radiowej Selex TBS (HF, VHF, UHF, SHF, EHF), opracowany zgodnie ze standardem TETRA (TErrestrial Trunked Radio). Obszerne bojowe centrum informacyjne (CIC – Combat Information Center) wraz z CeC (Combat-engagement Center) z miejsca uczyniło te jednostki idealnymi kandydatami do roli okrętów flagowych grup bojowych w zespołach międzynarodowych, co notabene stało się faktem [nawet w niedawnych (7 czerwca 2021 r.) jubileuszowych ćwiczeniach „Baltops 50” kanadyjska HMCS „Halifax” FFH 330 pełniła funkcję jednostki dowodzenia].

Podstawę systemów obserwacji technicznej stanowi wielofunkcyjny radar Thales SMART-S Mk 2 3D, który w tej roli zastąpił udaną, ale już nieco przestarzałą stację SPS-49(v)5. Wsparcie zapewnia mu oryginalny, aczkolwiek gruntownie zmodernizowany, radar obserwacji powietrznej i nawodnej Saab Sea Giraffe serii HC 150. Do kierowania ogniem artylerii jako urządzenia wsparcia stacji SAMRT-L służą najnowszej wersji stanowiska (według oryginalnej klasyfikacji są to dalocelowniki – directors) Saab CEROS-200 (dawniej SPG 503 STIR 1.8). Ponadto w ramach modernizacji dodano dwa wspomagające

3. Uniwersalna armata morska kalibru 57 mm

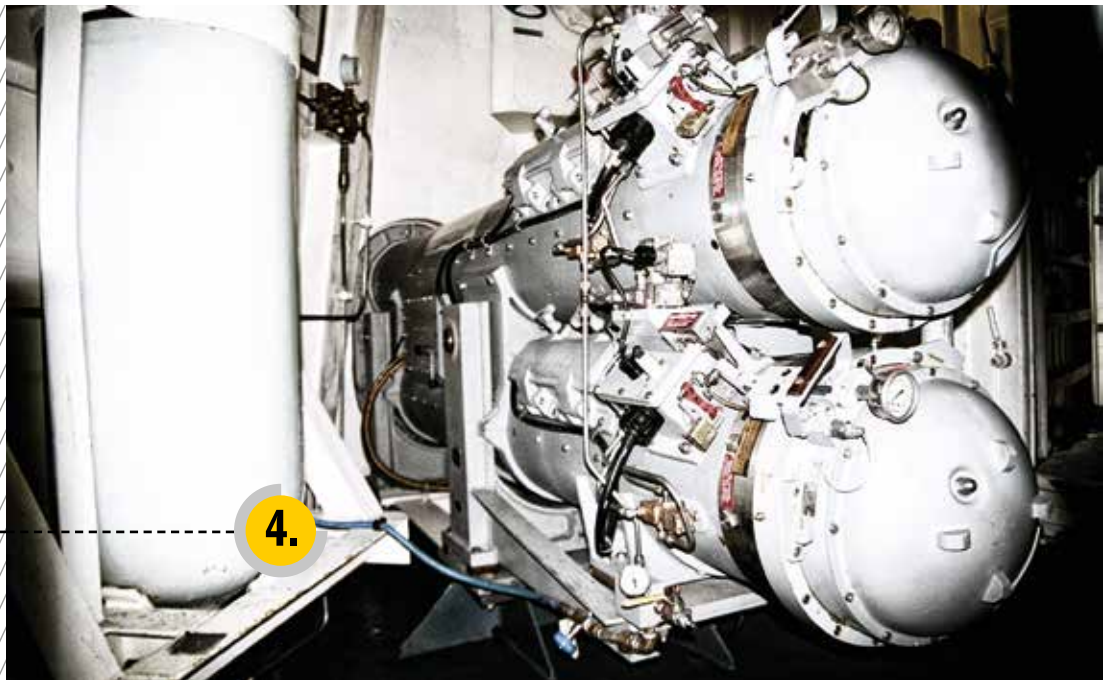
urządzenia do kierowania ogniem i śledzenia w podczerwieni z głowicą elektrooptyczną Thales „Sirius". Okręty dysponują dwoma nowoczesnymi radarami nawigacyjnymi Raytheon Anschütz systemu Pathfinder Mark II (jednym pasma „X", drugim pasma „S"). Stacje te zastąpiły starsze systemy Kelvin Hughes 1007 zdemontowane w ramach MLU (Mild-Life Upgrade). Z kolei za walkę radioelektroniczną odpowiadają zintegrowane systemy (ESCM/ECM) Ramses oraz dodany niedawno Elbit/Elistra z podsystemem identyfikacji „swój–obcy" (IFF) Mk-XII UPX-29 (v) Mod 5/S oraz z zestawami wyrzutni wielospektralnych celów pozornych Rheinmetall TKWA/MASS, czyli Multi Ammunition Softkill System (w miejsce Plessey SHIELD). Oba te systemy zastąpiły zamontowane w latach dziewięćdziesiątych ubiegłego wieku SLQ-501 i SLQ-505. Dzięki zwiększonym możliwościom aktywnego podsystemu ECM [dysponuje m.in. antenami o zmiennej mocy nadawczej na danych częstotliwościach TPO (Transmitter Power Output)] system może zakłócać stacje nawet niewielkich jednostek oraz systemy naprowadzania rakiet wystrzeliwanych z okrętów podwodnych.

Operacje lotnicze z udziałem śmigłowców, w tym działania z zakresu ZOP i wskazywania celów przez te platformy, będą kontrolowane przez najnowszą odsłonę lekkiego powietrznego wielozadaniowego systemu obrony LAMPS III (Light Airborne Multi Purpose System) z podsystemem L3 AN/SRQ-4 Hawklink. Wsparcia udziela mu system nawigacji lotniczej bliskiego zasięgu TACAN (TACtical Air Navigation), wykorzystujący fale radiowe o bardzo wysokiej częstotliwości VHF (Very High Frequency). Podstawowym jego zadaniem jest kontrolowanie działań z zakresu ZOP oraz zwalczania celów nawodnych. LAMPS III jest – podobnie jak system komunikacji i łączności satelitarnej – całkowicie kompatybilny z protokołami linii CDL (Common Data Link).

W działaniach z zakresu ZOP (ASW) jest używany podkilowy (aktywny) sonar Westinghouse AN/SQS-510 z cylindryczną anteną o średnicy 1,2 m zaopatrzoną w 360 przetwornic. Stacja ta jest stosowana głównie w fazie bezpośredniego ataku na okręt podwodny (zasięg skuteczny 5–30 km). W czasie poszukiwania okrętów podwodnych skuteczniejsza jest holowana stacja hydroakustyczna CDC AN/SQR-501 CANTASS (VDS). Składa się z 16 modułów przetwornic niskich, średnich i wysokich częstotliwości. Jest to bardzo nowoczesne urządzenie z kablo-liną długości aż 1800 m, mające możliwość zmiany głębokości anteny (np. poniżej warstw termicznych) nawet do 400 m. Ponadto okręty dysponują nową wersją elektro-akustycznego układu AN/SLQ-25A Nixie (lub AN/SLQ-61 LT). Jest to holowany emiter szumów. Służy do wabienia wrogich torped akustycznych przez generowanie dźwięków imitujących odgłosy śrub i maszyn.

POTENCJALNI NASTĘPCY

Kanada zaczęła mocno akcentować swoje prawa w Arktyce od czasów rządów premiera Paula Martina (w latach 2003–2006). Tego rodzaju polityka jest jed-



Wyrzutnie torped Mk 48 Mod. 5

ROYAL CANADIAN NAVY

RYS. 2. PROJEKT TYPE 26

Opracowanie własne.

nym z fundamentalnych kryteriów w sporach terytorialnych. Rząd Stephena Harpera (2006–2015) zwiększał obecność Kanady na terenach arktycznych. W pierwszej dekadzie XXI wieku zaczęto przeznaczać znaczne środki na badania naukowe. Choć operacje prowadzone na Dalekiej Północy są w całości klasyfikowane jako tajne lub ściśle tajne, należy przypuszczać, że mają podłoże głównie ekonomiczne i związane są z kolejnym etapem światowej walki o surowce. Jakby tego było mało, kwestią strategiczną dla Kanady jest handel zagraniczny stanowiący niebagatelne 40% PKB tego kraju. Przy tak rozległej linii brzegowej do jego ochrony potrzebna jest silna flota, jednak Royal Canadian Navy taką nie dysponuje. Ma się to jednak wkrótce zmienić.

Na same tylko okręty i jednostki pomocnicze (w tym Straży Wybrzeża) kraj ten ma zamiar przeznaczyć kwotę co najmniej 60 mld CAD (pierwotnie była mowa o 30–35 mld). Wcześniej, bo już w 2007 roku, zatwierdzono też fundusz w wysokości niebagatelnych 4,3 mld CAD na kompleksową modernizację wszystkich fregat patrolowych typu Halifax w ramach MLU (Mild-Life Upgrade) zgodnie z programem HCM/FELEX (Halifax Class Moderniza-

tion/Frigate Equipment Life EXtension) na lata 2010–2018 (głównym podmiotem wykonawczym był Lockheed Martin Canada odpowiedzialny między innymi za implementację nowego zintegrowanego systemu dowodzenia i zarządzania walką Saab 9LV Mk 4, znanego w Kanadzie jako CanACCS-9LV. Generalnie okręty te uważa się za udane, choć pod wieloma względami ustępują nieco najnowszym konstrukcjom zagranicznym. Ich największym niedostatkiem jest uznane za niewystarczające (jak na tę klasę jednostek) uzbrojenie przeciwlotnicze składające się z dwóch pionowych ośmiokomorowych bloków wyrzutni Mk 48 Mod. 0 VLS do rakiet ESSM lub ESSM Block 2 (które zastąpiły stosowane początkowo przestarzałe RIM-7) oraz pojedynczej licencyjnej szwedzkiej armaty kalibru 57 mm L/70 SAK Mk 3 Bofors i artyleryjskiego zestawu obrony bezpośredniej Mk 15 Phalanx Block IB.

Kanadyjski program rozbudowy sił morskich National Shipbuilding Strategy przewiduje utrzymanie jednostek typu Halifax co najmniej do 2030 roku, tj. do czasu, gdy do linii zaczną wchodzić już ich następcy – 15 nowych wielozadaniowych fregat rakietowych programu CSC (Canada Surface Combatant). Ich budową zajmą się Lockheed Martin Canada oraz brytyjski BAE Systems, którego fundamentem jest rozwojowy projekt Type 26 (rys. 2). Oferta BAE Systems pokonała dwa inne podmioty: Alion Canada wraz z Damen (projekt wykorzystujący konstrukcję holenderskich jednostkach typu De Zeven Provincien) oraz hiszpańską Navantię (projekt oparty na fregatach serii F-105). Nowe okręty, których budowa ma ruszyć jeszcze w tym roku, zastąpią w pierwszej kolejności wycofane już przez Kanadę niszczyciele rakietowe typu Iroquois i wesprą (ostatecznie także zastąpią) tuzin fregat rakietowych typu Halifax.

Nowe fregaty bazujące na gotowych rozwiązaniach technicznych jednostek serii Type 26 będą musiały zostać zintegrowane ze śmigłowcami pokładowymi Sikorsky CH-148 Cyclone, aby skutecznie prowadzić operacje ZOP w różnych regionach, w tym na Dalekiej Północy. Zresztą chęć wykorzystania fregat w działaniach zabezpieczających operacje prowadzone w Arktyce spowodowała (podobnie jak miało to miejsce w przypadku Halifaxów) opracowanie całej serii specjalnych wymagań technicznych co do ich kadłubów – od kształtu i wzmocnień dziobu oraz burt przez opancerzenie aż po wydajny system klimatyzacyjny. Nowe kanadyjskie okręty mogą mieć wyporność bojową na poziomie nawet dużo ponad 8000 t (wyporność standardowa jest oceniana na 7800 t). Założono, że ich długość całkowita będzie wynosić 151,4 m, szerokość aż 20,75 m, a średnie zanurzenie 8 m. Hybrydowy napęd w układzie CODLOG (Combined Diesel-Electric or Gas Turbine) ma umożliwić osiągnięcie prędkości maksymalnej powyżej 27 w., a spory zapas paliwa przekraczanie zasięgu operacyjnego 7000 Mm przy prędkości ekonomicznej.

Ilość generowanej mocy pozwoli w przyszłości na łatwy montaż broni energetycznej. W wersji podstawowej okręty zostaną wyposażone w 32-komorowy blok wyrzutni Mk 41 LMC VLS pozwalający na wykorzystanie rakiet serii Standard i ESSM, rakietotorped VL-Asroc czy nawet RGM-109 Tomahawk. Oznacza to, że Kanada będzie w końcu dysponowała bronią stricte ofensywną (lub przynajmniej będzie miała możliwość jej użytkowania). Na początek rząd kanadyjski zamierza zakupić 100 pocisków SM-2 w wersji Block IIIC oraz 100 pojemników startowych Mk 13 do ich przechowywania i odpalania z wyrzutni Mk 41 VLS. Departament Stanu USA oficjalnie wyraził na to zgodę 5 listopada 2020 roku. Uzbrojenie to zostanie zakupione w ramach programu Foreign Military Sales. Pocisk SM-2 Block IIIC jest najnowszym wariantem typoszeregu SM-2, powstałym przez połączenie korpusu i układu napędowego typowego dla tej rodziny ze zintegrowanymi z aktywnym układem samonaprowadzania pocisku z RIM-174 SM-6 ERAM (Extended Range Active Missile). Nie jest wykluczone zwiększenie zamówienia o pociski SM-6, a w przyszłości – być może – także o SM-3, o ile RCN zdecyduje się na budowę okrętów do kompleksowej obrony powietrznej. Dodatkowo okręty mają otrzymać dwie trójkomorowe pionowe wyrzutnie Lockheed ExLS dla 24 pocisków przeciwlotniczych CAMM-ER Sea Ceptor oraz dwa poczwórne kontenery dla rakiet przeciwokrętowych NSM od norweskiego Kongsberga. Uzbrojenie dodatkowe będzie tworzyła pojedyncza uniwersalna armata morska kalibru 127 mm (prawie na pewno najnowszej wersji), dwa zestawy artyleryjskie kalibru 30 mm, dwa zestawy CIWS kalibru 20 mm Mk 15 Phalanx Block 1B oraz cztery–sześć wielkokalibrowych karabinów maszynowych kalibru 12,7 mm.

Taki zestaw uzbrojenia pozwoli tym okrętom na stworzenie wielowarstwowej obrony przeciwlotniczej i przeciwrakietowej oraz umożliwi swobodne wykonywanie uderzeń na cele położone w głębi lądu, w tym znajdujące się na paku lodowym. Do tego dojdą zwiększone możliwości ZOP. Jednostki – oprócz śmigłowca i bezzałogowych statków powietrznych – otrzymają bogaty zestaw systemów do obserwacji technicznej najnowszej generacji (w tym stacje hydroakustyczne zarówno kadłubowe, jak i holowane) oraz wyrzutnie torped Mk 54 MAKO i zrzutnie grawitacyjnych bomb głębinowych Mk 11. Dodatkowe hangary dla łodzi okrętowych (będzie możliwość zabrania w morze do czterech 11-metrowych RHIB-ów i (lub) podwodnych pojazdów UAV/UUV) zwiększą możliwości prowadzenia działań ZOP i asymetrycznych, szczególnie w obrębie Arktyki.

* * *

Obecnie kanadyjska marynarka wojenna przeżywa istny renesans. W perspektywie najbliższych 15 lat może się stać kolejną potęgą morską. ■

Rozwój broni kosmicznej

KOSMOS PRZEKSZTAŁCA SIĘ STOPNIOWO W ODRĘBNĄ SFERĘ DZIAŁAŃ ZBROJNYCH, MIEJSCE ZUPEŁNIE NOWYCH JAKOŚCIOWO KONFRONTACJI I ROZSTRZYGNIĘĆ MILITARNYCH.

ppłk dr inż. Radosław Bielawski

Autor jest starszym specjalistą w Departamencie Innowacji Ministerstwa Obrony Narodowej.

Przestrzeń kosmiczną zaczęto intensywniej zbroić w czasie zimnej wojny, gdy trwała rywalizacja między największymi wtedy mocarstwami militarnymi: Stanami Zjednoczonymi i Związkiem Socjalistycznych Republik Radzieckich. Okres ten zapoczątkowało 4 października 1957 roku wyniesienie pierwszego sztucznego satelity Ziemi – Sputnika 1. Trwał on do przeprowadzenia wspólnej amerykańsko-radzieckiej misji Apollo–Sojuz 17 lipca 1975 roku. Powodem kosmicznego wyścigu zbrojeń była m.in. chęć zwiększenia potęgi militarnej rywalizujących ze sobą mocarstw.

Dzisiejszy wyścig kosmiczny charakteryzuje się zwiększoną liczbą podmiotów państwowych oraz globalnych i regionalnych mocarstw, do których zalicza się: Federację Rosyjską, Chińską Republikę Ludową, Iran, Koreańską Republikę Ludowo-Demokratyczną i Indie. Wskazani aktorzy państwowi rozwijają broń kosmiczną: kinetyczną, niekinetyczną, elektroniczną i cybernetyczną. Jej rozwój oraz potencjalne użycie mogą spowodować zagrożenie, a więc sytuację, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego[1] dla innych podmiotów, zarówno państwowych, jak i pozapaństwowych.

BROŃ KINETYCZNA

Jednym z państw ją rozwijających są Chiny. Od grudnia 2019 roku, wykorzystując eksperymentalnego satelitę geostacjonarnego SJ-17, prowadziły one operacje zbliżeniowe w stosunku do innych chińskich satelitów: Chinasat 6B, SJ-20 i Gaofen 13 (GF 13). W ich trakcie najmniejsza odległość między obiektami wynosiła 5 km. Oficjalnie strona chińska tłumaczy wykryte aktywności testami nowo opracowanego robota, który wspiera usuwanie śmieci kosmicznych. Inne źródła wskazują jednak, że konstrukcja obiektu odpowiada budowie orbitalnej broni ASAT (anti-satellite)[2].

Kolejne państwo, które zwiększa swoje zdolności do rażenia obiektów kosmicznych, to Rosja. Jednym ze środków bojowych jest system 14Ts033 Nudol PL-19. Od 2009 roku jest on rozwijany przez rosyjski koncern zbrojeniowy WKO „Ałmaz-Antiej". Jego podstawowym komponentem jest dwustopniowy pocisk rakietowy na paliwo stałe 14A042, opracowany w JSC OKB Novator. Daje on możliwość przemieszczania się obiektu z prędkością do Ma=10 na odległość 1500 km. Środek bojowy przed wyniesieniem jest umieszczany na wyrzutni mobilnej 14P222 transportowanej na podwoziu MZKT 12×12. Pocisk jest wyposażony w głowicę kinetyczną oraz elektrooptyczny system naprowadzania MOEGSN (14Sh129). Cele identyfikuje i śledzi stacjonarny system radiolokacyjny 14Ts031 rozmieszczony w pobliżu miasta Czechów w obwodzie moskiewskim. Docelowo ma on dysponować własnym systemem radiolokacyjnym. Od chwili jego skonstruowania przeprowadzono dziesięć testów (tab.). Ich skuteczność wynosiła 80%.

1 M.E. Kołodziejczak, *Różnica pojęć: wojna, konflikt zbrojny, kryzys, zagrożenie występujących w naukach o bezpieczeństwie* [w:] W. Sójka, M.E. Kołodziejczak (red.), *Zagrożenia bezpieczeństwa narodowego Rzeczypospolitej Polskiej w XXI wieku. Pojęcie, zakres i kwalifikacja*, AON, Warszawa 2016, s. 16.

2 T. Harrison at al., *Space Threat Assessment 2021*, Center for Strategic and International Studies, Washington 2021, s. 10.

RUSSIA MINISTRY OF DEFENCE

Dzisiejszy wyścig kosmiczny charakteryzuje się zwiększoną liczbą podmiotów państwowych oraz globalnych i regionalnych mocarstw, do których zalicza się: Federację Rosyjską (na zdjęciu), Chińską Republikę Ludową, Iran, Koreańską Republikę Ludowo-Demokratyczną i Indie.

TABELA. KALENDARIUM TESTÓW ROSYJSKIEGO SYSTEMU ASAT 14TS033 PL-19 NUDOL

Data przeprowadzenia	Miejsce startu	Rezultat
12.08.2014	kosmodrom Plesieck	w zależności od źródeł. Według Departamentu Obrony USA był nieudany
22.04.2015	kosmodrom Plesieck	test nieudany
18.11.2015	kosmodrom Plesieck	test udany
25.05.2016	kosmodrom Plesieck	test udany
16.12.2016	najprawdopodobniej poligon Kapustin Yar	test udany
26.03.2018	kosmodrom Plesieck (z wyrzutni mobilnej)	test udany
23.12.2018	kosmodrom Plesieck (z wyrzutni mobilnej)	test udany – 17 min lotu
15.04.2020.	kosmodrom Plesieck (z wyrzutni mobilnej)	test udany
16.12.2020	kosmodrom Plesieck (z wyrzutni mobilnej)	test udany
15.11.2021	kosmodrom Plesieck (z wyrzutni mobilnej)	test udany (rażenie satelity)

Opracowanie własne.

W ostatnim czasie (od 2020 roku) przeprowadzono trzy ważne testy tego środka walki. Pierwszy z nich 15 kwietnia 2020 roku. Wystrzelony z kosmodromu Plesieck (położony na północy Rosji) środek bojowy przeleciał 3000 km, po czym spadł do Oceanu Arktycznego – najprawdopodobniej bez kinetycznego oddziaływania na cel. Test pośrednio został zapowiedziany 11 kwietnia przez wydanie depeszy NOTAM. Wskazywano w niej na wykonanie niebezpiecznych operacji w rejonie Morza Łaptiewów.

Kolejny test balistyczny środka ASAT przeprowadzono 16 grudnia 2020 roku. Najprawdopodobniej jego zamierzeniem było przechwycenie potencjalnego celu. 15 listopada 2021 roku miał miejsce pomyślny test. Rosjanie poinformowali o udanej próbie środka antysatelitarnego, który z sukcesem raził kinetycznie nieaktywny rosyjski system satelitarny Tselina-D znajdujący się na wysokości 544–566 km i orbitujący w przestrzeni powietrznej od 1982 roku. W wyniku jego trwałego zniszczenia powstała znaczna liczba odłamków (około 1500 śledzonych śmieci kosmicznych), zagrażająca innym obiektom kosmicznym, w szczególności bezpieczeństwu Międzynarodowej Stacji Kosmicznej oraz pracującemu tam personelowi[3].

Strona rosyjska rozwijając broń kinetyczną najprawdopodobniej prowadzi operacje zbliżeniowe i wykonuje manewry w niedalekiej odległości od innych satelitów znajdujących się w szczególności na orbicie GEO. Przykładem takiego obiektu kosmicznego jest satelita Luch (Olymp). Według analizy opublikowanej przez Center for Strategic and International Studies w ostatnim roku obiekt kosmiczny wykonał tego typu operacje, zbliżając się do siedmiu satelitów, w tym amerykańskich, europejskich i brytyjskich.

Jako zagrożenie aktywów kosmicznych w ramach rozwoju ASAT strona rosyjska pracuje nad systemami rakietowymi klasy ziemia–powietrze S-400 i S-500, zdolnymi do rażenia satelitów orbitujących na LEO. Zasięg drugiego z nich jest szacowany na 600 km (o 200 km więcej niż S-400). W 2020 i 2021 roku odnotowano zintensyfikowane testy balistyczne obydwu systemów rakietowych. Szczególnie obiecująca jest nowsza wersja rozwojowa systemu – S-500 Prometeusz (Triumfator-M), przeznaczona do rażenia pocisków balistycznych, aerodynamicznych – samoloty, śmigłowce i bezzałogowe statki powietrzne, a także pocisków manewrujących i hipersonicznych przemieszczających się z prędkością do 7 km/s. Rosyjska Agencja Prasowa TASS 16 września 2021 roku wskazała, że rosyjskie siły zbrojne są wyposażone w pierwsze modele systemu S-500 z możliwością operacyjnego ich użycia.

Rozwój broni ASAT, a także widoczne sukcesy w prowadzeniu testów dają stronie rosyjskiej możli-

3 *14Ts033 Nudol PL-19 Anti-Satellite*, www.globalsecurity.org/wmd/world/russia/a-235-asat.htm/. 4.02.2022.

wość zrównoważenia potęgi kosmicznej NATO. Wynika ona bezpośrednio z liczby satelitów. Zatem niszczenie satelitów (lub ich czasowe zakłócanie) znacząco osłabia możliwości w zakresie C4ISR oraz potencjał militarny zarówno Sojuszu, jak i Stanów Zjednoczonych.

Drugim czynnikiem wpływającym na zwiększenie pozycji militarnej Rosji jest efekt odstraszania militarnego. Wynika on z posiadania zaawansowanej kinetycznej broni antysatelitarnej, jak również z potencjalnej możliwości jej skutecznego użycia w ramach prowadzenia wojny asymetrycznej. Z tego też powodu rosyjskie testy broni antysatelitarnej były szeroko potępiane publicznie przez amerykańskie Dowództwo Sił Kosmicznych. Dodatkowo można stwierdzić, że strona rosyjska dyplomatycznie wyraża chęć przystąpienia do wielostronnych rozmów dotyczących bezpieczeństwa kosmicznego i jego pokojowego wykorzystania, w tym do międzynarodowego porozumienia zakazującego rozmieszczenia broni w przestrzeni kosmicznej oraz do regulacji prawnych zapobiegających jej rozwojowi w wyścigu zbrojeń. Na potwierdzenie tej tezy można podać argument w postaci braku zapisów w rosyjskich dokumentach doktrynalnych dotyczących przewagi militarnej w Kosmosie i jej osiągania.

BROŃ NIEKINETYCZNA

Amerykańska Agencja Wywiadu Wojskowego wskazuje, że spośród 50 naziemnych ośrodków, w których może się znajdować broń laserowa, pięć rozmieszczonych jest na terenie Chin – w Szanghaju, Changchun, Pekinie, Wuhan i Kuming. Dwie z wymienionych baz mają zdolności mobilne. Ośrodki te są wyposażone najprawdopodobniej w systemy służące do śledzenia obiektów satelitarnych oraz oślepiania i niszczenia podsystemów satelitarnych. Oprócz nich Chiny posiadają kilka laserowych stacji radiolokacyjnych, których zadaniem jest śledzenie orbit satelitów oraz śmieci kosmicznych.

Kolejnym potentatem militarnym, który rozwija niekinetyczną broń kosmiczną, jest Federacja Rosyjska. Jedną z nich jest mobilny system laserowy Peresvet do rażenia obiektów powietrznych i kosmicznych. W lipcu 2018 roku rosyjskie Ministerstwo Obrony Narodowej opublikowało na kanale YouTube materiał wideo z przygotowania systemu laserowego do implementacji w rosyjskich siłach zbrojnych. Dodatkowo podano informacje na temat przeszkolenia operatów w Wojskowej Akademii Kosmicznej im. Możajskiego w Sankt Petersburgu, co potwierdziło obszar wykorzystania broni.

W grudniu 2018 roku rosyjski MON opublikował na Facebooku kolejny materiał wideo przedstawiający system Peresvet wraz z oświadczeniem, że jest on zdolny do zwalczania zagrożeń z Kosmosu oraz rażenia obiektów kosmicznych. Materiał ten został usunięty godzinę po jego publikacji ze stwierdzeniem przypadkowego upublicznienia. 1 grudnia 2019 roku rosyjski minister obrony narodowej wydał oświadczenie, że system ten rozlokowano w pięciu dywizjonach rakietowych. W 2021 roku upubliczniono plan możliwego jego rozmieszczenia na rosyjskich lotniskowcach, nie podając więcej szczegółów.

BROŃ ELEKTRONICZNA

Oprócz nabytych zdolności w zakresie systemów walki elektronicznej Chiny stały się również importerem tego typu uzbrojenia. Jednym z odbiorców jest Algieria. Pod koniec 2021 roku dostarczono jej zintegrowany system walki elektronicznej, którego producentem są chińskie przedsiębiorstwa: ELINC i CEIC. Niezidentyfikowany system najprawdopodobniej jest wersją rozwojową LDK-190. Ma on pasywne, zarówno ofensywne, jak i defensywne podsystemy, zdolne do wykrywania emisji radiowych i radiolokacyjnych w odległości do 600 km. Dodatkowo umożliwia on określenie pozycji emitujących środków i ich identyfikację. Urządzenie może zagłuszać łączność radiową, a także takich systemów, jak: GPS, BeiDou, Galileo, Glonass na odległość do 300 km w zakresie częstotliwości 0,5–40 GHz. System walki ma możliwości ofensywne – emisję ukierunkowanej energii o mocy do 500 kW.

Istnieją źródłowe potwierdzenia, że Chiny budują nowe struktury militarne w pobliżu linii demarkacyjnej LAC (Line of Actual Control) przy granicy z Indiami. W odległości 60 km od linii demarkacyjnej, w rejonie Nyanglu, rozmieszczono także środki walki elektronicznej, służące najprawdopodobniej do zagłuszania indyjskich satelitów.

Kolejnym aktorem państwowym rozwijającym elektroniczną broń kosmiczną jest Federacja Rosyjska, która dysponuje kilkoma jej systemami. Najnowsze z nich to mobilny system zagłuszania Tirada-2 oraz naziemny mobilny system walki elektronicznej Bylina-MM z elementami sztucznej inteligencji. Rosyjskie siły zbrojne są również wyposażone w systemy zagłuszające Krasuka-2 i Krasuka-4. Obecnie trwają prace rozwojowe dotyczące systemu wywiadu radioelektronicznego Liana. Jego zadaniem jest monitorowanie aktywności wojskowej obcych państw, śledzenie ruchu sił morskich i lądowych, a także wyznaczanie celów do uderzeń bronią precyzyjną. Trzonem systemu jest konstelacja satelitów Pion-NKS. W otwartych źródłach brakuje oficjalnych danych na jego temat. Diagnozy analityków wskazują, że jest on przeznaczony do pracy na orbicie okołoziemskiej na wysokości 250–270 km. W zależności od zaimplementowanych urządzeń rozmieszczonych na satelitach są one w stanie określić współrzędne obserwowanego obiektu z dokładnością od 1 km do 10 m.

Jednym z państw rozwijających zdolności ataków elektronicznych na aktywa kosmiczne jest Korea Północna. W kwietniu 2020 roku ogłosiła ona rozmieszczenie broni elektronicznej zdolnej do zakłócania systemów nawigacji satelitarnej. Źródła open source wskazują, że zidentyfikowane urządzenie zagłusza

komercyjne częstotliwości radiowe cywilnych sygnałów systemów GPS skierowanych głównie w stronę Korei Południowej.

Mobilnym systemem walki elektronicznej Samyukta dysponują również Indie. Służy on do przechwytywania, identyfikacji i ustalania pozycji emisji sygnałów komunikacyjnych i radiolokacyjnych w szerokim zakresie długości fal. Zestaw składa się z trzech segmentów komunikacyjnych i dwóch niekomunikacyjnych. Urządzenie ma możliwość pokrycia obszaru o wymiarach 150x70 km oraz zagłuszania sygnałów komunikacyjnych i radarowych w zakresie od HF do MMW. Innym indyjskim środkiem walki elektronicznej jest Himshakti. Stosowany jest on jako środek o działaniu zarówno ofensywnym, jak i defensywnym i służy do zagłuszania na obszarze 10 tys. km^2.

Obecnie w Indiach trwają zaawansowane prace w zakresie zabezpieczeń dotyczących komunikacji satelitarnej. Ostatnio przeprowadzono test komunikacji kwantowej między dwoma budynkami oddalonymi od siebie 300 m. Podczas testów w ten sposób przesłano dane tekstowe, obraz oraz wideo. Do transmisji użyto metodę Quantum Key Distribution (QKD), wykorzystującą implementacje protokołu kryptograficznego z elementami mechaniki kwantowej. Technika ta jest uważana za wyjątkowo bezpieczną z uwagi na szybkie zdiagnozowanie potencjalnego włamania i przekazanie informacji o tym nadawcy sygnału.

BROŃ CYBERNETYCZNA

Jednym z państw prowadzących aktywną działalność cybernetyczną jest Rosja. Potwierdziła ona swoje ofensywne zdolności w 2020 roku w ramach cyberataku o nazwie SolarWinds[4]. W tym wypadku wykorzystano atak na łańcuch dostaw (zwany też atakiem na stronę trzecią, atakiem na łańcuch wartości lub atakiem przez tylne drzwi), polegający na tym, że atakujący uzyskuje dostęp do sieci biznesowej za pośrednictwem dostawców będących podmiotami trzecimi lub przez łańcuch dostaw. Agresję przeprowadzono podczas aktualizacji platformy zarządzania siecią Orion. Odbiorcy, aktualizując oprogramowanie, nieświadomie infekowali swoje systemy komputerowe. Cyberatak odkryła w grudniu 2020 roku firma konsultingowa FireEye. Szacuje się, że podczas niego zainfekowano około 18 tys. użytkowników. Wśród nich amerykańskie departamenty: handlu, obrony, energii, bezpieczeństwa wewnętrznego i sprawiedliwości. Oprócz administracji rządowej jego celami były przedsiębiorstwa: Belkin, Cisco, Deloitte, Intel, Nvidia i Vmware. Najprawdopodobniej przeprowadzony cyberatak miał charakter wywiadowczy.

Zdolności walki cybernetycznej rozwija też Iran. Swoje możliwości zademonstrował, wykonując cyberataki na Izrael. Najprawdopodobniej do tego celu wykorzystano grupy hakerskie pracujące na zlecenie irańskiego rządu. Jedna z nich, Pay2Key, w grudniu 2020 roku przeprowadziła cyberatak na spółkę Israel Aerospace Industries – Elta Systems oraz inne podmioty. W jego wyniku zniszczono strony internetowe, dokonano kradzieży informacji umożliwiających identyfikację osób oraz zaimplementowano szkodliwe oprogramowanie. Obecnie nie ma informacji na temat irańskich cyberataków na obce aktywa kosmiczne. Jednak biorąc pod uwagę częstotliwość cyberataków oraz coraz bardziej zaawansowane techniki ich prowadzenia, aktywa kosmiczne mogą w przyszłości być celem irańskich oddziaływań cybernetycznych. Analizując tego typu potencjalne zdarzenia, należy zwrócić uwagę, że w styczniu 2021 roku podpisano umowę irańsko-rosyjską dotyczącą bezpieczeństwa informacyjnego. Na jej mocy przewidziano bliższą współpracę stron w dziedzinie bezpieczeństwa cybernetycznego. W ramach umowy sugeruje się również możliwość transferu technologii i wymianę doświadczeń. Ma to na celu rozwijanie przez Iran zdolności działań ofensywnych w cyberprzestrzeni, w tym również pozyskania zdolności do rażenia infrastruktury kosmicznej.

Departament Sprawiedliwości Stanów Zjednoczonych postawił zarzuty trzem programistom komputerowym, zidentyfikowanym jako członkowie północnokoreańskiej agencji wywiadu wojskowego. Są oni oskarżeni o przeprowadzenie wielu ataków cybernetycznych z lokalizacji w Rosji i Chinach, pracując na zlecenie rządu Korei Północnej. Motywem działania hakerów były pobudki materialne. Poza tego typu działalnością cybernetyczną w Korei Północnej powołano elitarną jednostkę do walki w cyberprzestrzeni. Cyber Warfare Guidance Unit (znana również jako Bureau) liczy 6 tys. hakerów, z czego wielu z nich działa poza Koreą Północną, w takich państwach jak: Chiny, Rosja, Indie, Malezja i Białoruś. Najprawdopodobniej jednostka Bureau ma w swojej strukturze dwie główne podgrupy. Pierwszą z nich jest Andarial (Andariel). Liczy ona 1600 członków i jest odpowiedzialna za działalność wywiadowczą na potrzeby prowadzenia przyszłych cyberataków. Druga grupa to Bluenoroff. Zrzesza ona 1700 hakerów, a jej działalność jest skoncentrowana na obiektach finansowych.

Korea Północna jest podejrzewana również o wykonanie serii cyberataków zgłoszonych przez Google w styczniu 2021 roku. Wykorzystywano w nich wyrafinowane techniki oszustwa w mediach społecznościowych oraz zastosowano technikę phishingu, za pomocą której przy kliknięciu na przesłany link uzyskano pełny dostęp do hakowanych komputerów. Dotychczasowe cyberataki Korei Północnej nie dotyczyły przestrzeni kosmicznej. Jednak ich częstotliwość oraz coraz to bardziej wyrafinowane metody wskazują, że w niedługim czasie ich przedmiotem mogą być elementy infrastruktury kosmicznej. ■

4 Nazwa cyberataku jest tożsama z nazwą przedsiębiorstwa, na które został on przeprowadzony.

Agresja na Ukrainę, czyli koncepcja rosyjskiej **wojskowej operacji specjalnej**

TOCZĄCY SIĘ OD WIOSNY 2014 ROKU KONFLIKT ZNACZNIE ZMIENIŁ ŚRODOWISKO BEZPIECZEŃSTWA W EUROPIE I PODAŁ W WĄTPLIWOŚĆ ISTOTĘ ZAWIERANYCH DOTYCHCZAS SOJUSZY ORAZ MOC PODPISYWANYCH UMÓW MIĘDZYNARODOWYCH.

płk rez. prof. dr hab. Marek Wrzosek

Wydarzenia roku 2022, tzn. specjalna operacja wojskowa armii rosyjskiej, zmusiły społeczność międzynarodową, w tym szczególnie wspólnotę europejską i NATO, do nowego spojrzenia na problem bezpieczeństwa. Po agresji rosyjskiej na Ukrainę wiele państw Starego Kontynentu zdało sobie sprawę, że Ukraina dla Polski i Europy jest strefą specjalną, jest buforem bezpieczeństwa oddzielającym świat zachodni od rosyjskiego imperializmu. Powszechnie znana jest teza marszałka Józefa Piłsudskiego, że *bez wolnej Ukrainy nie będzie wolnej Polski*, dlatego walka o odzyskanie ukraińskiej niepodległości stała się priorytetem w polityce zagranicznej Piłsudskiego. To wówczas zrodziła się idea współpracy (federacji) państw od Bałtyku po Morze Czarne[1].

W odniesieniu do współczesnej sytuacji wydaje się, że reakcja NATO na rosyjską ekspansywną politykę była właściwa i zrównoważona w swojej formie. Dość sprawnie i szybko deklaracje polityczne poszczególnych państw NATO przybrały konkretny wymiar, którego wyrazem liczba przekazanych Ukrainie jednostek sprzętu bojowego i wyposażenia. Unia Europejska natomiast przyjęła kolejne pakiety sankcji jako instrumenty politycznego oddziaływania, którego celem było ograniczenie zdolności ekonomicznych Rosji oraz wsparcie Ukrainy.

Autor jest pracownikiem naukowym w Wydziale Wojskowym Akademii Sztuki Wojennej.

TŁO AGRESJI

Konflikt rosyjsko-ukraiński jest uwarunkowany wieloma zdarzeniami, które zdeterminowały system

1 Polityczna idea Międzymorza (Intermarium), wysuwana przez Józefa Piłsudskiego w okresie międzywojennym, zakładająca utworzenie federacji państw Europy Środkowej i Wschodniej docelowo obejmowała obszar między morzami Adriatyckim, Bałtyckim i Czarnym (Morza ABC), a konkretnie Białoruś, Czechosłowację, Estonię, Jugosławię, Litwę, Łotwę, Polskę, Rumunię, Ukrainę i Węgry oraz ewentualnie Finlandię. Piłsudski uważał, że jej powstanie pozwoli uniknąć państwom Europy Środkowej dominacji Niemiec czy Rosji.

RAFAŁ MNIEDŁO/11 DKPANC

bezpieczeństwa międzynarodowego. Po upadku Wiktora Janukowycza na Krymie 23 lutego 2014 roku odbyły się demonstracje w Kerczu i Sewastopolu. W obydwu miastach ściągnięto flagi ukraińskie z budynków merostw, a na ich miejsce wywieszono rosyjskie. Na wiecu w Sewastopolu zainicjowano proces formowania sił samoobrony. Następnie 25 lutego w Symferopolu odbyła się demonstracja, której uczestnicy domagali się zwołania nadzwyczajnej sesji Rady Najwyższej Republiki Autonomicznej Krymu i rozpisania referendum w sprawie niepodległości. Demonstranci deklarowali, że nie uznają prawa stanowionego przez Radę Najwyższą w Kijowie. W nocy z 26 na 27 lutego rosyjscy żołnierze bez dystynkcji (tzw. zielone ludziki) zajęli budynki parlamentu i rządu Republiki Autonomicznej Krymu w Symferopolu, po czym wywiesili na nich rosyjskie flagi. Wobec braku zdecydowanych działań militarnych ze strony Ukrainy 28 lutego nad ranem grupa uzbrojonych rosyjskich żołnierzy bez znaków rozpoznawczych na mundurach opanowała port lotniczy Symferopol, następnie wojskowe lotnisko Belbek w Sewastopolu. Ponadto rosyjscy marynarze otoczyli ukraiński posterunek graniczny koło Sewastopola. Strona ukraińska podejmowała działania dyplomatyczne zmierzające do zatrzymania rosyjskiej interwencji. Tymczasem wojska rosyjskie na Krymie stopniowo zajmowały kolejne pozycje, blokując lub przejmując garnizony stacjonowania ukraińskich wojsk, które zgodnie z rozkazem z Kijowa nie podejmowały działań zbrojnych. W związku z bierną postawą ukraińskich wojsk rosyjscy żołnierze opanowali stanowiska startowe dywizjonu obrony przeciwlotniczej w Sewastopolu oraz zablokowali bazę w miejscowości Perewalne. Zablokowali także sztab floty wojennej Ukrainy w Sewastopolu. Na początku marca rosyjskie wojska specjalne wtargnęły na teren dwóch dywizjonów artyleryjsko-rakietowych w tym mieście w pobliżu przylądka Fiolent i przejęły nad nimi kontrolę. Ponadto Rosjanie opanowali siedzibę stacji przekaźnikowej radia i telewizji. Po jej przejęciu zostały wyłączone ukraińskie kanały *1+1* oraz *Kanał 5*, natomiast włączono nadawanie rosyjskiego kanału *Rossija 24*. Już 17 marca komisja ds. referendum ogłosiła, że według ostatecznych wyników 96,77% głosujących opowiedziało się za zjednoczeniem Krymu z Rosją. W tej sytuacji Rada Najwyższa Krymu przyjęła uchwałę o niepodległości półwyspu. Specjalny status w ramach republiki otrzymało miasto Sewastopol, w którym stacjonowała Flota Czarnomorska. Po przeprowadzonym referendum 21 marca prezydent Władimir Putin podpisał akty ratyfikacyjne traktatu o przyjęciu Republiki Krymu do Federacji Rosyjskiej.

W tym samym czasie w obwodzie ługańskim i donieckim dochodziło do demonstracji zwolenników autonomii lub wręcz przyłączenia obu obwodów do Rosji. Prorosyjscy separatyści proklamowali samozwańcze republiki. Nowe republiki powstałe wskutek rebelii zostały ustanowione: 7 kwietnia Doniecka, a 27 kwietnia 2014 roku Ługańska. 11 maja przeprowadzono w nich referendum, w wyniku którego ogłoszono deklarację niepodległości. Następnie 24 maja 2014 roku obie republiki podpisały porozumienie o powstaniu Federacyjnej Republiki Noworosji. Natomiast po zawarciu porozumienia mińskiego w 2015 roku o zawieszeniu broni funkcjonowanie Noworosji zostało zawieszone. Po ośmiu latach istnienia obu samozwańczych bytów 21 lutego 2022 roku obie republiki zostały uznane przez Federację Rosyjską.

W takcie narastania sytuacji konfliktowej strona rosyjska akcentowała fakt dodatkowego rozmieszczania wojsk NATO w pobliżu granic Federacji Rosyjskiej. Ponadto w środkach masowego przekazu Rosjanie podkreślali militarne zagrożenie państwa powodowane nadmierną koncentracją wojsk amerykańskich oraz rozmieszczanie wielonarodowych grup bojowych. W rosyjskiej doktrynie wojennej wśród głównych zagrożeń zewnętrznych wskazano *zwiększanie potencjału militarnego NATO oraz powierzenie mu globalnych funkcji, wykonywanych wbrew normom prawa międzynarodowego, zbliżenie militarnej infrastruktury państw członkowskich*

NATO do granic Federacji Rosyjskiej między innymi przez dalsze rozszerzenie bloku[2]. Ponadto w przekonaniu Federacji Rosyjskiej istotne zagrożenie stanowi *rozwijanie kontyngentów wojskowych innych państw (grupy państw) na terytorium państw sąsiadujących z Federacją Rosyjską oraz jej sojusznikami, jak również na przyległych akwenach między innymi w celu wywierania presji politycznej i militarnej na Federację Rosyjską.*

Nie bez znaczenia dla rozwoju sytuacji w wymiarze międzynarodowym miała deklaracja Ukrainy o zamiarze przystąpienia do NATO, a także wspólne ćwiczenia z wojskami państw Sojuszu. Już w 1991 roku Ukraina przystąpiła do powstałej wówczas Północnoatlantyckiej Rady Współpracy (NACC), a w 1994 roku jako pierwsze państwo ze Wspólnoty Niepodległych Państw dołączyła do programu *Partnerstwo dla pokoju*. Po agresji FR na Krym Ukraina zwróciła się do NATO o uruchomienie programu modyfikacji sektora bezpieczeństwa i obronności do standardów NATO. W efekcie po 2014 roku podjęto kilka projektów obejmujących:

– reorganizację i modernizację struktur organizacyjnych oraz zwiększanie ich zdolności w zakresie C4 (command, control, comunication, computers);

– reformę systemu logistycznego, w tym szczególnie w obszarze standaryzacji i normalizacji;

– zdolności do przeciwdziałania zagrożeniom cybernetycznym[3].

Ze względu na położenie Ukrainy w bezpośrednim sąsiedztwie NATO rola tego państwa w kształtowaniu bezpieczeństwa w regionie jest niezwykle istotna. Dlatego też zarówno poprzednia, jak i obecna wojna stanowi poważne wyzwanie. Wojskowe wsparcie państw europejskich samo w sobie nie zapewni Ukrainie bezpieczeństwa, jednak stanowi ważny element wzmacniania potencjału bojowego tego państwa w konfrontacji z Federacją Rosyjską.

Rosja rozpoczęła gromadzenie wojsk wokół granic Ukrainy jeszcze w październiku 2021 roku. Kolejne ćwiczenia zgrywające systemy walki i doskonalące umiejętności bojowe wojsk były prowadzone w listopadzie oraz w grudniu tegoż roku. Część tych wojsk znalazła się na Białorusi w ramach lutowych ćwi-

2 *Doktryna wojenna Federacji Rosyjskiej*, https://www.bbn.gov.pl/ftp/dok/01/DoktrynaFederacjiRosyjskiej.pdf/.

3 Zob.: S. Piotrowski, *Trzy dekady wojskowego wsparcia Ukrainy przez NATO (1991–2021)*, „Kwartalnik Bellona" 2021 nr 4, s. 15–26.

czeń „Sojusznicza stanowczość 2022", w których wzięło udział 30 tys. rosyjskich żołnierzy. W procesie przygotowania inwazji zbrojnej na Ukrainę zaobserwowano także przemieszczenie rakiet balistycznych 9M723 Iskander-M przewożonych transportem kolejowym w pobliże granicy z Ukrainą. Pod koniec 2021 roku rozpoczęto przygotowania do zaplanowanych na luty następnego roku wspólnych z armią białoruską wspomnianych nadzwyczajnych ćwiczeń. Zostały w nie zaangażowane jednostki operacyjne wojsk białoruskich oraz siły Wschodniego Okręgu Wojskowego (OW), a także przewidywane do realizacji zadań wsparcia bojowego wydzielone komponenty Sił Zbrojnych Federacji Rosyjskiej, w tym sił powietrzno-kosmicznych i wojsk powietrznodesantowych. Na podstawie ogólnej oceny zaangażowanych w ćwiczenia jednostek można wywnioskować, że brało w nim udział 60–80 tys. żołnierzy rosyjskich i białoruskich. Ważnym aspektem ćwiczeń był niezapowiedziany sprawdzian gotowości bojowej sił Wschodniego Okręgu Wojskowego (14 stycznia 2021)[4]. Alarmowe postawienie w stan gotowości sprawiło, że pierwszorzutowe związki taktyczne WOW po uzupełnieniu zapasów wojennych zostały transportem kolejowym skierowane na poligony rozmieszczone na Białorusi. Wojska przemieszczono na odległość ponad 7 tys. km. Strategicznego przerzutu jednostek Zachodniego Okręgu Wojskowego na Białoruś dokonano w ramach sprawdzianu sił reagowania państwa związkowego.

Ćwiczenia w zgodnej ocenie międzynarodowej opinii zostały odebrane jako kolejny etap wywierania presji na kraje zachodnie, w tym szczególnie na USA. Jednakże już wówczas w ocenach wywiadowczych zakładano, że zarówno obszar geograficzny, jak i charakter przedsięwzięć świadczyły o tym, że prawdopodobnym kierunkiem zainteresowania sił rosyjskich jest Ukraina. Uwaga obserwatorów skoncentrowała się na odmienności ćwiczeń „Sojusznicza stanowczość 2022", siły WOW bowiem po pierwsze ćwiczyły na poligonach w Europie. Po drugie poza Rosją. Po trzecie wreszcie we współdziałaniu z armią białoruską. Czwartym odmiennym elementem był fakt, że po stronie białoruskiej ćwiczenia stanowiły nowe rozwiązanie organizacyjne – były pierwszym przedsięwzięciem strategicznym armii białoruskiej realizowanym w zimie oraz wspólnie z jednostkami rosyjskimi, z którymi wcześniej siły zbrojne Białorusi nie ćwiczyły[5].

W kontekście rosyjskiego uderzenia na Ukrainę należy dostrzegać także to, że w ramach ćwiczeń miało miejsce przejście zgrupowania okrętów desantowych Floty Bałtyckiej i Floty Północnej na Morze Czarne. W wymiarze militarnym oznaczało to realne wzmocnienie potencjału Floty Czarnomorskiej w celu przygotowania operacji desantowej (np. opanowanie Odessy, Mariumpola). Należy przyjąć, że wspólne ćwiczenia oznaczały w praktyce faktyczną zgodę Mińska na wykorzystanie terytorium Białorusi do inwazji na Ukrainę.

AGRESJA

Interwencję zbrojną na Ukrainie oficjalnie ogłosił prezydent Federacji Rosyjskiej Władimir Putin w wystąpieniu telewizyjnym (24 lutego 2022). W rosyjskim przekazie informacyjnym *wojskowa operacja specjalna*, bo taką nazwę otrzymała zbrojna napaść na Ukrainę, miała na celu demilitaryzację i denazyfikację państwa oraz ochronę ludności separatystycznych, prorosyjskich republik Donbasu, czyli Ługańskiej i Donieckiej Republiki Ludowej. W przemówieniu prezydent Federacji Rosyjskiej wskazał, że reżim z Kijowa od 8 lat dopuszcza się ludobójstwa i prześladuje rosyjskojęzyczną ludność. W tej sytuacji strona rosyjska uznała za celowe przeprowadzenie operacji, której celem była po pierwsze *demilitaryzacja* państwa ukraińskiego, a więc wprowadzenie zakazu posiadania broni ofensywnej. Drugim celem była *neutralizacja obszaru Ukrainy, przez którą Rosja rozumiała* zakaz jej wejścia do NATO oraz do innych bloków wojskowych. Po trzecie Ukraina miałaby uznać Krym za część Rosji, a republiki ludowe za niepodległe państwa. Ponadto istotnym celem podejmowanych działań militarnych było przywrócenie odpowiedniego statusu językowi rosyjskiemu. Moskwa oczekiwała również zdelegalizowania przez Kijów partii politycznych i organizacji publicznych o poglądach *nacjonalistycznych* i *neonazistowskich* oraz unieważnienia ustaw gloryfikujących nacjonalistów.

Federacja Rosyjska pod pozorem ćwiczeń zgromadziła wokół granic Ukrainy od 90 do 120 tys. żołnierzy, a także zacieśniła współpracę z Białorusią, zwiększając w tym kraju liczebność swoich sił wojskowych. W ocenie ekspertów duże, regularne zgrupowania bojowe były gotowe do działania od początku stycznia 2022 roku. Prawdopodobnie 130 taktycznych grup batalionowych (każda około 800 żołnierzy) pozostawało na obszarze sąsiadującym z Ukrainą w stałej gotowości bojowej[6]. Były to wojska 8 Armii Południowego Okręgu Wojskowego i 20 Armii Zachodniego Okręgu Wojskowego oraz wydzielone siły i środki rosyjskiej Floty Czarnomorskiej. Oprócz tego w pobliżu granicy stacjonowały grupy 4 i 6 Armii Sił Powietrznych i Obrony Przeciwlotniczej. Ponadto siły 41 Armii Wschodniego Okręgu Wojskowego, zwykle dyslokowane w Nowosybirsku, po ćwiczeniach w europejskiej części kontynentu nie wróciły na Syberię, lecz przyłączyły się do zgrupowania

4 https://wydarzenia.interia.pl/zagranica/news-zwiazkowa-stanowczosc-2022-czy-to-poczatek-inwazji-na-ukrain,nld,5823992/. 1.02.2022.

5 A. Wilk, *Rosyjska demonstracja siły na Białorusi i oceanie światowym,* https://www.osw.waw.pl/pl/publikacje/analizy/2022-01-24/rosyjska-demonstracja-sily-na-bialorusi-i-oceanie-swiatowym/. 26.01.2022.

6 https://www.polsatnews.pl/wiadomosc/2021-11-25/rosja-gromadzi-armie-przy-granicy-z-ukraina-umacnia-sie-tez-militarnie-na-bialorusi/.

wojsk rosyjskich w pobliżu granicy z Ukrainą. Podsumowując, należy stwierdzić, że Rosja w okresie poprzedzającym uderzenie dysponowała niemal 130 taktycznymi grupami batalionowymi. Jeśli przyjąć, że każda liczyła około 800 żołnierzy, to w ogólnym rozrachunku siły armii rosyjskiej można oceniać na blisko 104 tys. żołnierzy.

Początkowy etap operacji zaczepnej nawiązywał swoim scenariuszem do czasów drugiej wojny światowej. Atak sił zbrojnych nastąpił o świcie (około 3:55) bez wypowiedzenia wojny, z zaskoczenia. Armia rosyjska rozpoczęła agresję od serii uderzeń lotniczo-rakietowych, ostrzału stanowisk bojowych sił ukraińskich oraz kluczowych ukraińskich obiektów wojskowych, w tym lotnisk, magazynów amunicji i ośrodków dowodzenia. W czasie ataku wykorzystano pociski balistyczne oraz samosterujące rakiety skrzydlate wystrzeliwane z wyrzutni lądowych, morskich i lotniczych. Jednocześnie Rosjanie zaatakowali infrastrukturę informatyczną Ukrainy[7].

Po artyleryjsko-rakietowym przygotowaniu ataku około godziny 8.00 kolumny rosyjskich jednostek lądowych wkroczyły na terytorium Ukrainy. Atak rosyjskich sił rozpoczął się z trzech kierunków operacyjnych (rys.).

Pierwszy kierunek operacyjny – wschodni (zasadniczy). Wojska rosyjskie z obszaru separatystycznych republik uderzyły w kierunku: Ługańsk – Krematorsk oraz Donieck – Zaporoże. Ukraiński wywiad ustalił, że na tym kierunku w rejonie Brańska, Kurska i Biełgorodu została rozmieszczona 20 Gwardyjska Armia Ogólnowojskowa (w czasie pokoju dowództwo stacjonuje w Woroneżu). W jej składzie były dwie dywizje zmechanizowane: 3 Wiślańska DZ oraz 144 Jelnińska DZ Gwardii, a także jednostki wsparcia i zabezpieczenia. Ponadto w rejonie Rostowa Rosjanie utrzymywali w gotowości 8 Gwardyjską Armię Ogólnowojskową z Nowoczerkaska. W jej składzie rozpoznano: 150 Idrycko-Berlińską Dywizję Zmechanizowaną oraz 20 Przykarpacko-Berlińską Brygadę Zmechanizowaną Gwardii. Natarcie wojsk rosyjskich prowadzono na przygotowane pozycje obronne, co w praktyce oznaczało zacięte walki, ukraińska bowiem linia obrony została rozbudowana pod względem inżynieryjnym i przygotowana do odparcia ataku. Rosjanie usiłowali przez obejście zasadniczych rejonów obrony otoczyć zgromadzone tam znaczne siły obrońców. Jednak Ukraińcy byli przygotowani do obrony manewrowej, w związku z tym na niektórych kierunkach przechodzili do kontrataków, uniemożliwiając Rosjanom rozwinięcie natarcia. Zacięte walki na obszarze Donbasu toczyły się od początku konfliktu – Ukraińcy, wykorzystując system obrony przestrzennej oraz znajomość terenu, skutecznie powstrzymywali natarcie agresora.

Rosjanie od początku wojny próbowali zdobyć Charków – miasto, które było dobrze przygotowane do obrony. Ukraińcy w ramach inżynieryjnego przygotowania terenu zniszczyli infrastrukturę drogową na głównych kierunkach rosyjskiego natarcia. Wysadzili co najmniej cztery mosty. Jeden od strony wschodniej (w kierunku Charkowa) i trzy z różnych stron w kierunku Kijowa. Na początku marca jednostki rosyjskie nadal walczyły o Charków. Zdobycie miasta okazało się jednak trudne. Rosjanie zdecydowali się więc na niszczenie infrastruktury i zakładów przemysłowych. Należy podkreślić, że Charków to ważny ośrodek branży pancernej (Zakłady im. Małyszewa) i lotniczej. W ostatnich latach miejscowe przedsiębiorstwa utraciły co prawda bieżące zdolności produkcyjne, ale ich potencjał miał istotne znaczenie dla produkcji sprzętu pancernego. Miasto było intensywnie ostrzeliwane ogniem artyleryjskim. Obiektem uderzeń były również osiedla mieszkalne i budynki administracyjne w jego centrum. W wyniku rosyjskiego ostrzału doszło do uszkodzenia gazociągów, sieci elektrycznych, wodociągów i innych ważnych obiektów infrastruktury. W obwodzie charkowskim siły ukraińskie przechodziły miejscami do kontrataków, natomiast na drogach dojazdowych do Charkowa rozbijano rosyjskie kolumny. Główne uderzenia wojsk rosyjskich koncentrowały się na zablokowaniu miasta i zniszczeniu jego cywilnej infrastruktury. Heroiczna obrona miasta spowodowała, że agresor nie mógł skierować swoich sił uderzeniowych w kierunku miejscowości Dnipro, aby wyjść na tyły obrońców do linii rzeki Dniepr. Rosjanom udało się jednak otoczyć Charków i przerwać pierścień jego obrony. Jednostki zmechanizowane wjechały nawet na centralne ulice miasta. Ostatecznie jednak zostały wyparte przez obrońców.

W całym Donbasie trwały zaciekłe walki. Rosjanom nie udało się wówczas zdobyć głównych miast, w tym Kramatorska, Słowiańska, Wołnowachy, na południu Mariupola, a na północy Siewierodoniecka. Tymczasem główne siły rosyjskie działające w obwodzie donieckim zmieniły kierunek natarcia i zwróciły się w stronę Zaporoża. Szybko zbliżyły się do miasta na odległość kilkunastu kilometrów. Rosjanie, wykorzystując luki w ugrupowaniu wojsk ukraińskich, posuwali się wzdłuż wschodniego brzegu Dniepru. Już 27 lutego osiągnęli Wasyliówkę położoną bezpośrednio nad tą rzeką. Następnie w nocy 4 marca przejęli kontrolę nad Zaporoską Elektrownią Jądrową w Enerhodarze (największa elektrownia jądrowa w Europie, zbudowana w latach 1980–1986). Teren elektrowni został ostrzelany, co spowodowało pożary w kilku budynkach. Zostały one jednak ugaszone i nie stanowiły zagrożenia dla reaktorów. Utrata kontroli nad elektrownią w Enerhodarze może spowodować w przy-

7 Przykładowo 23 lutego 2022 roku firmy ESET i Broadcom poinformowały, że celem przeprowadzonego cyberataku było kasowanie danych w sieciach komputerowych ukraińskich władz. Zob.: https://www.rp.pl/polityka/art35745821-cyberatak-na-ukrainie-celem-hakerow-bylo-czyszczenie-danych/.

szłości poważne problemy z zaspokojeniem zapotrzebowania na energię elektryczną na dużym obszarze.

Drugi kierunek operacyjny – północny. Wojska rosyjskie nacierały z północy w kierunku Kijowa. Według ukraińskich źródeł przy granicy z Białorusią stacjonowała 1 Gwardyjska Armia Pancerna z Zachodniego Okręgu Wojskowego, bardzo silne zgrupowanie uderzeniowe z nowoczesnym wyposażeniem i uzbrojeniem. Jego główną siłą bojową była słynna 4 Kantemirowska Dywizja Pancerna Gwardii (wyposażona w czołgi T-80U). Ponadto w skład armii wchodziła 2 Tamańska Dywizja Zmechanizowana Gwardii[8] oraz 6 Częstochowska Brygada Pancerna i 27 Sewastopolska Brygada Zmechanizowana Gwardii. Ponadto jednostki artylerii, przeciwlotnicze, inżynieryjne i inne. Natomiast w strefie tylnej armii, w rejonie Jelni na Białorusi, została rozmieszczona 41 Armia Ogólnowojskowa z Nowosybirska (Centralny Okręg Wojskowy), która brała udział w ćwiczeniach „Zapad" i pozostała na obszarze prowadzonej operacji.

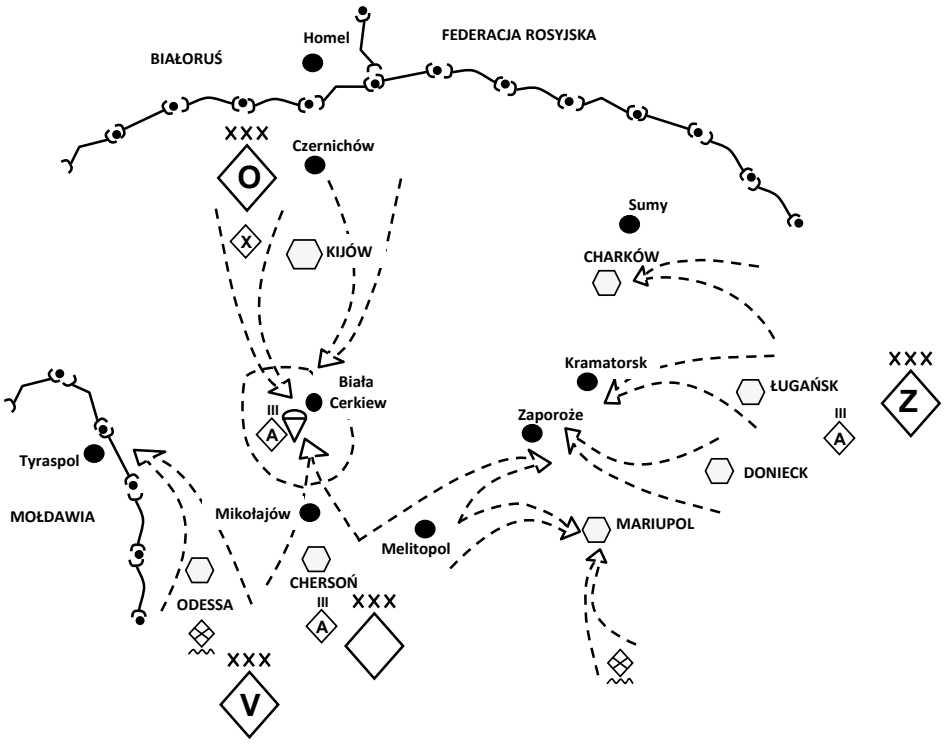
Wojska rosyjskie uderzyły z terytorium Białorusi. Nie napotykając poważniejszego oporu sił ukraińskich, podeszły do stolicy Ukrainy na odległość około 25 km. W ten sposób Rosjanie trafili na pierwszą linię jej obrony. Zajęli pozycje na północ i północny zachód od Kijowa. Walki toczyły się na przedmieściach. W samym mieście w ograniczonej skali operowały rosyjskie grupy dywersyjne i rozpoznawcze. Rosjanie rozpoczęli też okrążanie ukraińskiej stolicy od wschodu. Szczególnie ważne dla powodzenia natarcia było opanowanie lotnisk położonych w rejonie stolicy. Według informacji Sztabu Generalnego Sił Zbrojnych Ukrainy Rosjanie przeprowadzili desant na lotnisko im. Antonowa położone w miejscowości Hostomel na północny zachód od Kijowa z użyciem około 20 śmigłowców Ka-52 i Mi-8. Zaskakujący desant śmigłowcowy w połączeniu z przewagą w powietrzu umożliwił Rosjanom częściowe opanowanie lotniska. Zadaniem rosyjskich sił lądujących w pierwszym rzucie było opanowanie płyty lotniska, następnie wyjście z pasa startowego i powiększenie rejonu desantowania przez wyparcie obrońców daleko poza teren lotniska. W ten sposób siły desantowe zamierzały uniemożliwić bezpośredni ostrzał z broni przeciwpancernej i przeciwlotniczej kolejnej lądującej fali desantu. Jednak nie były w stanie pokonać i wyprzeć obrońców. W tej sytuacji atakujący zostali zablokowani na pasie startowym oraz w rejonie okolicznych zabudowań otaczających lotnisko. Obrońcy odparli atak sił desantowych, a ukraińska artyleria zniszczyła pas startowy, co uniemożliwiło lądowanie kolejnych sił desantu, w tym samolotów transportowych ze sprzętem koniecznym do wsparcia jednostek powietrznodesantowych i specjalnych. Po przegrupowaniu sił wojska ukraińskie odbiły lotnisko, jednak zniszczeniu uległy hangary i pas startowy[9]. Hostomel to strategiczny punkt otwierający dostęp do stolicy Ukrainy. W pierwszej fazie natarcia 24 lutego 2022 roku rosyjskie wojska zajęły teren elektrowni w Czarnobylu, gdzie przetrzymywały personel jako zakładników. Dopiero 21 marca, a więc trzy tygodnie po przejęciu elektrowni, pozwolono pracownikom opuścić placówkę. Dzięki temu częściowo wymieniono zespół jej obsługi.

Istotnym elementem walk na kierunku północnym była obrona Kijowa. Władze zarówno państwowe, jak i miejskie przystąpiły do przygotowania stolicy do obrony. Ukraińska obrona zakładała walkę z przeciwnikiem oraz niszczenie wojsk agresora na podejściach do miasta. Dlatego Kijów był gotowy do obrony, a dzięki okolicznym miejscowościom (Bucza, Hostomel, Irpień, Browary, Szczasływe) skutecznie odpierał kolejne ataki. Wzmocniono punkty kontrolne utworzone przed wjazdem na każdy z kijowskich mostów. Pojawiły się na nich betonowe bloki i stalowe jeże przeciwpancerne. W czasie obrony miasta użytkowano jedynie dwa mosty na Dnieprze, czyli Darnycky i Północny. Podobne blokady i punkty kontrolne pojawiły się przed wjazdem do zamkniętych osiedli mieszkaniowych. Stacje naziemne metra zostały zamknięte, natomiast stacje podziemne wykorzystano jako schrony. Władze stolicy pojęły decyzję o wprowadzeniu godziny policyjnej i zakazu wjazdu do miasta przy zachowaniu możliwości jego opuszczenia. W Kijowie zorganizowano ochotniczą obronę terytorialną. Bitwa o stolicę Ukrainy trwała od 25 lutego do 2 kwietnia 2022 roku. W trakcie walk ukraińska stolica znalazła się pod ostrzałem artyleryjskim. Dochodziło także do starć na ulicach, do ataków lotniczych oraz eliminowania rosyjskich grup dywersyjno-rozpoznawczych. Starcie zakończyło się zwycięstwem i ewakuacją wojsk rosyjskich z obwodu kijowskiego. Należy wskazać, że w ramach obrony Kijowa została zniszczona rosyjska przeprawa pontonowa w rejonie Hostomla na północny zachód od stolicy. W pierwszych dniach wojny Ukraińcy zdecydowali się na zalanie jednej z podkijowskich wsi. 25 lutego, w drugim dniu rosyjskiej inwazji, ukraińskie wojska zerwały tamę w Demidowie w obwodzie kijowskim i zalały najbliższą okolicę, uniemożliwiając ruch czołgów wroga w kierunku Kijowa. W ten sposób udało się powstrzymać ofensywę Rosjan na ukraińską stolicę. Powódź bowiem zablokowała północny kierunek natarcia na miasto na zachodnim brzegu Dniepru i odegrała kluczową rolę w marcowych walkach. Zalane tereny uniemożliwiły Rosjanom okrążenie Kijowa. Woda ze zbiornika stworzyła skutecz-

8 Obie jednostki znane są z dorocznych parad na placu Czerwonym w Moskwie, gdzie wystawiają swoje reprezentacyjne jednostki oceniane jako najlepsze w całej Rosji.

9 https://wiadomosci.wp.pl/ukraincy-odbilismy-lotnisko-w-hostomlu-pod-kijowem-6740916546534368a/.

RYS. KONCEPCJA ROSYJSKIEJ WOJSKOWEJ OPERACJI SPECJALNEJ (SCHEMAT)



Opracowanie własne.

ISTOTNYM ELEMENTEM WALK NA KIERUNKU PÓŁNOCNYM BYŁA OBRONA KIJOWA. *WŁADZE ZARÓWNO PAŃSTWOWE, JAK I MIEJSKIE PRZYSTĄPIŁY DO PRZYGOTOWANIA STOLICY DO OBRONY. UKRAIŃSKIE SIŁY ZAKŁADAŁY WALKĘ Z PRZECIWNIKIEM ORAZ NISZCZENIE WOJSK AGRESORA NA PODEJŚCIACH DO MIASTA.*

ną barierę dla czołgów i zmusiła agresora do zmiany kierunku natarcia przez teren zurbanizowany, czyli przez miejscowości Bucza, Irpień i Hostomel[10].

Rosyjskie batalionowe grupy taktyczne (BGT), które wycofały się z okolic Kijowa, prawdopodobnie mają niewielki potencjał bojowy, co można wywnioskować na podstawie liczby sprzętu, którym dysponują. Niekiedy ze składu BGT nie zostało nic poza grupą żołnierzy i być może niewielką liczbą pojazdów, które po wycofaniu muszą zostać wyremontowane lub przekazane do innych jednostek organizowanych na bazie rozbitych pododdziałów. W ocenie ekspertów straty niektórych jednostek sięgają 30%. W związku z tym są one nieskuteczne w walce. Ogólna ocena jednostek wycofywanych z rejonu Kijowa wskazuje, że większość rosyjskich sił prawdopodobnie wymaga odtworzenia zarówno stanów osobowych, jak i podstawowych środków walki.

Trzeci kierunek operacyjny – południowy. Obejmuje on obszar Krymu, gdzie stacjonowały 22 Korpus Armijny z dwoma brygadami zmechanizowanymi (jednostki obrony wybrzeża) oraz Flota Czarnomorska Rosji. Od wiosny 2021 roku był tu prawdopodobnie rozmieszczony także 56 Pułk Powietrznodesantowy[11] oraz inne jednostki. Z ukraińskiej oceny sytuacji wynika, że na Krymie znajduje się około 340 samolotów i 230 śmigłowców z 4 i 6 Armii Lotniczej i Obrony Powietrznej[12].

Wojska rosyjskie uderzyły z obszaru Krymu w kierunku: Chersoń – Biała Cerkiew oraz pomoc-

10 https://tvn24.pl/swiat/ukraina-demidow-zalana-wies-jak-powstrzymano-rosyjska-ofensywe-na-kijow-5691138/. 10.04.2022.

11 Rosyjski resort obrony 29 grudnia 2021 roku zakończył formowanie w położonej na Krymie Teodozji nowego pułku powietrznodesantowego, który wszedł w skład 7 Gwardyjskiej Dywizji Powietrznodesantowej, https://www.rp.pl/polityka/art19245411-rosja-sformowala-na-krymie-nowy-pulk-powietrzno-desantowy. Zob. także: https://defence24.pl/sily-zbrojne/rosja-odbudowuje-wojska-powietrzno-desantowe-raport/.

12 https://www.polityka.pl/tygodnikpolityka/swiat/2146446,1,czy-to-koniec-ukrainy-tak-moze-wygladac-scenariusz-inwazji.read/. 12.01.2021.

nicze siły w kierunku na Mariupol. W tym przypadku Rosjanie także nie napotkali zorganizowanego oporu wojsk ukraińskich. Informacje pozyskane z otwartych źródeł świadczą o tym, że pierwszego dnia operacji na niektórych odcinkach rosyjskie jednostki weszły na głębokość nawet kilkudziesięciu kilometrów w głąb Ukrainy, kierując się w stronę Chersonia i Mikołajewa.

Po długotrwałych walkach 3 marca 2022 roku zdobyły miasto Chersoń – stolicę obwodu. Otoczyły miasto i wykonując uderzenia wzdłuż głównych ulic, wyparły obrońców. Zajęcie miasta nie było równoznaczne z jego opanowaniem, jego mieszkańcy bowiem pokojowo protestowali przeciwko obecności rosyjskich żołnierzy. Opanowanie Chersonia sprawiło, że wojska rosyjskie utworzyły korytarz z Donbasu na Krym oraz przejęły kontrolę nad Kanałem Północnokrymskim. Został on zbudowany w latach 1961–1971 i stanowił istotny element struktury systemu wodnego, doprowadzał bowiem wodę ze Zbiornika Kachowskiego (na rzece Dniepr) na Półwysep Krymski, do miejscowości Zełenyj Jar. Stamtąd woda była transportowana specjalnym wodociągiem aż do Kerczu i Teodozji. Po aneksji Krymu przez Rosję w 2014 roku Ukraina zbudowała zaporę na kanale i odcięła dopływ wody ze Zbiornika Kachowskiego na Krym, co spowodowało jej niedobór na całym półwyspie. Po opanowaniu Chersonia 26 lutego 2022 roku tama na Kanale Północnokrymskim, która blokowała przepływ wody z Dniepru na półwysep, została wysadzona w powietrze przez Rosjan[13]. Po zajęciu miasta rozpoczęli oni tworzenie okupacyjnych organów władzy na opanowanym obszarze. Ustanowiono tu władze wojskowe, które zarządziły wyłączenie ukraińskich kanałów telewizyjnych i radiowych oraz zastąpienie ich rosyjskimi. Do wyjazdu na Ukrainę mobilizowano w Rosji funkcjonariuszy służb mundurowych, prokuratorów, a nawet pracowników sądów. Mieli oni stanowić trzon władzy na zajętych terenach, między innymi w Chersoniu, gdzie Rosjanie tworzą tzw. Chersońską Republikę Ludową. W proces jej budowy zaangażowano funkcjonariuszy rosyjskiej Federalnej Służby Bezpieczeństwa (FSB) zajmujących się operacjami informacyjno-psychologicznymi. Rosjanie w opanowanym mieście i jego okolicach rozdają pomoc humanitarną, ale tylko tym mieszkańcom, którzy przyjdą z paszportem i podpiszą zgodę na utworzenie pseudorepubliki.

Mariupol to kolejne miasto blokujące operację zaczepną sił rosyjskich. Prawdopodobnie na żadne miejsce w Ukrainie nie spadło od 24 lutego tyle bomb i żadne nie zostało do tego stopnia zniszczone. Sytuacja humanitarna w Mariupolu była tragiczna – duże grupy ludzi były pozbawione dostępu do żywności, wody i leków. Rosjanie postawili sobie za cel, by za wszelką cenę przejąć kontrolę nad miastem. Mariupol miał dla nich znaczenie nie tylko strategiczne, lecz także symboliczne. Jest to jedno z największych ukraińskich miast. Było już celem ataku Rosjan w 2014 roku. Wtedy zdobyli je separatyści, lecz siłom ukraińskim udało się miasto odbić. Teraz znów toczyły się tu krwawe walki. Mariupol to port położony nad Morzem Azowskim i ośrodek przemysłu ciężkiego. Miasto stało Rosjanom na przeszkodzie, by połączyć anektowany przed ośmioma laty Krym z separatystycznymi republikami: Doniecką i Ługańską. Zatem miasto i port mają ważne położenie strategiczne. Jego zdobycie pozwoli ustanowić lądowe połączenie Donbasu z Krymem. Kolejny powód, dla którego walki o Mariupol mają wymiar strategiczny, to jego wysoka ranga jako istotnego ośrodka gospodarczego. W mieście działały zakłady metalurgiczne oraz huty żelaza i stali, produkowano również maszyny. Szczególnie ważne dla miasta i całej Ukrainy były stocznie, które dodatkowo zyskały na znaczeniu, gdy w 2014 roku pod kontrolą separatystów znalazł się przemysłowy Donieck. Jednak Mariupol to przede wszystkim ważny port eksportowy ukraińskiej stali, węgla, kukurydzy i jęczmienia, głównie do Afryki i na Bliski Wschód. Zajęcie miasta przez Rosjan oznacza, że będą kontrolować ponad 80% ukraińskiego wybrzeża Morza Czarnego. W ten sposób odcięliby Ukrainę od handlu morskiego. Dla ukraińskiej gospodarki byłby to poważny cios. Zdobycie Mariupola przez Rosję ma także psychologiczne znaczenie dla obu stron tej wojny. Dla Kremla jest to szansa, by ogłosić sukces i zademonstrować światu, że Rosja realizuje na wojnie swoje cele. Natomiast dla Ukraińców utrata miasta jest poważnym ciosem zarówno w wymiarze militarnym, jak i ekonomicznym oraz psychologicznym.

Port w Mariupolu został odcięty pod koniec 2021 roku i mimo licznych protestów strony ukraińskiej zgłaszanych na forum międzynarodowym rosyjskie okręty wzbraniały podejście do portu i blokowały Cieśninę Kreczeńską. Należy przypomnieć, że 25 listopada 2018 roku okręty marynarki wojennej Ukrainy próbowały wpłynąć przez tę cieśninę z Morza Czarnego na Morze Azowskie. U wejścia do niej zostały zatrzymane przez rosyjski tankowiec zagradzający im przejście pod mostem Krymskim, następnie zaatakowane przez siły Służby Pogranicznej Federalnej Służby Bezpieczeństwa i Marynarki Wojennej Federacji Rosyjskiej. Wszystkie trzy ukraińskie okręty zostały przejęte przez Rosjan. Do niewoli trafiło 23 marynarzy, z których sześciu zostało rannych. Powstała sytuacja świadczy o dużej determinacji Rosji, by utrzymać Morze Azowskie jako morze wewnętrzne Federacji Rosyjskiej. Rosjanie utrudniali dostęp do ukraińskich portów nad Morzem Azowskim od czasu nielegalnego zajęcia Krymu. Symbolicznym tego przykładem było oddanie do użytku mostu nad Cieśniną Kerczeńską. Jego wysokość jest dostosowana do wymiarów rosyjskich jednostek. Jednostki większe, ukraińskie czy europejskie, mają

13 https://www.rp.pl/biznes/art35765691-rosjanie-wysadzili-tame-woda-poplynela-na-krym/. 28.02.2022.

problem z przepłynięciem pod mostem i dotarciem do portów na Morzu Azowskim. Jest to utrudnianie żeglugi nie tylko jednej ze stron konfliktu (Ukrainie), lecz także naruszenie praw innych międzynarodowych partnerów.

Na Morzu Czarnym w rejonie Odessy operowało 11 rosyjskich okrętów desantowych z Floty Czarnomorskiej, Bałtyckiej i Północnej oraz wspierające je kutry rakietowe. Okręty wyszły z Sewastopola 27 lutego. Prawdopodobnie miały wysadzić desant na wybrzeżu ukraińskim. Ostatecznie nie pozwolił na to stan morza. Wysoka fala przeszkadzała przez kilka dni i okręty desantowe powróciły na Krym. Celem przygotowywanego desantu morskiego była oczywiście Odessa, klucz do panowania na wybrzeżu czarnomorskim[14]. Do przeprowadzenia desantu Rosjanie dysponowali prawdopodobnie sześcioma jednostkami klasy Aligator i Ropucha z Floty Czarnomorskiej („Orsk", „Nikołaj Filczinkow", „Cezar Kunikow", „Nowoczerkaski", „Jamałm Azow"). Natomiast kolejnych sześć okrętów przypłynęło jako wsparcie z Floty Północnej i z Floty Bałtyckiej. Pięć z nich to jednostki klasy Ropucha („Koroliew", „Mińsk", „Kaliningrad", „Ołenogorskij Gorniak", „Georgij Pobiedonosiec"). Jedna z nich to najnowszy BDK klasy Iwan Gren („Piotr Morgunow"). Mając na uwadze zgromadzone siły, można wnioskować, że zgrupowanie okrętów desantowych w tym składzie może zabrać na pokład do 5 tys. żołnierzy piechoty morskiej, około 160 czołgów lub do 280 pojazdów opancerzonych. W skład sił biorących udział w desancie mogły wchodzić 810 Brygada Piechoty Morskiej (Sewastopol) i 382 Batalion Piechoty Morskiej (Temrjuk, obwód krasnodarski), wzmocnione jednostkami powietrzno-desantowymi i piechotą morską Floty Bałtyckiej i Północnej na pokładzie wspomnianych sześciu okrętów desantowych. W zasadzie działania mogą także wspierać mniejsze jednostki desantowe, w tym jednostki o małym zanurzeniu przeznaczone do zadań dywersyjnych[15].

WALKA W GŁĘBI OPERACYJNEJ

W ramach operacji głębokich Rosjanie zintensyfikowali ataki na ukraińskie obiekty wojskowe i przemysłowe. 10 marca zniszczono międzynarodowy port lotniczy Krzywy Róg, rodzinne miasto Wołodymyra Zełenskiego, stanowiące ważny ośrodek przemysłowy ze względu na wydobycie rudy żelaza. Rosyjskie siły powietrzne wielokrotnie atakowały wojskowe lotnisko w Łucku i Iwano-Frankiwsku[16]. Zniszczono jego infrastrukturę, czyniąc lotnisko czasowo niezdolnym do prowadzenia działalności operacyjnej. Przeprowadzono także atak rakietowy na kombinat metalurgiczny w mieście Dniepr. Na podstawie informacji amerykańskiego Departamentu Obrony można ocenić, że w ciągu pierwszych 15 dni inwazji Rosjanie mogli zrzucić na wyselekcjonowane cele na terytorium Ukrainy ponad 775 rakiet balistycznych i skrzydlatych krótkiego i średniego zasięgu[17].

W marcu Rosjanie wykorzystali lotnictwo strategiczne do wyeliminowania z obszaru operacji wysokowartościowych obiektów wojskowych. Prawdopodobnie operujący w rejonie Morza Czarnego bombowiec Tu-160 wystrzelił pociski samosterujące w kierunku lotnisk w Winnicy (Gawryszówka) i Starokonstantynowie. Oba zostały wyeliminowane z operacyjnego użycia oraz przyjmowania zaopatrzenia z zagranicy. Po rosyjskim ataku rakietowym na lotnisko w Winnicy położone w środkowej Ukrainie prezydent Wołodymyr Zełenski zwrócił się w nagraniu opublikowanym na Facebooku do Zachodu z apelem o zamknięcie przestrzeni powietrznej nad jego krajem lub przynajmniej o dostarczenie samolotów, by Ukraińcy mogli sami się bronić[18]. Rosjanie przeprowadzili także ataki lotnicze na zakłady zbrojeniowe w Żytomierzu oraz na obiekt militarny w miejscowości Ozerne, gdzie znajduje się lotnisko wojskowe[19].

Nad ranem 13 marca zostało zaatakowane Międzynarodowe Centrum Pokoju i Bezpieczeństwa pod Lwowem. Były to obiekty rozmieszczone na poligonie w Jaworowie dla zagranicznych ochotników, którzy deklarowali wolę wstąpienia do Legionu Międzynarodowego[20]. Według doniesień prasowych kilka dni wcześniej mieli tam przybyć pierwsi ochotnicy między innymi z Wielkiej Brytanii i USA[21].

Na Ukrainę zostały także skierowane jednostki Gwardii Narodowej FR. Mają one kontrolować tereny zajęte przez siły rosyjskie, zapewniając bezpieczeństwo na zapleczu walczących wojsk, a więc w strefie tylnej. Dlatego Rosgwardia nie brała udziału w pierwszych dniach ofensywy przeciwko Ukrainie. Została przemieszczona w obszar operacji dopiero wówczas, gdy Rosjanie na stałe zajęli niektóre rejony Ukrainy i próbowali je okupować, organizując

SIŁY ZBROJNE FEDERACJI ROSYJSKIEJ NIE ROZBIŁY ARMII UKRAIŃSKIEJ, NIE ZNISZCZONO JEJ POTENCJAŁU BOJOWEGO, NIE PRZEPROWADZONO DEMILITARYZACJI.

14 W 2014 roku rosyjscy dywersanci i miejscowi zdrajcy wywołali zamieszki, ale nie udało się im proklamować republiki ludowej.

15 https://polskatimes.pl/harpuny-i-neptuny-zatopia-rosyjski-desant-odessa-poza-zasiegiem-putina/ar/c1-16205333/. 3.04.2022.

16 https://forsal.pl/swiat/ukraina/artykuly/8377611,ukraina-rosjanie-atakuja-zachod-ukrainy-ostrzelano-lotniska-w-iwano-frankowsku-i-lucku.html/. 13.03.2022.

17 https://www.osw.waw.pl/pl/publikacje/analizy/2022-03-11/rosyjski-atak-na-ukraine-stan-po-15-dniach/. 12.03.2022.

18 https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8372948,lotnisko-w-winnicy-zelenski-wojna-w-ukrainie.html/. 6.03.2022.

19 https://www.wnp.pl/rynki-zagraniczne/ukraina-rosjanie-przeprowadzili-atak-lotniczy-na-zaklady-zbrojeniowe-w-zytomierzu,550307.html/. 5.03.2022.

20 https://tvn24.pl/swiat/wojna-rosja-ukraina-rosyjski-atak-na-jaworow-przy-granicy-z-polska-ostrzelano-miedzynarodowe-centrum-sil-pokojowych-i-bezpieczenstwa-5633373/. 13.03.2022.

21 Minister spraw zagranicznych Dmytro Kułeba 7 marca poinformował, że liczba wniosków składanych przez ochotników do Legionu Międzynarodowego w ukraińskich ambasadach zbliża się do 20 tys. Kandydaci do służby mieli pochodzić z 52 państw, w tym z Polski.

– bez powodzenia – nowe władze. Jednostki Rosgwardii podjęły działania pacyfikacyjne zarówno te o charakterze wojskowym, jak i policyjnym. W ten sposób uwolniły od obowiązku działań okupacyjnych wojska operacyjne. W sytuacji utrzymywania się wojsk rosyjskich przez dłuższy czas na terenach okupowanych rola Rosgwardii na pewno się zwiększy[22]. Dlatego prawdopodobnie będą kierowane na te tereny dodatkowe jej jednostki z Południowego i Zachodniego Okręgu Wojskowego w celu przejmowania kontroli nad zajętymi miejscowościami oraz zwalczania lokalnych protestów, demonstracji czy ewentualnych działań partyzanckich Ukraińców.

Warto zauważyć, że w ramach operacji głębokich Rosjanie nie wykorzystali wojsk powietrznodesantowych. Dokonywali jedynie lotniczych i rakietowych ataków na strategicznie ważne obiekty infrastruktury, m.in.: lotniska[23], zakłady naprawcze sprzętu bojowego, magazyny[24], węzły komunikacyjne czy ośrodki szkolenia (np. Międzynarodowe Centrum Operacji Pokojowych i Bezpieczeństwa w Jaworowie[25]). Rosja zapowiedziała wykonywanie w ramach operacji głębokich uderzeń rakietowo-lotniczych na transporty kolejowe i konwoje drogowe transportujące z zachodu na Ukrainę broń i amunicję oraz wyposażenie wojskowe. Może to oznaczać wzrost intensywności uderzeń bezpośrednich na obszarze zachodniej Ukrainy.

Podsumowując, należy stwierdzić, że Rosjanie przeprowadzili operację zaczepną na trzech głównych kierunkach, wprowadzając do walki zasadnicze siły wydzielone z trzech okręgów wojskowych.

W przebiegu rosyjskiej „wojskowej operacji specjalnej" należy odnotować duże postępy w ofensywie od strony Krymu. Natomiast nie udało się Rosjanom otoczyć Kijowa – ukraińska stolica pozostawała otwarta od południa, skutecznie odpierając lądowe ataki od północy i wschodu oraz neutralizując rosyjskie środki napadu powietrznego. Ciężkie i długotrwałe walki toczyły się w Donbasie. W wielu rejonach rosyjskim wojskom udawało się rozbijać siły obrońców, ale w wyniku ukraińskich kontrataków nie były w stanie utrzymać zajętego obszaru. Ponadto Rosjanie po wkroczeniu na teren Ukrainy napotkali poważne problemy logistyczne. Z jednej strony wynikały one z szybkiego tempa natarcia, z drugiej – z ukraińskich ataków na podążające za głównymi siłami jednostki logistyczne. Dopiero po kilku dniach wojska rosyjskie zmieniły sposób działania i zmniejszyły tempo przemieszczania się, co spowodowało wydłużenie okresu walki i dało armii ukraińskiej dodatkowy czas na organizację obrony na zagrożonych kierunkach.

O determinacji Ukraińców w walce z siłami rosyjskimi świadczy los flagowego okrętu marynarki wojennej Ukrainy – fregaty „Hetman Sahaidacznyj", która 24 lutego 2022 roku została zatopiona przez załogę w celu zablokowania wejścia do portu w Mikołajewie. 25 lutego siły ukraińskie przeprowadziły pierwszy poważniejszy kontratak. Zaatakowały rosyjską bazę lotniczą Millerowo pod Rostowem odległą o około 16 km od granicy. W ocenie uderzenia wskazano, że trafiła w nią co najmniej jedna rakieta balistyczna Toczka-U[26]. W wyniku ataku uszkodzona została infrastruktura lotniska[27].

ZNACZENIE INFRASTRUKTURY

W wyniku uderzeń sił rosyjskich w pierwszych dniach „wojskowej operacji specjalnej" miały zostać zniszczone 74 obiekty ukraińskiej infrastruktury militarnej, w tym 11 lotnisk, trzy stanowiska dowodzenia oraz baza floty ukraińskiej, a także 18 stacji radiolokacyjnych i kilka systemów przeciwlotniczych S-300 i Buk-M1. Atakowane były przede wszystkim cele we wschodniej części Ukrainy[28].

Od początku walk Rosjanie niszczyli infrastrukturę telekomunikacyjną. Dlatego, by umożliwić Ukraińcom dostęp do Internetu, na apel ukraińskiego prezydenta odpowiedział Elon Musk, który dostarczył partię urządzeń satelitarnego systemu Starlink. Sieć Starlink, która ma ponad 2100 satelitów na orbicie, została zaprojektowana do działania w obszarach, w których łączność jest zawodna lub całkowicie niedostępna. Uruchomiono ponad 5 tys. terminali internetowych Starlink[29], dzięki temu Ukraińcy uzyskali możliwość bezpiecznej komunikacji.

Konflikt zbrojny sprawił, że początkowo ograniczono, następnie całkowicie zamknięto cywilny ruch lotniczy. Zasadniczym powodem rezygnacji przez linie lotnicze z lotów nad Ukrainą było realne zagrożenie ostrzelania cywilnych statków powietrznych. Operatorzy przestrzeni powietrz-

22 https://tvn24.pl/swiat/rosgwardia-czy-jest-wewnetrzna-armia-putina-jak-dziala-czy-bierze-udzial-w-wojnie-w-ukrainie-liczebnosc-i-najwazniejsze-zadania-general-wiktor-zolotow-5649806/. 27.03.2022.

23 https://wiadomosci.radiozet.pl/Swiat/Rosja-zaatakowala-Lwow.-Rakiety-uderzyly-w-okolice-lotniska-i-fabryke/.

24 https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8382883,rosyjski-atak-na-magazyn-rakiet-i-amunicji-w-obwodzie-iwanofrankowskim.html/.

25 https://www.rp.pl/konflikty-zbrojne/art35855961-atak-na-poligon-w-jaworowie-rosja-zabilismy-180-najemnikow-ukraina-to-propaganda/.

26 https://www.rp.pl/konflikty-zbrojne/art35758821-ukraina-zaatakowala-rosyjska-baze-wojskowa/.

27 W mediach społecznościowych (w tym na Twitterze) pojawiły się zdjęcia i nagrania wideo z bazy lotniczej Millerowo, która stanęła w ogniu po ostrzelaniu. https://twitter.com/Liveuamap/status/1497101637109923864?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497101637109923864%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.rp.pl%2Fkonflikty-zbrojne%2Fart35758821-ukraina-zaatakowala-rosyjska-baze-wojskowa/.

28 T. Hypki, *Wojna u granic*, „Raport – Wojsko Technika Obronność" 2022 nr 3.

29 https://businessinsider.com.pl/wiadomosci/spacex-elona-muska-uruchomil-ponad-5-tys-terminali-internetowych-starlink-na-ukrainie/8el84st/.

nej pamiętali sytuację, jaka miała miejsce w czasie walk z separatystami w 2014 roku, kiedy został zestrzelony malezyjski Boeing 777. Zginęło wówczas 298 osób. Na zachodniej Ukrainie normalnie funkcjonował natomiast transport lądowy zarówno drogowy, jak i kolejowy. Dostępnych było też wiele dróg na wschodzie kraju na obszarach kontrolowanych przez siły obrońców. Sytuacja w pierwszym okresie konfliktu zbrojnego umożliwiała ograniczone funkcjonowanie gospodarki, w tym przemysłu (m.in. metalurgicznego na wschodzie), a także ewakuację ludności cywilnej z obszarów objętych działaniami wojennymi. Niestety całkowicie została zablokowana komunikacja morska. Z chwilą rosyjskiego ataku w dużych miastach rozpoczęto formowanie oddziałów obrony terytorialnej oraz wyposażanie ich w broń pochodzącą z magazynów i zagranicznych dostaw. Ponadto rozpoczęto przygotowywanie podręcznych środków walki, w tym tzw. koktajli Mołotowa. Mieszkańcy w obliczu zagrożenia powietrznego zaczęli przenosić się do piwnic, schronów i na stacje metra.

Wyjątkowego znaczenia w toku konfliktu zbrojnego nabrała kolej. Choć wojska rosyjskie podejmowały wysiłki, aby sparaliżować sieć kolejową, pociągi kursowały nadal i zapewniały zaopatrzenie dla armii oraz umożliwiały ewakuację uchodźców z zagrożonych terenów. Ukraina ma jedną z największych sieci kolejowych na świecie z niemal 20 tys. linii kolejowych. Można wnioskować, że rosyjskie problemy militarne wynikały z tego, że agresor nie był w stanie zniszczyć węzłów kolejowych i centrów logistycznych. Zasadniczym powodem, dla którego Rosjanie powstrzymali się od atakowania infrastruktury kolejowej, była prawdopodobnie koncepcja przejęcia kontroli nad nią. Wobec braku powodzenia w realizacji zakładanej koncepcji podjęli wysiłki zmierzające do zniszczenia ukraińskich stacji oraz ważnych węzłów kolejowych[30]. Mimo skoordynowanych uderzeń rakietowych Ukraińcy nadal utrzymują przejezdne niemal wszystkie szlaki kolejowe.

PODSUMOWANIE

Armia rosyjska próbowała po pierwszych niepowodzeniach militarnych odtworzyć potencjał bojowy wystarczający do wznowienia operacji zaczepnej. Jednak w związku z pogarszającą się sytuacją prawdopodobnie głównym celem działania w kolejnym etapie operacji nie będzie opanowanie wschodniej Ukrainy, lecz jedynie przejęcie i utrzymanie obwodów donieckiego i ługańskiego w ich granicach administracyjnych. Nie należy wykluczyć możliwości, że kolejnym celem strategicznym będzie opanowanie Mariupola [został już zdobyty w maju 2022 roku – przyp. red.] oraz budowa lądowego korytarza łączącego Donbas z Krymem.

Na podstawie dotychczasowych obserwacji działań podejmowanych przez armię rosyjską można stwierdzić, że w ciągu najbliższych kilku tygodni będzie miała trudności z organizacją zgrupowania uderzeniowego do prowadzenia walki w Donbasie.

Po pierwsze dlatego, że kierowane tu jednostki wycofywane z rejonu Kijowa muszą naprawić uszkodzony sprzęt bojowy oraz otrzymać dodatkowe wyposażenie.

Po drugie stan osobowy poszczególnych jednostek wymaga czasu, by odzyskać morale i utraconą wolę walki, której brak jest spowodowany zarówno niepowodzeniami, jak i stresem pola walki, a także emocjonalnym dyskomfortem utraty kolegów w wyniku poniesionych strat osobowych.

Po trzecie procesy odtwarzania gotowości bojowej trwają długo. Zatem nie da się ich zrealizować w ciągu kilku dni czy nawet tygodni. Dlatego rosyjskie jednostki wycofane z okolic Kijowa i skierowane do walki w Donbasie nie zostaną w najbliższych tygodniach w pełni odtworzone, lecz jedynie zreorganizowane na bazie istniejących batalionów. W związku z tym można wnioskować, że Rosjanie prawdopodobnie dokonają reorganizacji i przegrupowania sił zaangażowanych w dotychczasowe działania. Zatem częściowo odtworzone jednostki wojsk pancernych i zmechanizowanych zostaną wsparte artylerią i ponownie skierowane do działań ofensywnych. W tej sytuacji można przypuszczać, że zarówno ograniczony potencjał bojowych tych jednostek, jak i niskie morale sprawią, że wojska te zostaną wykorzystane do prowadzenia rozpoznania walką do czasu przemieszczenia w rejon operacji jednostek odwodowych ze składu Wschodniego i Zachodniego Okręgu Wojskowego. Należy jednak pamiętać, że zdolność bojowa jednostki to nie tylko siły i środki walki. To także czynnik niematerialny, a więc umiejętność organizowania walki oraz zdolność do działania jako zgrupowanie uderzeniowe, nie tylko jako samodzielna jednostka. Dlatego eksperci wojskowi zwracają uwagę na fakt, że nawet dobrze wyszkolona armia zawodowa potrzebuje czasu, aby przygotować operację połączoną w ramach zgrupowania zadaniowego. Przy tym rosyjscy żołnierze z poboru nie są dobrze wyszkoleni, nie mają także czasu na realizację procesu zgrywania bojowego.

Podsumowując, należy stwierdzić, że wojskowa operacja specjalna nie osiągnęła zakładanych celów. Siły Zbrojne Federacji Rosyjskiej nie rozbiły armii ukraińskiej, nie zniszczono jej potencjału bojowego, nie przeprowadzono demilitaryzacji. Ponadto nie dokonano zmiany władzy politycznej, jak również nie zapewniono ochrony ludności separatystycznych, prorosyjskich republik. Poza tym nie udało się także przeprowadzić procesu inkorporacji Ukrainy. ■

Artykuł został opracowany przez Autora w kwietniu 2022 roku.

30 https://www.wprost.pl/swiat/10698445/rosja-zbombardowala-stacje-kolejowe-na-zachodzie-ukrainy-sa-informacje-o-ofiarach.html/. 25.04.2022.

Potrzeby informacyjne w systemie bezpieczeństwa państwa

WSPÓŁCZESNE KONFLIKTY MILITARNE DOWODZĄ, ŻE UMIEJĘTNE WYKORZYSTYWANIE WŁAŚCIWEJ INFORMACJI STANOWI JEDEN Z ISTOTNYCH ELEMENTÓW BUDOWANIA PRZEWAGI INFORMACYJNEJ.

ppłk dr inż. Andrzej Mocarski

Autor jest p.o. kierownikiem Zakładu Rozpoznania Wojskowego i Walki Radioelektronicznej w Instytucie Taktyki Wydziału Wojskowego Akademii Sztuki Wojennej.

Zgodnie z obowiązującą doktryną rozpoznania wojskowego informacja jest definiowana jako *wyselekcjonowane i uporządkowane dane przekazujące znaczenie, które odpowiadają na pytania: kto, co, gdzie, kiedy. Informacje poddane analizie, przetworzeniu i porównaniu z posiadaną wiedzą tworzą produkty informacyjne*[1]. Od właściwie zdefiniowanych priorytetów informacyjnych są uzależnione zatem zarówno rozwiązania organizacyjne w systemie rozpoznania wojskowego, jak i efekty prowadzonych operacji militarnych.

Potrzeby informacyjne mają swoją wymierną wartość poznawczą wyrażaną poziomem świadomości sytuacyjnej. Tezy tej dowodzą nie tylko minione konflikty zbrojne, lecz także liczne opracowania naukowe, w których wskazuje się na konieczność właściwego kształtowania potrzeb informacyjnych.

WYDARZENIE NAUKOWE

Mając na uwadze przedstawione uwarunkowania, na Wydziale Wojskowym Akademii Sztuki Wojennej 14 kwietnia 2022 roku została zorganizowana piąta już edycja konferencji (w formie wideokonferencji) pt. *Organizacja systemu rozpoznania zagrożeń państwa*. Wiodące problemy, które na niej poruszano, to:

– potrzeby informacyjne systemu rozpoznania wojskowego w ocenie zagrożenia militarnego;

– wykorzystanie otwartych źródeł informacji na potrzeby rozpoznania zagrożeń państw;

– identyfikacja poziomu bezpieczeństwa państwa w aspekcie wiedzy o potencjalnych zagrożeniach;

– główne potrzeby informacyjne w obszarze walki radioelektronicznej w procesie uzyskiwania przewagi informacyjnej;

– wykorzystywanie wiedzy na temat konfliktów końca XX i początku XXI wieku – wnioski i doświadczenia.

W konferencji udział wzięli także przedstawiciele z innych ośrodków akademickich, w tym z: Akademii WSB (Dąbrowa Górnicza), Uniwersytetu Jana Kochanowskiego (Kielce), Akademii Kaliskiej im. Prezydenta Wojciechowskiego (Kalisz), Wyższej Szkoły Menedżerskiej (Warszawa), Wyższej Szkoły Finansów i Zarządzania (Białystok), Mazowieckiej Uczelni Publicznej (Płock). Uczestniczyli w niej też

1 *Doktryna rozpoznania wojskowego D-2(B)*, CDiSzSZ, Bydgoszcz 2020, s. 107–108.

przedstawiciele sił zbrojnych, w tym zastępca szefa Zarządu Analiz Wywiadowczych i Rozpoznawczych P-2 SGWP, Zarządu Rozpoznania i Walki Radioelektronicznej J2 DORSZ, dowódcy pułków rozpoznawczych, przedstawiciele ośrodków radioelektronicznych oraz szefowie G-2 związków taktycznych.

Konferencję rozpoczęło wystąpienie dziekana Wydziału Wojskowego Akademii Sztuki Wojennej płk. dr. Jacka Joniaka. Powitał on wszystkich jej uczestników i podkreślił znaczenie obecnego wydarzenia naukowego w procesie doskonalenia systemu rozpoznania wojskowego. Wskazał też na konieczność wykorzystywania doświadczeń i modyfikacji obowiązujących rozwiązań w praktyce dydaktycznej i naukowej Wydziału.

Następnie głos zabrał zastępca szefa Zarządu Analiz Rozpoznawczych i Wywiadowczych P-2 SGWP, który podkreślił szczególne znaczenie właściwego generowania potrzeb informacyjnych, umożliwiających wyprzedzające i trafne rozpoznanie zagrożeń dla bezpieczeństwa państwa. Jest to warunek *sine qua non* opracowania skutecznych planów reagowania państwa na zagrożenia. W swoim wystąpieniu przytoczył też jeden z imperatywów naszych sił zbrojnych, wskazany przez szefa Sztabu Generalnego, a mianowicie *wyprzedzającą bitwę rozpoznawczą*, rozumianą jako działania informacyjne i przedsięwzięcia ostrzegawcze (Intelligence and Warning – I&W). Podkreślił, że wojna informacyjna zawsze będzie elementem wyprzedzającym, a bez informacji nie można zaplanować żadnych działań. Zwrócił uwagę na to, że rozpoznanie i wywiad w systemie bezpieczeństwa państwa zawsze będą odgrywać zasadniczą rolę, dostarczając informacji o zagrożeniach dla decydentów. Stwierdził, że w opinii szefa SGWP wyprzedzająca bitwa rozpoznawcza jest rozgrywana już teraz, a środowisko informacyjne staje się kluczowym elementem środowiska operacyjnego. Istotna zatem jest nie tylko budowa fizycznego systemu zapewniającego pozyskiwanie danych i informacji o sytuacji, lecz także systemu zarządzania wymaganiami rozpoznawczymi (uwzględniając właściwe definiowanie potrzeb informacyjnych).

PIERWSZY PANEL

Prowadzący go prof. dr hab. Marek Wrzosek przypomniał zasadniczy temat konferencji – priorytetowe potrzeby informacyjne – i podkreślił złożoność problematyki z nim związanej.

Jako pierwszy wystąpił prof. dr hab. Bernard Wiśniewski. Przedstawił on kwestie metodologiczne oraz praktyczne związane z przygotowaniami obronnymi elementów ochronnych systemu obronnego państwa, które funkcjonują pod zwierzchnictwem ministra spraw wewnętrznych i administracji (MSWiA). Przypomniał interpretację terminów odnoszących się do systemu obronnego państwa, określając tym samym podstawy dalszych rozważań. Ponadto wskazał zasadnicze rozwiązania prawne dotyczące funkcjonowania elementów obronnych państwa oraz przedstawił zadania resortu spraw wewnętrznych i administracji (który jest zaliczany do elementów ochronnych systemu obronnego) w warunkach zewnętrznego zagrożenia państwa i wojny. Zwrócił uwagę, że resort w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa realizuje osiem obszarów zadaniowych, takich jak: ochrona informacji niejawnych, maskowanie bezpośrednie i operacyjne, przekazywanie informacji społeczeństwu, ostrzeganie i alarmowanie, zapewnienie obiegu poczty specjalnej oraz bezpośrednia ochrona obiektów i osób sprawujących kierownicze funkcje w państwie. Wykonuje również zadania związane z zapewnieniem bezpieczeństwa i porządku publicznego oraz ochroną przeciwpożarową i działaniami ratowniczymi. Referujący zaznaczył, że w warunkach wojny katalog tych zadań znacznie się zwiększa, zmienia się także ich kolejność.

W swojej wypowiedzi zwrócił również uwagę na to, że w procesie planowania obronnego problemy odnoszące sie do pozyskiwania informacji nie dotyczą tylko zagrożeń, lecz również i symptomów, czyli zdarzeń nadzwyczajnych postrzeganych w kategoriach skutków. Niezwykle istotną kwestią związaną z wiedzą i informacją są zadania resortu spraw wewnętrznych i administracji w zakresie odnoszącym się do systemu kierowania bezpieczeństwem narodowym.

Drugi prelegent, którym był dr hab. Andrzej Dawidczyk, w swoim wystąpieniu skupił się na identyfikacji zagrożeń w środowisku bezpieczeństwa państwa pod kątem projektowania strategii wojskowej. Przedstawiając strategiczne spojrzenie na identyfikację zagrożeń, podkreślił, że w środowisku bezpieczeństwa występuje bardzo duża liczba różnorodnych zagrożeń, które należy brać pod uwagę. Według niego nie możemy uwzględniać tylko tych najważniejszych czy też najsilniejszych sygnałów płynących ze środowiska bezpieczeństwa i na tej podstawie wypracowywać cele, do których osiągnięcia tworzyć koncepcje realizacyjne, ponieważ skuteczność prognoz opartych na identyfikacji kilkunastu zagrożeń jest bardzo niska. Dlatego też analiza strategiczna na poziomie państwa wymaga uwzględnienia całej złożoności otoczenia, czyli wszystkich zachodzących procesów i zdarzeń, nie tylko tych, które naszym zdaniem są najważniejsze.

Według prelegenta zagrożenia militarne bezpieczeństwa państwa, które mogą wystąpić za pięć, dziesięć czy piętnaście lat, są rezultatem kumulowania się różnych zagrożeń pierwotnych, które się ze sobą łączą, wpływając wzajemnie na siebie oraz wspólnie występując charakteryzują się pewną dynamiką. Przy tym podejściu wszystkie zidentyfiko-

wane zagrożenia stanowią podstawę planistyczną (żadnych zagrożeń nie pomijamy, nie odrzucamy). Przedstawiono również metody grupowania danych, które umożliwiają ich agregację i wyprowadzanie wniosków odnoszących się do kierunków i rozwoju w długich okresach.

Prelegent zaprezentował też metodę grupowania danych „k-means" (k-medoids), która umożliwia łączenie dużej liczby zagrożeń w określone klasy, pozwalając nie tylko na porządkowanie obrazu środowiska bezpieczeństwa państwa, lecz także na projektowanie celów politycznych i strategicznych, uwzględniających wpływ wielu czynników jednocześnie. Produktem analizy jest kompleks zagrożeń zagregowanych do postaci umożliwiającej ich operacjonalizację.

Kolejnym referującym był dr hab. Waldemar Scheffs, który skupił się na praktycznym sposobie wykorzystania bazy danych emiterów do osiągnięcia zakładanych celów. Zwrócił uwagę na to, kto tę bazę danych zasila i kto z niej korzysta oraz kto mógłby ją zasilać (czy też powinien). W czasie pokoju odbiorcami bazy danych są m.in.: okręty, które mają swoje radiolokatory identyfikacyjne, systemy obrony powietrznej, systemy telekomunikacyjne oraz walki radioelektronicznej. Doktor Scheffs przedstawił również ogólną budowę bazy danych emiterów, a także scharakteryzował ich parametry techniczne (te występujące w metrykach i dane pomiarowe) i analityczne (taktyczne wykorzystanie emitera, parametry skojarzeniowe), które ta baza zawiera. Złożoność ukazanego problemu wymaga odmiennego podejścia do procesu budowy potrzeb informacyjnych. W swoim wystąpieniu postawił tezę, że ze względu na dużą różnorodność środków emitujących energię elektromagnetyczną nie jest możliwe sklasyfikowanie ich wszystkich. Zwrócił uwagę na to, że baza danych czy też bazy danych, którymi dysponujemy, są przygotowane na czas pokoju i kryzysu, ale niestety nie na czas wojny. W czasie wojny musi wystąpić element rozpoznania, czyli wskazania miejsca występowania emitera. Zaznaczył, że podczas oceny sytuacji elektronicznej informacje z bazy danych emiterów powinny być łączone z wzorcami doktrynalnymi działania środków elektronicznych. W procesie dowodzenia, w którym generowane są potrzeby informacyjne, dane z bazy danych emiterów będą wykorzystywane do ustalenia priorytetowych obiektów do oddziaływania na nie w konkretnym czasie. Odniósł się również do aktualnej sytuacji w Ukrainie, przedstawiając prowadzone tam działania w kontekście rozpoznania radioelektronicznego oraz walki radioelektronicznej.

Kolejny referujący, gen. bryg. rez. dr Andrzej Tuz, nawiązał do potrzeb informacyjnych rozpoznania w dwóch aspektach: w czasie przygotowania polskiego kontyngentu wojskowego do udziału w operacji poza granicami kraju oraz w trakcie ich realizacji. Szczegółowo sprecyzował, jakie informacje są potrzebne podczas przygotowania kontyngentu, komu są potrzebne i dlaczego. Zwrócił uwagę na potrzeby informacyjne odnoszące się do sposobów działania potencjalnego przeciwnika, wykorzystywanego przez niego sprzętu i wyposażenia oraz jego silnych i słabych stron. Informacje te mają istotne znaczenie w planowaniu i prowadzeniu szkolenia, gdyż przygotowując żołnierzy i pododdziały, powinniśmy uczyć ich takich sposobów działania, które będą skuteczne podczas wykonywania zadań (będą odpowiedzią na działanie przeciwnika). Podkreślił też znaczenie systemu zbierania i upowszechniania doświadczeń. Zaznaczył, że w odniesieniu do PKW system ten nie zawsze działał właściwie, ponieważ gros informacji nie docierało do dowódców jednostek przygotowujących kolejne kontyngenty.

POTRZEBY INFORMACYJNE MAJĄ SWOJĄ WYRAŻANĄ POZIOMEM ŚWIADOMOŚCI

Następny prelegent, dr hab. Mirosław Banasik, skupił się na sposobach podejścia podczas oceny zagrożeń, wyróżniając trzy zasadnicze z nich, czyli: podmiotowy (kto i co?), scenariuszowy (jak?) oraz zdolnościowy (jakie efekty?). Charakteryzując podejście podmiotowe, odniósł się do zagrożeń klasycznych oraz asymetrycznych. Zwrócił uwagę na to, że w podejściu tradycyjnym w wypadku działań asymetrycznych niemożliwe jest zidentyfikowanie najbardziej prawdopodobnego i najbardziej niebezpiecznego wariantu działania przeciwnika. Z kolei metoda scenariuszowa nie wymaga posiadania tak dużej ilości informacji szczegółowych o przeciwniku jak w podejściu tradycyjnym. Powstałe w efekcie jej zastosowania produkty planistyczne są dostosowane tylko do wyselekcjonowanych scenariuszy, nie odpowiadają za szeroką gamę możliwych zagrożeń. Metoda zdolnościowa pozwala natomiast budować na dowolnym poziomie dowodzenia wykaz zdolności oraz na szybko przygotować odpowiedzi na zagrożenia. Charakteryzując podejście zdolnościowe do oceny zagrożeń, przedstawił trzy modele oceny realizowane w ramach tej metody,

a mianowicie model: taksonomiczny, atrybutowy i linii operacyjnych.

DRUGI PANEL

Poprowadził go dyrektor Instytutu Działań Informacyjnych Wydziału Wojskowego. Jako pierwszy zaprezentował się na nim dr Józef Kozłowski. Na wstępie przedstawił on rozumienie terminu *Crowdsourcing*, który polega na angażowaniu szerokiej grupy ludzi (internautów) do wykonywania zadań i proponowaniu rozwiązań, aby osiągnąć konkretne cele organizatora. Wymaga to trzech najważniejszych elementów: organizacji przygotowanej do podjęcia działania, stworzenia społeczności gotowej do wzięcia udziału w projekcie oraz zapewnienia wszystkim chętnym możliwości wzięcia w nim udziału. Prelegent wyróżnił cztery rodzaje crowdsourcingu: zbieranie i zarządzanie danymi, informacją i wiedzą, szukanie rozwiązań, szukanie i weryfikacja rozwiązań oraz analiza rozproszona. Zdaniem referującego dla struktur wywiadowczych i rozpoznawczych najważniejszym rodzajem jest zbieranie i zarządzanie danymi, informacją i wiedzą. Zasugerował podjęcie dyskusji na temat ewentualnej możliwości powstania nowego rodzaju działań rozpoznawczych *Crowdsourcing Intelligence*, których zadaniem byłoby gromadzenie określonych informacji, odpowiadających zapotrzebowaniu struktur państwa. Stwierdził też, że dalsze badania w wymiarze akademickim powinny się skupić na metodzie KBM w odniesieniu do Crowdsourcingu w strukturach rozpoznawczych i instytucjach wywiadowczych. Dotyczyć one powinny rozwoju nowych zdolności do generowania i testowania hipotez, modelowania procesów analitycznych, wstępnego przetwarzania danych, ich selekcji i analizy oraz budowania autonomicznych zdolności systemu rozpoznania i wywiadowczego.

Doktor inż. Stanisław Lipski zaprezentował z kolei potrzeby informacyjne dla zagrożeń uderzeniami pocisków rakietowych z platform mobilnych. Stwierdził, że w większości są one zautomatyzowane i posiadają sztuczną inteligencję, mają też zdolności autonomiczne i mogą funkcjonować w roju. Zwrócił uwagę na czas reakcji od wydania rozkazu do oddania strzału, który jest bardzo krótki, i wynosi od 2 do 10 min. Jego zdaniem, w odniesieniu do potrzeb informacyjnych, dotyczących zagrożeń uderzeniami pocisków rakietowych z platform mobilnych, musimy posiadać wiedzę na temat nowoczesnych technologii (tych dopiero tworzonych i będących przedmiotem badań), ich budowy, układów, z których się składają, wykorzystywanych algorytmów oraz sposobu działania. Podkreślił zmianę charakteru działań wojennych w odniesieniu do uderzeń pocisków rakietowych z platform mobilnych, wynikającą ze wzrostów prędkości, zasięgu, ładowności, manewrowości, elastyczności oraz sieciocentryczności. Stwierdził, że nasze siły zbrojne dysponują ograniczonymi zdolnościami związanymi z wykrywaniem rakietowych wyrzutni mobilnych i obecnie prawie niemożliwe jest monitorowanie lokalizacji mobilnych wyrzutni i okrętów podwodnych z pociskami rakietowymi w czasie rzeczywistym. Dlatego też niemożliwe jest również wykonanie uderzenia wyprzedzającego na przeciwnika.

Z kolei dr Wojciech Wasilewski zaprezentował swoje przemyślenia na temat pozyskiwania i analizy informacji z otwartych źródeł w procesie planowania ochrony ludności. Rozpoczynając wystąpienie, zwrócił uwagę na to, że ochrona ludności jest jednym z elementów systemu bezpieczeństwa narodowego. Natomiast czynnikiem wpływającym na nią jest informacja (pozyskiwanie, analizowanie, przetwarzanie i dystrybuowanie). Zaznaczył, że system ogólnodostępnych źródeł informacji stanowi szansę dla odporności społeczeństwa na zagrożenia w wypadku zagrożeń niemilitarnych, a jednocześnie ryzyko w razie zagrożenia militarnego. Zdaniem referującego w razie zagrożenia militarnego i prowadzonych działań zbrojnych ogólnodostępne źródła informacji mogą być czynnikiem zwiększającym zdolność państwa do ochrony, ale mogą również tę zdolność osłabiać (szanse oraz ryzyko). Stwierdził też, że zmieniające się środowisko bezpieczeństwa wymaga adekwatnego przygotowania systemu ochrony ludności, uwzględniającego rodzaj i skalę występujących zagrożeń. Planowanie ochrony ludności powinno odpowiadać współczesnemu środowisku informacyjnemu i zdolności pozyskiwania z niego danych.

WYMIERNĄ WARTOŚĆ POZNAWCZĄ SYTUACYJNEJ

PANEL TRZECI

Moderował go dr hab. Waldemar Scheffs, zapraszając płk. dr. Jarosława Wiśniewskiego do zaprezentowania zasadniczych potrzeb informacyjnych dowódcy na kanwie wojny między Ukrainą a Rosją (2022). Swoje wystąpienie rozpoczął od umiejscowienia podstawowych potrzeb informacyjnych w cyklu decyzyjnym procesu dowodzenia. Mówiąc

o otwartych źródłach informacji, wskazał na: literaturę dotyczącą podobnych konfliktów w przeszłości oraz szeroko pojęty Internet, radio i telewizję (w tym opinie ekspertów). Przedstawił wiedzę pozyskaną tylko z otwartych źródeł informacji w formie meldunku, który miał następujący układ: informacja ogólna, informacja w zakresie PMESII, w tym aktualna sytuacja operacyjno-taktyczna, oraz przewidywane działania strony rosyjskiej. Dodatkowo odniósł się do prowadzonych przez obie strony działań informacyjnych. Zwrócił uwagę na to, że strona ukraińska bardzo przestrzega, by do otwartych źródeł nie trafiały informacje na temat sposobów działania oddziałów i pododdziałów ich armii. Ocenił efektywność pozyskiwania zasadniczych potrzeb informacyjnych na bazie OSINT: na poziomie strategicznym – dobra, na poziomie operacyjnym – ograniczona, czasem zadowalająca, natomiast na poziomie taktycznym – znacznie ograniczona, wręcz niemożliwa.

Z kolei dr Dariusz Żyłka, omawiając potrzeby informacyjne systemu obrony powietrznej państwa, podkreślił znaczenie pozyskiwania informacji w czasie rzeczywistym. Zadanie to wykonują radary, samoloty AWACS, satelity, rozpoznanie elektroniczne oraz wzrokowe. Dlatego też potrzeby informacyjne są bardzo istotne w aspekcie realizacji dwóch zasadniczych funkcji tego systemu, tzn. informowania o zagrożeniu powietrznym oraz rażenia. Bardzo ważny jest ciągły rozwój technologiczny i zmieniający się charakter działania środków napadu powietrznego, które powodują konieczność nadążania systemu obrony powietrznej za coraz to nowymi trendami i wyzwaniami.

Kolejnym czynnikiem warunkującym potrzeby informacyjne jest zwiększający się poziom rozwoju technologii stosowanych w obronie powietrznej umożliwiający, z jednej strony większą jej skuteczność, z drugiej zaś wymagający coraz więcej wyrafinowanej i wyselekcjonowanej informacji. Wyzwaniem jest nie tylko walka z samolotami, które mogą osiągać prędkości ponaddźwiękowe, lecz także i z rakietami balistycznymi oraz wprowadzanymi do użycia pociskami hipersonicznymi.

Referujący zwrócił uwagę na to, że podstawowa potrzeba informacyjna systemu obrony powietrznej sprowadza się do wykrycia celu powietrznego oraz do jednoczesnego zachowania wiedzy o własnych obiektach powietrznych. Potem niezbędne jest stałe śledzenie tych dwóch kategorii obiektów powietrznych i przekazywanie informacji o nich bez opóźnień w czasie rzeczywistym na stanowiska dowodzenia.

Następnie głos zabrał dr Robert Janczewski. Zaprezentował on potrzeby informacyjne w procesie oceny cyberzagrożeń. Wyjaśnił też rozumienie takich terminów, jak: *cyberryzyko*, *cyberzagrożenie*, *podatność na cyberzagrożenie*, *ocena cyberzagrożeń*. Zwrócił uwagę na to, że dzisiaj mamy taką sytuację, w której jest coraz więcej danych, a jednocześnie coraz mniej informacji. Zdaniem referującego w procesie oceny cyberzagrożeń istotne znaczenie ma posiadanie wiedzy (informacji) na temat charakterystyki własnego systemu teleinformatycznego, informacji dotyczących elementów składowych tego systemu (są one w przekonaniu referującego dynamiczne, zmienne) oraz jego zasobów (typizacja tych zasobów). Ogromne znaczenie w procesie oceny cyberzagrożeń ma też zidentyfikowanie podatności systemu na zagrożenia. Ocenia się je, stosując różnego rodzaju testy bezpieczeństwa (penetracyjne i podatnościowe). W opinii dr. R. Janczewskiego ważne są wnioski z analiz pokontrolnych systemu teleinformatycznego (wyniki kontroli bieżących, planowych, prewencyjnych, detekcyjnych). Referujący wymienił i scharakteryzował jeszcze wiele innych potrzeb informacyjnych istotnych w procesie oceny cyberzagrożeń.

Na zakończenie panelu mgr Kamil Sawicki zaprezentował geopolityczne uwarunkowania bezpieczeństwa Polski w obliczu wojny w Ukrainie. Referujący na wstępie przedstawił teorie (myśli, koncepcje) geopolityczne, które stanowiły podstawę jego rozważań. Omawiając geopolityczną mapę XXI wieku, zwrócił szczególną uwagę na interesy takich mocarstw, jak Rosja i Stany Zjednoczone. Na koniec przedstawił aktualną sytuację geopolityczną naszego kraju, jaka wystąpiła po wybuchu wojny w Ukrainie.

Po zakończeniu panelu przewodniczący komitetu naukowego prof. dr hab. Marek Wrzosek zainicjował dyskusję odnoszącą się do treści poruszonych przez prelegentów podczas poszczególnych paneli. Złożoność problematyki sprawiła, że konieczne było jej ograniczenie jedynie do zasadniczych kwestii. W rozmowach odniesiono się do zagadnień wykorzystania walki radioelektronicznej (w tym systemów walki radioelektronicznej przez stronę rosyjską) w wojnie w Ukrainie. Kolejne omawiane problemy dotyczyły problematyki związanej z obroną przed pociskami hipersonicznym oraz uzyskania zdolności do wykrywania mobilnych wyrzutni rakietowych. Na zakończenie dyskusji prowadzący zachęcił jej uczestników, w tym także gości, do pozostawienia trwałego śladu prowadzonych rozważań na piśmie. Materiały, które zostały wygłoszone, zostaną w najbliższym czasie opublikowane nakładem Akademii Sztuki Wojennej.

PODSUMOWANIE

Konferencja stanowiła szeroką płaszczyznę wymiany poglądów oraz doświadczeń. Umożliwiła też przedstawienie najnowszych wyników badań naukowych w zakresie objętym tematem przedsięwzięcia. Udział w tym spotkaniu był szczególnie interesujący i inspirujący dla specjalistów, którzy bezpośrednio zajmują się zagadnieniami związanymi z bezpieczeństwem państwa. ■

Generał do zadań specjalnych

BYŁ AMBITNYM OFICEREM ARTYLERII O OGROMNYM DOŚWIADCZENIU WOJENNYM ZDOBYTYM W DZIAŁANIACH BOJOWYCH NA KILKU FRONTACH WIELKIEJ WOJNY, CO UMIEJĘTNIE POTRAFIŁ SPOŻYTKOWAĆ W CZASIE WALK O NIEPODLEGŁOŚĆ I GRANICE RZECZYPOSPOLITEJ W LATACH 1918–1920.

płk dr hab. Juliusz S. Tym

Autor pełni służbę na stanowisku profesora w Instytucie Strategii Wojskowej Wydziału Wojskowego ASzWoj.

W1918 roku do odradzającego się po latach zaborów Wojska Polskiego zgłaszali się oficerowie, którzy wcześniej pełnili służbę w armiach zaborczych. Część z nich okazała się wybitnymi dowódcami, których wiedza i umiejętności zostały zweryfikowane w surowym egzaminie wielkiej wojny, jak określano wówczas I wojnę światową. Oficerowie ci opinie, na które wówczas zapracowali, potwierdzili w walkach o niepodległość i granice Rzeczypospolitej. Wśród tych, którzy posiadali stopnie generalskie zdobyte na frontach I wojny, jednym z najwybitniejszych był wywodzący się z armii austro-węgierskiej Jan Romer.

PIERWSZE KROKI

Jan Edward Romer urodził się 3 maja 1869 roku we Lwowie, w rodzinie starosty lwowskiego Edmunda Romera i Ireny Körtvelyessy de Augusth. Był starszym bratem profesora Eugeniusza Romera, wybitnego polskiego geografa. Ukończył I Gimnazjum w Nowym Sączu. W 1887 roku rozpoczął naukę w austriackiej Wojskowej Akademii Technicznej funkcjonującej w dzielnicy Mödling w Wiedniu, którą ukończył w roku 1890. Został wówczas promowany na pierwszy stopień oficerski – podporucznika w korpusie oficerów artylerii i rozpoczął służbę w austriackim 11 Pułku Haubic Polowych, który jako jednostka artylerii korpuśnej stacjonował we Lwowie. W 1893 roku, jeszcze jako podporucznik, usiłował zdać egzamin do Akademii Sztabu Generalnego. Nie dostał się, ale w roku następnym już jako porucznik zdał egzaminy i został przyjęty. W 1896 roku po ukończeniu Akademii z oceną bardzo dobrą jako oficer Sztabu Generalnego otrzymał przydział służbowy właśnie do tej instytucji, stanowiącej centralny organ planowania strategicznego i dowodzenia siłami zbrojnymi monarchii austro-węgierskiej. W Sztabie Generalnym służył sześć lat.

Jan Romer był oficerem o dużych ambicjach zawodowych, sumiennie podchodzącym do obowiązków służbowych wynikających z zajmowanych stanowisk. Dbał zarówno o rozwój umysłowy, jak i tężyznę fizyczną, czego dowodem czynne uprawianie jazdy konnej, szermierki oraz modnej wówczas turystyki górskiej. Grał także w tenisa.

W 1902 roku wyznaczono go na stanowisko zastępcy szefa sztabu XV Korpusu w Sarajewie, a w roku 1909 został zastępcą dowódcy stacjonującego w Osieku w Sławonii 38 Pułku Armat Polowych ze składu XIII Korpusu. W tym samym roku przeniesiono go jednak do 32 Pułku Armat Polowych wchodzącego w skład 11 Brygady Artylerii Polowej będącej jednostką 11 Dywizji Piechoty. Pułk ten stacjonował we Lwowie. W tym czasie Jan Romer nawiązał kontakty z polskim tajnym ruchem niepodległościowym,

który w owych czasach intensywnie rozwijał się na terenie Galicji[1].

WIELKA WOJNA

W dniu 29 listopada 1913 roku ppłk Szt. Gen. Jan Romer został wyznaczony na stanowisko dowódcy 11 Pułku. W roku 1914 awansował na stopień pułkownika. Na czele tego oddziału brał udział w początkowych kampaniach I wojny światowej na froncie wschodnim. Jesienią 1915 roku wraz z pułkiem znalazł się na froncie włoskim, by po zakończeniu kampanii jesiennej ponownie znaleźć się na froncie wschodnim. W maju 1916 roku płk Szt. Gen. Jan Romer został wyznaczony na dowódcę 50 Brygady Artylerii Polowej w 50 Dywizji Piechoty w składzie XV Korpusu walczącego na froncie włoskim.

Po manifeście dwóch cesarzy ogłoszonym 5 listopada 1916 roku zgłosił swój akces do służby w Legionach Polskich. W związku z jego kandydaturą na dowódcę artylerii Legionów od 10 lutego do 1 maja 1917 roku przebywał w Warszawie.

Ponieważ nie doszło wówczas do utworzenia sił zbrojnych przyszłego państwa polskiego, w pierwszej dekadzie maja powrócił na front włoski, gdzie objął dowództwo 18 Brygady Artylerii Polowej. 6 lutego 1918 roku został awansowany na stopień generała majora ze starszeństwem z dniem 1 listopada 1917 roku i wyznaczony na stanowisko dowódcy artylerii IX Korpusu[2]. Należy zaakcentować, że na przełomie 1917 i 1918 roku zaczęła się wojenna sława gen. Romera jako specjalisty od zadań niewykonalnych. Coraz częściej nowo mianowanemu generałowi powierzano dowodzenie zgrupowaniami taktycznymi broni połączonych, jak określano taktyczne grupy bojowe. Dzięki temu zdobył praktyczne doświadczenie wojenne w dowodzeniu brygadą piechoty, brygadą górską oraz dywizją piechoty. Jako etatowy dowódca IX Brygady Górskiej został 3 listopada 1918 roku wzięty do niewoli brytyjskiej.

W ARMII POLSKIEJ

Z niewoli zwolniono go pod koniec listopada 1918 roku, a już 5 grudnia przybył do Krakowa, gdzie zgłosił się do służby w Wojsku Polskim. Następnie udał się do Warszawy, po czym powrócił po krótkim urlopie do Lwowa. Tam pod koniec drugiej dekady grudnia 1918 roku został wyznaczony na stanowisko dowódcy Okręgu Generalnego „Lublin". Służbę na tym stanowisku pełnił tylko dwa tygodnie, ponieważ z rozkazu naczelnego wodza Józefa Piłsudskiego objął 5 stycznia 1919 roku dowództwo Grupy Operacyjnej „Bug", czyli improwizowanego zgrupowania taktycznego, którego zadaniem było prowadzenie działań zaczepnych przeciwko oddziałom ukraińskim na kierunku Włodzimierz Wołyński – Sokal – Kamionka Strumiłowa w celu opanowania tych miejscowości oraz linii Bugu na północny wschód od Lwowa. Generał ocenił, że w ówczesnym położeniu główny wysiłek powinien być skupiony na prawym skrzydle ugrupowania jego wojsk, na kierunku Rawa Ruska – Żółkiew – Lwów. Odzwierciedleniem jego zamiaru był plan operacji, który zyskał aprobatę Naczelnego Wodza, a w dniach 7–10 stycznia 1919 roku został z sukcesem zrealizowany. Dzięki temu 10 stycznia 1919 roku gen. Jan Romer na czele swoich wojsk wkroczył do Lwowa po przełamaniu pierścienia okrążenia ukraińskiego na północ od miasta na odcinku od Brzuchowic do Dublan. Kolejne działania Grupy Operacyjnej „Bug" to wiele walk stoczonych między Rawą Ruską a Bełzem i Krystynopolem. Charakterystyczną cechą działań prowadzonych wówczas przez oddziały grupy była duża aktywność połączona z nieustannym przejmowaniem inicjatywy. Szereg wypadów na elementy ubezpieczeń przeciwnika oraz uderzeń na pojedyncze oddziały ukraińskie prowadzono przeważającymi siłami z kilku kierunków jednocześnie w celu zadania przeciwnikowi jak największych strat przy jak najmniejszych własnych. Stanowiło to zaprawę bojową zarówno dla dowódców, jak i żołnierzy. Tak prowadzone działania miały demoralizować oddziały ukraińskie, a w żołnierzach wojsk własnych kształtować świadomość przewagi nad przeciwnikiem, wyrabiać inicjatywę i aktywność oraz wytrzymałość psychofizyczną.

W dniu 17 marca 1919 roku gen. Jan Romer został wyznaczony na stanowisko szefa Polskiej Misji Wojskowej Zakupów w Paryżu, której zadaniem było pozyskanie uzbrojenia, amunicji i sprzętu wojskowego, a także koni na potrzeby Wojska Polskiego. Służbę na tym trudnym i odpowiedzialnym – przede wszystkim ze względów finansowych – stanowisku pełnił do 24 listopada 1919 roku.

Po powrocie do Polski 17 grudnia 1919 roku objął stanowisko dowódcy 13 Dywizji Piechoty, czyli związku taktycznego wywodzącego się z 1 Dywizji Strzelców Armii Polskiej we Francji, która przybyła do kraju wiosną 1919 roku i po połączeniu z nowo formowanymi oddziałami otrzymała nowy numer i nazwę. Dywizja została skierowana na front wojny z bolszewicką Rosją i weszła w skład Frontu Wołyńskiego. W dniu 1 stycznia 1920 roku naczelny wódz Józef Piłsudski w uznaniu zasług na stanowisku dowódcy Grupy Operacyjnej „Bug" odznaczył gen. Jana Romera Krzyżem Srebrnym Orderu Virtuti Militari i wyznaczył na członka Kapituły Tymczasowej Orderu[3].

UKRAIŃSKA EPOPEJA

W czasie przygotowań do operacji zaczepnej Wojska Polskiego na Ukrainie gen. Jan Romer zo-

1 W.M. Borzemski, *Pamiętnik tajnych organizacji niepodległościowych na terenie byłej Galicji w latach 1880–1897*, Lwów 1930, s. 190.

2 *Ranglisten des Kaiserlichen und Königlichen Heeres 1918*, Wien 1918, s. 43.

3 Rozkaz Naczelnego Wodza z 1 I 1920 r., „Dziennik Rozkazów Ministerstwa Spraw Wojskowych" 1920 nr 1, poz. 1.

stał wyznaczony na stanowisko generalnego inspektora służb, jednak 13 kwietnia 1920 roku dość niespodziewanie objął stanowisko dowódcy Dywizji Jazdy – związku taktycznego, którego w odrodzonym Wojsku Polskim dotychczas nie było. Stało się tak dlatego, że Józef Piłsudski uznał, iż żaden z ówczesnych dowódców brygad jazdy nie spełnia jego oczekiwań, jeżeli chodzi o umiejętności dowodzenia dwubrygadową dywizją tego rodzaju broni. Natomiast gen. Romer w ciągu ostatnich kilkunastu miesięcy I wojny światowej wyrobił sobie markę specjalisty od zadań niewykonalnych, a w czasie kilkunastu miesięcy służby w Wojsku Polskim swoimi czynami potwierdził tę opinię, czym zdobył zaufanie Naczelnego Wodza. Ten na stanowisko szefa sztabu dywizji wyznaczył oficera Adiutantury Generalnej Naczelnego Dowództwa Wojska Polskiego mjr. Szt. Gen. Tadeusza Piskora, oficera piechoty wywodzącego się z Legionów, szefa sztabu Grupy Jazdy płk. Beliny-Prażmowskiego w wyprawie wileńskiej w kwietniu 1919 roku, do którego Wódz Naczelny miał pełne zaufanie jako lojalnego wykonawcy zadań w myśl idei nakreślonej w rozkazach. W ten sposób na czele Dywizji Jazdy – nowego w Wojsku Polskim związku taktycznego – stanęli oficer artylerii znany z umiejętności wykonywania niewykonalnych zadań oraz oficer piechoty mający doświadczenie w planowaniu, organizowaniu i prowadzeniu zagonu kawaleryjskiego, czyli działań głębokich. Podkreślić jednak należy, że gen. Jan Romer i mjr Szt. Gen. Tadeusz Piskor znali się dobrze i mieli za sobą okres kilkunastotygodniowej owocnej współpracy, ponieważ ten ostatni był szefem sztabu Grupy Operacyjnej „Bug" w czasie, gdy dowodził nią gen. Romer.

Dowództwo i sztab Dywizji Jazdy miały zostać sformowane w bardzo krótkim czasie z oficerów wyznaczonych przez Naczelne Dowództwo Wojska Polskiego oraz z dziesięciu oficerów Centralnej Szkoły Jazdy w Przemyślu. Zdolność do dowodzenia dowództwo i sztab miały osiągnąć do 20 kwietnia 1920 roku. Terminu tego nie zdołano dotrzymać. Do organu dowodzenia włączono oficerów ze sztabów pułków IV i V Brygady Jazdy, stanowiących elementy struktury dywizji. Tego dnia liczyła ona 192 oficerów i 6260 szeregowych, w tym 96 oficerów i 2989 szabel stanu bojowego, 4204 konie wierzchowe i 1677 pociągowych. Była uzbrojona w 65 karabinów maszynowych oraz 16 dział.

W operacji zaczepnej Wojska Polskiego na Ukrainie duże znaczenie odgrywały działania zgrupowań jazdy – zarówno nowo sformowanej Dywizji Jazdy, jak i VII Brygady Jazdy. Plan ich użycia w tej operacji stanowił bezpośrednie nawiązanie do napoleońskich wzorców operacyjnego zastosowania kawalerii. Został on opracowany przez szefa Oddziału III Sztabu Generalnego ppłk. Szt. Gen. Juliana Stachiewicza, a także mjr. Bolesława Wieniawę-Długoszowskiego po dogłębnych studiach operacyjnego wykorzystania kawalerii francuskiej w wojnach napoleońskich oraz udziału kawalerii w I wojnie światowej, szczególnie kawalerii niemieckiej na froncie zachodnim w początkowym jej okresie. Zadaniem Dywizji Jazdy było opanowanie Koziatyna – węzła komunikacyjnego położonego za stykiem ugrupowania bojowego sowieckich XII i XIV Armii. Miejscowość ta miała zostać utrzymana do nadejścia oddziałów 15 Dywizji Piechoty 2 Armii. 19 kwietnia 1920 roku Naczelny Wódz wydał szczegółową instrukcję dla Dywizji Jazdy.

W dniu 22 kwietnia 1920 roku do Równego przybył pociąg sztabowy z Wodzem Naczelnym i jego ścisłym sztabem. W godzinach popołudniowych Józef Piłsudski wraz z gen. Stanisławem Hallerem i ppłk. Szt. Gen. Julianem Stachiewiczem przeprowadzili godzinną odprawę z dowódcami armii oraz jednostek wykonujących najważniejsze zadania, czyli z dowódcą: 6 Armii gen. Wacławem Iwaszkiewiczem, 2 Armii gen. Antonim Listowskim, Grupy gen. Rydza-Śmigłego gen. Edwardem Rydzem-Śmigłym oraz Dywizji Jazdy gen. Janem Romerem. Tego dnia Wódz Naczelny rozpoczął inspekcjonowanie jednostek na froncie, następnego zaś dnia dokonał ostatnich ustaleń z gen. Rydzem-Śmigłym i gen. Romerem. Czterdzieści godzin później rozpoczęła się operacja ukraińska.

O świcie 25 kwietnia 1920 roku Dywizja Jazdy rozpoczęła zagon na Koziatyn. Zasadnicza trudność wykonania tego zadania polegała na tym, że w celu osiągnięcia zaskoczenia należało do maksimum wykorzystać teren. W związku z tym oddziały dywizji wykonały zagon w pasie kompleksów leśnych rozciągających się między drogą Zwiahel – Żytomierz a linią kolejową Połonne – Berdyczów, przecinając zarazem drogi rokadowe Żytomierz – Cudnów i Żytomierz – Berdyczów. Dywizja, działając w jednej kolumnie, wykonała zagon na osi Młyny Ostrożeckie – Tartak – Luborski Hutor – Prutówka – Żółty Bród – Budyszcze – Nowa Rudnia i zatrzymała się na nocny postój ubezpieczony w rejonie wsi Rudnia nad rzeką Hniłopiat. 26 kwietnia 1920 roku wyruszyła w dalszy marsz po drodze Rudnia – Gwozdawa – Siomaki – Skakówka – Krasówka – Białopol. W rejonie tej ostatniej miejscowości zorganizowano dwugodzinny odpoczynek. Rejon ten stał się podstawą wyjściową dla poszczególnych elementów ugrupowania bojowego. Dywizja działając siłami czterech pułków jazdy w pierwszym rzucie, nad ranem 27 kwietnia 1920 roku opanowała Koziatyn przy minimalnych stratach własnych, zdobywając 120 parowozów i ponad 3000 wagonów[4]. Następnego dnia Koziatyn osiągnęły oddziały 15 Dywizji Piechoty, które zluzowały siły Dywizji Jazdy.

4 Z. Brochwicz-Lewiński, *Zagon na Koziatyn*, „Bellona" 1921 z. 4, s. 306–316; T. Piskor, *Działania dywizji kawalerii na Ukrainie. Od 20 IV do 20 VI 1920 roku*, Warszawa 1926, s. 16–66.

Generał Romer na zdjęciu drugi od lewej w pierwszym rzędzie

W dniu 30 kwietnia 1920 roku Naczelny Wódz rozkazał, aby Dywizja Jazdy opanowała Białą Cerkiew, przecinając zarazem połączenia kolejowe Czerkasy – Kijów i jednocześnie nawiązując współdziałanie z III Brygadą Jazdy w Fastowie. W dniach 1–3 maja 1920 roku wszystkie obiekty i linie terenowe nakazane rozkazem z 30 kwietnia zostały osiągnięte bez większego przeciwdziałania ze strony przeciwnika. 3 maja 1920 roku Dywizja Jazdy opanowała Białą Cerkiew położoną 105 km na wschód od Koziatyna. W miejscowości tej ludność polska i częściowo rosyjska entuzjastycznie powitały oddziały polskie, a po południu odprawiono nabożeństwo dziękczynne. W tym czasie związki taktyczne piechoty w całym pasie działania polskiej 6, 2 i 3 Armii metodycznie zajmowały teren. Do 3 maja 1920 roku wyszły na linię Jaruga nad Dniestrem – rzeka Briszka – Niemirów – Lipowiec (6 Armia), Lipowiec – Pohrebyszcze – Skwira – Żydowce (2 Armia), Żydowce – Brusiłów – Stawiszcze – Piaskówka (3 Armia). W następnych dniach w skład Dywizji Jazdy weszła III Brygada Jazdy. Od tej pory trzybrygadowa dywizja gen. Romera odgrywała ważną rolę w ugrupowaniu 2 Armii, ubezpieczając obszar między Dnieprem a linią kolejową Fastów – Czerkasy. W tym celu oddziały dywizji miały wyjść na linię Tripole – Rzyszczew – Karapiszcze – Biała Cerkiew i z tej rubieży prowadzić działania rozpoznawcze. 6 maja 1920 roku dywizja siłami trzech brygad opanowała Taraszczę (III Brygada Jazdy), Olszanicę (IV Brygada Jazdy) oraz Kahorlik (V Brygada Jazdy). Tego samego dnia do Białej Cerkwii udał się gen. Aleksander Karnicki wyznaczony na nowego dowódcę dywizji w miejsce gen. Jana Romera, któremu marszałek Józef Piłsudski postanowił powierzyć kolejną misję specjalną – stanowisko dowódcy Etapów Wojska Polskiego na Ukrainie.

Dowództwo Etapów wbrew swej nazwie było pierwszym w dziejach oręża polskiego organem współpracy cywilno-wojskowej przeznaczonym do współdziałania z władzami ukraińskimi oraz wsparcia ich wysiłków związanych z budową struktur niepodległej Ukrainy na wzór tych z czasów I wojny

Generał Romer był dowódcą cechującym się dążeniem do wykonywania zadań bojowych w sposób zaczepny, pamiętającym, że obrona jako forma działań taktycznych również musi cechować się aktywnością.

NARODOWE ARCHIWUM CYFROWE

światowej. Służba etapowa odpowiadała za zaopatrzenie wojsk prowadzących działania w obszarze odpowiedzialności poszczególnych związków operacyjnych oraz za funkcjonowanie wszystkich służb na zapleczu frontu. W tym przypadku zapleczem był teren sojuszniczej Ukrainy, dlatego gen. Jan Romer otrzymał dodatkowe zadanie wspierania wysiłków w tworzeniu ogniw infrastruktury władz ukraińskich, w formowaniu wojska itd. Na podstawie analizy dokumentów można postawić tezę, że skupienie problematyki etapów – dotychczas ściśle powiązanych z poszczególnymi frontami, a później z armiami – w jednym ręku na ukraińskim obszarze operacyjnym wynikało z konieczności uzgodnienia wszystkich kwestii z rządem Ukraińskiej Republiki Ludowej oraz powstającą w terenie administracją ukraińską. Występowało tu zarazem bardzo silne sprzężenie zwrotne między tymi dwoma głównymi nurtami działalności Dowództwa Etapów Wojska Polskiego na Ukrainie. Szczegółowa analiza struktury organizacyjnej tego organu dowodzenia oraz zakresu kompetencji jego poszczególnych komórek wskazuje, że rozwiązanie to wyprzedzało epokę i miało wiele wspólnego ze współpracą cywilno-wojskową realizowaną współcześnie przez Wojsko Polskie w czasie operacji stabilizacyjnych prowadzonych w różnych częściach świata. Również wybór na jego dowódcę gen. Jana Romera nie był przypadkowy. Był on osobą mającą bogate doświadczenie, jednocześnie niezwykle konkretne, zarazem koncyliacyjne, a ponadto przychylne sprawie ukraińskiej niepodległości podejście.

Generał Jan Romer objął obowiązki na stanowisku dowódcy Etapów Wojska Polskiego na Ukrainie 7 maja 1920 roku i po odebraniu instrukcji od Wodza Naczelnego w Żytomierzu wyjechał do Warszawy w celu uzgodnienia z polskim premierem zakresu współdziałania polsko-ukraińskiego. Jego służba na tym stanowisku to trudny i gorący okres. Prace organizacyjne związane z rozbudową ukraińskiej administracji i formowaniem sił zbrojnych napotykały wiele przeszkód, a możliwości działania rządu Ukraińskiej Republiki Ludowej były bardzo ograniczone. Jak wspominał gen. Romer, rząd ten tworzyły osoby należące do różnych stronnictw politycznych, nierzadko skonfliktowanych z Semenem Petlurą. Wiele z nich było zainteresowanych wyłącznie własną karierą i kwestiami materialnymi, co było źródłem korupcji. Generał oceniał, że jego Dowództwo Etapów Wojska Polskiego na Ukrainie miało lepsze rozeznanie co do liczebności wojsk ukraińskich niż ukraińskie Ministerstwo Spraw Wojskowych.

W związku z koniecznością opuszczenia Ukrainy ze względu na niemożność zerwania operacji zaczepnej wojsk sowieckiego Frontu Południowo-Zachodniego, której swoiste koło zamachowe stanowiły działania zaczepne sowieckiej I Armii Konnej, gen. Jan Romer w połowie czerwca 1920 roku, gdy działania wojenne przeniosły się na obszar Wołynia, został wyznaczony na stanowisko dowódcy Grupy Operacyjnej „Słucz". Została ona utworzona ze związków taktycznych przemieszczonych na ukraiński obszar operacyjny z litewsko-białoruskiego obszaru operacyjnego, czyli 3 Dywizji Piechoty Legionów i 6 Dywizji Piechoty (bez XII Brygady Piechoty, ale z przydzielonymi w jej miejsce 65 Pułkiem Piechoty i III Batalionem 3 Pułku Strzelców Podhalańskich). Do tego zgrupowania dołączono przybyłą z głębi kraju I Rezerwową Brygadę Piechoty, a ponadto – prowadzące cały czas działania na Ukrainie – Dywizję Jazdy oraz X Brygadę Piechoty 5 Dywizji Piechoty ze składu 6 Armii. Dodać przy tym należy, że podwładnym gen. Jana Romera był wówczas ówczesny por. Stanisław Maczek, pełniący służbę w sztabie Grupy Operacyjnej „Słucz" w Oddziale III, czyli operacyjnym.

Dowódca polskiego Frontu Ukraińskiego gen. Aleksander Listowski zamierzał na linii rzeki Uszy pobić wojska sowieckiej I Armii Konnej. Dysponując wiarygodnymi informacjami na temat działań przeciwnika pochodzącymi przede wszystkim z radio-

wywiadu, weryfikowanymi przez elementy rozpoznawcze walczących wojsk, ocenił, że główny wysiłek sowieckiej armii będzie skierowany na północny wschód od Zwiahla. Z tego właśnie powodu w rejon ten skierowano siły główne Grupy Operacyjnej „Słucz" gen. Romera, która we współdziałaniu z wojskami 3 Armii miała zatrzymać przeciwnika, zadać mu straty i nie dopuścić do przełamania linii frontu na kierunku Zwiahel – Równe[5].

Generał Jan Romer na podstawie informacji na temat działań sowieckiej I Armii oraz po skonstatowaniu spowolnienia tempa działań przeciwnika zarządził rozkazem operacyjnym nr 1 z 17 czerwca 1920 roku przeprowadzenie koncentrycznego natarcia na te siły, zanim w ten rejon podejdą dywizje strzeleckie XII Armii. Przejęte przez polski radiowywiad kolejne rozkazy dowódcy sowieckiej I Armii Konnej Siemiona Budionnego wskazywały, że zamierzał on opanować Korosteń z pozostawieniem za lewym skrzydłem Zwiahla. W związku z tym dowódca Frontu Ukraińskiego 18 czerwca 1920 roku nakazał, by prawe skrzydło 3 Armii związało przeciwnika od czoła w celu ułatwienia Grupie Operacyjnej „Słucz" wykonania uderzenia z kierunku południowo-zachodniego na lewe skrzydło sowieckiej I Armii Konnej.

W rozkazie operacyjnym Grupy Operacyjnej „Słucz" z 18 czerwca 1920 roku gen. Romer, nie mając pewności, jakie działania podejmie przeciwnik następnego dnia, nakazał, aby w sytuacji jego uderzenia już 19 czerwca na jednostki 3 Armii 6 Dywizja Piechoty bezzwłocznie natarła na jego lewe skrzydło, a 3 Dywizja Piechoty Legionów tego samego dnia uderzyła na skrzydło i tyły sowieckiej I Armii Konnej. Generał zakładał, że w przypadku natarcia sowieckiego na Korosteń zadaniem 3 Armii będzie utrzymywanie linii rzeki Uszy z przyczółkiem mostowym w Korosteniu. Natomiast Grupa Operacyjna „Słucz" miała uderzyć wzdłuż drogi Zwiahel – Żytomierz. Z kolei gdyby sowiecka I Armia Konna rozpoczęła działania na kierunku Zwiahel, miała ją zatrzymać od zachodu Grupa Operacyjna „Słucz", oczekując uderzenia 3 Armii od północy siłami zgrupowania taktycznego płk. Stefana Dęba-Biernackiego złożonego z 1 Pułku Piechoty Legionów i 12 Pułku Piechoty 6 Dywizji Piechoty, wspartych dywizjonem z 1 Pułku Artylerii Polowej Legionów.

Z powodu przemęczenia ludzi i koni, braku prowiantu oraz furażu sowieckie natarcie rozpoczęło się z opóźnieniem dopiero 19 czerwca 1920 roku około godziny 13.00, stanowiąc wstęp do kilkudniowych ciężkich walk. Niepowodzenie sowieckiej I Armii Konnej, która nie przełamała polskiej obrony, było efektem dzielnej postawy 3 Dywizji Piechoty Legionów oraz 6 Dywizji Piechoty przepełnionych duchem powodzenia odniesionego przed tygodniem na litewsko-białoruskim obszarze operacyjnym, jak też skutecznego dowodzenia gen. Romera, który konsekwentnie dążył do wykonania zadania i osiągnięcia celu, jakim było opisane uderzenie na skrzydło i tyły przeciwnika. Analiza dokumentów opracowanych przez dowództwo i sztab Grupy Operacyjnej „Słucz" wskazuje na niezwykle trafną ocenę położenia, w szczególności zaś na opinie o nieskoordynowanych w czasie i przestrzeni działaniach sowieckiej I Armii Konnej prowadzonych bez ogólnego planu, mających charakter natarcia czołowego bez prób zastosowania manewru. Oceny te kilka lat później powtórzył w swoim artykule mjr Szt. Gen. Mieczysław Biernacki analizujący działania sowieckiej I Armii Konnej[6].

Dlatego też sowieckie natarcie zaplanowane na 21 czerwca 1920 roku zostało poprzedzone uderzeniem polskiej 3 Dywizji Piechoty Legionów, 6 Dywizji Piechoty oraz Dywizji Jazdy na sowieckie 6 i 11 Dywizję Kawalerii, które zostały zmuszone do odwrotu w kierunku Żytomierza. Niestety przedwczesne wycofanie grupy płk. Stefana Dęba-Biernackiego w związku z zarządzonym odwrotem 3 Armii otworzyło sowieckiej 4 Dywizji Kawalerii drogę na północny wschód[7]. Generał Romer bezskutecznie interweniował w dowództwie Frontu Ukraińskiego w sprawie wstrzymania odwrotu 3 Armii do czasu pobicia I Armii Konnej przez Grupę Operacyjną „Słucz". W meldunku napisał, że prowadzone konsekwentnie natarcie *wedle opinii dowództwa grupy opartej na tempie, w jakim akcja się rozwija, byłby mógł doprowadzić do bardzo poważnego, jeżeli nie całkowitego rozbicia Armii Konnej Budionnego*[8].

W ten sposób działania przeciwko sowieckiej I Armii Konnej zostały przerwane w momencie najbardziej pomyślnego ich rozwoju. Dowódca 6 Dywizji Piechoty gen. Kazimierz Raszewski w swych wspomnieniach żałował niewykorzystanej okazji jej pobicia: *Akcja grupy gen. Romera stanęła w tej chwili na pozycji nadzwyczaj dogodnej dla zniszczenia Armii Konnej Budionnego. Udała się bowiem rzecz niebywała, mianowicie okrążenie konnej jazdy przez piechurów. Jeszcze jeden lub dwa dni dalszego marszu, a bylibyśmy tego niebezpiecznego przeciwnika zniszczyli*[9]. Wycofywanie sowieckiej 6 i 11 Dywizji Kawalerii w kierunku Żytomierza zostało wstrzymane na skutek przerwania polskiego natarcia oraz pod wpływem informacji o odwrocie polskiej 3 Armii. Jednakże jednostki I Armii Konnej po dwóch dniach ciężkich walk, poniesieniu dużych strat i wyczerpaniu

5 M. Biernacki, *Bitwa z Budionnym nad Uszą (19–21 VI 1920 r.)*, cz. 1, „Bellona" 1927 t. 26 z. 4, s. 75.

6 Ibidem, s. 74–106; tenże, cz. 2 , 1927 t. 26, z. 5, s. 190–210.

7 N. Kakurin, W. Mielikow, *Wojna z biełopoliakami w 1920 g.*, Moskwa 1925, s. 174 i nast.

8 M. Biernacki, *Bitwa z Budionnym nad Uszą*..., op.cit, cz. 2, s. 200.

9 K. Raszewski, *Wspomnienia z własnych przeżyć wojennych*, Poznań [1938], s. 221.

amunicji nie podjęły pościgu za odchodzącymi oddziałami polskimi. Bitwa nad Uszą miała ten skutek, że wojska polskiego Frontu Ukraińskiego wyzbyły się kompleksu wobec sowieckiej I Armii Konnej. Jak ocenił badacz tej problematyki dr Daniel Koreś: *Doświadczenia z walk GO „Słucz" gen. Romera wyraźnie wskazywały, że „konarmia" nie jest formacją niepokonaną i że najlepszym sposobem jej powstrzymania było połączenie twardej obrony piechoty z wykorzystaniem przeszkód terenowych i manewru silnej, jednolicie zorganizowanej i dowodzonej kawalerii*[10].

Reorganizacja systemu dowodzenia i podział sił na polskim Froncie Ukraińskim nastąpiły 25 czerwca 1920 roku. Nowym jego dowódcą został dotychczasowy dowódca 3 Armii gen. por. Edward Rydz-Śmigły, a dowództwo 3 Armii objął gen. Zygmunt Zieliński. Z Grupy Operacyjnej „Słucz" utworzono 2 Armię, dowodzenie którą przejął 2 lipca 1920 roku dotychczasowy dowódca 6 Dywizji Piechoty gen. ppor. Kazimierz Raszewski, natomiast gen. Jan Romer został wyznaczony na dowódcę prowadzącej działania na terenie Podola 6 Armii. Dotychczas tym związkiem operacyjnym z powodzeniem dowodził gen. Wacław Iwaszkiewicz, który jednak podupadł na zdrowiu i musiał udać się na urlop.

Niekorzystne położenie w centralnej części frontu na Ukrainie spowodowało, że nowy dowódca 6 Armii gen. por. Jan Romer nakazał dokonanie przegrupowania. Taktyczne właściwości terenu tzw. płyty podolskiej sprzyjające prowadzeniu działań obronnych umożliwiły poszerzenie pasa działania prawoskrzydłowej Armii Czynnej Ukraińskiej Republiki Ludowej, a brygady strzeleckie ukraińskiej 3 Żelaznej Dywizji Strzeleckiej zaczęły luzować oddziały polskiej 12 Dywizji Piechoty w rejonie Baru. Równocześnie polska dywizja przemieściła swe oddziały w rejon Latyczowa i Nowokonstantynowa, w dotychczasowy pas działania 18 Dywizji Piechoty, która została skierowana na lewe skrzydło 6 Armii w celu użycia jej w działaniach zaczepnych przeciwko sowieckiej I Armii Konnej. Z trzech dywizji polskiej 6 Armii jedynie 13 Dywizja Piechoty pozostała w dotychczasowym pasie działania.

W pierwszych dniach lipca dowódca 6 Armii wydał rozkazy dla 13 i 18 Dywizji Piechoty dotyczące rozpoczęcia działań mających na celu wyjście na skrzydło i tyły sowieckiej I Armii Konnej. Ich rezultatem były walki 18 Dywizji Piechoty dowodzonej przez gen. Franciszka Krajowskiego w rejonie Zasławia. Generał Romer w kolejnym rozkazie operacyjnym stwierdził: *Wprawdzie 6 Armia jest obecnie około 70 km przed frontem 2 Armii, dla odciążenia jednakowo tej Armii pozostanie 6 Armia w obecnej sytuacji* [położeniu]. *Dopiero w razie niepowodzenia w bitwie nad Horyniem i interwencji Grupy gen. Krajowskiego – 6 Armia wykona odwrót w kierunku Zbrucza, celem zasłonięcia wschodniej Małopolski*. [...] *Zostawiam 13 DP wolność rzucania lokalnych sił na Zasław w celu wygrania bitwy nad Horyniem*"[11]. 5 lipca 1920 roku o świcie oddziały grupy gen. Krajowskiego sforsowały Horyń oraz opanowały Zasław, który wieczorem został zaatakowany siłami trzech pułków kawalerii z sowieckiej I Armii Konnej, jednak natarcie to zdołano odeprzeć. Wobec przemęczenia oddziałów gen. Krajowski podjął decyzję o zatrzymaniu działań zaczepnych, odtworzeniu zdolności bojowej i jednoczesnym przygotowaniu natarcia na Ostróg 7 lipca 1920 roku.

Sztab sowieckiego Frontu Południowo-Zachodniego najprawdopodobniej na podstawie meldunków XIV Armii, częściowo również I Armii Konnej, zorientował się, że w rejonie Starokonstantynowa został ześrodkowany polski związek taktyczny, którego celem – jak przewidywano – jest wykonanie uderzenia na skrzydło i tyły I Armii Konnej, osłaniane przez oddziały 45 Dywizji Strzeleckiej. W związku z tym dowództwo sowieckie dla ratowania sytuacji nakazało zintensyfikowanie działań zaczepnych w całym pasie działania sowieckiej XIV Armii.

Ocena ogólnego położenia spowodowała, że 5 lipca 1920 roku gen. Jan Romer wydał rozkaz operacyjny, w którym planował przeprowadzenie odwrotu na linię rzeki Zbrucz. Odwrót ten miał nastąpić w czterech etapach oznaczonych liniami fazowymi, które stanowiły rzeki przecinające południkowo płytę podolską – dopływy Dniestru. Odwrót miał się rozpocząć 5 lipca o godzinie 23.00[12]. W kolejnych dniach związki taktyczne 6 Armii przeprowadziły w sposób planowy manewr odwrotowy. W działaniach tych 12 Dywizja Piechoty opóźniała przeciwnika na kierunku Płoskirów – Wołoczyska – Tarnopol. 13 Dywizja Piechoty odchodziła z zadaniem obrony rejonu Zbaraż – Załoźce, utrzymując łączność taktyczną z oddziałami 18 Dywizji Piechoty, która prowadziła działania opóźniające na kierunku Zasław – Ostróg, a następnie w rejonie Dubno – Krzemieniec przeszła do obrony, ubezpieczając w ten sposób kierunek Dubno – Brody, a zarazem lewe skrzydło ugrupowania bojowego 6 Armii.

W pasie działania tej armii dopiero 20 lipca 1920 roku wojska sowieckie zdołały przełamać obronę na linii rzeki Zbrucz na północ od Wołoczysk. Równocześnie powstało niekorzystne położenie w pasie działania 18 Dywizji Piechoty, gdzie przeciwnik wtargnął w lukę między nią a jednostkami 2 Armii. Z tego powodu gen. Jan Romer ocenił, że nie widzi możliwości utrzymania linii Zbrucza. Kiedy jednak Naczelne Dowództwo Wojska Polskiego rozkazem nr 7598/III nakazało utrzymać tę linię, generał lojalnie przystąpił do wykonania tego zadania. W kolej-

10 D. Koreś, *Organizacja i liczebność Grupy Operacyjnej Jazdy w lipcu 1920 r.*, „Przegląd Historyczno-Wojskowy" 2007 nr 2, s. 63.

11 WBH, *Dowództwo 6 Armii*, sygn. I 311.6.179, *Dowództwo 6 Armii* L. op. 2355/III, *Rozkaz operacyjny nr 28 z 3 VII 1920 r.*

12 WBH, *Dowództwo 6 Armii*, sygn. I 311.6.179, *Dowództwo 6 Armii* L. op. 2380/III, *Rozkaz operacyjny nr 29 z 5 VII 1920 r.*; *Dowództwo 6 Armii* L. op. 2382/III, *Dodatek do rozkazu operacyjnego nr 29 z 5 VII 1920 r.*

nych dniach linia Zbrucza została utrzymana mimo prób jej sforsowania podejmowanych w rejonie Iwanie Puste oraz pod Husiatynem, Satanowem i Wołoczyskami. 22 lipca 1920 roku 13 Dywizja Piechoty zagięła lewe skrzydło na Wiśniowiec i Komaryn, następnie rozpoczęła działania zmierzające do opanowania linii Horynka – Dunajów w celu nawiązania łączności z 18 Dywizją Piechoty, co poprawiło jej położenie. 24 lipca Husiatyn po raz kolejny przechodził z rąk do rąk. Na północ od Wołoczysk oddziały sowieckie zdołały opanować Medyń i Hnilice, a wieczorem opanowały przyczółek mostowy Wołoczyska. 12 Dywizja Piechoty wobec wyczerpania odwowania tworzące ugrupowania bojowe armii. Dzień wcześniej podjął – błędną, jak się okazało – decyzję o skierowaniu 101 Rezerwowego Pułku Piechoty stanowiącego załogę twierdzy Osowiec w kierunku na Knyszyn w celu uderzenia na prawe skrzydło przeciwnika prowadzącego działania między Białymstokiem a bagnami biebrzańskimi. Sprawa ta stała się powodem oskarżenia gen. Romera o nieudolność i skierowania sprawy do Najwyższej Wojskowej Komisji Opiniującej przy Naczelnym Wodzu. Znalazła swój epilog w 1921 roku. 28 lipca 1920 roku siły 1 Armii powstrzymały wszystkie sowieckie próby forsowania Narwi.

MARSZAŁEK JÓZEF PIŁSUDSKI, KTÓRY NIE WYWODZĄCYCH SIĘ Z BYŁEJ ARMII AUSTRO-

dów i braku możliwości wykonania kontrataków zagięła lewe skrzydło na Klebanówkę – Zbaraż.

Dalsze działania 6 Armia realizowała pod komendą poprzedniego dowódcy, czyli gen. Wacława Iwaszkiewicza, który powrócił z urlopu. Natomiast gen. Jan Romer został wyznaczony na dowódcę 1 Armii prowadzącej działania na lewym skrzydle polskiego frontu, na litewsko-białoruskim obszarze operacyjnym. Rozpoczęta 4 lipca 1920 roku operacja zaczepna wojsk sowieckiego Frontu Zachodniego przełamała obronę polską, w wyniku czego 14 lipca przeciwnik opanował Wilno. Sposób działania wojsk Frontu Litewsko-Białoruskiego był przedmiotem sporu i konfliktu między dowódcą tego frontu gen. Stanisławem Szeptyckim a naczelnym wodzem marszałkiem Józefem Piłsudskim. Upadek Wilna i kolejne niepowodzenia spowodowały, że Naczelne Dowództwo Wojska Polskiego utraciło zaufanie zarówno do dowódcy frontu, jak i do dowódcy 1 Armii gen. Gustawa Zygadłowicza odpowiedzialnego za obronę Wilna. W związku z tym nastąpiła zmiana na stanowisku dowódcy tej armii.

Generał Jan Romer objął dowodzenia 1 Armią w sytuacji, gdy jej związki taktyczne usiłowały ustabilizować położenie na froncie na linii rzeki Niemen, co jednak się nie udało. W rezultacie starano się opóźniać natarcie przeciwnika na kierunku Grodno – Białystok, natomiast znaczna część pozostałych sił uległa panice i uciekła. Zatem gen. Romer objął dowództwo związku operacyjnego w bardzo trudnym położeniu. Ocena sytuacji doprowadziła go do przekonania, że odwrót z linii Niemna na linię Narwi należy przeprowadzić etapami, opóźniając przeciwnika na kolejnych rubieżach terenowych. Dopiero 27 lipca 1920 roku zdołał on skontrolować poszczególne związki taktyczne oraz inne zgrupo-

Następnego dnia gen. Jan Romer został wezwany do Warszawy przez Naczelnego Wodza, który wyznaczył go na przewodniczącego delegacji rozejmowej, która miała udać się na rozmowy z przedstawicielami strony bolszewickiej do Baranowicz. Wysłanie tej delegacji było następstwem zgody premiera Władysława Grabskiego na znaczne ustępstwa ze strony polskiej w czasie lipcowej konferencji przedstawicieli ententy oraz Polski, Czechosłowacji i Niemiec na konferencji w Spa. Naczelnik państwa i naczelny wódz marszałek Józef Piłsudski uznał te działania za przekroczenie kompetencji i zdymisjonował premiera oraz jego rząd. Jak można było przypuszczać, rozmowy z bolszewikami nie doprowadziły do rozejmu, ponieważ ci byli przekonani o tym, że w ciągu najbliższych dni opanują Warszawę, a następnie „po trupie burżuazyjnej Polski" zaniosą rewolucję bolszewicką na zachód Europy.

KOLEJNE LATA

Gdy delegacja rozejmowa powróciła do Warszawy, Józef Piłsudski dokonał kolejnej reorganizacji systemu dowodzenia i podziału sił na froncie przeciwbolszewickim. Nie mógł zaproponować gen. Romerowi objęcia jakiegokolwiek stanowiska. Polecił zatem generałowi udać się na urlop zdrowotny. Dopiero pod koniec września 1920 roku gen. Romer został wyznaczony na stanowisko szefa Naczelnej Kontroli Wojskowej, na którym pełnił służbę do 1 sierpnia 1921 roku. W tym czasie Najwyższa Wojskowa Komisja Opiniująca przy Naczelnym Wodzu w trakcie posiedzenia 23 listopada 1920 roku rozpatrzyła sprawę gen. Romera i uznała, że jego decyzja użycia 101 Rezerwowego Pułku Piechoty była nieprawidłowa z powodu *błędnej oceny sytuacji*[13]. Natomiast po otrzymaniu 20 kwietnia 1921 roku wyjaśnień marszałka

13 Instytut Józefa Piłsudskiego w Ameryce, *Sprawy sądowe i honorowe Generałów i wyższych dowódców*, sygn. 701/5/5, *Akta Najwyższej Wojskowej Komisji Opiniującej – sprawa gen. Jana Romera, dowódcy 1 Armii,* Najwyższa Wojskowa Komisja Opiniująca przy Naczelnym Wodzu L.dz. 57/Pf., uchwała z 23 XI 1920 r.

Józefa Piłsudskiego uznała 6 maja 1921 roku sprawę za załatwioną.

Generał Jan Romer 25 września 1921 roku został wyznaczony na stanowisko dowódcy Okręgu Korpusu nr 2 w Lublinie. 3 maja 1922 roku zweryfikowano go w stopniu generała dywizji ze starszeństwem z dniem 1 czerwca 1919 roku i ósmą lokatą w korpusie generałów. 1 września 1924 roku minister spraw wojskowych powołał generała na członka Rady Wojennej – organu doradczego Prezydenta Rzeczypospolitej w ówczesnym systemie kierowania i dowodzenia siłami zbrojnymi. Po zamachu majowym 10 lipca 1926 roku gen. Jan Romer został wyznaczony na stanowisko inspektora armii. 13 maja 1932 roku został zwolniony z tego stanowiska, a z dniem 31 lipca 1932 roku przeniesiony w stan spoczynku. Osiadł w Warszawie. Zmarł po długiej chorobie 5 marca 1934 roku w Szpitalu Ujazdowskim w Warszawie. Został pochowany na Cmentarzu Wojskowym na warszawskich Powązkach.

Był on dowódcą cechującym się dążeniem do wykonywania zadań bojowych w sposób zaczepny, pamiętającym, że obrona jako forma działań taktycznych również musi cechować się aktywnością. Z tego powodu nie czekał na aktywność przeciwnika, lecz dążył do uprzedzenia jego działań. Miał przy tym świadomość, że tak prowadzona walka wiąże się z ryzykiem, które potrafił dobrze oceniać. Nie zrażał się niepowodzeniami, poszukując innej możliwości pokonania przeciwnika. Zarazem potrafił rozwijać w podwładnych umiejętności bojowe oraz kształtować pozytywne cechy, które przekładały się na wysokie morale wojsk. Dzięki dbałości o rozwój tężyzny fizycznej jako pięćdziesięciolatek mógł imponować sprężystą sylwetką, żołnierską postawą oraz wytrzymałością psychofizyczną. Jego największą wadą w dowodzeniu na poziomie operacyjnym – co wyszło na jaw latem 1920 roku – okazała się chaotyczność połączona z zagłębianiem się w drobiazgi, które zaciemniały obraz całości położenia. Na tym szczeblu nie powinny one zaprzątać umysłu dowódcy.

MIAŁ WYSOKIEGO MNIEMANIA O GENERAŁACH WĘGIERSKIEJ, BARDZO CENIŁ GEN. JANA ROMERA

POKŁOSIE

Jeżeli chodzi o sferę prywatną, 29 września 1908 roku ówczesny ppłk Szt. Gen. Jan Romer zawarł związek małżeński ze Stefanią Lityńską. Z małżeństwa tego przyszło na świat troje dzieci – córka Maria Anna (ur. 1909) i synowie Jan Adam (ur. 1911) oraz Adam (ur. 1917), który niestety zmarł na szkarlatynę latem 1921 roku.

Był autorem dwóch artykułów opublikowanych w „Bellonie" oraz wspomnień zatytułowanych *Pamiętniki*, które zostały zredagowane przez rodzinę i wydane we Lwowie cztery lata po jego śmierci na podstawie pamiętnika. Zaczął go prowadzić podczas pełnienia misji w Paryżu w 1919 roku, a od lutego 1920 roku nadał mu formę dziennika i doprowadził do końca roku 1927. Drugie wydanie wspomnień ukazało się w 2011 roku staraniem Muzeum Historii Polski i zostało opatrzone wstępem oraz opracowane naukowo przez prof. Janusza Odziemkowskiego.

Generał Jan Romer został odznaczony Krzyżem Komandorskim i Krzyżem Srebrnym Orderu Wojennego Virtuti Militari, Krzyżem Komandorskim z Gwiazdą i Krzyżem Komandorskim Orderu Odrodzenia Polski, Krzyżem Walecznych (czterokrotnie) oraz Złotym Krzyżem Zasługi. Ponadto orderami zagranicznymi: Wielką Wstęgą Orderu Korony Rumunii, węgierską Wielką Wstęgą Orderu Zasługi oraz orderami austriackimi. Był również Wielkim Oficerem i Komandorem Orderu Legii Honorowej.

Marszałek Józef Piłsudski, który nie miał wysokiego mniemania o generałach wywodzących się z byłej armii austro-węgierskiej, bardzo cenił gen. Jana Romera. Za dowodzenie w wojnie Polski z bolszewicką Rosją otrzymał on bardzo dobrą ocenę, aczkolwiek wytknięte zostały również jego przywary. Opiniując w 1922 roku generalicję polską, Marszałek napisał o gen. Romerze: *Człowiek o niezwykłej energii, bystrym umyśle, prawym charakterze i wysokim poczuciu honoru żołnierskiego. Wykształcony oficer o bardzo wielkiej śmiałości i odwadze. Wymaga bardzo dużo od siebie, lecz stawia zbyt wysokie wymagania innym. W pracy jest porywczy i z tego powodu chaotyczny. Przy dłuższym dowodzeniu zmęczyć może wojsko i łatwo je zdezorganizuje. Wytrwały jest w pracy niesłychanie, o przysłowiowej w armii wytrzymałości fizycznej. O ile myśli jasno i zdrowo, o tyle w pracy samej wskutek porywczości i aktywności charakteru czepia się drobiazgów, nie umiejąc dowodzić spokojnie i dzielić racjonalnie pracę wśród podwładnych. Ładny typ żołnierza, specjalnie zdolnego do ryzyka i śmiałych przedsięwzięć. Wytrzymały na niepowodzenia, podczas których z uporczywą energią szuka rewanżu. Pod względem techniki dowodzenia łatwo da sobie radę z armią; potrzebowałby przy tym szefa sztabu o silnym charakterze, który nie zrażając się niczym, wprowadziłby porządek w chaotyczne nieraz rozporządzenia dowódcy armii*[14]. ■

14 M. Cieplewicz, *Generałowie polscy w opinii Józefa Piłsudskiego*, „Wojskowy Przegląd Historyczny" 1966 nr 1; *Polska generalicja w opiniach Marszałka Piłsudskiego*, wstęp i oprac. nauk. K. Stepan, Warszawa 2020, s. 46–48.

Dear Readers!

The key phenomenon related to effective process of command at every level is possessing information both, about a combat group, and most of all about an enemy. A rapid collection and effective availability of information depends to a significant extent on properly organized communication system (exchanging data and phonic information in close to real time). This shows how the communication system, including the subsystem for information exchange, is an important component of the command system. Today, the role of communication system increased to the rank of primary factor ensuring effectiveness in commanding forces and success of operation conducted by the armed forces.

The main subject of this edition of Przegląd Sił Zbrojnych (PSZ) is about this service branch of the armed forces. The author of the first article presents the requirements for contemporary communication systems in the armed forces and the potential to introduce them with the inclusion of present and future ways of distant communication. He further suggests that all hardware and software used for communication in the assisting command subunits should be compatible.

Another authors present the threats functioning in virtual space, as well as the systems of protection against them while claiming that system security is as strong as its weakest element. On how an advancing automation of armament or a creation of integrated image of tactical situation contribute to new threats that could affect commanding posts, including an advanced system of field communication, write another authors. They focus on presenting the possibility of potential adversary in recognizing and destroying elements of communication system with the use of electronic warfare and performing precise attacks. They also discuss the ways to minimize these threats. A crucial problem is ensuring a high level of cryptographic security within own armed forces as well as within the coalition and international cooperation. For that reason, a number of security programs for information safety is created, which is described in the next article.

The following articles discuss: how the KF radio communication system facilitates the functioning of combat group at every level of command based on the experience from the exercises of the 12th Mechanized Division; what systems should function in our armed forces to deliver in real time (or close to real time) the data on the location of own forces; the system of monitoring of own forces within a NATO friendly force tracking system (FFTS), which is a crucial information source for automated systems of command support, reconnaissance, warfare means control and logistic support for operations.

In this edition, we also publish more of articles of the graduates of the Operational and Tactical Course, which they took in the War Studies University (ASzWoj). The authors discuss their opinions on warfare methods in tank units on urbanized areas as well as during coastal defense.

Last but not least, there is a material on the Russian concept of "military special operation" and its effects during the ongoing conflict in Ukraine.

Finally, we highly recommend reading all articles, as we hope that they will help in broadening one's knowledge on given subjects.

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.

Edycja limitowana

WOJSKA SPECJALNE

ALBUM POŚWIĘCONY ELITARNEMU RODZAJOWI POLSKICH SIŁ ZBROJNYCH

WOJSKOWY INSTYTUT WYDAWNICZY

15 LAT WOJSK SPECJALNYCH

sklep.polska-zbrojna.pl

Partnerzy

KGHM POLSKA MIEDŹ

PZL Mielec
A Lockheed Martin Company

GISS
Global Infrastructure & Security Solutions

KenBIT

PRENUMERATA WYDAŃ CYFROWYCH

sklep.polska-zbrojna.pl

Już dziś zamów jeden z naszych periodyków i ciesz się lekturą na telefonie lub tablecie!

Roczna prenumerata „Polski Zbrojnej” za jedyne 50 zł

POLSKA ZBROJNA · HISTORIA POLSKA ZBROJNA · PRZEGLĄD SIŁ ZBROJNYCH · KWARTALNIK BELLONA