Przyszłe konflikty zbrojne

Co z tą cyberprzestrzenią?

Kierunki rozwoju zdolności obronnych

PRZEGLĄD SIŁ ZBROJNYCH

Cena 10 zł (w tym 8% VAT)

nr 4 / 2021
lipiec–sierpień

WOJSKOWY INSTYTUT WYDAWNICZY

ISSN 2353-1975

Szanowni **Czytelnicy!**

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

Dyrektor Wojskowego
Instytutu Wydawniczego:
MACIEJ PODCZASKI
e-mail: sekretariat@zbrojni.pl
tel.: 261 849 007, 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

Opracowanie infografik:
PAWEŁ KĘPKA

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: ARTDRUK
ul. Napoleona 2
05-320 Kobyłka

Zdjęcie na okładce:
SHUTTERSTOCK

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

Krzysztof Wilewski

W połowie lat osiemdziesiątych ubiegłego wieku na jednej z amerykańskich uczelni wojskowych zapytano absolwentów, jakie będzie przyszłe pole walki. Zazwyczaj odpowiedź brzmiała: skomputeryzowane. Z perspektywy czasu należy ocenić, że żołnierze, którzy dziś są najczęściej emerytami, mieli rację. Komputery są dzisiaj wszechobecne. To za ich pomocą steruje się platformami bezzałogowymi i to one obliczają nastawy dział do prowadzenia ognia oraz naprowadzają pociski rakietowe na wybrany cel.

Przygotowanie do wojny przyszłości polega na wyszkoleniu sił zbrojnych do prowadzenia działań w czterech domenach jednocześnie. Muszą one być gotowe do walki z przeciwnikiem, który dysponuje porównywalnym potencjałem militarnym, jak również z asymetrycznym wrogiem. Te zagadnienia, jak i wiele innych, znalazły się w kręgu zainteresowania strategów oraz ośrodków naukowych zajmujących się scenariuszami przyszłych konfliktów zbrojnych. Jednak nawet najlepszy wojskowy strateg czy analityk nie jest w stanie prawidłowo opisać pola walki przyszłości w zmieniającym się dynamicznie środowisku bezpieczeństwa międzynarodowego. Należy zatem przygotowywać się do wojen, które będą, a nie do tych, które były.

W niniejszym wydaniu „Przeglądu Sił Zbrojnych" znajdą Państwo artykuły poświęcone wyzwaniom, jakie niesie przyszłe pole walki. Swoją wiedzą na ten temat podzielili się: płk dr hab. inż. Norbert Świętochowski, płk dypl. rez. Dariusz Rewak, kpt. Agnieszka Maciejewska-Miedziak, mjr Jarosław Patałuch, płk rez. dr inż. Marek Andruszkiewicz, ppłk rez. dr inż. Dariusz Szkołuda, mjr Andrzej Zajączkowski, kmdr por. rez. Grzegorz Kolański oraz dr inż. Marek Dąbrowski.

Uzupełnieniem ich rozważań są opracowania dotyczące znaczenia cyberprzestrzeni w przyszłych zmaganiach militarnych, jak również jej roli w zapewnianiu bezpieczeństwa lotniczego i kosmicznego.

Szczególnej uwadze Państwa polecam materiały wyłonione w ramach konkursu na najlepszy artykuł, zorganizowanego w Wydziale Wojskowym ASzWoj przez „Przegląd Sił Zbrojnych". W numerze tym prezentujemy prace: mjr. Piotra Fanfary i mjr. Krzysztofa Stamborskiego dotyczące rozwoju zdolności obronnych naszych sił zbrojnych oraz mjr. Marcina Wawro o znaczeniu militarnym wybranych regionów naszego kraju, jak również mjr. Kamila Organisty o sposobach organizowania łączności w różnych środowiskach pola walki.

Problematykę logistyczną reprezentują artykuły autorów z Centrum Szkolenia Logistyki. Publikujemy także opracowanie o znaczeniu infrastruktury komunikacyjnej naszego kraju dla sprawnego manewru zgrupowań zadaniowych.

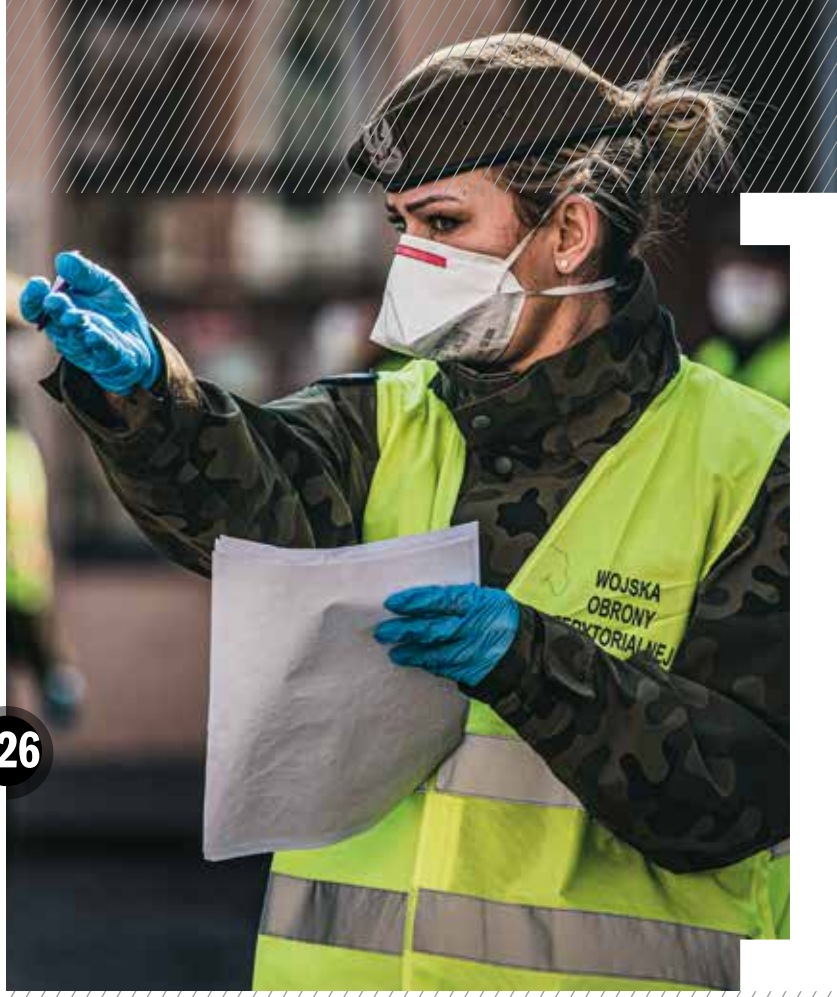
Życzę miłej lektury

nr 4 / 2021

Spis treści

TEMAT NUMERU – PRZYSZŁE POLE WALKI

SZKOLENIE



Sprostowanie

W trzecim numerze „Przeglądu Sił Zbrojnych" do artykułu *Rozpoznanie wojskowe w walce informacyjnej*, którego autorem jest prof. dr hab. Marek Wrzosek, wkradł się błąd. Otóż pomylono nazwisko jednego z prelegentów i jego przynależność organizacyjną. Prelegentem był ppłk dr inż. Tomasz Kulik z Lotniczej Akademii Wojskowej. Również mjr dr Daniel Michalski reprezentował tę uczelnię, a nie – jak podano – Akademię Wojsk Lądowych. Za pomyłkę przepraszamy.

PERUN

PROJEKT REALIZOWANY PRZEZ ZAKŁADY MECHANICZNE „TARNÓW" S.A., STEKOP S.A. ORAZ WAT. EFEKTEM KOŃCOWYM BĘDZIE AUTONOMICZNY CZTEROKOŁOWY POJAZD O MASIE CAŁKOWITEJ DO 900 KG I DUŻEJ DZIELNOŚCI TERENOWEJ, WYPOSAŻONY W ZDALNIE STEROWANY MODUŁ UZBROJENIA Z SYSTEMEM ŚLEDZENIA CELU.

ZM TARNÓW S.A.

Przyszłe konflikty zbrojne

WYZWANIEM STAJE SIĘ ZDEFINIOWANIE PRZYSZŁOŚCI Z TAKĄ PRECYZJĄ, BY UJĄĆ JĄ W STRATEGICZNYM PLANOWANIU WOJSKOWYM, PAMIĘTAJĄC O TYM, ŻE PRAKTYKA CZĘSTO ZNACZNIE RÓŻNI SIĘ OD ZAŁOŻONEJ TEORII.

płk dr hab. inż. Norbert Świętochowski

Autor jest dyrektorem Instytutu Dowodzenia Akademii Wojsk Lądowych.

Współczesną wojnę można rozpatrywać jako zjawisko pojawiające się okresowo w procesie funkcjonowania państwa. Mimo że występuje bardzo często, na szczęście nadal rozważane jest jako pewna anomalia w funkcjonowaniu społeczeństw. Mówiąc o *zjawisku*, które jest osadzone na słowie *zjawa*, na myśl nasuwa się coś tajemniczego, mało poznanego, nie w pełni zrozumiałego[1]. Takimi nadal są dla człowieka wszelkie wojny i konflikty zbrojne, zwłaszcza te, które mogą się dopiero wydarzyć. Nie ma innej drogi do określenia perspektyw ewolucji przyszłych wojen i konfliktów zbrojnych niż doskonała znajomość historii sztuki wojennej, umiejętne wyciąganie z niej wniosków oraz predykcja tego, co może nastąpić. Należy również wyjaśnić pojęcia *konflikt zbrojny* i *wojna*, często używane zamiennie. Międzynarodowy Trybunał Karny dla byłej Jugosławii orzekł 2 października 1995 roku, że konflikt zbrojny istnieje zawsze wtedy, gdy między państwami dochodzi do użycia sił zbrojnych lub długotrwałej przemocy zbrojnej między władzami rządowymi i zorganizowanymi grupami zbrojnymi lub między takimi grupami na terytorium jednego państwa. Pojęcie konfliktu zbrojnego jest szersze od pojęcia wojny, gdyż obejmuje wszelkie przejawy walki zbrojnej. Natomiast wojna, ujmowana tradycyjnie, jest przeciwstawiana stanowi pokoju i oznacza sytuację walki zbrojnej między państwami.

ZAMIAST WSTĘPU

Charakterystycznymi dla ery industrialnej konfliktami zbrojnymi były bez wątpienia obie wojny światowe, które ukształtowały myśl wojskową XX wieku. Cechowało je użycie masowych armii wyposażonych w najnowocześniejszy sprzęt dostępny dzięki rozwojowi przemysłu ciężkiego. Artyleria, potem czołgi i samoloty stały się synonimem śmiercionośności i skuteczności w bitwach i operacjach. Wiele wojen w drugiej połowie minionego stulecia nosiło znamiona wojen światowych, charakteryzując się masowością i linearnością. W wybuchających na całym globie lokalnych konfliktach zbrojnych także wykorzystywano wszelką dostępną broń śmiercionośną. W wielu przypadkach były to czołgi i artyleria, nadal decydujące o powodzeniu w bitwie.

Swoistym novum była koncepcja operacji powietrzno-lądowej rozwinięta przez teoretyków wojskowych USA oraz później NATO pod koniec lat osiemdziesiątych. Zakładała ona współpracę sił powietrznych z manewrującymi wojskami lądowymi, która miała na celu zniszczenie potencjału bojowego przeciwnika nie tylko na przednim skraju, lecz także w głębi ugrupowania. Przełomem w tej koncepcji było zastosowanie lotniczych pocisków i bomb precyzyjnego rażenia, a także wysuniętych obserwatorów kontroli przestrzeni powietrznej (JTAC), którzy

Trzy fale, które przetoczyły się w historii ludzkości, są to: rewolucja agrarna (I fala), przemysłowa (II fala) oraz informacyjna (III fala). Zmieniły one ludzkość, ale każda z nich występowała równocześnie z kolejną, tak jak i dziś w erze trzeciej fali zdobywającej dominację na świecie są państwa i narody tkwiące jeszcze w drugiej, a nawet i w pierwszej fali.

SHUTTERSTOCK

1 M. Wrzosek, *Wojny przyszłości,* Warszawa 2018, s. 18.

wyposażeni w odpowiedni sprzęt łączności i naprowadzania statków powietrznych integrowali uderzenia lotnicze z działaniami walczących wojsk.

Wiele elementów nowej koncepcji prowadzenia wojen dostrzeżono w pierwszej wojnie w rejonie Zatoki Perskiej w 1991 roku. Operacja „Pustynna burza" miała w sobie niemało cech konfliktu zbrojnego opartego na technologii z Toflerowskiej trzeciej fali, to znaczy na komputerach i informacji. Tak zresztą konflikt ten został przedstawiony w mediach (raczej na takie jego pokazanie zgodziło się dowództwo amerykańskie). Przeciętny widz mógł zobaczyć na ekranie pociski uderzające precyzyjnie w cel, a przekaz nadawany bezpośrednio z kabiny pilota utwierdzał społeczeństwo w przekonaniu o zastosowaniu nowej technologii w konflikcie. W rzeczywistości amunicja precyzyjna stanowiła niewielki procent całej amunicji zużytej w tej wojnie, a o powodzeniu operacji nadal decydował raczej śmiercionośny ogień, krótki czas reakcji ogniowej i manewr sprzętem.

Niemniej operacja „Pustynna burza" zainicjowała wdrażanie na wielką skalę technologii informatycznej, otwierając w historii rozwoju sił zbrojnych epokę postindustrialną, w której zasadniczym czynnikiem walki jest wiedza, informacja, szybkość reagowania na zmiany oraz ograniczony do minimum czas reakcji ogniowej. Kolejne konflikty zbrojne z udziałem pierwszej armii trzeciej fali, jak można nazwać siły zbrojne USA, były prowadzone w dużej mierze z użyciem lotnictwa i broni precyzyjnej (Bałkany oraz operacja „Iracka wolność"), wojsk specjalnych i czynników pozamilitarnych (operacja „Enduring Freedom"). Niewątpliwie dalszy rozwój coraz bardziej wyrafinowanych środków walki pozwoli na ewolucję konfliktów w kierunku ich dalszego utechnicznienia, a zastosowanie platform bezzałogowych i robotów w roli żołnierzy ograniczy straty we własnych wojskach.

Obok tego rewolucyjnego nurtu nadal będą jednak rozgrywane konflikty zbrojne oparte na technologiach i ideach drugiej fali. Konflikt w Syrii, wojna z tzw. Państwem Islamskim i w Donbasie, ostatnia wojna o Górny Karabach i inne lokalne konflikty zbrojne toczone współcześnie na świecie pokazują, że wiele państw i organizacji długo jeszcze będzie opierać swoje siły zbrojne i doktryny na założeniach wojny konwencjonalnej, ponieważ na to pozwala im ich potencjał gospodarczy, technologiczny czy społeczny. Nie zmieni tego nawet wybiórcze stosowanie nowoczesnych technologii, na przykład bezzałogowych platform przez Rosję na wschodniej Ukrainie, bojowych BSP przez Azerbejdżan, czy też precyzyjnych uderzeń wykonywanych przez lotnictwo rosyjskie w Syrii, gdzie po raz pierwszy zastosowano terminale KRUS Strielec do naprowadzania sił powietrznych[2].

PRZYCZYNY

Według A. i H. Tofflerów przemianom społecznym zawsze towarzyszył konflikt. Metaforyczne ujęcie rewolucyjnych zmian zachodzących na świecie jako fal pozwala zrozumieć, że są one zazwyczaj bardzo dynamiczne i wywołują przeciwprądy. Powodują zderzenie cywilizacji, wymieszanie różnych systemów i spojrzenia na świat. Trzy fale, które przetoczyły się w historii ludzkości, są to: rewolucja agrarna (I fala), przemysłowa (II fala) oraz informacyjna (trzecia fala). Zmieniły one ludzkość, ale każda z nich występowała równocześnie z kolejną, tak jak i dziś w erze trzeciej fali zdobywającej dominację na świecie są państwa i narody tkwiące jeszcze w drugiej, a nawet i w pierwszej fali. To swoiste wymieszanie struktur i systemów powoduje napięcia i konflikty. Zatem nie można mówić obecnie o konflikcie między Wschodem i Zachodem, czy też Północą i Południem, lecz między cywilizacjami[3]. Rozpoczynająca się era komputerów i informacji, będąca trzecią falą cywilizacyjną, stanowi kolejną rewolucję na naszej planecie *i trudno spodziewać się spokoju i pokoju, to szczyt naiwności*[4].

Odchodząc od teorii zderzeń fal cywilizacyjnych jako źródła konfliktów, należy przyjrzeć się typowym ich przyczynom postrzeganym przez pryzmat społeczny, ekonomiczny i polityczny. Badania naukowe wskazują na kilkanaście najczęściej występujących czynników ryzyka wybuchu konfliktów, do których można zaliczyć:

– zdolność państwa i jego instytucji do wypełniania swoich funkcji,

– występowanie zróżnicowanych grup etnicznych i religijnych w państwie,

– stopień jego demokratyzacji,

– poziom rozwoju gospodarczego,

– niezależność ekonomiczną państwa,

– zdolność organizacji międzynarodowych do realizacji swoich zadań,

– stopień respektowania umów i prawa międzynarodowego,

– dostęp do technologii uzbrojenia oraz stopień ich rozpowszechnienia,

– dostęp do zasobów naturalnych, zwłaszcza kluczowych dla systemu energetycznego państwa,

– inne[5].

Przygotowywane modele rozwoju sytuacji polityczno-ekonomicznej na świecie przewidują, że jeśli nie dojdzie do nieprzewidzianych katastrof natural-

2 M. Gawęda, *Bitwa powietrzno-lądowa po rosyjsku. Przykład z Syrii,* https://www.defence24.pl/bitwa-powietrzno-ladowa-po-rosyjsku-przyklad-z-syrii-analiza/. 15.09.2020.

3 A. Toffler, H. Toffler, *Wojna i antywojna: jak przetrwać na progu XX w.,* Warszawa 1998, s. 24.

4 Ibidem, s. 28.

5 T. Szayna et al., *What Are the Trends in Armed Conflicts, and What Do They Mean for U.S. Defence Policy?,* Rand Corporation 2017, s. 3.

nych lub spowodowanych działalnością człowieka oraz nie nastąpi poważny kryzys ekonomiczny dorównujący skalą wielkiemu kryzysowi z lat trzydziestych dwudziestego wieku, to liczba konfliktów zbrojnych zarówno między państwami, jak i konfliktów wewnętrznych pozostanie na niskim poziomie i nie powinna przekraczać średnio jednego do dwóch rocznie, przy światowej średniej z ostatnich stu lat wynoszącej 2,2 konfliktu rocznie. Sytuacja może jednak zmienić się diametralnie w przypadku wystąpienia globalnego kryzysu, takiego jak choćby pandemia COVID-19, katastrofy naturalne, upadek państw czy też nieusprawiedliwiona agresja jednego z państw pretendujących do roli lokalnego lub globalnego hegemona na państwa słabsze.

Wydaje się, że w obecnej sytuacji geopolitycznej na świecie można wyróżnić kilka zjawisk, które mogą mieć poważny wpływ na bezpieczeństwo. Po pierwsze, wzrost znaczenia Chin. Niedawno prezydent tego kraju Xi Jinping obiecał *wielkie odmłodzenie Chin* – przywrócenie tego, co postrzegają jako należne im miejsce na świecie, i odwrócenie *wieku upokorzenia*.

Po drugie, Rosja, choć nie jest tym samym mocarstwem co dawny Związek Radziecki, staje się coraz bardziej agresywna, interweniując w Mołdawii, Gruzji, na Ukrainie i w Syrii i potwierdzając swoją pozycję wielkiego mocarstwa.

Po trzecie, Unia Europejska jest coraz bardziej podzielona i mniej zainteresowana operacjami pokojowymi. Częściej skupia się na swoich problemach wewnętrznych, pogrążona w kryzysie migracyjnym, zmagająca się ze wzrostem prawicowego populizmu i utrzymującymi się skutkami kryzysu strefy euro. Spowoduje to, że wspólnota europejska nie będzie w stanie zgodnie i skutecznie reagować na pojawiające się na świecie sytuacje kryzysowe.

Wreszcie, mimo międzynarodowej kampanii antyterrorystycznej, Bliski Wschód nadal jest dotknięty islamskim dżihadystycznym terroryzmem, problemami politycznymi i gospodarczymi oraz wzrastającym napięciem między Iranem i Arabią Saudyjską, a także Iranem i Izraelem, co wpływa na konflikty w Syrii i Jemenie, i poza tymi krajami. Nie wydaje się, by problemy te zostały szybko rozwiązane. Prawdopodobnie w kolejnych latach będą stwarzały zagrożenie dla stabilności nie tylko w regionie, lecz także na całym świecie.

Podsumowując, należy stwierdzić, że w ciągu ostatnich stu lat zmniejszyła się liczba zbrojnych konfliktów międzynarodowych oraz wewnętrznych. Istnieją poważne przesłanki, by sądzić, że ów spadek utrzyma się w kolejnej dekadzie. Nie oznacza to jednak wygaszenia wszelkich konfliktów na świecie. Należy zatem liczyć się z możliwością powstania kolejnych o zróżnicowanym natężeniu i zasięgu. W wojnach tych na niespotykaną skalę będzie odgrywać rolę nowoczesna technologia cyfrowa charakterystyczna dla cywilizacji trzeciej fali.

ŚRODKI WALKI

Pod koniec ostatniego stulecia broń osiągnęła maksymalne wartości takich parametrów, jak zasięg, prędkość oraz śmiercionośność. Umożliwił to postęp technologiczny wprost proporcjonalny do liczby wdrażanych kolejnych udoskonaleń i innowacji.

Szybkość miotanego pocisku jest uzależniona od siły wyrzucającej go – jest tak w przypadku tradycyjnej amunicji. Jednakże broń laserowa pozwala razić cele promieniem poruszającym się z prędkością światła, dlatego może być skuteczna w niszczeniu najszybszych nawet rakiet i samolotów. Zgodnie z prawami fizyki nic nie może bowiem poruszać się szybciej. Obecnie broń laserowa jest testowana przez kilka przynajmniej krajów natowskich oraz największe armie spoza Sojuszu, w tym rosyjską i chińską.

Współczesna broń konwencjonalna jest ponad sto tysięcy razy bardziej śmiercionośna niż ta wytwarzana na początku rewolucji przemysłowej. Natomiast broń nuklearna właściwie jest zdolna do unicestwienia ludzkości. Wszystkie te zdolności i cechy broni osiągnęły szczyt możliwości w ostatnich dziesięcioleciach[6].

Z drugiej strony symbolem wojen toczonych w drugiej połowie XX wieku był karabinek AK 47 opracowany przez Kałasznikowa – broń używana najchętniej zarówno przez siły zbrojne, jak i ugrupowania paramilitarne i terrorystyczne. Ten symbol wojen minionej epoki, mimo że nadal groźny i skuteczny, musi odejść do lamusa wraz z wdrożeniem broni precyzyjnego rażenia oraz wykazującej cechy inteligentne, przede wszystkim jednak technologii informacyjnych mających ogromny wpływ na postrzeganie rzeczywistości przez społeczeństwa, takich jak: media, portale społecznościowe czy narzędzia do walki w cyberprzestrzeni. Prowadzone obecnie obserwacje pozwalają na stwierdzenie, że w konfliktach między państwami najważniejsze mogą okazać się pozyskanie przychylności opinii publicznej, izolowanie danego państwa na arenie międzynarodowej, zmiana ogólnie przyjętego systemu wartości czy też destabilizacja jego sytuacji gospodarczej i politycznej.

Nie ulega wątpliwości, że nowe technologie pozwolą na konstruowanie kolejnych środków walki, do których mogą należeć następujące:

– broń geofizyczna,
– broń skierowanej energii,
– broń dźwiękowa,
– platformy bezzałogowe,
– nanotechnologia,
– bionika,
– medycyna genetyczna.

6 Ibidem, s. 36–37.

U.S. AIR NATIONAL GUARD

KONSEKWENCJĄ ROZWOJU TECHNOLOGII KOMPUTEROWYCH I TELEKOMUNIKACYJNYCH JEST CORAZ WIĘKSZA ROLA DZIAŁAŃ PROWADZONYCH W CYBERPRZESTRZENI, KTÓRE BĘDĄ POPRZEDZAĆ PRZYSZŁE KONFLIKTY ZBROJNE I IM TOWARZYSZYĆ.

W wielu pozycjach naukowych traktujących *o broni nieśmiercionośnej* można spotkać tezę, że w przyszłych konfliktach zbrojnych znajdzie ona szersze zastosowanie, choćby ze względów humanitarnych. Powszechnie stosowane są już niekinetyczne środki oddziaływania, takie jak choćby elementy walki radioelektronicznej. W niektórych armiach wdrożono pociski karbonowe lub bomby elektromagnetyczne zwane bombami E, a także broń akustyczną i lasery oślepiające. W fazie badań są natomiast przeciwmaterialne środki chemiczne.

Broń palna, a nawet nuklearna muszą ustąpić nowemu istotnemu czynnikowi cechującemu Toflerowską trzecią falę cywilizacyjną, czyli informacji. Wspierała ona poprzednio broń kinetyczną, teraz sama staje się bronią. Informacja przestaje być wyłącznie czynnikiem umożliwiającym użycie broni śmiercionośnej do zniszczenia celów i żołnierzy przeciwnika czy też pozbawienia go ważnej infrastruktury. Stała się bronią zapewniającą zwycięstwo. Oddziaływanie na ludzi w mediach społecznych, wpływanie na ich psychikę, wywoływanie lęku, a nawet paniki powodują polityczną destabilizację państwa i osłabienie jego gospodarki.

Nie ulega wątpliwości, że żyjemy w wieku informacji, co jest konsekwencją szybkiego rozwoju komputerów oraz technologii przesyłania danych na dowolną odległość z szybkością światła. Połączenie komputerów z telekomunikacją doprowadziło do wybuchu rewolucji informacyjnej, w której informacja jest już nie tylko wiadomością, lecz swoistym medium, czyli integralną częścią systemu, za pomocą którego jest ona przesyłana i odbierana[7]. Informacja staje się niematerialnym dobrem, bronią o randze nie mniejszej niż nowoczesne czołgi i wozy bojowe. Bronią, która decyduje o powodzeniu w walce. Według A. i H. Tofflerów może nadejść taki dzień, w którym więcej żołnierzy będzie posługiwało się komputerami niż tradycyjnie rozumianą bronią[8].

Dzięki technologii komputerowej przewaga ilościowa, charakterystyczna dla wojen epoki industrialnej, ustąpiła pierwszeństwa przewadze technologicznej, w której decydujące jest posiadanie wiarygodnych i aktualnych informacji na temat własnych jednostek oraz przeciwnika, zapewniających pełną świadomość sytuacyjną pola walki. Technologia przesyłania danych pozwala na dzielenie się wiedzą

7 Ł. Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*, Kraków 2009, s. 210–211.

8 A. Toffler, H. Toffler, *Wojna i antywojna...,* op.cit., s. 104.

nie tylko w strukturze pionowej (przełożony-podwładny), lecz także poziomej, czyli na dostarczanie ich do wszystkich uczestników walki. To z kolei pozwala na szybsze podejmowanie decyzji niż przeciwnik oraz na skuteczniejsze reagowanie na zachodzące na polu walki zmiany.

Paradoksem jest to, że broń oparta na najnowszej technologii jest skuteczna przeciwko armiom dysponującym zaawansowaną bronią. Bomba naprowadzana na cel przez fale elektromagnetyczne emitowane przez ten cel nie będzie natomiast skuteczna w walce z bojownikiem dysponującym przenośną wyrzutnią przeciwlotniczą czy przeciwpancerną. Zatem broń zaawansowana może okazać się nieskuteczna wobec wojsk państw trzeciego świata lub organizacji militarnych z nich się wywodzących.

FORMY PRZYSZŁYCH KONFLIKTÓW ZBROJNYCH

Jakie więc formy mogą przybrać przyszłe konflikty zbrojne? W opinii autora, nie można obecnie wykluczyć wybuchu *konwencjonalnych konfliktów zbrojnych* (konflikty technologiczne) toczących się między państwami (sojuszami). W odróżnieniu od XX wieku podstawowym warunkiem zwycięstwa w konflikcie technologicznym zamiast przewagi ognia i pancerza będzie supremacja informatyczna. Wydajne i sprawne systemy dowodzenia i rozpoznania umożliwią szybsze podejmowanie decyzji i wdrażanie jej w życie, a zatem zapewnią przewagę nad wolniej działającymi jednostkami przeciwnika oraz umożliwią rażenie go bronią precyzyjną.

W ten sposób stopniowo *konflikt technologiczny* może przerodzić się w *wojnę sieciocentryczną*. Jest to oparta na przewadze informacyjnej koncepcja prowadzenia działań bojowych, według której wzrost siły bojowej jest generowany przez połączenie w sieć informacyjną sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia i tempa operacji oraz synchronizacji działań bojowych. Czy przyjmie to formę wojny robotów? Wiele przesłanek świadczy o tym, że tak! Jednakże, na co wskazuje lokalny konflikt w Górnym Karabachu, precyzyjne pociski wystrzeliwane z pokładów platform bezzałogowych oraz skuteczny system wsparcia ogniowego nadal mogą przesądzić o wyniku starcia.

Wojna asymetryczna to sposób walki stosowany przez państwo lub częściej podmiot niepaństwowy, na przykład ugrupowania partyzanckie lub terrorystyczne, odrzucające reguły i zasady wojny charakterystyczne dla przeciwnika oraz podejmujące działania niespodziewane i diametralnie różniące się od metod i instrumentów wojny uznawanych ogólnie za legalne i akceptowalne. Działania asymetryczne wykorzystują słabe punkty strony przeciwnej i podważają jej przewagę militarną, polityczną i ekonomiczną. Konieczność podjęcia działań asymetrycznych najczęściej jest związana z dużą przewagą technologiczną przeciwnika. Słabsza strona nie jest w stanie stanąć z nim oko w oko, zatem próbuje zmienić niekorzystną asymetrię technologiczną na korzystną dla siebie asymetrię taktyczną.

Działania takie są podejmowane w cieniu groźby użycia broni masowego rażenia, w tym nuklearnej, chemicznej i biologicznej. Arsenały jądrowe nadal stanowią skuteczny czynnik odstraszania i nie ma wątpliwości, że w ich posiadanie mogą wejść kolejne państwa, a nawet, co gorsza, ugrupowania terrorystyczne.

Analizując działania rosyjskie w Donbasie, nie można nie zauważyć *nieformalnej* i niewypowiedzianej wojny, jaką prowadzi to państwo z Ukrainą. Wspieranie rebeliantów w formie ich szkolenia oraz dostarczania sprzętu wojskowego, żywności i surowców niezbędnych do funkcjonowania samozwańczych republik są działaniami realizowanymi w ramach tej wojny, mającymi na celu usankcjonowanie zaistniałej sytuacji, a przy tym trwałe utrzymanie zagarniętego Krymu. Niewypowiedziane wojny nie są niczym nowym w historii ludzkości. Klasycznym przykładem jest wojna domowa w Hiszpanii toczona w latach 1936–1939, w której po jednej stronie walczyły jednostki faszystowskie z Włoch oraz Niemiec, po drugiej zaś przeszkoleni przez Związek Radziecki bojownicy komunistyczni. Okres zimnowojenny także charakteryzował się konfliktami lokalnymi, w których były zaangażowane dwa biegunowe mocarstwa toczące ze sobą niewypowiedzianą wojnę, wspierające i szkolące żołnierzy koreańskich, wietnamskich, syryjskich, egipskich, izraelskich i innych uczestników lokalnych wojen. Nie będzie zatem błędem, jeśli przyszłe konflikty zbrojne zostaną podzielone na wojny formalne i nieformalne (wypowiedziane i niewypowiedziane) oraz na tzw. szarą strefę wojny, czyli stan pośredni między wojną a pokojem[9].

Wojna nieformalna z założenia określonego na początku XXI wieku miała toczyć się między państwem i organizacją, siłami i ugrupowaniami niepaństwowymi, nieformalnymi z punktu prawnego, niestanowiącymi prawnych podmiotów międzynarodowych[10]. Wojny nieformalne będą prawdopodobnie wybuchać, tak jak do tej pory, na tle konfliktów etnicznych, rasowych, religijnych, ekonomicznych i ideologicznych. Niewypowiedzianych konfliktów zbrojnych toczonych w drugiej połowie XX wieku przez państwo przeciwko podmiotom niepaństwowym można wyliczyć wiele. Klasycznym przykładem jest wojna między Republiką Wietnamu Połu-

9 S. Metz, *Armed Conflicts in the 21st Century: The Information Revolution and post-Modern Warfare*, Strategic Studies Institute, Carlisle 2000, s. 27.

10 Ibidem, s. XII.

dniowego i Wietkongiem, Izraelem i Hezbollahem czy międzynarodowa walka z Al-Kaidą, samozwańczym Państwem Islamskim itp. Za wieloma organizacjami stały jednak państwa wspierające je w walce przeciwko innym państwom, jak choćby Wietkong wspierany był przez Wietnam Północny, Chiny i ZSRR, Iran zaś wspierał Hezbollah. Ukraina walcząca z samozwańczymi republikami donieckimi musi stawić w rzeczywistości czoła Rosji wspierającej je ekonomicznie, politycznie i militarnie. Zatem mamy tu do czynienia z klasyczną formą nieformalnej wojny nie tylko między państwem i podmiotami niepaństwowymi, lecz także między dwoma państwami. Taka wojna ma miejsce bez wątpienia również między Izraelem i Iranem czy też Arabią Saudyjską i Katarem oraz wspomnianym Iranem. Zdaniem autora, wojny nieformalne mogą występować coraz częściej, choćby ze względu na postęp technologii informatycznych pozwalających na skryte oddziaływanie na wybrane państwo metodą cyberataków i działań informacyjnych. Będą one zjawiskiem częstszym niż wojny formalne, a zatem będą miały strategiczny wpływ na sytuację polityczno-gospodarczą na świecie.

Konsekwencją rozwoju technologii komputerowych i telekomunikacyjnych jest coraz większa rola *działań informacyjnych* oraz prowadzonych *w cyberprzestrzeni*, które będą poprzedzać przyszłe konflikty zbrojne i im towarzyszyć. Im większy jest stopień rozwoju technologicznego państwa, tym większe ma ono zdolności do prowadzenia wojny w cyberprzestrzeni. Jednakże staje się bardziej podatne na ataki w tej sferze. Według Johna Adamsa *państwa dysponujące dużymi zdolnościami do wojny informacyjnej są jednocześnie najbardziej podatne na atak* […] *pojedyncza osoba uzbrojona jedynie w komputer i modem może dosłownie wziąć Amerykę jako zakładnika*[11]. Czy zatem przyszłe wojny będą toczone wyłącznie w cyberprzestrzeni? Trudno odpowiedzieć jednoznacznie na to pytanie. Nie ulega jednak wątpliwości, że dziś walka w cyberprzestrzeni toczy się zarówno w obszarach polityczno-ekonomicznych, jak i militarnych. W siłach zbrojnych tworzone są wyspecjalizowane jednostki do walki w tej domenie.

W 2007 roku F. Hoffman, emerytowany oficer armii Stanów Zjednoczonych, przedstawił koncepcję *wojny hybrydowej*, definiując ją jako działania prowadzone z zastosowaniem różnych sposobów walki (legalnych i nielegalnych), w tym w formie konwencjonalnych działań zbrojnych, działań nieregularnych, informacyjnych, w cyberprzestrzeni, aktów terrorystycznych oraz przestępstw kryminalnych.

Najważniejszą różnicą między konfliktem hybrydowym i konwencjonalnym jest to, że wszelkie niekonwencjonalne działania ofensywne podejmowane przez siły regularne i nieregularne nie służą wsparciu w walce wojsk operacyjnych (konwencjonalnych), lecz same w sobie są narzędziem do osiągnięcia zwycięstwa oraz zamierzonych korzyści politycznych. Nie są zatem elementem wspierającym, lecz głównym sposobem realizacji zadań.

NAJCENNIEJSZĄ I NAJSKUTECZNIEJSZĄ KTÓREJ BĘDZIE MOŻNA WYGRYWAĆ

Groźbę pojawienia się wojny hybrydowej, w której obiektem agresji mogą być państwa zachodnie, dostrzeżono już pod koniec lat dziewięćdziesiątych XX wieku. Elementami działań hybrydowych znamionowały się: wojny czeczeńskie prowadzone w latach 1994–1996 oraz 1999–2000, wojna gruzińska (sierpień, 2008) oraz działania Hezbollahu przeciwko Izraelowi w 2006 roku. W tym ostatnim przypadku po raz pierwszy w historii mocarstwo militarne nie zdołało pokonać paramilitarnych sił organizacji niepaństwowej. Hoffman w swojej pracy pod tytułem *Conflict in the 21st Century: The Rise of Hybrid Wars*[12] przedstawił zagrożenia hybrydowe łączące różne sposoby walki zbrojnej, w tym działania konwencjonalne oraz nieregularne, akty terrorystyczne z użyciem każdej możliwej przemocy skierowanej zwłaszcza przeciwko życiu ludzkiemu, a także akty kryminalne. Do podstawowych zagrożeń bezpieczeństwa państwa płynących z ataku hybrydowego zaliczył:

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

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

– dążenie do izolacji politycznej państwa atakowanego;

– sankcje ekonomiczne;

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

11 J. Adams, *The Next World War. The Warriors and Weapons of the New Battlefield in Cyberspace,* Arrow, London 1999, s. 4.

12 F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf/. 15.09.2020.

– ofensywę propagandową w mediach, zwłaszcza w telewizji oraz na forach internetowych, w tym wpływanie na opinię publiczną przez przekazywanie stronniczych, a nawet sfałszowanych wiadomości (*fake news*) oraz opinii;
– akty sabotażu i dywersji;
– ataki terrorystyczne;
– akty kryminalne.

O wojnie hybrydowej można mówić w przypadku, gdy wystąpi większość wymienionych zagrożeń jednocześnie i spowodują one poważną destabilizację sytuacji politycznej i ekonomicznej w danym państwie oraz wywołają niezadowolenie dużych grup społeczeństwa.

W wojnie tej obiektami ataku są przede wszystkim elementy newralgiczne dla sprawnego funkcjonowania państwa *(critical functions)*. Są to najistotniejsze przedsięwzięcia oraz działania polityczne, wojskowe, ekonomiczne, społeczne, informacyjne i infrastrukturalne, których zatrzymanie lub zakłócenie spowoduje znaczące obniżenie zdolności państwa do realizacji stojących przed nim zadań[13]. Elementami krytycznymi mogą być ważni politycy, jednostki wojskowe i uzbrojenie, sieć energetyczna państwa, system prawny, ustrój i wiele innych.

Wojna hybrydowa ma w zamierzeniu ułatwić szybkie osiągnięcie celów politycznych skierowanych przeciwko każdemu państwu (zarówno o mniejszym, jak i większym potencjale militarnym i gospodarczym) dzięki wykorzystaniu jego słabości. Jest to przeciwieństwo tradycyjnie pojmowanych konfliktów zbrojnych, w których z zasady zwyciężała strona mającą przewagę militarną, materialną, technologiczną i inną.

Mimo braku oficjalnego wypowiedzenia wojny w konflikcie hybrydowym potencjalny agresor, jeśli sytuacja go do tego zmusi, w każdej chwili może użyć regularnych sił wojskowych, tak jak uczynił to na Ukrainie. Rosja nie wahała się zaangażować batalionowych grup bojowych oraz artylerii, w tym rakietowej, mającej ogromną siłę rażenia. Niemniej mogą to być także mniejsze jednostki (wielkości kompanii i plutonu), wyposażone w lekkie, ale nowoczesne i skuteczne systemy obrony przeciwlotniczej oraz środki przeciwpancerne. W ten sposób agresor będzie starał się osiągnąć lokalną przewagę w powietrzu i na lądzie. Jest wysoce prawdopodobne, że w wyniku takich działań siły powietrzne zaatakowanego państwa nie będą zdolne do sprawnego działania, tak jak stało się to z lotnictwem Ukrainy.

WIELE NIEWIADOMYCH

Podsumowując przedstawione rozważania, należy podkreślić, że formy konfliktów zbrojnych podlegają nieustannym przeobrażeniom. Podejmuje się więc kroki w celu pokonania ograniczeń z poprzedniej wojny. Zmiany polegają na wdrażaniu nowych technologii, takich jak między innymi efektywniejsze sensory, komunikacja satelitarna, platformy bezzałogowe i broń nieśmiercionośna.

Nie ulega wątpliwości, że zmiany środowiskowe – podobnie jak czynniki polityczne – są często głównym elementem kształtującym konflikt, czego godnym uwagi przykładem jest wojna domowa w Syrii[14]. Od dawna uważa się, że poważnym determinantem konfliktów zbrojnych są w coraz bardziej zglobalizowanym świecie aspekty ekonomiczne. Dobrobyt państw zależy od handlu i dostępu do kredytów międzynarodowych. Działania gospodarcze mogą służyć również jako potężne narzędzia wojenne używane zamiast przemocy. Sposób prowadzenia wojen mogą nadal determinować inne czynniki, takie jak prawo międzynarodowe, opinia publiczna, media i ich coraz większy zasięg czy też postępująca urbanizacja.

Jaka jest zatem przyszłość wojen? Nie ma jednej odpowiedzi na to pytanie. Problemu tego nie można sprowadzić do rozwoju technologii informatycznych, sztucznej inteligencji, broni precyzyjnej czy też ekspansji Rosji i Chin bez względu na to, jak znaczący może być każdy z tych indywidualnych trendów. Wydaje się, że główną lekcją z przeszłości jest to, by nie skupiać się wyłącznie na jednym trendzie czy zjawisku, ale starać się dostrzegać całościowo prawidłowości zachodzące w środowisku bezpieczeństwa międzynarodowego. Zdaniem autora, najcenniejszą i najskuteczniejszą bronią będzie wiedza, dzięki której będzie można wygrywać wojny, a także im zapobiegać. Przyszli żołnierze, „wojownicy wiedzy", będą doskonale posługiwać się nowoczesną techniką bojową, a także będą rozumieli zachodzące zjawiska i procesy w środowisku bezpieczeństwa i sztuce wojennej. Informacja będzie ich bronią, która pozwoli im szybciej podejmować decyzję, szybciej się przemieszczać i celniej razić przeciwnika. To przesłanie należy przekazać młodym adeptom sztuki wojennej. ■

BRONIĄ BĘDZIE WIEDZA, DZIĘKI WOJNY, A TAKŻE IM ZAPOBIEGAĆ

13 *Understanding Hybrid Warfare*, A Multinational Capability Development Campaign Project, MCDC, January 2017, s. 9.
14 Zob.: P.H. Gleick, *Water, Drought, Climate Change, and Conflict in Syria* [w:] *Weather, Climate, and Society,* Vol. 6, No. 3, July 2014.

Artyleria w zwalczaniu **systemów antydostępowych**

DYSPONOWANIE CORAZ WIĘKSZYMI ZDOLNOŚCIAMI DO PRECYZYJNEGO I GŁĘBOKIEGO RAŻENIA MOŻE OKAZAĆ SIĘ DECYDUJĄCYM CZYNNIKIEM POZWALAJĄCYM NA ZDOMINOWANIE SYSTEMÓW A2/AD ORAZ UMOŻLIWI REALIZACJĘ ZADAŃ WŁASNEMU LOTNICTWU.

płk dr hab. inż. Norbert Świętochowski, płk dypl. rez. Dariusz Rewak

Norbert Świętochowski jest dyrektorem Instytutu Dowodzenia Akademii Wojsk Lądowych.

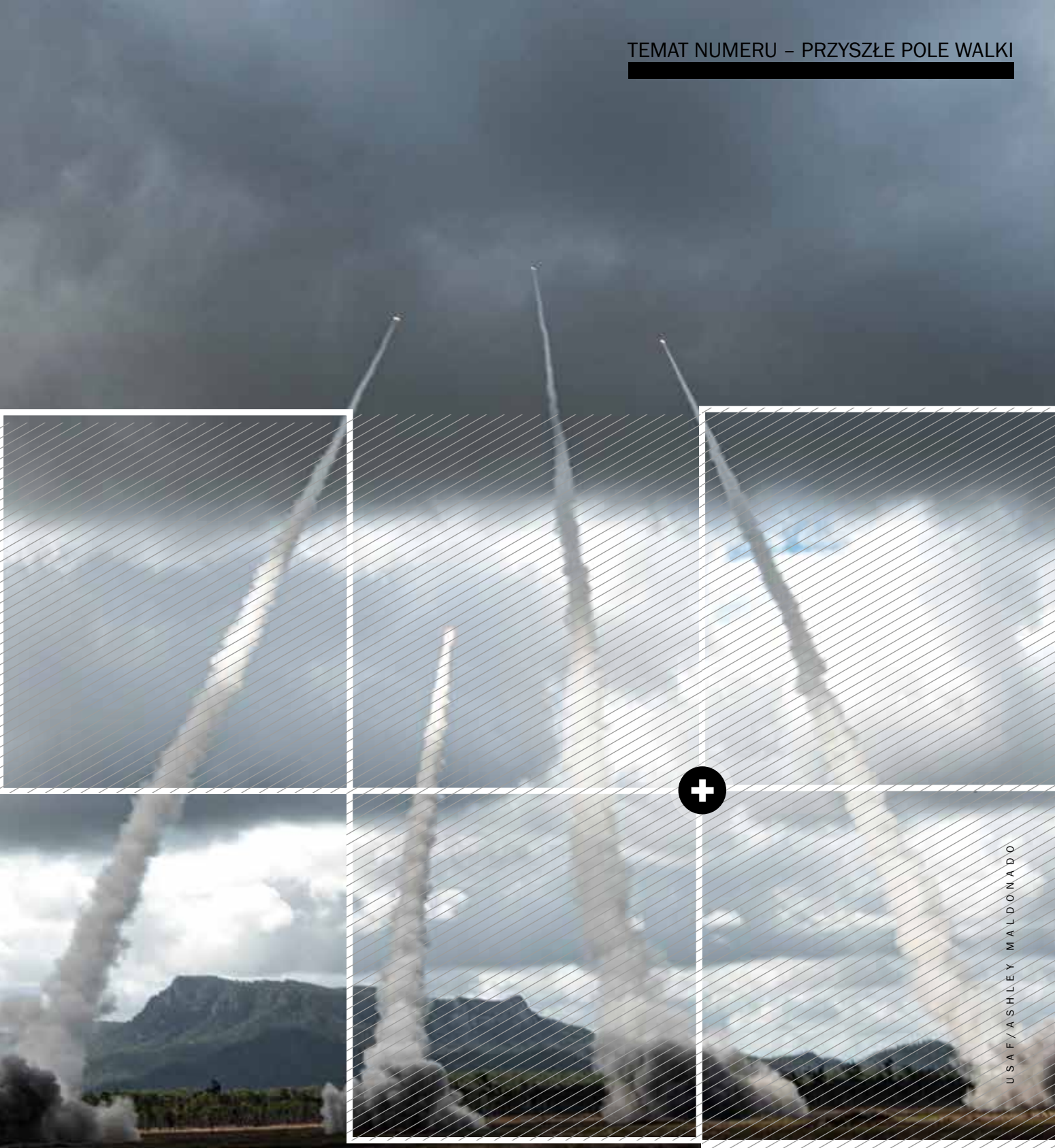
Dariusz Rewak jest doktorantem w Szkole Doktorskiej WAT.

Współczesne systemy antydostępowe A2/AD (Access Denial/Area Denial) są definiowane jako połączenie oddziaływania wszelkich możliwych środków, które mogą wielowarstwowo ograniczyć dostęp potencjalnego przeciwnika do danego obszaru (teatru) działań. Ich działanie polega między innymi na radioelektronicznym zakłócaniu systemów naprowadzających, na paraliżowaniu systemów łączności, komunikacji i cyfrowej transmisji danych oraz na zestrzeliwaniu pocisków manewrujących dalekiego zasięgu, BSP i samolotów. Głównym założeniem koncepcji antydostępowej jest pozbawienie przeciwnika możliwości wejścia na teren danego teatru działań (A2 – *Anti-Access*) za pomocą środków rażenia dalekiego zasięgu. Ponadto pozbawienie go swobody działania na tym obszarze (AD – *Area-Denial*) za pomocą środków rażenia średniego i krótkiego zasięgu. Do realizacji zadań A2/AD używa się pocisków typu ziemia–powietrze (*Surface-to-Air Missile* – SAM), przeciwokrętowych pocisków balistycznych (*Anti-Ahip Balistic Missile* – ASBM) oraz pocisków manewrujących (*Anti-Ship Cruise Missile* – ASCM), a w ostatnim czasie również amunicji artyleryjskiej o zwiększonej donośności *(Long Range Precision Fires* – LRPF*)*.

PRZESŁANIE

Doświadczenia wyniesione z działań prowadzonych na wschodzie Ukrainy oraz obserwacja konfliktu w Syrii pozwalają stwierdzić, że do czasu pozbawienia jednej ze stron konfliktu zdolności antydostępowych wywalczenie przewagi w powietrzu przez siły drugiej strony będzie praktycznie niemożliwe lub bardzo utrudnione. W związku z tym w armiach wchodzących w skład NATO, w tym w Siłach Zbrojnych Rzeczypospolitej Polskiej, radykalnej zmianie powinna ulec koncepcja prowadzenia operacji powietrzno-lądowych, z większym niż dotychczas zaangażowaniem wojsk rakietowych i artylerii. Podjęta w artykule problematyka jest próbą wykazania, że w obecnych uwarunkowaniach geopolitycznych nasze siły zbrojne, wspólnie z sojusznikami z państw NATO, w najbliższej perspektywie czasowej muszą odbudować swoje zdolności uderzeniowo-ogniowe, głównie komponentu lądowego, który w warunkach braku osłony i wsparcia z powietrza będzie odgrywał główną rolę w przełamywaniu systemów A2/AD przeciwnika. Potencjał ogniowy systemów rażenia, zwłaszcza wojsk rakietowych i artylerii, jakim w początkowej fazie działań powinien dysponować dowódca sił połączonych (naczelny dowódca), pozwoli mu w krótkim czasie na utworzenie w systemie obrony przeciwlotniczej przeciwnika luk i korytarzy bezpiecznego przelotu dla manewrujących pocisków rakietowych precyzyjnego rażenia dalekiego zasięgu, BSP oraz załogowych statków sił powietrznych Sojuszu realizujących zadania izolacji oraz bezpośredniego wsparcia powietrznego.

W scenariusze te doskonale wpisuje się prowadzona obecnie bardzo dynamiczna modernizacja polskiej artylerii połączona z zapowiedziami wprowadzenia do jej wyposażenia nowoczesnych rodzajów amunicji artyleryjskiej i rakietowej, w tym precyzyjnego rażenia, pozwalającej na realizację skutecznych uderzeń ogniowych ze stref wolnych



USAF/ASHLEY MALDONADO

Artyleria operacyjna będzie dysponować systemami rakietowymi M270 MLRS (*Multiple Launch Rocket System*) i M142 HIMARS (*High Mobility Artillery Rocket System*), dla których przewiduje się maksymalną donośność strzelania pociskami taktycznymi PrSM (*Precision Strike Missle*) nawet do 700 km.

od oddziaływania artylerii przeciwnika. Niemniej proces ten powinien iść w parze z zasadniczymi zmianami w taktyce użycia wojsk rakietowych i artylerii w działaniach bojowych, w systemie strzelania i kierowania ogniem, a także – co najważniejsze – ze zmianami w procesie szkolenia polskich artylerzystów.

Należy zatem określić zdolności artylerii do zwalczania systemów antydostępowych A2/AD, polegające na precyzyjnych uderzeniach na zwiększonych donośnościach strzelania w ramach LRPF (*Long Range Precision Fires*). Autorzy zakładają, że siły NATO w pierwszym okresie konfliktu pełnoskalowego z równorzędnym przeciwnikiem utracą panowanie w powietrzu, priorytetem będzie zatem szybkie jego odzyskanie. Artyleria jako rodzaj wojsk mający coraz większe możliwości precyzyjnego i głębokiego rażenia może stać się decydującym czynnikiem pozwalającym na zdominowanie systemów A2/AD i umożliwiającym realizację zadań własnemu lotnictwu.

ELEMENTY SYSTEMU ANTYDOSTĘPOWEGO HIPOTETYCZNEGO PRZECIWNIKA

Państwa potencjalnie słabsze jako przeciwwagę dla wyższości technologicznej sił zbrojnych NATO, zwłaszcza armii Stanów Zjednoczonych, od lat rozwijają swoje instalacje A2/AD z wykorzystaniem systemów radarowych, pocisków rakietowych obrony powietrznej, pocisków klasy ziemia–ziemia oraz ziemia–woda, przeznaczonych do izolacji określonych obszarów pola walki oraz wykonywania uderzeń na różnorodne cele lądowe i morskie. Systemy te w założeniu mają uniemożliwić dostęp silniejszemu przeciwnikowi do obszaru działań, zwłaszcza drogą powietrzną. Ocenia się, że obecnie najlepiej rozwiniętym systemem A2/AD dysponuje Rosja. *Obronna bańka* to potoczna nazwa, jakiej używają Rosjanie dla systemu będącego kombinacją wielu zestawów uzbrojenia, m.in.: walki elektronicznej, przeciwlotniczych i przeciwbalistycznych systemów rakietowych i radarowych, pocisków manewrujących dalekiego zasięgu, zestawów rakiet balistycznych, systemów BSP oraz innych środków precyzyjnego rażenia wycelowanych w obiekty naziemne i morskie. Trzon systemu A2/AD Federacji Rosyjskiej stanowią siły powietrzno-kosmiczne, w skład których wchodzi obrona przeciwlotnicza dysponująca zestawami rakietowymi różnego rodzaju i typu, m.in.: S-300 i S-400, Buk, Tor, Pancyr i Tunguska. Oprócz instalacji stacjonarnych Rosjanie mają wiele zestawów mobilnych, którymi można szybko manewrować, uelastyczniając tym samym własne antydostępowe możliwości obronne. Rosyjska strategia A2/AD polega na angażowaniu nie tylko przeciwlotniczych zestawów rakietowych, lecz także różnorodnych środków i systemów walki radioelektronicznej (WRE). Szczególnie groźne są zestawy 1RŁ257 Krasucha-4, które oprócz możliwości zagłuszania sygnałów radiolokacyjnych mogą przechwytywać i zakłócać sygnały emitowane przez satelity rozpoznawcze, samoloty wczesnego ostrzegania, bezzałogowe statki powietrzne oraz naziemne stacje naprowadzania. Zestawy tego typu o zasięgu skutecznego oddziaływania wynoszącym od 150 do 300 km są kluczowym elementem A2/AD. Dodatkowo mogą być uzupełniane naziemnymi zestawami artyleryjskimi i rakietowymi, dzięki którym można atakować zarówno cele naziemne, jak i nawodne w odległości 120 km i większej, w tym także z użyciem amunicji precyzyjnego rażenia. Przykładowo, rosyjska brygada zmechanizowana w porównaniu z jej polską odpowiedniczką dysponuje miażdżącą przewagą w sile ognia artyleryjskiego oraz możliwościach oddziaływania WRE, mając w swojej strukturze ponad 80 różnych dział i wyrzutni rakietowych oraz batalion walki radioelektronicznej.

Większość rosyjskich zgrupowań wojskowych, zwłaszcza tych wchodzących skład Zachodniego Okręgu Wojskowego, już na szczeblu dywizji, a także brygady i batalionu dysponuje systemami obrony antydostępowej. Zgromadzony na terenie obwodu kaliningradzkiego oraz Zachodniego Okręgu Wojskowego, w ostatnim czasie również na terytorium Białorusi, potencjał bojowy jest obecnie głównym zagrożeniem dla sił Sojuszu w obszarze północno-wschodniej flanki NATO. Federacja Rosyjska posiada w tej dziedzinie ogromną przewagę w postaci ognia artyleryjskiego i rakietowego oraz oddziaływania A2/AD. Oznacza to, że w przypadku wybuchu konfliktu będzie zdolna do bezkarnego oddziaływania nie tylko na obiekty znajdujące się w bezpośredniej strefie działań, lecz także do niszczenia i obezwładniania wojsk podchodzących do rejonów działań oraz drugich rzutów rozmieszczonych w rejonach wyjściowych i ześrodkowania. Ponadto będzie kontrolować przestrzeń powietrzną Litwy, południowej części Łotwy oraz całej północnej części naszego kraju. Bardzo ważnym elementem systemu A2/AD na terenie obwodu kaliningradzkiego jest stacja radarowa typu Woroneż-DM[1], która ma zdolność do kontrolowania przestrzeni powietrznej nie tylko nad Bałtykiem, lecz również nad obszarem prawie całej Europy Północnej.

Trzon sił lądowych w tym obwodzie stanowi 11 Korpus Armijny[2], którego ofensywnym atutem są wojska rakietowe oficjalnie wyposażone w systemy rakietowe typu Toczka-U i Toczka-M (w kodzie NATO: SS-21 Scarab), a nieoficjalnie w zestawy

1 Stacja Woroneż-DM może wykrywać obiekty na dystansie do 6 tys. km. Wchodzi w skład rosyjskiego systemu wczesnego ostrzegania przed pociskami balistycznymi. Biorąc pod uwagę lokalizację (najbardziej na zachód wysunięty taki obiekt), ma ona bardzo duże znaczenie w razie zbrojnego konfliktu z NATO.

2 11 Korpus Armijny w Kaliningradzie został sformowany prawdopodobnie wiosną 2016 roku. Stało się to bez rozgłosu. Pierwsze informacje medialne pojawiły się dopiero 9 maja 2016 roku przy okazji parady zwycięstwa.

Iskander-M/K (w kodzie NATO: SS-26 Stone). Rakiety te wykonane w technologii *stealth* mogą teoretycznie razić cele na obszarze prawie całego naszego kraju, sięgając również Berlina i Sztokholmu, a rakiety systemu Kalibr-NK – większą część Europy Zachodniej. Co więcej, rosyjska armia zamierza w najbliższym czasie zwiększyć liczbę wyrzutni Iskander w brygadach rakietowych z 12 do 16, co realnie zwiększy ich możliwości jednoczesnego rażenia do 32 obiektów. Według doniesień prasowych system Iskander został włączony ostatnio do odpowiednika rosyjskiego systemu targetingu przez rosyjski wojskowy internet.

Na terenie obwodu kaliningradzkiego oraz Białorusi można wyodrębnić wiele systemów rakietowych i artyleryjsko-rakietowych, które powinny znaleźć się na priorytetowych listach celów NATO do rażenia przez systemy artyleryjskie i rakietowe sił sojuszniczych. Zdaniem autorów artykułu, do najważniejszych obiektów można zaliczyć:

– systemy obrony przeciwlotniczej S-400 i S-300PS oraz Tor;

– hipersoniczne pociski rakietowe P-800 Oniks (w kodzie NATO: SS-N-26 Strobile) z rakietowego kompleksu nadbrzeżnego K-300P Bastion-P (w kodzie NATO: SS-C-5 Stooge) o zasięgu około 450 km;

– pociski rakietowe X-35 Uran z rakietowego kompleksu nadbrzeżnego Bał/ZK60 (w kodzie NATO: SSC-6 Sennight) o zasięgu od 120 do 260 km;

– mobilne kompleksy rakietowe klasy woda–woda P-35 Riedut z naddźwiękowymi pociskami przeciwokrętowymi P-35 o zasięgu do 250 km;

– mobilne zestawy rakiet balistycznych klasy ziemia–ziemia systemu Iskander-M (w kodzie NATO: SS-26 Stone) o oficjalnym zasięgu do 500 km, nieoficjalnie nawet do 1500 km;

– okręty wyposażone w rakiety manewrujące 3M14 systemu Kalibr o zasięgu do 2500 km, które mogą być odpalane również z mobilnych wyrzutni systemu Iskander-K;

– mobilne zestawy rakietowe Polonez o zasięgu sięgającym od 200 do 300 km;

– mobilne zestawy rakiet balistycznych systemu Toczka-U o zasięgu do 120 km i Toczka-M o zasięgu do 185 km;

– mobilne wyrzutnie rakietowe systemów BM-21 Tornado-G o zasięgu do 40 km, BM-27 Uragan o zasięgu do 70 km i BM-30 Smiercz o zasięgu do 90 km, a ostatnio nawet do 120 km w przypadku systemu Tornado-S.

Zestawienie to dowodzi, że oprócz skutecznego blokowania dostępu sił powietrznych i bezzałogowych systemów rozpoznawczych do obszaru działań w obrębie przesmyku suwalskiego strona przeciwna ma wystarczające siły i środki, by móc skutecznie oddziaływać na cele naziemne i morskie położone na całej głębokości ugrupowania operacyjnego. Mimo prowadzonego przez sojusznicze siły intensywnego rozpoznania zgromadzonego na obrzeżach wschodniej flanki NATO potencjału wojskowego wciąż pozostaje on wielką niewiadomą, którą można analizować i oceniać tylko w wielkim przybliżeniu, głównie na podstawie doniesień i relacji medialnych.

TRENDY ROZWOJU ARTYLERII NATO

Siły zbrojne NATO muszą być przygotowane do prowadzenia działań w warunkach zakłóceń oraz braku wsparcia z powietrza. Taki stan rzeczy będzie się utrzymywał praktycznie do momentu zmniejszenia potencjału zintegrowanej obrony powietrznej przeciwnika oraz stworzenia warunków do wywalczenia przewagi w powietrzu i wprowadzenia do walki sojuszniczych sił powietrznych. W tej fazie konfliktu należy liczyć się ze zmasowanymi uderzeniami artyleryjsko-rakietowymi wykonywanymi pociskami manewrującymi oraz amunicją precyzyjnego rażenia, skierowanymi m.in. na: lotniska, porty, obiekty infrastruktury krytycznej, stanowiska i centra dowodzenia oraz rejony ześrodkowania wojsk. W konsekwencji konieczne będzie wykorzystanie zaawansowanych platform i systemów ISR (Intelligence, Surveillance and Reconnaissance – wywiad, rozpoznanie, obserwacja) w ramach Alliance Ground Surveillance[3], głównie bezzałogowych statków powietrznych typu RQ-4 Global Hawk[4] z obniżonym widmem widzialności elektromagnetycznej, uzupełnionych flotą samolotów rozpoznawczych typu AWACS 20 E-3 operujących na pułapie, który zapewni im możliwość prowadzenia niezakłóconego rozpoznania. Amerykańskie systemy satelitarne będą prawdopodobnie w stanie zagwarantować siłom Sojuszu niezakłóconą transmisję danych, nawigację lądową, śledzenie i lokalizację celów, naprowadzanie amunicji precyzyjnej i korygowanie ognia, a także prowadzenie aktywnej walki radioelektronicznej mającej na celu zakłócanie i obezwładnianie rosyjskich systemów A2/AD[5].

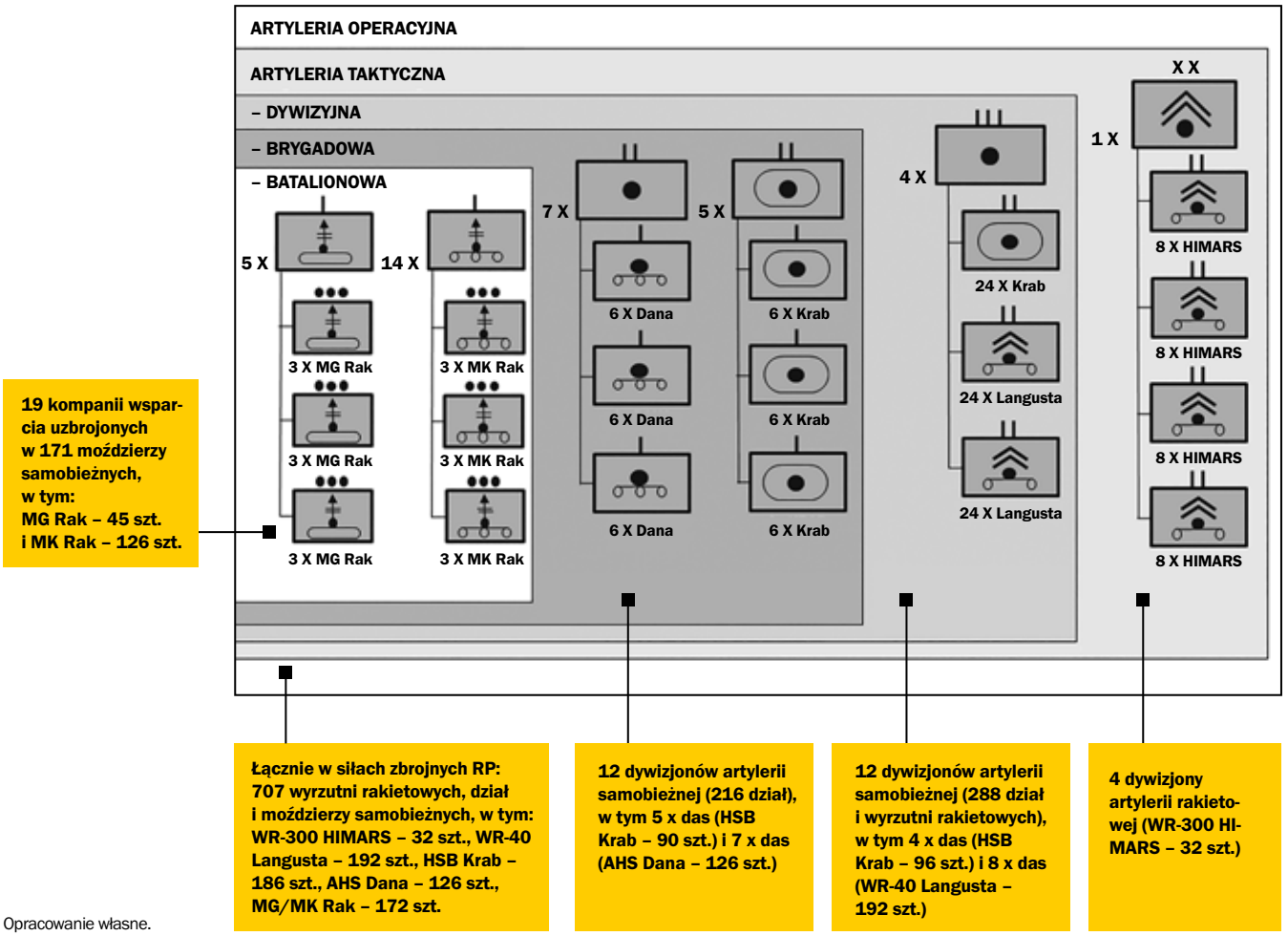
Armia Stanów Zjednoczonych od pewnego czasu pracuje nad koncepcją tzw. operacji wieloaspektowej, która zakłada prowadzenie działań bojowych w warunkach konfliktu zbrojnego z udziałem lub przy zaangażowaniu sił zbrojnych Rosji, a także Chin. Przewiduje się, że w początkowej fazie operacji nie będzie możliwe użycie precyzyjnych środków rażenia dalekiego zasięgu przenoszonych przez lotnictwo, co dodatkowo negatywnie wpłynie na zdolność do prowa-

3 NATO Alliance Ground Surveillance – to jednostka Sojuszu przeznaczona do prowadzenia obserwacji powietrznej z użyciem bezzałogowych statków powietrznych. Miejscem stacjonowania jest baza Sigonella na Sycylii.

4 RQ-4 Global Hawk – to BSP przystosowany do zadań rozpoznawczych, należący do kategorii HALE *(High Altitude Long Endurance)*, czyli operujący na dużej wysokości i z dużą długotrwałością lotu. Prędkość maksymalna RQ-4D to 575 km/h, zasięg wynosi do 16 113 km, natomiast pułap operacyjny – do 18 288 m. Maksymalny czas przebywania w powietrzu to 32 godziny.

5 R.D. Hooker Jr., *How to defend the Baltic States,* The Jamestown Fundation 2019, s. 31.

RYS. STRUKTURA ORGANIZACYJNA WOJSK RAKIETOWYCH I ARTYLERII (WARIANT)



Opracowanie własne.

dzenia działań przez inne rodzaje sił zbrojnych. W związku z tym artyleria, zwłaszcza dalekonośna typu LRPF (*Long Range Precision Fires*), wykonując precyzyjne uderzenia, może stworzyć warunki do wywalczenia panowania w powietrzu. W tym celu w amerykańskich programach modernizacyjnych artylerię podzielono na trzy grupy[6]: taktyczną o bliskim zasięgu (close), operacyjną o głębokim zasięgu (deep) i strategiczną (strategic) o zasięgu powyżej 1000 km.

Artyleria taktyczna będzie obejmować systemy artylerii lufowej (w tym również moździerze) o maksymalnej donośności strzelania nieco ponad 100 km, a docelowo do 200 km. W ramach programu ERCA (*Extended Range Cannon Artillery*) planuje się przezbrojenie istniejących już 155-milimetrowych systemów M777 (holowanego) i M109 (samobieżnego) w nowe lufy długości 55 kalibrów (dla M777) i 58 kalibrów (dla M109 A7 Palladin) oraz wydłużone komory nabojowe obydwu dział mieszczące dodatkowy siódmy modułowy ładunek miotający. Na potrzeby nowych dział opracowano amunicję kalibru 155 mm o symbolu XM1113[7]. Dodatkowo haubica M109 A7

6 B. Kucharski, *AUSA 2018 – przyszłość artylerii za Atlantykiem*, „Wojsko i Technika" 2019, s. 29.

7 XM1113 – pocisk z dodatkowym wzmocnionym ładunkiem SuperCharge XM654, wspomagany rakietowo, kompatybilny z zestawem zapalnika korygującego PGK *(Precision Guidance Kid)*, który przekształca 155-milimetrowe pociski artyleryjskie w sterowaną przez GPS broń umożliwiającą precyzyjną odpowiedź na ostrzał w każdych warunkach atmosferycznych z dokładnością do 50 m. Zob.: B. Kucharski, *AUSA 2018 – przyszłość*..., op.cit., s. 29.

będzie wyposażona w automat ładujący, zapewniający jej szybkostrzelność do sześciu strzałów na minutę.

Artyleria operacyjna będzie dysponować systemami rakietowymi M270 MLRS (*Multiple Launch Rocket System*) i M142 HIMARS (*High Mobility Artillery Rocket System*), dla których przewiduje się maksymalną donośność strzelania pociskami taktycznymi PrSM (*Precision Strike Missle*) nawet do 700 km. Podstawowym zadaniem tego rodzaju artylerii będzie ograniczanie zdolności manewrowych przeciwnika, zwalczanie jego systemów obrony przeciwlotniczej oraz ruchomych celów lądowych i morskich. W odniesieniu do siły rażenia amerykańskiej artylerii rakietowej planuje się zwiększenie maksymalnej donośności pocisków rakietowych kalibru 227 mm w wersji GMLRS-ER do 170 km. Docelowo zestaw HIMARS ma być zintegrowany z systemem zarządzania obroną powietrzną IBCS (*Integrated Air and Missile Defense Battle Command System*). W ten sposób rakiety ATACMS (*Army Tactical Missile System*) kalibru 607 mm będą mogły być włączone do systemu obrony przeciwbalistycznej (wykrywanie i niszczenie wrogich wyrzutni rakiet)[8].

Artyleria strategiczna będzie obejmować dwa systemy[9]:

– działo elektromagnetyczne w ramach artyleryjskiego systemu SSCA (*Strategic Strike Cannon Artillery*) o przewidywanej maksymalnej donośności strzelania do 1600 km;

– rakietowy dwustopniowy system składający się z manewrującego pocisku hipersonicznego o prędkości odpowiadającej Ma do 5, wynoszonego za pomocą nośnika rakietowego SFM (*Strategic Fires Missile*), który według założeń będzie miał zdolność rażenia celów na maksymalnej donośności do 1400 Mm (około 2250 km). Atutem tego rozwiązania, zwłaszcza podczas przełamywania obrony przeciwlotniczej przeciwnika, będzie możliwość pokonania wchodzących w jej skład systemów przeciwrakietowych.

Oprócz działań modernizacyjnych armia Stanów Zjednoczonych dostosowuje obowiązujące doktryny dotyczące użycia artylerii do wyzwań wojny wieloaspektowej. W nowej koncepcji użycia artylerii polowej dużą wagę przywiązuje się do jej współdziałania z innymi rodzajami sił zbrojnych, głównie z siłami powietrznymi, zwłaszcza z lotnictwem taktycznym oraz z systemami obrony powietrznej. Współdziałanie to polega na włączeniu ich do zintegrowanego systemu pozyskiwania danych rozpoznawczych na potrzeby ognia artylerii. W ramach koncepcji połączonego rażenia (*Joint Fires*) amerykańska artyleria rakietowa wykonuje strzelania z wyrzutni MLRS i HIMARS do celów wskazanych przez myśliwce sił powietrznych i marynarki wojennej. Podczas wielu ćwiczeń udowodniono, że ten rodzaj współdziałania może odegrać ważną rolę w warunkach występowania zakłóceń antysystemowych A2/AD, ponieważ wskazywanie celów dla artylerii z bardzo wysokiego pułapu (poza zasięgiem systemów A2/AD) przez samoloty sił powietrznych wyposażone w precyzyjne systemy rozpoznawcze może być realizowane w sposób niezakłócony.

Dzięki modernizacji artyleria polowa jest gotowa do działań w warunkach przyszłego pola walki. W doktrynie jej użycia odchodzi się od koncepcji długotrwałego powierzchniowego rażenia celów amunicją konwencjonalną na rzecz uderzeń precyzyjnych. Dzięki temu wiele celów może zostać wyeliminowanych szybciej i skuteczniej. Poza tym zwiększenie donośności strzelania konwencjonalnych środków artyleryjskich pozwoli na wyprowadzenie ich poza zasięg skutecznego rażenia artyleryjskiego przeciwnika i uniknięcie tym samym ognia kontrbateryjnego (*counterfire*) oraz zakłóceń systemów antydostępowych. Duży zasięg ognia umożliwi rażenie celów rozmieszczonych w głębi ugrupowania przeciwnika i na skrzydłach, a manewr ogniem będzie można zastosować bez potrzeby wykonania czasochłonnego manewru pododdziałami.

POŻĄDANE ZDOLNOŚCI ARTYLERII SIŁ ZBROJNYCH RP

Rozważania na ten temat należy rozpocząć od analizy jednego ze scenariuszy opracowanego przez ekspertów z The Jamestown Fundation, dotyczącego wariantu prowadzenia przez NATO kolektywnej obrony państw bałtyckich w obrębie tzw. przesmyku suwalskiego i na granicy z obwodem kaliningradzkim[10]. Zgodnie z jego założeniami polskie związki taktyczne będą stanowić jeden z najważniejszych elementów składowych komponentu lądowego sił zbrojnych Sojuszu, który zostanie zaangażowany do prowadzenia działań bojowych na tym obszarze. W wariancie tym przewiduje się podejmowanie działań ofensywnych polegających na wykonaniu uderzenia lądowego na obszar obwodu kaliningradzkiego w celu rozbicia rozlokowanych tam sił oraz zneutralizowania rozmieszczonych elementów systemu A2/AD zagrażających innym siłom Sojuszu prowadzącym działania na terenie państw bałtyckich. Polska artyleria – jako zasadniczy element systemu połączonego rażenia sił Sojuszu przeznaczony do zmniejszania potencjału elementów systemu A2/AD przeciwnika – powinna spełnić wiele wymagań i warunków, aby osiągnąć pełną interoperacyjność z sojuszniczymi systemami targetingu, rozpoznania, dowodzenia i kierowania ogniem na poziomie taktycz-

8 Ibidem, s. 31.

9 Ibidem, s. 32.

10 R.D. Hooker Jr., *How to defend...*, op.cit., s. 33.

nym i operacyjnym. W tym celu wojska rakietowe i artyleria (WRiA) SZRP muszą: dokonać nowego podziału sił i środków przeznaczonych do wykonywania zadań rażenia; zwiększyć zasięg ognia oraz szybkostrzelność artylerii; zmodernizować będące w wyposażeniu sił zbrojnych systemy artyleryjskie; skrócić czas reakcji ogniowej; wprowadzić do uzbrojenia gamę amunicji specjalnej i precyzyjnego rażenia; zwiększyć żywotność artylerii na polu walki oraz dostosować doktryny, regulaminy i instrukcje do nowych wymagań.

W ocenie autorów, jedynym procesem, który jest w stanie zapewnić właściwy poziom interoperacyjności WRiA z innymi armiami NATO na wszystkich poziomach dowodzenia oraz zintegrować posiadane przez naszą artylerię zdolności oddziaływania (rażenia) z sojuszniczymi systemami rozpoznania, jest *targeting*. Tylko dzięki sprawnie funkcjonującemu systemowi targetingu wspomagającemu na wszystkich poziomach dowodzenia i szczeblach organizacyjnych proces dowodzenia, wykorzystującemu nowoczesne systemy i technologie zdobywania, przetwarzania i dystrybucji informacji, SZRP mogą osiągnąć niespotykane dotąd możliwości prowadzenia operacji ukierunkowanych (*effect-based operations* – EBO). W 2016 roku została zatwierdzona przez ministra obrony narodowej, opracowana w Dowództwie Operacyjnym Rodzajów Sił Zbrojnych, *Koncepcja organizacji i funkcjonowania targetingu w Siłach Zbrojnych RP*, w której precyzyjnie opisano systemowe rozwiązania dotyczące organizacji, funkcjonowania oraz koordynacji procesu targetingu. Jej celem było uświadomienie dowódcom różnych poziomów dowodzenia i szczebli organizacyjnych znaczenia procesu targetingu podczas planowania oraz prowadzenia działań bojowych oraz utworzenia kompatybilnych z NATO jego struktur.

Nasze siły zbrojne w nadchodzącej perspektywie powinny dysponować adekwatnymi do potrzeb zdolnościami rażenia na wszystkich poziomach dowodzenia. W tym celu autorzy rekomendują następujący wariant podziału artylerii pod kątem wykonywanych zadań rażenia (rys.):

• *artyleria operacyjna*, w której skład wchodziłby związek taktyczny artylerii – brygada artylerii rakietowej (BAR) podporządkowana dowódcy komponentu lądowego, a w warunkach działań bojowych – dowódcy sił połączonych. W skład BAR wchodziłyby cztery dywizjony rakietowe wyposażone w wyrzutnie rakietowe HIMARS[11]. BAR, dysponując pociskami GMLRS i GMLRS ER, byłaby zdolna do rażenia obiektów na głębokości do 150 km, a z użyciem pocisków taktycznych ATACMS do 300 km, docelowo również do 700 km. W przyszłości BAR, wykorzystując pociski PRSM (*Prototypy Precision Strike Missile*), będzie zwalczać również ruchome cele lądowe i nawodne (morskie), dzięki czemu będzie mogła stanowić uzupełnienie systemu obrony wybrzeża;

• *artyleria taktyczna*, w której skład wchodziłyby cztery pułki artylerii związków taktycznych wyposażone w zestawy artyleryjskie Krab. Z haubicy Krab można strzelać wszystkimi pociskami artyleryjskimi NATO kalibru 155 mm, w tym kasetowymi typu M864 DPCIM, SMArt 155, FFV BONUS czy M898 SADARM, i niszczyć nimi czołgi, pojazdy opancerzone, a także działa samobieżne. Natomiast strzelając konwencjonalną amunicją odłamkowo-burzącą, można trafiać w cel z dokładnością do kilkunastu metrów na maksymalnej donośności strzelania wynoszącej nawet do 120 km[12]. Kolejne środki ogniowe na szczeblu taktycznym to artyleryjskie wyrzutnie rakietowe WR-40 Langusta. Zastosowanie różnych pakietów amunicyjnych, w tym kalibru 122, 160 i 305 mm, umożliwi rażenie celów na donośności od 40 do 150 km. Natomiast dywizjony artylerii oddziałów ogólnowojskowych wyposażone w haubice Krab oraz w zmodernizowane do kalibru 155 mm armatohaubice Dana (po unifikacji do kalibru 155 mm z docelową zdolnością oddziaływania na cele do 40 km), a także batalionowe kompanie wsparcia wyposażone w nowoczesne systemy moździerzowe MK i MG Rak będą realizowały zadania bliskiego i głębokiego wsparcia ogniowego.

Uzyskanie właściwego poziomu skuteczności rażenia ogniowego jest uwarunkowane posiadaniem gwintowanych środków ogniowych o dużej szybkostrzelności, która – według najnowszych poglądów – powinna wynosić minimum sześć wystrzałów na minutę. Będące obecnie w wyposażeniu oddziałów artylerii działa mają szybkostrzelność na poziomie około trzech–czterech wystrzałów na minutę. W konsekwencji w ramach dalszego rozwoju programu „Regina" haubicę Krab należy wyposażyć w automatyczny system ładowania pocisków i ładunków prochowych do lufy. Na zwiększenie jej możliwości ogniowych może wpłynąć wprowadzenie systemu uzupełniania zapasów do magazynu amunicyjnego działa bezpośrednio z opancerzonego wozu amunicyjnego dysponującego taką samą trakcją gąsienicową jak działo. Pozwoli to na dodawanie zapasów amunicji nawet w trakcie wykonywania zadania ogniowego bez konieczności zbęd-

11 Liczba dywizjonów powinna wynikać z liczby związków taktycznych, na korzyść których będą one realizowały zadania rażenia. W warunkach funkcjonowania w komponencie lądowym SZRP czterech dywizji, adekwatnie do ich liczby brygada rakietowa powinna posiadać cztery dwubateryjne (po cztery wyrzutnie HIMARS w baterii) dywizjony rakietowe.

12 Zamiast standardowych zapalników do amunicji konwencjonalnej stosuje się specjalne zapalniki typu PGK *(Precision Guidance Kit*). Konstrukcja tych zapalników sprawia, że maksymalne uchylenie pocisku od celu na donośności 30 km nie przekracza 50 m. Por.: D. Storsved, *PGK and the Impact of Affordable Precision on the Fires Mission*, 43rd Annual Guns & Missiles Symposium, 21–24 April 2008.

nego manewrowania haubicą do rejonów rozmieszczenia punktów amunicyjnych.

Modernizacja armatohaubicy wz. 1977 Dana kalibru 152 mm mogłaby polegać w dużej mierze na: zwiększeniu opancerzenia działa, zmianie kalibru na 155 mm oraz doposażeniu w inercyjne systemy nawigacji lądowej, cyfrowe kalkulatory balistyczne, terminale dowódcy działa i urządzenia do transmisji danych. Wymienione systemy pozwoliłyby na pełną integrację pododdziałów Dana z niemal dowolnym natowskim systemem dowodzenia C4I oraz kierowania ogniem.

W celu zwiększenia żywotności artylerii na polu walki powinno się w pierwszej kolejności wyprowadzić rejony manewrowania nią (*Artillery Maneuver Area* – AMA) spod ognia kontrbateryjnego przeciwnika. Oznacza to oddalenie AMA od linii styczności wojsk, które stało się możliwe dzięki znacznemu wzrostowi donośności strzelania oraz niespotykanej dotąd precyzji ognia. Kolejnym ważnym czynnikiem jest dopancerzenie dział i wyrzutni do poziomu minimum drugiego STANAG-u 4569. Dobrym przykładem jest niemiecka Panzerhaubitze-2000, której opancerzenie zapewnia ochronę na poziomie czwartym. Wobec niemożliwej do zniwelowania przewagi liczebnej artylerii hipotetycznego przeciwnika kluczowym czynnikiem będzie ograniczony czas przebywania dział i wyrzutni na stanowiskach ogniowych od momentu rozpoczęcia ostrzału celu do wykonania manewru przeciwogniowego. Czas ten nie powinien przekraczać 3 do 4 minut.

Zmiany zapisów w instrukcji strzelania i kierowania ogniem artylerii powinny uwzględniać takie czynniki, jak: pełna autonomiczność dział i wyrzutni oraz właściwości amunicji artyleryjskiej, zwłaszcza specjalnej i precyzyjnego rażenia; możliwości pozyskiwania danych z rozpoznania na potrzeby ognia artylerii z innych źródeł niż naziemne rozpoznanie wzrokowe, w tym z rozpoznania lotniczego i satelitarnego; konieczność prowadzenia obserwacji i śledzenia celów podczas ich ostrzału; wymóg prognozowania niezamierzonych strat oraz oceny skutków rażenia; ograniczony łączny czas przebywania dział i wyrzutni na stanowiskach ogniowych; jak również cyfrowe określanie nastaw do strzelania.

Dotychczas obowiązujący *Regulamin działań taktycznych artylerii (brygada, pułk)* z 2002 roku w znaczący sposób odbiega od przyjętych obecnie form i metod prowadzenia działań. Zapisy doktrynalne dotyczące bojowego użycia artylerii muszą podlegać ciągłej ocenie oraz okresowej ewaluacji stosownie do przewidywanego zagrożenia ze strony przeciwnika oraz możliwości jego środków ogniowych. Dalszy rozwój doktryn, regulaminów i instrukcji dotyczących bojowego użycia WRiA wymaga podjęcia wielu kompleksowych działań mających na celu wnikliwą ocenę aktualnego stanu wiedzy na ten temat oraz aktualizację dotychczasowych poglądów na sposób użycia artylerii w walce zarówno w teorii, jak i w praktyce.

WNIOSKI

Konsekwentna i szybka modernizacja artylerii i innych systemów walki wchodzących w skład systemu połączonego rażenia Sił Zbrojnych RP powinna skutecznie odstraszać potencjalnego agresora, i w razie konieczności zapewnić optymalne zdolności do obniżenia potencjału A2/AD.

Wprowadzenie do uzbrojenia nowoczesnych systemów artyleryjskich Krab, a w najbliższej przyszłości również systemów rakietowych typu HIMARS, przy równocześnie prowadzonej modernizacji technicznej starszych typów uzbrojenia, m.in. armatohaubicy Dana czy WR-40 Langusta, w znacznym stopniu wzmocni potencjał oraz zdolności komponentu lądowego SZRP do realizacji zadań głębokiego wsparcia ogniowego i prowadzenia ognia operacyjnego, szczególnie w ramach zwalczania elementów systemu A2/AD potencjalnego przeciwnika. Pojawiające się nowe, niespotykane dotąd, możliwości artylerii wykonywania samodzielnych precyzyjnych głębokich uderzeń ogniowych – w ramach połączonego rażenia i ognia operacyjnego z wykorzystaniem wchodzącej do uzbrojenia artylerii całej gamy amunicji dalekonośnej precyzyjnego rażenia – pozwolą na niszczenie oraz obezwładnianie wielu obiektów znajdujących się w obszarach zainteresowania dowódcy komponentu lądowego oraz naczelnego dowódcy sił zbrojnych (dowódcy sił połączonych), które dotychczas były poza jej skutecznym zasięgiem.

Sukcesywne wprowadzanie do uzbrojenia kolejnych dywizjonów rakietowych HIMARS w perspektywie najbliższych lat prawdopodobnie umożliwi utworzenie na szczeblu wojsk lądowych samodzielnego oddziału (brygady artylerii rakietowej) dysponującego potencjałem i zdolnościami bojowymi pozwalającymi na oddziaływanie na obiekty znajdujące się poza strefami odpowiedzialności związków taktycznych pierwszego rzutu. W związku z tym zasadne wydaje się, by w procesie opracowywania struktury organizacyjnej nowej jednostki artylerii rakietowej oraz planowania jej podległości służbowej i taktycznej rozważyć podporządkowanie jej bezpośrednio dowódcy wojsk lądowych, a w czasie prowadzenia działań bezpośrednio naczelnemu dowódcy sił zbrojnych (dowódcy sił połączonych).

Niniejszy artykuł stanowi zaledwie wstęp do kompleksowego podejścia oraz podjęcia prac mających na celu aktualizację dotychczasowych poglądów na sposób użycia artylerii w walce zarówno w teorii, jak i w praktyce. W opinii autorów opracowanie koncepcji użycia artylerii w warunkach współczesnych zagrożeń powinno stać się jednym z najważniejszych i najpilniejszych zadań środowiska artylerzystów w trzeciej dekadzie XXI wieku. ■

NASZE SIŁY ZBROJNE W NADCHODZĄCEJ PERSPEKTYWIE POWINNY DYSPONOWAĆ ADEKWATNYMI DO POTRZEB ZDOLNOŚCIAMI RAŻENIA NA WSZYSTKICH POZIOMACH DOWODZENIA.

Zagrożenie bronią masowego rażenia w przyszłych **konfliktach zbrojnych**

OBOWIĄZUJĄCY OD 1970 ROKU *UKŁAD O NIEROZPRZESTRZENIANIU BRONI JĄDROWEJ* STAŁ SIĘ GWARANCJĄ BEZPIECZEŃSTWA ŚWIATOWEGO DĄŻĄCĄ DO ZAPOBIEGANIA MOŻLIWOŚCI WYBUCHU WOJNY JĄDROWEJ.

Autorka jest wykładowcą w Zespole OPBMR Zakładu Wsparcia Bojowego Instytutu Dowodzenia Akademii Wojsk Lądowych.

kpt. mgr inż. Agnieszka Maciejewska-Miedziak

Trwające obecnie konflikty zbrojne stale są obserwowane i poddawane analizie, a wyciągnięte wnioski stają się skarbnicą wiedzy zarówno dla środowisk militarnych, jak i cywilnych. Zastanawiające jest jednak, w jaki sposób i w jakim stopniu będą one wpływały na kształt przyszłych konfliktów zbrojnych, czy będą je determinować całkowicie, czy tylko wyznaczać kierunki zmian w ich prowadzeniu. Rozwój techniki i nowe technologie dały początek wielkim modernizacjom światowych armii, często kosztem redukcji ich potencjału. Przyszłe wojny, niezależnie od czasoprzestrzeni, nadal będą wykorzystywać broń konwencjonalną w swoich działaniach. Jednocześnie możemy się spodziewać także zastosowania broni masowego rażenia (BMR) do osiągnięcia konkretnych celów, biorąc pod rozwagę skutki, jakie będzie ona wywoływała. Bardziej też należy oczekiwać wystąpienia konfliktów lokalnych czy regionalnych, sprowadzających się do eskalacji agresji między państwami, których celem nie będzie pozbawienie wrogiego państwa podmiotowości prawnej na arenie międzynarodowej.

BROŃ CHEMICZNA

Broń masowego rażenia była i będzie obiektem pożądania wielu państw, organizacji dążących do osiągnięcia swoich celów politycznych i ekonomicznych, jak również organizacji terrorystycznych, które stały się jednym z największych zagrożeń współczesnego świata. Pod pojęciem *zdarzeń CBRN* (*Chemical Biological Radiological Nuclear Weapon*) rozumiemy broń chemiczną, biologiczną, radiologiczną, jądrową oraz niektóre toksyczne środki przemysłowe[1], a także inne zdarzenia, w których doszło do uwolnienia substancji toksycznych, promieniotwórczych czy biologicznych.

Broń chemiczna, czyli bojowe środki trujące (BST), to substancje chemiczne mogące występować w postaci gazu, par, aerozoli, substancji ciekłych i stałych, które przedostają się do organizmu drogą oddechową, pokarmową, przez błony śluzowe, oczy, skórę i w konsekwencji oddziałują na systemy fizjologiczne organizmu, powodując duże straty w ludziach i przyczyniając się do długotrwałego skażenia terenu, sprzętów i obiektów.

Jeśli będziemy chcieli sklasyfikować BST, możemy przyjąć różnorodne kryteria. Jednym z zasadniczych jest podział ze względu na skutki, jakie wywołują: czyli uśmiercające i obezwładniające. Możemy też przyjąć kryterium toksykologiczne, które przedstawia skutki oddziaływania na organizmy

1 *OPBMR w operacjach połączonych DD/3.8(A),* Bydgoszcz 2013, s. 17.

Broń chemiczna to substancje, które przedostają się do organizmu drogą oddechową, pokarmową, przez błony śluzowe, oczy, skórę i oddziałują na systemy fizjologiczne organizmu, powodując duże straty w ludziach i przyczyniając się do długotrwałego skażenia terenu.

ALEKSANDER RAWSKI

żywe. Obejmuje ono takie grupy środków, jak: paralityczno-drgawkowe (np. VX, sarin, tabun), ogólnotrujące (np. chlorocyjan, cyjanowodór), duszące (np. fosgen), parzące (np. iperyt siarkowy, luizyt), drażniące (z podziałem na lakrymatory – chloroacetofenon oraz sternity – adamsyt), psychochemiczne (np. psylocybiny, LSD-25) oraz fitotoksyczne (np. herbicydy).

Bojowe środki trujące *to jedne z najstarszych, niekonwencjonalnych narzędzi prowadzenia wojen*[2], które nadal cieszą się dużym zainteresowaniem, mimo istnienia międzynarodowych porozumień w sprawie zakazu ich stosowania. *Konwencja o zakazie broni chemicznej* (*Chemical Weapons Convention* – CWC) podpisana w Paryżu w 1993 roku, a obowiązująca od roku 1997 i zrzeszająca 190 państw, ma za zadanie zapewniać bezpieczeństwo i gwarantować nieużywanie tych środków. Na straży przestrzegania traktatu stoi powołana w tym celu Organizacja ds. Zakazu Broni Chemicznej.

Atrakcyjność bojowych środków trujących, idąca w parze z rozwojem technologii i ze znacznymi środkami finansowymi będącymi w posiadaniu terrorystów czy państw wspierających terroryzm, może skutkować powstawaniem nowych laboratoriów, w których środki chemiczne będą syntezowane i realnie wykorzystywane.

W ostatnich dziesięcioleciach niejednokrotnie mogliśmy zaobserwować użycie bojowych środków trujących. Przeprowadzony przez sektę Najwyższa Prawda zamach terrorystyczny w tokijskim metrze w 1995 roku z użyciem sarinu czy ataki gazowe rebeliantów w Syrii w 2013 i 2017 roku również z wykorzystaniem tego środka – to tylko niektóre przykłady, o których dowiedziała się światowa opinia.

Trwająca od starożytności fascynacja środkami chemicznymi, w tym bojowymi środkami trującymi, głównie najniebezpieczniejszymi, jakimi są środki paralityczno-drgawkowe, jest bardzo silna i przez to niebezpieczna. Użycie toksycznych substancji chemicznych jest jak najbardziej realne, mimo że wymaga to specjalistycznego przygotowania oraz odpowiednich warunków atmosferycznych. Skutki, jakie one wywołują, to nie tylko masowe porażenia, lecz także strach, dezorganizacja i chaos, dlatego z powodzeniem mogą być stosowane jako narzędzie szantażu czy przekupstwa.

Istotne zagrożenie stanowią także zakłady przemysłowe wykorzystujące środki chemiczne, które mogą stać się kartą przetargową i bezpośrednim

2 M. Żuber, *Broń masowego rażenia w działalności terrorystycznej,* Warszawa 2015, s. 78.

Broń masowej zagłady, niszczycielska i przerażająca, stwarza ciągłe zagrożenie dla pokoju i bezpieczeństwa na świecie.

celem ataków czy sabotażu, w wyniku których może dojść do katastrofy.

BROŃ JĄDROWA

Broń jądrowa charakteryzuje się najbardziej destrukcyjnym działaniem ze wszystkich rodzajów broni masowego rażenia. Jest to kompletny zestaw urządzeń (np. typu implozyjnego, artyleryjskiego czy termojądrowego), który w swej ostatecznej konfiguracji, po zakończeniu procedury uzbrajania i odpalania, jest zdolny do zainicjowania niekontrolowanej reakcji jądrowej z uwolnieniem energii. Charakteryzując broń jądrową, możemy brać pod uwagę różne kryteria. Jednym z nich jest rodzaj ładunków, możemy tu wyróżnić cztery generacje (ładunki rozszczepialne, termojądrowe, neutronowe), czy też sposób uzyskania energii jądrowej (ładunki jednofazowe, dwufazowe czy trójfazowe). Możemy też dokonać podziału według mocy ładunku oraz sposobu przeprowadzenia wybuchów jądrowych. Najistotniejszą kwestią w wypadku użycia broni jądrowej będą bezpośrednie i pośrednie skutki przez nią wywołane, które zostały zdefiniowane w postaci czynników rażenia. Należy do nich zaliczyć: błysk, promieniowanie cieplne, falę uderzeniową, promieniowanie przenikliwe, promieniotwórcze skażenie terenu, impuls elektromagnetyczny i zwiększoną aktywność jonosfery[3].

Impuls elektromagnetyczny, z uwagi na swoje rażące działanie, stał się na tyle istotny, że w ostatnich latach coraz częściej mówi się o rozwoju nowego typu broni, jakim jest broń elektromagnetyczna. Jest to bezpośrednio związane z rozwojem techniki, a przede wszystkim elektroniki.

Scenariuszy związanych z użyciem broni jądrowej jest wiele, podobnie jak sposobów pozyskania jej przez ugrupowania terrorystyczne. Może się to odbywać na zasadzie współpracy z państwem posiadającym broń jądrową, co jest raczej mało prawdopodobne, kradzieży lub nielegalnego zakupu czy samodzielnej konstrukcji ładunku jądrowego[4]. Do posiadania broni jądrowej dążą nie tylko terroryści. Obserwujemy to również w wypadku niektórych państw, które prowadzą prace nad dostępem do technologii jądrowych (jak podają dane izraelskiego wy-

3 *OPBMR w operacjach połączonych*..., op.cit., s. 25.

4 M. Żuber, *Broń masowego rażenia w działalności*..., op.cit., s. 85.

NARA

wiadu)[5]. Jako przykład można tutaj wskazać broń nowego typu, jaką są zminiaturyzowane ładunki jądrowe, czy, idąc dalej, miniaturowe głowice, określane jako tak zwane bomby plecakowe lub walizkowe[6].

Niszczycielskie skutki użycia broni jądrowej będą widoczne nie tylko w postaci zniszczonych budynków i sprzętu, lecz wiążą się również z niewidocznym zagrożeniem w postaci promieniowania przenikliwego, które sieje spustoszenie w organizmie, doprowadzając do zatrzymania jego funkcjonowania. Broń jądrowa wraz ze swoimi czynnikami rażenia może zostawić ślad użycia na bardzo wiele lat, w wyniku czego będą cierpieć przyszłe pokolenia.

BROŃ RADIOLOGICZNA

Na szczególną uwagę zasługuje także broń radiologiczna, której czynnikiem rażącym jest rozproszony materiał promieniotwórczy pochodzący z ośrodków realizujących cywilne lub wojskowe programy jądrowe, a także odpady promieniotwórcze z reaktorów badawczych czy środki promieniotwórcze stosowane w przemyśle lub medycynie[7]. Rozwiązaniem konstrukcyjnym służącym do użycia broni radiologicznej są radiacyjne urządzenia rozpraszające (*Radiological Exposure Devices* – RED). Pojawia nam się tutaj pojęcie *brudnej bomby* wykorzystującej odpady promieniotwórcze – radioizotopy w połączeniu z materiałem detonującym (trotylem czy dynamitem). Z uwagi na niewielkie zagrożenie związane z jej działaniem rażącym, w porównaniu z innymi rodzajami broni masowego rażenia, nie jest to broń atrakcyjna militarnie, która miałaby być wykorzystywana w działaniach bojowych. Natomiast może stanowić ona doskonałe narzędzie w rękach terrorystów, wywołując strach i przyczyniając się do destabilizacji w kraju, w którym dokonano takiego ataku.

BROŃ BIOLOGICZNA

Niewątpliwym źródłem zagrożeń z uwagi na konsekwencje jej stosowania jest broń biologiczna. Tak zwana broń ubogich ze względu na niskie koszty produkcji może się stać jednym z najgroźniejszych współcze-

5 R. Frister, *Wyścig rakiet,* „Polityka" 2008 nr 6, s. 54–55.

6 M. Żuber, *Broń masowego rażenia w działalności*..., op.cit., s. 84.

7 *OPBMR w operacjach połączonych*..., op.cit., s. 23.

snych zagrożeń. Ten rodzaj broni niekonwencjonalnej, podobnie jak broń chemiczna, był i jest obiektem zainteresowania wielu państw.

Jako broń biologiczną określamy środki biologiczne, a więc mikroorganizmy, które wywołują choroby u ludzi, roślin i zwierząt wraz ze środkami ich przenoszenia (urządzeniami lub zwierzętami).

Środki biologiczne obejmują:

– bakterie (z kategorii A według CDC: wąglik, dżuma, tularemia; z kategorii B: chlamydia);

– wirusy (z kategorii A według CDC: ospa czarna, wirus gorączki krwotocznej, np. Ebola, Lassa);

– toksyny (z kategorii A według CDC: toksyna botuliny, z kategorii B: rycyna)[8];

– pasożyty;

– grzyby.

Broń biologiczna, oprócz niewielkich kosztów wytwarzania, charakteryzuje się również dużą skutecznością, słabą wykrywalnością w początkowym etapie i zazwyczaj krótkim okresem inkubacji[9]. Ten szczególny rodzaj broni masowego rażenia znajdował się w arsenałach wojskowych wielkich mocarstw. Obecnie środki biologiczne mogą być przenoszone przez bomby lotnicze, pociski artyleryjskie, rozpylane w postaci aerozolu w powietrzu czy też wysyłane pocztą w kopertach, tak jak w wypadku ataków terrorystycznych w Stanach Zjednoczonych w 2001 roku. Broń biologiczna, która sięgała swoich początków w starożytności, posiadała w arsenale zatrute toksynami strzały, jadowite węże, pszczoły, ciała zmarłych na dżumę czy krew trędowatych.

Pod koniec XX wieku pojawiło się zjawisko określane mianem *bioterroryzmu*. Jest ono utożsamiane z nielegalnym użyciem patogenów wobec ludzi z zamiarem wymuszenia określonego działania lub zastraszenia rządu czy społeczeństwa dla osiągnięcia celów politycznych, społecznych lub religijnych.

W ostatnich dziesięcioleciach nastąpił znaczny wzrost zainteresowania bronią biologiczną, między innymi wśród fanatycznych sekt religijnych (np. Najwyższa Prawda z Japonii) czy ugrupowań politycznych (np. prawicowe ugrupowanie tzw. białych patriotów w USA). Równocześnie mogliśmy zaobserwować przypadki działań z użyciem tego rodzaju broni, jak chociażby wspomniana już seria ataków terrorystycznych z wykorzystaniem śmiercionośnej bakterii *Bacillus anthracis,* która wywołała skutek globalny w postaci pandemii strachu i znacznej utraty poczucia bezpieczeństwa w większości cywilizowanych krajów. Dlaczego jednak to broń biologiczna może się stać jednym z najniebezpieczniejszych zagrożeń dla współczesnego świata?

W dobie panującego rozwoju naukowego i postępu technologicznego możliwość rozpoznania jednostki chorobotwórczej może być bardzo trudna i wymagająca czasu, a czas w wypadku rozwoju choroby i szerzenia się epidemii jest *na wagę złota*. Z uwagi na występowanie w przypadku środków biologicznych okresu inkubacji, a więc opóźnionego działania czynnika rażenia, daje to użytkownikom tej broni czas na zatarcie śladów i ucieczkę z miejsca zdarzenia. Przewidzenie zasięgu rażenia nie jest możliwe do zrealizowania. Niektóre symptomy chorobotwórcze są wspólne dla wielu chorób, dopiero w razie wystąpienia masowych zachorowań możliwe będzie stwierdzenie, czy faktycznie był to atak biologiczny. Identyfikację może również utrudniać patogen wywołujący rzadką chorobę, z którym personel medyczny mógł się nigdy nie spotkać albo też czynnik chorobotwórczy, który jest niespotykany na danym obszarze. Dochodzi również kwestia modyfikacji genetycznych czy wprowadzenia do środowiska organizmów żywych całkiem nowego patogenu, niezidentyfikowanego co do skutków, jakie wywoła i tym samym jeszcze bardziej niebezpiecznego.

Skutki użycia broni biologicznej mogą obejmować różny zasięg – od jednostkowych przypadków po szerzącą się w krajach epidemię czy pandemię na świecie. Reagowanie na takie zagrożenie wiąże się z działaniami podejmowanymi w wielu kierunkach i na wielu płaszczyznach. Jest ono związane z badaniami chorych, środowiska, izolacją czy ewakuacją chorych, ich kwarantanną, izolacją obszarów objętych zakażeniem, profilaktyką, metodami leczenia, istnieniem szczepionki i dostępnością do niej, jak również do leków, surowic i innych niezbędnych środków sanitarnych.

Broń biologiczna, wywołująca długofalowe skutki epidemiologiczne, zarówno bezpośrednie (masowe toksemie), jak i pośrednie (zakażenie/skażenie zwierząt, pokarmów, wody pitnej) albo w postaci wprowadzenia do środowiska puli genów (które mogą być genami kodującymi toksyny, lekooporność czy produkty inżynierii genetycznej), przyczyni się do rozprzestrzeniania czynnika strachu, dezorientacji i destabilizacji kraju. Może to również prowadzić do wystąpienia głębokich skutków ekonomicznych, społecznych i gospodarczych.

Szczególną formą terroryzmu biologicznego jest agroterroryzm. Uderza on przede wszystkim w gospodarkę – rolnictwo i przetwórstwo żywności, a więc w hodowlę i uprawy. Efekty przeprowadzonego ataku na sektor rolniczy są bardzo groźne dla obywateli, a także innych państw, z którymi zaatakowany kraj jest powiązany gospodarczo. W dzisiejszych czasach wybuch epizootii czy epifitozy będzie tragiczny w skutkach nie tylko dla właścicieli gospodarstw, lecz przede wszystkim dla ludności. Będzie on oddziaływał na gospodarkę i ekonomię całych regionów czy krajów.

8 https://emergency.cdc.gov/bioterrorism/, /. 31.07.2020.

9 A. Maciejewska-Miedziak, J. Miedziak, M. Stankiewicz, Z. Zielonka, *Poradnik do szkolenia z Obrony przed Bronią Masowego Rażenia*, sygn. WSOWL wewn. 156/2014, Wrocław 2014, s. 21.

USAF

Głównym czynnikiem rażenia broni zapalającej jest temperatura spalania rzędu 800–3000°C uzyskiwana zależnie od rodzaju środka zapalającego.

Prace nad programem pozyskania i wykorzystania broni biologicznej, w tym również plany związane z sektorem rolniczym, były prowadzone przez niektóre państwa już w czasie II wojny światowej[10]. Znane są również przypadki użycia patogenów chorobotwórczych skierowanych w uprawy lub hodowlę. Jak podają dane z Instytutu Studiów Międzynarodowych w Monterey, od 1915 do 2000 roku wystąpiło 19 aktów agroterrorystycznych na świecie, w tym pięć w USA[11]. Rolnictwo jest słabo chronioną gałęzią gospodarki i o tym, jak istotna jest wiedza i świadomość o zagrożeniach, przekonywali eksperci Federalnego Biura Śledczego (FBI) oraz Inspekcji Weterynaryjnej Stanów Zjednoczonych (APHIS) podczas konferencji oraz warsztatów szkoleniowych, które odbyły się w naszym kraju w 2018 roku.

BROŃ ZAPALAJĄCA

Jednym z zagrożeń, o którym warto wspomnieć, a które trochę zostało zapomniane, jest broń zapalająca. Analizując kierunki rozwoju techniki wojskowej naszego potężnego wschodniego sąsiada, można z całym przekonaniem stwierdzić, że właśnie ten rodzaj broni przeżywa swój renesans, czego przykładem jest nowe wcielenie wyrzutni pocisków termobarycznych TOS-2 (Tosoczka)[12]. Głównym czynnikiem rażenia broni zapalającej jest temperatura spalania rzędu 800–3000°C uzyskiwana zależnie od rodzaju środka zapalającego. Najczęściej stosowany podział tych środków jest związany ze stanem skupienia – ciekłym (napalm) i stałym (termit, fosfor biały).

Modernizacja, a wraz z nią nowe możliwości broni zapalającej, spowodowały modyfikacje w zakresie sposobów jej użycia zarówno na poziomie taktycznym, jak i strategicznym, co nie pozostało niezauważone przez opinię publiczną.

REFLEKSJE

Broń masowej zagłady, niszczycielska i przerażająca, stwarza ciągłe zagrożenie dla pokoju i bezpieczeństwa na świecie. Prawdopodobieństwo jej użycia nie jest duże, ale zdecydowanie realne. Niektóre cechy czynią ją atrakcyjną, dlatego jest obiektem pożądania wielu organizacji na świecie. Wykorzystanie broni masowego rażenia wywołuje skutki nie tylko w postaci strat w ludziach i skażenia terenu, lecz jest również źródłem paniki, wprowadza chaos i dezorganizację. Możemy przypuszczać z dużym prawdopodobieństwem, że wojna jądrowa nam nie grozi, jednak lokalne użycie bojowych środków trujących jest możliwe, a wykorzystanie środków biologicznych wydaje się najbardziej prawdopodobne.

Występujące na świecie pandemie lub epidemie – świńskiej grypy, HIV czy SARS, przyczyniły się do wprowadzenia nowego sposobu funkcjonowania państw. Rządy wielu krajów podejmowały radykalne decyzje związane z izolacją i znacznymi ograniczeniami w zakresie ekonomii i gospodarki. Prawa i wolności obywateli zostały mocno ograniczone. Wprowadzenie takich obostrzeń oraz dane docierające z różnych stron świata o liczbie zakażonych i zgonów powodowały strach wśród ludności, dezorganizację życia codziennego, a w dalszej konsekwencji spowolnienie gospodarki i kryzys, którego skutki są i będą jeszcze odczuwane. Z takimi sytuacjami mamy wciąż do czynienia, w wypadku niektórych mikroorganizmów sytuacja jest w dalszym ciągu nieopanowana, a przyszłość nadal niepewna.

To jeden ze scenariuszy, jakie przewidują dla ludzkości zagrożenia CBRN, a w tym wypadku szczególnie środki biologiczne użyte z zamiarem osiągnięcia konkretnych celów.

Na straży stabilizacji bezpieczeństwa globalnego stoją między innymi instytucje bezpieczeństwa międzynarodowego, takie jak Organizacja Narodów Zjednoczonych, wspierane przez międzynarodowe sojusze, traktaty i konwencje. Prawie z każdym rodzajem broni masowego rażenia związane są międzynarodowe akty prawne, które mają zagwarantować, że nie będzie ona używana przez strony danego porozumienia. Niezależne organizacje stale monitorują oraz analizują przestrzeganie zapisów umów międzynarodowych, kontrolują, by nie doszło do proliferacji oraz przedstawiają wnioski w zakresie rozbrojenia i nadzorują stan posiadanego uzbrojenia.

Możliwości wykorzystania broni masowego rażenia są różnorodne. Nieprzewidywalne skutki takich działań będą obejmowały wiele płaszczyzn i kierunków. Możemy tworzyć scenariusze zastosowania CBRN, próbując mniej lub bardziej przewidywać jej użycie, jednak dopiero faktyczne użycie broni masowego rażenia stworzy nową architekturę świata. ■

10 Ibidem, s. 116.

11 CNS-2001. *Agro-terrorism. Chronology of CBW Attacks Targeting Crops &Livestock 1915-2000,* Chemical & Biological Weapons Resource Page. Monterey Institute of International Studies, 2002, http://cns.miis.edu/.

12 https://www.defence24.pl/tos-2-tosoczka-nowe-wcielenie-rosyjskiej-broni-termobarycznej-analiza/. 2.08.2020.

Broń elektromagnetyczna **w obronie przeciwlotniczej**

WYŚCIG ZBROJEŃ STAŁ SIĘ SWOISTYM KOŁEM ZAMACHOWYM POSTĘPU TECHNOLOGICZNEGO.

mjr mgr inż. Jarosław Patałuch, płk rez. dr inż. Marek Andruszkiewicz

Jarosław Patałuch jest kierownikiem Zespołu Wojsk Obrony Przeciwlotniczej w Instytucie Dowodzenia Akademii Wojsk Lądowych.

Marek Andruszkiewicz jest starszym wykładowcą w Zespole Wojsk Obrony Przeciwlotniczej w Instytucie Dowodzenia Akademii Wojsk Lądowych.

Początek i rozwój obrony przeciwlotniczej jest związany z wykorzystaniem lotnictwa i aparatów latających, np. sterowców i rakiet, w konfliktach zbrojnych. Pojawiła się wówczas realna konieczność znalezienia środków do ich zwalczania[1]. Ewolucja środków napadu powietrznego obejmowała nie tylko ich konstrukcję, lecz przede wszystkim uzbrojenie, czyli środki rażenia. Platformy załogowe wyposażone w kierowane pociski rakietowe i stacje radiolokacyjne dalekiego zasięgu charakteryzują się zmniejszoną skuteczną powierzchnią odbicia (SPO) i są powszechnie używane w wielu armiach na świecie.

Kolejne koncepcje wykorzystania platform bezzałogowych wspólnie z samolotami załogowymi mają stanowić antidotum na pokonywanie najnowocześniejszych systemów obrony powietrznej.

EWOLUCJA ZAGROŻEŃ

Oprócz samolotów załogowych najnowszej generacji również bezzałogowe statki powietrzne (BSP) przeobraziły się w środki napadu powietrznego (ŚNP), zdolne do wykonywania samodzielnych misji o zasięgu operacyjno-strategicznym. Kolejnym krokiem zastosowania BSP jest ich użycie w tak zwanych rojach. Intencją takiej *powietrznej armady* jest przeciążenie, obezwładnienie oraz oślepienie systemów obrony powietrznej. Koncepcja ta zakłada, że wykorzystując dużą liczbę platform bezzałogowych przeładowuje się kanały celowania środków obrony przeciwlotniczej, które, z uwagi na cykl strzelania oraz prawdopodobieństwo trafienia, nie są w stanie zwalczać wszystkich zagrożeń.

Odrębnym obiektem zainteresowania obrony przeciwlotniczej są efektory przenoszone przez samoloty. Całe spektrum środków rażenia wymaga zastosowania różnorodnych systemów antydostępowych, które mogą skutecznie je neutralizować. Przykładem jest konflikt w Syrii. W początkowej jego fazie obrona przeciwlotnicza nie radziła sobie z rakietami manewrującymi wystrzeliwanymi przez Izrael. Antidotum na to zagrożenie okazały się rosyjskie zestawy artyleryjsko-rakietowe Pancyr-S, wyposażone w armaty kalibru 30 mm, rakiety oraz radiolokatory pozwalające naprowadzać je jednocześnie na cztery cele. Nawet jeśli brakuje rakiet, armaty są skutecznym środkiem niszczenia rakiet przeciwnika.

Odpowiedzią na zastosowanie tych systemów przeciwlotniczych było użycie bomb szybujących, które charakteryzowały się zmniejszoną SPO oraz możliwością wykorzystania systemów nawigacyjnych INS/GPS. Uderzenia lotnictwa izraelskiego były przeprowadzane z samolotów, które nie wchodziły w przestrzeń powietrzną Syrii[2]. Działały one nad Izraelem, wzgórzami Golan oraz znad sąsiedniego Libanu, wobec czego nie naruszały syryjskiej przestrzeni powietrznej i nie mogły być atakowane. W ten sposób ich działanie można określić jako *spoza zasięgu prawa*.

Zaprezentowane zagrożenia wskazują, że obrona powietrzna oparta tylko na konwencjonalnych środ-

1 M. Andruszkiewicz, *Organizacja, uzbrojenie i wyposażenie wojsk obrony przeciwlotniczej w Polsce w latach 1919–1945*, „Zeszyty Naukowe WSOWL" 2007 nr 3.

2 https://trybuna.info/swiat/wyscig-technologii-na-syryjskim-niebie/.

System Phalanx CIWS

1.

US NAVY

kach rażenia nie jest wystarczająca. Wydawałoby się że złotym środkiem na systemy bezzałogowe może się okazać system zagłuszający komunikację tych platform z centrum dowodzenia lub operatorem. Tego typu systemy są stosowane już w wielu armiach, także w naszej, gdzie wykorzystuje się system Lanca 2.0 opracowany przez Polską Grupę Zbrojeniową. Tego typu systemy składają się z czujnika wykrywającego łączność radiową, radiolokatora skanującego chroniony obiekt oraz systemu zakłóceń. Wydawałoby się, że jest to odpowiednie remedium, ale w myśl zasady akcja–reakcja powstały bezzałogowe statki powietrzne, które w chwili zagłuszenia realizują zaprogramowane wcześniej zadanie, czyli np. atak na cele zapasowe lub wcześniej rozpoznane i zapamiętane obiekty. Dlatego też samo zagłuszanie nie jest w stanie zapewnić oczekiwanego bezpieczeństwa ochranianych obiektów.

Następnym czynnikiem, który zmusza do poszukiwania nowych środków do zwalczania zagrożenia powietrznego, jest miniaturyzacja środków rażenia przenoszonych przez platformy powietrzne czy też wyrzutnie naziemne. Pierwsze z nich, którego reprezentantem jest wspomniana bomba szybująca, charakteryzują się małą SPO, co sprawia że ich wykrycie jest bardzo trudne, a po zidentyfikowaniu pozostaje mało czasu na reakcję. Istotną ich cechą jest także zasięg, który pozwala na odpalanie spoza zasięgu obrony powietrznej. Amerykańska bomba szybująca GBU-39 SDB potrafi dolecieć do celu oddalonego o 110 km.

Mogłoby się zdawać, że obrona powietrzna w swoim zainteresowaniu ma tylko efektory powietrze–ziemia. Obecnie obrona przeciwlotnicza musi uwzględniać także zagrożenia typu: rakiety–artyleria–moździerze (*Rocket, Artillery and Mortars* – RAM)). Są to o tyle trudne wyzwania, że determinują systemy OPL do natychmiastowego oddziaływania z uwagi na krótki czas wykrycia i reakcji oraz małą skuteczną powierzchnię odbicia tych środków rażenia.

Jednym z reprezentantów wyspecjalizowanym w walce z tego typu zagrożeniami jest izraelski system Iron Dome. Został on zaprojektowany do obrony przed wystrzeliwanymi z odległości od 5 do 70 km artyleryjskimi pociskami rakietowymi i pociskami moździerzowymi. W oficjalnych źródłach izraelskich możemy przeczytać, że skuteczność tego posługującego się niewielkimi rakietami systemu wynosi 90%. Jednak porównując cenę jednej baterii, która jest szacowana na około 180 mln dolarów – w stosunku do zagrożeń, z jakim się mierzy, jest to bardzo kosztowny system.

Do walki z obiektami typu RAM wykorzystuje się także inne środki walki, na przykład amerykański system Phalanx CIWS[3] (fot. 1). Jest to okrętowy system obrony, którego zasięg wynosi około 1,5 km. Jest to więc system bardzo krótkiego zasięgu, który przy odpieraniu zmasowanego ataku może się okazać niewystarczający.

Rozpatrując całe spektrum zagrożeń, z jakim muszą sobie radzić systemy obrony przeciwlotniczej, naturalne staje się poszukiwanie nowych rozwiązań, które mogą sprostać aktualnym wyzwaniom, jak i tym, które przyniesie przyszłość. Oczywiście nie należy rezygnować z udoskonalania dotychczasowych

3 https://www.raytheonmissilesanddefense.com/capabilities/products/phalanx-close-in-weapon-system/.

środków, opartych na konwencjonalnych pociskach rakietowych oraz broni lufowej. Jednak należy wziąć pod uwagę, że uzbrojenie bazujące na chemicznych źródłach energetycznych (silniki rakietowe, proch) osiągnęło już swoją maksymalną efektywność. Dalszy jego rozwój nie będzie na tyle wydajny, by mógł znacząco wpłynąć na pozyskiwanie skuteczniejszych systemów obrony. Wydaje się, że nowymi środkami walki będą takie, które będą wykorzystywać energię elektromagnetyczną.

BROŃ ELEKTROMAGNETYCZNA

Pojęcie to odnosi się nie tylko do jednego środka walki, lecz określa całą ich kategorię. Zatem *broń elektromagnetyczną stanowią środki i urządzenia wykorzystujące w swym działaniu energię elektromagnetyczną, występującą najczęściej w postaci fal elektromagnetycznych, rozchodzących się swobodnie w przestrzeni, zarówno w gruncie, wodzie, jak i atmosferze*[4]. Można się pokusić o jej klasyfikację i wyróżnić: broń impulsową (EMP), broń mikrofalową, działo elektromagnetyczne (railgun) oraz broń laserową.

Nad *bronią impulsową* pracowano już podczas II wojny światowej. Już wtedy stosowano nadajniki, które skutecznie zakłócały pracę stacji radiolokacyjnych. Kolejnym krokiem było wykorzystanie czynników rażenia wybuchu bomby jądrowej, kiedy zauważono powstawanie tzw. burzy elektromagnetycznej, uniemożliwiającej prowadzenie łączności radiowej i funkcjonowanie urządzeń elektronicznych. Współcześnie powstał pomysł skonstruowania *bomby E*, która, wysyłając bardzo silny, krótkotrwały impuls elektromagnetyczny o wielkiej mocy, spowoduje zniszczenie lub poważne uszkodzenie systemów elektronicznych[5]. Prace nad nią kontynuują Stany Zjednoczone w programie *Counter-electronics High-powered Microwave Advanced Missile Project* (CHAMP). Jego celem jest zbudowanie rakiety, której atak spowoduje zniszczenie na określonym obszarze urządzeń elektronicznych. Rakieta CHAMP, lub raczej jej wersja rozwojowa, oparta na modelu rakiety manewrującej JASSM-ER, będzie zdolna przebywać nad określonym obszarem i emitować promieniowanie w kierunku przeciwnika, generując silne impulsy mikrofal bez użycia broni jądrowej. Kondensatory pocisku mają mieć tyle energii, by oddać około 100 *strzałów*.

16 października 2012 roku nad poligonem w Utah z samolotu B-52 wystrzelono testowy pocisk, który przeleciał po zaprogramowanej trasie. W czasie lotu zniszczył on urządzenia elektroniczne w siedmiu testowanych obiektach i po wykonaniu zadania uległ samozniszczeniu.

System Phaser

RAYTHEON

Broń mikrofalowa, zwana także wiązkową, to broń, której działanie polega na emisji wiązki mikrofal. Jej przedstawicielem jest aktywny system uniemożliwiający dostęp (*Active Denial System*). Tak nazywa się ten system, który został wdrożony do użytku przez armię Stanów Zjednoczonych. Broń ta może wysłać silną wiązkę mikrofal na odległość około kilometra. Dociera ona w głąb skóry na mniej niż milimetr i podgrzewa wodę zawartą w tkankach. Jej działanie sprawia, że żołnierz ma uczucie, jakby się gotował lub stanął przed mocno rozgrzanym piecem. Po przerwaniu emitowania wiązki wrażenie natychmiast ustaje.

Kolejnym przedstawicielem tych środków walki jest opracowany przez firmę Raytheon Missile Systems mikrofalowy system dużej mocy Phaser. Jest on zdolny do wykrywania i śledzenia celów powietrznych za pomocą własnej stacji radiolokacyjnej i do rażenia ich silnymi falami radiowymi. System ten podczas testów w październiku 2018 roku skutecznie unieszkodliwił 33 bezzałogowe statki powietrzne, w tym trzy jednocześnie[6]. Departament Obrony USA podpisał kontrakt na dostarczenie siłom powietrznym prototypu tego systemu (fot. 2).

Specjaliści zajmujący się zagadnieniami obrony powietrznej, tworząc nowe systemy antydostępowe, nie są zainteresowani przedstawionymi kategoriami środków walki. Inaczej ma się z dwoma pozostałymi.

4 N. Świętochowski, *Współczesna broń nieśmiercionośna. Podział i charakterystyka*, „Zeszyty Naukowe WSOWL" 2013 nr 2, s. 10.

5 T. Szubrycht, T. Szymański, *Broń elektromagnetyczna jako nowy środek walki w erze informacyjnej*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005 nr 3 (162), s. 2.

6 https://www.milmag.pl/news/view?news_id=2889/.

Railgun – działo elektromagnetyczne

BAE SYSTEMS

Działo elektromagnetyczne, zwane też elektrycznym czy szynowym, jest rodzajem kinetycznego środka artyleryjskiego (fot. 3). Zasada jego działania, mimo dużego zaawansowania technologicznego, jest dość prosta, gdyż wykorzystuje się tu siłę Lorentza. Pocisk jest tu przewodnikiem i został umieszczony między dwiema nieruchomymi szynami podłączonymi do źródła zasilania. W momencie włączenia zasilania między szyną – pociskiem – szyną powstaje obwód, który generuje bardzo silne, poprzeczne pole magnetyczne. Na obwód działa siła elektrodynamiczna, wskutek czego pocisk jako jedyny ruchomy element jest wyrzucany na zewnątrz.

Obecne prototypy railgunów, bo tak nazywają się te działa, wystrzeliwują pociski z prędkością blisko Ma=8, czyli około 2700 m/s. Olbrzymia prędkość i niewielka masa pocisku sprawiają, że potrafią one osiągnąć niedostępną dla prochowych dział odległość około 550 km. Działo aktualnie jest w zaawansowanej fazie testów. Dużą zaletą tej broni jest niewątpliwie cena jednego strzału szacowana na 25 tys. dolarów. Minusem energia, jaka jest potrzebna do wytworzenia pola elektromagnetycznego, co wiąże się z wielkością całego systemu.

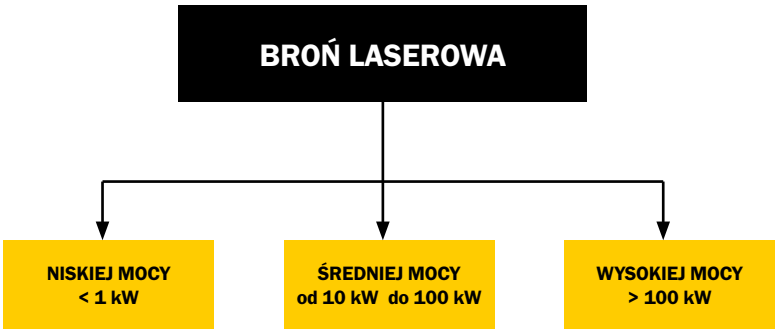
Broń laserowa to ostatni z wymienionych przedstawicieli broni elektromagnetycznej, która w ostatnich latach bardzo szybko się rozwija. Laser, czyli *Light Amplification by Stimulated Emission of Radiation,* dosłownie oznacza wzmocnienie światła przez wymuszoną emisję promieniowania. Jest on generatorem promieniowania elektromagnetycznego z zakresu długości fal od mikrofal do promieniowania X. Jest to zjawisko emisji wymuszonej, czyli stymulowanej lub indukowanej. Emisja wymuszona stanowi podstawę działania laserów. Od standardowego źródła światła światło laserowe różni się zasadą działania oraz właściwościami emitowanego promieniowania. Jest ono koherentne, czyli spójne w czasie i przestrzeni, monochromatyczne (szerokość linii widmowej nie przekracza zwykle 0,002 nm), skolimowane (promienie są równoległe), czyli ma bardzo małą rozbieżność wiązki i dużą moc, oraz jest spolaryzowane i ukierunkowane. Te właściwości pozwalają uzyskać emisję promieniowania w bardzo wąskim przedziale widma o wysokiej mocy.

Laser składa się z trzech zasadniczych elementów, czyli: ośrodka aktywnego (czynnego), rezonatora i układu pompującego[7]. Pierwszy z nich, czyli ośrodek aktywny, jest z reguły podstawą klasyfikacji laserów. Struktura ośrodka czynnego decyduje o najważniejszych parametrach lasera takich, jak: moc, długość fali, sposób pompowania oraz zastosowanie. W zależności od stanu skupienia stosowanego materiału jako ośrodka czynnego rozróżniamy lasery: gazowe, chemiczno-gazowe, na ciele stałym, na cieczy (barwnikowe), półprzewodnikowe (złączowe i bezzłączowe) oraz na swobodnych elektronach.

Rezonator z kolei jest układem optycznym, który spaja promieniowanie charakterystyczne dla danego ośrodka z tym ośrodkiem. Tylko światło o charaktery-

7 B. Ziętek, *Lasery,* Toruń 2008.

RYS. 1. KLASYFIKACJA BRONI LASEROWEJ WEDŁUG POZIOMU MOCY



Opracowanie własne.

styce ustalonej przez rezonator będzie wzmacniane do tego stopnia, by doprowadzić do reakcji laserowej. Trzeci element, czyli układ pompujący, odpowiada za wytworzenie inwersji obsadzeń między stanami zaangażowanymi w przejście laserowe. Pompowanie lasera następuje wskutek: błysku lampy błyskowej (flesza), błysku innego lasera, zderzenia atomów, reakcji chemicznej, przepływu prądu (wyładowanie) w gazie lub wstrzelenia wiązki elektronów do substancji.

W siłach zbrojnych lasery zostały wykorzystane w systemach łączności, ale znalazły też powszechne zastosowanie jako dalmierze i wyznaczniki celu. Służą one do określenia odległości do obiektu i jego prędkości. Mogą zapewnić zakres pomiarowy od kilku metrów do kilkudziesięciu kilometrów. Lasery te emitują krótkie impulsy o czasie trwania około 10 ns z niską częstotliwością ich powtarzania, około 1–20 Hz, z użyciem optycznych długości fal, które zapewniają niskie tłumienie transmisji atmosferycznej.

Kolejną z dziedzin, w której jest wykorzystywany laser, to teledetekcja Light Detection and Ranging (LIDAR) lub Laser Radar (LADAR), czyli technika pomiaru (obrazowanie i mapowanie w 3D), która działa na tej samej zasadzie co radar, tj. promieniuje wiązkę laserową (impulsową lub ciągłą) nad obszarem zainteresowania i przetwarza odbity lub rozproszony sygnał w celu określenia odległości do obiektu. W porównaniu z tradycyjnym radarem radar laserowy zapewnia zwiększoną dokładność pomiaru zasięgu, prędkości i przemieszczenia kątowego. Laserowe urządzenia do teledetekcji są wykorzystywane do różnych zastosowań, takich jak trójwymiarowe mapowanie terenu, identyfikacja i ocena uszkodzeń bojowych w czasie rzeczywistym, planowanie misji na podstawie mapowania 3D, wykrywanie środków chemicznych, nawigacja i naprowadzanie platform bezzałogowych, samolotów itp.[8].

ZASTOSOWANIE BOJOWE

Koncepcja bojowego wykorzystania lasera w obronie przeciwlotniczej i przeciwrakietowej nie jest nowa. Niestety, pierwsze lasery były niskoenergetyczne, co wykluczało ich użycie. Przełom nastąpił z chwilą skonstruowania lasera chemiczno-gazowego, gdzie jako ośrodek czynny wykorzystano tlenek jodu. W 1999 roku Departament Obrony Stanów Zjednoczonych oficjalnie uznał lasery za przyszłą broń, co zapoczątkowało intensyfikację badań, a w efekcie szybki ich rozwój. W 2000 roku utworzono Wspólne Biuro Technologii Laserów Wysokoenergetycznych w celu połączenia wysiłków i opracowania kompleksowego systemu broni laserowej.

Jednym ze sposobów klasyfikowana broni laserowej jest poziom pobierania energii (mocy) – rys. 1.

Lasery niskiej mocy (niskoenergetyczne), czyli mniejszej niż 1 kW, są przede wszystkim używane w systemach symulacji pola walki (np. MILES 2000) lub w systemach komunikacyjnych do zagłuszania sensorów. Lasery o mocy od 10 do 100 kW, czyli średniej mocy, są wykorzystywane do niszczenia urządzeń optycznych lub optoelektronicznych na obiektach naziemnych lub powietrznych. Lasery wysokiej mocy (*High Energy Laser* – HEL) są stosowane w systemach przeciwlotniczych i przeciwrakietowych. Zapewniają one krótki czas działania w zależności od terenu, prędkości celu i od zasady działania, czyli mogą pracować impulsowo lub ciągłe.

W wielu krajach, np. w USA, Rosji, Chinach, Wielkiej Brytanii, Indiach czy RFN, prowadzi się badania nad wysokoenergetycznymi laserami, które można umieścić na pokładach okrętów lub wykorzystać do obrony powietrznej. Należy założyć, że systemy początkowo będą stosowane do osłony obiektów infrastruktury krytycznej, lotnisk czy stanowisk dowodzenia. Jednak by je wykorzystywać, muszą spełnić określone wymagania odnoszące się do wydajnej pracy, tj. dotyczące chłodzenia, przechowywania paliwa laserowego, ochrony środowiska i bezpieczeństwa obsług. Podczas generowania wiązki lasera wytwarza się ogromna ilość ciepła, dlatego systemy chłodzenia są bardzo ważnym elementem każdego z nich.

Kolejny problem to zapewnienie odpowiedniego zapasu paliwa lub energii elektrycznej, by umożliwić długotrwałe działanie systemu i jednoczesne zwalczanie wielu celów. Obecnie do ich budowy używa się głównie pięciu typów laserów, czyli: chemicznego (*Chemical Laser*), na ciele stałym (*Solid State Laser* – SSL), na swobodnych elektronach (*Free Electron Laser* – FEL), światłowodowego (*Fiber Laser*) oraz lasera płynnego (*Liquid Laser*).

8 Ibidem.

Lasery chemiczne to najbardziej dojrzała technologia, która generuje dużą moc w wyniku egzotermicznych reakcji chemicznych do silnego promieniowania podczerwonego. Popularnym ośrodkiem czynnym jest fluorowodór (HF), fluorek deuteru (DF) i chemiczny laser tlenowo-jodowy (*Chemical Oxygen Iodine Laser* – COIL). Są one jednak dość trudne w użytkowaniu, ponieważ do prawidłowego działania wymagają dużej ilości ośrodka czynnego i wydajnego układu chłodzenia. Armia amerykańska we wrześniu 2005 roku zaprzestała prac z laserem chemicznym m.in. ze względu na:

– duży, fizyczny rozmiar takiego lasera w porównaniu z laserem na ciele stałym;

– zbyt duże uwalnianie szkodliwych odpadów do atmosfery;

– trudności w przechowywaniu i przenoszeniu niebezpiecznych płynów DF w zbiornikach ciśnieniowych;

– problemy związane z obsługą logistyczną wynikającą z zastosowania unikatowych środków chemicznych DF[9].

Lasery oparte *na ciele stałym* (*Solid State Laser* – SSL) wykorzystują stałe medium laserowe, takie jak pręt wykonany ze szkła lub kryształu. Oprócz prętu lub materiału macierzystego znajduje się w nich materiał aktywny, taki jak: chrom, neodym, holm lub tytan. Jednym z popularniejszych laserów SSL jest laser neodymowo-itrowo-glinowy (Nd: YAG). Działa on przy długości fali 1064,5 nm i może pracować impulsowo lub z falą ciągłą. Ich zaletą jest to, że długość fali i czas trwania impulsu można zmieniać. Poziom mocy może osiągnąć nawet kilka megawatów, gdy używa się przełączania w celu uzyskania krótkich długości impulsów. Różne interakcje z laserem i różnymi materiałami krystalicznymi mogą podwoić częstotliwość elektromagnetyczną, co zmniejszy o połowę długość fali, przenosząc wiązkę laserową do zakresu widzialnego, 532 nm (zielony). Długość fali można dalej podzielić trzy lub cztery razy, dzięki czemu zakres lasera wynosi od bliskiej podczerwieni do ultrafioletu. Inne zalety tych urządzeń to to, że mogą być bardzo małe, wytrzymałe, tanie i zasilane bateriami.

Lasery *światłowodowe* to odmiana laserów na ciele stałym. Zasilane są energią elektryczną, która wzbudza lasery diodowe pompujące ośrodek aktywny (włókna szklane). Dzięki temu są niezwykle mobilne. W większości przypadków ośrodkiem aktywnym jest włókno poddane działaniu jonów metali ziem rzadkich, takich jak Er3 +, Nd3 +, iterb (Yb3 +), tyllium (Tm3 +) lub prazeodym (Pr3 +). Lasery światłowodowe okazały się znacznie lepsze od opartych na ciele stałym. Są również niezwykle wydajne, jednak nie mogą dobrze funkcjonować w każdych warunkach pogodowych.

Laser *na swobodnych elektronach* (*Free Electron Laser* – FEL) wykorzystuje energię swobodnych elektronów, która następnie jest przekształcana w zmiennym polu magnetycznym, gdzie generuje się wiązkę światła o dużej intensywności. Główną cechą charakteryzującą te lasery jest dostrajalność do różnych długości fal. To z kolei zapewnia dynamiczną zdolność do zmieniających się warunków atmosferycznych, czyli środowiska propagacji.

KTO Stryker wyposażony w mobilny system MEHEL

4.

US ARMY

PRZYKŁADY

Armia Stanów Zjednoczonych prowadzi kilka programów związanych z wprowadzeniem do uzbrojenia systemów laserowych. Badania obejmują zarówno wojska lądowe, siły powietrzne, jak i marynarkę wojenną. Jednym z nich jest program *Multi-Mission High Energy Laser* (MMHEL), który skupia się na zintegrowaniu lasera o mocy 50 kW do zapewnienia wsparcia systemu obrony przeciwlotniczej krótkiego zasięgu (SHORAD) dla brygad ekspedycyjnych. Jest to kontynuacja programu *Mobile Experimental High Energy Laser* (MEHEL) US Army, którego efektem było umieszczenie na transporterze kołowym Stryker lasera o mocy 5 kW (fot. 4). Zgodnie z założeniami tego programu firmy Northrop Grumman i Raytheon mają rok na wyprodukowanie podsystemów laserowych, zintegrowanie ich z platformą Stryker i przeprowadzenie testu wydajności w zakresie różnych zagrożeń. Po ocenie wykonanych testów US Army planuje zakup trzech transporterów wyposażonych w systemy laserowe, które będą eksploatowane w wojskach do 2022 roku.

Kolejny był program *High Energy Laser Tactical Vehicle Demonstration* (HEL-TVD), obejmujący opracowanie lasera klasy 100 kW, który zamontowano na samochodzie ciężarowo-terenowym (fot. 5) do osłony obiektów stacjonarnych i mobilnych przed

9 M. Lavan, *High Energy Laser Systems for Short Range Defense. Acta Physica Polonica Series a*. 115. 10.12693/APhysPolA.115.959.

5.

***High Energy Laser Tactical Vehicle Demonstration* (HEL-TVD), obejmujący opracowanie lasera klasy 100 kW, który zamontowano na samochodzie ciężarowo-terenowym.**

LOCKHEED MARTIN

rakietami oraz pociskami artyleryjskimi i moździerzowymi (C-RAM). HEL-TVD miał być elementem systemu obrony powietrznej krótkiego zasięgu (SHORAD). Program ten w styczniu 2020 roku został zmieniony na *Indirect Fire Protection Capability-High Energy Laser* (IFPC-HEL). Wykorzystując efekty programu HEL-TVD, US Navy zamierza opracować system o większej mocy z lepszymi zdolnościami bojowymi.

Do 2022 roku ma zostać opracowany demonstrator o mocy 300 kW, a do 2024 roku US Army chce przetestować cztery ich prototypy. Wynikiem prac ma być mobilny system przeznaczony do bezpośredniej ochrony obiektów przed uderzeniami rakiet, pocisków artyleryjskich i moździerzowych oraz bezzałogowych statków powietrznych.

Laser Weapon System (LaWS) to przedstawiciel systemu opracowywanego na potrzeby US Navy. Jest to prototypowy system oparty na światłowodowym laserze, przeznaczony do zwalczania bliskich zagrożeń, takich jak rakiety, BSP czy małe łodzie (fot. 6). Został opracowany w ramach programu *Advanced Test High Energy Asset* (ATHENA) przez firmę Lockheed Martin. Wyniki testów okazały się na tyle zadowalające, że stał się on podstawą do uruchomienia nowego programu *Solid State Laser Technology Maturation* (SSL-TM). W jego ramach opracowano laser o mocy do 150 kW, który został zainstalowany na USS „Portland". W maju 2020 roku US Navy poinformowało, że system z powodzeniem zneutralizował bezzałogowy statek powietrzny.

Kolejnym programem US Navy jest *High Energy Laser and Integrated Optical* (HELIOS). Zakłada on opracowanie dwóch systemów laserowych dużej mocy (60–150 kW) z przeznaczeniem do niszczenia małych łodzi, BSP, a także rakiet. System ma być zintegrowany z systemem wykrywania, naprowadzania i kierowania ogniem okrętów (*Aegis Combat System*). Docelowym założeniem programu HELIOS jest zastąpienie systemów MK-15 Phalanx (CIWS) i systemu rakietowego RIM-116.

Z kolei firma Raytheon oferuje *High Energy Laser Weapon System* (HELWS) na pojeździe osobowo-terenowym wysokiej mobilności Polaris MRZR4, zintegrowany z systemem śledzącym *Multi-Spectral Targeting System* (MTS). Do zasilania wykorzystuje się tu ogniwa litowo-jonowe, wymagające ponownego ładowania po oddaniu 20–40 strzałów lub czterogodzinnej pracy w trybie rozpoznania. Co ciekawe, urządzenie może być ładowane z sieci o napięciu 220 W. W marcu 2018 roku podczas testów systemu zniszczono sześć pocisków moździerzowych oraz 12 manewrujących celów powietrznych[10].

Prace nad systemami laserowymi prowadzi się także w wielu innych krajach. W RFN dwie firmy – MBDA oraz Rheinmetall – opracowują swoje produkty w ramach *High Energy Laser System* (HELS). W grudniu 2018 roku przeprowadzono udane testy z laserem o mocy 20 kW. Docelowo ma powstać laser generujący energię od 50 do 80 kW w wersji mobilnej. W Chinach opracowano prototyp systemu przeciwlotniczego, który jest oparty na włóknowych źró-

10 https://www.milmag.pl/news/view?news_id=3012/.

6. System laserowy LaWS na pokładzie okrętu desantowego USS „Ponce”

US NAVY

dłach promieniowania laserowego. Jest to laser półprzewodnikowy o mocy 40 kW i zasięgu 4000 m. Docelowo system ma osiągnąć moc 100 kW.

W Rosji za rozwój systemów laserowych odpowiada Koncern WKO „Ałamaz-Antej”. Prowadzi on badania nad laserem gazodynamicznym, gdzie ośrodkiem czynnym jest dwutlenek węgla. W Izraelu rozpoczęto już próbną eksploatację lasera w ramach systemu Iron Beam. Jego głównym przeznaczeniem jest walka z celami typu C-RAM.

PRZYSZŁOŚĆ

Z przedstawionych rozważań wynika, że broń laserowa i działo elektromagnetyczne wydają się stanowić przyszłość środków walki przeznaczonych do systemów obrony powietrznej i przeciwlotniczej. Kwestią najbliższych lat będzie miniaturyzacja systemów zasilających, dzięki czemu będzie można umieścić je na platformach mobilnych. Na promienie lasera nie ma wpływu grawitacja ani opór atmosferyczny. Oznacza to, że nie są wymagane złożone obliczenia do określenia trajektorii balistycznych i innych charakterystyk – jak w wypadku lotu amunicji konwencjonalnej. Laser jest niezwykle dokładny, dzięki czemu ten precyzyjny środek walki umożliwia przeprowadzanie uderzeń z niewielkimi lub zerowymi stratami ubocznymi. Broń laserowa może być dostosowana do różnych efektów uderzeń – zabójczych lub nieśmiercionośnych, niszczących lub destrukcyjnych. Osiąga się to dzięki regulacji ilości energii i czasu skupionego na celach. Koszt jednego strzału w porównaniu z amunicją konwencjonalną jest niewielki. Na przykład cena rakiety *Patriot Advanced Capability-3* (PAC-3) to 3,3 mln dolarów, rakiety *Terminal High Altitude Area Defense* (THAAD) – 9 mln dolarów, rakiety RIM-161 *Standard Missile 3* (SM-3) – 10–15 mln dolarów, gdy cena jednego strzału bronią laserową ma wynosić zaledwie od 1 do 30 dolarów, przy osiągnięciu jednocześnie równego lub większego prawdopodobieństwa trafienia.

Kolejna zaleta broni laserowej jest związana z mniejszymi ograniczeniami odnoszącymi się do dostępności amunicji niż w wypadku systemów konwencjonalnych. Dostępność ta ograniczona jest jedynie dostępnością mocy i wymaganiami produktów ubocznych podczas generowania wiązki, takich jak ciepło czy chemikalia.

Jednak mimo swoich walorów broń laserowa ma także ograniczenia. Moc energii rozprasza się wraz z parą wodną, pyłem, substancjami zaciemniającymi i turbulencjami atmosferycznymi, czyniąc ją podatną na ukształtowanie terenu i niekorzystne warunki pogodowe. Wiązka laserowa porusza się po linii prostej, co oznacza, że nie jest zdolna do prowadzenia ognia pośredniego nad terenem i przeszkodami oraz nie może strzelać poza ich horyzont widzenia. W zależności od typu lasera, jego zapotrzebowanie na moc oraz produkty uboczne generowania wiązki, takie jak ciepło, mogą znacznie ograniczyć rodzaj platformy potrzebnej do jej zamontowania. Niektóre z ograniczeń i wyzwań obejmują zdolność do generowania wystarczającej mocy do określonych celów. Dzisiaj, aby wygenerować 1 kW mocy lasera, potrzebujemy około 3 kW energii elektrycznej. Silniki montowane w pojazdach zwykle mają moc od 80 do 100 kW i mogą generować znacznie ponad 20 kW mocy lasera w sposób elektryczny, co jest już dużym postępem, ale niewystarczającym, by laser tego typu mógł zniszczyć samolot bojowy. Do tego jest potrzebny laser o mocy powyżej 120 kW. Lasery do 20 kW mogą neutralizować optoelektronikę na odległość od 5 do 10 km, BSP w odległości do 3 km, amunicję średniego kalibru z odległości do 2 km. Jeśli weźmiemy pod uwagę rażenie pocisków moździerzowych, mówimy o mocy 100 kW. Użycie lasera, jako ukierunkowanej broni wysokoenergetycznej, wymaga wystarczającej ilości mocy w megawatach, aby spowodować znaczne uszkodzenia odległego celu. Jednak broń laserowa może być także nieskuteczną metodą niszczenia celów, ponieważ jeśli jest obsługiwana nieprawidłowo, może spowodować obrażenia zarówno celu, jak i użytkownika. Siły zbrojne pracują nad wieloma problemami, by zrekompensować niestabilność wiązki spowodowaną ruchem celu lub platformy.

Mimo ograniczeń potencjał, jaki posiada broń laserowa, nie pozostaje niezauważony. Perspektywa wykorzystania laserów wysokoenergetycznych oraz możliwość uzyskania efektywnej broni stosunkowo niskim kosztem uczyniła tę technologię niezwykle kuszącą. Szybkość rozwoju systemów laserowych może oznaczać, że technologia laserowa w najbliższej przyszłości zdominuje przestrzeń walki. ■

Prowadzenie działań niekonwencjonalnych na **obszarze własnego kraju**

BUDOWANIE SYSTEMU OBRONY POWSZECHNEJ WYKORZYSTUJĄCEGO POTENCJAŁ NASZEGO SPOŁECZEŃSTWA I PAŃSTWA POWINNO BYĆ PODSTAWĄ SKUTECZNEGO OPORU W WYPADKU POJAWIENIA SIĘ ZAGROŻEŃ.

Dariusz Szkołuda jest adiunktem w Zakładzie Wojsk Pancernych i Zmechanizowanych Instytutu Dowodzenia AWL.

Andrzej Zajączkowski jest asystentem w Zakładzie Dowodzenia Instytutu Sztuki Operacyjnej i Taktyki Wydziału Wojskowego ASzWoj.

ppłk rez. dr inż. Dariusz Szkołuda, mjr mgr Andrzej Zajączkowski

Jaki wpływ na niepodległość danego kraju mogą mieć dobrze zorganizowane przez przeciwnika działania niekonwencjonalne (*Unconventional Warfare*), mogliśmy się przekonać w 2014 roku, kiedy to Federacja Rosyjska (FR) dokonała aneksji Krymu. W kolejnej fazie konfliktu prorosyjscy separatyści – przy bezpośrednim zaangażowaniu uzbrojonych grup Rosjan – przejęli władzę we wschodniej Ukrainie i na początku kwietnia 2014 roku proklamowali Doniecką Republikę Ludową i Ługańską Republikę Ludową[1].

Aneksja Krymu oraz działania we wschodniej Ukrainie naruszyły podstawowe zasady prawa międzynarodowego oraz podważyły filary systemu bezpieczeństwa europejskiego, w tym naszego kraju. Ma to przełożenie na postrzeganie zagrożeń w nowej *Strategii bezpieczeństwa narodowego RP* (2020), w której jest zapis, że najpoważniejsze zagrożenie stanowi neoimperialna polityka władz Federacji Rosyjskiej, realizowana również przy użyciu siły militarnej[2]. W artykule zostanie przedstawiony jeden z możliwych wariantów działań niekonwencjonalnych prowadzonych na obszarze naszego kraju, który zostanie zajęty przez przeciwnika. Zatem, w odróżnieniu od aktywności sił zbrojnych FR na Krymie i we wschodniej Ukrainie, której celem było zajęcie terenu sąsiedniego państwa, w artykule zobrazowano – na podstawie przeprowadzonych badań – jak można planować, organizować i prowadzić działania niekonwencjonalne podczas walki o niepodległość własnego kraju dla odzyskania utraconego terenu.

PODSTAWY TEORETYCZNE

Działania niekonwencjonalne w doktrynie armii Stanów Zjednoczonych są zaliczane do działań nieregularnych. Stanowią jedno z pięciu podstawowych zadań, jakie mogą wykonywać amerykańskie wojska specjalne *w celu umożliwienia ruchowi oporu, na terenach przez nie zajmowanych, wymuszenie, zakłócenie lub doprowadzenie do upadku rządu albo sił okupacyjnych, przy pomocy podziemia, partyzantki i grupy wsparcia (społeczeństwo)*[3]. Duże znaczenie

1 I. Katchanovski, *The Separatist War in Donbas: A Violent Break-up of Ukraine*?, s. 2, https://www.researchgate.net/publication/299383810_The_Separatist_War_in_Donbas_A_Violent_Break-up_of_Ukraine/. 20.11.2020.

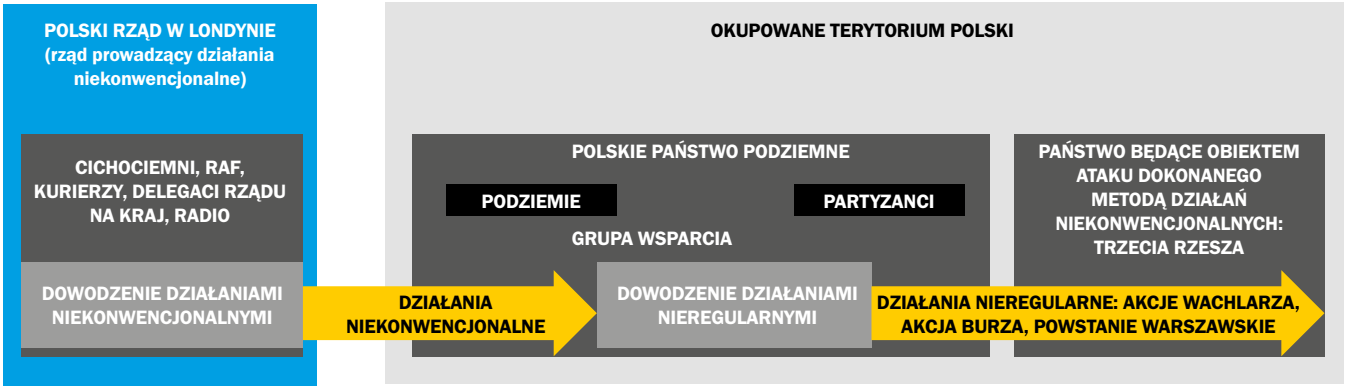
2 *Strategia bezpieczeństwa narodowego RP*, Warszawa 2020, s. 6.

3 D.M. Witty, *Irregular Warfare – A SOF Perspective Newsletter,* Center for Army lessons Learned, s. 35, http://www.globalsecurity. org/ military/ library/. 13.01.2019. Tekst oryginalny: *Activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary and guerrilla force in a denied area.*

W obowiązujących w Siłach Zbrojnych RP regulaminach nie występuje pojęcie *działania niekonwencjonalne*. Używany jest natomiast termin *działania nieregularne*.

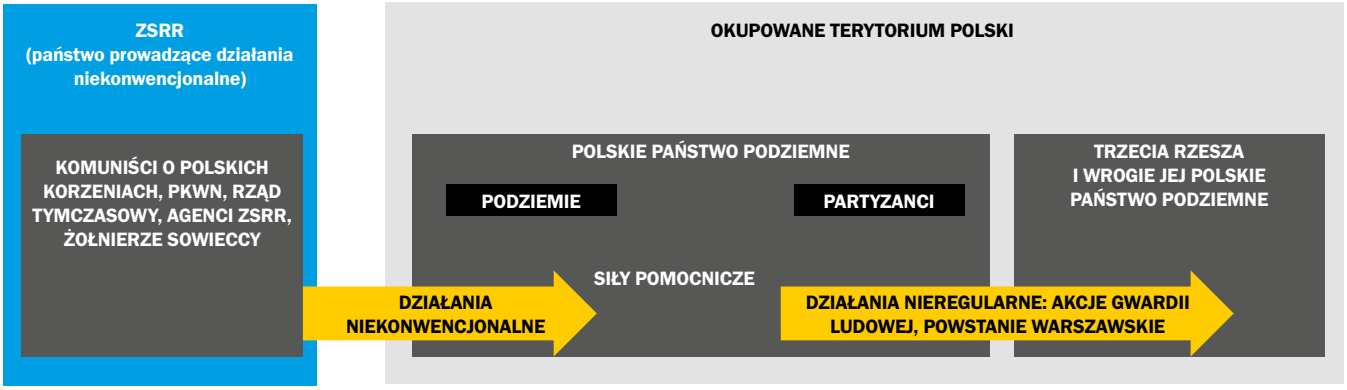
ARCH. 12 BOT

RYS. 1. DZIAŁANIA NIEKONWENCJONALNE POLSKIEGO RZĄDU NA UCHODŹSTWIE W CZASIE II WOJNY ŚWIATOWEJ



Opracowano na podstawie: A. Zajączkowski, *Działania niekonwencjonalne i nieregularne w doktrynach i praktyce – stan obecny i perspektywy* [w:] *Działania nieregularne w uwarunkowaniach współczesnego pola walki*, red. K. Frącik, D. Szkołuda, M. Fryc, Toruń 2018, s. 32.

RYS. 2. DZIAŁANIA NIEKONWENCJONALNE ZSRR W POLSCE



Opracowanie własne.

dla osiągnięcia powodzenia tego przedsięwzięcia ma ograniczanie zdolności przeciwnika przez wspieranie działań powstańczych. Mają one na celu stworzenie warunków do wykonania ataku militarnego lub pokojowego przeprowadzenia zmian (obalenie władzy, zmuszenie sił okupacyjnych do wycofania się).

Partyzantka jest organizowana przez miejscową ludność z zadaniem prowadzenia działań militarnych na terytorium zajętym przez przeciwnika lub przez niego kontrolowanym.

Podziemie natomiast to komórka organizacyjna ruchu oporu zdolna do prowadzenia działań (np. wywrotowych, sabotażu, zbierania informacji) na obszarach niedostępnych dla partyzantów, na przykład na terenach miejskich będących pod kontrolą lokalnych sił bezpieczeństwa przeciwnika.

Grupa wsparcia zaś to część społeczeństwa, która aktywnie wspiera oddziały partyzanckie lub podziemia. Może to dotyczyć prowadzenia działalności wywiadowczej, zabezpieczenia logistycznego lub też wykonywania innych czynności. Członkami grup wsparcia są obywatele, którzy okresowo włączają się w działalność powstańczą.

M. Usydus zwraca uwagę, że *działania niekonwencjonalne mogą być prowadzone w trakcie wojny klasycznej (regularnej), jako wsparcie dla ruchu oporu lub powstania, na teatrze działań wojennych lub tylko jego części, ograniczonej do określonego regionu, jak i w warunkach wojny ograniczonej*[4] *(toczonej w granicach konkretnego terytorium, z użyciem nie wszystkich dostępnych środków, w której przeciwnik musi zostać pokonany na określonym obszarze i nie dochodzi do okupacji jego terytorium). Mogą one przyjmować formę wsparcia bezpośredniego dla sił powstańczych lub ruchu oporu, bez oczekiwania na ewentualne wprowadzenie sił konwencjonalnych*[5].

W dokumentach doktrynalnych NATO pojęcie działań niekonwencjonalnych funkcjonuje od niedawna. W *Słowniku terminów i definicji NATO (AAP-06)* określono, że *niekonwencjonalne działania wojenne to działania wojskowe prowadzone przez lub z udziałem ugrupowań konspiracyjnych oraz oddziałów partyzanckich w celu umożliwienia ruchowi oporu wywierania wpływu, zakłócania działań, a także obalenia rządu lub sił okupacyjnych*[6].

W obowiązujących w Siłach Zbrojnych RP regulaminach nie występuje pojęcie *działania niekonwencjonalne*. Używany jest natomiast termin *działania nieregularne*. Jedynie w dokumencie *Zasady użycia Wojsk Obrony Terytorialnej* określono, że są to działania prowadzone przez te wojska *w terenie czasowo zajętym przez przeciwnika w celu dezorganizacji jego działań, obniżenia potencjału materialnego i morale, uniemożliwienia wykorzystania miejscowych zasobów, a także stworzenia dogodnych warunków do odzyskania utraconego terenu przez wojska operacyjne*[7].

NIECO HISTORII

Zgodnie z przyjętą w NATO definicją działania niekonwencjonalne można postrzegać jako sposób kierowania działaniami nieregularnymi na terytorium kontrolowanym przez obcy rząd lub siły okupacyjne. Można zatem uznać, że Polski Rząd na Uchodźstwie w czasie II wojny światowej, wysyłając do kraju kurierów i łączników oraz nadając audycje radiowe, prowadził działania niekonwencjonalne (rys. 1). Poza tym Armia Krajowa (AK) kierowana przez ten rząd wywierała nacisk na niemieckie władze okupacyjne i zakłócała ich funkcjonowanie, a w trakcie akcji „Burza" dążyła do całkowitego obalenia niemieckiej władzy i odzyskania kontroli nad częścią okupowanego obszaru kraju.

Należy zauważyć, że prowadzenie działań niekonwencjonalnych nie byłoby możliwe, gdyby nie zdolności Wielkiej Brytanii do:

- zapewnienia infrastruktury umożliwiającej funkcjonowanie polskiego rządu i sił zbrojnych na jej terytorium;
- przygotowywania i nadawania audycji radiowych na obszary okupowane przez hitlerowskie Niemcy;
- przekazywania informacji drogą radiową do ośrodków oporu na terenach okupowanych;
- zorganizowania środków do przerzutu ludzi i sprzętu drogą powietrzną;
- zapewnienia na okupowanym terytorium środków łączności radiowej dalekiego zasięgu;
- utrzymania bazy szkoleniowej dla żołnierzy polskich sił specjalnych (cichociemnych).

Należy podkreślić, że po klęsce wrześniowej przystąpiono do organizowania podziemnych lokalnych struktur w ramach takich organizacji, jak Armia Krajowa, Narodowe Siły Zbrojne, Bataliony Chłopskie i wielu innych, które podjęły walkę z okupantem. Tworzenie struktur podziemnych oraz wyposażenie i szkolenie członków tych organizacji zajęło sporo czasu. Niektóre pododdziały były gotowe do rozpoczęcia walki dopiero w 1942, a nawet w 1943 roku[8]. Taki stan rzeczy miał miejsce między innymi dlatego, że w planach obronnych nie przewidywano przejścia sił zbrojnych do prowadzenia działań partyzanckich na terenach opanowanych przez wojska niemieckie[9]. Dopiero działania niekonwencjonalne podjęte przez Polski Rząd w Londynie uaktywniły ruch oporu oraz pozwoliły na zachowanie ciągłości dowodzenia podziemnymi strukturami.

Z kolei ZSRR zainicjował działania niekonwencjonalne (rys. 2) w celu zagarnięcia Polski prawdopodobnie już w 1942 roku. Metodą zabiegów dyplomatycznych i przez wysyłanych agentów Rosjanie skutecznie realizowali swoje cele polityczne.

4 http://stosunki-miedzynarodowe.pl/slownik/68-w/775-wojna-ograniczona/. 14.01.2019. Według słownika wojna ograniczona jest prowadzona do określonej linii, której zwycięskie wojska zobowiązywały się nie przekraczać. Wojna w Korei, Wietnamie, w rejonie Zatoki Perskiej w 1991 roku, w Afganistanie w 2001 roku, a także wojna w Iraku w 2003 roku są – z perspektywy Stanów Zjednoczonych – przykładami wojen toczonych w ograniczony sposób.

5 M. Usydus, *Zbrojny ruch oporu – studium teorii i praktyki działań nieregularnych*, AON, Warszawa 2017, s. 29.

6 *AAP-6 (2014) Słownik terminów i definicji NATO*, s. 403.

7 *Zasady użycia Wojsk Obrony Terytorialnej DT-3.40.1 (projekt),* Warszawa 2016, s. 17.

8 Zob.: Ł. Grzywacz-Świtalski, *Z walk na Podkarpaciu*, Warszawa 1971.

9 D. Szkołuda, *Dowodzenie wojskami obrony terytorialnej w działaniach taktycznych*, ASzWoj, Warszawa 2020, s. 47.

TABELA. FAZY, ETAPY I CZYNNOŚCI WYKONYWANE PODCZAS DZIAŁAŃ NIEKONWENCJONALNYCH NA TERENIE OKUPOWANYM PRZEZ PRZECIWNIKA

Prowadzenie działań niekonwencjonalnych			Główni organizatorzy i wykonawcy
Faza 1	**Przygotowanie**	*Badania naukowe i szkolenie przygotowujące zalążki sztabów i kadr szkoleniowych:* • badania poświęcone prowadzeniu działań niekonwencjonalnych i nieregularnych; • opracowanie jawnego katalogu zdolności do prowadzenia działań niekonwencjonalnych przez SZRP i układ pozamilitarny; • opracowanie doktryn, regulaminów i instrukcji oraz przeprowadzenie szkoleń dla wytypowanej kadry i dowództw; • opracowanie stałych procedur operacyjnych oraz przeprowadzenie ćwiczeń w wytypowanych dowództwach i pododdziałach	– ośrodki naukowe, badawcze i uczelnie wojskowe; – wojska specjalne; – wojska obrony terytorialnej (WOT)
		Uszczegółowienie katalogu zdolności, określenie i wypełnienie luki w zdolnościach: • opracowanie niejawnego katalogu zdolności do prowadzenia działań niekonwencjonalnych przez siły zbrojne i układ pozamilitarny oraz określenie istniejącej luki w zdolnościach; • wypełnianie luki w zdolnościach oraz określenie obszarów niemożliwych do samodzielnego wypełnienia ich przez siły zbrojne i wybrane podmioty układu pozamilitarnego państwa	– Dowództwo Generalne Rodzajów Sił Zbrojnych; – Dowództwo Operacyjne Rodzajów Sił Zbrojnych; – Dowództwo Wojsk Specjalnych; – Dowództwo WOT
		Umowy, uzgodnienia i inne działania o międzynarodowym charakterze: • zawarcie umów z państwami sojuszniczymi i innymi podmiotami (w tym podmiotami pozapaństwowymi) w celu uzupełnienia pozostałej luki w zdolnościach; • zawarcie umów z państwami sojuszniczymi, przyjaznymi i neutralnymi w celu zapewnienia dogodnych warunków funkcjonowania rządu, SZRP, ośrodków kultury i informacji oraz schronienia dla obywateli w sytuacji utraty własnego terytorium; • prawne zapewnienie ciągłości funkcjonowania rządu i SZRP na czas ewakuacji z kraju w przypadku jego zajęcia przez wrogie siły lub przejmowania władzy w kraju przez marionetkowy rząd; • przygotowanie materialnych podstaw funkcjonowania i finansowania rządu Rzeczypospolitej Polskiej, uchodźców i SZRP poza granicami kraju z zapewnieniem dywersyfikacji	– rząd Rzeczypospolitej Polskiej; – Agencja Wywiadu; – Dowództwo Generalne Rodzajów Sił Zbrojnych; – państwa sojusznicze, neutralne i przyjazne; – aktorzy niepaństwowi (*non-governmental organization* – NGO): korporacje, organizacje, armatorzy, firmy transportowe, grupy przestępcze zajmujące się przemytem itp.
		Działania przed zajęciem własnego terytorium przez przeciwnika: • przygotowanie i sprawdzenie niezależnego od państw sojuszniczych systemu zapewniającego łączność rządu RP z ośrodkami ulokowanymi poza terytorium kraju; • powołanie dowództwa lub specjalistycznej komórki przeznaczonej do prowadzenia działań niekonwencjonalnych; • informacyjne przygotowanie przyszłych działań, opracowanie wariantów działania, wydanie zarządzeń przygotowawczych, opracowanie draftu rozkazu operacyjnego i innych dokumentów dowodzenia; • przeprowadzenie akcji edukacyjnej z udziałem prasy, radia i telewizji w celu integracji społeczeństwa oraz przygotowania obywateli do stawiania oporu; • opracowanie planu ewakuacji oraz zorganizowanie zapasowego miejsca rozmieszczenia rządu RP na obszarze innego województwa lub poza granicami kraju; • przygotowanie zapasowych rejonów rozmieszczenia stanowisk dowodzenia, ośrodka szkoleniowego, ośrodków kultury, wydawnictwa oraz rozgłośni radiowej i telewizyjnej w kraju i za granicą; • utworzenie i wyposażenie magazynów: środków łączności, broni, amunicji, materiałów wybuchowych, paliwa i żywności; • zorganizowanie zalążka struktury zbrojnego ruchu oporu oraz podstaw finansowania jego działalności	– marynarka wojenna; – siły powietrzne; – wojska łączności i informatyki; – wojska specjalne; – wojska obrony terytorialnej; – Agencja Wywiadu; – Policja; – Straż Graniczna; – administracja; – Radio i Telewizja; – szkolnictwo

Prowadzenie działań niekonwencjonalnych			Główni organizatorzy i wykonawcy
Faza 1	**Przygotowanie**	*W trakcie zajmowania obszaru kraju przez przeciwnika:* przejęcie dowodzenia przez personel rozlokowany w zawczasu przygotowanych centrach i zapasowych stanowiskach dowodzenia; ewakuacja rządu, SZRP, ośrodków kultury i informacji oraz wytypowanych obywateli; intensyfikacja działań informacyjnych ukierunkowanych na podtrzymanie morale własnego społeczeństwa; stopniowa ewakuacja większości potencjału SZRP	– rząd RP; – Agencja Wywiadu; – SZRP
		Po zajęciu obszaru kraju przez przeciwnika: pełne rozwinięcie poza okupowanym terytorium stanowisk dowodzenia, ośrodka szkoleniowego, ośrodków kultury, wydawnictwa, rozgłośni radiowej i telewizyjnej; przejście wytypowanych żołnierzy i funkcjonariuszy do głębokiej konspiracji; organizowanie przez wytypowanych funkcjonariuszy protestów społecznych i obywatelskiego nieposłuszeństwa; intensyfikacja działań informacyjnych ukierunkowanych na podtrzymanie morale własnego społeczeństwa: audycje radiowe i telewizyjne oraz informacje przekazywane przez media społecznościowe	– ewakuowany rząd, SZRP i funkcjonariusze państwowi; – służby specjalne; – wojska specjalne; – WOT
Faza 2	**Nawiązanie kontaktu**	*W przypadku pomyślnej realizacji fazy 1 faza 2 nie będzie realizowana.* Zapewniona będzie bowiem ciągłość funkcjonowania rządu i sił zbrojnych. • Należy się spodziewać, że państwa sojusznicze będą się starały realizować fazę 2 w ramach własnych działań niekonwencjonalnych w celu wsparcia ruchu oporu w naszym kraju, jak również przejęcia nad nim kontroli i ukierunkowania jego działań zgodnie z własnymi potrzebami. Prawdopodobne będą prowokacje oraz próby tworzenia fikcyjnego ruchu oporu przez służby specjalne okupanta. • W przypadku niespodziewanego zajęcia części terytorium naszego kraju przez wrogie państwo lub oderwania się jego części (np. województwa) konieczne może być nawiązanie kontaktu z przedstawicielami opozycji wywodzącej się z lokalnych przywódców politycznych i aktywistów.	– służby specjalne
Faza 3	**Przeniknięcie**	*W przypadku pomyślnej realizacji fazy 1 faza 3 będzie realizowana w ograniczonym zakresie*. Na utraconym terytorium zostaną bowiem wytypowani żołnierze i agenci, którzy będą dysponowali środkami zapewniającymi autonomiczną i bezpieczną łączność z rządem i dowództwem. • W przypadku zaniedbań w trakcie realizacji fazy 1 konieczne może się okazać przeniknięcie żołnierzy wojsk specjalnych na teren okupowany. Siły powietrzne, marynarka wojenna oraz zakontraktowani aktorzy niepaństwowi zabezpieczą transport. Celowe jest wykorzystanie znających teren i lokalne uwarunkowania żołnierzy WOT oraz funkcjonariuszy Straży Granicznej. • Wysłane grupy agentów i żołnierzy potwierdzą porozumienie z lokalnymi liderami ruchu oporu i skoordynują przybycie kolejnych zespołów. • Zespoły żołnierzy wojsk specjalnych nawiążą kontakt ze swoimi partnerami z ruchu oporu.	– służby specjalne; – wojska specjalne; – wojska obrony terytorialnej; – Straż Graniczna; – państwa sojusznicze, neutralne i przyjazne; – NGO; – ruch oporu
Faza 4	**Organizacja**	• Rozwijane będą struktury ruchu oporu oraz system jego finansowania i zaopatrzenia. • Żołnierze wojsk specjalnych nawiążą współpracę z dowództwem ruchu oporu oraz dokonają oceny sytuacji i przygotują plany działania. • Rozpocznie się werbunek wytypowanych żołnierzy WOT do ruchu oporu. • Rząd za pośrednictwem działań niekonwencjonalnych wojsk specjalnych i WOT będzie kierował ruchem oporu i jego działaniami na okupowanym obszarze.	– wojska specjalne; – WOT; – ruch oporu
Faza 5	**Rozbudowa**	• Żołnierze będą: wspierać ruch oporu, rozwijać infrastrukturę do zabezpieczenia działań, prowadzić uzupełniające szkolenia oraz kierować działaniami w celu zdobycia środków materiałowych i umożliwienia członkom ruchu oporu nabycia doświadczenia bojowego. • Doskonalony będzie plan prowadzenia działań bojowych na większą skalę, zmierzający do wybuchu powstania.	– wojska specjalne; – WOT; – ruch oporu; – Dowództwo Operacyjne Rodzajów Sił Zbrojnych
Faza 6	**Powstanie**	W sprzyjającej sytuacji politycznej i militarnej kierownictwo polityczne wydaje decyzję o rozpoczęciu powstania. Powstańcy prowadzą działania bojowe kierowani i wspierani przez żołnierzy wojsk specjalnych i WOT. Jeżeli istnieje taka możliwość, działania mogą być wspierane przez lotnictwo i artylerię. SZRP i państwa sojusznicze wspierają powstanie, zapewniając walczącym świadomość sytuacyjną i wsparcie militarne. Siły zbroje przeciwnika zostają pokonane, a rząd marionetkowy obalony.	– wojska specjalne; – WOT; – siły powietrzne; – wojska lądowe
Faza 7	**Normalizacja**	Kierownictwo ruchu oporu wspomagane przez doradców z wojsk specjalnych przechodzi pod bezpośrednią kontrolę polskiego rządu, którego przedstawiciele stopniowo wracają na odzyskane terytorium. Pododdziały ruchu oporu przechodzą w podporządkowanie sił zbrojnych, policji lub innych służb. Faza ta może być realizowana w ramach operacji stabilizacyjnych lub operacji reagowania kryzysowego. Do odbudowy państwa angażuje się doradców wojskowych i specjalistów cywilnych, w tym organizacje pozarządowe.	– polski rząd; wojska specjalne; WOT; partyzanci; wojska lądowe; Żandarmeria Wojskowa; siły powietrzne; marynarka wojenna; Policja; służby specjalne

Opracowano na podstawie ćwiczeń „Brama-19”.

ARCH. 12 BOT

Utworzona siatka Ludowego Komisariatu Spraw Wewnętrznych (NKWD) likwidowała kurierów, delegatów rządu i innych członków polskiego podziemia. Dodatkowo w okupowanym kraju i na arenie międzynarodowej prowadzono akcję propagandową zarzucającą Armii Krajowej bierność lub kolaborację z Niemcami[10].

W wyniku tych działań doszło do osłabienia pozycji AK, zintensyfikowania dywersyjnej działalności lewicowej partyzantki oraz stworzenia warunków do uczynienia naszego kraju satelitą Związku Radzieckiego. Poza tym, według części polskich historyków, działania komunistów sprowokowały Armię Krajową do niepotrzebnych walk z Niemcami. W wydanej przez IPN antologii *Żeby Polska była Polską* czytamy: *Wbrew opinii całego narodu, wbrew jego najgłębszemu instynktowi, pchany jest żołnierz AK do współpracy z Moskwą. Żołnierzowi polskiemu chce się narzucić rolę narzędzia politycznego w rękach Kremla.* […] *W miarę posuwania się frontu bolszewickiego w głąb kraju coraz to nowe oddziały AK otrzymywały rozkaz ujawnienia się i współdziałania z Armią Czerwoną*[11].

PRZYKŁADOWY SCENARIUSZ

Efektem prowadzonych badań, między innymi w ramach ćwiczeń studyjnych organizowanych w Akademii Sztuki Wojennej, są prezentowane możliwe scenariusze prowadzenia działań niekonwencjonalnych na obszarze naszego kraju. Analizie poddano również sytuację, w której działania niekonwencjonalne byłyby prowadzone w przypadku okupacji zajętych przez przeciwnika terenów (tab.). Analizę prowadzono według siedmiu faz wyodręb-

10 M.R. Bombicki, *AK i WIN przed sądami specjalnymi*, Poznań 1993, s. 10–11.

11 P. Zychowicz, *Opcja niemiecka, czyli jak polscy antykomuniści próbowali porozumieć się z III Rzeszą*, Poznań 2014, s. 363–364.

Zgodnie z przyjętą w NATO definicją *działania niekonwencjonalne* można postrzegać jako sposób kierowania działaniami nieregularnymi na terytorium kontrolowanym przez obcy rząd lub siły okupacyjne.

nionych w dokumentach doktrynalnych armii amerykańskiej. Przy czym, co należy podkreślić, doktryna ta przewiduje prowadzenie działań niekonwencjonalnych tylko poza terytorium Stanów Zjednoczonych.

WIELE PRZED NAMI

Doświadczenia z walk o wyzwolenie naszego kraju spod okupacji niemieckiej w czasie II wojny światowej wskazują, że prowadzenie w przyszłości działań niekonwencjonalnych może być dla rządu i sił zbrojnych nie kwestią wyboru, lecz koniecznością. Nasz kraj powinien być przygotowany do ich prowadzenia z użyciem sił zbrojnych w rejonach zajętych przez przeciwnika.

Szczególnie istotną cechą tych działań jest ryzyko. Dotyczy ono podejmowania przez dowódców poziomu taktycznego decyzji o negatywnych konsekwencjach politycznych. Związek działań bojowych z konsekwencjami politycznymi sprawia, że działania niekonwencjonalne są szczególnie narażone na oddziaływania agenturalne i wymagają terminowej, skrytej i sprawnej łączności między dowódcami na terenie okupowanym a dowództwem znajdującym się poza tym obszarem.

W związku z tym, że procedury amerykańskie, którymi posługiwano się w trakcie ćwiczeń w ASzWoj, nie przewidują wariantu odzyskiwania własnego terytorium dzięki zastosowaniu działań niekonwencjonalnych, są dla nas mało przydatne. Celowe jest więc kontynuowanie badań zmierzających do opracowania i wdrożenia procedur adekwatnych do położenia geopolitycznego naszego kraju, istniejących zagrożeń i posiadanych zasobów. Dlatego też w trakcie ćwiczeń dowódczo-sztabowych należy przerabiać scenariusze, zgodnie z którymi tracimy całość lub część naszego terytorium i jesteśmy zmuszeni stosować omawiane działania. Efektem badań powinien być katalog zdolności, jakie należy osiągnąć, by skutecznie je prowadzić. ■

Okrętowe **systemy walki**

ZINTEGROWANIE W SPÓJNĄ CAŁOŚĆ WSZYSTKICH PODSYSTEMÓW UMOŻLIWIA DOWÓDCY OKRĘTU SZYBKĄ REAKCJĘ NA SYTUACJĘ TAKTYCZNĄ.

kmdr por. rez. Grzegorz Kolański

Autor jest samodzielnym referentem w Oddziale Planowania Operacji w COM-DKM.

Zwiększenie roli lotnictwa w prowadzeniu działań na morzach oraz rozwój technik rakietowych spowodowało duże zmiany w całościowym podejściu do zagadnień związanych z projektowaniem okrętów. Nowe zagrożenia wymogły nie tylko zmianę pokładowych systemów uzbrojenia i wyposażenia, lecz także wprowadzenie rozwiązań dostosowujących jednostki do nowej rzeczywistości wojny na morzu. Jednym z takich rozwiązań są okrętowe systemy walki.

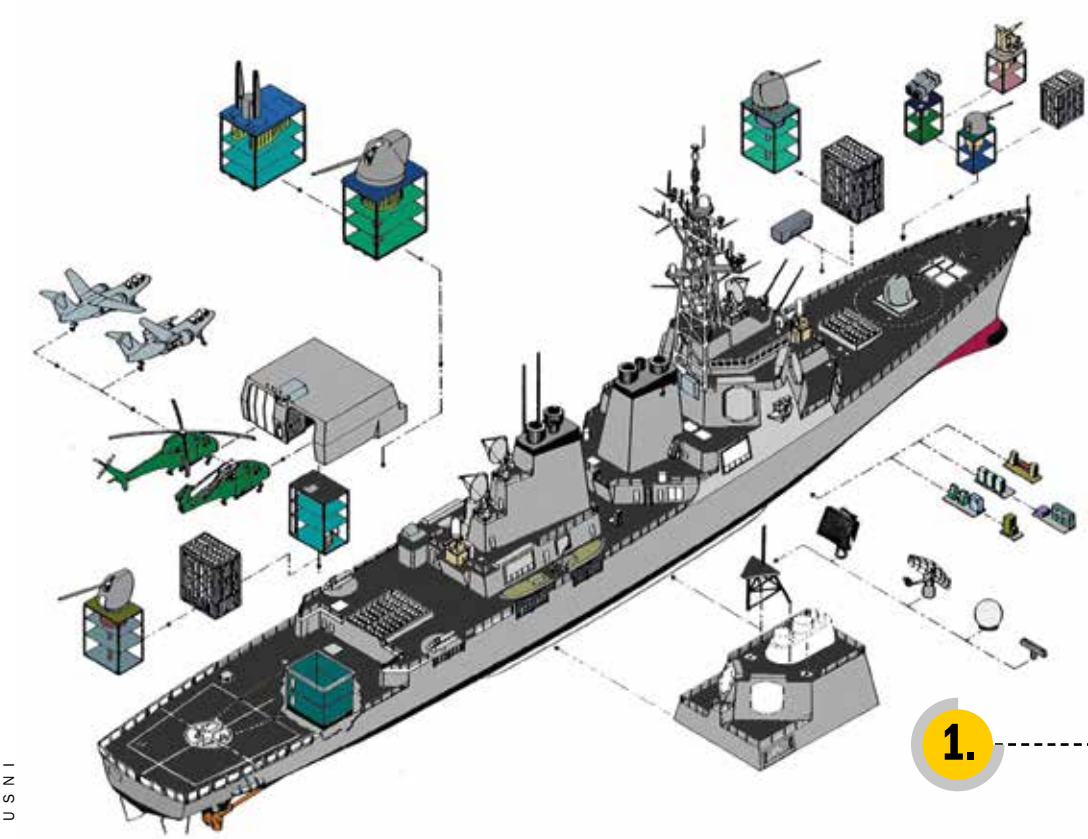
KWESTIA CZASU?

Można się rozpisywać na temat współczesnego morskiego teatru działań wojennych lub też spróbować opisać go dość krótko. Czyli, że jest on złożony, trudny do przewidzenia, wymagający szybkiej analizy dużej ilość danych i szybkiego procesu decyzyjnego, zakończonego wypracowaniem optymalnej decyzji. Do głównych czynników kształtujących jego oblicze w ciągu ostatnich kilkudziesięciu lat można zaliczyć rozwój możliwości bojowych lotnictwa oraz systemów rakietowych. Już te dwa elementy powodują, że czas stał się jednym z podstawowych kryteriów decydujących o przeżywalności jednostek, czyli ma się tu na myśli czas potrzebny na wykrycie zagrożenia i jego ocenę. Czas niezbędny, aby przeanalizować sytuację i przeprowadzić proces decyzyjny. Czas potrzebny na wprowadzenie decyzji w życie i zastosowanie odpowiednich środków zaradczych. A wszystko to w warunkach zagrożenia z lądu, morza i z powietrza. Dobrze, jeśli wiadomo, kto jest przeciwnikiem i gdzie się znajduje. Ale dzisiaj nie jest to takie proste i łatwe do stwierdzenia. Proliferacja rakietowych systemów przeciwokrętowych spowodowała, że uzbrojone są w nie nie tylko podmioty państwowe, dysponują nimi także mniej lub bardziej formalne organizacje o charakterze wojskowym czy też terrorystycznym. Systemy rakietowe, przenoszone przez platformy morskie, powietrzne i lądowe, są uważane obecnie za największe zagrożenie dla jednostek pływających. Główne atuty rakiet to prędkość i małe wymiary. Ale nie można przy tym zapominać o torpedach i minach. Podobnie jak rakiety są one również coraz trudniejsze do wykrycia i stają się coraz inteligentniejsze. A im później zagrożenie zostanie wykryte, tym mniej czasu pozostaje na reakcję.

Prawdopodobnie właśnie czas stał się czynnikiem, który wymusił zautomatyzowanie procesu walki na okrętach. Automatyzacja pozwala na zrzucenie wielu zadań na urządzenia elektroniczne i systemy teleinformatyczne, przez co skraca czas potrzebny na ich realizację. A przy okazji ogranicza ingerencję czynnika ludzkiego i zmniejsza prawdopodobieństwa popełnienia przez ludzi błędu.

ROLA I ZADANIA

Okrętowy system walki można opisać jako pokładowy supersystem, który łączy z sobą poszczególne podsystemy okrętowe i pozwala na wymianę danych zarówno wewnątrz okrętu, jak i ze środowiskiem zewnętrznym. Jego podstawowe składniki funkcjonalne to okrętowe sensory i efektory. Do tych pierwszych należą systemy radiolokacyjne, hydrolokacyjne,



USNI

1.

Modułowość i otwarta architektura. Pod tymi hasłami kryje się nie tylko zdolność do wymiany wyposażenia i uzbrojenia, lecz także – a może przede wszystkim – podatny na modyfikacje okrętowy system walki.

optoelektroniczne i rozpoznawcze. Czyli wszystkie te, które dostarczają informacji o środowisku, w którym okręt prowadzi działania.

Do zbioru efektorów należą systemy i zestawy pokładowego uzbrojenia, a także pasywne i aktywne systemy walki radioelektronicznej. Czyli wszystko to, co pozwala na oddziaływanie na środowisko zewnętrzne. Sensory i efektory połączone są dzięki pokładowym systemom teleinformatycznym umożliwiającym wymianę danych wewnątrz okrętu. Z kolei na wymianę informacji z innymi platformami pozwala system łączności.

A jak to wszystko działa? Oczywiście w pewnym uproszczeniu. Dane dostarczane przez sensory okrętowe są wykorzystywane do budowania świadomości sytuacyjnej wokół jednostki. I to zarówno w wymiarze nawodnym, podwodnym, jak i powietrznym. Kolejnym krokiem jest zamiana tych danych w informację. Odbywa się to w wyniku ich interpretacji, porównania i oceny. Dzięki temu powstaje obraz sytuacyjny. Na jego podstawie dowódca przeprowadza proces decyzyjny, który kończy się wypracowaniem rozwiązania adekwatnego dla danej sytuacji. Jego wprowadzenie w życie jest związane z zaangażowaniem systemów kierowania ogniem i uzbrojenia czy też systemów walki radioelektronicznej.

Niektóre elementy opisanego procesu mogą być wykonywane w sposób zautomatyzowany lub nawet niemal całkowicie automatycznie. Zawsze jednak obecny jest w nich czynnik ludzki – jako osoba kontrolująca, interpretująca czy też podejmująca lub zatwierdzająca ostateczną decyzję. W przyszłości rola człowieka może zostać jeszcze bardziej ograniczona, na przykład dzięki szerszemu zastosowaniu sztucznej inteligencji. Umożliwi to zarówno skrócenie czasu trwania całego procesu, jak też wypracowania decyzji zbliżonej do optymalnej i pozbawionej wpływu ludzkich błędów i osądów. Czy jednak pozwoli to na całkowite wyeliminowanie czynnika ludzkiego? Nawet w obliczu tendencji do zmniejszania liczby członków załóg okrętowych? I kolejne pytanie: czy taki oparty na sztucznej inteligencji system będzie lepszy niż wyszkolona i przygotowana załoga. Może i popełniająca błędy, ale i zdolna do nieszablonowego procesu myślowego, niedającego się tak łatwo odwzorować w postaci kodu maszynowego.

Idea okrętowego systemu walki jest dość prosta, w przeciwieństwie do jej realizacji. Każdy system musi zostać opracowany pod kątem danego okrętu oraz przenoszonego przez niego uzbrojenia i wyposażenia. Każdorazowa zmiana tej konfiguracji wymusza również zmiany w oprogramowaniu systemu walki. Pożądaną cechą jest więc także jego elastyczność i podatność na modernizacje i modyfikacje. W jakimś stopniu musi on również uwzględniać tak-

THALES

TACTICOS pozwala na łatwe zgranie operatorów, także dzięki ścianie współpracy (*collaborationwall*), czyli grupie monitorów umożliwiających szybką orientację w ogólnej sytuacji.

tykę działania jednostek danej klasy lub też doktrynę funkcjonowania danej marynarki wojennej.

EWOLUCJA

Początków okrętowych systemów dowodzenia można szukać w latach sześćdziesiątych ubiegłego wieku. Realia zimnej wojny wymogły zastosowanie technologii komputerowych w systemach kierowania ogniem i pierwszych systemach kierowania walką. Ich głównym obszarem działania były wody oceaniczne, a przeciwnik był dość jasno określony. Jak można było się domyśleć, ówczesne technologie informatyczne znacznie odbiegały od dzisiejszych standardów, co wiązało się przede wszystkim z małą mocą obliczeniową i niską niezawodnością. Początki były jednak bardzo obiecujące i zapotrzebowanie na tego typu zdigitalizowane systemy zwiększało się bardzo szybko. Brakowało im jednak nie tylko mocy obliczeniowej, lecz także zdolności do przechowywania danych i zobrazowania informacji. Pomocny okazał się postęp technologiczny oraz rozwój mikroprocesorów i związany z tym rozwój mikrokomputerów. Dzięki rewolucji informatycznej możliwe było przejście od scentralizowanych komputerów mainframowych do lokalnych sieci komputerowych.

Kolejny etap ewolucji jest związany z zastosowaniem systemów otwartej architektury i produktów komercyjnych. Pozwala to na wykorzystanie sprzętu i oprogramowania wielu producentów, a to ułatwia ewentualne modernizacje oraz obniża koszty produkcji i eksploatacji.

Okrętowe systemy walki w dużym stopniu determinują możliwości bojowe współczesnych okrętów (fot. 1). Nic więc dziwnego, że firmy zajmujące się wyposażeniem i uzbrajaniem tych jednostek poszły za wezwaniem rynku i opracowały swoje wersje systemów walki. Część z nich nie jest dostępna na wolnym rynku, a ich sprzedaż – czasem związana z przekazaniem wrażliwych technologii – dotyczy tylko bliskich sojuszników. Jest jednak kilka systemów, które można kupić z tzw. półki. Należy jednak przy tym pamiętać, że nawet taki komercyjny system musi zostać dopasowany do konkretnej jednostki. Oznacza to potrzebę zintegrowania z nim praktycznie każdego systemu pokładowego wyposażenia i uzbrojenia. Dlatego też koszty zakupu systemu walki nie są małe, a o jego dojrzałości świadczyć mogą lata doświadczeń i... zadowoleni klienci. W literaturze angielskojęzycznej okrętowy system walki jest określany jako *Combat System*, czasami z dopiskiem *naval*, aby zaznaczyć jego morskie przeznaczenie i zastosowanie. Zamiennie z tym określeniem może być stosowana nazwa *Combat Management System*, chociaż w tym wypadku jego znaczenie może być ograniczone do kierowania (dowodzenia) tylko samym procesem walki. A więc do integracji sensorów i efektorów oraz zarządzania nimi.

TACTICOS

Jednym z najbardziej znanych produktów na komercyjnym rynku okrętowych systemów walki jest TACTICOS firmy Thales (fot. 2). Według informacji producenta jest on używany na ponad 180 okrętach znajdujących się w służbie 20 światowych marynarek. Do tej liczby trzeba zaliczyć także i naszą marynarkę wojenną z kutrami rakietowymi typu Orkan i okrętem patrolowym ORP „Ślązak”.

Początków systemu należy szukać w latach dziewięćdziesiątych ubiegłego wieku. W tym okresie wprowadzono do służby pierwsze wersje systemów STACOS (ówczesnej firmy Signaal, obecnie Thales Nederland) i TAVITAC (firmy Thomson-CSF, obecnie Thales). W wyniku połączenia firm i związanej z tym faktem unifikacji systemów powstał TACTICOS. Wersję systemu z lat dziewięćdziesiątych oznaczono jako Baseline 0. W 2005 roku pojawiła się wersja Baseline 1 z zaimplementowanym systemem przesyłania danych Link-16. Kolejna wersja, Baseline 2, weszła do służby w 2009 roku.

System jest reklamowany jako produkt modułowy, zapewniający duży stopień elastyczności w doborze i integracji podsystemów. Na podstawie zebranych doświadczeń Thales przygotował kilka modułów zadaniowych (*Mission Solution*), odpowiadających przeznaczeniu potencjalnej platformy, która ma zostać wyposażona w system TACTICOS. Wymagający najmniejszego stopnia integracji podsystemów i decyzyjności moduł MS100 (*Mission Solution 100*) jest przeznaczony do wykonywania działań związanych z zapewnieniem bezpieczeństwa w strefie wód przybrzeżnych. Kolejny moduł, MS150, służy do realizacji tych samych zadań, ale już w strefie oceanicznej. Te dwa moduły są przeznaczone odpowiednio dla małych i dużych jednostek patrolowych, w domyśle głównie dla straży wybrzeża. Dla jednostek marynarki wojennej dedykowano moduły 300, 400 i 500, które odpowiadają działaniom bojowym o niskim, średnim i wysokim stopniu intensywności. Przekładając to na język praktycznej realizacji, oznaczają one zdolność do samoobrony (*point defence*) z wykorzystaniem tylko artylerii (300), artylerii i rakiet (400) oraz zdolność do obrony rejonu (*area defence*) z wykorzystaniem artylerii i rakiet (500). Firma oferuje jeszcze jeden moduł zadaniowy, oznaczony liczbą 1000, który jest związany z implementacją na platformie bojowej zdolności do prowadzenia obrony przeciw rakietom balistycznym.

O słuszności wprowadzonych rozwiązań i elastyczności systemu TACTICOS świadczą jego zastosowania praktyczne. A te obejmują zarówno jednostki patrolowe, jak i duże okręty bojowe. Wśród tych drugich można wymienić niemieckie fregaty typu Sachsen, przeznaczone do zwalczania celów powietrznych, korwety typu Braunschweig i zaopatrzeniowiec „Berlin". We współpracy z firmą Northrop Grumman opracowano wersję systemu TACTICOS dla amerykańskich jednostek typu Independence (*Integrated Combat Management System* – ICMS).

Aby utrzymać aktualność systemu, Thales co sześć miesięcy wydaje pakiet modernizacyjny, który jest dostępny w jego ośrodkach szkoleniowych. W roku 2015 firma opracowała i udostępniła klientom moduł przeznaczony do prowadzenia działań przeciwko piratom i przemytnikom. Kolejny duży krok w rozwoju systemu TACTICOS zaplanowano na rok 2022, kiedy to zostanie wydana wersja Baseline 3, m.in. z najnowszymi technologiami z dziedziny walki radioelektronicznej i bezpieczeństwa informatycznego.

System 9LV firmy Saab może zostać zaimplementowany nie tylko na jednostkach nawodnych, lecz także na okrętach podwodnych.

Z TACTICOS-em jest związany południowokoreański system walki Naval Shield. Firmy z tego kraju aktywnie współpracowały z europejskimi konsorcjami dostarczającymi elektronikę i oprogramowanie dla przemysłu okrętowego. Przykładem mogą być spółki Samsung Thales i późniejsza Hanwha Thales. Efektem współpracy była m.in. implementacja systemu TACTICOS na okręcie desantowym (szturmowym) typu Dokdo. System Naval Shield został opracowany przez konsorcjum Hanwha Thales i zaimplementowany po raz pierwszy na koreańskich fregatach typu Incheon.

W 2016 roku Hanwha Group wykupiła udziały od Thalesa i zmieniła nazwę konsorcjum na Hanwha Systems, stając się największym dostawcą elektroniki wojskowej w Korei Południowej. W kolejnych latach czysto koreański Naval Shield został wybrany na system walki dla fregat typu Daegu, pokonując TACTICOS. W grudniu 2020 roku poinformowano, że Hanwha Systems została wybrana do opracowania systemu walki oraz systemu radiolokacyjnego dla perspektywicznych koreańskich niszczycieli KDDX.

SZWEDZKI 9LV

Podobnie jak system TACTICOS również system 9LV szwedzkiej firmy SAAB jest przeznaczony do zastosowania na okrętach różnych klas, wykonujących zadania zarówno w strefie wód przybrzeżnych, jak i na wodach oceanicznych. System może zostać zaimplementowany na platformach nawodnych i podwodnych (fot. 3). W zależności od potrzeb za-

4.

W 2012 roku firma Lockheed uruchomiła wraz z wprowadzeniem do użytku systemu Aegis w wersji Baseline 9.0 usługę CSL (*Common Source Library*), umożliwiającą użytkownikom systemu dostęp m.in. do danych związanych ze szkoleniem operatorów.

LOCKHEED MARTIN

5.

Nowe amerykańskie fregaty typu Constellation zostaną wyposażone w system walki będący pochodną systemów Aegis i COMBATSS-21. Na zdjęciu wizja fregat typu FFG-62.

USNI

Sala do szkolenia operatorów kanadyjskiego systemu walki CMS 330. Oprogramowanie szkoleniowe wykorzystuje te same aplikacje, które są obecne w oprogramowaniu instalowanym na okrętach.

6.

LOCKHEED MARTIN CANADA

mawiającego firma może dostarczyć trzy jego warianty, które różnią się stopniem integracji z pokładowymi systemami uzbrojenia i wyposażenia.

W wariancie najbardziej rozbudowanym firma odgrywa rolę dostawcy systemu walki (*Combat System* – 9LV CS) i odpowiada za integrację wszystkich jego podsystemów. Wybór tych ostatnich zależy tylko od zamawiającego, a ich integracja z systemem jest możliwa dzięki dużej jego elastyczności. SAAB może dostarczyć również mniej rozbudowaną wersję, a w zasadzie centralną część systemu, określaną jako system zarządzania walką (*Combat Management System* – 9LV CMS). Dzięki otwartej architekturze możliwa jest także integracja wybranych elementów systemu z produktami innych firm. W pełnym wydaniu w skład 9LV CMS wchodzi również system kierowania ogniem (*Fire Control System* – 9LV FCS), który może być także dostarczony jako osobny element innego systemu walki.

Oznaczenie systemu – 9LV – pochodzi z lat sześćdziesiątych ubiegłego wieku. Litery LV to skrót od szwedzkiego słowa *luftvärn* (przeciwlotniczy). Cyfra 9 oznacza natomiast produkty wykonane w Szwecji przez tamtejszy oddział firmy Philips – Philips Teleindustri AB. Firma ta otrzymała w 1969 roku kontrakt na opracowanie pierwszej wersji systemu 9LV Mk 1, przeznaczonej dla szwedzkich jednostek typu Norrköping. Od tamtej pory w system ten wyposażono ponad 250 okrętów pływających pod banderą ponad 20 marynarek. W różnych odsłonach został on zaimplementowany m.in. na pokładzie australijskich okrętów desantowych typu Hobart oraz fregat typu ANZAC. Innym przykładem jego zastosowania są szwedzkie korwety typu Visby i okręty podwodne typu Gotland.

AEGIS

Prawdopodobnie najbardziej znanym okrętowym systemem walki jest amerykański system Aegis (fot. 4). Jego historia rozpoczęła się w 1963 roku wraz z przerwaniem prac nad pociskami rakietowymi Typhoon i jednym z pierwszych radarów ze skanowaniem fazowym AN/SPG-59. Jednocześnie zadecydowano o rozpoczęciu prac nad kolejnym programem ASMS (*Advanced Surface Missile System*), który w 1969 roku został przemianowany na Aegis. Jego celem było opracowanie jednego systemu radiolokacyjnego, zdolnego do wykrywania i śledzenia celów powietrznych oraz do naprowadzania na nie własnych pocisków. Radar miałby ciągle śledzić wykryte cele, a nie odświeżać o nich informacji z częstotliwością zgodną z czasem obrotu anteny. Rozwiązanie takie pozwoliłoby na zwiększenie liczby jednocześnie zwalczanych celów bez potrzeby instalacji na okręcie coraz większej liczby urządzeń radiolokacyjnych do naprowadzania rakiet (obrazowo mówiąc: jeden duży radar zamiast kilku lub kilkunastu mniejszych).

Ciągły rozwój i zwiększanie możliwości bojowych systemu zaowocowało zdolnościami do zwalczania

szerokiej gamy celów nawodnych, podwodnych, lądowych i powietrznych. Najbardziej zaawansowane wersje systemu umożliwiają obecnie zwalczanie rakiet balistycznych i są wykorzystywane zarówno na platformach okrętowych, jak i lądowych (*Aegisashore*). Sercem systemu walki Aegis jest system zarządzania uzbrojeniem (*Aegis Weapon System* – AWS), w skład którego wchodzą systemy: radiolokacyjny AN/SPY-1, kierowania ogniem Mk 99, kontroli uzbrojenia (*Weapon Control System* – WCS) oraz pociski rakietowe rodziny Standard (SM-1/2/3). System Aegis jest zintegrowany z innymi pokładowymi systemami uzbrojenia i wyposażenia obejmującymi m.in. systemy artyleryjskie, walki radioelektronicznej czy też zwalczania okrętów podwodnych.

W bliskiej przyszłości przed systemem stoją problemy związane z integracją nowych systemów radiolokacyjnych (np. amerykański SPY-6) i systemów uzbrojenia (system laserowy *High Energy Laser with Integrated Optical-dazzler and Surveillance* – HELIOS). Dużym wyzwaniem na pewno będzie potrzeba dostosowania możliwości obronnych do nowego zagrożenia, jakim są przeciwokrętowe pociski hipersoniczne.

System Aegis jest kojarzony przede wszystkim z amerykańskimi krążownikami typu Ticonderoga i niszczycielami typu ArleighBurke. Oprócz nich został on także zaimplementowany na japońskich niszczycielach typu Kongi i Atago, na północnokoreańskich Sejong the Great (jednych z najlepiej uzbrojonych okrętów na świecie pod względem liczby przenoszonych pocisków rakietowych), australijskich typu Hobart oraz hiszpańskich fregatach Alvaro de Bazan i norweskich Fridtjof Nansen.

W niektórych opracowaniach można spotkać rozwinięcie słowa Aegis jako skrótowca od *Advanced Electronic GuidedInterceptor System* (zaawansowany system elektroniczny kierowanych pocisków przechwytujących). Rozwinięcie to jednak nie znajduje się w oficjalnym użytku, a nazwa Aegis jest wiązana z mitologiczną tarczą greckiego boga Zeusa (Egidą).

US Navy oprócz systemów walki Aegis wykorzystuje także system COMBATSS-21, zaimplementowany na modułowych jednostkach LCS (*Littoral Combat Ship*) typu Freedom. Nazwa systemu (*Component-Based Total-Ship System – 21st Century*) wskazuje, że ma to być okrętowy system walki XXI wieku. I są na to duże szanse, ponieważ COMBATSS-21 jest pochodną systemu Aegis i wykorzystuje tę samą bibliotekę danych (*Common Source Library* – CSL). Z pewnym uproszczeniem można stwierdzić, że jest to zubożona wersja systemu Aegis pod względem możliwości bojowych. Ale też i COMBATSS-21 nie jest implementowany na jednostkach przeznaczonych do strefowej obrony powietrznej czy też obrony przed rakietami balistycznymi. Producent obu systemów – firma Lockheed Martin – został wybrany na dostawcę systemu walki dla przyszłych amerykańskich fregat typu Constellation FFG-62 (fot. 5) – program FFG(X). Kolejne zamierzenie firmy jest związane z perspektywicznym programem budowy nowego typu niszczycieli rakietowych DDG(X).

SSDS

Starania Lockheed Martin są związane z zapowiedziami amerykańskich wojskowych o tym, że w przyszłości amerykańska marynarka wojenna chciałaby wykorzystywać na swoich okrętach jeden system walki. System korzystający z jednej biblioteki danych znacznie ułatwiłby jego modernizację. Według obrazowych wypowiedzi w zakresie instalacji i użytkowania działałby on podobnie jak system instalowany na smartfonach firmy Apple. Czyli bez konieczności instalowania dodatkowych komponentów (aplikacji) spoza wspólnej biblioteki. Obecnie konkurencją dla systemu Aegis jest *Ship Self-Defence System* (SSDS), wykorzystywany na lotniskowcach i okrętach desantowych. Z uwagi na możliwości bojowe i zastosowanie obu klas okrętów SSDS skupia się głównie na budowaniu świadomości sytuacyjnej wokół okrętu, samoobronie (w tym przed atakami przeciwokrętowych pocisków rakietowych) oraz kontroli działań lotnictwa.

Jedna z najnowszych wersji systemu została zaimplikowana na lotniskowcu USS „Gerald R. Ford" CVN-78. System wykorzystuje funkcję *Cooperative Engagement Capability* (CEC), pozwalającą na budowanie obrazu sytuacji powietrznej nie tylko z wykorzystaniem własnych radarów AN/SPY-3 i AN/SPY-4, lecz także innych, zewnętrznych źródeł. Zebrane w ten sposób dane są przetwarzane przez system i na ich podstawie zapada decyzja o użyciu systemów samoobrony obejmujących rakiety ESSM (*Evolved Sea Sparrow Missile*) i RAM (*Rolling Airframe Missile*).

Jako zewnętrzne źródło informacji SSDS może wykorzystywać dane z platform powietrznych. Po ich przetworzeniu informacja o sytuacji taktycznej może być rozpowszechniona wśród pozostałych okrętów wchodzących w skład grupy zadaniowej. W 2018 roku przeprowadzono zakończone sukcesem próby z użyciem samolotu F-35B i okrętu desantowego USS „Wasp". Wykorzystano w nich SSDS w wersji Mk2 zmodyfikowanej o dodanie systemu transmisji danych Link-16 DAC (*Digital Air Control*).

CMS 330

Wspomniane systemy Aegis i COMBATSS nie są jedynymi produktami firmy Lockheed Martin odnoszącymi się do okrętowych systemów walki. Kanadyjski oddział firmy (Lockheed Martin Canada) jest dostarczycielem systemu walki CMS 330, obecnego m.in. na pokładzie 12 kanadyjskich fregat typu Halifax. Okręty te w latach 2010–2018 poddano gruntownej modernizacji, w ramach której m.in. zaimple-

7.

Firma BAE Systems zamierza wprowadzić okrętowe systemy walki w nowy wymiar wirtualnej rzeczywistości.

BAE SYSTEMS

mentowano na nich system CMS 330, zastępując nim jego wcześniejszą wersję SHINPADS (*Shipboard Integrated Processing and Display System*). Cały program modernizacyjny kosztował około 4,1 mld dolarów, z czego modernizacja systemu walki pochłonęła kwotę około 2 mld dolarów. Obejmuje ona koszt nie tylko oprogramowania, lecz także zakupu i integracji nowych systemów uzbrojenia i wyposażenia (fot. 6).

CMS 330 zawiera pewne elementy szwedzkiego systemu 9LV w wersji Mk IV, jak chociażby radiolokacyjny i optoelektroniczny system kierowania ogniem Ceros 2000. Jest to zgodne z przyjętą filozofią organizacji systemu CMS 330, która zakłada zastosowanie technologii otwartej architektury. Pozwala to na integrację CMS 330 z innymi sprawdzonymi podsystemami, co finalnie zmniejsza ryzyko związane z rozwojem systemu i jego późniejszymi modernizacjami. Umożliwia również jego dostosowanie do specyficznych wymagań ewentualnego klienta.

Jako produkt kanadyjski system jest reklamowany jako niezależny od amerykańskich przepisów dotyczących międzynarodowego handlu bronią (*International Traffic in Arms Regulations* – ITAR). Rdzeń oprogramowania CMS 330 jest wykorzystywany do tworzenia sztucznego środowiska zaawansowanego szkolenia operatorów systemu (*Synthetic Environment Advanced Combat Operator Training System*). Dzięki temu szkolenie załóg odbywa się na takim samym oprogramowaniu, jakie występuje na okrętach, a nie na oprogramowaniu symulującym. Pozwala to na zmniejszenie kosztów użytkowania całego systemu i na wierne odtworzenie w ośrodku szkoleniowym nawet najbardziej złożonych sytuacji zagrożenia.

CMS 330 oprócz kanadyjskich jednostek typu Halifax jest zainstalowany także na nowozelandzkich fregatach typu ANZAC oraz na chilijskich fregatach Typu 23, modernizowanych do roli fregat obrony powietrznej. W najbliższej przyszłości pojawi się też na nowych kanadyjskich okrętach budowanych w ramach programu *Canadian Surface Combatant* według projektu brytyjskich fregat Typu 26.

INTeGEN

W wydaniu brytyjskim fregaty Typu 26 zostaną wyposażone w system walki INTeGEN, rozwijany przez firmę BAE Systems. Jego początki sięgają lat osiemdziesiątych ubiegłego wieku i przetargu na budowę nowego systemu walki dla atomowych okrętów podwodnych z rakietami balistycznymi typu Vanguard. Do tego okresu brytyjskie jednostki podwodne były wyposażane w systemy komputerowe opierające się na układach budowanych specjalnie dla wojska i dostarczanych przez formę Ferranti. Dzięki nowym zasadom obowiązującym w przetargu wygrało go konsorcjum Gresham-CAP, oferujące produkty komercyjne.

Dalsze prace doprowadziły do powstania systemu walki dla okrętów podwodnych (*Submarine Combat System* – SMCS). Jego najnowsza wersja SMCS-NG została do 2008 roku zaimplikowana na wszystkich brytyjskich jednostkach podwodnych. Jej cechą

YANDEX

8.

Terminale systemu walki Sigma na korwecie typu Stierieguszczij

wyróżniającą spośród innych systemów walki jest wykorzystanie środowiska systemu operacyjnego Windows firmy Microsoft. Z tego też względu SMCS-NG nosi przydomek *Windows for Warships*.

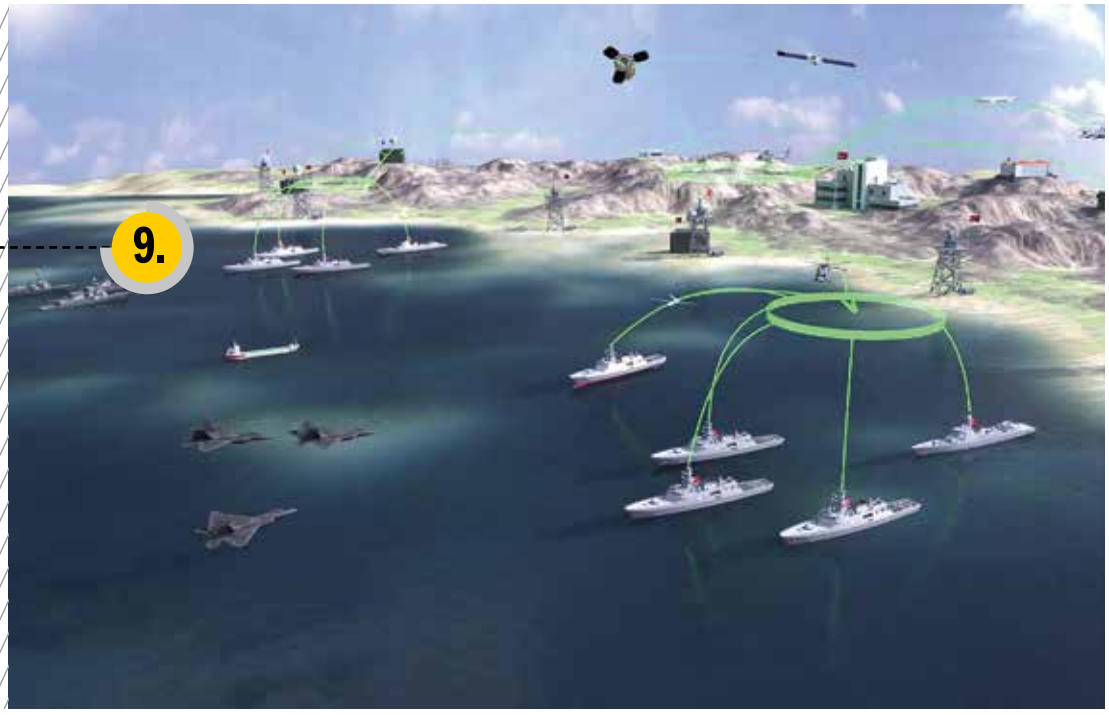
W wypadku brytyjskich okrętów nawodnych wydarzeniem przyspieszającym prace nad nowoczesnym systemem walki była wojna falklandzka i zatopienie HMS „Sheffield". Wnioski płynące z konfliktu wskazywały na potrzebę zmian w dotychczas używanych systemach, co doprowadziło do powstania *Surface-Ship Command System* (SSCS), który po raz pierwszy zaimplementowano na fregatach Typu 23. W niektórych źródłach system ten występuje pod nazwą DNA(2) i oprócz wspomnianych fregat znalazł zastosowanie także na brytyjskich jednostkach desantowych.

Po serii zmian własnościowych i fuzji w branży brytyjskich i europejskich firm zbrojeniowych prace nad kolejnym pokoleniem systemu walki dla brytyjskich jednostek przejęła firma BAE Systems. Pod jej egidą opracowano system walki CMS-1, który zaimplikowano na niszczycielach Typu 45, okrętach patrolowych typu River oraz na lotniskowcach typu Queen Elizabeth.

Nazwa najnowszego brytyjskiego systemu walki – INTeGEN – ma nawiązywać do jego możliwości w zakresie łączenia (*interconnecting, integrating*), interoperacyjności (*interoperable*) i potencjalnych zastosowań międzynarodowych (*international*). Jego zasadniczą częścią ma być system zarządzania walką INTeACT, którego nazwa ma odzwierciedlać jego aktywne i interaktywne zdolności (*active and interactive*). Prace nad nowym systemem odbywają się z wykorzystaniem dostępnych technologii zobrazowania, ale zamiarem firmy jest przeniesienie okrętowych systemów walki w nowy wymiar (fot. 7). W przyszłości zebrane dane mają być przetwarzane z pomocą sztucznej inteligencji i prezentowane na wielkoformatowych i trójwymiarowych ekranach. Interakcja z systemem ma się stać łatwiejsza i pełniejsza dzięki zastosowaniu urządzeń rozszerzonej rzeczywistości. Prace nad goglami tego typu już są prowadzone z wykorzystaniem nahełmowego wyświetlacza Striker II, opracowanego dla pilotów samolotów Typhoon.

BIUSY

W literaturze rosyjskojęzycznej systemy walki są określane jako bojowe systemy informacji i dowodzenia (*Bojewaja Informacionno-Uprawljajuszczaja Sistiema* – BIUS). Podobnie jak na Zachodzie, ich początki sięgają lat sześćdziesiątych ubiegłego wieku, chociaż prace nad zautomatyzowanymi systemami dowodzenia prowadzono w ZSRR już w latach pięćdziesiątych ubiegłego wieku. Pierwsze dwa pokolenia tych systemów charakteryzowały się dość niskim stopniem automatyzacji. Dopiero trzecie pokolenie, reprezentowane przez system Liesorub, zapewniało zadowalający stopień automatyzacji procesu dowodzenia okrętem. W system ten wyposażono ostatnie pokolenie radzieckich okrętów nawodnych, które służbę pełnią jeszcze dzisiaj. Należą do niego m.in. lotniskowiec „Admirał Kuzniecow" (projekt 11435), niszczyciele typu Udałoj (projekt 1155 i 11551) czy też krążowniki typu Kirow (pro-



9.

Turecki okrętowy system walki GENESIS ADVENT jest projektowany nie jako aplikacja dla pojedynczego okrętu, lecz jako system walki dla całych sił morskich.

HAVELSAN

10.

Dokonania skromne, ale nasze rodzime. I miejmy nadzieję, że z czasem ewoluują w coraz bardziej technologicznie zaawansowane projekty. Na razie jednak cieszmy się niszczycielami min z systemem walki Scot.

OBR CTM

jekt 11442). Czwarte pokolenie radzieckich okrętowych systemów walki jest reprezentowane przez system Tron zaimplikowany na fregacie „Nieustraszimyj" (projekt 1154). Podobnie jak i poprzednie pokolenie, system ten radził sobie dobrze w wypadku wsparcia dowodzenia pojedynczą jednostką, ale wykazywał niedostatki w zakresie współpracy w ramach grupy okrętów. Dlatego też do realizacji zadań w większym zespole miał służyć osobny system Diplomat. Z tego samego względu na lotniskowcu „Kuzniecow" oprócz systemu Liesorub zainstalowano system dowodzenia lotnictwem Tur i wymiany danych Trojnik.

Problem współdziałania z wykorzystaniem systemu walki w ramach grupy rozwiązano wraz z wprowadzeniem do użycia systemu walki Sigma (fot. 8). Jedną z jego pierwszych wersji zainstalowano na zakupionych przez Chiny niszczycielach typu Sowriemiennyj (projekt 956). Od tamtej pory Sigma stał się sztandarowym produktem rosyjskiego przemysłu i jest instalowany obecnie na większości wprowadzanych do służby okrętach rosyjskich. Wśród nich można wymienić przede wszystkim fregaty typu Admirał Gorszkow (projekt 22350) oraz korwety typu Stierieguszczij (projekt 20380/5/6) i uzbrojone w system rakietowy Kalibr korwety typu Karakurt (projekt 22800), a także najnowsze okręty patrolowe: modułowe typu Wasilij Bykow (projekt 22160) i arktyczne typu Iwan Papanin (projekt 23550).

Jak można wywnioskować z różnorodności zastosowań, system walki Sigma charakteryzuje się dużą elastycznością i zapewnia wsparcie dowodzenia przy wykonywaniu całej gamy zadań realizowanych przez współczesne okręty. System będzie także wspierać nowe okręty desantowe typu Iwan Gren (projekt 11711) i być może znajdzie się na pokładzie przyszłych rosyjskich okrętów szturmowych typu Iwan Rogow (projekt 23900). Jest to bardzo prawdopodobne, ponieważ system Sigma jest instalowany nawet na modernizowanych jednostkach rosyjskiej floty, wśród których wymienić można lotniskowiec „Admirał Kuzniecow" czy też atomowy krążownik „Admirał Nachimow". Tym samym stopniowo ze służby będzie wycofywany system Liesorub, a Sigma umocni swoją pozycję jako wiodący okrętowy system walki rosyjskiej marynarki wojennej.

Wiodący, ale nie jedyny, ponieważ rosyjskie fregaty typu Iwan Grigorowicz (projekt 11356P/M) są wyposażone w system walki Triebowanije. Oprócz trzech jednostek rosyjskich system znalazł zastosowanie na wybudowanych wcześniej fregatach typu Talwar (projekt 11356) dla marynarki wojennej Indii. W wyposażeniu rosyjskich sił morskich system ten znalazł się trochę przypadkiem i z konieczności. Triebowanije został opracowany prawdopodobnie głównie na potrzeby eksportowe. Dopiero problemy z budową fregat typu Gorszkow zmusiły Rosjan do wykorzystania sprawdzonego projektu 11356 do budowy jednostek dla własnych sił morskich. Zapewne by zaoszczędzić na czasie i na środkach finansowych, zdecydowano o zachowaniu oryginalnego systemu walki. Możliwe jednak, że w przyszłości przy okazji modernizacji fregaty typu Grigorowicz, tak jak i inne rosyjskie okręty, otrzymają Sigmę. Chociaż według informacji sprzed kilkunastu lat to właśnie system walki Triebowanije, a raczej jego rozwinięcie w postaci systemu Citadiel, miał się stać podstawowym okrętowym systemem walki rosyjskich sił morskich.

GENESİS

Z kolei dla tureckich sił morskich podstawowym okrętowym systemem walki staje się system GENESİS i jego pochodne. Prace nad nim rozpoczęto w Turcji pod koniec lat dziewięćdziesiątych w związku z potrzebą zwiększenia zdolności bojowych ośmiu fregat typu Gabya (czyli amerykańskich fregat typu OHP). Nazwę GENESİS można rozwinąć jako *Gemi Entegre Savaş Sistemi*, czyli zintegrowany okrętowy system walki. Przy pracach nad nim założono wykorzystanie w jak największym stopniu możliwości tureckich ośrodków naukowych i przemysłowych. System został w całości opracowany przez centrum badawcze tureckich sił morskich AMERKOM (Araştırma Merkezi Komutanlığı). Jako wykonawcę systemu i główny podmiot integrujący prace nad nim wybrano oczywiście turecką firmę Havelsan. System zapewnia zbieranie danych z dostępnych źródeł, ich obróbkę i dystrybucję, także na inne jednostki, ocenia również sytuację pod kątem zagrożenia. W wypadku zagrożenia z powietrza automatycznie proponuje wykorzystanie dostępnych systemów uzbrojenia. Oprócz fregat typu Gabya system zaimplikowano także na tureckich korwetach typu Ada.

Chociaż GENESİS jest określany jako system czysto turecki, to nie należy zapominać, że pierwszymi systemami walki wykorzystywanymi w tureckiej marynarce były STACOS na kutrach rakietowych typu Dogan i TACTICOS na fregatach typu Barbaros (MEKO-200). Zapewne opierając się na doświadczeniach zdobytych w trakcie ich wykorzystywania, zdecydowano się na opracowanie własnego systemu oznaczonego jako K-5 dla fregat typu Tepe, czyli amerykańskich fregat typu Knox w tureckiej służbie. Kolejnym krokiem był GENESİS, następnym będzie ADVENT. System ten jest obecnie testowany na najnowszej korwecie TCG Kınalıada typu Ada, a w przyszłości znajdzie się na okręcie desantowym (z funkcją lekkiego lotniskowca) TCG Anadolu i na modernizowanych fregatach typu Barbaros.

GENESİS ADVENT zostanie zaimplikowany również na czterech najnowszych fregatach typu Istambuł, z których pierwszą zwodowano w styczniu 2021 roku. Advent został zaprojektowany jako system modułowy o otwartej architekturze z funkcją *plug and play,* mającą uprościć przyszłe modernizacje i ułatwić instalację na kolejnych platformach (fot. 9). A mają to być zarówno okręty nawodne, jak i podwodne oraz platformy lądowe (zapewne w rozumieniu lądowych dowództw).

SCOMBA

Firma Lockheed Martin od lat współpracuje z hiszpańskim przemysłem stoczniowym (stocznia Navantia) i tak też będzie w wypadku czterech nowych fregat typu Bonifaz, których budowa rozpocznie się w 2023 roku. Według zapowiedzi Navanti otrzymają one okrętowy system walki SCOMBA (*Sistema de COMbate de los Buques de la Armada*) z radarami AN/SPY-7, z którymi współpracuje również Aegis. To nie jedyny element łączący systemy Aegis i SCOMBA, a wynikający z tej międzynarodowej współpracy. Przewidziana do instalacji na nowych fregatach wersja systemu SCOMBA ma wykorzystywać funkcje ciągłego śledzenia celów i oceny skutków ognia (*International Aegis Fire Control Loop* – IAFCL). Mniej zaawansowane wersje systemu SCOMBA zainstalowano obecnie na okręcie szturmowym „Juan Carlos I", okręcie zaopatrzeniowym „Cantabria" oraz na okrętach patrolowych typu Meteoro. W system ten mają zostać wyposażone także hiszpańskie okręty podwodne typu S80.

SENIT I SETIS

Początki francuskich systemów walki także sięgają lat sześćdziesiątych. Wtedy też do służby wprowadzono dwa niszczyciele obrony powietrznej typu

Suffren wyposażone w pierwszą wersję systemu SENIT (*Systèmed'Exploitation Navale des Informations Tactiques*). Poziom funkcjonalności zbliżony do poziomu obecnych systemów walki osiągnięto 20 lat później – przy wprowadzaniu do służby kolejnych jednostek obrony powietrznej oraz niszczycieli typu Cassard wyposażonych w system SENIT 6. W 2001 roku do służby wszedł lotniskowiec „Charles de Gaulle" z systemem SENIT 8, w którym zastosowano komercyjne rozwiązania sprzętowe. Pozwoliło to nie tylko zmniejszyć koszty, lecz także zwiększyć moc obliczeniową całego systemu. Jednym z ostatnich zastosowań systemu SENIT stały się norweskie jednostki typu Skjold z systemem SENIT 2000.

Podążając z duchem zmian technologicznych i operacyjnych, firma DCNS (obecnie Naval Group) opracowała system SETIS. Punktem wyjściowym dla nowego systemu był francusko-włoski program budowy fregat typu FREMM. Powstałe w jego ramach jednostki francuskie otrzymały nowy system walki, który później wprowadzono także na korwetach typu Gowind. System zapewnia realizację szerokiego spektrum zadań stawianych przed francuskimi okrętami, wliczając w to także zdolność do niszczenia celów naziemnych z użyciem pocisków manewrujących. W najbardziej rozbudowanej wersji system wspiera również działania w zakresie obrony przed rakietami balistycznymi. Prawdopodobnie taka wersja systemu zostanie zainstalowana na francuskich fregatach FREMM (typ Aquitaine) w wersji jednostek obrony powietrznej (podtyp Alsace).

W wypadku jednostek FREMM i Gowind, budowanych w celach eksportowych i zakupionych przez Maroko, Egipt i Malezję, funkcjonalność systemu została zapewne dopasowana do wymagań i możliwości finansowych kupującego.

ATHENA

Okrętowe systemy walki są określane w języku włoskim jako SADOC (*Sistema Automatico per la Direzionedelle Operazioni di Combattimento*). Pochodzące z lat osiemdziesiątych i dziewięćdziesiątych, ale wciąż znajdujące się w służbie jednostki włoskie, są wyposażone w SADOC Mk 2, nazywany też SADOC 2. Wybudowane już w XXI wieku niszczyciele rakietowe Horizon oraz włoskie fregaty FREMM (typ Bergamini) wyposażono w nowszy system SADOC Mk 3 ATHENA. Zmiana jednej cyfry sugerowałaby, że jest to po prostu kolejna wersja tego samego systemu walki, dostosowana do kolejnych jednostek. Ale byłaby to mylna sugestia. ATHENA (*Architecture & Technologies Handling Electronic Naval Applications*) korzysta oczywiście z doświadczeń płynących z eksploatacji SADOC Mk 2 nie tylko we włoskiej marynarce, lecz także u zagranicznych kontrahentów kupujących włoskie jednostki. Pod innymi względami jest to jednak całkowicie nowy system walki z cechami funkcjonalnymi wynikającymi z dobrej praktyki morskiej. Liczba terminali systemu wynika z charakteru zadań realizowanych przez daną jednostkę. W wypadku fregat typu Bergamini jest ich 16, a na budowanym jeszcze okręcie szturmowym (lekkim lotniskowcu) Trieste będzie ich 40. Zazwyczaj jednak nie wszystkie są wykorzystywane, ponieważ nie ma takiej potrzeby. Dla znajdujących się w służbie okrętów 70% czasu upływa na prowadzeniu działań w warunkach braku zagrożenia lub z małym prawdopodobieństwem jego wystąpienia. Do takich działań potrzebnych jest siedem konsol. Reszta terminali nie musi nawet znajdować się w tym samym pomieszczeniu. Filozofia ta znajdzie odzwierciedlenie w wyposażeniu nowych włoskich okrętów budowanych w ramach programu wielozadaniowego okrętu patrolowego PPA (*Pattugliatore Polivalented'Altura*).

Jednostki powstałe w ramach PPA otrzymają od 12 do 16 terminali, w zależności od przeznaczenia oraz stopnia wyposażenia w systemy elektroniczne i uzbrojenia (od okrętu patrolowego do wielozadaniowej fregaty). Liczba aktywnych konsol będzie zależeć od trybu pracy systemu walki (szkolenie, obrona, walka) i związanego z tym stopnia zagrożenia.

W przyszłości ATHENA będzie wykorzystywać elementy sztucznej inteligencji (SI). W początkowym okresie SI znajdzie zastosowanie do szkolenia w podsystemach symulujących przyszłe środowisko działań. Kolejnym krokiem ma być zatrudnienie sztucznej inteligencji do analizy danych spływających do systemu, a w dalszej perspektywie ma ona stać się narzędziem wspomagającym proces planowania działań.

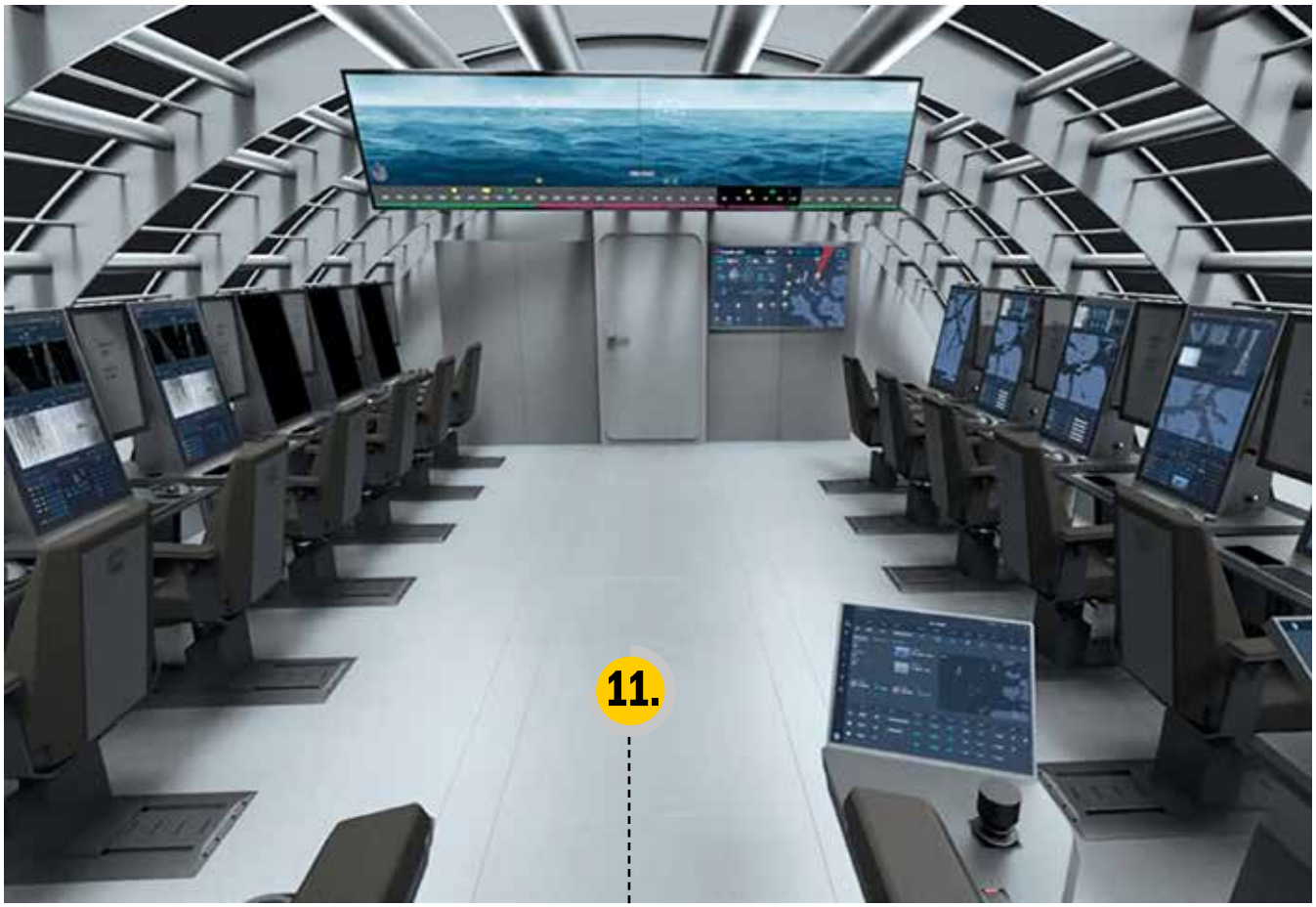
SCOT

Na tle światowych potentatów dokonania polskiej myśli w dziedzinie okrętowych systemów walki nie wyglądają zbyt okazale. Niemniej możemy się pochwalić opracowaniem takiego produktu i wdrożeniem w życie w postaci systemu Scot. System ten powstał w gdyńskim Centrum Techniki Morskiej z myślą o niszczycielach min typu Kormoran. Do tej pory w pełni zaimplementowano go na prototypowej jednostce ORP „Kormoran". Doświadczenia płynące z jego eksploatacji wykorzystano przy budowie i wyposażaniu kolejnych dwóch jednostek: ORP „Mewa" i ORP „Albatros"

Zadaniem systemu jest wspomaganie załogi okrętu w zakresie wykorzystania okrętowych sensorów i efektorów oraz planowanie działań i kontrola stopnia ich realizacji. System zaprojektowano tak, by w przyszłości można było zainstalować go na innych klasach jednostek, w tym m.in. na okręcie projektu Ratownik, a także na okrętach wyposażonych w broń rakietową (fot. 10).

WNIOSKI

Okrętowe systemy walki stają się podstawowym składnikiem każdego współczesnego okrętu, zarówno bojowego, jak i pomocniczej jednostki pływają-



ATLAS ELEKTRONIK

W dyskusjach na temat możliwości bojowych okrętów, liczby przenoszonych torped i rakiet lub rodzaju ich napędu pomija się jakoś jeden z najważniejszych tematów. Temat okrętowego systemu walki faktycznie decydującego o pełnym wykorzystaniu dostępnych możliwości. Na zdjęciu zobrazowanie przedstawiające terminale systemu ORCCA – systemu walki dla konwencjonalnych okrętów podwodnych.

cej. Dotyczy to jednostek nowo budowanych oraz starszych, poddawanych modernizacjom mającym na celu zwiększenie ich możliwości bojowych. W przyszłości każdy okręt wraz ze swoim systemem walki będzie jednym z elementów szerszego, sieciocentrycznego systemu. Sieciocentrycznego, czyli takiego, w którym o sukcesie będzie decydować zdolność do wymiany informacji. W każdym wymiarze: wewnątrz pojedynczego okrętu, w ramach grupy zadaniowej, w siłach morskich i w całych siłach zbrojnych.

W naszym kraju od lat toczy się dyskusja towarzysząca planom zakupów nowych okrętów. W wypadku np. jednostek podwodnych skupia się ona na takich zagadnieniach, jak: posiadanie zdolności do użycia pocisków manewrujących czy też rodzaj napędu: spalinowo-elektryczny, czy niezależny od powietrza atmosferycznego? A może dyskusja powinna się skupić na tym, jaki system walki zostanie zaimplementowany na nowych jednostkach? Rakiety można przystosować do strzelania z wykorzystaniem okrętowych wyrzutni torped, a napęd można wstawić w postaci modułu rozcinając okręt. Może się to wydawać kosztowne, ale kosztowny jest dopiero zakup oprogramowania integrującego wszystkie elementy w jeden organizm (fot. 11).

Systemy walki są przykładem, który potwierdza założenie, że w przyszłości o możliwościach bojowych będzie decydować oprogramowanie. Podobnie jak i przy wykorzystywanych na co dzień smartfonach, o sukcesie danej marki nie decydują już tylko parametry sprzętu, lecz software – oprogramowanie. Musi ono nie tylko zapewniać sprawne działanie urządzenia, lecz także być przyjazne dla użytkownika. Oczywiście, wiążą się z tym pewne potrzeby i wymagania. Oprogramowanie musi być ciągle aktualizowane, aby eliminować ukryte w nim błędy, stwarzać nowe funkcjonalności lub rozszerzać stare i dbać o bezpieczeństwo całego systemu. Dlatego warto inwestować w oprogramowanie i dbać o rozwój instytucji zajmujących się jego tworzeniem. Doświadczenie nie jest towarem, który łatwo kupić. I nie jest nawet ważne, czy oprogramowanie jest tworzone dla wojsk lądowych, sił powietrznych lub też dla marynarki. Przecież czasem wystarczy zmienić kilka linijek kodu. ■

Awionika **teraz i jutro**

SYSTEMY ELEKTRONICZNE PRZEZNACZONE DO STEROWANIA, NAWIGACJI, POZYSKIWANIA I PRZETWARZANIA DANYCH, DO SAMOOBRONY ITP. ODGRYWAJĄ WSPÓŁCZEŚNIE DECYDUJĄCĄ ROLĘ W KONSTRUKCJI SAMOLOTU LUB ŚMIGŁOWCA.

Systemy awioniczne zamontowane w kokpicie wielozadaniowej maszyny F-35 Lightning II reprezentują najbardziej zaawansowane środowisko pracy pilota samolotu bojowego.

USAF

dr inż. Marek Dąbrowski

Autor jest publicystą zajmującym się tematyką militarną.

Chociaż postęp techniczny jest niezwykle istotny, człowiek jest skłonny niczego nie zmieniać w tradycyjnych obszarach funkcjonowania znanych mu od lat i powszechnie akceptowanych. Są jednak strefy naszego życia, w których jesteśmy w stanie pogodzić wypróbowane metody działania z pewnymi ich modyfikacjami (np. związane z nowoczesną technologią) oraz takie, w których wolimy pozostać w tzw. spoczynku rozwojowym. Należy jednak pamiętać, że w przypadku obszaru czysto militarnego takie postępowanie może mieć poważne konsekwencje, a finalnie nawet powodować straty. Współczesne rozwiązania technologiczne są bowiem jednym z czynników (obok na przykład taktyki czy wyszkolenia) wypływających zasadniczo na efektywność prowadzonej walki. Dotyczy to zwłaszcza lotnictwa, przede wszystkim w kontekście osiągania zupełnie nowych możliwości przez ten rodzaj wojsk. Nawet głęboko zakorzenieni w tradycji lotniczej piloci i konstruktorzy zdają sobie sprawę z konieczności wprowadzania zmian tak, by sprostać wymaganiom przyszłego pola walki. Nowe technologie wpływają na wykonywanie wszelkiego rodzaju misji bojowych przez pilotów oraz wymuszają korzystanie przez nich z bardziej zaawansowanego uzbrojenia czy systemów wsparcia działań powietrznych.

ZARYS ROZWOJU

Udoskonalaniu konstrukcji lotniczych tak naprawdę towarzyszy niemal równoczesny rozwój sposobów praktycznego sterowania nimi w powietrzu. Pilot od zawsze zajmował tu szczególne miejsce, a maszyna musiała być mu w pełni posłuszna, zarazem dla niego bezpieczna. Kabiny stawały się ergonomiczniejsze, wyposażane w coraz doskonalsze instrumenty pilotażowe, wskaźniki, układy sterowania, systemy wymiany danych czy prowadzenia rozpoznania. Ich odpowiednie umieszczenie ułatwiało prawidłową ocenę sytuacji wokół samolotu, w tym pod nim. Sprzyjało też większej efektywności pracy pilotów oraz ułatwiało wykonywanie przez nich zadań w powietrzu. Z czasem montowane na pokładach środki łączności pozwalały na przekazywanie informacji nie tylko z rozpoznania wzrokowego, lecz umożliwiały także pozyskiwanie danych z naziemnych systemów dowodzenia. Przy tym i sam radiolokator zapewniał wgląd w sytuację na większym dystansie.

Wprowadzanie do przenoszonego uzbrojenia różnej klasy pocisków rakietowych znacznie zwiększyło możliwości prowadzenia walk powietrznych oraz zwalczania celów naziemnych i nawodnych z coraz większej odległości. Przyczyniło się ponadto do zwiększenia bezpieczeństwa maszyn i obsługujących je załóg oraz pozwoliło na wykonywanie ataków nie tylko z przedniej półsfery. Trzeba przy tym pamiętać, że parametry pocisków rakietowych, takie jak zasięg, precyzja uderzenia, zwrotność czy odporność na zakłócenia są coraz lepsze, jednak tak naprawdę wciąż

USAF

F-35 – wielkoformatowy wyświetlacz LAD (*large display screen*) zapewniający duży obszar wizualizacji do prezentacji informacji o locie i danych taktycznych

o ich użyciu decyduje pilot. Nawet w przypadku pierwszych generacji takich systemów pilot często musiał naprowadzać samolot w pobliże celu. Również i dziś nierzadko musi go podświetlać. Zatem jego umiejętności miały i nadal mają kluczowe znaczenie dla precyzyjnego rażenia celu bombami lub rakietami.

Nawet obecnie stosowanych rakiet nie można nazwać inteligentnymi. Co prawda na podstawie pozyskiwanych danych mogą one, na przykład, wykonywać samodzielnie manewry, ale nie jest to działanie wymuszone zmianami w otoczeniu, w którym działają, możliwymi dla pilota do przewidzenia. Układ ich sterowania ma z góry określony algorytm działania, a nie swobodę podejmowania decyzji w odpowiedzi na sytuację powietrzną lub na polu walki. Nie może zatem samodzielnie rozwiązywać problemów napotkanych na drodze, po której zmierza rakieta do celu.

Istotnym skokiem było wprowadzenie wskaźnika przeziernego *HUD* (*Head-Up Display*) zastępującego celowniki refleksyjne i żyroskopowe czy też umożliwienie pilotowi sterowania samolotem i obsługiwania uzbrojenia bez odrywania rąk od drążka sterowego w postaci *HOTAS* (*Hands On Stick and Throttle*). Pilot nie musiał już przenosić często wzroku z otoczenia wokół maszyny na przyrządy pokładowe, bo te najistotniejsze informacje miał tuż przed sobą w zasięgu wzroku.

Wielofunkcyjne wskaźniki (wyświetlacze) MFD (*multi-function displays*) znacząco poprawiły świadomość sytuacyjną, skróciły czas reakcji na powstałe zagrożenie oraz ułatwiły wypracowanie na nie odpowiedzi. Umożliwiły takie manewrowanie daną platformą powietrzną, by zająć idealne miejsce do wykonania precyzyjnego ataku.

Do naprowadzania kierowanych pocisków klasy powietrze–powietrze czy powietrze–ziemia wykorzystywano wspomniane już radiolokatory, z czasem także pasywne głowice optoelektroniczne. Wprowadzono również interfejsy z szerokim polem widzenia (wymuszające zwiększony ruch gałek ocznych) oraz systemy celownicze montowane na hełmie pilota, które śledziły linię jego wzroku.

IDZIE NOWE

Obecnie można stwierdzić, że systemy awioniczne zamontowane w kokpicie wielozadaniowej maszyny F-35 Lightning II reprezentują najbardziej zaawansowane środowisko pracy pilota samolotu bojowego. Jest to pierwszy typ platformy powietrznej, która wykorzystuje jeden wielkoformatowy wyświetlacz LAD (*large display screen*) zapewniający duży obszar wizualizacji do prezentacji informacji o locie i danych taktycznych (fot.). Ten wyświetlacz to pierwszy krok w kierunku odejścia od tradycyjnych kilku mniejszych (tzw. *glass cockpit*), na których oddzielnie przedstawiano określone dane. Oczywiście uzupełnieniem jest wyświetlacz montowany na hełmie pilota oraz sieć systemów rozproszonej apertury DAS (*distributed aperture systems*). To wszystko zapewnia pełną widoczność w strefie 360º wokół samolotu, nawet w gorszych warunkach atmosferycznych panujących w obszarze wykonywania planowanych zadań.

Wspólny nahełmowy system celowniczy dla F-35 opracowało konsorcjum VSI (Vision Systems International), czyli joint venture Rockwell Collinsa i Elbitu. Z kolei JHMCS (*Joint Helmet-Mounted Cueing System*) bazuje na DASH III oraz Agile Eye i wyświetla monochromatyczny obraz rzutowany na wizjer hełmu na wysokości prawego oka pilota. Wykorzystuje czujniki elektromagnetyczne do ustalania pozycji jego głowy.

W nowym zintegrowanym JHMCS II zastosowano optyczno-inercyjny system ustalania pozycji głowy pilota oraz interfejs przekaźnikowy ACIU (*Aircraft Interface Unit*). Ma on mniejszą masę, w pełni kolorową symbolikę i jest kompatybilny z goglami noktowizyjnymi. Nawet starsze samoloty mogą uzyskać zupełnie nowe możliwości dzięki dostosowaniu ich awioniki do nowoczesnych rozwiązań. Tak jest na przykład w przypadku wielozadaniowej maszyny F-16. W jej najnowszej wersji F-16V zastosowano na kolumnie środkowej tablicy przyrządów duży wielkoformatowy centralny wyświetlacz CPD (*central pedestal display*), a oryginalne trzy komputery zostały zastąpione przez jeden modułowy komputer misji MMC (*Modular Mission Computer*). MMC ma dziesięć razy większą pojemność pamięci i dwa razy większą moc obliczeniową oraz zapewnia lepszą integrację systemów czy też możliwość pokazania większej licz-

by potrzebnych w danej chwili danych. CPD o wymiarach 6x8 cali i wysokiej rozdzielczości obrazu pozwala na wyświetlanie mapy nawigacyjnej lub danych o sytuacji taktycznej z większą szczegółowością oraz w większym formacie niż to zapewniał dotychczasowy ekran o wymiarach 4x4 cale. Obszar wyświetlania można podzielić na dwa mniejsze o wymiarach 6x6 i 2x6 cali.

Z kolei koncern Boeing dla śmigłowców AH-64E proponuje wyświetlacze LAAD (*Large Area Avionics Display*) o wymiarach 11x19 lub 8x20 cali. Duży wyświetlacz ciekłokrystaliczny przewidywany dla V-280 *Valor* będzie się składać z niewielkich modułów (tak by pojedyncze uszkodzenie nie wyłączyło całego urządzenia).

Natomiast BAE Systems pracuje nad koncepcją wykorzystania rzeczywistości rozszerzonej (*augmented reality* – AR) do utworzenia w pełni funkcjonalnych wirtualnych wyświetlaczy, zastępujących dotychczas stosowane, oraz różnych przycisków i manipulatorów. AR w formie półprzezroczystej kopuły wyświetlałaby obiekty wirtualne na żywo, zapewniając przy tym efekt dźwięku 3D i komunikację głosową oraz środki do dotykowego sprzężenia zwrotnego. To już zupełna nowość znana dotychczas jedynie z filmów lub powieści *science fiction*. Dzięki takiemu rozwiązaniu oraz zastosowaniu elementów sztucznej inteligencji do sterowania samolotem rola pilota nie będzie się ograniczać do tej funkcji, lecz sprowadzać do nadzorowania obszaru prowadzonej walki, w tym dowodzenia bojowymi BSP (koncepcja: lojalny skrzydłowy).

Inne pomysły polegają na zastosowaniu metod nadzoru z wykorzystaniem oka jako elementu technologii śledzenia. Ponadto na wprowadzeniu kontroli neuronowej oraz czujników fizyko- i psychometrycznych do ciągłego monitorowania zdrowia pilota i jego zdolności psychofizycznych. I tak w sytuacji gdy pilot samolotu lub śmigłowca nie reaguje na ważne dane lub informacje o przeciwniku lub gdy, na przykład, traci przytomność w wyniku oddziaływania na niego dużego przeciążenia czy w warunkach niskiego poziomu dostarczanego mu tlenu, komputer misji czy autopilot automatycznie przejmują kontrolę nad maszyną, by wyprowadzić ją i człowieka z krytycznej sytuacji. Taka koncepcja pojawiła się w zasadzie po raz pierwszy w brytyjskim samolocie bojowym kolejnej generacji Tempest.

Ta maszyna przyszłości dzięki właściwości określanej jako *Cooperative Engagement Capability* będzie pozyskiwać dane z innych powietrznych i naziemnych lub morskich platform oraz zachowa możliwość przejęcia kontroli nad ich systemami ogniowymi. Wymagać to będzie tworzenia zintegrowanego obszaru prowadzonych działań na podstawie własnych danych oraz tych pozyskiwanych z innych platform (satelity, BSP, rozpoznanie, stanowiska dowodzenia itp.).

Z kolei dla pilotów śmigłowców opracowano ANVIS (*Aviator Night Vision Systems*), który we współpracy z wyświetlaczem nahełmowym HMD (*Helmet Mounted Displays*) zapewni im wektorową symbolikę grafiki i raster obrazu. Widok w warunkach nocnych wspomaga FLIR (*Forward Looking Infrared*).

Dzięki rozwojowi wyświetlaczy LCD, LCOS i 3LCD oraz DLP generowany przez diody LED lub elektroluminescencyjne OLED obraz może być wyświetlany w dużej rozdzielczości i sprzężeniu z HMD zasobników celowniczych oraz głowic optoelektronicznych.

Takie urządzenie jak ANVIS staje się szczególnie przydatne w krytycznych obszarach określanych jako DVE (*degraded visual environments*), w których wykonują misje załogi śmigłowców, na przykład lądujące w terenie pustynnym lub zaśnieżonym. W takich warunkach gęsty pył lub chmura śniegu blokują pilotowi pole widzenia, szczególnie w pobliżu ziemi, czyli w najtrudniejszym krytycznym momencie lądowania. ANVIS ma to zmienić i znacznie poprawić komfort pracy pilota i załogi.

Innym krytycznym czynnikiem dla załóg śmigłowców jest gęsty dym, wobec czego opracowano system BRITENITE zapewniający bardzo szerokie pole widzenia z matrycą czujników termowizyjnych dostarczających wyraźny obraz obszaru zniekształconego na przykład przy lądowaniu. Czujniki odgrywają rolę urządzeń ostrzegających o powstałym zagrożeniu, a wspierać je może DAS ze współpracujących ze śmigłowcami maszyn F-35.

Pilotage Distributed Aperture Sensor (PDAS) to modułowa zintegrowana sieć obejmująca czujniki podczerwieni, sprzęt (wyświetlacze załóg) i oprogramowanie (*open-architcture procesor* – OPA), tak aby zapewnić pilotom i załodze 360-stopniową strefę orientacji sytuacyjnej wokół maszyny. PDAS zapewnia w czasie rzeczywistym zobrazowanie o wysokiej rozdzielczości, sprzężone z HMD pilotów. Ponadto umożliwia załodze śmigłowca skanowanie obszaru przed desantowaniem, koordynowanie działań strzelców pokładowych, zarządzanie zewnętrznym systemem wyciągarki oraz przenoszeniem ładunku.

Z kolei ALIAS (*Aircrew Labour In-Cockpit Automation System*) nadzoruje wykonanie całej misji – od momentu startu do lądowania, nawet wówczas, gdy wystąpią nieprzewidywane zdarzenia, takie jak na przykład awarie poszczególnych systemów maszyny. Wówczas ALIAS monitoruje ich stan i automatycznie wprowadza nowe procedury związane z lotem. Ten inteligentny modułowy system automatyzacji pracy w kokpicie jest dostosowany do zabudowy w różnego rodzaju statkach powietrznych, zapewniając wysoki poziom automatyzacji procesu lotu, m.in. wykonywanie misji przy zmniejszonej liczebnie załodze.

Samo pole walki jest stale monitorowane i mapowane przez różnego rodzaju czujniki, radiolokatory i systemy identyfikacji (IFF). Dlatego w przyszłych (wspomnianych już) maszynach V-280 zastosowano omówiony system PDAS. Składa się on z sześciu

czujników podczerwieni rozmieszczonych wokół płatowca, przekazujących dane do HMD załóg oraz na wyświetlacze w kokpicie przez procesor o otwartej architekturze (OAP). Chociaż obecnie system obsługuje porty dla dwóch użytkowników (członków załogi), ostatecznie powinien pełnić swoje funkcje nawet dla sześciu osób. Umożliwi to zobrazowanie środowiska dzięki całemu spektrum pozyskanych i napływających informacji oraz związanych z nimi zagrożeń. Kolejne jego modyfikacje będą zmierzać do integracji z multimodalnym połączeniem czujnika MMSF

RSPACE (*Resilient Synchronized Planning and Assessment for the Contested Environment*) ma na celu stworzenie możliwości planowania rozproszonego dla zapewnienia niezawodnego dowodzenia i kontroli (C2) oraz zarządzania operacjami, nawet gdy komunikacja jest ograniczona i zawodna. RSPACE opracowuje ukierunkowane na człowieka oprogramowanie wspomagające podejmowanie decyzji, które z uwzględnieniem intencji dowódcy pomoże innym uczestnikom walki w obszarze C2 kontrolować jej prowadzenie, komponując pakiety misji (w razie po-

SAMOLOT PRZYSZŁOŚCI TO NIE BĘDZIE COŚ W RODZAJU CENTRUM DOWODZENIA

(*Multi-Modal Sensor Fusion*) z wieloma innymi, co pomaga przywrócić świadomość sytuacyjną załodze w DVE i umożliwia pozycjonowanie w obszarach, w których zanika sygnał lub brakuje sygnału z nawigacji satelitarnej.

Nowoczesne rozwiązania HMD wspomagają pilota szczególnie dzięki technice *off boresight* (zapewnienie obrazu celu nieznajdującego się bezpośrednio przed pilotowaną maszyną). Informacje są wyświetlane w wizjerze hełmu w postaci symboli zawsze znajdujących się w polu widzenia pilota. Nie musi on już manewrować całym statkiem powietrznym i utrzymywać przeciwnika w celowniku HUD przed odpaleniem pocisków rakietowych (szczególnie tych manewrowych typu HOBS – *High Off-Boresight*) i w trakcie ich odpalania. Oglądany obraz jest dostarczany przez różne sensory w czasie rzeczywistym, a technologia *obrazu w obrazie* pozwala na otwieranie nowych okien zadaniowych.

Świadomość sytuacyjna (*situation awareness* – SA) to podstawowy i najbardziej krytyczny aspekt związany z wykonywaniem działań w powietrzu. Od niej zależy efektywność działania pilota i jego maszyny. Niezbędne dane każda współczesna bojowa platforma powietrzna pozyskuje samodzielnie oraz od innych załogowych lub bezzałogowych platform rozmieszczonych w pewnej odległości od obszaru prowadzonej walki lub działających w jego otoczeniu. Wybrany samolot otrzymuje te sekwencje, które bezpośrednio go dotyczą. Na nich są zobrazowane dane zarówno o własnych systemach walki, jak i przeciwnika, tych zidentyfikowanych lub nie (mogących zagrozić powodzeniu misji). Informacje są na bieżąco wzbogacane o nowe dane pozyskiwane z własnych sensorów, umożliwiając pilotom (lub całej załodze) szybką reakcję na zmieniające się warunki walki. Chodzi tu nie tylko o wykonanie ataku, lecz także o ochronę maszyny (prowadzenie walki radioelektronicznej czy na przykład uwalnianie flar i dipoli).

trzeby koordynowane przez sieć), reagować na pojawiające się nowe możliwości oraz dokonywać oceny postępów w osiąganiu określonego celu działania. RSPACE koncentruje się na poziomie operacyjnym w dziedzinie prowadzenia operacji lotniczych.

Jego elementem składowym jest DIRECT (*Distributed, Interactive Command-and-Control Tool*) przeznaczony do poprawy świadomości w przestrzeni powietrznej. Do jego generowania jest wykorzystywany interfejs zobrazowujący zaistniałe zdarzenia w czasie rzeczywistym z przeznaczeniem do oceny obszarów budzących obawy podczas planowania i realizacji misji. Oprogramowanie to automatycznie dostosowuje się do zmian zachodzących w trakcie wykonywania zadań, ułatwia przepływ danych, ustala priorytety oraz efektywnie współpracuje z człowiekiem.

MYŚLĄCE PLATFORMY

Technika lotnicza, podobnie jak i inne obszary zastosowania militarnego, w coraz większym stopniu korzysta ze sztucznej inteligencji (*artificial intelligence* – AI) i uczenia maszynowego (*machine learning* – ML), głównie do analizy napływających danych i ich selekcji oraz opracowania optymalnych sposobów realizacji zadań stawianych przed pojedynczymi maszynami czy zespołami zadaniowymi. Ale nie tylko.

Początkowo eksploatowany sprzęt elektryczny i elektroniczny składający się na awionikę danego typu platformy powietrznej oraz zdolności przetwarzania przez nią pozyskiwanych danych nie wystarczał do zintegrowanego prezentowania wszystkich potrzebnych pilotowi informacji. Potrzebne było zastosowanie kilku wskaźników (wyświetlaczy) oraz nadal dublujących się niektórych analogowych czujników. Scalenie tych wszystkich informacji w pojedynczy obraz sytuacji było wstępnie niemożliwe, co z czasem wymusiło, że w maszynie bojowej oprócz pilota zasiadał również operator systemów walki.

Magistrale danych i architektura cyfrowa umożliwiły wprowadzenie wyświetlaczy sytuacyjnych, które

przedstawiały już pełny plan misji bojowej. Jednak nadal zarządzanie poszczególnymi czujnikami wymagało od pilotów tzw. przewijania wielu stron, by efektywnie wykonać określone zadanie. Ponadto samo śledzenie obrazu celu na małym wyświetlaczu nie było łatwe, zwłaszcza gdy sytuacja w powietrzu rozwijała się dynamicznie, a samolot przemieszczał się z dużą prędkością i jednocześnie napływały do pilota nowe informacje.

Dlatego tak ważne było zastosowanie wspomnianych już wyświetlaczy typu LAD, w które obecnie są wyposażone takie maszyny, jak najnowsze warianty F-16V, F-15X, Gripen E i F-18 E/F. Na LAD są wyświetlane tylko te informacje, które są niezbędne pilotowi w określonym czasie realizowanej misji, co zmniejsza jego obciążenie pracą oraz w zasadzie może zredukować załogę do jednej osoby. LAD ułatwia planowanie, ocenę sytuacji i zarządzanie informacjami, a w połączeniu z wyświetlaczem na hełmie zapewnia zdolność do pokazywania danych w skoordynowanym widoku na linii wzroku pilota.

Ale to nie wszystko. W kolejnych projektach przewiduje się zastosowanie nowych kanałów sensorycznych, takich jak funkcje 3D dźwięku i dotyku. Skuteczność dźwięku 3D w dużym stopniu zależy od zdolności pilota do rozróżniania kierunków, z których on pochodzi. Takie sygnały przestrzenne są przetwarzane przez mózg bez większego wysiłku, ale sprawa komplikuje się wówczas, gdy zbyt wiele napływa ich w tym samym czasie. Wobec tego dźwięk 3D może być stosowany tylko w razie przekazywania informacji krytycznych. Z kolei za pomocą dotyku można nadzorować wiele systemów jednocześnie. Jest to działanie intuicyjne i możliwe nawet w warunkach stresu czy dużego obciążenia zadaniami.

Wyświetlacz umieszczony blisko oka nakłada wirtualne obiekty cyfrowe na rzeczywiste obrazy nieba lub ziemi. Te wirtualne to zazwyczaj punkty nawigacyjne, obiekty dynamiczne (np. własne samoloty i przeciwnika) czy przeszkody (np. anteny, przewody itp.). Ma to na celu przedstawienie rozpoznanych niebezpieczeństw w czasie rzeczywistym.

Firma Elbit Systems opracowała system Supervision z przeznaczeniem do prezentacji danych załodze w sposób intuicyjny, redukujący jej obciążenie i poprawiający sprawność pilotażu. Informacje o przeszkodach terenowych, o zagrożeniach w powietrzu, a także zalecenia dotyczące kierunku lotu są nakładane na rzeczywisty obraz, w tym ten pochodzący z kamer noktowizyjnych i termowizyjnych.

System ALPHA dąży natomiast do zmniejszenia prawdopodobieństwa popełnienia błędów przez pilota, a to głównie dzięki dużej szybkości przetwarzania danych. Tzw. wirtualny drugi pilot działający w tym systemie może pobierać pełne dane ze wszystkich sensorów, porządkować je oraz tworzyć scenariusze przyszłych działań nawet dla czterech maszyn działających we wspólnej formacji. Może to być szczególnie przydatne w realizacji idei tzw. lojalnych skrzydłowych, czyli bojowych BSP kolejnej generacji współpracujących z platformami załogowymi.

POJEDYNCZA MASZYNA BOJOWA, LECZ DZIAŁANIAMI W POWIETRZU W MAŁEJ SKALI

Takie systemy byłyby w stanie polepszyć świadomość sytuacyjną, odpowiadać na określone reakcje, wybierać sposób walki, zarządzać użyciem uzbrojenia itp. Ponadto zastosowana w nich AI pozwoli na efektywniejszą obronę przeciwko pociskom rakietowym wystrzelonym w kierunku samolotu oraz sprawi, że maszyna zacznie się uczyć rozwiązywania nowych problemów (takich jak na przykład znalezienie odpowiedniej reakcji na nowe sposoby walki zastosowane przez siły przeciwnika).

Z kolei taki system jak OMS zapewnia integrację maszyny załogowej z podległymi jej BSP. Należy przy tym zaznaczyć, że te operacje rozproszone zależne są od niezawodności i wydajności systemu przekazywania danych odpornego na oddziaływanie systemów WRE przeciwnika.

Przyszłe samoloty w dużo większym stopniu będą się opierać również na wspomnianej już AI, przy czym jej powszechniejsze wprowadzenie na pokłady maszyn bojowych to nie tylko problem techniczny, lecz związany także z przekonaniem pilotów do korzystania z jej usług. Pilot powinien mieć pełne zaufanie do takiej własnej inteligentnej maszyny.

A przecież pierwsze symulowane, w zasadzie eksperymentalne, walki powietrzne pokazały, jak dużą przewagę ma samolot bojowy wspomagany sztuczną inteligencją (AI) nad klasyczną platformą powietrzną. Szczególnie dotyczy to sytuacji, gdy AI wyręcza pilota w podejmowaniu działań defensywnych (np.: wykrycia pocisków rakietowych wystrzelonych przez przeciwnika, uruchomienia systemów samoobrony czy wykonania manewrów uniku). Nad takim jej wykorzystaniem prowadzą obecnie intensywne badania Izraelczycy, Anglicy i Amerykanie. Chińczycy i Rosjanie również nie pozostają w tyle.

W USA w oprogramowaniu ALPHA wykorzystuje się AI w metodzie nazwanej *Fuzzy Logic* do podejmowania w powietrzu szybkich decyzji dotyczących zarządzania walką oraz wyboru najlepszego planu działania charakteryzującego się maksymalnym prawdo-

podobieństwem powodzenia. W symulowanych sytuacjach oprogramowanie ALPHA jest na tyle szybkie, że wygrywa z najlepszymi pilotami USAF (może w dynamicznym środowisku walki analizować i wybierać najlepsze scenariusze ponad 250 razy szybciej niż doświadczeni jej przeciwnicy – piloci). Program ALPHA oparto na hybrydowym podejściu z wykorzystaniem logiki rozmytej i algorytmów genetycznych. Jest w stanie wypracować sposoby obrony przed zmasowanym atakiem rakiet typu powietrze–powietrze i ziemia–powietrze i jednocześnie atakować wybrane cele, koordynować działania skrzydłowych, a przede wszystkim uczyć się zachowań przeciwnika, jego taktyki i możliwości.

Samoloty mające w wyposażeniu system OMS (*Open Mission System*) są zdolne do łączenia i przesyłania informacji między różnymi platformami za pomocą standardowego łącza Link-16 i tzw. utajnionego łącza wymiany danych wykorzystywanego w takich platformach, jak F-22. OMS ułatwia integrację platform załogowych i bezzałogowych.

Agencja DARPA prowadzi badania nad opracowaniem zintegrowanych systemów łączących technologię SOSIT pozwalającą platformom załogowym nadzorować działania ich lojalnych skrzydłowych. Zgodnie z założeniami programu ACE (*Air Combat Evolution*) to AI miałaby przejąć prowadzenie walki w sposób gwarantujący zmaksymalizowanie potencjału własnej maszyny. Odpowiednio wypracowane i w ułamkach sekund wprowadzone do wykonania manewry pozwolą na efektywną walkę z każdym przeciwnikiem. Pilot zatem nie koncentruje się już się na bezpośrednim zagrożeniu, lecz nadzoruje walkę prowadzoną przez lojalnych skrzydłowych.

Z kolei firmy BAE i Collins Aerospace wspólnie rozwijają narzędzia i technologie przeznaczone do ulepszenia architektury systemu otwartego podejścia, mające zabezpieczyć elektronikę samolotu przed cyberatakiem.

Weźmy na przykład radiolokatory z aktywnym skanowaniem elektronicznym AESA (*Active Electronically Scanned Array*), które są uważane powszechnie za najnowocześniejszy system wykrywania celów i naprowadzania na nie uzbrojenia samolotów obecnej i kolejnych generacji. Charakteryzują się one tym, że skanują cały zadany im obszar jednocześnie w przeciwieństwie do rozwiązań stosowanych w konwencjonalnych radiolokatorach, a pozyskane informacje po przetworzeniu są albo odrzucane, albo zbierane w bazie danych. Sprzyja to jednak przemyceniu do systemu również informacji niepożądanych (zainfekowanych). Opracowując więc lub modyfikując takie radiolokatory, dąży się wciąż do zbudowania inteligentnego systemu nadzoru (czujników) wszelkich informacji wpływających, który je zbiera i klasyfikuje. W przypadku gdy nie pasują one do znanych charakterystyk, czujnik cały czas próbuje pozyskać informacje na temat aktualnego stanu takiej informacji. Brak nadzoru i blokady takiej informacji staje się dogodnym miejscem do ataku z zewnątrz (np. cyberataku). Ponieważ radary stanowią bazę wszelkich danych dla systemów ich przetwarzania, analizy i nadzoru, a także systemów uzbrojenia, pilotażu i samoobrony, jest to otwarta droga do ich neutralizacji lub przejęcia nad nimi kontroli.

Zgodnie ze statystycznymi wyliczeniami 90% systemów zainstalowanych na pokładzie F-35 działa w systemie sieci informatycznej tego samolotu nadzorowanej przez zespolony system informatyczny. W odniesieniu do F-22 jest to około 70% systemów pokładowych, B-2 – około 60%, a F-15 już tylko 20%. Sprzyja to zewnętrznym „atakom".

Jedną z rozważanych opcji jest separacja systemów sterowania samolotem (np. odrębne systemy nadzoru i wykorzystania uzbrojenia czy łączności i przekazywania danych, tak by w razie zainfekowania jednego z nich można było nadal używać pozostałych). Przy czym jest to proces zwiększający koszty pozyskania i eksploatacji takich systemów, które nie zapewnią jednak w 100% bezpieczeństwa załodze czy maszynie.

NOWA JAKOŚĆ

Każdy współcześnie eksploatowany w siłach zbrojnych samolot lub śmigłowiec ma swoje wady i zalety. Jedno pozostało niezmienne – rola pilota ulega ciągłej zmianie. Kiedyś samo utrzymanie maszyny w powietrzu czy start i lądowanie to już były wyzwania. Technologia sprawiła jednak, że doskonale latają nawet samoloty aerodynamicznie niestabilne, a sam pilotaż ułatwia przejęcie przez systemy informatyczne zainstalowane na pokładzie kontroli nad awionika, czujnikami, uzbrojeniem, silnikami itp.

Dziś nowe technologie szybko zmieniają lotnictwo bojowe oraz sposoby prowadzenia przez nie walki w powietrzu. Sztuczna inteligencja na pokładach może już w niedalekiej przyszłości wykonywać przynajmniej część zadań, które obecnie należą do ludzi, odciążyć pilotów i wspomóc ich w wykonaniu zadanej misji. Wsparciem będzie również wirtualna prezentacja danych czy zastosowanie samouczenia się. Słowo pilot już w niedługim czasie może nie kojarzyć się wyłącznie z lataniem, a zamiennikiem dla niego będzie określenie *menedżer* pola walki powietrznej.

Samolot przyszłości bowiem to nie będzie pojedyncza maszyna bojowa, lecz coś w rodzaju centrum dowodzenia działaniami w powietrzu w małej skali. Dzięki zaawansowanemu udostępnianiu informacji zmniejszy się liczba platform załogowych, a autonomiczne BSP będą w stanie samodzielnie wykonać operację startu i lądowania oraz dotarcia do obszaru realizacji misji z jednoczesnym unikaniem zagrożeń. Tam kontrolę przejmą nad nimi załogowe platformy, które będą nadzorować wykonywanie precyzyjnych ataków oraz prowadzenie działań przez zgrupowanie powietrzne. One też dzięki nowym technologiom na bieżąco będą wypracowywać sposoby prowadzenia działań wymuszone wszelkimi ruchami potencjalnego przeciwnika. ■

Co z tą **cyberprzestrzenią?**

BRAK JEDNOLITEGO APARATU POJĘCIOWEGO ZARÓWNO W DOKUMENTACH NATO, JAK I NARODOWYCH SKUTKUJE DOWOLNOŚCIĄ INTERPRETACJI WIELU ZJAWISK POLA WALKI ORAZ CHAOSEM WE WŁAŚCIWYM ICH ROZUMIENIU.

ppłk dr inż. Stanisław Czeszejko

Autor jest starszym specjalistą w Oddziale Szkolenia Zarządu Wojsk Radiotechnicznych Inspektoratu Sił Powietrznych DGRSZ.

W ostatnim czasie stała się ona jednym z najdynamiczniej rozwijających się obszarów zmagań militarnych, co wynika bezpośrednio z rozwoju cywilizacyjnego świata, w tym jego aspektów bezpieczeństwa. Choć wykorzystanie urządzeń i systemów elektronicznych w wielu wypadkach różni się od prowadzenia klasycznych działań militarnych, to cel działań pozostaje spójny. Gdzie jest miejsce cyberprzestrzeni na polu walki i jaki jej zakres wchodzi w skład działań militarnych? Podejmę próbę oceny tego zjawiska.

ZJAWISKA FIZYCZNE – NAJISTOTNIEJSZE ASPEKTY

Występujące w naturze zjawiska fizyczne, związane z silnymi wyładowaniami elektrycznymi w atmosferze i towarzyszące zwykle burzom, były bacznie obserwowane przez ludzi przez kolejne tysiąclecia. Odkryto również wiele zjawisk, w czasie których powstawało zdecydowanie mniej energii elektrycznej, np. ładunków elektrostatycznych, czyli tzw. elektryzowanie się. W rozważaniach prowadzonych na nasze potrzeby należy ocenić w pierwszej kolejności źródła powstawania promieniowania elektromagnetycznego. W naturze występuje ich wiele, np. promieniowanie słoneczne czy wyładowania atmosferyczne[1], ale w praktyce na wszystkie naturalne źródła promieniowania elektromagnetycznego człowiek nie potrafi wpływać w taki sposób, by doprowadzić formę ich promieniowania do postaci użytecznej dla niego (pożądanej przez niego).

Wraz ze zgłębianiem wiedzy na ten temat możliwe stało się konstruowanie urządzeń elektrycznych i elektronicznych, również tych będących sztucznymi źródłami promieniowania elektromagnetycznego. Należy mieć na uwadze, że jedynie urządzenia elektroniczne są w stanie wytwarzać i przetwarzać skomplikowane sygnały elektryczne użyteczne obecnie dla człowieka (w tym cyfrowe), które mogą być zamieniane na postać pożądanego promieniowania elektromagnetycznego (i odwrotnie).

W związku z tym wyraźnie widać, że użyteczne promieniowanie elektromagnetyczne jest jedynie skutkiem funkcjonowania urządzeń elektronicznych i nie jest jedynym ich produktem wykorzystywanym przez człowieka. Jednocześnie zaczęto konstruować urządzenia elektryczne i elektroniczne[2] coraz bardziej

1 T. Rybak, *Raport o stanie środowiska w 2010 r. 6. Promieniowanie elektromagnetyczne*, http://www.wios.rzeszow.pl/cms/upload/edit/file/stan_srodowiska_2010/r6.pdf/. 24.02.2014.

2 Wyróżnienie elektroniki z ogólnego pojęcia *elektrotechniki* nastąpiło około 1906 roku. Wtedy to Lee De Forest wynalazł triodę, dzięki której bez użycia urządzeń mechanicznych można było już wówczas wzmacniać urządzeniem elektrycznym słabe sygnały radiowe lub akustyczne. Do lat pięćdziesiątych XX wieku dziedzina ta sprowadzała się do radiotechniki (tak ją nazywano), a jej zasadnicze zastosowania obejmowały projektowanie nadajników, odbiorników i lamp próżniowych. Historycznie elektronika wyrosła więc z radiotechniki – pierwszymi układami elektronicznymi były powstające w czasach I wojny światowej nadajniki i odbiorniki radiowe. Współcześnie większość urządzeń elektronicznych projektuje się z użyciem elementów półprzewodnikowych, za pomocą których można sterować przepływem elektronów podobnie jak w lampach elektronowych, http://pl.wikipedia.org/wiki/Elektronika/. 16.02.2014.

skomplikowane, a na pewnym etapie ich rozwoju możliwe stało się łączenie ich w różnego rodzaju systemy.

Wraz z rozwojem militarnych urządzeń i systemów elektronicznych rozpoczęto opracowywanie teorii ich bojowego wykorzystania (w tym ustalanie nazewnictwa) oraz zaczęto uwzględniać je w obowiązujących doktrynach. Na przestrzeni lat utworzono wiele pojęć i przedstawiano różne propozycje uregulowań zagadnień z nimi związanych, a rozbieżności w ich postrzeganiu budzą nadal wiele wątpliwości. Zatem potwierdza się pogląd M. Mazura, że *dążąc do wyjaśnienia czegoś, należy zacząć od analizy zjawisk i dopiero po wyodrębnieniu istotnych pojęć*[3] *należy nadawać im określone nazwy*[4]. Ponadto w nadawaniu nazw należy się kierować zasadami semantyki[5], co zdecydowanie upraszcza rozpoznawanie problemu, który się kryje za daną nazwą.

GENEZA PODZIAŁU DZIAŁAŃ MILITARNYCH

Rozmach prowadzonych działań militarnych w historii ludzkości zależał od posiadanych możliwości i środków walki, jakie były dostępne. Najpierw militarnie zmagano się na lądzie, następnie zapewniono sobie zdolności do prowadzenia takich działań na morzu, a na początku XX wieku rozwinięto je w powietrzu. Niemal równolegle z rozwojem walk powietrznych pojawił się nowy rodzaj działań militarnych, który wykorzystywał urządzenia i systemy elektroniczne. Przed wybuchem I wojny światowej i w początkowej jej fazie najpowszechniejszymi środkami łączności były telegraf i telefon, które już wówczas tworzyły złożone systemy (tzw. systemy łączności). Łączność radiowa była rozpowszechniona jedynie w siłach morskich i właśnie w tym rodzaju sił zbrojnych odnotowano pierwszą aktywność w zakresie rozpoznania radiowego. Miało to miejsce podczas wojny rosyjsko-japońskiej w 1904 roku[6].

Wkrótce po wybuchu I wojny światowej łączność radiowa znalazła powszechniejsze zastosowanie[7]. Z kolei w okresie międzywojennym nastąpił kolejny, ogromny jak na ówczesne warunki, postęp w dziedzinie elektroniki[8].

W drugiej połowie XX wieku do celów militarnych wykorzystywano już Kosmos. Stało się tak od momentu wystrzelenia pierwszego satelity, co miało miejsce w 1957 roku[9]. Być może w pierwszej fazie jego wykorzystania nie postrzegano Kosmosu jako kolejnego wymiaru prowadzenia działań, gdyż nie toczono tam nigdy otwartego konfliktu zbrojnego, lecz również tam prowadzono tzw. zimną wojnę[10]. Z czasem zaczęto w pełni dostrzegać jego znaczenie w działaniach militarnych.

W trakcie II wojny światowej działania z wykorzystaniem urządzeń i systemów elektronicznych (w tym radarów oraz istniejących już systemów rozpoznania radiolokacyjnego) stały się dość ważnym elementem zabezpieczenia działań bojowych, doczekały się nawet własnej nazwy – *wojna radioelektroniczna.* Miało to racjonalne uzasadnienie, gdyż wykorzystywano fale radiowe (promieniowanie elektromagnetyczne) pochodzące z radiowych urządzeń elektronicznych.

---

3 *Pojęcie* – myślowe odzwierciedlenie całościowego ujęcia istotnych cech przedmiotów (rzeczy) czy zjawisk – jest myślowym odzwierciedleniem nazwy. L. Ciborowski, *Pojęciowa interpretacja terminu „informacja" i jej pochodnych*, „Zeszyty Naukowe AON" 2010 nr 4(81), s. 67.

4 M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970, s. 27 [za:] L. Ciborowski, *Pojęciowa interpretacja* ..., op.cit., s. 58.

5 *Semantyka* (gr. *semantikos*) – dyscyplina badająca relacje znaczeniowe występujące między znakami językowymi a przedmiotami, do których się one odnoszą. Semantyka zajmuje się badaniem znaczenia słów, czyli interpretacją znaków oraz interpretacją zdań i wyrażeń języka. Semantykę nazywa się także *teorią znaczenia* lub *teorią oznaczania* (*Quine*). L. Ciborowski, *Pojęciowa interpretacja...*, op.cit., s. 67.

6 H. Piekarski, *Walka radioelektroniczna*, Wydawnictwo MON, Warszawa 1980, s. 19.

7 Na potrzeby rozpoznania radiowego wprowadzono wówczas w krótkim czasie namierniki radiowe, rozwinięto również działalność związaną z rozszyfrowywaniem utajnianych informacji przesyłanych drogą radiową oraz stosowano dezinformację radiową. Zbudowano i zastosowano pierwsze specjalizowane urządzenia do zakłócania łączności radiowej, choć była to w istocie bardziej działalność doświadczalna niż bojowa.

8 Dotyczył on w pierwszej fazie rozwoju elementów i podzespołów wykorzystywanych do budowy urządzeń łączności (głównie lamp elektronowych). W następnych fazach objął rozwój radiotelegrafii, telewizji, radiolokacji oraz radionawigacji. Wówczas to powstawały specjalizowane systemy wykorzystujące różnego rodzaju urządzenia elektroniczne mające specjalne przeznaczenie, np. brytyjski system obrony powietrznej znany z bitwy o Anglię opierał się zasadniczo na radarach (elektronicznych urządzeniach rozpoznania radiolokacyjnego) oraz na elementach elektronicznych łączności radiowej i przewodowej (radiostacje naziemne, radiostacje lotnicze, telefony, łącznice telefoniczne itp.).

9 Pierwszym sztucznym satelitą w Kosmosie był wykonany przez człowieka Sputnik 1, wyniesiony w 1957 roku na orbitę wokół Ziemi przez Związek Radziecki. Według stanu na 2015 rok w Kosmosie znajdowało się ponad 3 tys. sztucznych satelitów, http://pl.wikipedia.org/wiki/Sztuczny_satelita/. 26.01.2015.

10 *Zimna wojna* – umowne określenie stanu stosunków międzynarodowych charakteryzujących się trwałym konfliktem, a także niemożnością jego rozstrzygnięcia przez konfrontację militarną. Choć wiele konfliktów w historii można określić tym mianem, obecnie zimną wojną nazywa się globalny konflikt po II wojnie światowej (wówczas określenie to weszło do powszechnego użytku). Zimna wojna po II wojnie światowej rozpoczęła się jako konflikt między ZSRR a światem demokracji zachodnich, jednak stopniowo front konfrontacji rozszerzył się i zróżnicował. W tym okresie charakteryzowała się silnym, choć zmiennym napięciem politycznym, wyścigiem zbrojeń, konfrontacją ideologiczną i wojną psychologiczną, walką o wpływy na terenach peryferyjnych z punktu widzenia głównych protagonistów oraz instrumentalnym traktowaniem wymiany handlowej i kulturalnej, przy jednoczesnej powściągliwości w działaniach wojskowych. Główne strony konfliktu weszły w posiadanie broni jądrowej, jednak unikały jej użycia, a konfrontację przenosiły najczęściej na obszary peryferyjne, https://encyklopedia.pwn.pl/haslo/zimna-wojna;4001555.html/. 1.09.2020.

Swoje poglądy na ten temat przedstawił brytyjski historyk Michael Howard[11] w książce pt. *Wojna w dziejach Europy* (w rozdziale VII pt. *Wojny techników*), wydanej w 1976 roku w Wielkiej Brytanii. W jego ocenie już w czasie I wojny światowej powstał nowy – *czwarty wymiar wojny* (po lądowym, morskim i powietrznym)[12], tzn. wojny związanej z zastosowaniem elektronicznych urządzeń łączności, kryptografii, walki i rozpoznania radioelektronicznego oraz radiolokacji, wykorzystujących głównie promieniowanie elektromagnetyczne. W czasie II wojny światowej nastąpił dalszy, intensywny jego rozwój. Ważny z punktu naszych rozważań jest fakt, iż nie nazwał on nowego czwartego wymiaru wojny, lecz jedynie wskazał na jego istnienie.

Podsumowując, militarne zmagania na koniec II wojny światowej prowadzono w wymiarach: lądowym, morskim, powietrznym i radioelektronicznym.

Spojrzenie M. Howarda na tę problematykę znalazło odzwierciedlenie w rodzimych opracowaniach, w których spotyka się m.in. określenie *czwarty wymiar konfrontacji zbrojnej z przeciwnikiem*[13]. Profesor Leopold Ciborowski, znany teoretyk zajmujący się problematyką rozpoznania i walki elektronicznej (RiWE) oraz walką informacyjną, już pod koniec lat dziewięćdziesiątych ubiegłego wieku wskazał, iż nawet w trakcie pierwszej wojny w rejonie Zatoki Perskiej twierdzono, że walka wkroczyła w *czwarty wymiar*, którym jest *przestrzeń elektromagnetyczna*[14].

Naturalnym efektem, będącym reakcją na wskazanie kolejnego wymiaru wojny, były próby jego nazwania. Jedną z nich podjął w połowie lat osiemdziesiątych ubiegłego wieku oficer Bundeswehry płk Rudolf Grabau. Nie ograniczył się on jedynie do wskazania nazwy dla czwartego wymiaru wojny (nazwał go: *spektrum elektromagnetyczne*), lecz także przedstawił własny podział wojny na sześć jej wymiarów[15]: odległość (utożsamiającą oddalenie w linii prostej), powierzchnię (szerokość i głębokość – utożsamiającą teren), wysokość (utożsamiającą przestrzeń przez dopełnianie powierzchni), spektrum elektromagnetyczne, czas i informacje. Wskazał wówczas, że ostatnie trzy czynniki będą mieć decydujący wpływ na charakter przyszłych konfliktów zbrojnych.

Niewykluczone, że przyjęte przez płk. R. Grabau nazewnictwo dla czwartego wymiaru wojny M. Howarda (*spektrum elektromagnetyczne*) jest pewnego rodzaju pokłosiem stosowania w kręgach militarnych różnych państw pojęcia *wojna radioelektroniczna*, utożsamiana jednoznacznie z wykorzystaniem fal radiowych (elektromagnetycznych). Pewnym wytłumaczeniem poprawności przyjętego przez niego podziału może być fakt, że wymienione przez M. Howarda elektroniczne urządzenia kryptografii można umiejscowić w podziale R. Grabau w obszarze informacji.

ŚRODOWISKO ELEKTROMAGNETYCZNE

W rodzimych opracowaniach też funkcjonuje nazwa *środowisko elektromagnetyczne*, które jest rozumiane jako środowisko rozprzestrzeniania się energii elektromagnetycznej[16]. Można też znaleźć informacje, w których nasi specjaliści twierdzą, że *widmo elektromagnetyczne (obok cyberprzestrzeni) jest kolejnym wymiarem współczesnego pola walki*[17].

Niektóre źródła wskazują, że w ramach ogólnego podziału prowadzenia walki informacyjnej[18] wyróżnia się jej osobową oraz techniczną przestrzeń. Podobny podział przyjęto dla rozpoznania[19], które dzieli się na rozpoznanie osobowe i techniczne. Ten drugi rodzaj rozpoznania prowadzi się z wykorzystaniem specjalistycznych urządzeń, które mogą rozpoznawać i rejestrować efekty i zjawiska w środowiskach: elektromagnetycznym, sprężystym, elektrycznym, magnetycznym oraz chemicznym. Wymienione środowiska występują w opracowaniach dotyczących zarówno walki informacyjnej, jak i rozpoznania i w obu wymieniono środowisko elektromagnetyczne.

Należy zatem zadać pytanie, czy pojęcie *środowisko elektromagnetyczne* można uznać za właściwą nazwę dla czwartego wymiaru wojny. Używane w przeszłości pojęcie *środowisko elektromagnetyczne* miało swoje pragmatyczne uzasadnienie, choć niekoniecznie rzeczywiste. W dobie wszechobecnych sieci komputerowych innego znaczenia nabrało wykorzy-

11 Sir Michael Howard (29.11.1922–30.11.2019) profesor, brytyjski historyk wojskowości. Był m.in. kierownikiem ośrodka badań wojen na uniwersytecie w Oksfordzie, gdzie kierował katedrą historii współczesnej. Pozostaje członkiem Akademii Brytyjskiej, honorowym członkiem Amerykańskiej Akademii Nauk oraz był honorowym prezydentem Międzynarodowego Instytutu Badań Strategicznych w Londynie. W swoim czasie to jeden z najbardziej wpływowych Brytyjczyków w obszarze kształtowania badań strategicznych nt. obronności i bezpieczeństwa państwa, był konsultantem w tym zakresie premier Margaret Thatcher, http://en.wikipedia.org/wiki/Michael_Howard _(historian)/. 20.06.2020.

12 H. Michael, *Wojna w dziejach Europy*, Wrocław 1990, s. 167.

13 H. Piekarski, *Walka radioelektroniczna...*, op.cit., s. 5.

14 L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 35.

15 R. Grabau, *Sechs Dimissionen des Krieges. Versuch einer analytischen Betrachtung*, „Soldat und Technik" 1985 nr 5, s. 245.

16 W. Scheffs, *Proces oceny przeciwnika w aspekcie elektronicznym* [w:] materiały z międzynarodowej konferencji naukowej nt. *Sieci teleinformatyczne w działaniach sieciocentrycznych* – 2006, AON, Warszawa 2007, s. 121.

17 M. Blach, *Bazy danych elementem skuteczności rozpoznania elektronicznego* [w:] materiały z międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych,* AON, Warszawa 2008, s. 28.

18 L. Ciborowski, *Walka informacyjna...*, op.cit., s. 112.

19 W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa 2002, s. 31.

Walka elektroniczna (walka radioelektroniczna) ogranicza się do prowadzenia działań militarnych z użyciem energii elektromagnetycznej. Mimo jednoznaczności określenia obszaru działań prowadzonych w jej ramach we wszystkich wskazanych definicjach niektórzy polscy teoretycy dostrzegali potrzebę poszerzenia zakresu przedsięwzięć wchodzących w jej skład.

USAF

stywanie energii elektrycznej do wytwarzania i przesyłania sygnałów, jak również zmienia się używaną terminologię.

Podsumowując, militarne zmagania ludzkości na przełomie XX i XXI wieku prowadzono już na lądzie, na morzu, w powietrzu, w środowisku elektromagnetycznym i w Kosmosie. Dlatego też pojęcie *środowisko elektromagnetyczne* nie spełnia wymaganych warunków, aby zyskać miano *czwartego wymiaru wojny.* Określenie to (wcześniej *spektrum elektromagnetyczne* lub *przestrzeń elektromagnetyczna*) zatraciło swoją aktualność.

WALKA ELEKTRONICZNA CZY RADIOELEKTRONICZNA?

Po II wojnie światowej ukształtowało się i funkcjonuje kolejne pojęcie *walka elektroniczna* (*Electronic Warfare*), które wywodzi się bezpośrednio z określenia *wojna radioelektroniczna*. Z przeprowadzonej analizy definicji zawartych w literaturze przedmiotu i w dokumentach normatywnych NATO wynika jednoznacznie, że walka elektroniczna ogranicza się do prowadzenia działań militarnych z użyciem energii elektromagnetycznej. Warto tutaj zapoznać się także z definicjami obowiązującymi w armiach, które odgrywają wiodącą rolę w dziedzinie walki elektronicznej i w związku z tym niejednokrotnie kreują pojęcia obowiązujące w NATO. Oto przykłady przedstawiające chronologicznie interesujący nas obszar działań militarnych jako:

– walka elektroniczna[20] (według USA – 1999 rok) – to każde działanie militarne wiążące się z użyciem energii lub atakowaniem przeciwnika;

– walka elektroniczna[21] (według USA – 2010 rok) – działalność militarna obejmująca użycie energii elektromagnetycznej i wiązkowej w celu kontroli spektrum elektromagnetycznego lub ataku prowadzonego przeciwko przeciwnikowi;

– walka elektroniczna (według NATO – 2015 rok)[22] – działania militarne, które wykorzystują energię elektromagnetyczną, aby zapewnić świadomość sytuacyjną oraz osiągnięcie efektów zarówno ofensywnych, jak i defensywnych[23].

Natomiast jedną z ważniejszych pozycji w rodzimej literaturze opisującą walkę elektroniczną jest praca Leopolda Ciborowskiego z 1993 roku, w której autor

20 R. Szpyra, *Militarne operacje informacyjne*, AON, Warszawa 2003, s. 108 (tłumaczenie z: AFDD 2-5.1: *Electronic Warfare*, Washington D.C., 1999).

21 *Cyberspace Operations* (*DD 3-12*), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 52. Wskazano tam, że definicja została zaczerpnięta z: *Joint Publication (JP) 1-02*, Department of Defense Dictionary of Military and Associated Terms, USA.

22 *Electronic Warfare in Air Operations* (*ATP 3.6.3*), Edition A Version 1, NATO Standardization Office (NSO), 2015, załącznik "Lexicon", s. Lex-2.

23 *Electronic Warfare – is military action that exploits electromagnetic energy (EM) to provide situational awareness and achieve offensive and defensive effects.*

szeroko stosował analizę i modelowanie matematyczne. L. Ciborowski jest przedstawicielem szkoły, dla której aparat matematyczny był podstawą wszelkich rozważań naukowych, dlatego też we wskazanej pozycji większość hipotez zweryfikowano z wykorzystaniem metod matematycznych. Już na pierwszych stronach pracy autor wskazuje, że *walka elektroniczna zakłóca proces informacyjny przeciwnika (obieg i treść informacji) w sferze elektromagnetycznej*[24], co jednoznacznie charakteryzuje zakres jej działania. Przedstawia również podział rozpoznania ogólnego na[25]: rozpoznanie osobowe i rozpoznanie elektroniczne (podział rozpoznania ogólnego w późniejszych latach zmienił się i obejmował rozpoznanie osobowe i rozpoznanie techniczne)[26].

Należy mieć natomiast na uwadze, że w krajowej literaturze termin *walka radioelektroniczna* stosowano do 2002 roku[27], a powrót do użycia tego określenia nastąpił w 2014 roku[28]. W latach 2002–2014 obowiązywało pojęcie *walka elektroniczna*.

Podobne poglądy (definicje) do panujących w NATO oraz w siłach zbrojnych USA można ostatecznie odnaleźć w dokumentach SZRP. Interesujący nas obszar działań militarnych opisywano w nich jako:

– walka radioelektroniczna[29] (według AON – 1994 rok) – to całokształt przedsięwzięć i działań wojsk, które, wykorzystując energię elektromagnetyczną, zmierzają do rozpoznania i zdezorganizowania systemów radioelektronicznych przeciwnika oraz zapewnienia warunków stabilnej pracy systemom wojsk własnych;

– walka elektroniczna[30] (według SGWP – 2003 rok) – działania militarne polegające na rozpoznawaniu źródeł emisji elektromagnetycznej oraz dezorganizowaniu pracy systemów elektronicznych przeciwnika wykorzystujących energię elektromagnetyczną, w tym energię wiązkową, przy jednoczesnym zapewnieniu warunków ich efektywnego użycia przez wojska własne;

– walka radioelektroniczna (według SZRP – 2015 rok)[31] – to działania wojskowe wykorzystujące energię elektromagnetyczną (EM) do zapewnienia świadomości sytuacyjnej oraz uzyskania efektów ofensywnych i defensywnych;

– środowisko elektromagnetyczne (według SZRP – 2015 rok)[32] – to nieograniczona przestrzeń, w której emitowana jest energia EM na różnych zakresach częstotliwości spektrum EM oraz samoistnie lub celowo działają urządzenia elektroniczne sił zbrojnych podczas prowadzenia działań w środowisku operacyjnym.

Praktycznie wszystkie dostępne definicje, zarówno natowskie, sił zbrojnych USA, jak i innych państw Sojuszu, wskazują, że walka elektroniczna (walka radioelektroniczna) ogranicza się do prowadzenia działań militarnych z użyciem energii elektromagnetycznej. Mimo jednoznaczności określenia obszaru działań prowadzonych w jej ramach we wszystkich wskazanych definicjach niektórzy polscy teoretycy dostrzegali potrzebę poszerzenia zakresu przedsięwzięć wchodzących w jej skład.

W pracy studyjnej z 2001 roku pracownik AON płk Józef Janczak wymienia w ramach rozpoznania elektronicznego następujące elementy[33]: rozpoznanie radioelektroniczne, rozpoznanie radiolokacyjne, rozpoznanie informatyczne, rozpoznanie optoelektroniczne oraz czujnikowe. Podobnie przedstawił on podział zakłóceń aktywnych, które zgodnie z jego poglądami składają się z zakłóceń[34]: radiowych, radiolokacyjnych, radionawigacyjnych, optoelektronicznych oraz informatycznych. Wskazuje również, że działania militarne w ramach walki elektronicznej są prowadzone na specyficznym *elektronicznym polu walki*, które można określić mianem *środowiska elektromagnetycznego* (dotyczącego środków elektronicznych promieniujących i odbierających energię elektromagnetyczną)[35].

Poglądy J. Janczaka wyraźnie kierują się w stronę szerszego postrzegania problematyki wykorzystania urządzeń i systemów elektronicznych w działaniach militarnych, czego dowodem jest włączenie w tę tematykę również informatyki.

W niektórych źródłach przedstawiono podział rozpoznania technicznego według kryterium wyróżnialności[36], jakim jest *środowisko nośników danych.* Dzieli się je na rozpoznanie: elektromagnetyczne; czujnikowe, prowadzone w środowisku akustycznym, elektrycznym, magnetycznym oraz chemicznym; informatyczne, związane z techniką komputerową i jej otoczeniem, w tym z monitorowaniem promieniowania z monitora lub jego części zewnętrznych, np. połączeń kablowych.

24 L. Ciborowski, *Rozpoznanie i walka elektroniczna*, AON, Warszawa 1993, s. 13.

25 Ibidem, s. 58.

26 W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych...,* op.cit., s. 29.

27 K. Dymanowski, Z. Groszek, *Walka radioelektroniczna w działaniach SP we współczesnych konfliktach zbrojnych*, AON, Warszawa 2008, s. 5.

28 *Walka elektroniczna – DD 3.6*, CDiSzSZ, Bydgoszcz 2015, *Słownik terminów i definicji*, s. 1.

29 *Walka radioelektroniczna w SZ RP*, red. Z. Magnucki, AON, Warszawa 1994, s. 11.

30 *Walka elektroniczna,* sygn. Szt.Gen. 1549/2003, Załącznik C – *Słownik terminów, definicji i skrótów*.

31 *Walka elektroniczna – DD 3.6*..., op.cit.

32 Ibidem, s. 24.

33 J. Janczak, *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, AON, Warszawa 2001, s. 17.

34 Ibidem, s. 131.

35 Ibidem, s. 203.

36 W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych*..., op.cit., s. 36.

Dwaj inni oficerowie – pracownicy AON, Marian Łokociejewski oraz Waldemar Scheffs, w swojej pracy z 2005 roku twierdzą, że prowadzenie walki elektronicznej nie powinno ograniczać się jedynie do przestrzeni elektromagnetycznej, lecz należy rozszerzyć jej oddziaływanie na inne urządzenia elektroniczne (w tym na te niewykorzystujące energii elektromagnetycznej)[37]. Według tych autorów takie podejście umożliwia rozszerzenie walki elektronicznej na oddziaływanie kinetyczne (ogniowe) z wykorzystaniem pocisków samonaprowadzających się na systemy elektroniczne oraz pozwala na inne spojrzenie na obronę elektroniczną, w tym na systemy informatyczne. Swoje poglądy uzasadniają tym, że gdyby ograniczać się do prowadzenia działań militarnych w przestrzeni elektromagnetycznej, należałoby pozostać przy użyciu nazwy *walka radioelektroniczna* jako bardziej adekwatnej.

Dalsze rozważania w podobnym kierunku prowadził płk Waldemar Scheffs, który w swoim wystąpieniu na międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych* w 2008 roku wskazał, że oprócz przestrzeni elektromagnetycznej można wyróżnić inne środowiska, w których toczy się walkę elektroniczną. Zaliczył do nich wówczas: przestrzeń działania systemów informatycznych, przestrzeń akustyczną oraz pole magnetyczne[38]. Podsumowując rozważania odnoszące się do walki elektronicznej, należy zauważyć, że[39]:

– zgodnie z regułami nazewnictwa pojęcie *walka* wymaga dodania wyrazu uzupełniającego, który będzie związany z identyfikacją sfery, w której jest, była lub będzie ona prowadzona;

– identyfikacja przedmiotu walki decyduje natomiast nie o jej nazewnictwie, lecz o doborze narzędzi do jej prowadzenia oraz sposobów ich wykorzystywania w konkretnym działaniu.

W związku z tym, że nie wszystkie działania związane z użyciem urządzeń i systemów elektronicznych są walką, nie możemy objąć pojęciem *walka elektroniczna* całego obszaru działań militarnych prowadzonych z zastosowaniem urządzeń i systemów elektronicznych.

ŚRODOWISKO INFORMACYJNE – WALKA INFORMACYJNA

Innym interesującym nas rodzajem walki, który zdefiniowano na potrzeby prowadzenia działań militarnych (i nie tylko), jest walka informacyjna. Należy zauważyć, że choć może nie występowała ona pod taką nazwą wcześniej, to prowadzono ją od zarania dziejów. Skonstruowane przez człowieka urządzenia i systemy elektroniczne stały się tylko narzędziem do prowadzenia tego rodzaju walki.

L. Ciborowski w swojej pracy z końca lat dziewięćdziesiątych na temat walki informacyjnej wskazuje, że większą precyzję w interpretacji omawianych pojęć zapewnia słownictwo cybernetyczne i matematyczne[40]. Przedstawia również części składowe walki informacyjnej, wyodrębnione w USA w 1994 roku, które obejmują[41]: walkę elektroniczną, działania psychologiczne oraz walkę informatyczną. Wskazuje też przykładowo na poglądy byłego oficera sił powietrznych USA płk. rez. D. Camptena, który rozszerzył zakres walki informacyjnej na sferę pozamilitarną[42].

Takie ujęcie podziału środowisk walki znalazło odzwierciedlenie w amerykańskich dokumentach normatywnych, w których *środowisko informacyjne*[43] pierwotnie zdefiniowano jako *zbiór jednostek, organizacji i systemów, które prowadzą zbiór informacji oraz je przetwarzają, dystrybuują oraz gromadzą (zapisują)*[44]. Znalazło to akceptację i potwierdzenie w innych dokumentach[45], gdzie wskazuje się, że w skład *środowiska operacyjnego* walki wchodzą domeny: lądowa, morska, powietrzna, kosmiczna i środowiska informacyjnego.

Podobne poglądy można odnaleźć w doktrynie NATO z 2009 roku[46], w której w skład operacji informacyjnych (*Information Operations* – IO) prowadzonych przez Sojusz oprócz innych czynników zalicza się m.in. dwa najważniejsze rodzaje działań związanych z wykorzystaniem urządzeń i systemów elektronicznych, tj. walkę elektroniczną (*Electronic Warfare* – EW) oraz działania w sieciach informatycznych (*Computer Network Operations* – CNO).

Natomiast już w 2011 roku można dostrzec wyraźną różnicę w amerykańskich poglądach w stosunku do poprzednio prezentowanych. W dokumentach dotyczących bezpieczeństwa państwa wskazuje się, że operacje informacyjne prowadzi się równolegle z działaniami w sieciach informatycznych oraz z walką elektroniczną. Wymienione rodzaje działań, choć niejedyne, są w USA równoważnymi narzędziami polityki bezpieczeństwa państwa o nazwie *Informacja*,

37 M. Łokociejewski, W. Scheffs, *Walka elektroniczna w operacji i* walce, AON, Warszawa 2005, s. 10.

38 W. Scheffs, *Założenia walki elektronicznej w środowisku sieciocentrycznym* [w:] materiały z międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych* – 2008, AON, Warszawa 2008, s. 113.

39 L. Ciborowski, *Walka informacyjna*..., op.cit., s. 69.

40 Ibidem, s. 95.

41 Ibidem, s. 37.

42 Ibidem, s. 39.

43 *JP 3-0 Joint Operations*, United States Marine Corps, 17.09.2006, s. iv.

44 *Information environment – the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information*, *JP 3-0 Joint Operations*, United States Marine Corps, 17.09.2006, Glossary, s. GL-15.

45 *National Military Strategy for Cyberspace Operations – NMS-CO,* Joint Chiefs of Staff, Waszyngton 2006, s. 3.

46 *Połączona sojusznicza doktryna operacji informacyjnych* (*AJP-3.10*), Agencja Standaryzacji NATO (NSA), 2009, pkt 0126, pkt 0129.

jednymi z wielu elementów tworzących potęgę narodową Stanów Zjednoczonych[47].

Z przedstawionych przykładów wynika brak konsekwencji w umiejscawianiu dwóch najważniejszych rodzajów działań prowadzonych z wykorzystaniem urządzeń i systemów elektronicznych (tj. EW i CNO). Rozbieżność ta świadczy o ciągłym poszukiwaniu oraz kształtowaniu się poglądów w tej dziedzinie. Można też dostrzec złożoność tej problematyki i próby poszukiwania własnych (jak widać na amerykańskim przykładzie) rozwiązań, niekiedy rozbieżnych w stosunku do Sojuszu.

Daje się również zaobserwować dążenie do interpretowania walki informacyjnej jako *czwartego wymiaru wojny* M. Howarda. Otóż w 1995 roku Martin Libicki, pracownik National Defence University w Waszyngtonie, podzielił operacje informacyjne na siedem form (elementów)[48], czyli: wojnę w zakresie dowodzenia i kontroli (*Command and Control War* – C2W), wojnę wywiadowczo-rozpoznawczą (*Inteligence-Based War*), wojnę elektroniczną (*Electronic War*), wojnę hakerską (*Hacker War*), wojnę o informacje ekonomiczne (*Economic Information War*), wojnę cybernetyczną lub sieciową (*Cyber or Net War*) oraz operacje psychologiczne (*Psychological Operations*). Możemy odnaleźć tu prawie wszystkie obszary wykorzystania urządzeń i systemów elektronicznych, ale należy mieć cały czas na uwadze, że nie są one jedynymi elementami tych operacji.

Większość definicji walki i operacji informacyjnych, ujętych w amerykańskich oraz natowskich dokumentach normatywnych z lat dziewięćdziesiątych XX wieku i z pierwszej dekady XXI wieku, nie opisuje relacji (zależności) między walką informacyjną a urządzeniami i systemami elektronicznymi (walką elektroniczną oraz cyberprzestrzenią). Dlatego pojęcie *walka informacyjna* nie jest właściwe do opisywania działań z użyciem urządzeń i systemów elektronicznych, tzn. walka ta nie może być nazywana *czwartym wymiarem wojny*.

CYBERPRZESTRZEŃ – PRZESTRZEŃ CYBERNETYCZNA

Terminem, którego od pewnego czasu używa się na potrzeby nazwania pewnej części prowadzonych działań militarnych, jest określenie *cyberprzestrzeń*. Jaka jest zatem geneza tego pojęcia i jak zostało ono pierwotnie zdefiniowane? Spróbujmy to przeanalizować.

II wojna światowa przyspieszyła rozwój powiększającej się w szybkim tempie dziedziny nauki, do której głównych przedmiotów należy informacja. W 1947 roku Norbert Wiener jedną ze swoich prac zatytułował *Cybernetyka, czyli sterowanie i przesyłanie informacji u zwierząt i maszyn*. W tytule zamieścił zaczerpnięty z Platona (Georgiasz, 511)[49] termin *cybernetyka* (gr. *kybernetes* – sternik, zarządca).

Dynamiczne przeobrażenia techniki związanej z informacją i cybernetyką (w jej obecnym rozumieniu) nastąpiły zasadniczo przed II wojną światową i w jej trakcie, kiedy to do odwzorowania działań bojowych i wspomagania procesów decyzyjnych coraz szerzej rozpoczęto wykorzystywać takie dyscypliny naukowe, jak np.: psychologia, socjologia, badania operacyjne, oraz osiągnięcia rodzącej się wówczas cybernetyki i informatyki[50]. Potwierdzeniem tego faktu jest ogłoszony przez rząd brytyjski po zakończeniu II wojny światowej raport, w którym oceniono wpływ osiągnięć nauki na jej przebieg. Urządzenia elektroniczne (np. radar) oraz badania operacyjne uzyskały w nim jedną z najwyższych ocen, a choć zdobycze z zakresu cybernetyki i informatyki nie należały do tego elitarnego klubu, również zostały w nim ujęte. Dostrzeżono znaczenie ich istnienia i użyteczność, które stały się zrozumiałe zarówno dla szerokiego grona wojskowych, jak i polityków.

Aby skrócić czas przesyłania danych z rozpoznania radiolokacyjnego i ich zobrazowania na stanowiskach dowodzenia, a tym samym zyskać czas na podjęcie decyzji, w siłach powietrznych USA wprowadzono pod koniec lat pięćdziesiątych ubiegłego wieku komputery[51], które zautomatyzowały wiele procesów dotychczas powierzonych ludziom. W nowym systemie radary połączono z komputerami siecią sztywnych łączy stacjonarnych. Jak można było się domyślić, stanowiło to kamień węgielny dla przyszłych sieci komputerowych o dzisiaj znanej architekturze[52].

Konsekwencją rozwoju były również rozważania teoretyczne, które zostały przedstawione w wystąpieniu byłego sekretarza obrony USA Franka Carlucci w 1988 roku. Wskazał on w nim, że w niedalekiej przyszłości *inteligentna technika rażenia celów, zinte-*

47 Materiały z kursu pt. *Special Operations Forces Integration Course* przeprowadzonego w Akademii Obrony Narodowej (21–25.03.2011) przez przedstawicieli m.in. *Joint Special Operations University* z USA, s. 2.

48 A. Nowak, *Założenia dla perspektywicznego systemu rozpoznania*, AON, Warszawa 2004, s. 65 [za:] M. Libicki, *What is Information Warfare*, Washington 1995.

49 I. Ihnatowicz, *Człowiek. Informacja. Społeczeństwo*, Warszawa 1989, s. 9.

50 A. Barczak, *Komputerowe gry wojenne*, Warszawa 1996, s. 11.

51 Opracowany przez firmę IBM komputer Whirlwind II ważył 250 t i miał 49 tys. lamp próżniowych. D. Winkler, *Searching the Skies – the legacy of the United States Cold War Defense Radar Program,* USAF ACC, Langley 1997, s. 32.

52 Rozważania dotyczące automatycznego, komputerowego zbioru informacji pochodzących z systemu rozpoznania radiolokacyjnego systemu obrony powietrznej USA były bezpośrednim powodem opracowania koncepcji będącej pierwszą ideą (podstawą) współcześnie funkcjonującego Internetu. Projekt globalnej sieci komputerowej opisał w 1960 roku J. Licklider. Twórcą koncepcji Internetu jest Paul Baran, który w 1962 roku opublikował 12-tomową pracę będącą projektem wytrzymałych, rozproszonych (nie gwiaździstych) sieci cyfrowych transmisji danych, zdolnych przetrwać przewidywaną wówczas III wojnę światową, wykonanym na zlecenie amerykańskich sił zbrojnych.

growana informatycznie z automatycznymi procesami zbierania i przetwarzania informacji, stanowić będzie w niedalekiej przyszłości najważniejszy komponent ewentualnego pola walki[53].

Na początku lat dziewięćdziesiątych płk John A. Warden z sił powietrznych Stanów Zjednoczonych w teorii strategicznego paraliżu ujął działania w nowej przestrzeni nazwanej przez niego przestrzenią cybernetyczną. Obejmowała ona również działania w sieciach komputerowych. Warden postrzegał przeciwnika jako system systemów[54], składającego się z pięciu kręgów: elit politycznych (sprawujących ogólne kierownictwo); instytucji podstawowych (transponujących energię z jednego kręgu do drugiego); infrastruktury; społeczeństwa (ludzie) i systemów obronnych. Według niego każdą organizację (np.: państwo, firmę, wojsko, organizację terrorystyczną czy gang przestępczy) należy traktować jako strukturę składającą się z systemu pięciu wzajemnie powiązanych kręgów, tworzących całość i pełniących założone dla nich funkcje[55].

Każdy z kręgów Wardena funkcjonuje w pięciu wymiarach (rys. 1), na które składają się: morze, ląd, powietrze, przestrzeń kosmiczna, przestrzeń cybernetyczna (zwana również cyberprzestrzenią). Z opracowanego przez niego modelu wynika, że umiejscowienie w nim przestrzeni cybernetycznej potwierdza istnienie kolejnego wymiaru walki (tu w kolejności piątego ze względu na ujętą przestrzeń kosmiczną)[56]. Można wnioskować, że chociaż nie odniósł się on w żaden sposób do podziału dokonanego przez M. Howarda, to jego czwarty wymiar wojny w dużym uproszczeniu nazwał po prostu *przestrzenią cybernetyczną*.

Teoria Wardena znalazła odzwierciedlenie w oficjalnych amerykańskich poglądach dotyczących prowadzenia działań militarnych. Przykładem jest przyjęta w 2004 roku *Narodowa strategia militarna*, według której amerykańskie siły zbrojne muszą posiadać zdolność do prowadzenia operacji na lądzie, na morzu, w powietrzu, w Kosmosie i w cyberprzestrzeni, które razem tworzą przestrzeń walki (*battlespace*)[57]. Równocześnie z takim pojmowaniem podziału przestrzeni walki w innych amerykańskich dokumentach z 2006 roku wskazuje się, że *środowisko operacyjne*[58] składa się z domeny: lądowej, morskiej, powietrznej, kosmicznej oraz środowiska informacyjnego[59]. Przy ostatnim podziale podkreśla się, że traktowanie cyberprzestrzeni jako domeny stanowi wyznacznik rozumienia i definiowania jej miejsca w operacjach militarnych.

Na podstawie przytoczonych przykładów wyraźnie rysuje się pewnego rodzaju brak spójności w ówczesnym pojmowaniu przez amerykańskich teoretyków znaczenia i umiejscowienia cyberprzestrzeni w działaniach militarnych.

Należy pamiętać, że pojęcie *cyberprzestrzeń* sformułował w 1984 roku amerykański pisarz *science fiction* William Gibson[60] na potrzeby swojej powieści zatytułowanej *Neuromancer*. Na początku lat dziewięćdziesiątych weszło ono do powszechnego użytku. Obecnie jego znaczenie zmieniło się i oznacza ono głównie wirtualną przestrzeń, w której połączone siecią komputery, np. Internet lub inne media cyfrowe (telefonia komórkowa), wymieniają dane w cyfrowej postaci. Określa się też potocznie, że jest to przestrzeń informatyczna, a nie cybernetyczna. W relacjach społecznych cyberprzestrzeń jest synonimem nowego typu przestrzeni społecznej, w której spotykają się internauci.

Patrząc na naturalną ewolucję tego pojęcia, warto przedstawić kilka jego definicji:

– cyberprzestrzeń[61] (według NATO – 2007/2008) – cyfrowy świat stworzony przez komputery i sieci komputerowe, w którym współistnieją ze sobą ludzie i komputery, i który obejmuje wszystkie aspekty działalności w sieci komputerowej;

– cyberprzestrzeń[62] (Wielka Brytania – 2009 rok) – obejmuje wszystkie formy cyfrowych aktywności sieciowych, które są prowadzone w cyfrowych sieciach lub osiągane z wykorzystaniem cyfrowych sieci;

– cyberprzestrzeń[63] (według USA – 2010 rok) – jest globalną domeną zawartą w środowisku infor-

53 L. Ciborowski, *Nowe systemy i środki walki oraz kierunki ich rozwoju w SZ państw obcych*, AON, Warszawa 1993, s. 13.

54 System systemów – opracowana w USA pod koniec XX wieku koncepcja integrująca wiele elementów z dziedziny wojskowości, łączności, sieci komputerowych oraz z informatyki, którą nazwano później działaniami sieciocentrycznym (ang. *Network Centric Warfare* – NCW). M. Żukowski, *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Sieci teleinformatyczne w działaniach sieciocentrycznych* – 2006, AON, Warszawa 2007, s. 69.

55 M. Vego, *Systemowe kontra klasyczne podejście do działań bojowych*, „Kwartalnik Bellona" 2009 nr 2, s. 185.

56 P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość ?,* Kraków 2004, s. 374.

57 *The National Military Strategy of the USA,* Joint Chiefs of Staff, Waszyngton 2004, Rozdział 3. *Securing Battlespace*, s. 18.

58 *National Military Strategy for Cyberspace Operations – NMS-CO,* Joint Chiefs of Staff, Waszyngton 2006, s. 3.

59 *JP 3-0 Joint Operations*, United States Marine Corps, 17.09.2006, s. iv.

60 https://pl.wikipedia.org/wiki/William_Gibson_pisarz_science_fiction/. 20.06.2020.

61 *AC/322(SC/2-NC3TS)L(2007)0002*, *Definicje związane z cyberwojną*, 11.04.2007; *MC 571 – Koncepcja NATO w zakresie Cyberobronności*, 21.02.2008 [w:] *NATO Bi-SC Informator Operacji Informacyjnych v.1,* Allied Command Transformation, Norfolk 2010, s. 84.

62 *Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space,* The Parliamentary Bookshop, Londyn 2009, s. 7.

63 *Cyberspace Operations* (*DD 3-12*), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 51 [w:] *Joint Publication (JP) 1-02*, *Department of Defense Dictionary of Military and Associated Terms, USA*.

macyjnym, składającą się z niezależnej sieci informacyjnej opartej na infrastrukturze technologicznej, zawierającej Internet, sieci telekomunikacyjne i systemy komputerowe oraz wbudowane procesory i kontrolery.

Poglądy polskie (SZRP – 2013 rok) definiujące cyberprzestrzeń są sformułowane tak: *Jest to miejsce składające się z komputerów, urządzeń teleinformatycznych, współzależnych sieci telekomunikacyjnych i wszelkich mediów cyfrowych, w którym realizowane są procesy informacyjne*[64].

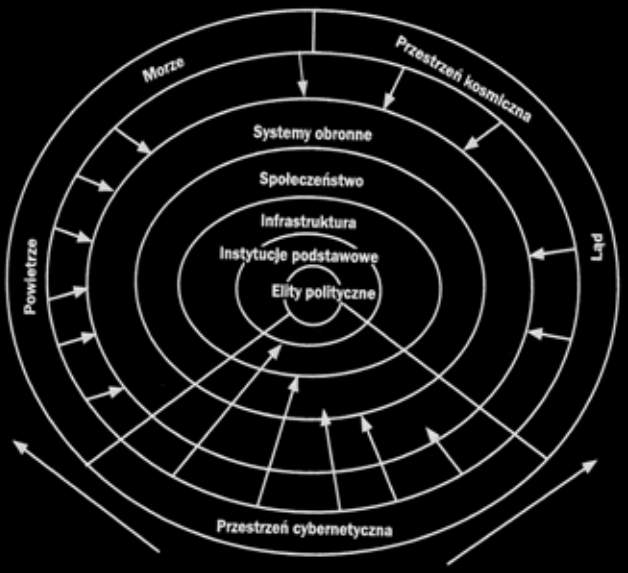
Ponadto na użytek prowadzonych rozważań zwraca uwagę pewien zapis, który rozszerza zdolności bojowe sił zbrojnych USA. Brzmi on następująco: *Integracja operacji cybernetycznych z innymi domenami*[65] [według USA – 2010] – *istotą tego procesu jest pozyskanie możliwości poszerzania zdolności pochodzących z pozostałych, poszczególnych domen w celu uzyskania unikalnych efektów, tzw. „efektów decyzyjnych". Wykorzystanie cyberprzestrzeni ewaluowało, obecny stan jego rozwoju stanowi potencjał, który umożliwia rozwiązywanie problemów nowymi metodami, co pozwala realizować zakładane narodowe cele. Obecnie wszystkie domeny działań militarnych są silnie powiązane przez cyberprzestrzeń* [rys. 2], *co należy uwzględniać w rozważaniach dotyczących współczesnych działań militarnych*[66].

Gdy zapoznamy się z materiałem pojęciowym dotyczącym cyberprzestrzeni, nasuwa się zasadnicze pytanie: czy pojęcie *cyberprzestrzeń* zasługuje na miano *czwartego wymiaru wojny*. Otóż nie. Ponieważ mimo zauważalnej ewolucji i powiększenia obszaru oddziaływania cyberprzestrzeni, we wszystkich sojuszniczych dokumentach doktrynalnych cały czas równolegle występowało pojęcie *walka elektroniczna*. Świadczy to o tym, że nie wszystkie urządzenia i systemy elektroniczne zostały wówczas podporządkowane funkcjonowaniu w cyberprzestrzeni.

PRZESTRZEŃ CZY ŚRODOWISKO?

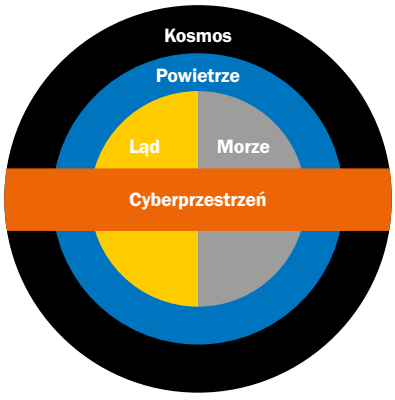
W różnych publikacjach bardzo często pojawiają się dwa pojęcia: *przestrzeń* oraz *środowisko*. Które z nich jest bardziej adekwatne do podziału działań militarnych? Wykorzystywanie pojęcia *przestrzeń* w naukach wojskowych wzięło swój początek w okresie, w którym szeroko posługiwano się analizą i modelowaniem matematycznym. Oto definicje

RYS. 1. WARDENOWSKI MODEL PIĘCIU WYMIARÓW WALKI



Źródło: P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość ?*, t. 1, Kraków 2004, s. 375.

RYS. 2. ZALEŻNOŚCI MIĘDZY DOMENAMI WEDŁUG TEORETYKÓW SIŁ POWIETRZNYCH USA



Źródło: *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA 2010, s. 20.

64 R. Janczewski, *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym* [w:] materiały z XX Konferencji Naukowej Automatyzacji Dowodzenia 2013, AON, Gdynia–Warszawa 2013, s. 101.

65 *Cyberspace Operations* (*DD 3-12*), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 19.

66 Ibidem. Wskazano, że taki sposób pojmowania zaczerpnięto z: Convertino Sebastian, *Flying and Fighting in Cyberspace*, lipiec 2007, Air University, s. 11.

POJĘCIE CYBERPRZESTRZENI SFORMUŁOWAŁ W 1984 ROKU AMERYKAŃSKI PISARZ *SCIENCE FICTION* WILLIAM GIBSON NA POTRZEBY SWOJEJ POWIEŚCI ZATYTUŁOWANEJ *NEUROMANCER*. NA POCZĄTKU LAT DZIEWIĘĆDZIESIĄTYCH WESZŁO ONO DO POWSZECHNEGO UŻYTKU.

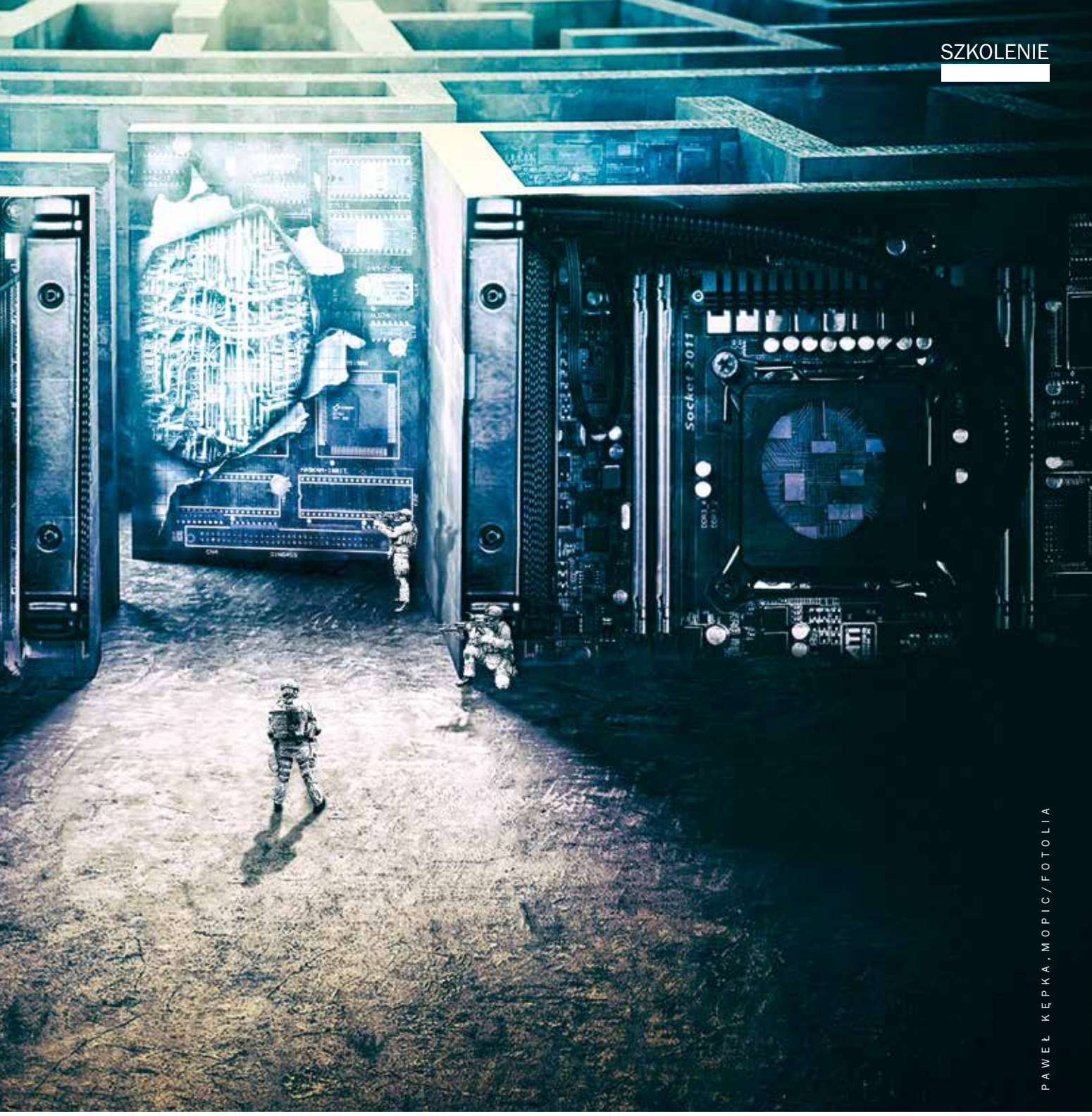
interesujących nas pojęć, sformułowane przez prof. L. Ciborowskiego:

– *przestrzeń*[67] – *zbiór dowolnych przedmiotów (liczb, stanów układu, wektorów itp.), między którymi zostały ustalone pewne relacje natury geometrycznej bądź abstrakcyjnej*;

– *środowisko walki* (*sfera walki*)[68] – *jest otoczeniem przedmiotu walki, gdzie jest on zlokalizowany. Stosownie do warunków panujących w otoczeniu należy wyodrębnić tylko takie narzędzia walki, które będą się nadawać do wykorzystania w tym środowisku (w tej sferze)*.

Na przykładzie definicji sformułowanych przez L. Ciborowskiego *przestrzeń* jest typowym pojęciem matematycznym wykorzystywanym do weryfikacji hipotez z zastosowaniem metod matematycznych

67 L. Ciborowski, *Walka informacyjna...*, op.cit., s. 8.
68 Ibidem, s. 100.



PAWEŁ KĘPKA, MOPIC/FOTOLIA

i jego użycie na potrzeby militarne nie do końca jest uzasadnione. Natomiast jego definicja *środowiska walki* jest bardziej uniwersalna i pozostaje dla prowadzonych tu rozważań jak najbardziej użyteczna. Jednocześnie należy zapoznać się i ocenić ogólne definicje środowiska podawane przez różne źródła, gdzie oznacza ono:

– *ogół elementów otoczenia*[69];

– *ogół wszystkich czynników otoczenia (ożywionych i nieożywionych), mniej więcej jednolitych na danym terenie, oddziałujących na organizmy żywe, ulegających zmianom pod wpływem tych organizmów*[70];

– *dopełnienie wyróżnionego systemu do całej przestrzeni, czyli zbiór wszystkich obiektów (wraz z ich atrybutami oraz relacjami między tymi atrybutami),*

69 J. Bralczyk, *Słownik 100 tysięcy słów*, Warszawa 2005, s. 829.

70 S. Dubisz, *Uniwersalny słownik języka polskiego*, Warszawa 2003, s. 731.

RYS. 3. UMIEJSCOWIENIE ŚRODOWISKA ELEKTRONICZNEGO

Źródło: S. Czeszejko, *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji,* AON, Warszawa 2011, s. 123.

RYS. 4. ZMODERNIZOWANY MODEL ODDZIAŁYWANIA J.A. WARDENA

Źródło: W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej* [w:] materiały z XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011, „Journal of KONBiN" 2011 nr 3 (19), s. 127.

które z uwagi na przyjęte kryteria przynależności do systemu nie zostały do niego zaliczone[71].

Z analizy przedstawionych definicji *przestrzeni* oraz *środowiska* nasuwa się wniosek, że bardziej odpowiednim pojęciem, które definiuje otoczenie prowadzenia działań militarnych, będzie określenie *środowisko*.

ŚRODOWISKO ELEKTRONICZNE

W piśmiennictwie anglojęzycznym można spotkać określenie *środowisko elektroniczne*. Autorzy publikacji używają go okazjonalnie i intuicyjnie, przy czym nie podają ani jego definicji, ani też umiejscowienia w podziale działań militarnych.

W tłumaczeniu książki Alfreda Price'a pt. *Narzędzia mroku. Historia walki radioelektronicznej 1939–1945*, wydanej w 1967 roku, można odnaleźć określenie *środowisko elektroniczne*[72], które autor utożsamia z funkcjonowaniem systemów radiolokacyjnych oraz radiowych. Takie pojęcie można spotkać w angielskojęzycznych opracowaniach również dzisiaj.

Przykładem współczesnego zastosowania na użytek militarny takiego sformułowania jest *Program rozwoju Marynarki Wojennej USA* z 2003 roku[73], gdzie w podrozdziale pt. *Pocisk AGM-88E AARGM* na stronie 123 użyto wyrażenia *electronic environment*[74], które w tłumaczeniu oznacza *środowisko elektroniczne*.

W rozważania teoretyczne aktywnie włączyli się także polscy oficerowie. Według poglądów jednego z oficerów byłego Dowództwa Sił Powietrznych *cyberprzestrzeń*[75] jest jedynie elementem działań militarnych, który poszerza i współtworzy istniejący już czwarty wymiar wojny Howarda (oparty głównie na walce elektronicznej). Otrzymał on nazwę: *środowisko elektroniczne*. Autor przedstawił również własny podział wymiarów wojny, który obejmuje środowisko (rys. 3)[76]: lądowe, morskie, powietrzne, elektroniczne (tworzy go walka elektroniczna oraz cyberprzestrzeń) i kosmiczne. Uważał, że taki podział wpłynie pozytywnie na zwiększenie efektywności wykorzystania urządzeń i systemów elektronicznych (ich synergii) na polu walki, w tym także świadomości sytuacyjnej. Ponadto wskazał, że urządzenia i systemy elektroniczne są wyróżnikiem oraz

71 B. Kaczorowski, *Wielka encyklopedia PWN*, t. 2, Warszawa 2005, s. 47.

72 A. Price, *Narzędzia mroku. Historia walki radioelektronicznej 1939–1945*, Wrocław 2006, s. 9.

73 *Roczny raport w zakresie kierowania, testów operacyjnych oraz rozwoju pt. FY 2003*, Ministerstwo Obrony Narodowej USA 2003, s. 123.

74 *The target sets must emulate the threat system in physical appearance as well as in the electronic environment.*

75 S. Czeszejko, *Konflikty ery informacyjnej*, „Przegląd Sił Powietrznych" 2011 nr 6, s. 9.

76 Idem, *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa 2011, s. 123.

wspólnym mianownikiem działań militarnych prowadzonych w środowisku elektronicznym.

Natomiast w swojej pracy końcowej z czerwca 2011 roku, powstałej w trakcie Podyplomowych Studiów Operacyjno-Strategicznych w AON, kwalifikuje w środowisku elektronicznym działania na prowadzone[77]: z wykorzystaniem energii elektromagnetycznej, w cyberprzestrzeni (sieciach komputerowych), z użyciem urządzeń i systemów elektronicznych oraz różne interakcje między środowiskiem elektronicznym a pozostałymi środowiskami.

Specyfiką środowiska elektronicznego jest to, że podejmowane w nim działania mogą wchodzić w interakcję z innymi środowiskami walki, np. narzędzia walki (lub szerzej: narzędzia działań w środowisku elektronicznym – urządzenia i systemy elektroniczne) mogą być niszczone z użyciem narzędzi przynależnych naturalnie do innych środowisk (np. niszczenie ogniem artylerii nadajników zakłóceń elektronicznych). Innym przykładem jest wykrywanie obiektów powietrznych z zastosowaniem pochodzącego z radaru promieniowania elektromagnetycznego (echa), gdzie zachodzi interakcja między przedmiotem walki środowiska elektronicznego (wypromieniowany sygnał elektromagnetyczny, następnie odbiór jego odbitej formy, tzw. echa) a środowiskiem powietrznym (obiekt powietrzny odbijający wypromieniowany sygnał elektromagnetyczny).

Aby prawidłowo interpretować prowadzone rozważania, autor zdefiniował takie pojęcia, jak[78]:

– *środowisko elektroniczne* (środowisko prowadzenia działań elektronicznych) – jest ono otoczeniem sygnałów elektrycznych oraz pochodzącego od nich promieniowania elektromagnetycznego (przedmiotów walki lub przedmiotów działań w środowisku elektronicznym), w którym można je wykorzystywać oraz na nie oddziaływać. Narzędziami oddziaływania (walki) w tym środowisku będą urządzenia i systemy elektroniczne (głównie militarne), które będą się nadawać do użycia w nim;

– *urządzenia i systemy elektroniczne* – to zasadnicze elementy środowiska elektronicznego, które należy rozumieć jako zbiór elementów nieożywionych powstałych w wyniku działalności człowieka, występujących w określonym umiejscowieniu, między którymi mogą istnieć wzajemne powiązania oraz mogą występować wzajemne oddziaływania; mogą one również pozostawać we wzajemnej zależności – stosownie do panujących warunków.

Z kolei były wykładowca Akademii Obrony Narodowej płk Waldemar Scheffs w swoim wystąpieniu w trakcie konferencji w październiku 2011 roku zaproponował unowocześnienie *modelu Wardena* przez zastąpienie pojęcia *przestrzeń cybernetyczna* określeniem *środowisko elektroniczne*. Dodatkowo postulował on podział piątego kręgu tego modelu (*środowisko elektroniczne*) na dwie części (rys. 4)[79]: środowisko elektromagnetyczne (środowisko EM) oraz środowisko cybernetyczne.

Natomiast w opracowaniu pt. *Środowisko działania walki elektronicznej* z 2015 roku W. Scheffs zwiększył liczbę elementów składowych środowiska elektronicznego i zaproponował jego nowy podział (rys. 5)[80] na: środowisko elektromagnetyczne, środowisko informatyczne (cybernetyczne/cyberprzestrzeń) oraz środowisko walki elektronicznej. Ponadto autor wspomnianego opracowania sformułował definicję środowiska elektronicznego. Brzmi ona następująco[81]: *środowisko elektroniczne – to otoczenie materii nieożywionej (urządzeń elektronicznych) działających w określonym obszarze, w którym występuje przesyłanie i odbiór sygnałów elektrycznych (przebiegów prądowych) oraz generowane są sygnały elektromagnetyczne*.

Nadmienić należy, że w trakcie badań literatury przedmiotu oraz dokumentów normatywnych nie natrafiono na żadne inne definicje środowiska elektronicznego niż przedstawione. Biorąc pod uwagę powiązanie *środowiska elektromagnetycznego* ze *środowiskiem walki elektronicznej* oraz z aktualnie obowiązującymi definicjami tych pojęć, należy uznać, że stanowią one jedno wspólne środowisko. Inaczej mogło by być tylko w wypadku, gdy zmagania w środowisku informatycznym/cybernetycznym/cyberprzestrzeni (m.in. stosowanie wirusów) oraz w środowisku elektromagnetycznym (np. zakłócenia radioelektroniczne[82] itp.) uznamy jednocześnie za prowadzenie walki elektronicznej. Wówczas byłaby konieczna zmiana wszystkich definicji, przy czym nie sposób walki elektronicznej nazwać środowiskiem. Mogłaby ona uzyskać jedynie statut *działań*, ale nie ma podstaw, by nazwać ją środowiskiem.

ŚRODOWISKO SIECIOCENTRYCZNE – SIECIOCENTRYCZNOŚĆ

Kolejnym pojęciem, które w pewnym stopniu ma związek z wykorzystywaniem urządzeń i systemów elektronicznych, jest *sieciocentryczność*. Autorami

77 Idem, *Działania elektroniczne, a świadomość sytuacyjna pola walki* [w:] materiały z XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011, „Journal of KONBiN" 2011 nr 2, s. 11.

78 Idem, *Radar surveillance in the electronic environment of the 21st century* [w:] materiały z *15th International Radar Symposium IRS-2014*, Gdańsk 2014, s. 321.

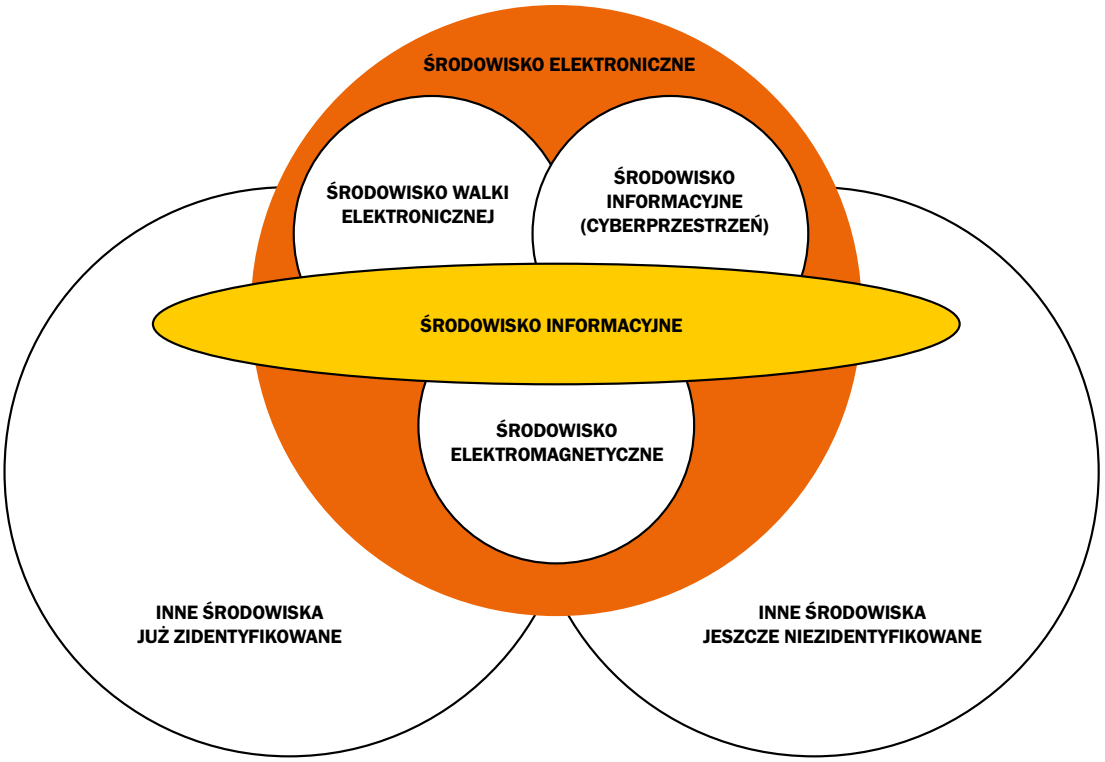
79 W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej* [w:] materiały z XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011, „Journal of KONBiN" 2011 nr 3, s. 127.

80 Idem, Środowisko działania walki elektronicznej, Warszawa 2015, s. 28.

81 Ibidem, s. 40.

82 Nazwa według aktualnie obowiązującej w SZRP frazeologii zawartej w dokumentach normatywnych.

RYS. 5. ŚRODOWISKA SZTUCZNE ZIDENTYFIKOWANE NA POTRZEBY UŻYCIA ŚRODKÓW ELEKTRONICZNYCH W DZIAŁANIACH MILITARNYCH



Źródło: W. Scheffs, *Środowisko działania walki elektronicznej,* Warszawa 2015, s. 28.

pierwszej definicji sieciocentryczności byli J. Garstka, D. Alberts i F. Stein, których uważa się za jednych z prekursorów tej koncepcji. W największym skrócie opiera się ona na skupianiu siły, która może być wygenerowana przez efektywne połączenie (sieciowanie) elementów ugrupowania bojowego[83] (w tym z wykorzystaniem urządzeń i systemów elektronicznych, głównie łączności i teleinformatyki).

Autorzy uważają również, że zaistniała konieczność odejścia od używania pojęcia *pole walki* na rzecz określenia *środowisko walki sieciocentrycznej* jako *przestrzeni realizacji zadań*. W przestrzeni tego rodzaju nie będzie występować wyraźna granica między walczącymi żołnierzami a ludnością cywilną. W związku z tym walkę sieciocentryczną należy traktować jako element szerzej definiowanej walki informacyjnej[84].

Należy mieć na uwadze, że obecnie dość swobodnie używa się pojęcia *środowisko*, bez podania w dokumentach normatywnych jego definicji. Ogólny jego sens w wypadku używania w określonym kontekście jest zrozumiały. Jednak by nazewnictwo precyzyjnie oddawało istotę danego terminu, jest potrzebny oficjalny i jednoznaczny system zdefiniowanych pojęć.

Poddajmy analizie dostępne definicje związane z sieciocentrycznością, w tym *środowiska sieciocentrycznego*:

83 J. Garstka, D. Alberts, F. Stein, *Network Centric Warefare*, DoD C4ISR Cooperative Research Program, Washington D.C. 2000, s. 88 [w:] S. Zajas (red. nauk.), *Studium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa 2009, s. 21.

84 Ibidem.

– *sieciocentryczność*[85] (według AON – 2007 rok) – *w ujęciu informatycznym (systemowym) to integracja z innymi systemami (fuzja informacji) prowadząca do utworzenia jednego wspólnego systemu (nadsystemu)*;

– *środowisko sieciocentryczne*[86] (według AON – 2008 rok) – *zespół czynników wynikających z głębokich przemian w wyposażeniu wojsk oraz połączenia sieciowego wszystkich uczestniczących w działaniach sił, od żołnierza i pojazdu do najwyższych szczebli włącznie. Stwarzając określone warunki, które wpływają na zachodzące w działaniach wojsk (innych uczestników) zjawiska, sprzężenia i interakcje, determinują charakter dowodzenia i sposób prowadzenia działań, nadając im nowe specyficzne cechy*;

– *środowisko sieciocentryczne*[87] (według AON – 2013 rok) – *środowisko zaawansowanych systemów wspomagania procesów informacyjno-decyzyjnych wykorzystywane na potrzeby sił zbrojnych. Powstanie i rozwój koncepcji prowadzenia działań w środowisku sieciocentrycznym wymuszone zostały przemianami zachodzącymi w świecie technologii informatycznych oraz wzrostem znaczenia informacji jako czynnika odgrywającego niezwykłą rolę we współczesnych konfliktach zbrojnych.*

Sieciocentryczność jako nowa idea prowadzenia działań bojowych, co można zaobserwować w ostatnich latach, znajduje się jeszcze na etapie koncepcyjnym[88]. Oceniając ją i mając na uwadze interesujące nas wykorzystanie urządzeń i systemów elektronicznych, można stwierdzić, że działania sieciocentryczne swoim znaczeniem najbardziej są zbliżone do walki informacyjnej. Należy zauważyć, że zasadnicza różnica polega na tym, iż sieciocentryczność opiera się w głównej mierze na wykorzystaniu urządzeń i systemów elektronicznych z obszaru łączności i teleinformatyki.

Umiejscowienie środka ciężkości na najważniejszych aspektach walki informacyjnej polega na tym, że urządzenia i systemy elektroniczne są głównie źródłami informacji, natomiast w działaniach sieciocentrycznych ich podstawowym zadaniem jest elektroniczne *spinanie* wszystkich elementów ugrupowania bojowego w całość, z czego wojsko czerpie dodatkową siłę. Jednak w obu wypadkach zasadniczym przedmiotem działania jest informacja, a nie urządzenia i systemy elektroniczne. Wszystko wskazuje na to, że w pierwszym etapie swego (jeszcze nienazwanego) istnienia (rozwoju) sieciocentryczność była (w obu przypadkach niejednokrotnie poprzez niezależne od siebie wykorzystanie komputerów):

– walką informacyjną opartą na użyciu środków łączności i wspieraniu procesów związanych ze zdobywaniem informacji;

– przetwarzaniem i dystrybucją informacji.

Dopiero połączenie tych dwóch nurtów rozwojowych w jedno rozwiązanie systemowe stworzyło warunki do utworzenia koncepcji sieciocentryczności.

Sieciocentryczność w żaden sposób nie pretenduje do czwartego wymiaru wojny, ponieważ jej głównym celem jest umożliwienie osiągania większej synergii działań militarnych prowadzonych we wszystkich wymiarach jednocześnie, a nie prowadzenie działań w nowym, kolejnym wymiarze wojny. Ponadto, rozpatrując podział na środowiska walki, zakładanym (docelowym) efektem zastosowania sieciocentryczności jest uzyskanie jednego wspólnego super *środowiska sieciocentrycznego*, które zastąpi wszystkie dotychczasowe środowiska walki.

DZIAŁANIA CYBERNETYCZNO-ELEKTROMAGNETYCZNE

Kolejnym krokiem w rozwoju poglądów amerykańskich, przedstawionych w dokumencie doktrynalnym pt. *Cyberspace Operations (DD 3-12)* z 2010 roku, w którym wskazano na wstępne zależności między domenami operacyjnymi w trakcie działań wojennych według teoretyków sił powietrznych USA (rys. 5), jest aktualizacja tego dokumentu z 30 listopada 2011 roku. W wydaniu tym przedstawiono nowe podejście systemowe zawarte w załączniku *Annex* 3-12 – *Cyberspace Operations*[89]. Cyberprzestrzeń oraz spektrum elektromagnetyczne ujęto w nim (zamknięto) w jednym wspólnym obszarze (rys. 6).

Nowy wymiar działań militarnych nie został nazwany przez teoretyków SP USA, ale cyberprzestrzeń oraz spektrum elektromagnetyczne określono w nim jako przenikający się wzajemnie obszar (przestrzeń, środowisko, domena). Idąc tym tropem, w siłach zbrojnych USA utworzono na szczeblu strategicznym komórkę wewnętrzną o nazwie Centrum Broni Połączonych Wojsk Lądowych USA (*United States Army Combined Arms Center* – US ACAC)[90], które jest odpowiedzialne za wydawanie doktryn i innych dokumentów normatywnych na potrzeby broni połączonych (*Combined Arms Doctrine Directorate*). Jednym

85 M. Żukowski, *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Sieci teleinformatyczne w działaniach sieciocentrycznych*, AON, Warszawa 2007, s. 70.

86 J. Posobiec, *Dowodzenie w środowisku sieciocentrycznym,* rozprawa habilitacyjna, „Zeszyty Naukowe AON" 2008, s. 52.

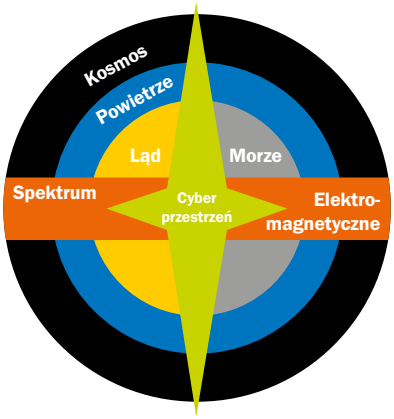
87 K. Frącik, *Proces dowodzenia jako zasadniczy komponent systemu dowodzenia w uwarunkowaniach środowiska zaawansowanych systemów wspomagania procesów informacyjno-decyzyjnych* [w:] materiały z XX Konferencji Naukowej Automatyzacji Dowodzenia, AON, Gdynia–Warszawa 2013, s. 24.

88 S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych*, AON, Warszawa 2008, s. 69.

89 *Annex 3-12 – Cyberspace Operations",* Curtis E. Lemay Center for Doctrine Development and Education, 30.11.2011.

90 http://usacac.army.mil/. 11.10.2014.

RYS. 6. ZALEŻNOŚCI MIĘDZY DOMENAMI WEDŁUG TEORETYKÓW SIŁ POWIETRZNYCH USA



Źródło: *Annex DD 3-12 – Cyberspace Operations*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA 2011, s. 18.

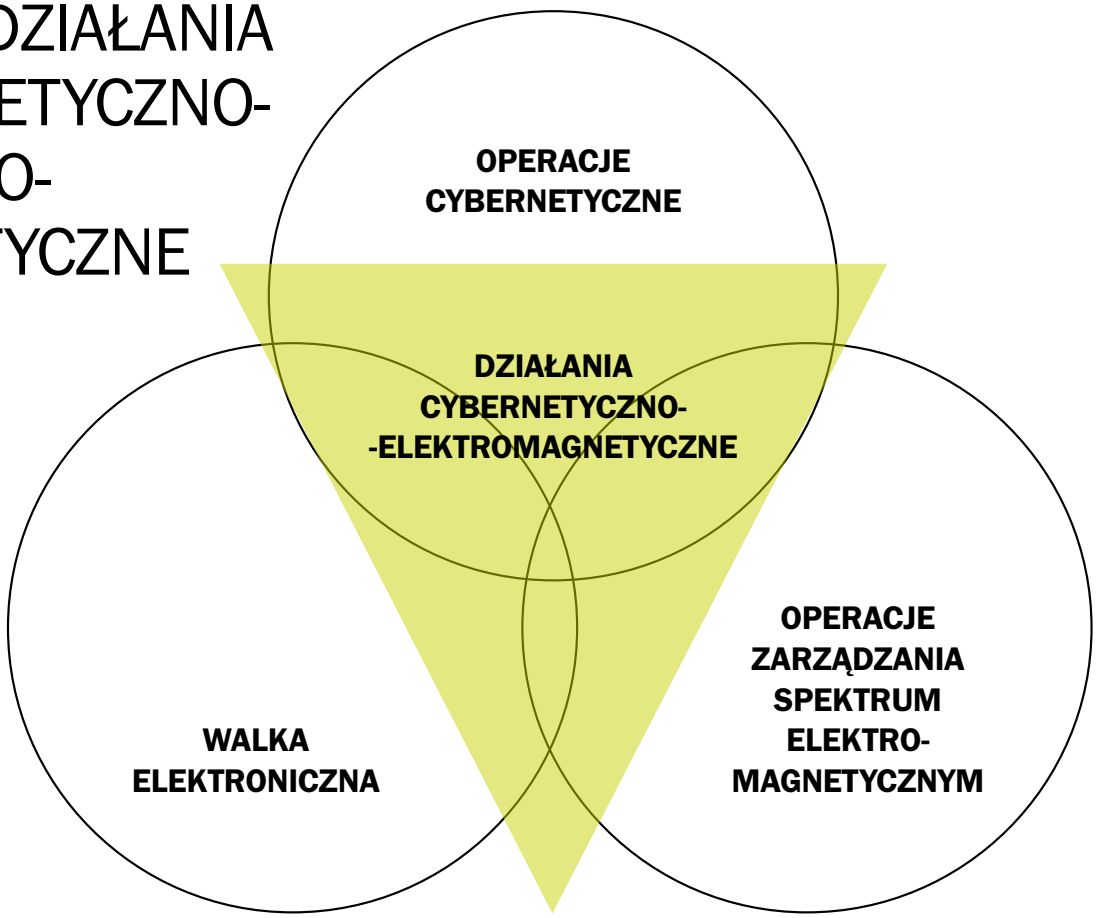
z najnowszych dokumentów Centrum, opracowanym na podstawie nowych założeń teoretycznych, jest podręcznik *FM 3-38 Cyber Electromagnetic Activities*[91], który dotyczy rozszerzenia zakresu odpowiedzialności każdego dowództwa wojsk lądowych USA.

Zgodnie z zapisami ujętymi w podręczniku do zadań dowódcy wojsk lądowych USA i jego sztabu należy również prowadzenie działań cybernetyczno-elektromagnetycznych (*Cyber Electromagnetic Activities* – CEMA)[92], w skład których wchodzi prowadzenie (rys. 7): operacji cybernetycznych (*Cyberspace Operations* – CO), walki elektronicznej (*Electronic Warfare* – EW) oraz operacji zrządzania spektrum elektromagnetycznym (*Spectrum Management Operations* – SMO).

Działania cybernetyczno-elektromagnetyczne (*Cyber Electromagnetic Activities* – CEMA) są definiowane jako *aktywność o rozszerzonym zakresie, zachowywanie i wykorzystywanie przewagi nad przeciwni-*

91 *FM 3-38 Cyber Electromagnetic Activities*, Department of the Army, Waszyngton D.C. 12.02.2014.
92 Ibidem, s. 1-1.

RYS. 7. DZIAŁANIA CYBERNETYCZNO--ELEKTRO-MAGNETYCZNE



Źródło: *FM 3-38 Cyber Electromagnetic Activities*, Department of the Army, Waszyngton D.C. 12.02.2014, s. 1–2.

kiem w dwu zakresach: cyberprzestrzeni oraz spektrum elektromagnetycznym, w czasie jednoczesnego wypierania i degradacji przeciwnika przy wykorzystaniu obu zakresów (cyberprzestrzeni i spektrum elektromagnetycznego) oraz ochrona własnego systemu dowodzenia[93]. W definicji nie wspomina się o niezbędnym elemencie koordynacji tej działalności, tj. o operacjach zrządzania spektrum elektromagnetycznym (*SMO*), które przywołuje się dopiero w kolejnym punkcie dokumentu w ramach formułowania zadania dla dowódcy i jego sztabu w zakresie integracji CEMA.

Czy w koncepcji CEMA nie widać analogii do założeń przedstawionych przez polskich oficerów? Jest ona wyraźna, na co wskazuje przyjęty podział elementów składowych tego rodzaju działań. Ale podobne jest coś jeszcze, czego dotychczas tutaj nie opisano: zaakcentowanie wyraźnej potrzeby koordynacji funkcjonowania poszczególnych elementów zarówno w środowisku elektronicznym (SZRP), jak i w ramach prowadzenia działań cybernetyczno-elektromagnetycznych (CEMA – WLąd USA). Z tego wynika, że mamy istotne osiągnięcia, nie odstajemy w innowacjach od czołówki światowej.

Według teoretyków amerykańskich podział wymiarów wojny powinien obejmować następujące środowiska: lądowe, morskie, powietrzne, operacji cybernetycznych, walki elektronicznej, operacji zarządzania spektrum elektromagnetycznym (*Spectrum Management Operations* – SMO) i kosmiczne. W tym wypadku również dyskusyjne jest to, czy walka elektroniczna oraz operacje zrządzania spektrum elektromagnetycznym nie powinny być traktowane jako jedno wspólne środowisko?

ŚRODOWISKO CZY DOMENA?

Jak już wspomniano, w polskojęzycznej literaturze przedmiotu najadekwatniejszą nazwą wykorzystywaną do podziału działań militarnych jest określenie *środowisko*. Jednak coraz częściej spotyka się pojęcie *domena*, szczególnie w połączeniu z określeniem *cyberprzestrzeń* (*Cyber Domain*). Z analizy dostępnej literatury anglojęzycznej wynika, że w żadnym z militarnych dokumentów normatywnych nie zawarto definicji pojęcia *domena*, co potwierdza oficer kanadyjskich sił zbrojnych mjr Gary Wolfman[94], który również jej poszukiwał. Dlatego też konieczne było sprawdzenie w dostępnych słownikach anglojęzycznych definicji tego pojęcia. Ma ono kilka znaczeń. Oto niektóre z nich:

Pojęcie *cyberprzestrzeń* odgrywa wiodącą rolę w obecnie używanej specjalistycznej terminologii, choć, jak wykazano, zdania teoretyków i poglądy na ten temat są jeszcze na etapie kształtowania się.

93 *ADRP 6-0 Mission Command*, Department of the Army, Waszyngton D.C. 17.05.2012, pkt 3-23, s. 3-6.

94 G. Wolfman, *Don't fire until you see the whites of their 1s: proposing a component-level targeting cycle for Cyberspace Operations*, Canadian Forces College, Minister of National Defence, 2019, https://www.cfc.forces.gc.ca/259/290/405/305/wolfman.pdf, s. 3/. 30.08.2020.

RYS. 8. PODZIAŁ DOMEN WALKI WEDŁUG NATO – 2018 ROK

Opracowano na podstawie: *Allied Joint Doctrine for Cyberspace Operations (AJP 3-20)*, Edition A Version 1, NATO Standardization Office (NSO)2018, pkt 1.16, s. 5.

– obszar charakteryzujący się specyficznymi cechami, typem pokrycia lub dzikiego świata zwierzęcego itp.[95];

– obszar zainteresowania lub obszar, nad którym osoba sprawuje kontrolę[96]*;*

– obszar pewnego terytorium, pozostający w posiadaniu lub kontroli szczególnego władcy lub rządu[97]*;*

– szczególny obszar myślenia, działania lub interesów, przede wszystkim ten, nad którym ktoś ma kontrolę, posiada na niego wpływ lub ma do niego prawa[98].

Z przytoczonych definicji wynika, że nie są one jednoznacznie pasującymi do podziału działań militarnych i nie są do końca adekwatne do określenia *środowisko*. Jednak z perspektywy użytkowników języka angielskiego wynika, że mimo zawiłości słownikowych pojęcie *domena* jest rozumiane i użytkowane podobnie do naszego *środowiska*. Jest też ono przenoszone do słownictwa polskiego w bezpośredniej formie *domena.* Nie unikniemy tego w praktyce, więc musimy się do tego przyzwyczaić i powinniśmy ten fakt zaakceptować. Jednak należy mieć na uwadze, że obowiązuje nas ustawa z 7 października 1999 roku o języku polskim z późniejszymi zmianami, dlatego w dokumentach normatywnych należy używać pojęcia *środowisko* z uzupełnieniem w nawiasie *domena*, wówczas zachowamy stosowną pisownię wraz z bezpośrednim transponowaniem rozumienia z języka angielskiego.

W bezpośrednim kontakcie z dokumentami NATO ułatwi nam to rozumienie kontekstu, co działa jednocześnie w drugą stronę. W trakcie analizy natowskich dokumentów lub innych anglojęzycznych wydawnictw wystąpi natychmiastowe skojarzenie w odniesieniu do pojęć obowiązujących oficjalnie w SZRP.

DOMENA CYBERPRZESTRZENI

Pojęcie *przestrzeń cybernetyczna* (*cyberprzestrzeń*) zasadniczo funkcjonuje już na stałe w dokumentach normatywnych dotyczących bezpieczeństwa. W sojuszniczych poglądach odnoszących się do prowadzenia operacji cybernetycznych możemy nie tylko znaleźć definicję cyberprzestrzeni, lecz napotykamy tam również odmienny podział środowisk (domen) walki, których wymienia się obecnie cztery[99], tj. domenę (rys. 8): morską, lądową, powietrzno-kosmiczną (ujętą jako jedna domena) oraz cyberprzestrzeni. Należy mieć przy tym na uwadze, że domeny te w ramach prowadzenia operacji cybernetycznych pogrupowano na[100]: cyberprzestrzeń oraz domeny fizyczne[101].

W najnowszych dokumentach cyberprzestrzeń zdefiniowano następująco:

– cyberprzestrzeń (według NATO – 2018 rok)[102] – *globalna domena składająca się z wszystkich połączonych ze sobą technologii komunikacyjnych, informacyjnych oraz innych systemów i sieci elektronicznych (i ich zasobów danych), w tym tych, które są odseparowane i niezależne, które również przetwarzają, przechowują lub przesyłają dane*[103];

– cyberprzestrzeń [według European Union Military Staff (EUMS) – 2019 rok][104] – *wirtualna globalna i wspólna domena, zawierająca się w środowisku informacyjnym składającym się zarówno z wszystkich sieci połączonych ze sobą (współzależnych), jak*

95 *A region characterized by a specific feature, type of growth or wildlife, etc.*, https://www.dictionary.com/browse/domain/. 30.08.2020.

96 *An area of interest or an area over which a person has control,* https://dictionary.cambridge.org/dictionary/english/domain/. 30.08.2020.

97 *An area of territory owned or controlled by a particular ruler or government,* https://www.lexico.com/definition/domain/. 30.08.2020.

98 *A particular field of thought, activity, or interest, especially one over which someone has control, influence, or rights*. Źródło: https://www.collinsdictionary.com/dictionary/english/domain/. 30.08.2020.

99 *Allied Joint Doctrine for Cyberspace Operations* (*AJP 3-20*), Edition A Version 1, NATO Standardization Office (NSO), 2018, pkt 1.14, s. 5.

100 Ibidem, pkt 1.16, s. 5.

101 Do domen fizycznych zaliczono domenę: morską, lądową, powietrzną i kosmiczną (ujęte jako jedna domena: powietrzno-kosmiczna).

102 *Allied Joint Doctrine for Cyberspace Operations* (*AJP 3-20*), Edition A Version 1, NATO Standardization Office (NSO), 2018, pkt 1.13, s. 4.

103 *Cyberspace – the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data*.

104 *EUMC Glossary of Acronyms and Definitions – Revision 2019*, European Union Military Committee, EEAS (2020) Rev 2, 2020, litera "C", s. 68.

i niezależnych sieci, opartych na globalnej, organizacyjnej i narodowej infrastrukturze informacyjnej, funkcjonującej na podstawie Internetu i sieci telekomunikacyjnych, poszerzanej przez inne sieci, systemy komputerowe i osadzone w nich procesory, oraz zawierająca również samodzielne systemy i sieci[105].

Przy tym nieustająco w dokumentach normatywnych definiuje się pojęcie *walki elektronicznej* oraz *środowiska elektromagnetycznego*, które funkcjonują jednocześnie z pojęciem *cyberprzestrzeń*.

PODSUMOWANIE

Odnotowany dynamiczny rozwój różnorodnych militarnych urządzeń i systemów elektronicznych przyczynił się jednocześnie do powstania coraz bardziej skomplikowanych relacji na polu walki do takiego stopnia, że niektórych rodzajów działań bez ich wykorzystania nie można już prowadzić w sposób wysoce efektywny (charakterystyczny dla ery tzw. konfliktów informacyjnych)[106]. Potwierdzają to wnioski z ostatnich konfliktów zbrojnych, z których wynika jednoznacznie, że nastąpił wzrost znaczenia nowego wymiaru prowadzenia działań militarnych. Szczególne znaczenie miała tutaj pierwsza wojna w rejonie Zatoki Perskiej, którą określono mianem pierwszej tzw. wojny informacyjnej. Stanowi ona doskonały przykład ogromnego wpływu elektronicznych systemów rozpoznania, łączności i automatyzacji dowodzenia na efektywność bojową wojsk. Na świecie dostrzeżono wówczas znaczącą rolę najnowocześniejszych technologii elektronicznych i ich wpływ na funkcjonowanie systemów militarnych (zwłaszcza wykorzystywanych na rzecz systemów informacyjnych) oraz ukształtował się charakter przyszłych wojen, w trakcie których dominującą rolę zaczęły odgrywać jednocześnie telekomunikacja, informatyka oraz teleinformatyka. Dowodem utrzymywania się tego trendu jest przebieg drugiej wojny w rejonie Zatoki Perskiej.

Jak wskazują niektórzy specjaliści na przykładzie działań sieciocentrycznych[107], rozbieżność terminologiczna jest cechą charakterystyczną dla polskojęzycznej literatury przedmiotu. Charakteryzuje to również literaturę innych państw, co wynika z dynamiki rozwoju urządzeń i systemów elektronicznych oraz ich zastosowania w działaniach militarnych. Przekłada się to pośrednio na zmiany sposobów prowadzenia walki z ich użyciem, które mają bezpośredni wpływ na zasady walki (np. walki radioelektronicznej), te natomiast są częścią składową zasad sztuki wojennej. Nie pozostaje to niezauważone również przez polskich specjalistów. Opisuje to w swojej pracy S. Markiewicz[108], który zaznacza przy tym wyraźnie, że Z. Galewski wskazuje na fakt weryfikacji reguł prowadzenia tego rodzaju walki w trakcie konfliktów zbrojnych[109]. Należy jednak pamiętać, że nie same zasady sztuki wojennej, nawet najnowocześniejsze, lecz umiejętne ich zastosowanie w walce może doprowadzić do pokonania przeciwnika.

W interdyscyplinarny charakter działań, w których wykorzystuje się urządzenia i systemy elektroniczne, wpisuje się wiele dziedzin, dyscyplin i specjalności naukowych, a ich systemowe i kompleksowe postrzeganie pozwala na ich pełne zrozumienie. Uwzględnianie w rozważaniach aspektów techniki oraz technologii dotyczących urządzeń i systemów elektronicznych pozwala na dogłębne zbadanie następstw przyczynowo-skutkowych w tej dziedzinie, które determinują również stosowaną na jej użytek terminologię.

Mimo rozwijania różnych teorii i będących ich konsekwencją rozwiązań systemowych w zakresie wykorzystania urządzeń i systemów elektronicznych oraz ich wpływu na działania militarne, należy pamiętać, że istota zadań poszczególnych rodzajów sił zbrojnych w przyszłych operacjach pozostanie taka sama, może zostać ona jedynie nieznacznie zmodyfikowana w zależności od warunków, jakie będą towarzyszyć realizacji stojących przed nimi zadań.

WNIOSKI

Pojęcie *cyberprzestrzeń* odgrywa wiodącą rolę w obecnie używanej specjalistycznej terminologii, choć jak wykazano, zdania teoretyków i poglądy na ten temat są jeszcze na etapie kształtowania się. Niemniej konieczne jest sformułowanie wniosków, które pomogą ukierunkować dalsze działania w tej dziedzinie. Do najważniejszych należy zaliczyć:

- wśród specjalistów nastąpiło przekierowanie i silne wybiórcze skupienie się nad aktualnym problemem: *cyberprzestrzenią* – dynamicznym rozwojem systemów teleinformatycznych (m.in. kompute-

105 *Cyberspace – the virtual global and common domain within the information environment consisting of all interconnected and interdependent networks of global, organizational and national information infrastructure, based on the Internet and telecommunications networks, to be extended by other networks, computer systems and embedded processors, and containing also stand-alone systems and networks.*

106 Oczywiście możliwe jest prowadzenie działań militarnych bez użycia urządzeń i systemów elektronicznych, ale oznacza to znaczne zmniejszenie ich efektywności i automatyczne cofnięcie się do okresu poprzedzającego erę tzw. konfliktów informacyjnych.

107 J. Janczak, *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Sieci teleinformatyczne w działaniach sieciocentrycznych* – 2006, AON, Warszawa 2007, s. 23.

108 S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych* 2008, AON, Warszawa 2008, s. 64.

109 Z. Galewski, *Czynniki powodzenia we współczesnej walce*, Warszawa, 1986, s. 152 [za:] S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych* [w:] materiały z międzynarodowej konferencji naukowej nt. *Walka elektroniczna w działaniach sieciocentrycznych* 2008, AON, Warszawa 2008, s. 64.

Twórcze zastosowanie zasad sztuki wojennej z wykorzystaniem najnowszych środków walki może doprowadzić do szybkiego pokonania przeciwnika.

AFCENT

rów, baz danych, sieci komputerowych itp.) – który obecnie stanowi rzeczywiście istotne wyzwanie. W związku z tym doszło do tego, że w odniesieniu do działań zbrojnych nadano jej rangę środowiska (domeny), podobnie jak to miało wcześniej miejsce w przypadku walki elektronicznej, którą obecnie całkowicie pominięto w tym podziale;

• brak jednoznacznego umiejscowienia na tle działań zbrojnych wszystkich militarnych przedsięwzięć realizowanych z wykorzystaniem urządzeń i systemów elektronicznych (m.in. cyberprzestrzeni czy walki elektronicznej) jako całości (jedno środowisko, domena), co powoduje chaos informacyjny, rozpoczynający się niestety już w dokumentach normatywnych (m.in. doktrynach czy regulaminach). Dlatego konieczny jest ostateczny podział działań militarnych według nowego wzorca, prowadzonych w poszczególnych środowiskach, precyzyjnie zdefiniowanych i opisanych;

• konieczność i konsekwencją przyjęcia ostatecznego podziału działań militarnych według nowego wzorca jest opracowanie solidnych i jednoznacznych podstaw teoretycznych dotyczących terminologii związanej z użyciem urządzeń i systemów elektronicznych. Właściwe zdefiniowanie aparatu pojęciowego umożliwi w dalszym etapie tworzenie rozwiązań systemowych w rozważanej tematyce;

• opracowywanie rozwiązań systemowych opartych na jednoznacznych podstawach teoretycznych i dotyczących terminologii związanej z zastosowaniem urządzeń i systemów elektronicznych musi mieć miejsce jednocześnie na forum NATO i sił zbrojnych USA z udziałem SZRP, co będzie gwarantem identyczności przyjętych praktycznych rozwiązań w rozważanej tematyce jednolicie w całym Sojuszu;

• ujednolicenie przyjętych rozwiązań systemowych w odniesieniu do rozpatrywanej kwestii w ramach NATO pozwoli:

– na właściwe przyswojenie niezrozumiałych zagadnień na wszystkich poziomach kierowania i dowodzenia;

– pokonywać ograniczenia organizacyjne;

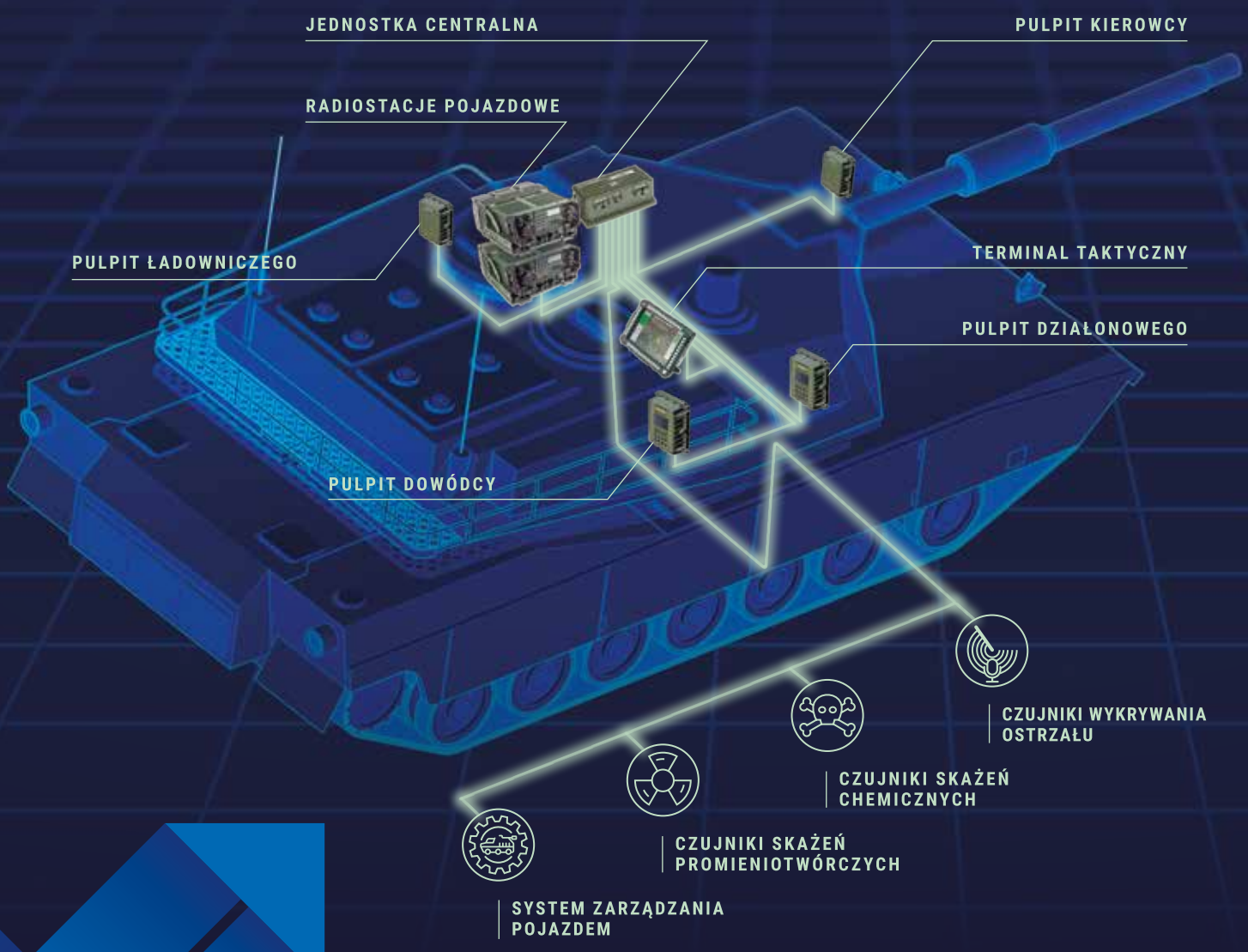
– w prowadzonych działaniach militarnych z wykorzystaniem urządzeń i systemów elektronicznych na ich dalsze, coraz szersze zastosowanie, a w przyszłości sprawne i skuteczne osiąganie przypisanych ich celów;

– na zwiększenie efektywności ich funkcjonowania, w tym jakości i sprawności działań.

W przyjętym według nowego wzorca podziale działań militarnych, prowadzonych w poszczególnych środowiskach, jako nazwę dla tych prowadzonych z użyciem urządzeń i systemów elektronicznych należy przyjąć ostatecznie określenie *cyberprzestrzeń*. Konieczne jest też szerokie rozpropagowanie tego nowego podziału zarówno w opracowaniach teoretycznych, jak i w praktycznym działaniu. Ważne jest zastosowanie istniejącego już aparatu pojęciowego, głęboko zakorzenionego w świadomości specjalistów, co umożliwi harmonijne przejście do nowego podziału działań militarnych zarówno w NATO, jak i w poszczególnych państwach członkowskich. ■

FONET

CYFROWA PLATFORMA INTEGRACJI SYSTEMÓW ŁĄCZNOŚCI I SENSORÓW POJAZDOWYCH



Takie pojazdy też znamy

System FONET został sprawdzony w warunkach bojowych przez siły zbrojne wielu państw.

WDROŻONY DO SŁUŻBY

GRUPA WB

www.wbgroup.pl

W OSTATNIEJ DEKADZIE NATOWSKIE SYSTEMY I SIECI TELEINFORMATYCZNE BYŁY PRZEDMIOTEM CZĘSTYCH CYBERATAKÓW PODEJMOWANYCH PRZEZ PODMIOTY PAŃSTWOWE.

SHUTTERSTOCK/GORODENKOFF

Prawo a cyberprzestrzeń w bezpieczeństwie **lotniczym i kosmicznym**

OBOK ŚRODOWISKA LĄDOWEGO, MORSKIEGO, POWIETRZNEGO I KOSMICZNEGO JEST TO NOWY WYMIAR, W KTÓRYM MOŻNA PROWADZIĆ DZIAŁANIA, W TYM O CHARAKTERZE MILITARNYM.

mgr Aleksandra Radomska

Zdefiniowanie cyberprzestrzeni nie jest łatwe. Opracowano wiele jej definicji, w których usiłowano określić jej kluczowe właściwości. Przede wszystkim ma ona unikatową cechę, jakiej nie ma żadna z innych domen, to znaczy brak wyraźnych fizycznych, politycznych i społecznych granic. Uznawana jest za alternatywną rzeczywistość, z której prężnego funkcjonowania nie zawsze zdajemy sobie sprawę. Cyberprzestrzeń można określić również jako niezależną sieć o globalnym zasięgu, warunkowaną rozwojem technologicznym, której przeznaczeniem jest wymiana informacji za pomocą internetu. Chociaż przestrzeń cybernetyczna nie ma żadnych fizycznych form pozwalających zobrazować lub wyobrazić sobie system jej funkcjonowania, została objęta normami prawnymi. Wśród nich można wyróżnić akty ujęte w porządku prawnym Rzeczypospolitej Polskiej i Unii Europejskiej oraz Organizacji Traktatu Północnoatlantyckiego, dotyczące polityki ochronnej i obronnej mającej na celu zapewnienie bezpieczeństwa w cyberprzestrzeni. Podział ten przyjęto na potrzeby analizy dokumen-

Autorka jest doktorantką w Szkole Doktorskiej WAT.

tów prawodawstwa krajowego oraz międzynarodowego w sferze cywilnej i wojskowej.

PRAWODAWSTWO KRAJOWE

W odniesieniu do regulacji prawnych obowiązujących w naszym kraju należy wymienić *Ustawę z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, która powstała na bazie *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*. Przytoczony akt precyzuje powszechnie obowiązującą w prawodawstwie polskim definicję cyberprzestrzeni. Zgodnie z założeniami przyjętymi w art. 1 ust. 1 niniejszej ustawy konieczność wprowadzenia pojęcia *cyberprzestrzeń* nawiązuje do zagrożeń zewnętrznych godzących w bezpieczeństwo państwa. Wśród nich wymieniono działania w przestrzeni cybernetycznej oraz te o charakterze terrorystycznym. Przez wspomniane zagrożenia, w myśl ustawy, należy rozumieć działalność, która może doprowadzić do zachwiania bezpieczeństwa interesów gospodarczych Polski, godzić w jej niepodległość i niepodzielność, a także każde inne działania podejmowane przez podmioty zewnętrzne uniemożliwiające bądź zakłócające funkcjonowanie naszego kraju w normalnych warunkach. W razie wystąpienia takiego rodzaju zagrożenia prezydent ma prawo, na mocy nadanych mu kompetencji, do wprowadzenia stanu wyjątkowego na części lub całym terytorium państwa (Dz.U. 2011 nr 222 poz. 1323). Na podstawie analizy wspomnianej ustawy można wskazać najważniejsze kwestie, które bezpośrednio z niej wynikają. Pierwsza dotyczy opracowania ogólnej definicji przestrzeni cybernetycznej, co pozwoli na przybliżenie zasad jej funkcjonowania. Co więcej, na mocy tego dokumentu włączono to zgadnienie także do *Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym* oraz *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*. Natomiast druga odnosi się do postrzegania cyberprzestrzeni jako środowiska, które może zostać z powodzeniem wykorzystane do zagrożenia bezpieczeństwa państwa. Należy również zauważyć, że ustawa nie precyzuje nielegalnych działań podejmowanych w tej przestrzeni ani nie przewiduje sposobów jej ochrony przez powołane do tego organy państwowe. Opracowany termin *cyberprzestrzeń* nawiązuje do innego aktu prawnego, w którym zawarto z kolei definicję systemów teleinformatycznych. Jest nim *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (art. 3 pkt 3), odsyłająca do *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (art. 2 pkt 3). W tym drugim dokumencie znajduje się pełne wyjaśnienie użytego określenia. W *Ustawie z dnia 21 lipca 2000 r. „Prawo telekomunikacyjne"* zaś zawarto pojęcia *telekomunikacja* oraz *urządzenia telekomunikacyjne*. Wymienione regulacje oraz definicje z zakresu telekomunikacji wskazują nie tylko na potrzebę umieszczania ich w różnych aktach prawnych, lecz świadczą także o podjęciu prób zrozumienia mechanizmu działania szeroko pojmowanego środowiska przestrzeni cybernetycznej.

Oprócz regulacji prawnych istotnym dokumentem jest *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej* (SBN RP). Została ona podpisana 5 listopada 2014 roku przez ówczesnego prezydenta Bronisława Komorowskiego na wniosek prezesa Rady Ministrów. Jest ona zgodna z wartościami i zasadami zawartymi w *Konstytucji Rzeczypospolitej Polskiej*, a także zbieżna ze strategiami zarządzania rozwojem kraju przez międzynarodowe organizacje, takie jak NATO oraz UE. Składa się z czterech rozdziałów. W pierwszym opisano państwo pojmowane jako podmiot bezpieczeństwa. Zidentyfikowano interesy narodowe, cele strategiczne oraz strategiczny potencjał bezpieczeństwa narodowego państwa. W rozdziale drugim scharakteryzowano współczesne środowisko bezpieczeństwa. Szczególną uwagę zwrócono na specyfikę zagrożeń. Z omawianego dokumentu wynika, że obecnie zanikły wyraźne granice między militarnymi i niemilitarnymi zagrożeniami, jak również wewnętrznymi i zewnętrznymi, a o braku ich przewidywalności decyduje proces globalizacji. To właśnie jego rozwój decyduje o wzroście znaczenia cyberprzestrzeni. Dlatego w podrozdziale 2.1 pkt 31 wymienia się ją jako nowy rodzaj zagrożeń, które obejmują: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo i cyberkonflikty. Dochodzi do nich między podmiotami o charakterze niepaństwowym. Jednocześnie wymieniony dokument definiuje termin *cyberwojna* jako konflikt rozgrywający się między podmiotami państwowymi w przestrzeni cybernetycznej. W tej części dokumentu wskazano na zwiększające się możliwości wystąpienia tych zagrożeń, co jest uzależnione w największym stopniu od rozwoju nowych technologii, takich jak systemy teleinformatyczne oraz sieci internetowe. W związku z tym należy dążyć do zapewnienia jak najwyższego poziomu bezpieczeństwa domeny cyfrowej, ponieważ to od niej może zależeć ogólne bezpieczeństwo kraju. Ochrona systemów teleinformatycznych jest niezbędna, zważywszy na wzrastające uzależnienie od tej technologii. Na tej podstawie można wysnuć wniosek, że w podrozdziale 2.1 pkt 31 *Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej* zdefiniowano cyberprzestrzeń jako środowisko, które może stać się potencjalnym obszarem wystąpienia różnorodnych konfliktów między podmiotami o charakterze państwowym, a także niepaństwowym. Potwierdzenie tego zagrożenia można znaleźć w podrozdziale 2.2 pkt 47, w którym podkreślono istotę i znaczenie bezpieczeństwa w przestrzeni cybernetycznej. Co więcej, zawarto w nim zalecenie ochrony oraz obrony cyberprzestrzeni przez rząd. Na jakość podejmowanych

w związku z tym działań wpływa w naszym kraju polityka oraz współpraca z innymi państwami członkowskimi Organizacji Traktatu Północnoatlantyckiego oraz Unii Europejskiej. Podrozdział 2.3 pkt 57 poświęcono zagadnieniu zapewniania bezpieczeństwa infrastrukturze technicznej umożliwiającej szeroko rozumiany obieg informacji w cyberprzestrzeni, czyli systemom teleinformatycznym. Ich sprawność jest niezbędna do prawidłowego funkcjonowania państwa, natomiast ochrona odbieranych, przesyłanych, przetwarzanych i przechowywanych danych w systemach poufnych jest podstawowym wyzwaniem w tej sferze. Rozwiązaniem mogą być odpowiednio dobrane środki ochronne, lecz do ich implementacji potrzebny jest określony zasób wiedzy na temat procesów zachodzących w cyberprzestrzeni, a także nieustanne dążenie do uświadamiania społeczeństwu istniejących zagrożeń. Dwie pierwsze części *Strategii…* identyfikują nadrzędne interesy naszego kraju oraz środowisko bezpieczeństwa narodowego, w którym funkcjonujemy. Z kolei rozdział trzeci analizowanego dokumentu przedstawia koncepcję działań strategicznych w dziedzinie polityki bezpieczeństwa i obronnej. Ich zaplanowanie oraz wdrożenie z wykorzystaniem adekwatnych środków ma na celu zmniejszenie ryzyka, a także prawdopodobieństwa wystąpienia omawianych zagrożeń. Dokonano w nim podziału na działania obronne i ochronne. W ramach działań obronnych w podrozdziale 3.1 pkt 77 rozważano cyberprzestrzeń jako środowisko, w którym możliwe jest prowadzenie walki zbrojnej. Rozróżniono również pojęcie *cyberkonflikt* jako spór między podmiotami niepaństwowymi oraz *cyberwojna* jako konfrontację między podmiotami państwowymi. W obu przypadkach konieczne jest dysponowanie przez siły zbrojne zdolnościami i środkami, przede wszystkim jednak wiedzą, jak odstraszać potencjalnego przeciwnika metodą oddziaływania ofensywnego i defensywnego. Ponadto muszą być w nieustannej gotowości do współpracy w tej dziedzinie z państwami sojuszniczymi, by konflikty w przestrzeni cybernetycznej nie rozprzestrzeniały się na większą skalę. Odnosząc się do działań ochronnych, zalecenia dotyczące zapewnienia bezpieczeństwa w cyberprzestrzeni omówiono w podrozdziale 3.2 pkt 84. Można zauważyć znaczny dysonans między nimi. Działania obronne odnoszą się bowiem do aspektów związanych z niekwestionowaną gotowością SZRP do zwalczania cyberzagrożeń, natomiast działania ochronne nawiązują do aspektów cywilnych w systemie bezpieczeństwa państwa, do których należy między innymi infrastruktura krytyczna, a także sektor publiczny. Wypracowanie adekwatnych rozwiązań w tym przypadku opiera się głównie na założeniach dotyczących osiągnięcia stanu pożądanego oraz prognoz, bez określenia tak restrykcyjnych wymagań, jak wobec działań obronnych, których wykonawcą są siły zbrojne. Wymienione zostały m.in.: profilaktyka zabezpieczeń przed nielegalną działalnością w cyberprzestrzeni; wypracowanie technik sprawnej komunikacji; wykrywanie cyberzagrożeń i cyberprzestępstw, a także zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej; wymiana zdobytych doświadczeń oraz dobrych praktyk. Ostatni rozdział SBN RP to koncepcje przygotowań strategicznych, których istotą jest właściwe połączenie elementów wchodzących w skład systemu bezpieczeństwa narodowego. Zalicza się do niego składniki wewnętrzne i zewnętrzne oraz militarne i niemilitarne. Aby realizacja tych koncepcji była możliwa, niezbędne jest podjęcie działań opartych na priorytetach preparacyjnych. Dokonano ich podziału oraz wskazano na: wdrożenie stosownej integracji podsystemu kierowania bezpieczeństwem narodowym; profesjonalizację podsystemów operacyjnych (ochronnych i obronnych); powszechność przygotowań podsystemów wsparcia (społecznych i gospodarczych). Wzmianka o cyberprzestrzeni znajduje się w podrozdziale 4.3 pkt 128 i nawiązuje do podsystemów ochronnych. Została w nim poruszona kwestia instytucji właściwych do spraw cyberbezpieczeństwa. Zawiera także zalecenie odnoszące się do wieloaspektowego, systemowego podejścia do problematyki cyberbezpieczeństwa w takich wymiarach, jak: określenie ram jego zapewnienia przepisami prawa, ustalenie struktur organizacyjnych i przede wszystkim zdobycie odpowiednich zasobów technicznych. W odniesieniu do norm prawnych położono nacisk na rozwój Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej w celu utworzenia sprawnego mechanizmu aktywnej obrony przed cyberzagrożeniami. Rozważając rozwiązania organizacyjne, wspomniano o potrzebie utworzenia narodowego ośrodka koordynacji, a także o wymianie informacji oraz dobrych praktyk między podmiotami odpowiedzialnymi za cyberbezpieczeństwo. Analizując aspekt techniczny, należy wspomnieć w pierwszej kolejności o stworzeniu warunków do implementacji rozwiązań technologicznych służących utrzymaniu wysokiego poziomu bezpieczeństwa cyberprzestrzeni. Całokształt tych zadań przygotowawczych ma zapewnić ochronę przestrzeni cybernetycznej przed różnorodnymi atakami.

Kolejnym dokumentem jest *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Została ona opracowana jako akt rządowy stanowiący koncepcyjny i wykonawczy załącznik do SBN RP. Zawarte w niej treści zatwierdziła 12 stycznia 2015 roku Rada Bezpieczeństwa Narodowego. W doktrynie tej określono cele strategiczne w dziedzinie cyberbezpieczeństwa, jego środowisko, koncepcję podejmowanych działań operacyjnych, a także zadań preparacyjnych[1]. Co najważniejsze, *Doktryna…* dokładnie definiuje środowi-

1 *Doktryna cyberbezpieczeństwa RP,* Publikacje BBN, https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html/. 12.08.2018.

sko cyberbezpieczeństwa RP w wymiarze wewnętrznym i zewnętrznym, poddając je wnikliwej analizie z podziałem na prawdopodobieństwo wystąpienia zagrożeń oraz z uwzględnieniem wyzwań (szanse i ryzyka). Można zatem ocenić, że przesłania zawarte w *Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej* zostały rozszerzone w omawianej *Doktrynie…*, wskazując nie tylko na odmienny charakter dotychczas niekoniecznie znanych niebezpieczeństw pochodzących z cyberprzestrzeni, lecz precyzując jednocześnie w większym stopniu wynikające z nich ryzyka, a także szanse wzmocnienia ochrony. W dokumencie uznano, że działania operacyjne związane z ochroną cyberprzestrzeni, które stanowią cel strategiczny, powinny być realizowane przez sektory: prywatny, obywatelski i publiczny (w dwóch aspektach: krajowym i międzynarodowym), a także w wymiarze transsektorowym. Określono ich zadania, co pozwala na bardziej szczegółowe monitorowanie działalności w cyberprzestrzeni, na wymianę doświadczeń, analizy systemowe, audyt, rozwijanie zdolności aktywnej cyberobrony czy zachowanie kompatybilności z wymaganiami państw sojuszniczych, w tym standardami NATO i UE. W odniesieniu do działań przygotowawczych, według zaleceń *Doktryny…*, niezbędne jest wcześniejsze zrozumienie cyberbezpieczeństwa jako złożonego procesu prowadzącego finalnie do zapewnienia kompleksowej i sukcesywnej ochrony cyberprzestrzeni. Dotyczy ona implementacji rozwiązań w zakresie prawnym, organizacyjnym oraz technicznym, gwarantujących bezpieczeństwo systemom teleinformatycznym. Ważnym efektem tych prac jest również zachowanie swoistej elastyczności, możliwości dostosowania do nowych sytuacji, z jednoczesnym utrzymaniem skuteczności działania[2].

Przytoczone dokumenty wskazują nie tylko na sukcesywny wzrost znaczenia cyberprzestrzeni oraz podejmowanie działań w celu jej ochrony jako części polityki państwa, lecz definiują także związane z nią pojęcia.

Należy również zauważyć, że rozwój lotnictwa komunikacyjnego, rozumianego w tym przypadku jako rodzaj transportu, wdrażanie nowych technologii, zintegrowanych systemów awioniki pokładowej czy systemów nawigacyjnych wymagają odpowiedniego zabezpieczenia informacji przekazywanej między poszczególnymi urządzeniami technicznymi i odbiornikami z jednoczesną ochroną tych systemów teleinformatycznych. W związku z tym konieczne jest objęcie ochroną cyberprzestrzeni na potrzeby sprawnego oraz bezpiecznego cywilnego ruchu lotniczego, w tym minimalizacja skutków wystąpienia cyberataków lub cyberzagrożeń oraz ich zwalczanie. Dlatego też Urząd Lotnictwa Cywilnego jako jednostka budżetowa, którego prezes jest naczelnym organem administracji właściwej do spraw lotnictwa cywilnego, w drodze porozumienia z Ministerstwem Cyfryzacji oraz Ministerstwem Infrastruktury i Budownictwa podjął się realizacji projektu polegającego na utworzeniu jednostki odpowiedzialnej za cyberbezpieczeństwo w lotnictwie, czyli Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (*Computer Security Incident Response Team* – CSIRT). Ma to być pierwszy w Europie tego rodzaju podmiot w branży lotniczej i administracji publicznej, współpracujący z Narodowym Centrum Cyberbezpieczeństwa. Co więcej, prezes ULC podpisał porozumienie z Europejską Agencją Bezpieczeństwa Lotniczego (*European Union Aviation Safety Agency* – EUASA) w sprawie testowania w kraju pilotażowego europejskiego programu związanego z problematyką cyberbezpieczeństwa w lotnictwie. Należy zauważyć, że lotniczy transport komunikacyjny rozwija się niezwykle dynamicznie, co powoduje jego uzależnienie od systemów teleinformatycznych. Stanowi to niekwestionowaną wygodę dla pasażerów obsługiwanych w portach lotniczych, lecz jednocześnie sprawia, że wzrasta prawdopodobieństwo wystąpienia cyberataku.

W odniesieniu do branży kosmicznej należy podkreślić, że Polska Agencja Kosmiczna (*Polish Space Agency* – POLSA), występując w roli instytucji państwowej właściwej do spraw budowania polskiego przemysłu kosmicznego, zakłada, że nasz kraj do 2030 roku będzie realizować zadania związane z obronnością i bezpieczeństwem państwa w takich obszarach, jak satelitarna obserwacja Ziemi, obserwacja przestrzeni kosmicznej, a także nawigacja i łączność kosmiczna. By podjąć takie działania, niezbędne będzie wypracowanie koncepcji ochrony urządzeń technicznych znajdujących się w przestrzeni kosmicznej przed cyberzagrożeniami na podstawie zapisów obowiązującego prawodawstwa krajowego.

OBECNA POLITYKA CYBERBEZPIECZEŃSTWA OCHRONY OPERATOROM USŁUG KLUCZOWYCH

PRAWO UNII EUROPEJSKIEJ

Skuteczność polityki w sferze ochrony cyberprzestrzeni i niwelowania skutków cyberprzestępstw w przypadku tej organizacji międzynarodowej wymaga współpracy wszystkich państw członkowskich

2 *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Biuro Bezpieczeństwa Narodowego, 2015.

(ich liczba w 2020 roku wynosiła 27), w tym implementacji jednakowych standardów i minimalnych wymagań, jak również promowania zagadnień bezpieczeństwa przestrzeni cybernetycznej na arenie międzynarodowej. W związku z tym konieczne jest nie tylko poznanie oraz ustalenie jednolitych potrzeb państw, lecz także ich wspólne działanie na rzecz Unii Europejskiej. Jeden z pierwszych dokumentów wprowadzonych przez UE miał na celu zabezpieczenie danych obiegających cyberprzestrzeń. Była to *Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 5 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym*. Określono, że przedmiotem dyrektywy jest harmonizacja odnosząca się do przepisów prawnych obowiązujących we wszystkich państwach członkowskich. Podkreślono konieczność zapewnienia odpowiedniego poziomu ochrony podstawowych praw i wolności, w tym prywatności każdego z użytkowników lub abonentów, wobec przetwarzania danych osobowych przez systemy teleinformatyczne w sektorze telekomunikacyjnym Wspólnoty Europejskiej[3]. Aktem prawnym zastępującym, jednocześnie uzupełniającym ten dokument, jest *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej*. Dyrektywa z 2002 roku powiela postulaty zawarte w tej z roku 1997. Jednocześnie zwraca uwagę na rozwój społeczeństwa informacyjnego w wyniku wdrażania coraz nowszych technologii (również cyfrowych), co z kolei sprzyja digitalizacji pozwalającej na tworzenie globalnych rynków i dostępu do usług za pomocą internetu.

W grudniu 2003 roku przyjęto *Europejską strategię bezpieczeństwa – bezpieczna Europa w lepszym świecie*, która stosunkowo niewiele miejsca poświęca cyberbezpieczeństwu. Co ważniejsze, zwrócono w niej uwagę na wzrost liczby cyberprzestępstw (czy też nasilenie przestępczości internetowej) jako czynów mogących ewoluować ze względu na dość uniwersalne środowisko pochodzenia, jakim jest przestrzeń cybernetyczna. Bez względu na przedmiot cyberataku w państwach członkowskich (instytucje prywatne lub rządowe) oraz zakłócanie działania ich systemów teleinformatycznych istnieje zagrożenie, że zwiększy się jego skala, powodując, iż tego rodzaju nielegalna działalność stanie się nową bronią polityczną oraz militarną. Dlatego też konieczne jest kontynuowanie prac mających na celu opracowanie kompleksowego podejścia wobec zacieśniania współpracy międzynarodowej między państwami oraz większej świadomości skutków cyberprzestępstw. Na podstawie przytoczonych aktów prawnych i strategii można jednoznacznie stwierdzić, że na początku rozwoju prawa unijnego w dziedzinie ochrony cyberprzestrzeni priorytetem było zapewnienie prywatności przetwarzanych danych osobowych, dostrzeżenie ekspansji technologii cyfrowych oraz potrzeba znalezienia rozwiązań profilaktycznych w kwestii przeciwdziałania cyberprzestępstwom. W 2004 roku nastąpił istotny postęp w dziedzinie polityki cyberbezpieczeństwa Unii Europejskiej – na podstawie rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady z 10 marca 2004 roku została powołana Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*European Network and Information Security Agency* – ENISA). Jest to wyspecjalizowany organ dysponujący wiedzą na temat zapewniania bezpieczeństwa cyberprzestrzeni w Europie. Agencja, której główna siedziba znajduje się w Heraklionie na Krecie (Grecja), liczy obecnie 65 pracowników. Początkowo jej zadaniem było prowadzenie prac analitycznych oraz badawczych. Powodem tak nakreślonej działalności była potrzeba śledzenia i rozpoznawania cyberprzestępstw. Należy zauważyć, że w momencie powstania ENISA świadomość w kwestii wykorzystania przestrzeni cybernetycznej do nielegalnej działalności nie była tak powszechna jak obecnie. Zadaniem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, wspólnie z instytucjami oraz państwami członkowskimi UE, jest przygotowanie praktycznych rozwiązań oraz opracowanie porad (zarówno dla sektora publicznego, jak i prywatnego) zapobiegających destrukcyjnej ingerencji z cyberprzestrzeni, a także udzielanie wskazówek, w jaki sposób wykrywać i reagować na tego rodzaju zagrożenia[4]. W kwestii rozwoju prawa Unii Europejskiej dotyczącego cyberprzestrzeni oraz jej ochrony należy jeszcze wspomnieć

SKUPIA SIĘ NA ZAGWARANTOWANIU ORAZ DOSTAWCOM USŁUG CYFROWYCH

3 *Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym,* s. 5.

4 Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), https://europa.eu/european-union/about-eu/agencies/enisa_pl/. 26.08.2018.

o *Decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataku na systemy informatyczne*. Nadrzędnym celem tego dokumentu jest usprawnienie współpracy między organami ścigania państw członkowskich UE. Do tych organów należy sądownictwo i policja oraz inne wyspecjalizowane jednostki. W *Decyzji…* znajdują się zalecenia w sprawie kompleksowego podejścia do kwestii zapewnienia co najmniej akceptowalnego poziomu bezpieczeństwa sieci, systemów i przetwarzanych informacji. Podkreślono, że największe utrudnienie na drodze do podejmowania skoordynowanych działań w dziedzinie zapewniania cyberbezpieczeństwa stanowią luki w prawodawstwie karnym poszczególnych państw członkowskich i jego niespójność[5]. Ze względu na globalny wymiar przestrzeni cybernetycznej ustalenie wspólnych zasad i procedur jest kluczową sprawą w zapobieganiu aktom bezprawnej ingerencji w tej przestrzeni. Dlatego też tak istotne jest ujednolicenie wspólnych, minimalnych standardów, a także promowanie zagadnienia zapewniania bezpieczeństwa w cyberprzestrzeni przez wszystkie kraje.

Następnym ważnym dokumentem jest *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, w kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r.* W tym akcie prawnym dokonano podziału cyberprzestępstw na trzy grupy. Pierwszą stanowią te popełniane z użyciem sieci i systemów informatycznych, do których zalicza się: oszustwa, kradzież tożsamości oraz fałszerstwa dokonywane w środowisku cybernetycznym. Drugą są publikacje w internecie nielegalnych treści nawołujących na przykład do rasizmu lub ksenofobii. Ostatnią grupą cyberprzestępstw podaną w *Komunikacie…* są nielegalne działania wymierzone w sieci i systemy informatyczne, czyli przykładowo cyberataki. Na tej podstawie można stwierdzić, że dostrzeżono konieczność poszerzenia zakresu znaczeniowego tego pojęcia z uwagi na wzrastającą częstotliwość występowania cyberprzestępstw oraz ich różnorodny charakter. W omawianym dokumencie po raz kolejny wezwano państwa członkowskie UE do implementacji spójnego prawa krajowego w dziedzinie ochrony przestrzeni cybernetycznej. Oprócz tego zachęcono poszczególne kraje do utworzenia wspólnego systemu informacji na temat cyberprzestępstw, które występują na ich terytorium. Każde z nich powinno być świadome, że podstawą właściwego funkcjonowania ich infrastruktury krytycznej są technologie cyfrowe, a ingerencja w ich pracę bądź uszkodzenie może mieć dramatyczne konsekwencje dla społeczeństwa[6].

W ciągu kilku następnych lat Unia Europejska wdrażała kolejne inicjatywy związane z działaniami (głównie ochronnymi) w cyberprzestrzeni. Wraz z pojawianiem się nowych cyberzagrożeń i cyberprzestępstw implementowano nowe przepisy, rozwijając w ten sposób prawodawstwo unijne. Można zatem uznać, że ekspansja tego rodzaju zagrożeń była niejednokrotnie impulsem do sporządzania aktów prawnych, strategii i komunikatów. Wśród nich warto wspomnieć o *Wspólnym komunikacie Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* podpisanym w 2013 roku. Dokument ten składa się z kilku zasadniczych części. Przede wszystkim określa zasady cyberbezpieczeństwa zdefiniowanego na podstawie przyjętych kryteriów, takich jak[7]:

– ochrona praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności;

– dostęp dla wszystkich;

– demokratyczne i efektywne zarządzanie wielostronne;

– wspólna odpowiedzialność za zapewnienie bezpieczeństwa.

Na podstawie tych zasad opracowano priorytety w procesie zapewniania bezpieczeństwa cybernetycznego na szczeblu strategicznym, czyli:

– osiągnięcie odporności na zagrożenia tego rodzaju;

– radykalne ograniczenie cyberprzestępczości;

– opracowanie polityki obronnej oraz rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO);

– zwiększenie zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego;

– ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej oraz promowanie podstawowych wartości UE.

W omawianym *Wspólnym komunikacie…*, biorąc pod uwagę najważniejsze aspekty nieuwzględnione w poprzednich dokumentach, nadmieniono, że państwa członkowskie muszą dążyć do implementacji rygorystycznych przepisów w sektorach publicznych i prywatnych odnośnie do popełnionych cyberprzestępstw, a także współpracować z ENISA. Ponadto UE będzie wspierać wszystkie kraje w identyfikacji braków w ich systemach informatycznych w formie programów finansowych. Chociaż wdrażanie w Unii Europejskiej nowych dokumentów wiązało się z roz-

5 *Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne,* Dz.U. WE L 69/68 z 16.03.2005.

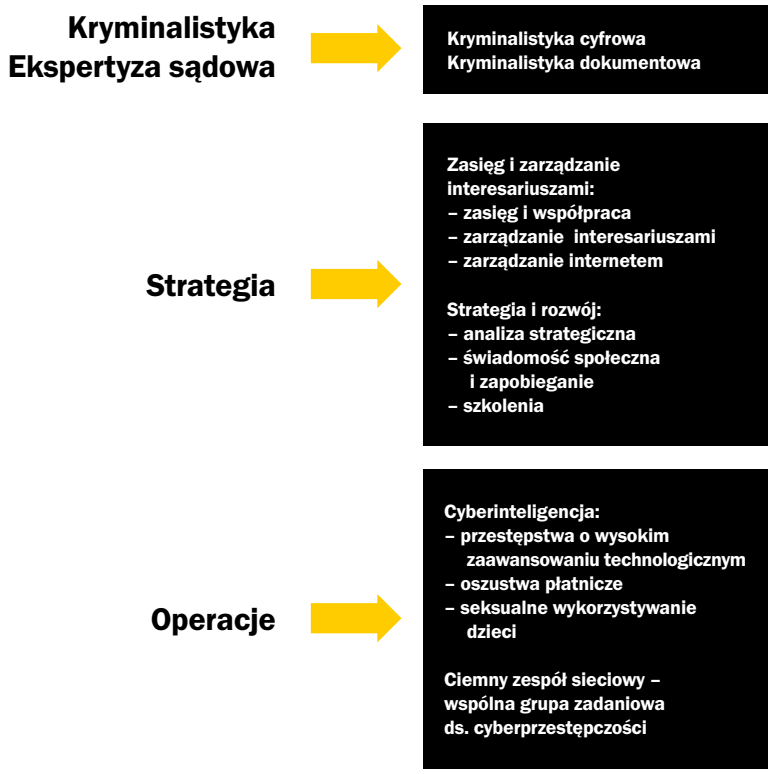
6 *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 22 maja 2007 r.,* Belgia.

7 *Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń,* Komisja Unii Europejskiej, Belgia 2013.

szerzeniem działalności związanej z ochroną cyberprzestrzeni, perspektywą podniesienia poziomu jej bezpieczeństwa oraz faktycznym wprowadzeniem zmian w prawodawstwie krajowym wszystkich państw członkowskich, należy zauważyć, że stanowiły one jedynie ogólne wytyczne. Jakość cyberbezpieczeństwa zaczęła się poprawiać, odkąd powołano wyspecjalizowany organ, jakim jest ENISA. W związku z jej funkcjonowaniem wszystkie kraje należące do Wspólnoty mogą otrzymywać praktyczne porady na temat rozwiązywania problemów z zakresu występujących cyberzagrożeń. Wobec tego unijne koncepcje doprowadziły do powołania kolejnego, ważnego z punktu widzenia bezpieczeństwa cybernetycznego, organu, którym jest Zespół Szybkiego Reagowania na Zagrożenia w Cyberprzestrzeni (*Computer Emergency Response Team* – CERT). Jego powstanie zapowiedziano w *Europejskiej Agendzie Cyfrowej* w 2010 roku w celu dalszego podnoszenia poziomu bezpieczeństwa sieci oraz informacji w agencjach Unii Europejskiej. CERT-EU wykorzystuje zasoby jednostek oraz instytucji UE, takich jak: Komisja Europejska, Rada, Parlament, Komitet Regionów, Komitet Ekonomiczno-Społeczny i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji. Jego utworzenie było pierwszym etapem wzmocnienia cyberbezpieczeństwa, natomiast kolejnym krokiem miało być powołanie w poszczególnych państwach członkowskich krajowych organów o tym charakterze. Obecnie w naszym kraju funkcjonuje Rządowy Zespół Reagowania na Incydenty Komputerowe: CERT.GOV.PL. Nadrzędnym celem wszystkich jednostek CERT jest archiwizacja i gromadzenie informacji na temat cyberzagrożeń, wczesne i skuteczne reagowanie na nie, jak również opracowywanie rozwiązań profilaktycznych. Idea zobligowania wszystkich państw członkowskich UE do implementacji jednostek CERT nie była jedyną inicjatywą.

Należy także wspomnieć o koncepcji, która pojawiła się w 2013 roku i dotyczyła powołania przez EUROPOL Europejskiego Centrum ds. Walki z Cyberprzestępczością (*European Cybercrime Centre* – EC3). Zasadniczym powodem jego zorganizowania była konieczność wzmocnienia reakcji organów ścigania na cyberprzestępczość w UE, a tym samym ochrona europejskich obywateli, przedsiębiorstw i rządów przed tego rodzaju przestępstwami. Choć trudno podać rzetelne dane szacunkowe, niektóre raporty branżowe sugerują, że globalne koszty cyberprzestępczości wynoszą setki miliardów euro rocznie. Każdego roku EC3 publikuje *Ocenę zagrożenia przestępczości zorganizowanej w internecie* (*Internet Organised Crime Threat Assessment* – IOCTA). Jest to sztandarowy raport strategiczny na temat kluczowych odkryć i pojawiających się zagrożeń oraz postępów w cyberprzestępczości. Dzięki takiemu działaniu ujawniane są przestępstwa dokonywane w przestrzeni cybernetycznej. Należy zauważyć, że Europejskie Centrum ds. Walki z Cyberprzestępczością jest organem odpowiadającym za egzekwowanie prawa, natomiast ENISA oraz CERT-EU są odpowiedzialne za bezpieczeństwo sieci i informacji (rys. 1).

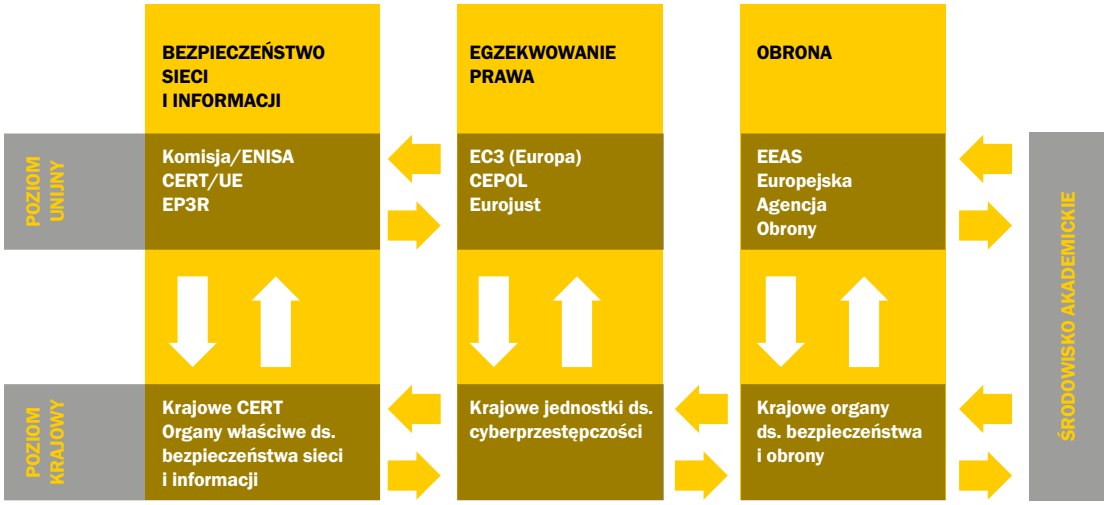
RYS. 1. WYMIARY DZIAŁALNOŚCI PROWADZONEJ PRZEZ EUROPEJSKIE CENTRUM DS. WALKI Z CYBERPRZESTĘPCZOŚCIĄ



Opracowano na podstawie: European Cybercrime Centre – EC3, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/. 27.08.2018.

Należy zaznaczyć, że przedstawione organizacje nie są jedynymi powołanymi do zapewnienia bezpieczeństwa cyberprzestrzeni, wymuszającymi przestrzeganie przepisów jej dotyczących. Warto jednak zwrócić uwagę na relacje zachodzące między instytu-

RYS. 2. SCHEMAT KOORDYNACJI DZIAŁAŃ I RELACJI NA RZECZ CYBERBEZPIECZEŃSTWA W WYMIARZE KRAJOWYM, UNIJNYM I MIĘDZYNARODOWYM



Opracowano na podstawie: M. Górecki, *Otwarta, bezpieczna i chroniona cyberprzestrzeń – nowa jakość internetowej komunikacji czy poważny spór wokół nowej dyrektywy Komisji Europejskiej?* „Świat Idei i Polityki" 2014 nr 13, s. 17.

cjami oraz organizacjami na trzech szczeblach: krajowym, unijnym i międzynarodowym w sferach bezpieczeństwa sieci i informacji oraz egzekwowania prawa i obrony (rys. 2).

Kontynuując rozważania na temat prawodawstwa unijnego w kontekście ochrony cyberprzestrzeni, konieczne jest wymienienie aktu prawnego, jakim jest *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, nazywana potocznie dyrektywą NIS (*Network and Information Systems Directive*). Obejmuje ona wyłącznie dwa rodzaje podmiotów: operatorów usług kluczowych oraz dostawców cyfrowych usług. Operatorzy usług kluczowych są powiązani z właściwym funkcjonowaniem poszczególnych sektorów infrastruktury krytycznej danego państwa. Są to m.in.: energetyka, transport, służba zdrowia, bankowość i finanse czy ujęcia wody. Natomiast dostawcy usług cyfrowych to podmioty świadczące na przykład usługi przetwarzania danych w chmurze czy wyszukiwarki internetowe i wirtualne platformy handlowe. Dyrektywa NIS identyfikuje operatorów usług kluczowych oraz dostawców usług cyfrowych, kładąc szczególny nacisk na fakt, że dotyczące ich określenia powinny być spójne i jednakowo definiowane przez wszystkie państwa członkowskie Wspólnoty. Dokument mobilizuje również poszczególne kraje do sporządzenia wykazu tych podmiotów w celu przedstawienia ich listy Komisji Europejskiej, która powinna dokonać oceny, czy zastosowana metoda pozwoliła na jednakowe rozumienie związanych z nimi terminów przez wszystkie kraje[8]. Mając na celu zachowanie wysokiego poziomu bezpieczeństwa sieci i informacji w odniesieniu do operatorów usług kluczowych oraz dostawców usług cyfrowych, konieczne jest posiadanie przez każde z państw krajowej strategii ich ochrony, sprecyzowanie celów strategicznych oraz zaproponowanie działań operacyjnych. By mieć zdolność do realizacji działań ochronnych, we wszystkich państwach członkowskich UE powinny powstać struktury organizacyjne oraz zasoby techniczne. Dyrektywa NIS wskazuje, że każdy kraj musi posiadać prężnie funkcjonujące CSIRT, nazywane dalej CERT. Wiedzę specjalistyczną w obszarze cyberbezpieczeństwa

8 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii,* Wspólnoty Europejskie.

zapewnia ENISA, która powinna zarazem zachęcać państwa do współpracy i wymiany informacji na temat występujących na ich terytorium incydentów w cyberprzestrzeni. Taka dobra praktyka wsparłaby opracowywanie nowych rozwiązań w sferze zapobiegania cyberzagrożeniom w Unii Europejskiej.

Wymienione inicjatywy UE w aspekcie rozwoju porządku prawnego dotyczącego ochrony cyberprzestrzeni, opracowania działań operacyjnych, wprowadzenia nowych definicji i wspólnych przepisów czy promowania cyberbezpieczeństwa spowodowały, że zaczęto podejmować podobne działania w organizacjach lotniczych.

Na szczeblu europejskim jednym z najważniejszych instytucjonalnych filarów zajmujących się szeroko rozumianą problematyką bezpieczeństwa ruchu lotniczego jest Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (*European Union Aviation Safety Agency* – EUASA). W dziedzinie zapewniania bezpieczeństwa cyberprzestrzeni zadaniem EUASA jest zagwarantowanie uwzględniania zagrożeń cybernetycznych podczas projektowania, rozwoju i eksploatacji samolotów, następnie ich kontrola w celu uniknięcia negatywnego wpływu na bezpieczeństwo obywateli państw zrzeszonych w tej organizacji. W 2017 roku firma IOActive zaangażowała się za pośrednictwem EUASA w tzw. odpowiedzialne ujawnianie pewnych luk, które wykryto w pokładowym systemie satelitarnym zapewniającym internet pasażerom. Proces odpowiedzialnego ujawniania informacji polega na tym, że potencjalne zagrożenia zostaną wyeliminowane przed ujawnieniem luki w zabezpieczeniach. Po zakończeniu tego procesu EUASA koordynowała działania z operatorami i odpowiednimi organami oraz przeprowadzała niezależne weryfikacje. Ponadto dostawca skorygował luki w zabezpieczeniach i po ustaleniu, że korekty zostały wprowadzone, a system nie był dostępny z internetu, uzgodniono z IOActive, że mogą publikować swoje badania po całkowitym skorygowaniu niesprawności[9]. Po tych ustaleniach Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego opracowała plan działania w zakresie cyberbezpieczeństwa, który został zatwierdzony przez zarząd w listopadzie 2015 roku. Od tego czasu organizacja pracuje nad jego wdrożeniem. W celu realizacji przyjętych zamierzeń z nim związanych uruchomiono wiele inicjatyw, by lepiej rozwiązywać problemy dotyczące cyberbezpieczeństwa w lotnictwie, zwiększając odporność wbudowanych zabezpieczeń. Oprócz działań polegających na tworzeniu przepisów instytucjonalnych EUASA na bieżąco pracuje nad poprawą międzynarodowej współpracy w tym zakresie, a także nad promowaniem wymiany informacji między zainteresowanymi stronami z branży lotniczej. Osiągnięcie odpornego na cyberataki systemu lotniczego i włączenie cyberbezpieczeństwa do pojęć związanych z bezpieczeństwem wymaga skoordynowanego wysiłku zainteresowanych stron z sektora lotniczego. W tym celu powołano Strategiczną Europejską Platformę Koordynacji (*Strategic European Coordination Platform*), w której skład mają wchodzić przedstawiciele kluczowych podmiotów z branży, państw członkowskich i instytucji UE. Współpraca przyczynia się do harmonizacji średnioterminowych celów zainteresowanych stron oraz do uzgodnienia planu działania, zapobiegając w ten sposób powielaniu wysiłków. Aby promować dobrowolną wymianę informacji i współpracę ekspercką, EASA wspiera utworzenie Europejskiego Centrum Bezpieczeństwa Cybernetycznego w Lotnictwie (*European Centre for Cybersecurity in Aviation* – ECCSA) i zapewnia początkowe zdolności operacyjne we współpracy z CERT-UE[10]. ECCSA to przede wszystkim centrum informacyjne służące cyberbezpieczeństwu w lotnictwie, które zapewnia między innymi usługi sieciowe i wymianę informacji między zainteresowanymi stronami, będącymi kluczowymi czynnikami umożliwiającymi tworzenie odpornej cyberprzestrzeni lotniczej. Centrum udostępnia swoim członkom bezpieczne sposoby wymiany odpowiednich informacji dotyczących bezpieczeństwa cyberprzestrzeni, na przykład luk w zabezpieczeniach (słabości, które mogą być wykorzystywane do szkodliwych celów), a także zdarzeń i incydentów, którymi warto podzielić się ze społecznością lotniczą. Zespół operacyjny analityków ECCSA zapewnia dodatkowe dane wejściowe oraz kontekst do informacji udostępnianych przez uczestników w celu ułatwienia tworzenia wiedzy o zagrożeniach związanych z bezpieczeństwem cybernetycznym i ryzykiem oraz zarządzania nimi. Obecnie udział w Centrum jest dobrowolny, podobnie jak wymiana informacji. Organizacje istotne dla bezpieczeństwa i ochrony lotnictwa cywilnego mogą ubiegać się o członkostwo w nim.

OBRONA CYBERPRZESTRZENI W NATO

Trzecim kryterium przyjętym na potrzeby analizy prawodawstwa odnoszącego się do cyberbezpieczeństwa jest porządek prawny obowiązujący w Organizacji Traktatu Północnoatlantyckiego (*North Atlantic Treaty Organization* – NATO), wyznaczający kierunki realizacji polityki ochronnej i obronnej cyberprzestrzeni. W 2020 roku NATO zrzeszało 29 państw, których zasadniczym celem, w ujęciu syntetycznym, jest obrona militarna, podejmowanie działań stabilizacyjnych oraz zapobieganie rozprzestrzenianiu się zagrożeń regionalnych na większą skalę.

Aby usystematyzować wiedzę w tym zakresie oraz skoncentrować się na współczesnych problemach związanych z ochroną przestrzeni cybernetycznej, należy dokonać przeglądu inicjatyw podejmowanych

9 *EASA engaged in a "responsible disclosure" of cybersecurity issues in coordination with operators and authorities* – online, https://www.easa.europa.eu/newsroom-and-events/news/easa-engaged-"responsible-disclosure"-cybersecurity-issues-coordination/. 19.01.2019.

10 *European Centre for Cybersecurity in Aviation (ECCSA)*, https://www.easa.europa.eu/eccsa/. 19.01.2019.

w różnych latach podczas szczytów NATO. Konieczność ta wynika z utrudnionego dostępu do wewnętrznych dokumentów Sojuszu. Na szczycie NATO, który odbył się w Walii w 2014 roku, zgodnie uznano, że w cyberprzestrzeni obowiązuje prawo międzynarodowe, wpływ zaś cyberataków może być równie szkodliwy dla społeczeństw jak atak przeprowadzony z użyciem broni konwencjonalnej. W rezultacie cyberobrona została uznana za część podstawowego zadania w ramach obrony zbiorowej wszystkich państw członkowskich przeciwko zagrożeniom pochodzących z cyberprzestrzeni. Natomiast na szczycie NATO w Warszawie w 2016 roku kraje należące do Sojuszu uznały cyberprzestrzeń za kolejną domenę operacji wojskowych. Postawiono ją na równi z materialnymi wymiarami środowisk prowadzenia działań militarnych, takich jak powietrze, ląd i akweny morskie. Tego rodzaju podejście do rozumienia przestrzeni cybernetycznej jako obszaru o niematerialnych właściwościach umożliwia dowódcom zapewnienie lepszej ochrony przed cyberzagrożeniami prowadzonym operacjom. Uznanie cyberprzestrzeni za domenę nie zmienia mandatu NATO. Podobnie jak we wszystkich dziedzinach operacyjnych, jego działania mają charakter defensywny, proporcjonalny i zgodny z obowiązującym prawem międzynarodowym. W czasie warszawskiego szczytu przedstawiciele państw członkowskich przyjęli także *Zobowiązanie w sprawie obrony cybernetycznej* (*Cyber Defence Pledge*), które ma na celu wzmocnienie cyberobrony krajowych sieci i infrastruktur. W związku z tym każde państwo jest odpowiedzialne za własną obronę cybernetyczną przed zagrożeniami pochodzącymi z cyberprzestrzeni, która – jak wiadomo – ma zasięg globalny. Nie oznacza to, że zobligowanie państw członkowskich nie zostanie wsparte przez NATO w zakresie implementacji działań obronnych przed cyberzagrożeniami. Podejmowanie coraz radykalniejszych i stanowczych kroków mających na celu wzmocnienie potencjału Sojuszu do obrony cyberprzestrzeni wynika z raportów świadczących o tym, że w ostatniej dekadzie natowskie systemy i sieci teleinformatyczne były przedmiotem częstych cyberataków podejmowanych przez podmioty państwowe. Podobne zdarzenia są odnotowywane ze zwiększającą się częstotliwością. Większość z nich jest analizowana przez autonomiczne systemy Sojuszu, których najważniejszym zadaniem jest rozpoznanie źródła i rodzaju cyberataku. Jednakże postępująca złożoność cyberzagrożeń wymaga dodatkowej oceny i interwencji ze strony ekspertów specjalizujących się w cyberobronie. W 2016 roku NATO odnotowało w miesięcznej skali średnio 500 incydentów pochodzących z cyberprzestrzeni, co stanowi wzrost o około 60% w stosunku do 2015 roku.

W 2017 roku w Brukseli eksperci odpowiedzialni za bezpieczeństwo cybernetyczne systemów i sieci Sojuszu Północnoatlantyckiego potwierdzili zauważalną ewolucję w dziedzinie cyberataków. Przede wszystkim zostały one ukierunkowane na tak zwane miękkie systemy, do których zaliczają się choćby urządzenia osobiste i sieci powiązane z NATO. Co ważniejsze, nie są one objęte współcześnie ochroną organizacji, ułatwiając potencjalnym hakerom zdobycie pożądanych danych w znacznie prostszy sposób. W ramach wzmacniania cyberobrony w 2017 roku państwa członkowskie postulowały za utworzeniem nowego Centrum Operacji Cybernetycznych (*Cyber Operations Centre* – COC). Obecnie trwają prace nad jego konfiguracją. Centra te mają powstać we wszystkich państwach członkowskich NATO i stanowić militarny odpowiednik CERT-EU. Nadrzędnym ich zadaniem jest sprawowanie kontroli nad wojskowymi systemami łączności, kierowania i dowodzenia oraz prowadzenie operacji obronnych w cyberprzestrzeni z zastosowaniem oprogramowania, a także narzędzi teleinformatycznych. W ramach operacji obronnych będą realizowane takie działania, jak: wykrywanie, rozpoznawanie i neutralizacja złośliwego oprogramowania; blokowanie i odpieranie cyberataków przeprowadzanych przez hakerów; zwalczanie wszelkich innych cyberzagrożeń godzących w bezpieczeństwo cybernetyczne. Biorąc pod uwagę tajny charakter działań COC, nie ujawniono, jakie komórki wchodzą w skład Centrum ani też jakie zadania wykonują jego pracownicy. Prawdopodobnie są to żołnierze wykwalifikowani w zakresie matematyki i informatyki, jak również kryptoanalizy, czyli umiejętności łamania kodów i szyfrów[11]. Konieczność utrzymania akceptowalnego poziomu bezpieczeństwa cybernetycznego narzuca potrzebę poszukiwania nowych rozwiązań technicznych oraz rozwoju zdolności technologicznych do odpierania cyberzagrożeń. W tym celu powołano w strukturach Sojuszu kilka instytucji funkcjonujących na różnorodnych poziomach, zapewniając wszechstronne podejście do tej problematyki. Jedną z nich jest Zespół Reagowania na Incydenty Komputerowe NATO (*NATO Computer Incident Response Capability* – NCIRC). Powołanie Zespołu jest o tyle istotne, że jest to pierwszy zdecydowany krok Sojuszu służący zabezpieczaniu przestrzeni cybernetycznej. Stanowi on techniczne centrum, znajdujące się w Brukseli oraz w Mons, całodobowo chroniące systemy i sieci, a także zapewniające specjalistyczne usługi w dziedzinie zapobiegania incydentom cybernetycznym, wykrywania ich i reagowania na nie. Zespół NCIRC zapewnia cyberodporność nie tylko systemom oraz sieciom należącym bezpośrednio do Sojuszu, lecz także wszystkim państwom członkowskim. Poddaje bowiem bieżącej analizie występujące cyberincydenty, następnie sporządza raporty, które są przekazywane krajom NATO, by miały wiedzę na temat występujących

11 *W Polsce tworzona jest armia cyberwojowników*, „Rzeczpospolita", https://www.rp.pl/Sluzby- mundurowe/305019924-W-Polsce-tworzona-jest-armia-cyberwojownikow.html#ap-1/. 6.09.2018.

TABELA. INSTYTUCJE I PLATFORMY NATO ZWIĘKSZAJĄCE ZDOLNOŚCI DO SKUTECZNEJ CYBEROBRONY

Placówka NATO	Siedziba	Zadania
Platforma NATO Cyber Range (nazywana także cyberpoligonami)	Tartu (Estonia)	opracowana w celu doskonalenia umiejętności cyberspecjalistów w dziedzinie cyberobrony przez symulowane ćwiczenia prowadzone w wirtualnym środowisku
Sojusznicze Centrum Doskonalenia Obrony przed Cyberatakami (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE)	Tallinn (Estonia)	ośrodek badawczo-szkoleniowy zajmujący się edukacją, badaniami i wszechstronnym rozwojem obrony cybernetycznej
Akademia ds. Łączności i Informacji NATO (NATO Communications and Information Academy)	Oeiras (Portugalia)	ośrodek szkoleniowy uruchomiony w trzecim kwartale 2019 roku, odpowiadający za szkolenie personelu cywilnego i wojskowego z cyberobrony systemów oraz sieci NATO
Szkoła NATO	Oberammergau (RFN)	prowadzi szkolenia na tematy cybernetyczne, by wspierać w tej dziedzinie politykę, doktrynę i procedury Sojuszu Północnoatlantyckiego
Kolegium Obrony NATO (NATO Defence College)	Rzym (Włochy)	wspiera strategiczne myślenie w sprawach polityczno-wojskowych, w tym w zakresie cyberobrony

Opracowano na podstawie dokumentów North Atlantic Treaty Organization, 2019.

współcześnie zagrożeń w cyberprzestrzeni. Organizacja Traktatu Północnoatlantyckiego, podobnie jak Unia Europejska, podejmuje działania wspierające państwa członkowskie w kwestiach związanych z ochroną i obroną przestrzeni cybernetycznej. Zalicza się do nich[12]:

– udostępnianie w czasie rzeczywistym informacji o cyberincydentach za pośrednictwem przeznaczonej do tego celu platformy wymiany informacji o złośliwym oprogramowaniu, a także najlepszych praktyk w radzeniu sobie z zagrożeniami cybernetycznymi;

– utrzymywanie zespołów cyberobrony do szybkiego reagowania, które mogą zostać wysyłane, by pomóc sojusznikom w radzeniu sobie z wyzwaniami cybernetycznymi;

– opracowanie wspólnych celów dla zrzeszonych państw dla ułatwienia spójnego i zrównoważonego podejścia do ich zdolności i możliwości w dziedzinie cyberobrony;

– inwestowanie w edukację, szkolenia i ćwiczenia, takie jak „Koalicja cybernetyczna" („Cyber Coalition"), będących jednymi z największych ćwiczeń cybernetycznych na świecie.

Dostrzegając potrzebę koordynowania i kontroli procesów zachodzących w cyberprzestrzeni, po szczycie NATO w Bukareszcie w 2008 roku powołano kolejną jednostkę – Radę NATO ds. Zarządzania Cyberobroną (*The Cyber Defense Management Board* – CDMB). Jej najważniejszym zadaniem jest ocena aktualnej zdolności państw Sojuszu do obrony przed cyberatakami, wzmacnianie tej zdolności narodowych systemów bezpieczeństwa cybernetycznego, a także integracja instytucji cywilnych z militarnymi w celu współpracy oraz wymiany doświadczeń[13]. Ze względu na to, że systemy i sieci NATO są coraz częściej narażone na cyberataki, powstał Zespół Szybkiego Reagowania (*Rapid Reaction Team* – RRT) w celu przywracania technicznej sprawności systemom będącym celem takiego ataku. Zespół jest postrzegany na międzynarodowym forum jako instytucja gotowa udzielić pomocy państwom członkowskim w przypadku zaistnienia cyberincydentu, co przekłada się na formę ostrzeżenia potencjalnych cyberprzestępców przed dokonaniem nielegalnego czynu[14]. Ponadto do jednostek odpowiedzialnych za cyberobronę należy *The Cyber Defence Committee*

12 NATO Cyber Defence, *Fact Sheets,* February 2019.

13 *NATO wobec wyzwań i zagrożeń w cyberprzestrzeni,* Biuletyn OPINIE FAE (7).

14 Ibidem, s. 7.

Sojusznicze Centrum Doskonalenia Obrony przed Cyberatakami w Tallinie zajmuje się edukacją, badaniami i wszechstronnym rozwojem obrony cybernetycznej.

CCDCOE

(CDC), będący przede wszystkim organem eksperckim zajmującym się doradzaniem państwom członkowskim w tej sferze oraz pełnieniem nadzoru nad spójnością polityki NATO na rzecz cyberobrony. Z kolei *The NATO Consultation, Control and Command* (NC3) jest zespołem o charakterze doradczym, jednocześnie odpowiedzialnym za udzielanie wskazówek, a także praktycznych porad dotyczących wdrażania rozwiązań obronnych zapobiegających cyberatakom w państwach Sojuszu. Należy nadmienić, że istnieją również zespoły, ośrodki szkoleniowe i grupy zewnętrzne, które pomagają NATO oraz poszczególnym państwom członkowskim w poprawie zdolności do cyberobrony ich systemów (tab.).

Organizacja Traktatu Północnoatlantyckiego współpracuje z wieloma partnerami, w tym z organizacjami międzynarodowymi, przedstawicielami przemysłu i środowiskiem akademickim. Cyberobrona jest jednym z obszarów zacieśnionej współpracy między NATO i Unią Europejską w ramach skoordynowanych wysiłków obu organizacji na rzecz przeciwdziałania zagrożeniom hybrydowym w cyberprzestrzeni. Sojusz i UE dzielą się informacjami na temat kryzysu cybernetycznego i wymieniają najlepszymi praktykami czy zaleceniami profilaktycznymi. NATO pomaga również zrzeszonym krajom w radzeniu sobie z wyzwaniami, jakie stanowią cyberzagrożenia. Należy nadmienić, że nie tylko przedstawiciele rządów państw członkowskich decydują o kierunkach polityki w zakresie cyberbezpieczeństwa i cyberobrony. Niezwykle ważną funkcję pełni także sektor prywatny, który również ma doświadczenie w sferze występujących cyberincydentów oraz sposoby niwelowania ich skutków. W celu nawiązania współpracy z tym sektorem i nakłonienia go do dzielenia się dobrymi praktykami NATO umacnia swoje stosunki z przemysłem za pośrednictwem inicjatywy *NATO Industry Cyber Partnership*. Platforma ta wspiera wysiłki Sojuszu dążącego do ochrony sieci, zwiększenia jej odporności oraz pomocy dla zrzeszonych krajów w rozwijaniu ich zdolności obrony cybernetycznej. Wymiana informacji, ćwiczenia, szkolenia i edukacja to tylko kilka obszarów, które mogą posłużyć za przykład współpracy NATO z prywatnym sektorem przemysłu. Zagrożenie coraz częstszymi cyberatakami może osiągnąć skalę, kiedy przerodzą się one w cyberkonflikt.

W związku z tym zasadne byłoby uwzględnienie w przyszłości w *Traktacie Północnoatlantyckim,* sporządzonym w Waszyngtonie 4 kwietnia 1949 roku, w odniesieniu do artykułu IV oraz artykułu V aspektów cyberobrony. Artykuł IV zobowiązuje państwa członkowskie do wzajemnych konsultacji za każdym razem, gdy w ich opinii zostanie zagrożona integralność terytorialna, bezpieczeństwo lub niezależność polityczna[15]. Na jego podstawie, w kontekście bezpieczeństwa cybernetycznego, może być dokonywana wymiana doświadczeń i dobrych praktyk między

15 *Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r.,* Stany Zjednoczone 1999, Dz.U. 2000 nr 87 poz. 970.

krajami, a na ich bazie kreowanie nowych rozwiązań zapobiegających zagrożeniom pochodzącym z cyberprzestrzeni. Natomiast artykuł V zobowiązuje do kolektywnej obrony. Oznacza to, że jeżeli którekolwiek z państw członkowskich położonych na terytorium Europy lub Ameryki Północnej zostanie zbrojnie napadnięte, pozostałe kraje bezzwłocznie podejmą działania w celu przywrócenia stabilizacji oraz bezpieczeństwa temu obszarowi. O wystąpieniu zbrojnej napaści na państwo Sojuszu zostanie natychmiast powiadomiona również Rada Bezpieczeństwa NATO. Biorąc pod uwagę treść artykułu V oraz konieczność dostosowania go do kwestii związanych z cyberkonfliktami, kontekst dyskusyjny nabiera znaczenie zbrojnej napaści. Otóż ataki i zagrożenia cybernetyczne nie mają żadnej materialnej formy, lecz mogą osiągać skalę równoznaczną z konwencjonalnym konfliktem między stronami. Z tego powodu każdy rodzaj konfliktu – zarówno konwencjonalny, jak i cybernetyczny – mający formę napaści na którekolwiek państwo Sojuszu powinien wymuszać reakcję obrony tego kraju przez NATO. Niestety artykuł V nie określa, jaka pomoc ma zostać udzielona napadniętemu państwu.

KONKLUZJE

Dokonując przeglądu aktów prawnych odnoszących się do zapewniania bezpieczeństwa w przestrzeni cybernetycznej, wyróżniono ich podział ze względu na porządek prawny obowiązujący w naszym kraju, w Unii Europejskiej oraz w Organizacji Traktatu Północnoatlantyckiego.

W odniesieniu do prawodawstwa polskiego bardzo ważną kwestią jest zawarcie w ustawie powszechnie obowiązującej definicji cyberprzestrzeni, która nawiązuje do terminów powiązanych z sektorem telekomunikacyjnym. Umieszczenie związanych z tym obszarem sformułowań w licznych dokumentach świadczy o tym, że wykorzystanie przestrzeni cybernetycznej może być uniwersalne. Stąd też konieczność zagwarantowania jej ochrony. Skonkretyzowane kierunki działań na rzecz cyberbezpieczeństwa najczęściej przybierają postać zmian w aspekcie prawnym, organizacyjnym i technicznym. Należy podkreślić, że analizowane dokumenty odnoszą się w największym stopniu do zagwarantowania właściwego funkcjonowania cyberprzestrzeni w kontekście bezpieczeństwa państwa. Nie istnieją natomiast akty prawne, które wyznaczałyby zakres tej działalności lub wynikające z niej ograniczenia i sankcje dla lotnictwa oraz eksploracji kosmosu. Powstanie w strukturach Urzędu Lotnictwa Cywilnego nowej komórki – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego daje nadzieję, że bezpieczeństwo cybernetyczne zostanie ujęte w krajowym prawodawstwie lotniczym, jakim jest *Ustawa „Prawo lotnicze" z dnia 3 lipca 2002 r.*, a także we współpracy z Polską Agencją Żeglugi Powietrznej powstanie program ochrony systemów radionawigacyjnych.

Wnioski z analizy prawodawstwa unijnego upoważniają do stwierdzenia, że pierwsze regulacje dotyczące cyberprzestrzeni nawiązują do ochrony obiegu w niej danych osobowych użytkowników. Unia Europejska jako organizacja międzynarodowa wdraża tego rodzaju innowacyjne rozwiązania również w państwach członkowskich, co stanowi wyzwanie w związku z prowadzeniem spójnej polityki cyberbezpieczeństwa oraz ujednolicaniem przepisów prawnych obowiązujących w poszczególnych krajach do standardów UE. Zachęca również do dzielenia się doświadczeniami oraz dobrymi praktykami na forum Wspólnoty. Niezwykle ważną kwestię stanowi wspólne, jednomyślne interpretowanie definicji powiązanych z cyberprzestrzenią. Obecna polityka cyberbezpieczeństwa skupia się na zagwarantowaniu ochrony operatorom usług kluczowych oraz dostawcom usług cyfrowych, na promowaniu aspektów bezpieczeństwa cyberprzestrzeni, jak również na kreowaniu nowych rozwiązań z uwzględnieniem występujących cyberzagrożeń.

Niestety, podobnie jak w przypadku prawodawstwa krajowego, wdrażanie procedur na rzecz cyberbezpieczeństwa na szczeblu europejskim nie jest praktykowane w lotnictwie i sektorze kosmicznym. Możliwość wystąpienia jakiegokolwiek rodzaju cyberzagrożenia jest ujmowane wyłącznie w kontekście projektowania i eksploatacji statków powietrznych, a także kontroli tych procesów w celu unikania tego rodzaju zagrożeń. Co prawda Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego opracowała program odnoszący się do bezpieczeństwa cybernetycznego, lecz obecnie trwają dopiero prace nad jego wdrożeniem. Organizacja podejmuje działania na rzecz międzynarodowej integracji zrzeszonych państw, czemu może przysłużyć się strategiczna europejska platforma koordynacji pozwalająca krajom na wymianę doświadczeń. Jedną z kluczowych inicjatyw jest utworzenie Centrum Bezpieczeństwa Cybernetycznego w Europie, które umożliwiłoby kompatybilne połączenie z CERT-EU, jak również wymianę informacji o lotniczych incydentach w cyberprzestrzeni.

Polityka Organizacji Traktatu Północnoatlantyckiego w obszarze obrony przed zagrożeniami pochodzącymi z cyberprzestrzeni oraz ochrony własnych systemów opiera się głównie na powoływaniu wyspecjalizowanych komórek w strukturach NATO oraz instytucji zewnętrznych. Ich zróżnicowane misje po rozwinięciu pełnych zdolności operacyjnych mogą zapewnić kompleksową obronę i ochronę cyberprzestrzeni, które są zadaniami stosunkowo prostszymi do wykonania niż aktywna walka z cyberprzestępczością. Niestety podczas szczytów NATO nie dyskutowano ani nie podejmowano żadnych działań ukierunkowanych na zapewnienie ochrony wojskowym systemom telekomunikacyjnym w lotnictwie lub tym stosowanym w przestrzeni kosmicznej.

Przytoczone akty prawne w prawodawstwie polskim i unijnym oraz sposoby realizacji polityki cyberbezpieczeństwa nie wyczerpują jednak tematu. ■

Dwa lata CYBER.MIL.PL

CYBERBEZPIECZEŃSTWO TO FUNDAMENT FUNKCJONOWANIA W DOBIE WSZECHOBECNEGO INTERNETU. ODNOSI SIĘ ZARÓWNO DO INDYWIDUALNYCH UŻYTKOWNIKÓW KORZYSTAJĄCYCH Z SIECI, JAK I GLOBALNYCH KORPORACJI, PAŃSTW ORAZ NARODÓW.

Autor był w latach 2018–2020 sekretarzem stanu w Ministerstwie Obrony Narodowej, pełnomocnikiem ministra obrony narodowej do spraw bezpieczeństwa w cyberprzestrzeni.

Tomasz Zdzikot

Wzrastająca rola cyfrowych technologii, które stanowią nieodzowny element niemal wszystkich usług i procesów decyzyjnych, sprawia, że umiejętność zapewnienia bezpieczeństwa obywateli także w tym wymiarze oraz zdolność do zabezpieczenia własnych sieci i systemów dołączyły do podstawowych wyzwań w sferze bezpieczeństwa narodowego. W związku z tym cyberprzestrzeń znalazła się w sposób oczywisty w polu zainteresowania państw członkowskich oraz struktur Sojuszu Północnoatlantyckiego. Biorąc pod uwagę stan zaawansowania technologicznego, za wizjonerską należy uznać potrzebę zapewnienia obrony przed atakami cybernetycznymi wyartykułowaną podczas szczytu NATO w Pradze w 2002 roku. Ważne decyzje w ramach Sojuszu zostały podjęte później. Kluczowe znaczenie miały w tym względzie szczyty w 2014, 2016 i 2018 roku. W deklaracji końcowej szczytu NATO, który odbył się w Walii w 2014 roku, potwierdzono, że zagrożenia i ataki cybernetyczne będą coraz częstsze, bardziej złożone i potencjalnie o niszczącym działaniu. Jednocześnie podkreślono, że obrona cybernetyczna należy do podstawowych zadań kolektywnej obrony Sojuszu.

POCZĄTKI

Podczas szczytu NATO w 2016 roku w Warszawie uznano cyberprzestrzeń za obszar działań, w którym należy bronić się tak samo skutecznie, jak w powietrzu, na lądzie czy morzu. Natomiast szczyt NATO w Brukseli w 2018 roku poza podkreśleniem znaczenia tej nowej domeny w działaniach bojowych przyniósł także decyzje o utworzeniu Centrum Operacji w Cyberprzestrzeni (*Cyberspace Operations Centre* – CyOC), jak również zespołów przeciwdziałania zagrożeniom hybrydowym (*Counter Hybrid Support Team* – CHST), które na prośbę krajów członkowskich mogą zostać wysłane do nich w celu wsparcia ich działań narodowych.

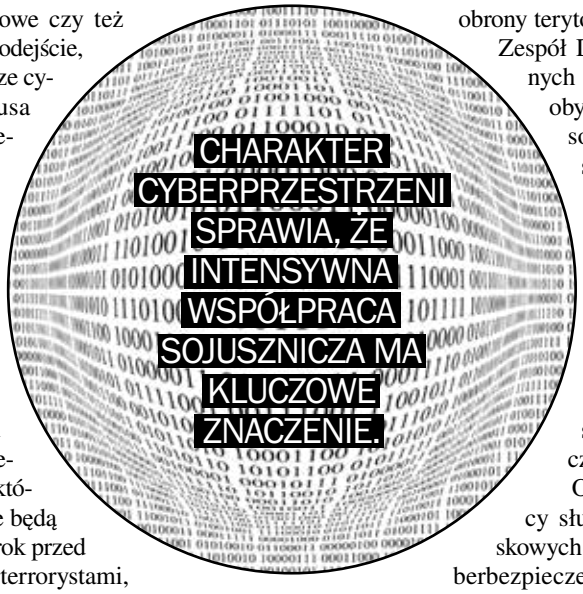
Istotne znaczenie cyberbezpieczeństwa znajduje także wyraz w przepisach prawa. W polskim porządku prawnym do zakresu działania administracji rządowej w dziedzinie obrony narodowej, którą kieruje minister obrony narodowej, należą w czasie pokoju sprawy bezpieczeństwa cyberprzestrzeni w wymiarze militarnym. W wymiarze cywilnym pozostają w dziale informatyzacji. Ustawodawca starał się więc wydzielić z całości spraw cyberbezpieczeństwa obszar militarny związany z działalnością Sił Zbrojnych RP oraz osiąganiem zdolności do samodzielnego lub sojuszniczego działania. Ogólnie zakreślony zakres zadań został skonkretyzowany w uchwalonej w lipcu 2018 roku ustawie o krajowym systemie cyberbezpieczeństwa, która w rozdziale 10 wyszczególnia zadania ministra obrony narodowej. Są one związane zarówno z zapewnianiem i rozwijaniem zdolności Sił Zbrojnych RP w tej dziedzinie, z pozyskiwaniem narzędzi i współpracą z NATO, jak i rozbudową kompetencji w czasie stanu wojennego oraz z kierowaniem reakcją na incydenty włącznie. Również z odpowiedzialnością za prowadzenie jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (*Computer Security Incident Response Team* – CSIRT MON).

Mając na względzie zobowiązania prawne i sojusznicze, na początku 2018 roku przystąpiono w Mini-

sterstwie Obrony Narodowej do prac nad skonstruowaniem programu budowy zdolności Sił Zbrojnych RP do działania w cyberprzestrzeni.

Podczas konferencji zorganizowanej 5 lutego 2019 roku w Wojskowej Akademii Technicznej zaprezentowano założenia programu CYBER.MIL.PL. Po nieco ponad dwóch latach wdrażania programu warto podsumować dotychczasowe działania, w ramach których zrealizowano zamierzenia strategiczne, często szybciej niż przewidziano w harmonogramach.

Przygotowując koncepcję strategiczną programu oraz składający się na nią katalog projektów i zamierzeń, założono, że największym kapitałem i przewagą konkurencyjną naszego kraju w cyfrowym świecie są zasoby ludzkie. Nasi informatycy, kryptolodzy i matematycy będą głównym elementem nowej architektury bezpieczeństwa tak bardzo zależnej od technologii. Prymat człowieka, jego zdolności i woli nad technologią to nie jest nowe czy też szczególnie przełomowe podejście, jednak z pewnością w sferze cyberbezpieczeństwa pokusa bezkrytycznego zawierzenia i oparcia się jedynie na technologii jest szczególnie silna. Cyberprzestrzeń to jedyna domena wykreowana w całości przez człowieka. W jej ramach wszystkie pojawiające się rozwiązania mają służyć użytkownikom i z myślą o nich powstają, o ich zaś bezpieczeństwo dbać muszą ci, których wysokie kompetencje będą pozwalały być zawsze o krok przed cyberprzestępcami, cyberterrorystami, czy po prostu służbami specjalnymi i siłami zbrojnymi innych państw.



TWORZENIE SYSTEMU

Program CYBER.MIL.PL został podzielony na cztery filary. Pierwszy – to konsolidacja i budowa struktur cyberbezpieczeństwa; drugi – edukacja, szkolenie i trening; trzeci – współpraca i budowanie silnej pozycji międzynarodowej oraz czwarty – podniesienie poziomu bezpieczeństwa resortowych i militarnych sieci oraz systemów. W ramach konsolidacji i budowania struktur cyberbezpieczeństwa utworzono czytelne podstawy funkcjonowania resortowego ekosystemu cyberbezpieczeństwa, w którym kluczową rolę odgrywa Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, wspierany przez Zespół Pełnomocnika, w skład którego wchodzą między innymi przedstawiciele Sztabu Generalnego WP, wojskowego wywiadu i kontrwywiadu oraz innych jednostek i komórek organizacyjnych resortu. Z połączenia i przeformowania Inspektoratu Informatyki oraz Narodowego Centrum Kryptologii powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), na którego czele stoi gen. bryg. Karol Molenda, pełniący równocześnie funkcję pełnomocnika MON ds. utworzenia wojsk obrony cyberprzestrzeni (WOC). W ramach NCBC sformowano też CSIRT (*Computer Security Incident Response Team*) MON, czyli jeden z trzech wspomnianych już zespołów reagowania na incydenty bezpieczeństwa komputerowego [obok CSIRT GOV, prowadzonego przez szefa ABW, i CSIRT NASK, za który odpowiada NASK-PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy)], działających na poziomie krajowym. Postępują także prace zmierzające do utworzenia kolejnego rodzaju wojsk, czyli wojsk obrony cyberprzestrzeni. Od 2020 roku w ramach NCBC działa grupa organizacyjna ds. sformowania dowództwa WOC. W strukturze wojsk obrony terytorialnej powstał natomiast Zespół Działań Cyberprzestrzennych jako oferta dla polskich obywateli, którzy mając wysokie kompetencje w obszarze cyfrowym, chcą łączyć pracę zawodową ze służbą wojskową. Rekrutacja to zresztą niezwykle ważny aspekt, dlatego w 2020 roku uruchomiono specjalną infolinię na temat służby i pracy w resortowych strukturach cyberbezpieczeństwa.

Obecnie żołnierze pełniący służbę w jednostkach wojskowych odpowiedzialnych za cyberbezpieczeństwo, kryptologię oraz projekty informatyczne, należący do grup osobowych kryptologii, cyberbezpieczeństwa i projektowo-programowej informatyki, zgodnie z rozporządzeniem ministra obrony narodowej z lutego 2020 roku w sprawie dodatków do uposażenia zasadniczego żołnierzy otrzymują dodatek służbowy o charakterze stałym z tytułu zajmowania stanowiska służbowego, a także jednorazowy dodatek służbowy po zakończeniu roku kalendarzowego. Stały miesięczny dodatek służbowy to kwota w wysokości od 450 zł do 2100 zł, natomiast dodatek roczny o charakterze uznaniowym wynosi od 100 do 620% kwoty dodatku miesięcznego. Wyszkolenie i pozyskanie takiego specjalisty to jedno, natomiast utrzymanie go w służbie – to drugie.

Niezwykle ważna jest też interdyscyplinarna analiza strategiczna, dlatego powstały nowe *think tanki*: przy Akademii Marynarki Wojennej – Morskie Centrum Cyberbezpieczeństwa oraz przy Akademii Sztuki Wojennej – Akademickie Centrum Polityki Cyberbezpieczeństwa. Rozporządzeniem zaś Rady Ministrów Wojsko-

wemu Instytutowi Łączności im. prof. dr. hab. Janusza Groszkowskiego 1 października 2020 roku nadano status Państwowego Instytutu Badawczego, kończąc w ten sposób długotrwałą procedurę związaną z dokonaniem zewnętrznej oceny dotychczasowej działalności Instytutu. Do jego zadań będzie należało zapewnienie ochrony kryptologicznej, w tym projektowanie algorytmów i protokołów kryptograficznych oraz prowadzenie prac z zakresu kryptoanalizy, a także cyberbezpieczeństwa i rozpoznawania cyberzagrożeń.

ZAPEWNIENIE KADR

Należy przy tym pamiętać, że o specjalistów z dziedziny cyberbezpieczeństwa trwa prawdziwy wyścig, w którym biorą udział zarówno międzynarodowe korporacje, jak i krajowe firmy wielu branż, operatorzy infrastruktury krytycznej, administracja państwowa i samorządowa oraz służby mundurowe i specjalne. W tej międzysektorowej rywalizacji sektor publiczny, do którego zalicza się siły zbrojne, jest często w trudnej sytuacji ze względu na ograniczone możliwości stosowania zachęt finansowych. W przypadku sił zbrojnych to także kwestia wysokich wymagań stawianych samym kandydatom, dotyczących m.in.: kondycji fizycznej, umiejętności funkcjonowania w strukturach hierarchicznych, czy wreszcie nieposzlakowanego życiorysu i przymiotów charakterologicznych pozwalających uzyskać poświadczenie bezpieczeństwa umożliwiające dostęp do resortowych systemów informatycznych. Dlatego tak istotna jest umiejętność wykorzystania wszelkich atutów będących w zasięgu oddziaływania sektora militarnego.

Uznano, że jednym z nich jest rozbudowa i właściwe wykorzystanie resortowego systemu kształcenia i doskonalenia zawodowego. Ukończenie pięcioletnich studiów w murach uczelni wojskowej i wieńcząca je promocja oficerska pozwalają oczekiwać, że decyzja o związaniu się młodego człowieka z siłami zbrojnymi była przemyślana – stanowi świadomy wybór ścieżki życiowej. Spośród pięciu wojskowych akademii, dziś dwie: Wojskowa Akademia Techniczna oraz Akademia Marynarki Wojennej – prowadzą studia o specjalnościach związanych z szeroko rozumianym obszarem cyfrowym. W WAT to kryptologia i cyberbezpieczeństwo, informatyka oraz elektronika i telekomunikacja, w AMW zaś informatyka i systemy informacyjne w bezpieczeństwie. Dlatego też postanowiono zwiększyć liczbę podchorążych na tych kierunkach. Przykładowo w roku akademickim 2015/2016 limit na kierunku kryptologia i cyberbezpieczeństwo w WAT wynosił 15 miejsc. W roku akademickim 2020/2021 liczba przyjętych na studia zwiększyła się do 116. Od 2015 roku łączny limit przyjęć na studia w uczelniach wojskowych uległ prawie potrojeniu – z 522 do 1461 (w przypadku AMW o ponad 450% więcej – z 28 do 130). W odniesieniu do studiów o specjalnościach cyfrowych to wzrost ze 146 miejsc do 500, a zatem o ponad 340%. Oczywiście proces kształcenia jest długotrwały, jednak podjęte decyzje zapewnią w najbliższych latach stały dopływ kadr do nowego rodzaju wojsk. Jest to koncepcja, w myśl której rozwój istniejących jednostek, których zadaniem jest prowadzenie operacji w cyberprzestrzeni, a także formowanie wojsk obrony cyberprzestrzeni będą się opierać na kadrach kształconych w uczelniach wojskowych. Korpus podoficerów to zaś domena Szkoły Podoficerskiej SONDA, utworzonej w październiku 2019 roku. Jej zadaniem jest między innymi kształcenie kandydatów na podoficerów o specjalności łączność i informatyka.

Dbając o jak najlepsze przygotowanie i predyspozycje kandydatów aspirujących do podjęcia studiów wojskowych, a następnie wstąpienia do służby w sektorze cyberbezpieczeństwa, rozwijana jest również oferta edukacyjna adresowana do młodzieży szkół średnich. Pierwszoplanową rolę odgrywa tu utworzone przez MON w lutym 2019 roku WOLI, czyli Wojskowe Ogólnokształcące Liceum Informatyczne przy Wojskowej Akademii Technicznej, któremu nadano imię „Polskich Kryptologów". Pilotażowo w 2019 roku, a w pełnym wymiarze w roku 2020 ruszył też program CYBER.MIL z Klasą, mający charakter eksperymentu pedagogicznego, w ramach którego w 16 zakwalifikowanych do udziału w skali kraju szkołach ponadpodstawowych powstają klasy realizujące program o profilu cyberbezpieczeństwo i nowoczesne technologie informatyczne. Organ prowadzący szkołę może liczyć na pokrycie do 80% kosztów realizacji tego programu z dotacji celowej udzielanej przez MON.

Ważną częścią edukacyjnego systemu jest również funkcjonujący od kilku lat program ochotniczego przeszkolenia wojskowego studentów cywilnych w ramach Legii Akademickiej. Od 2019 roku jej moduł szkoleniowy został rozszerzony o komponent cyberbezpieczeństwa realizowany przez NCBC według specjalnie zaprojektowanej ścieżki kształcenia. Wzbudzenie zainteresowania tematyką cyberbezpieczeństwa i kryptologii oraz poszukiwanie wartościowych współpracowników było też podstawą do ustanowienia Nagrody im. Mariana Rejewskiego za najlepszą pracę inżynierską, licencjacką i magisterską oraz rozprawę doktorską poświęconą cyberbezpieczeństwu i kryptologii. Po raz pierwszy została przyznana w roku 2019. W Akademii Sztuki Wojennej jest wydawane od tegoż roku nowe dwujęzyczne czasopismo naukowe „Cybersecurity & Law", którego łamy są otwarte dla ekspertów i naukowców zajmujących się tą dziedziną wiedzy.

W ramach doskonalenia zawodowego na uczelniach wojskowych przygotowano ofertę w postaci specjalistycznych studiów podyplomowych, w tym studiów z zakresu zarządzania cyberbezpieczeństwem w WAT, których druga edycja, mimo ograniczeń związanych z pandemią, dobiega końca. Resort, dzięki zaangażowaniu Akademii Marynarki Wojennej, konsekwentnie realizuje również projekty szkoleniowo-eksperckie w ramach letniej i zimowej szkoły cyberbezpieczeństwa. Kluczowe znaczenie dla przyszłości ma decyzja dotycząca działającego już Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa (ECSC). Według za-

twierdzonej przez ministra obrony narodowej w lipcu 2020 roku koncepcji Centrum szkoli żołnierzy i pracowników wojska, a także podnosi kwalifikacje osób odpowiedzialnych za prowadzenie działań w cyberprzestrzeni. ECSC ma się stać jednym z podstawowych ogniw w systemie cyberbezpieczeństwa państwa, przygotowując najwyższej klasy ekspertów na wszystkich poziomach dowodzenia Sił Zbrojnych RP.

Niezwykle istotne, zwłaszcza z perspektywy szans rekrutacyjnych, jest budowanie marki cyberkomponentu sił zbrojnych i jego rozpoznawalności z uwzględnieniem wizerunku, motywacji i wyzwań, w tym związanych ze stałą interakcją z dobrze przygotowanym i silnie zmotywowanym przeciwnikiem. Dlatego przedstawiciele resortu są obecni na wszystkich znaczących spotkaniach i konferencjach. Ponadto MON od 2019 roku jest partnerem największego stacjonarnego *hackathonu* w Europie, przygotowując zadania w kategorii *cybersecurity*. W tymże roku Ministerstwo było również między innymi gospodarzem NATO TIDE Hackathon, organizowanego przez NATO ACT, a jego przedstawiciele wygrali konkurs w dwóch z trzech kategorii. Sukcesy przedstawicieli resortu w międzynarodowych zawodach i konkursach, jak choćby czołowe lokaty w ćwiczeniach „Locked Shields", potwierdzają, że mamy wybitnych specjalistów. Podstawowym zatem zadaniem jest tworzenie odpowiednich warunków do wykorzystania ich potencjału. To także jeden z elementów budowania silnej pozycji międzynarodowej naszego kraju w obszarze cyberbezpieczeństwa, co należy do trzeciego filaru programu CYBER.MIL.PL.

INICJATYWY MIĘDZYNARODOWE

Charakter cyberprzestrzeni sprawia, że intensywna współpraca sojusznicza ma kluczowe znaczenie. W tym celu w lipcu 2019 roku rząd naszego kraju podpisał Memorandum of Understanding (MoU) z Sojuszem Północnoatlantyckim. Porozumienie określa ramy współdziałania w dziedzinie cyberobrony. Również w 2019 roku zawarto porozumienie o współpracy ze Stanami Zjednoczonymi. W ramach umowy będą podejmowane działania polegające na wymianie informacji oraz wspólnym rozwijaniu zdolności ukierunkowanych na skoordynowane działania obronne, w tym również wspólne ćwiczenia. W styczniu 2020 roku podpisano w Warszawie porozumienie z Republiką Korei Południowej o współpracy resortów obrony narodowej w obszarze cyberbezpieczeństwa. To także partner o ogromnym potencjale i doświadczeniu, szczególnie w reagowaniu na incydenty związane z działalnością niezwykle aktywnych w tej sferze aktorów azjatyckich.

W grudniu 2020 roku zawarto porozumienie o współpracy między NCBC oraz Zarządem J6 i Cyberobrony Sił Obronnych Izraela. Na jego podstawie możliwa będzie między innymi wymiana informacji i doświadczeń oraz prowadzenie wspólnych szkoleń i realizowanie przedsięwzięć edukacyjnych.

Uczestnicząc w projekcie Cyber Rapid Reponse Teams and Mutual Assistance in Cyberspace, podjętym w ramach Stałej Współpracy Strukturalnej UE (PESCO), w marcu 2020 roku w Zagrzebiu zawarto porozumienie z szefami resortów obrony Chorwacji, Estonii, Litwy, Holandii i Rumunii. Na jego mocy już w 2021 roku nasz kraj przejął na rok rolę koordynatora oraz międzynarodowego Zespołu Szybkiego Reagowania w Cyberprzestrzeni.

WIELE PRZED NAMI

Ze względu na specyfikę i niejawny charakter działań najtrudniej podsumować prace prowadzone w ramach czwartego filaru programu CYBER.MIL.PL.

Podkreślenia wymaga fakt ujęcia potrzeb związanych z cyberbezpieczeństwem w dokumentach planistycznych MON. Zarówno w *Priorytetowych kierunkach badań*, jak i w *Planie modernizacji technicznej Sił Zbrojnych RP* przewidziano realizację projektów w obszarze kryptologii i cyberbezpieczeństwa, w tym związanych z tworzeniem narzędzi i oprogramowania. Wciąż rozbudowywany jest istotny w tym kontekście kompleks NCBC, który w 2020 roku wzbogacił się o kolejne dwa ośrodki: Centrum Obliczeniowo-Projektowe oraz Centrum Projektowo-Konstrukcyjne.

Wśród wielu działań, takich jak modernizacja pokładowej sieci transmisyjnej IPRON czy opracowanie wstępnych założeń taktyczno-technicznych dotyczących systemu ochrony kryptograficznej nowej generacji, zwraca uwagę projekt „Merkury". Jest to zaprojektowany, wytworzony i wdrożony przez NCBC komunikator zapewniający bezpieczną komunikację tekstowo-głosową oraz możliwość bezpiecznego dzielenia się plikami multimedialnymi. W ramach kompleksowego projektu dbałość o wysoki poziom bezpieczeństwa usługi obejmuje zabezpieczenia kryptograficzne, a także poszczególne części składowe systemu, takie jak infrastruktura, środowiska serwerowe, czy bezpieczne mobilne łącza komunikacyjne.

Przedstawione przedsięwzięcia to nadal niepełny zbiór inicjatyw podejmowanych w ramach programu CYBER.MIL.PL. W ciągu zaledwie dwóch lat zrealizowano już setki mniejszych, większych i naprawdę strategicznych projektów. Program wciąż się rozwija, stwarzając warunki dla kolejnych przedsięwzięć. Resort obrony narodowej jako jedyny dysponuje zasobami niezbędnymi do utworzenia i rozwoju kompletnego ekosystemu cyberbezpieczeństwa. Składają się na niego zarówno jednostki wojskowe, jak i uczelnie wyższe, szkoły średnie, instytuty badawcze czy *think tanki*. To także sektor gospodarczy realizujący zamówienia na rzecz Ministerstwa Obrony Narodowej. Zapewnienie cyberbezpieczeństwa w wymiarze krajowym i sojuszniczym wymaga zaangażowania i współpracy wielu sektorów, instytucji i osób. Program CYBER.MIL.PL, którego wyróżnikiem są konkretne cele oraz skuteczność we wdrażaniu kolejnych projektów, pozwolił na wyzwolenie znaczącego, często ukrytego potencjału. Oby tak dalej. ■

O SPECJALISTÓW Z DZIEDZINY CYBERBEZPIECZEŃSTWA TRWA PRAWDZIWY WYŚCIG, W KTÓRYM BIORĄ UDZIAŁ ZARÓWNO MIĘDZYNARODOWE KORPORACJE, JAK I KRAJOWE FIRMY ORAZ SŁUŻBY MUNDUROWE I SPECJALNE.

Protokół kryptograficzny – Secure Communication Interoperability Protocol

ZAPEWNIENIE BEZPIECZNEJ WYMIANY INFORMACJI NIEJAWNYCH MIĘDZY WSPÓŁDZIAŁAJĄCYMI ZGRUPOWANIAMI RÓŻNYCH PAŃSTW STANOWI DUŻE WYZWANIE DLA ICH INFRASTRUKTUR ZARZĄDZANIA KLUCZAMI KRYPTOGRAFICZNYMI.

kmdr por. Paweł Kamiński

Autor jest starszym specjalistą w Wydziale Bezpieczeństwa Kryptograficznego Oddziału Bezpieczeństwa Systemów Łączności i Informatyki w Zarządzie Wsparcia Dowodzenia i Łączności Inspektoratu Rodzajów Wojsk DGRSZ.

W trakcie planowania i wdrażania zabezpieczenia teleinformatycznego dla wielonarodowych sił NATO zidentyfikowano jeden z problemów, który wiąże się z bezpiecznym (poufnym) przekazywaniem informacji między jednostkami wojskowymi. Dotyczy on zapewnienia bezpiecznej wymiany informacji na wszystkich poziomach dowodzenia, ze szczególnym uwzględnieniem poziomu taktycznego w heterogenicznym środowisku telekomunikacyjnym. O ile wszystkie jednostki dysponują środkami łączności będącymi w stanie nawiązać i utrzymywać jawną łączność, opierając się na przyjętych standardach i procedurach, o tyle w wypadku urządzeń zapewniających poufność przesyłanych danych brakuje obowiązujących standardów wymiany informacji niejawnych z zachowaniem ich poufności, integralności oraz sposobów uwierzytelnienia[1].

Dodatkowy problem stwarza zagwarantowanie poprawnej, nieprzerwanej dystrybucji kluczy kryptograficznych, zapewniających poufność, zwłaszcza na poziomie taktycznym przy dużej liczbie urządzeń kryptograficznych oraz ich wymianie. Panaceum na przedstawione problemy oraz na realizację kryptograficznych wymagań wydawał się być projekt bezpiecznej komunikacji głosowej (*Secure Communication Interoperability Protocol* – SCIP).

GENEZA

Amerykańskie Ministerstwo Obrony Narodowej (DoD), we współpracy z National Security Agency (NSA) w ramach projektu wspierającego bezpieczną komunikację multimedialną (*Future Narrowband Digital Terminal* – FNDT)[2], rozpoczęło prace nad opracowaniem standardu, który miał zastąpić wykorzystywane aparaty telefoniczne z modułem kryptograficznym STU III. Projekt ten został udostępniony krajom NATO i przekształcony w projekt SCIP, ponieważ był kompatybilny z koncepcją zmiany infrastruktury informacyjnej (*NATO Network Enabled Capabilities* – NNEC). Stwarzał on również szansę na unifikację urządzeń kryptograficznych krajów członkowskich. Pomysł NNEC opiera się na założeniu posiadania systemów

1 *Secure Communications Interoperability Protocol,* J.S. Collura, RTO Meeting Proceeding Paper, 2006.

2 *The Future Narrowband Digital Terminal*, E.J. Daniel, K.A. Teague, R. Sleezer, J. Brewer, J. Ramond, W.J. Beck, J. Hershberger, *The 2002 45th Midwest Symposium on Circuits and Systems,* 2002. MWSCAS-2002, pp. II-589 - II-592 vol. 2.

zdolnych do tworzenia sieci komunikacyjnych w celu wymiany informacji między wszystkimi krajami członkowskimi NATO i państwami sprzymierzonymi. Dokumenty standaryzacyjne protokołu SCIP zostały opracowane przez General Dynamics na zamówienie NSA. Za rozwój i aktualizację dokumentacji odpowiadała International Interoperability Working Group, a obecnie nadzór nad pracami został przekazany do NATO Communication and Information Agency (NCIA).

Założenia do opracowania protokołu SCIP dla urządzeń kryptograficznych zostały zebrane i usystematyzowane w 2005 roku przez państwa NATO, które uczestniczyły w pracach standaryzacyjnych. Skupiały się one na opracowaniu standardu kryptograficznego, umożliwiającego budowę urządzeń zapewniających sygnalizację i kryptografię w telekomunikacyjnych środowiskach heterogenicznych. Główny nacisk położono na możliwość pracy urządzeń w dowolnych systemach teleinformatycznych, wykorzystujących różnorodne technologie transportowe, takie jak: w sieciach przewodowych PSTN, ISDN, sieciach pakietowych, opartych na protokołach IPv4 (TCP, UDP, RTP, RTCP, VoIP), oraz w sieciach bezprzewodowych: GSM, TETRA, HF i VHF[3]. Urządzenia zgodne z protokołem SCIP miały być zdolne do współpracy z szeroką gamą urządzeń telekomunikacyjnych, które są w stanie zapewnić poprawne zestawienie kanału transmisyjnego, umożliwiając tym samym zastosowanie protokołu SCIP w ich różnych heterogenicznych systemach łączności.

Strategia bezpiecznej komunikacji fonicznej NATO (*NATO Secure Voice Strategy*) zdefiniowała kluczowe filary, które gwarantowały osiągnięcie interpretacyjnego standardu zapewniającego bezpieczną komunikację foniczną E2E (*End to End*) – użytkownik – użytkownik oraz użytkownik – proces[4]. Jednym z podstawowych założeń było zapewnienie przez urządzenia SCIP możliwości zarówno przesyłania informacji w warstwie aplikacji oraz poufności informacji fonicznych, jak i transmisji danych. Do najważniejszych filarów protokołu SCIP zaliczamy:

– zdolność do operowania w ewoluujących, różnorodnych technologiach sieciowych dzięki oparciu protokołu sygnalizacyjnego i kryptograficznego na warstwie aplikacji, natomiast pozostawienie problemu zestawienia kanałów transmisyjnych urządzeniom odpowiedzialnym za warstwy transportowe;

– dostępność nowych technologii kryptograficznych polegającą na możliwości implementacji i wykorzystania narodowych czy też nowych mechanizmów kryptograficznych – jako minimalne wymagania interoperacyjności urządzeń implementujących protokół SCIP;

– zapewnienie interoperacyjności dzięki znormalizowanemu protokołowi sygnalizacji oraz negocjacji mechanizmów kryptograficznych, które będą wykorzystywane w celu zestawienia i zapewnienia bezpiecznej komunikacji;

– zapewnienie uproszczonego systemu dystrybucji kluczy. Urządzenia z zaimplementowanym protokołem miały być zdolne do wykorzystania infrastruktury klucza publicznego lub też funkcjonowania zgodnie z kryptografią asymetryczną w celu negocjacji klucza do szyfrowania danych (*Transmission Encryption Key* – TEK). Pozwoli to wyeliminować jedną z głównych trudności w zabezpieczeniu kryptograficznym danych – fizyczną dystrybucję kluczy kryptograficznych opartą na mechanizmach zaopatrywania kryptograficznego infrastruktury zarządzania kluczami.

OGÓLNA CHARAKTERYSTYKA

W myśl *Strategii bezpiecznej komunikacji fonicznej NATO* protokół SCIP jest standardem, który umożliwia bezpieczną wymianę informacji fonicznych oraz danych zgodnie z przyjętymi standardami kryptograficznymi, zapewniającymi kryptograficzną interoperacyjność. Protokół SCIP pozwala na zestawienie poufnej transmisji danych w warstwie aplikacji modelu OSI w relacjach punkt–punkt oraz punkt–wielopunkt.

Osadzenie protokołu SCIP w warstwie aplikacji zapewnia interoperacyjność z systemami telekomunikacyjnymi, które zestawiają łącza transmisji danych, weryfikują poprawność przesłanych danych oraz utrzymują parametry warstwy fizycznej. Sam protokół, po zestawieniu łącza transmisyjnego, zapewnia odpowiednią sygnalizację zarządzającą przepływem danych oraz negocjuje bądź też narzuca określone parametry pracy i mechanizmy kryptograficzne. Poczynając od sygnalizacji rozpoczęcia i zakończenia transmisji danych, przekazywania raportów potwierdzających otrzymanie przesyłanych ramek, zliczania i weryfikacji ich poprawności, żądania ponownego ich przesłania, kończąc na ustalaniu parametrów przesyłanych danych, wymianie informacji o posiadanych kluczach, wymianie certyfikatów czy na synchronizacji kryptograficznej.

Standard SCIP umożliwia prace w następujących trybach:

– bezpiecznej wymiany informacji fonicznych (*Secure Voice*);

– bezpiecznej wymiany danych (*Secure Data*);

– wymiany danych o podwyższonym poziomie bezpieczeństwa (*Enhanced Secure Data*);

– przesyłania informacji fonicznych z wykorzystaniem kodeka MELP (*Clear MELP Voice*);

– bezpiecznego przesyłania danych multimedialnych (*Secure Multimedia*);

– przesyłania informacji fonicznych (*Native Voice, Clear Voice*);

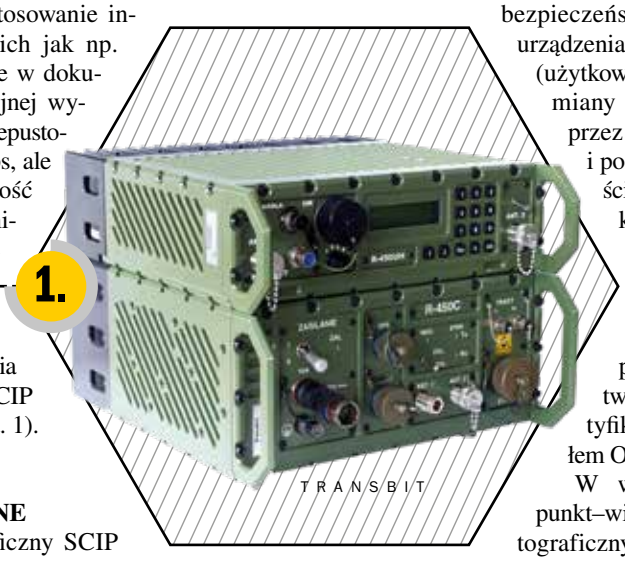
– bezpiecznej, elektronicznej wymiany kluczy (*Secure Electronic Rekey*).

3 *SCIP 220 Requirement Document.*

4 *Open Framework for The NATO Secure Voice Strategy,* K.D. Tuchs, R.B. Monleon, H. Wietgrefe, A. Alkassar, T. Korte, *The 2010 Military Communication Conference – Unclassified Program – System Perspective Track.*

Minimalne wymagania funkcjonalności protokołu SCIP, określone w *Minimum Implementation Protocol* (MIP), zapewniają interoperacyjność urządzeń, implementujących ten protokół, oraz umożliwiają bezpieczną i bezproblemową wymianę informacji między użytkownikami. W minimalnych wymaganiach interoperacyjności wymienione są mechanizmy kryptograficzne, zasady zestawienia połączenia, wymagane kodeki głosu, a także wymagane tryby pracy i inne[5].

Wskazane w MIP kodeki głosu, takie jak *Mixed Excitation Linear Prediction – enhanced* (MELPe), zapewniające stosunkowo wysoką jakość dźwięku przy prędkości transmisji danych 2,4 Kbps i opcjonalnie dopuszczone stosowanie innych wokoderów, takich jak np. G.729.D, które są ujęte w dokumentacji standaryzacyjnej wymagającej większej przepustowości łącza od 6,4 Kbps, ale zapewniają lepszą jakość dźwięku[6], definiując minimalną przepustowość łącza telekomunikacyjnego w celu zapewnienia działania protokołu SCIP w trybie fonicznym (fot. 1).



Radiostacja wielozakresowa R-450W z wewnętrznym modułem szyfrującym, opartym na protokole SCIP – zgodnym ze STANAG-iem 5068

MECHANIZMY KRYPTOGRAFICZNE

Protokół kryptograficzny SCIP w dokumentach standaryzacyjnych zawiera dwa modele zarządzania kluczami kryptograficznymi: czyli ogólny model zarządzania kluczami symetrycznymi i asymetrycznymi oraz zarządzania kluczami z wykorzystaniem infrastruktury klucza publicznego (*Public Key Infrastructure* – PKI) i standardu X.509.

Model ogólny jest oparty na istniejących narodowych i natowskich infrastrukturach zarządzania kluczami (*Key Management Infrastructure* – KMI) z wykorzystaniem elektronicznych systemów do zarządzania dystrybucją kluczy symetrycznych i asymetrycznych. Zarządzanie kluczami asymetrycznymi zbudowano na podstawie centralnej infrastruktury generującej, dystrybuującej i zarządzającej kluczami.

Model PKI, oparty na standardzie X.509, wykorzystuje standardowe mechanizmy opisane w protokole infrastruktury klucza publicznego z uszczegółowieniem pewnych funkcjonalności, takich jak np. wykorzystanie przez urządzenia SCIP w procesie negocjacji i wymiany certyfikatów, podpisanego przez Urząd Certyfikacji (*Certification Authority* – CA), statusu OCSP swojego certyfikatu w celu weryfikacji jego ważności (zasada działania odpowiada funkcjonowaniu OCSP Stapling w protokole TLS). Funkcjonalność ta znacząco zmniejsza ruch sieciowy (radiowy) między terminalami a infrastrukturą PKI dzięki wysyłaniu zapytań i odpowiedzi w celu potwierdzenia ważności certyfikatów z zastosowaniem protokołu OCSP.

Wykorzystanie infrastruktury klucza publicznego przez urządzenia kryptograficzne z zaimplementowanym protokołem SCIP zapewnia wiele możliwości wynikających z zastosowania kryptografii asymetrycznej. Jedną z tych funkcji, między innymi, jest możliwość zarządzania użytkownikami danej domeny bezpieczeństwa dzięki odłączaniu urządzenia czy też grupy urządzeń (użytkowników) od systemu wymiany informacji niejawnych przez anulowanie certyfikatu i podanie tego do wiadomości pozostałym użytkownikom systemu w wyniku aktualizacji listy anulowanych certyfikatów (*Certificate Revocation List* – CRL) lub też przez niewydanie potwierdzenia ważności certyfikatu zgodnie z protokołem OCSP.

W wypadku komunikacji punkt–wielopunkt protokół kryptograficzny SCIP nie przewiduje możliwości wykorzystania kryptografii asymetrycznej. Sposób weryfikacji użytkowników oraz negocjacji klucza sesji między wieloma uczestnikami korespondencji nie został opracowany. Ponadto wykorzystanie kryptografii asymetrycznej w tym trybie pracy wiązałoby się z koniecznością zapewnienia odpowiedniej przepustowości łącza danych, zwłaszcza w celu wymiany certyfikatów wszystkich korespondentów, potwierdzenia ich aktualności oraz negocjacji klucza szyfrowania transmisji danych.

Wymiana danych w trybie punkt–wielopunkt jest możliwa jedynie z wykorzystaniem uprzednio zaimplementowanych kluczy symetrycznych (*Pre Placed Keys* – PPK) z użyciem infrastruktury zarządzania kluczami do dystrybucji dokumentów kryptograficznych. Dystrybuowanie kluczy symetrycznych PPK do terminali z zastosowaniem sieci teleinformatycznych (radiowych) w protokole SCIP jest w trakcie opracowywania[7].

Protokół SCIP pozwala na poufną wymianę informacji między różnymi grupami użytkowników oraz w różnych domenach bezpieczeństwa, wykorzystując

5 *SCIP 221 Minimum Implementation Profile (MIP).*

6 *Open Framework for The NATO Secure Voice Strategy...,* op.cit.

7 *SCIP – 120 Rev 1.0 March 2010, s. 3–7.*

przeznaczone do tego klucze symetryczne PPK i standaryzowane mechanizmy kryptograficzne. W związku z tym możliwe jest prowadzenie niejawnej korespondencji fonicznej przeznaczonej dla grupy użytkowników, która składa się z przedstawicieli danej nacji, lub też korespondencji z użytkownikami krajów członkowskich NATO czy też państw sojuszniczych współdziałających w ramach prowadzonej operacji. Możliwość zastosowania różnych zaimplementowanych mechanizmów kryptograficznych pozwala na zachowanie poufności korespondencji każdej z grup z osobna przy wykorzystaniu tego samego urządzenia kryptograficznego[8]. Mechanizm wybiera się w ramach procedury zestawienia połączenia zgodnego z protokołem SCIP.

Protokół ten, po wymianie komunikatów sygnalizacyjnych, inicjujących wymianę informacji między dwoma terminalami, wymienia ze sobą dane dotyczące zdolności do nawiązania komunikacji (*Capabilities Message*), pracy terminali w określonych trybach oraz zdolności kryptograficznych do zapewnienia bezpiecznej korespondencji. Jeśli terminal ma poszerzone zdolności kryptograficzne (dodatkowe mechanizmy kryptograficzne), wysyłana jest również wiadomość zawierająca te informacje. Jeśli terminale będą w stanie uzgodnić posiadane obustronnie zdolności kryptograficzne, które będą mogły być wykorzystane, wówczas jest nawiązywane bezpieczne połączenie. W przeciwnym razie urządzenie sygnalizuje możliwość prowadzenia wymiany informacji jedynie w trybie jawnym, które nie jest zabezpieczone kryptograficznie.

Terminale, negocjując warunki połączenia, wybierają obopólnie dostępne mechanizmy kryptograficzne, które pozwalają na wymianę informacji o możliwe najwyższej klauzuli. Protokół SCIP opcjonalnie zapewnia poufność negocjowanych warunków połączenia, szyfrując dane procesu zestawiania połączenia kryptograficznego (*Call Setup Encryption* – CSE) i wykorzystując wcześniej wprowadzone do urządzenia SCIP klucze symetryczne przez lokalne struktury zarządzania infrastrukturą kluczy. Klucze te są takie same dla danej grupy użytkowników, co umożliwia nawiązanie bezpiecznego połączenia jedynie członkom tej grupy.

W ramach wiadomości dotyczących zdolności terminali do realizacji połączenia przesyłane są również informacje odnoszące się do grupy użytkowników biorących udział w wymianie informacji, dla których przypisane są z góry założone zdolności kryptograficzne, wykorzystywane w celu zapewnienia poufności, integralności i uwierzytelnienia korespondencji. Te zasady, przypisane do grup użytkowników, narzucają kolejność wyboru zdolności kryptograficznych. Istotną cechą jest to, że to grupy użytkowników określają sobie zasady doboru zdolności kryptograficznych.

Protokół SCIP posiada system kontroli dostępu (*Secure Access Control System* – SACS), który umożliwia lokalnemu terminalowi weryfikowanie innych terminali i komunikowanie się z nimi. Aktualność systemu kontroli dostępu utrzymują terminale, a polega to na weryfikowaniu certyfikatów, przeprowadzaniu protokołu weryfikowania statusu certyfikatów (OCSP) lub też listy odwołanych certyfikatów (CRL).

W przypadku pracy z wykorzystaniem kluczy symetrycznych terminale dążą do posiadania aktualnych list skompromitowanych kluczy (*Compromised Keys List*) przez wymianę tych wiadomości ze stacjami zarządzającymi.

Protokół SCIP ma opisane w dokumentach standaryzacyjnych możliwości użycia różnych algorytmów kryptograficznych, które pozwalają na szyfrowanie kluczami symetrycznymi w celu zapewnienia poufności transmisji danych. Dokumentacja opisująca protokół SCIP wymienia między innymi takie algorytmy, jak: AES czy Medley. Aby zapewnić uwierzytelnienie i integralność danych w protokole SCIP, wykorzystuje się techniki CBC MAC i HMAC (fot. 2).

ALGORYTMY KRYPTOGRAFICZNE

Kryptolodzy belgijscy, Joan Daemen i Vincent Rijmen, opracowali symetryczny szyfr blokowy (*Advanced Encrytpion Standard* – AES), nazwany od ich nazwisk Rijndael. Został on wybrany w ramach ogłoszonego konkursu, którego celem było wskazanie nowego algorytmu szyfru symetrycznego, będącego następcą algorytmu *Data Encrypthion Standard* (DES).

Prace nad utworzeniem nowego standardu zostały zapoczątkowane w 1997 roku przez National Institute of Standards and Technology (NIST). W ramach projektu DESCHALL, przeprowadzonego przez amerykańską organizację non profit Electronic Fronier Foundation, odszyfrowano w ciągu trzech dni z użyciem dostępnego sprzętu komputerowego wiadomość zaszyfrowaną algorytmem DES.

Pierwsza próba kryptoanalizy liniowej miała miejsce w 1994 roku, a pierwszy opisany teoretyczny atak na system DES z zastosowaniem kryptoanalizy różnicowej został opublikowany już w 1992 roku. Algorytm szyfrowania symetrycznego Rijndael został wyłoniony z wyselekcjonowanych 15 kandydatów spełniających narzucone przez NIST wymagania dotyczące konieczności szyfrowania bloków 128-bitowych z wykorzystaniem kluczy o długości 128, 192 i 256 bitów. Wybierając zwycięzcę, analizowano proponowane szyfry pod kątem kryptoanalizy, analizy różnicowej oraz jednoznaczności praw autorskich do szyfrów.

Po przestudiowaniu wszystkich dostępnych materiałów NIST ogłosił symetryczny algorytm kryptograficzny Rijndael zwycięzcą konkursu, a 26 listopada 2001 roku opublikowano dokumentację standaryzacyjną FIPS 197 dla Advanced Encryption Standard (AES), opartego na symetrycznym szyfrze blokowym Rijndael. Zwycięstwo to osiągnięto dzięki bardzo dobrym wynikom wydajności szyfru, które opierały się na szybkim działaniu i relatywnie małym zużyciu pamięci jednostek obliczeniowych. Jego niewielkie wymagania po-

8 *Reference Module 350 – Interoperable Priority (TP) Community of Interest (COI) Specification Revision 1.2.*

zwalają użytkować go w środowiskach ograniczonych, takich jak ośmiobitowe karty procesorowe.

Algorytm kryptograficzny MEDLEY należy do algorytmów klasy A, wykorzystywanych przez NSA w celu ochrony szczególnie wrażliwych informacji narodowych USA. Został on opisany w dokumentach standaryzacyjnych w 2001 roku i jest szeroko stosowany – głównie do szyfrowania transmisji informacji fonicznych.

Protokół SCIP wykorzystuje algorytmy szyfrowania asymetrycznego, oparte na krzywych eliptycznych z zastosowaniem dwóch protokołów negocjacji klucza sesji Diffie-Hellman (DH) oraz jego uwierzytelnianej wersji Menezes-Qu-Vanstone (MQV). Protokół MQV jest protokołem zawartym w dokumentach standaryzacyjnych i został ogłoszony przez NSA kluczowym mechanizmem wymiany kluczy w celu ochrony informacji niejawnych organizacji rządowych USA[9].

Radiostacje rodziny COMP@N mają zaimplementowany protokół SCIP zgodny ze STANAG-iem 5068.

W dobie intensywnego rozwoju komputerów kwantowych wykorzystywane przez protokół SCIP algorytmy szyfrowania, oparte na krzywych eliptycznych, nie są zalecane przez amerykańską agencję standaryzacyjną National Institute of Standard and Technology (NIST) jako docelowe i perspektywiczne algorytmy szyfrowania asymetrycznego. Agencja zaleca wstrzymanie się z implementowaniem tych algorytmów do czasu opublikowania standardu algorytmu niesymetrycznego, odpornego na kryptoanalizę kwantową. NIST zapoczątkował w 2017 roku proces poszukiwania algorytmu szyfrowania, odpornego na dedykowane algorytmy wykorzystujące komputery kwantowe, który ma być zakończony w 2022 roku z opracowanym standardem opisującym ten algorytm[10].

DOMENY BEZPIECZEŃSTWA

Zgodnie z ustawą o ochronie informacji niejawnych z 2010 roku w naszym kraju obowiązują cztery klauzule niejawności informacji: *zastrzeżone*, *poufne*, *tajne* i *ściśle tajne*[11]. Nie wszystkie one będą wykorzystywane na wszystkich poziomach dowodzenia, będą też stosowane z różną intensywnością. Dlatego istnieje potrzeba przypisania klauzul niejawności przetwarzanych informacji do konkretnego poziomu w hierarchii dowodzenia i współdziałania. Przypisanie klauzul umożliwiłoby opracowanie systemu wymiany informacji, będącego kompromisem między potrzebami informacyjnymi, efektywnością systemu zabezpieczenia kryptograficznego a zdolnościami systemów teleinformatycznych z podsystemami ochrony kryptograficznej zabezpieczającymi te potrzeby.

Henryk Dóżdż i Edward Sędek[12] proponują rozdzielenie i ograniczenie liczby domen bezpieczeństwa w systemach teleinformatycznych wykorzystujących protokół SCIP do dwóch poziomów niejawności przetwarzanych informacji, czyli *zastrzeżone* i *tajne*. Rozwiązanie to umożliwiłoby wykorzystanie domeny bezpieczeństwa o klauzuli *zastrzeżone* głównie na najniższych szczeblach dowodzenia, będących najliczniejszymi pod względem liczby użytkowników. Poziom *tajny* domen bezpieczeństwa funkcjonowałby na wyższych poziomach i obejmował elementy dowodzenia od batalionu wzwyż do poziomu politycznego włącznie.

Ograniczenie liczby domen bezpieczeństwa, wykorzystywanych przez systemy teleinformatyczne pracujące w trybie bezpieczeństwa systemowego, umożliwi ograniczenie *air gaps* między systemami wiążących się z koniecznością fizycznego przenoszenia informacji między domenami lub też tworzenia skomplikowanych i kosztownych bram międzysystemowych. Problem ten rozwiąże się, gdy zostaną ukończone prace nad teleinformatycznym systemem wielopoziomowym i wszystkie dotychczasowe systemy będą mogły pracować w jednej domenie informacyjnej, określonej maksymalną klauzulą przetwarzanych informacji z mechanizmami kryptograficznymi udostępniającymi informacje o danej klauzuli użytkownikom – zgodnie z posiadanym przez nich poziomem poświadczeń bezpieczeństwa. Prace koncepcyjne nad takim systemem zostały już zapoczątkowane w NATO.

Bezpieczna, foniczna łączność radiowa, z wykorzystaniem kryptografii asymetrycznej, zwłaszcza na poziomie taktycznym, zakłada możliwość pracy urządzeń kryptograficznych opartych na protokole SCIP w trybie punkt–wielopunkt. W wypadku zastosowania

9 H. Krawczyk, *HMQV: A high – Performance Secure Diffie-Hellman Protocol*, 5.07.2005.

10 *NIST's Post-Quantum Cryptography Program Enters „Selection Round"* 22.07. 2020, www.nist.gov/news-event/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round/. 8.09.2020.

11 *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz.U. nr 182 poz. 1228.

12 H. Dóżdż, E. Sędek, *Prezentacja nowych technologii SICP – NINE oraz ich wykorzystania na potrzeby kierowania stacjami radiolokacyjnymi*, „Elektronika" 2017 nr 3.

do tego rodzaju komunikacji kluczy symetrycznych protokół SCIP powinien posiadać zdolności do ich wymiany prezentowane przez protokół *On The Air Rekeying* (OTAR). Realizacja tych założeń pozwoli na wykorzystanie wszystkich niezbędnych w dzisiejszych czasach funkcjonalności upraszczających dystrybucję kluczy kryptograficznych, umożliwiając współpracę różnych grup użytkowników.

Wykorzystanie funkcjonalności protokołu SCIP, polegającej na posiadaniu zaimplementowanych różnych wybieralnych procedur kryptograficznych do zapewnienia poufności, integralności i uwierzytelniania informacji dla różnych grup użytkowników w ramach pracy jednego urządzenia kryptograficznego, będzie wymagało zgody krajowej władzy akredytacyjnej na pracę konkretnego urządzenia w domenach bezpieczeństwa o różnym poziomie niejawności. W wypadku przetwarzania wyłącznie informacji fonicznych, bez możliwości ich zapisywania i dalszego przetwarzania, problem ten wydaje się być prosty do rozwiązania. Natomiast jeśli weźmiemy pod uwagę możliwość wykorzystania urządzeń opartych na protokole SCIP do przetwarzania danych w różnych domenach bezpieczeństwa, które następnie będą przetwarzane przez dołączone stacje robocze czy też sieci teleinformatyczne, jego rozwiązanie zaczyna się komplikować. W takim wypadku pomóc mogłaby nowa, dodatkowa funkcjonalność protokołu SCIP, która polegałaby na rozpoznawaniu urządzeń podłączonych do sieci po stronie Red, np. przez wykorzystanie certyfikatów klucza publicznego. Z ich pomocą urządzenie dysponujące zaimplementowanym protokołem SCIP pozwalałoby na wykorzystanie jedynie dozwolonych mechanizmów kryptograficznych w celu zestawienia bezpiecznego kanału wymiany danych na poziomie aplikacji z urządzeniami/sieciami teleinformatycznymi dopuszczonymi do pracy w danej domenie informacyjnej.

Innym sposobem rozwiązania problemów na poziomach klauzul domen bezpieczeństwa jest przyjęcie, że wszyscy użytkownicy wykorzystują urządzenia z zaimplementowanym protokołem SCIP, umożliwiające pracę w domenie bezpieczeństwa do klauzuli *tajne*. Z kolei posiadane klucze wprowadzone do urządzenia kryptograficznego oraz wybrane mechanizmy definiują grupę użytkowników i poziom przetwarzanych informacji. Użytkownik lub też urządzenie, uwierzytelniając się dla urządzenia kryptograficznego, uzyskuje dostęp do określonych procedur kryptograficznych wraz z zaimplementowanymi kluczami, umożliwiającymi pracę w domenie bezpieczeństwa zgodnej z klauzulą poświadczenia bezpieczeństwa użytkowników uczestniczących w wymianie informacji. Urządzenie kryptograficzne po wylogowaniu się użytkownika lub też po zakończeniu pracy z urządzeniem systemu teleinformatycznego przechowuje wszystkie dane w formie zaszyfrowanej, stając się urządzeniem jawnym, które podlega zaewidencjonowaniu jako materiał kryptograficzny i jest przechowywane zgodnie z procedurami kryptograficznymi określonymi w stosownych dokumentach.

WIELE DO ZROBIENIA

Rozważając skalowalność systemów teleinformatycznych, budowanych zgodnie z protokołem SCIP, oraz możliwość tworzenia nowych domen informacyjnych, a także dołączania (odłączania) z wykorzystaniem modelu klucza publicznego grup użytkowników, idea protokołu SCIP wydaje się być bardzo obiecująca. Łączenie domen informacyjnych, dzięki wykorzystaniu certyfikatów krzyżowych, stwarza duże możliwości współpracy między jednostkami, siłami koalicyjnymi czy też sojuszniczymi na poziomie taktycznym wprowadzanymi do działań *ad hoc*.

Niestety, główny problem protokołu SCIP to brak możliwości realizacji połączeń punkt–wielopunkt w architekturze infrastruktury klucza publicznego. Stanowi to istotną niedogodność, zwłaszcza w fonicznej komunikacji radiowej, dla której ten protokół wydaje się nie być przeznaczony.

W dobie upowszechniania się protokołu IP w każdej domenie telekomunikacyjnej zanikające sieci PSTN czy ISDN powodują utratę znaczenia protokołu kryptograficznego SCIP na rzecz protokołów kryptograficznych dedykowanych sieciom IP, takim jak protokół kryptograficzny NINE. Pewną niszą, która wciąż wymaga kryptograficznego wypełnienia, jest wąskopasmowa łączność radiowa. By to uczynić, protokół SCIP powinien posiadać funkcjonalność pracy punkt–wielopunkt, zapewniającą odpowiednią skalowalność, efektywność i elastyczność systemu, na przykład dzięki wykorzystaniu zaktualizowanego i dostosowanego modelu klucza publicznego czy też wykorzystaniu kryptografii symetrycznej wzorowanej na modelu zdalnej wymiany kluczy kryptograficznych OTAR (mając na uwadze jego wszystkie ułomności[13]).

Koncepcja jednostopniowego poziomu niejawności informacji niejawnych, opierająca się na symetrycznych kluczach PPK w celu zapewnienia poprawnej skalowalności systemu, wymagałaby wdrożenia w protokole SCIP zdolności proponowanych przez OTAR. Bez adaptacji tego rodzaju rozwiązania infrastruktura zarządzania kluczami może być zupełnie niewydolna, zwłaszcza przy organizowaniu *ad hoc* wymiany informacji niejawnych między grupami użytkowników.

Posiadanie w dokumentacji standaryzacyjnej protokołu kryptograficznego SCIP nieperspektywicznych już algorytmów szyfrowania asymetrycznego, opartych na krzywych eliptycznych, wymusza konieczność ich zaktualizowania. Aktualizacja ta będzie już najprawdopodobniej możliwa, kiedy zostanie ostatecznie rozstrzygnięty konkurs, a zwycięskie algorytmy asymetryczne przedstawione w oficjalnych dokumentach standaryzacyjnych. ■

13 *Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System,* S. Clark, T. Goodspeed, P. Metzager, Z. Wasserman, K. Xu, M. Blaze, University of Pennsylvania.

Celownik holograficzny
HWS 552.A65

PRAKTYCZNE SPRAWDZENIE TEORETYCZNYCH OBLICZEŃ POWINNO WYPOSAŻYĆ SZKOLONYCH ŻOŁNIERZY W NIEZBĘDNĄ WIEDZĘ Z ZAKRESU ZASAD STRZELANIA Z BRONI Z NOWYM OSPRZĘTEM.

Autor jest dowódcą 141 Batalionu Lekkiej Piechoty w 14 Brygadzie Obrony Terytorialnej.

ppłk mgr inż. Maciej Paul

Dynamiczny proces doposażania pododdziałów zmechanizowanych i zmotoryzowanych w nowoczesny sprzęt i oprzyrządowanie do broni strzeleckiej spowodował konieczność opanowania przez żołnierzy umiejętności ich wykorzystania zarówno podczas szkolenia, jak i na polu walki. Wraz z nowymi egzemplarzami broni do pododdziałów trafiły między innymi celowniki holograficzne HWS model 552 EOTech. W związku z tym dowódcy pododdziałów, organizując zajęcia ze szkolenia strzeleckiego (ogniowego), muszą uwzględnić punkt nauczania właściwego przygotowania broni i celownika do strzelania. Jest to zadanie mobilizujące do perfekcyjnego opanowania zasad posługiwania się tym celownikiem nie tylko przez strzelca, lecz także przez cały pododdział.

Wraz z wprowadzeniem nowego elementu do systemu uzbrojenia nie wdrożono, niestety, właściwych instrukcji i poradników, które zawierałyby wytyczne dotyczące szkolenia z jego eksploatacji. Często dochodziło do niewykonania strzelań lub uzyskiwania słabych wyników, mimo że pododdział był wyposażony w celowniki HWS. Powód jest prosty: żołnierze w większości nie znają zasad strzelania z broni z tym celownikiem, nie potrafią jej skonfigurować oraz dobrać właściwego punktu celowania. Dlaczego tak się dzieje? Odpowiedź na to pytanie jest bardziej złożona, niż mogłoby się wydawać. Jednocześnie trudno wymagać od szkolonego przez nas żołnierza właściwych umiejętności, gdy sami nie znamy balistyki broni z nowymi przyrządami optycznymi.

Ogólnie rzec biorąc, każdy fabrycznie nowy celownik holograficzny założony na szynie montażowej Picantinny jest zwizowany (ustawiony). Problem polega jedynie na tym, że strzelec musi znać odległość, na jaką jest on ustawiony (rys. 1). Jeżeli do tego będzie znał zasady strzelania i poprawnie wypracuje dane, to trafi precyzyjnie w cel. Świadczyć to będzie o dobrym jego wyszkoleniu, niestety źle zaś o przygotowaniu merytorycznym.

WIZOWANIE I PRZYSTRZELIWANIE

W instrukcji dotyczącej celownika holograficznego HWS pojawiła się tarcza do zwizowania broni na dystansie 10 m, tzw. tarcza „4,3". Znając właściwości ustawienia broni, jesteśmy w stanie dość szybko poprawnie wykonać tę czynność. Problem polega na wprowadzonym tu błędzie pomiarowym, a w zasadzie błędzie merytorycznym. Docelowo tarcza ta była przeznaczona dla rodziny broni M-16 i pochodnych, nie zaś dla kbs Beryl (rys. 2). Zwizowanie według niej (czyli ustawień producenta) danego typu broni (M16A4 lub M4MWS) odpowiada dystansowi 300 m. Po weryfikacji naszych potrzeb i sprawdzeniu zarówno obliczeniowym, jak i ogniowym okazuje się, że po zamontowaniu celownika HWS na szynie montażowej Picatinny możliwe jest zwizowanie kbs Beryl na odległość 150 m. Różnica ta (mimo tego samego kalibru broni) wynika ze specyficznego sposobu mocowania celownika na tym karabinku, który nie jest typową bronią użytkowaną w armiach państw NATO. Przyrządy mechaniczne bowiem nie znajdują się

KRZYSZTOF PLAŻUK

UMIEJĘTNOŚĆ POSŁUGIWANIA SIĘ NOWYMI RODZAJAMI WYPOSAŻENIA JEST KONIECZNOŚCIĄ, Z JAKĄ MUSI ZMIERZYĆ SIĘ KAŻDY ŻOŁNIERZ.

w jednej osi z przyrządami optycznymi. Różnica wynosi aż 4,8 cm. Dla żołnierza, którego przeżycie na polu walki zależy od umiejętności oraz przygotowania uzbrojenia, jest ona znacząca. Dlatego też, by móc wykorzystać tarczę do zwizowania karabinka Beryl, należy ją zmodyfikować. Punkt wizowania względem osi lufy (jej rzutu) powinien zostać podniesiony do 7,2 cm. Wówczas uzyskamy wynik wizowania właściwy dla dystansu 300 m.

WIZOWANIE SZYBKIE

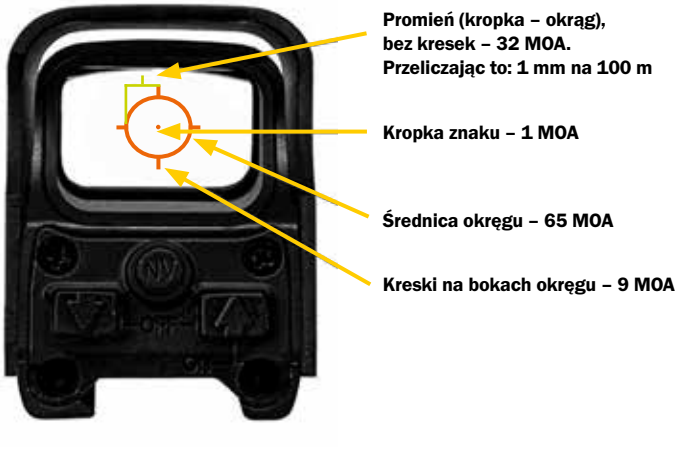
Możliwe jest sprawdzenie aktualnie ustawionej wartości wprowadzonej poprawki lub zwizowanie od nowa celownika HWS na żądaną odległość przez porównanie ustawień przyrządów mechanicznych z pozycją na tarczy ustawionej w odległości równej regulowanej nastawie (z charakterystycznym, oddalonym punktem) a znakiem celownika holograficznego (rys. 3).

Na podstawie przeprowadzonych badań przyjąłem, że dla przystrzelenia tak ustawionej broni (kbs Beryl z celownikiem HWS) najlepiej przyjąć punkt kontrolny (PK) jako koło o średnicy 5 cm na dystansie 100 m oraz koło o średnicy 1,25 cm na dystansie 25 m.

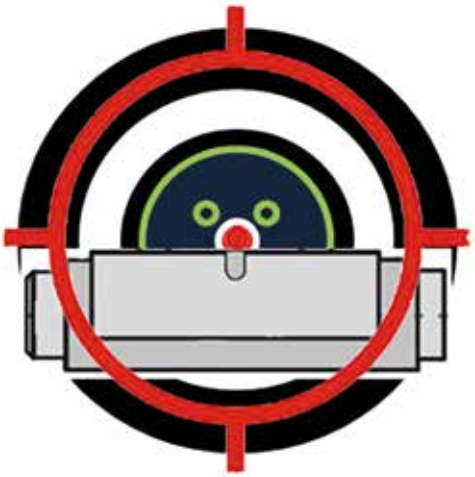
OGNIOWE PRZYSTRZELENIE SZYBKIEGO WIZOWANIA

Sposób ustawienia i przystrzelenia polega na umieszczeniu broni najlepiej na stojaku. Na cel lub charakterystyczny punkt znajdujący się w odległości 100 m ustawiamy przyrządy celownicze z nastawą „1". Dla tak ustawionej broni regulujemy znak celowniczy celownika HWS do momentu, aż pokryje się z punktem celowania przyrządów mechanicznych. Tak przygotowana broń jest wstępnie zwizowana do strzelania na dystansie zasięgu skutecznego. Dla odległości 100 m będzie to środek celu. Znając zasady strzelania, możemy przez odpowiednie podniesienie znaku celowania razić cele w zasięgu ognia skutecznego. Dopiero strzelenie da nam miarodajny wynik w postaci przestrzeliny w tarczy, najlepiej w punkcie kontrolnym odpowiadającym danej nastawie.

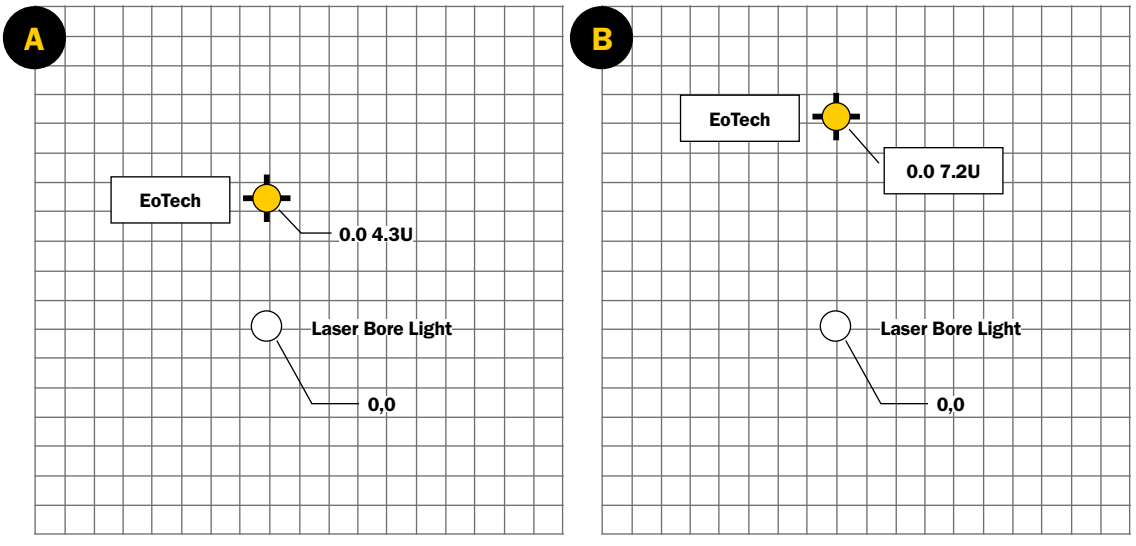
RYS. 1. WARTOŚĆ WIELKOŚCI ZNAKU CELOWNICZEGO NA WYŚWIETLACZU CELOWNIKA HOLOGRAFICZNEGO HWS DLA ODLEGŁOŚCI 100 M



RYS. 3. SPOSÓB ZGRANIA PRZYRZĄDÓW MECHANICZNYCH ZE ZNAKIEM CELOWNIKA HWS NA CELU



RYS. 2. UNIWERSALNA TARCZA DO WIZOWANIA HWS 552



A: Tarcza do wizowania kbs BERYL z HWS na 150 m

B: Tarcza do wizowania kbs BERYL z HWS na 300 m

Opracowanie własne (3).

Zasięg ognia skutecznego do celu wynosi 300 m przy punkcie celowania w środek tarczy (niezmiennie). Wysokość tarczy wynosi 75 cm, szerokość – 45 cm. Punkt celowania pokrywa się ze środkiem wysokości tarczy, czyli znajduje się na wysokości 37 cm.

PRZYSTRZELANIE METODĄ KLASYCZNĄ

Metoda ta została już opisana, chociażby w artykule kpt. Zbigniewa Szymocha opublikowanym w PSZ nr 4 z 2017 roku, jednakże nie uwzględniono w niej „korekty pionowej" wynikającej z różnicy wysokości linii celowniczej przyrządów mechanicznych i optyki. Takie ustawienie celownika dodatkowego powinno zostać sprawdzone ogniowo. Postępujemy wówczas podobnie jak w przypadku celownika noktowizyjnego PCS-5. Strzelamy do tarczy nr 1 umieszczonej w odległości 100 m. Przed strzelaniem powinniśmy nakleić 4-centymetrowy pasek papieru u podstawy tarczy (różnica linii celowniczych optyki i mechaniki, tzw. korekta pionowa). Korekta pionowa wynosi 2,1 MOA (minuta kątowa) na 100 m, odpowiada więc wielkości naklejonego paska.

Celownik zwizowany jest na odległość 100 m do tarczy bojowej, którą jest figura bojowa nr 40 (biegnący). Punkt celowania to środek tarczy – stała niezmienna. Poszczególne kolory odpowiadają dystansowi „oddalenia" tarczy od strzelca.

Przed strzelaniem można również sprawdzić na strzelnicy poprawność ustawienia przyrządów celowniczych. W stronę tarczy znajdującej się w odległości 100 m kierujemy broń w podstawę celu z nastawą przyrządów celowniczych na wartość „4" (rys. 4, po lewej).

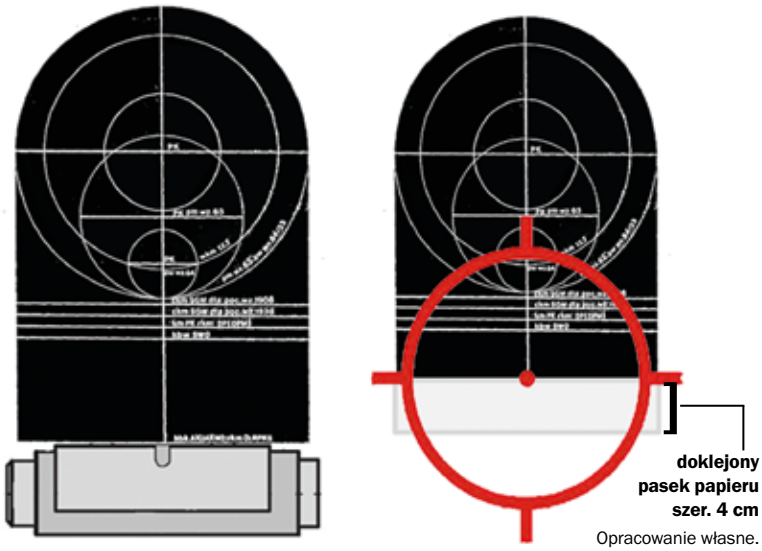
Broń najlepiej umieścić w stojaku uniwersalnym, by ją usztywnić. Następnie naklejamy pasek białego papieru o szerokości 4 cm (patrz rys. 4) i ustawiamy celownik HWS na podstawę celu (rys. 4, po prawej). Wykonanie tych czynności da nam pewność, że celownik jest ustawiony na odległość strzału bezwzględnego do celu o wysokości 50 cm, czyli popiersia. By właściwie ustawić celownik, powinniśmy znać dane balistyczne zawarte w tabeli 1.

Do regulacji celownika HWS służą dwie śruby regulacyjne, których skok (klik) na dystansie 100 m odpowiada wartości 1,4 cm na tarczy. Wynik jest zadowalający, jeżeli średni punkt trafienia (ŚPT) mieści się w polu kontrolnym tarczy. Pełne przekręcenie śruby pozwoli na zmianę punktu celowania o 28 cm (około 10 MOA). Jest to metoda najdokładniejsza, ponieważ uwzględnia na etapie zgrywania korektę pionową, wynoszącą w tym przypadku 4 cm (szerokość naklejonego paska).

PRZYSTRZELANIE DO TARCZY KONTROLNEJ

Drugą metodą zwizowania celownika HWS zamontowanego na broni jest ustawienie i przystrzelanie jej z użyciem specjalnie przygotowanej tarczy (nakładka foliowa). Znając właściwości balistyczne oraz

RYS. 4. SPOSÓB ZGRANIA PRZYRZĄDÓW MECHANICZNYCH ZE ZNAKIEM CELOWNIKA HWS NA CELU



Opracowanie własne.

TAB. 1. DANE BALISTYCZNE DLA KBS BERYL KALIBRU 5,56 MM ORAZ POCISKU RS Z ZAMONTOWANYM CELOWNIKIEM HWS I BEZ NIEGO

Celownik /zero	Odległość [m]								
	25	50	75	100	200	300	400	500	600
	przewyższenie [cm]								
100*	-5,5	-2,8	-1,3	0	2,8	10,1	20,1	32,9	49,2
100	-2,7	-0,9	-0,3	0	4,7	12,7	23,1	36,3	55,5

* Górny wiersz – dane dla celownika HWS; dolny wiersz – dane dla przyrządów mechanicznych. Porównanie przewyższenia toru lotu pocisku z uwzględnieniem korekty pionowej.

TAB. 2. WARTOŚCI PRZESUNIĘĆ ŚRUB REGULACYJNYCH NA DYSTANSIE 100 M

Liczba klików	Przesunięcie w cm na 100 m	Ustawienie w odległości
-4 (w lewo)	-5,6	25 m
-3 (w lewo)	-4,2	–
-2 (w lewo)	-2,8	50 m
-1 (w lewo)	-1,4	–
0	0	100 m
1 (w prawo)	1,4	–
2 (w prawo)	2,8	200 m
3 (w prawo)	4,2	–
4 (w prawo)	5,6	–
5 (w prawo)	6,9	–
6 (w prawo)	8,3	–
7 (w prawo)	9,7	300 m
8 (w prawo)	11,1	–
9 (w prawo)	12,5	–
10 (w prawo)	13,9	–
11 (w prawo)	15,3	–
12 (w prawo)	16,7	–
13 (w prawo)	18,1	–
14 (w prawo)	19,5	400 m
15 (w prawo)	20,9	–
...	.....	.....
23 (w prawo)	32.2	500 m
...	.....	.....
35 (w prawo)	49	600 m

Opracowanie własne.

wartości przewyższenia toru lotu pocisku dla różnych odległości strzelania, wykonujemy tarczę kontrolną. Jest to czarny okrąg o średnicy 5 cm naklejony na biały ekran do przystrzeliwania. Główną rolę będzie odgrywać specjalnie przygotowana folia, na którą jest naniesiona siatka regulacyjna o średnicy 1,4 cm (odpowiadającej 0,5 MOA na dystansie 100 m dla celownika HWS), oraz okręgi kontrolne odpowiadające punktom nastaw celowniczych na dystansie od 25 do 600 m. Jest to dość proste rozwiązanie, niewymagające specjalnego przygotowania tarcz. Jedna folia z naniesionymi danymi może być używana wielokrotnie. Tarczę umieszcza się na dystansie 100 m. Uwzględniono na niej obliczenia wykonane w ramach korekty pionowej. Tak przygotowana tarcza pozwala na dokonanie sprawdzenia:

– uprzednio przystrzelonego celownika na różnych dystansach, a zatem określenie dokładności skoku regulacyjnego. Okazać się może bowiem, że na przykład między nastawą na 200 i 300 m występuje znaczny błąd i celownik trzeba będzie skierować do naprawy;

– w sposób ogniowy (bez wstępnego ustawienia), na jaki dystans jest ustawiony nasz celownik. Strzelamy do tarczy i z przestrzelin odczytujemy zakres ustawienia celownika. Możemy również go wyregulować, ponieważ jedna kratka równa jest jednemu klikowi. Pozwala to na przeprowadzenie regulacji na żądany przez nas dystans;

– w sposób ogniowy ustawień po wstępnym zwizowaniu celownika z bronią i wykonaniu regulacji.

Ponadto oszczędzamy czas i amunicję: mniej czasu i mniej wystrzelonej amunicji przy tym samym efekcie.

ARCH. AUTORA

Zestaw składający się z celownika holograficznego HWS oraz monokularu noktowizyjnego MU-3

Dodatkowo nie musimy zapotrzebowywać specjalnych tarcz. Wystarczy biały ekran i koło o średnicy 5 cm i oczywiście odpowiednio wcześniej wykonana nakładka foliowa.

Wizowanie na tak przygotowanej tarczy jest bardzo podobne do poprzedniego. Konieczne będzie usztywnienie broni w stojaku i w odległości 100 m zamocowanie tarczy. Nastawa przyrządów celowniczych broni na „1", punkt celowania – to środek celu. Dla tak ustawionej broni regulujemy celownik optyczny, również kierując go w środek celu. Po wykonaniu strzelania przestrzeliny powinny znaleźć się w punkcie kontrolnym, czyli w punkcie celowania (czarny okrąg). Po uzyskaniu zadowalających wyników z przystrzeliwania, znając wartości przesunięcia znaku celowniczego, możemy ustawić celownik holograficzny na dowolną odległość. Co to oznacza? Jeżeli mamy przystrzeloną broń na dystansie 100 m w punkt, a chcemy ustawić ją na odległość strzelania 200 m, musimy wyregulować przyrządy w elewacji o dwa kliki, czyli 2,8 cm. Zostanie wówczas podniesiony punkt celowania, co odpowiada trajektorii lotu pocisku wystrzelonego z nastawy „2" do tarczy znajdującej się w odległości 100 m.

Wartość ustawienia na 300 m da nam siedem kliknięć (przesunięcie o 10,1 cm w elewacji). Aby ustawić wartość strzału bezwzględnego, musimy wykonać 14 kliknięć. Podobnie z obniżeniem punktu celowania. I tak, by osiągnąć wartość ustawienia na dystansie 50 m, musimy wykonać regulację o dwa kliki, natomiast na dystansie 25 m – odpowiednio o cztery kliknięcia (tab. 2).

ZASADY STRZELANIA

Strzelanie z wykorzystaniem celownika HWS jest dość proste. Skraca w znacznym stopniu czas zgrania przyrządów celowniczych, pozwalając na szybsze otwarcie ognia. Wykorzystanie tego celownika z monokularem noktowizyjnym MU-3A (fot.) zamontowanym równolegle umożliwia skonfigurowanie celownika noktowizyjnego i równie skuteczne rażenie celów w warunkach ograniczonej widoczności bez konieczności wymiany celownika holograficznego HWS.

Najważniejsza zasada, jaką należy się kierować podczas strzelania z wykorzystaniem celownika holograficznego HWS, dotyczy doboru punktu celowania. Znając ustawienia celownika, jesteśmy w stanie razić cele w zasięgu skutecznym broni. Musimy tylko podnieść o określoną wartość punkt celowania. Znajomość odczytywania charakterystyk znaku celowniczego pomoże nie tylko w określeniu odległości do celu, lecz także w ustaleniu i zastosowaniu poprawek.

Aby właściwie wykorzystać celownik holograficzny 552 EOTech użytkowany przez pododdziały zmechanizowane i zmotoryzowane, należy zapoznać się z kilkoma jego właściwościami:

- środkowa kropka znaku celowniczego – to główny znak celowniczy wynoszący 2,8 cm na 100 m;
- pierścień koła znaku celowniczego wynosi 65 MOA – to wzrost przeciętnego mężczyzny widzianego z odległości 100 m (rys. 5);
- podczas strzelania na dystansie 25 m należy użyć dolnej części koła, gdzie znak krzyżyka przecina je jako punkt celowania, a nie kropki;
- strzelając na dystansie 50 m, trzeba użyć czerwonej kropki jako odniesienia do celu widzianego z około 50 do 200 m. Punkt celowania – to środek celu; punkt uderzenia powinien znajdować się w środku celu (przy założeniu zgrania broni na dystansie 200 m – rys. 6).

Znając zasady celowania z użyciem siatki celownika holograficznego, można również odczytać przybliżone odległości do celów (rys. 7). Dane te wpłyną na zwiększenie skuteczności ogniowej w trakcie pojedynków ogniowych na polu walki.

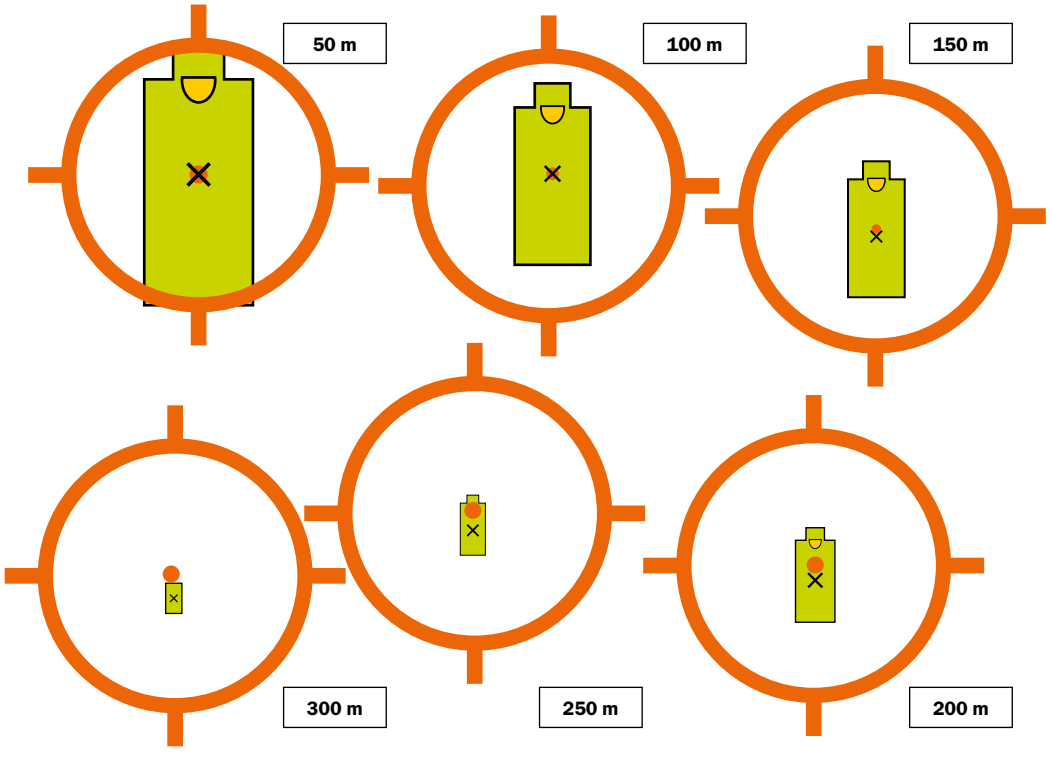
Osobną kwestią jest wykorzystanie omawianego celownika podczas walki w małej odległości. Szkolenie strzeleckie oraz strzelanie w małej odległości

RYS. 5. ŻOŁNIERZ WIDZIANY PRZEZ CELOWNIK HWS Z ODLEGŁOŚCI 100 M

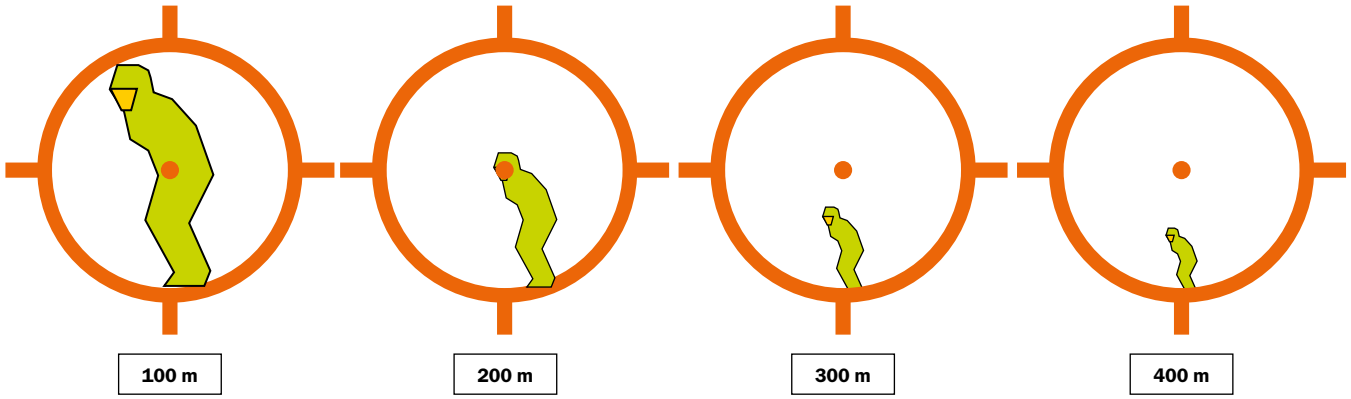
nie są domeną pododdziałów zmechanizowanych. Wiąże się to z możliwościami bazy szkoleniowej, warunkami użytkowania strzelnic garnizonowych oraz doświadczeniem instruktorów (dowódców). Ten stan rzeczy powoli zmienia się we właściwym kierunku. Wykorzystując doświadczenia z działań PKW oraz wzorując się na rozwiązaniach szkoleniowych wojsk specjalnych, możemy przyjąć następujący model szkolenia strzeleckiego przygotowującego do strzelania w małej odległości z użyciem celownika HWS (rys. 8).

Mając dane balistyczne, możemy pokusić się o przygotowanie tarczy wielosekcyjnej. Jest ona umieszczana w odległości 100 m. Ma jeden główny punkt celowniczy – to czarny okrąg o średnicy 15 cm. Ponadto nad i pod głównym znakiem są kręgi kontrolne odpowiadające poszczególnym odległościom. Służy ona do oceny sprawności celownika oraz do sprawdzenia ogniowej wartości jego przystrzelania. Można także sprawdzić, czy wartości klików zgadzają się z praktycznymi przestrzelinami. Celujemy w główny punkt celowania. Jeżeli przestrzeliny pokrywają się z odpowiednimi okręgami kontrolnymi, wówczas mamy pewność, że celownik jest sprawny.

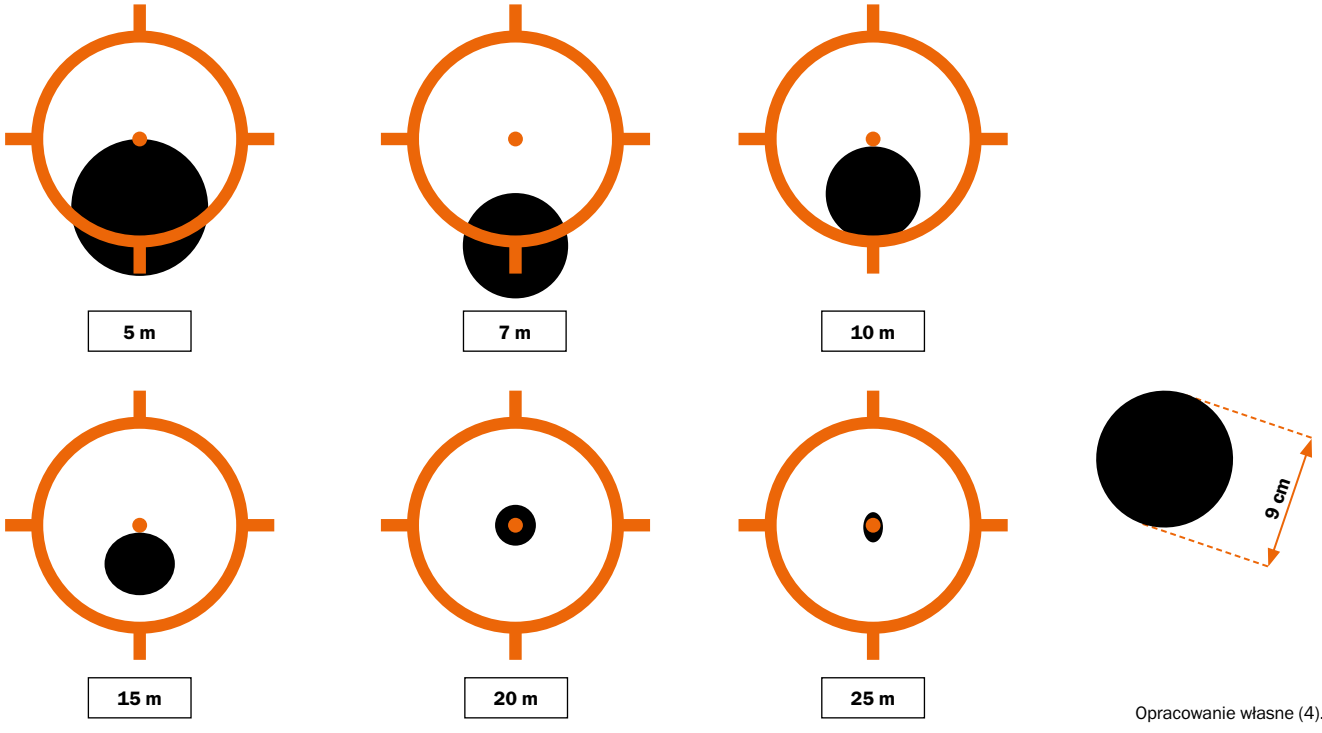
RYS. 6. ZASADY CELOWANIA Z CELOWNIKIEM HWS ZWIZOWANYM NA DYSTANSIE 200 M



RYS. 7. SPOSOBY ODCZYTYWANIA ODLEGŁOŚCI DO CELU Z WYKORZYSTANIEM CELOWNIKA HWS

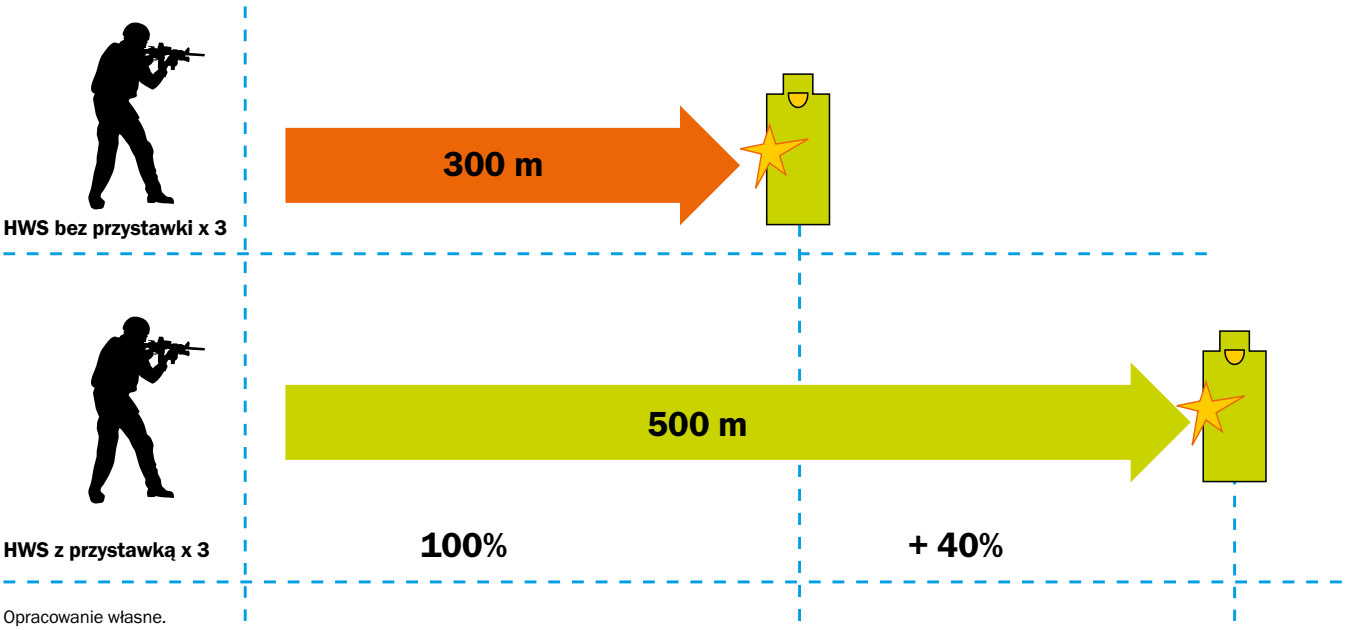


RYS. 8. ZASADY STRZELANIA DO KOŁA O ŚREDNICY 9 CM Z KBS BERYL Z CELOWNIKIEM HWS ZWIZOWANYM NA ODLEGŁOŚĆ 300 M



Opracowanie własne (4).

RYS. 9. WZROST SKUTECZNOŚCI ODDZIAŁYWANIA STRZELCA WYPOSAŻONEGO W KBS BERYL Z CELOWNIKIEM HWS ORAZ PRZYSTAWKĄ POWIĘKSZAJĄCĄ TRZYKROTNIE



Opracowanie własne.

Tarcza ma układ siatki wyskalowanej w kwadratach o boku 1,4 cm, czyli 0,5 MOA. Pozwoli to na właściwą regulację celownika podczas sprawdzania ogniowego.

UMIEĆ WYKORZYSTAĆ

Wprowadzenie holograficznego celownika HWS wywołało rewolucję w strzelaniu. Jednakże, by w pełni wykorzystać możliwości, jakie zapewnia ten przyrząd, właściwe byłoby wyposażenie żołnierzy w przystawki powiększające. Urządzenia te powiększające obraz trzykrotnie mogą być stosowane nie tylko podczas wykonywania zadań ogniowych, lecz są niezastąpione również w czasie obserwacji terenu. Strzelając z broni wyposażonej w taki zestaw, strzelec prowadzi ogień skuteczny na odległość 300 m tak, jakby strzelał z użyciem celownika HWS na odległość 100 m.

Mając do dyspozycji wspomnianą przystawkę, żołnierz jest w stanie zauważyć uchylenie pocisku, wprowadzić poprawki oraz razić skutecznie cele znajdujące się dotychczas poza jego zasięgiem. Strzelanie powyżej 300 m z kbs Beryl było do tej pory wyzwaniem. Po zastosowaniu opisanego rozwiązania jest realne. Nierzadko można niszczyć cel w odległości do 500 m (rys. 9).

Żołnierz wyposażony w takie narzędzie jest w stanie podczas szkolenia ogniowego czy kierowania ogniem wykonać zadanie mniejszą liczbą amunicji, ostrzeliwując i trafiając większość wykrytych celów. Z badań własnych przeprowadzonych w ciągu ostatnich siedmiu lat wynika, że skuteczność ognia wzrosła o 70% w dzień i 45% w nocy. Ponadto realnemu zwiększeniu uległ zasięg ognia skutecznego z 300 do 500 m. Zmieniony został także system prowadzenia ognia przez pododdział, gdyż realnie zwiększył się zasięg ognia najliczniej występującego środka ogniowego, czyli karabinka szturmowego kbs Beryl (rys. 9). Należy zatem pamiętać, że umiejętność posługiwania się nowymi rodzajami wyposażenia jest koniecznością, z jaką musi zmierzyć się każdy żołnierz. Mając odpowiednie oprzyrządowanie, wiedzę oraz wyszkolenie, jest on w stanie skuteczniej, szybciej i dokładniej wykonać każde zadanie ogniowe. ■

Kierunki rozwoju **zdolności obronnych**

(ARTYKUŁ DYSKUSYJNY)

POWINNIŚMY SIĘ ZASTANOWIĆ, JAK NALEŻY KSZTAŁTOWAĆ POTENCJAŁ OBRONNY NASZEGO KRAJU, MAJĄC NA UWADZE SKOMPLIKOWANĄ WSPÓŁCZESNĄ RZECZYWISTOŚĆ ORAZ WIELKĄ NIEWIADOMĄ DOTYCZĄCĄ POTENCJALNYCH ZAGROŻEŃ.

mjr dypl. SZRP Piotr Fanfara

Autor jest zastępcą dowódcy batalionu zmechanizowanego – szefem sztabu w 20 Brygadzie Zmechanizowanej.

Wynikają one z posiadanego potencjału, ten zaś jest rozumiany bardzo szeroko. Na jego wielkość wpływ ma wiele rozmaitych czynników – począwszy od stanu sił zbrojnych, przez możliwości gospodarcze, stan infrastruktury, potencjał ludzki, a na sojuszach z innymi państwami kończąc. Kształtowanie zdolności obronnych nie może być także oderwane od charakteru potencjalnych konfliktów zbrojnych, jakie mogą zagrażać nam w przyszłości. Od mądrości współczesnych teoretyków oraz praktyków zajmujących się tą właśnie dziedziną wiedzy zależy, w jakim kierunku należy owe zdolności rozwijać. Ma to niebagatelne znaczenie, zważywszy na obciążenia budżetowe oraz czasochłonność, jakie nierozerwalnie łączą się z ich budową.

Za Alvinem i Heidi Tofflerami, autorami książki zatytułowanej *Wojna i antywojna*, można stwierdzić, że w przyszłości wojny będą prowadzone inaczej niż dotychczas[1]. Zgodnie z ich rozważaniami, przedstawionymi w przywołanym opracowaniu, czekają nas konflikty tzw. trzeciej fali. Autorzy twierdzą, iż trzecia fala, związana z rozwojem cywilizacji, zmniejszaniem się znaczenia państw narodowych i zwiększaniem roli korporacji międzynarodowych oraz kapitału międzynarodowego, to tylko niektóre przejawy współczesnej skomplikowanej rzeczywistości.

ZAŁOŻENIA OGÓLNE

Analizując potencjalne zagrożenia, z których należałoby wysnuć ewentualne kierunki rozwoju zdolności obronnych, można posłużyć się książką Samuela P. Huntingtona *Zderzenie cywilizacji i nowy kształt ładu światowego*[2]. Autor zauważa, że po upadku bloku komunistycznego, kiedy niejako w jednym momencie dziejowym wydawało się, że nie będzie już w przyszłości poważnych zagrożeń wojennych, on dowodzi, iż może być zupełnie inaczej. Twierdzi, że podłoża przyszłych konfliktów zbrojnych swoje najpoważniejsze źródła będą miały w różnicach wynikających ze wzrostu znaczenia, a tym samym ścierania się poszczególnych światowych cywilizacji wynikających zasadniczo z różnic kulturowych oraz religijnych. Świat nie będzie już ani dwubiegunowy, ani jednobiegunowy jak do tej pory. Stanie się areną rywalizacji, zarówno w skali mikro oraz makro (niekoniecznie oczywiście w każdym wypadku militar-

1 A. Toffler, H. Toffler, *Wojna i antywojna*, Warszawa 1997, s. 93.

2 S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Poznań 2019.

nej) wielu dotychczas niejako uśpionych cywilizacji. Nasz kraj autor zaliczył do grupy państw tworzących cywilizację świata zachodniego.

Nie uciekniemy także od kolejnego problemu w naszych rozważaniach. Jeżeli zaczerpniemy z opracowania Tofflerów wizję przyszłych wojen, to jako kraj musimy uświadomić sobie nasze mocne i słabe strony. Do mocnych można zaliczyć brak w strukturze naszego społeczeństwa większych mniejszości narodowych. Z drugiej jednak strony jesteśmy wciąż państwem na tzw. dorobku, które nie dysponuje nadmiernym bogactwem. A wojny tzw. trzeciej fali często są konfliktami wysoko zaawansowanymi technologicznie, a to przecież kosztuje. Musimy zatem szukając rozwiązań w kwestii kształtowania zdolności obronnych znaleźć przysłowiowy złoty środek. W jego odnalezieniu będą nam pomocne konkretne przypadki kształtowania zdolności obronnych (potencjału obronnego) wybranych państw. Celem tego zabiegu jest zaprezentowanie takich rozwiązań, które mogłyby być przeniesione na nasz grunt.

JEDNYM Z ZASADNICZYCH ZAŁOŻEŃ KONCEPCJI JEST UZYSKANIE EFEKTÓW Z JEDNOCZESNĄ

JAK TO ROBIĄ INNI

Stany Zjednoczone Ameryki Północnej bez wątpienia są najpotężniejszym państwem na arenie międzynarodowej. Swoje zdolności obronne pozyskują z ogromnego potencjału, jakim dysponują. Bezpieczeństwo narodowe tego kraju jest rozumiane jako kompleksowa działalność w wielu dziedzinach funkcjonowania państwa. Do tych dziedzin należą: sprawy wojskowe (militarne), polityka zagraniczna oraz interesy kraju prowadzone na całym świecie, utrzymywanie właściwych relacji z sojusznikami, a także utrzymanie przewagi militarnej nad jakimkolwiek innym państwem czy też grupą państw. Ponadto do istotnych spraw z zakresu bezpieczeństwa narodowego zaliczana jest działalność polegająca na przeciwstawianiu się wszelkim siłom destrukcyjnym zarówno w kraju, jak i poza jego granicami.

W aspekcie posiadanych zdolności obronnych funkcjonują wzajemnie uzupełniające się dwa podsystemy. Tymi podsystemami są: obrona militarna, czyli siły zbrojne, oraz podsystem obrony cywilnej. Dlatego też uważa się, że siły zbrojne są gotowe do zapewniania przetrwania instytucji państwa, infrastruktury krytycznej, ochrony życia oraz majątku prywatnego, a także zachowania stylu i jakości życia obywateli kraju.

Niezwykle istotną rolę w kształtowaniu zdolności obronnych zapewnia Gwardia Narodowa. Wypełnia ona zadania zarówno federalne, jak i stanowe. Głównym zadaniem federalnym jest utrzymanie wyszkolonych i wyposażonych jednostek, które są gotowe do natychmiastowej mobilizacji oraz ich operacyjnego rozwinięcia na wypadek zagrożenia. Zadania na poziomie stanowym wiążą się z utrzymaniem sił na potrzeby wystąpienia sytuacji kryzysowych na obszarze stanu. Odnoszą się one do niesienia pomocy ofiarom klęsk żywiołowych, usuwania skutków awarii przemysłowych, kontrolowania i tłumienia zamieszek czy też ochrony imprez publicznych. Niezwykle istotne są także działania Gwardii Narodowej związane ze wspieraniem władzy publicznej, zarówno federalnej, jak i stanowej, w walce z handlem narkotykami, udzielaniem pomocy w zakresie usług transportowych, wspieraniem ośrodków penitencjarnych czy też świadczeniem pomocy medycznej. Przykład Gwardii Narodowej uzmysławia nam, jak istotną rolę w kształtowaniu zdolności obronnych państwa odgrywa świadome i zorganizowane społeczeństwo. Należałoby zatem się zastanowić, czy w warunkach polskich obecny stan odnoszący się do samoorganizacji społeczeństwa w dziedzinie bezpieczeństwa publicznego jest wystarczający.

Koncepcja obrony w *Szwecji* opiera się na tzw. obronie totalnej. Rozszerza ona pojęcie *bezpieczeństwa*, które oznacza bezpieczeństwo nie tylko w sferze militarnej, lecz także zagrożeń i wyzwań o charakterze niemilitarnym. Obejmuje działania, które mają na celu przygotowanie społeczeństwa do przeciwstawienia się zewnętrznym zagrożeniom oraz do zreorganizowania go do warunków czasu wojennego. Obrona totalna Szwecji składa się z nadrzędnego podsystemu kierowania, obrony militarnej oraz obrony cywilnej.

Siły zbrojne Szwecji są obciążone znaczną liczbą zadań obronnych. Wynika to przede wszystkim z tego, że kraj ten ma status państwa neutralnego. Kładzie się więc w nim duży nacisk na powszechność obowiązku obrony oraz rozwój sprawnego komponentu wojsk terytorialnych – Gwardii Narodowej. Ma ona do wykonania bardzo różnorodne zadania w zakresie obronności, tzn.: przeciwdziała sabotażom dzięki ochronie kluczowych węzłów infrastruktury krytycznej, elektrowni, rozgłośni radiowych, magazynów amunicji i zapasów mobilizacyjnych, prowadzi także działania rozpoznawcze w miejscu stacjonowania.

Specyficznym elementem obrony totalnej jest obrona ochotnicza. W jej skład wchodzi wiele organizacji, które mają określone zadania w zakresie

zarówno wsparcia sił zbrojnych, jak i obrony i ochrony ludności cywilnej. Podobnie jak w wypadku USA, można wyciągnąć wniosek, że świadome społeczeństwo ma niebagatelny wpływ na wzrost poziomu zdolności obronnych.

Wśród organizacji należących do obrony ochotniczej wyróżnia się struktury kontraktowe, które mają odpowiednie zadania z zakresu obrony cywilnej. Zawierają one porozumienia z zainteresowanymi obywatelami w sprawie pełnienia służby w okresie zwiększonego zagrożenia. Kolejną grupę stanowią organizacje ochotnicze, które zrzeszają ponad 600 tys. członków, z czego duża część to personel etatowy.

WZMACNIANIA ZDOLNOŚCI OBRONNYCH MINIMALIZACJĄ KOSZTÓW BUDŻETOWYCH

Szwecja, co istotne, w dalszym ciągu prowadzi szkolenia w zakresie powszechnej służby wojskowej.

Polityka obronna *Republiki Federalnej Niemiec* obejmuje szeroki zakres działań w dziedzinie bezpieczeństwa. *Obrona powszechna – ogólna*, bo takie pojęcie tam funkcjonuje, skupia wszystkie niezbędne polityczne, militarne i cywilne przedsięwzięcia państwa zarówno w wymiarze narodowym, jak i sojuszniczym. W Republice Federalnej Niemiec używane jest pojęcie *obrona powszechna*. W jej ramach wyróżniamy podsystemy: militarny, obrony cywilnej oraz podsystem kierowania, który nimi zarządza. Przed niemieckimi siłami zbrojnymi postawiono zadania zarówno militarne, jak i niemilitarne. Niemcy przywiązują istotną wagę do zobowiązań sojuszniczych, co sprawia, że użycie sił zbrojnych poza granicami państwa może się odbywać jedynie w ramach zawartych sojuszy (NATO).

Państwo niemieckie stworzyło komponent, jakim jest Wojskowa Organizacja Terytorialna. Główne jej zadania obejmują: obronę terytorium kraju, wsparcie obrony cywilnej, reprezentowanie interesów wojskowych, wspieranie sojuszników oraz reprezentowanie narodowych interesów wobec NATO. Niezwykle istotny jest sektor cywilny, który w ramach obrony cywilnej kraju wykonuje wiele zadań. Główne jego zadania są związane z utrzymaniem ciągłości funkcji państwowych i administracyjnych oraz ochroną ludności cywilnej. Istotną rolę odgrywa on także w zakresie dostarczania towarów i usług na rzecz sił zbrojnych. Wynika to zapewne z wysokiego poziomu rozwoju gospodarczego. Podsystem obrony cywilnej w RFN jest związany z podsystemem obrony militarnej.

Zdolności obronne tego kraju wynikają z wysokiego poziomu rozwoju gospodarki narodowej, a tylko w niewielkim stopniu z zaangażowania społeczeństwa w sprawy bezpieczeństwa. Gospodarka tego państwa w istotnym stopniu odgrywa rolę usługową dla sił zbrojnych, a znaczny asortyment środków walki jest dostępny na rodzimym rynku. Takie podejście sprawia, że duża część środków budżetowych wydatkowanych na bezpieczeństwo pozostaje w kraju.

Szwajcaria i jej zdolności obronne są definiowane przyjętą zasadą neutralności. Siły zbrojne tego kraju nie dysponują istotnym potencjałem odstraszania. Społeczeństwo szwajcarskie, państwo oraz jednostki samorządu terytorialnego są wkomponowane w proces budowy i umacniania bezpieczeństwa państwa. Już kilkadziesiąt lat temu szwajcarskie przepisy prawa budowlanego były tak konstruowane, by nowo budowane budynki spełniały jednocześnie funkcję schronów i ukryć. Zaowocowało to potencjalnie niskimi kosztami budowy schronów w skali całego kraju. Dlatego obecnie Szwajcaria dysponuje znaczną liczb schronów i ukryć dla ludności cywilnej.

Z siłami zbrojnymi współpracuje obrona cywilna. Obie organizacje mają wiele wspólnych obszarów działania i wspólnych celów. Przykładem jest chociażby to, że szpitale cywilne, służby ratownicze i cały system służby zdrowia wykonuje zadania na rzecz sił zbrojnych. Armia intensywnie uczestniczy w wielu programach realizowanych przez obronę cywilną, a społeczeństwo aktywnie bierze udział w procesie wzmacniania zdolności obronnych państwa. Zdolności te wynikają ze świadomości i sukcesywnego uczestnictwa w różnego typu szkoleniach z zakresu bezpieczeństwa. Na szczeblu władz państwowych i lokalnych organizowane są regularne szkolenia związane z posługiwaniem się bronią, co tworzy tym samym kulturę posługiwania się nią w społeczeństwie. Kultury tej brakuje w naszym społeczeństwie od zakończenia II wojny światowej. W znacznej części szwajcarskich domów znajduje się wyposażenie (pewna część wyekwipowania) potrzebne do natychmiastowej obrony lokalnej społeczności w sytuacji zagrożenia.

KONCEPCJE

Przejdźmy zatem do naszego kraju i zastanówmy się nad możliwościami, jakimi dysponuje on w zakresie kształtowania zdolności obronnych, które są wypadkową poziomu rozwoju społecznego, gospodarczego oraz zdefiniowanych zagrożeń. Zagrożenia dla funkcjonowania państwa i jego bezpieczeństwa mogą pochodzić zarówno ze źródeł zewnętrznych, jak i wewnętrznych.

Nasz kraj potrzebuje społeczeństwa w znacznie większym stopniu zaangażowanego w życie zbiorowe narodu. Potrafimy się organizować, co historia naszego kraju wielokrotnie udowodniła, ale pozostało jeszcze wiele do zrobienia w tej materii. Dobre przykłady samoorganizacji społeczeństwa przy współudziale państwa, tak jak jest to w Szwecji oraz Szwajcarii, moglibyśmy zaadaptować u nas.

Funkcjonujące jednostki obrony terytorialnej mają zadania związane ze wsparciem zgrupowań operacyjnych w działaniach bojowych, ale będą także w wypadku zagrożeń ochraniać społeczności lokalne. Koszty funkcjonowania obrony terytorialnej jako rodzaju sił zbrojnych są znaczne. Dobrym rozwiązaniem (niejako uzupełniającym obronę terytorialną) jest stworzenie możliwości samoorganizacji na zasadzie szwedzkiej obrony narodowej, która posiada status organizacji pożytku publicznego. Spełniałaby ona rolę uzupełniającą w zakresie działań ochronnych w razie zaistnienia zagrożeń bezpieczeństwa. Wydaje się, że obecnie brakuje u nas takich stowarzyszeń, których zadania byłyby związane z ochroną ludności cywilnej w wypadku zagrożeń zarówno kryzysowych, jak i typowo wojennych. A koszty ich funkcjonowania w stosunku do potencjalnych korzyści byłyby niewielkie. Jako organizacja pożytku publicznego mogłaby ona dodatkowo być wspierana finansowo przez społeczeństwo w formie odpisów podatkowych czy też darowizn. Takie instrumenty prawnofinansowe można z łatwością stworzyć.

Kolejnym rozwiązaniem, mającym na celu wspieranie rozwoju zdolności obronnych, byłoby wsparcie przez państwo czy samorząd cywilnych stowarzyszeń, które wpływałyby na rozwój szeroko pojętego bezpieczeństwa w kraju dzięki utworzeniu funduszu celowego. Obecnie wiele tego typu form organizacyjnych korzysta z uprawnień wynikających z nadania im statusu organizacji pożytku publicznego. Wspierane finansowo z funduszu celowego byłyby organizacje działające zarówno na rzecz obronności, jak też ochrony ludności, ratownictwa cywilnego oraz inne, ważne społecznie stowarzyszenia. Warunkiem koniecznym funkcjonowania tego typu funduszu byłby transparentny wykaz organizacji, stowarzyszeń czy też innych form organizacyjnych działających na rzecz bezpieczeństwa publicznego. Środki z funduszu byłyby przeznaczane chociażby na zakup: sprzętu medycznego, sprzętu dla straży pożarnych czy też policji, do przeprowadzania szkoleń oraz zaspokajania wielu innych potrzeb. Środki z funduszu mogłyby także wspierać siły zbrojne, jak miało to miejsce w okresie międzywojennym.

Społeczeństwo wspierające fundusz musiałoby mieć zapewnioną możliwość współdecydowania w wypracowanej formie o celu wydatkowania środków w nim gromadzonych. Niewielkim nakładem budżetowym ze strony państwa, jak również jednostek samorządu terytorialnego oraz przy zaangażowaniu świadomego przecież coraz bardziej naszego społeczeństwa, można byłoby wiele uczynić, aby zwiększyć zdolności obronne państwa.

Istotnym elementem wzmacniającym zdolności obronne jest też wspieranie rodzimego przemysłu obronnego. Wiąże się to z wydatkowaniem środków publicznych na zakup uzbrojenia w polskich zakładach zbrojeniowych. Nasz przemysł zbrojeniowy obecnie nie jest w stanie zaspokoić wszystkich potrzeb sił zbrojnych, istotne jest jednak, by wspierać badania naukowe i rozwojowe w zakresie tych możliwości, które może on zapewnić. Środki wydatkowane na ten cel należy traktować jako inwestycje, które zwrócą się w perspektywie czasowej i przyniosą tym samym państwu korzyści gospodarcze. Zakup sprzętu wojskowego w rodzimych firmach wpłynie na rozwój wielu dziedzin gospodarki narodowej, a w konsekwencji na produkt krajowy brutto (PKB). Może też przynieść korzyści z eksportu wyprodukowanego uzbrojenia.

Następne rozwiązanie mające na celu wsparcie zdolności obronnych to wykorzystanie potencjału organizacji zarówno paramilitarnych, jak i innych w zakresie propagowania postaw prospołecznych. Mogłoby się to odbywać dwojako: dzięki promocji swojej działalności przy okazji innych wydarzeń oraz poprzez działania edukacyjne. Taka forma działalności przyczyni się do budowy świadomości i postaw prospołecznych. Działania tego typu są stosunkowo tanie, nie wymagają też wielkiego zaangażowania logistycznego ze strony państwa czy też samorządu terytorialnego.

PROPOZYCJA

Zdolności obronne naszego kraju należy kształtować wielotorowo. Ich wielkość oraz charakter wynikają głównie z potencjału obronnego państwa, który też jest formowany zwykle w dłuższej perspektywie czasowej. Zatem wzmacnianie zdolności obronnych można oprzeć na realizacji dwóch programów koncepcyjnych. Są to:

– program powszechnego przeszkolenia strzeleckiego społeczeństwa,

– powołanie korpusu żołnierzy niezawodowych.

By realizacja wspomnianych programów była skuteczna, należałoby zacząć od:

– kształtowania postaw patriotycznych w społeczeństwie;

– kształtowania świadomości – bezpieczeństwo – wspólne zadanie;

– odbudowy w społeczeństwie kultury posługiwania się bronią;

– wyszkolenia zasobów osobowych na potrzeby sił zbrojnych i innych służb odpowiedzialnych za zapewnienie bezpieczeństwa przy zaangażowaniu niewielkich środków finansowych oraz przedsięwzięć logistycznych obciążających podmioty publiczne;

– powołania nowej, niezawodowej, ochotniczej formacji w celu zapewnienia ochrony ludności cy-

RYS. 1. SCHEMAT ORGANIZACJI PROGRAMU POWSZECHNEGO PRZESZKOLENIA STRZELECKIEGO

Opracowanie własne.

wilnej w sytuacjach wynikających z zagrożeń zarówno militarnych, jak i niemilitarnych.

Do najważniejszych zasad programu społecznego powszechnej nauki posługiwania się bronią moglibyśmy zaliczyć takie zasady, jak: dobrowolność, powszechność, świadomość, budowa wzajemnego zaufania, minimalizacja kosztów finansowych oraz zaangażowanie logistyczne.

Zgodnie z *zasadą dobrowolności* każdy zdrowy oraz niekarany obywatel naszego kraju, wyrażający dobrowolnie chęć udziału, uczestniczy w programie. Jest on skierowany zarówno do mężczyzn, jak i kobiet.

Zasada powszechności mówi, że program jest skierowany do całego społeczeństwa. Przy jego realizacji należy jednak liczyć się z ograniczonymi możliwościami szkoleniowymi jednostek wojskowych. Trzeba też pamiętać, że jego przeprowadzanie stwarza dodatkowe obciążenie dla dowódców jednostek wojskowych, które byłyby w to zaangażowane.

Zasada świadomości z kolei odnosi się do kształtowania postaw patriotycznych w społeczeństwie. Jej celem jest budzenie postaw prospołecznych polegających na braniu przez obywateli czynnego udziału w kształtowaniu właściwego poziomu bezpieczeństwa w kraju. Rezultatem takich działań może być liczniejszy, czynny udział społeczeństwa w samoorganizacji na rzecz bezpieczeństwa publicznego.

Zasadniczym celem *zasady budowy wzajemnego zaufania* jest przybliżenie społeczeństwu zagadnień związanych z wojskiem. Skutkiem tego będzie większe zainteresowanie społeczne zawodową służbą wojskową.

Jednym z głównych założeń koncepcji wzmacniania zdolności obronnych jest uzyskanie efektów z jednoczesną *minimalizacją kosztów budżetowych*. Realizacja programu powszechnego przeszkolenia strzeleckiego w społeczeństwie nie może być obciążona zbyt wysokimi kosztami w stosunku do celów, jakie są zakładane. Spełnienie tego założenia zapewni akceptację społeczną samej koncepcji.

Zasada minimalizacji zaangażowania logistycznego odnosi się do logistycznego potencjału kraju i jego zaangażowania w realizację koncepcji. Podobnie jak zasada minimalizacji kosztów budżetowych może się przyczynić do społecznej akceptacji koncepcji.

PRZESZKOLENIE STRZELECKIE

W realizację programu powszechnego przeszkolenia strzeleckiego byłyby zaangażowane następujące podmioty: wójt (burmistrz, prezydent miasta), wojskowy komendant uzupełnień (WKU) oraz dowódca jednostki wojskowej (rys. 1). Na jego potrzeby byłby opracowany program szkolenia, który przewidywałby stopniowanie trudności w zakresie zdobywanej wiedzy oraz umiejętności. Obejmowałby on: podstawową wiedzę i umiejętności dotyczące budo-

RYS. 2. SCHEMAT ORGANIZACJI POWOŁANIA DO KORPUSU ŻOŁNIERZY NIEZAWODOWYCH

Opracowanie własne.

wy broni, bezpiecznego posługiwania się nią, jej obsługi czy zasad strzelania. W dalszej części przewidziano by przeprowadzanie strzelań wraz ze stopniowaniem ich trudności oraz podtrzymywanie umiejętności strzeleckich w ramach kolejnych turnusów jednodniowych. Turnusy szkoleniowe mogłyby być organizowane w soboty.

Realizacja programu powszechnego przeszkolenia strzeleckiego obciążałaby jednak znacznie jednostki wojskowe. Zatem ich dowódcy, aby sprostać temu zadaniu, mogliby wyznaczyć odpowiednio wcześniej żołnierzy, którzy by je wykonywali, a program mógłby być modyfikowany oraz uszczegóławiany w zależności od potrzeb.

Program powszechnego przeszkolenia strzeleckiego generowałby problemy logistyczne, które powinny zostać rozstrzygnięte na etapie jego projektowania. W związku z tym należałoby:

– wytypować podmioty biorące w nim udział;

– wypracować stosowne procedury postępowania z uczestnikami programu;

– wytypować jednostki wojskowe zaangażowane w realizację programu;

– wypracować ustalenia organizacyjne na poziomie jednostki wojskowej dotyczące programu;

– zaangażować logistycznie wojskowe oddziały gospodarcze (WOG), w tym podmioty nadrzędne, w działania odnoszące się do zabezpieczenia materiałowego i finansowego programu;

– opracować programy szkolenia;

– wypracować procedury powoływania uczestników programu do służby wojskowej zarówno zawodowej, jak i w korpusie żołnierzy niezawodowych.

KORPUS ŻOŁNIERZY NIEZAWODOWYCH

Do najważniejszych zasad nowo powołanej formacji moglibyśmy zaliczyć zasadę: dobrowolności, elastyczności, gotowości, budowy wzajemnego zaufania, trwałości poziomu wyszkolenia, terytorialności, minimalizacji kosztów finansowych i zaangażowania logistycznego. Zasady dotyczące korpusu żołnierzy niezawodowych byłyby powiązane z zasadami programu powszechnego przeszkolenia strzeleckiego.

Zasada dobrowolności zakłada, że podstawowym sposobem rekrutacji byłoby odbycie kursu w ramach powszechnego programu przeszkolenia strzeleckiego oraz podtrzymywanie nabytych umiejętności w czasie kolejnych szkoleń.

Zasada elastyczności odnosi się do procesu szkolenia. Polega na tym, że kursy strzeleckie w ramach powszechnego programu strzeleckiego (szczególnie te, które dotyczą korpusu żołnierzy niezawodowych) będą organizowane w terminach zaplanowanych z właściwym wyprzedzeniem. Aby swobodnie dokonać wyboru terminu szkolenia, uczestnicy aplikują na te terminy, które im odpowiadają. Zapewni to także jednostkom wojskowym czas niezbędny na właściwe przygotowanie się.

Zasada gotowości dotyczy możliwości szybkiej reakcji na potencjalne zagrożenia. Opiera się na ciągłości procesu szkolenia oraz przechowywaniu wyposażenia żołnierskiego (z wyjątkiem broni) w domu.

Zasada budowy wzajemnego zaufania jest związana z programem powszechnego przeszkolenia strzeleckiego. Uczestnicy szkolenia wykonują inne zawody i szkolą się w ramach swojego korpusu dla dobra lokalnej społeczności. Pomagając ludziom, budują wzajemne zaufanie.

Zasada trwałości odnosi się do sukcesywnego podtrzymywania nabytych podczas szkolenia umiejętności .

Zasada terytorialności polega na tym, że członek korpusu żołnierzy niezawodowych pełni służbę w swojej społeczności lokalnej, w której zamieszkuje.

Zasada minimalizacji kosztów finansowych dotyczy wydatków ze środków budżetowych na potrzeby działalności szkoleniowej i oznacza również jej funkcjonowanie przy możliwym minimalnym zaangażowaniu zasobów logistycznych z gospodarki narodowej.

Powołanie do pełnienia służby w korpusie żołnierzy niezawodowych byłoby dobrowolne (rys. 2). Rekrutacja do niego odbywałaby się spośród uczestników programu powszechnego przeszkolenia strzeleckiego. Zasadniczym celem powołania korpusu byłaby aktywizacja społeczeństwa (a konkretnie społeczności lokalnej) pod kątem dbałości o bezpieczeństwo będące dobrem wspólnym. Przeznaczenie korpusu żołnierzy niezawodowych mogłoby być dość szerokie. Nowo powołana struktura wspierałaby lokalną społeczność, z której się wywodzi, na wypadek wystąpienia zagrożeń zarówno niemilitarnych, jak i militarnych. W wypadku zagrożeń militarnych jej głównym zadaniem byłaby ochrona ludności, jej ewakuacja oraz udzielanie niezbędnej pomocy.

Propozycja powołania korpusu żołnierzy niezawodowych wynika z potrzeby stworzenia formacji, której główne zadania byłyby związane z ochroną ludności cywilnej w sytuacji zagrożenia bezpieczeństwa. Zadania dotyczyłyby zarówno zagrożeń militarnych, jak i niemilitarnych w czasie pokoju, kryzysu i wojny. Do rozstrzygnięcia zatem pozostałyby następujące problemy natury logistycznej (na początkowym etapie tworzenia):

– wytypowanie podmiotów biorących udział w programie;

– wypracowanie procedur postępowania uczestników programu;

– opracowanie struktury organizacyjnej korpusu żołnierzy niezawodowych;

– zaangażowanie logistyczne wojskowych oddziałów gospodarczych (WOG), w tym podmiotów nadrzędnych, w realizację zabezpieczenia materiałowego i finansowego;

– wypracowanie ustaleń dotyczących przydziału wyposażenia wojskowego na rzecz żołnierzy korpusu;

– ustalenia odnoszące się do miejsc przechowywania broni;

– wypracowanie programu szkolenia żołnierzy korpusu.

W dalszym etapie rozwoju korpusu żołnierzy niezawodowych do rozstrzygnięcia byłyby następujące problemy: wypracowanie kierunków (koncepcji) jego rozwoju, dostosowanie do potrzeb programów szkolenia, wypracowanie wymagań odnoszących się do sprzętu wojskowego (SpW) oraz pozostałego wyposażenia zgodnie z przyjętą linią rozwoju.

REFLEKSJE

Można zatem na koniec zadać następujące pytanie. Jeżeli przyszłe, potencjalne konflikty zbrojne (zgodnie ze wspomnianą tzw. trzecią falą) będą prowadzone z użyciem coraz bardziej zaawansowanych technicznie środków walki i tym samym wysoko wykwalifikowanych żołnierzy, nie mówiąc już o samych sposobach prowadzenia działań, to po co trwonić wysiłek na tworzenie korpusu żołnierzy niezawodowych, a także zrzucać na siły zbrojne ciężar realizacji programu powszechnego przeszkolenia strzeleckiego? Odpowiedź na tak postawione pytanie (według opinii autora) brzmi następująco. Położenie geopolityczne naszego kraju z jednej strony daje nam wielkie szanse, z drugiej zaś, jak uczy historia, przynosi wiele zagrożeń, które wynikają z położenia między mocarstwami dążącymi do osiągania swoich celów, niekoniecznie zbieżnych z naszymi. Ponadto, mimo z jednej strony dynamicznego rozwoju gospodarczego, z drugiej zaś niedoinwestowania wielu dziedzin funkcjonowania państwa, wydaje się, że nieprędko osiągniemy taki stopień nakładów środków publicznych na armię, jaki pozwoli jej w pełni spełnić wymagania wojen tzw. trzeciej fali.

Realizując program powszechnego przeszkolenia strzeleckiego oraz tworząc korpus żołnierzy niezawodowych, osiągniemy wiele istotnych z punktu widzenia bezpieczeństwa publicznego celów, nie nadwyrężając przy tym wydatków publicznych – co jest bardzo istotne. Dodatkowo niezaprzeczalnym atutem jest upowszechnienie w społeczeństwie kultury posługiwania się bronią, co także wzmocni nasz kapitał odstraszania. ■

Siły zbrojne w sytuacjach kryzysowych

POWODZIE, KATASTROFY PRZEMYSŁOWE, EPIDEMIE CZY TEŻ NARUSZENIA BEZPIECZEŃSTWA PUBLICZNEGO TO SYTUACJE, W KTÓRYCH GOTOWOŚĆ DO DZIAŁANIA OKREŚLONYCH ELEMENTÓW SYSTEMU BEZPIECZEŃSTWA PAŃSTWA ORAZ ICH SKUTECZNOŚĆ SĄ NIEZBĘDNE.

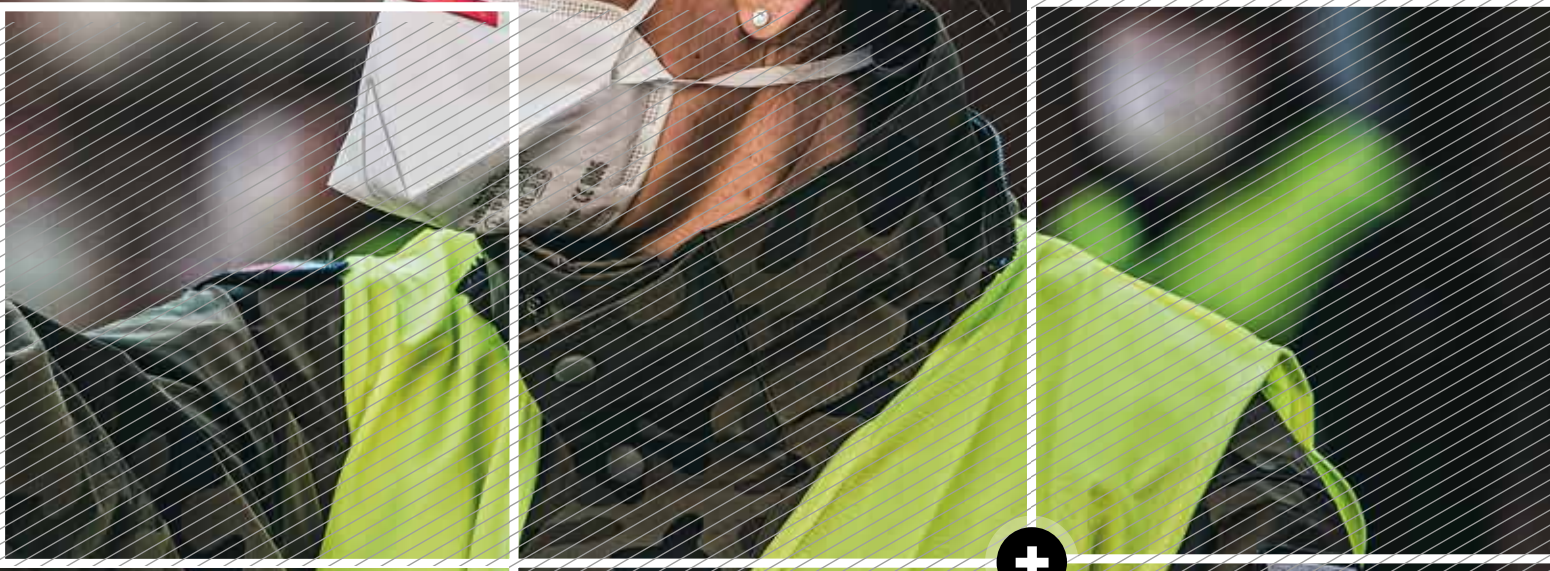
mjr dypl. SZRP Krzysztof Stamborski

Autor jest szefem Sekcji Planowania Logistyki w 21 Bazie Lotnictwa Taktycznego.

Jednym z ważniejszych zadań, jakie wypełnia państwo w reagowaniu na sytuacje kryzysowe, jest zapewnienie bezpieczeństwa ludności oraz jej mienia w sytuacjach zagrożenia. Do realizacji wymienionych zadań powołano organy oraz instytucje wraz z niezbędnymi siłami i środkami, koniecznymi do ratowania życia i zdrowia obywateli, którzy mogą być ofiarami klęsk żywiołowych, katastrof naturalnych bądź awarii technicznych. Zgodnie z ustawą o zarządzaniu kryzysowym[1] *sytuacja kryzysowa to stan rzeczy, który wpływa negatywnie na poziom bezpieczeństwa ludzi, mienia lub środowiska w znacznych rozmiarach, wywołując znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.*

Skuteczność prowadzonych zadań, które zapewnią pomoc poszkodowanym, jest zależna od właściwej organizacji oraz odpowiednich sił i środków umożliwiających prowadzenie akcji ratowniczych. Często w wyniku dokonanej analizy okazuje się, że podjęte działania są niewystarczające i po uruchomieniu funkcjonujących regulacji prawnych podejmuje się decyzję o wykorzystaniu sił zbrojnych. Są one zaliczane do najlepiej zorganizowanych podmiotów, przygotowa-

1 *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 nr 89 poz. 590.



Siły zbrojne wspierają działania, dzięki którym możliwe jest zatrzymanie epidemii koronawirusa oraz łagodzenie jej skutków.

nych do sprawnego i skutecznego działania zarówno w czasie pokoju, kryzysu i wojny. Wydzielone siły, specjalistycznie wyszkolone i dysponujące odpowiednim wyposażeniem oraz potencjałem logistycznym, stają się kluczowym instrumentem do wsparcia podmiotów niemilitarnych na obszarze całego kraju.

ZASADY WYKORZYSTANIA

W ciągu ostatnich dziesięcioleci wystąpiły wyraźne zmiany w poglądach dotyczących bezpieczeństwa naszego kraju, w tym przede wszystkim wobec występujących w stosunku do niego zagrożeń . Fakt ten wynika z przesunięcia na bardziej odległy plan zagrożeń militarnych w Europie. Te bowiem zmniejszyły się po wstąpieniu do Sojuszu Północnoatlantyckiego. W zaistniałej sytuacji wzrasta ryzyko powstawania zagrożeń niemilitarnych, a także zmienia się pojęcie *ochrony ludności*, które jest definiowane jako *zapewnienie bezpieczeństwa ludziom, ich mieniu i środowisku przed wypadkami i klęskami każdego typu i rodzaju, w tym także w stanie zagrożenia epidemicznego*. Ochronę ludności możemy zdefiniować jako zapewnienie bezpieczeństwa życia i zdrowia ludzi oraz ich mienia, a także utrzymania właściwych warunków środowiskowych do ich przeżycia, świadczenia pomocy socjalnej i psychologicznej osobom poszkodowanym oraz osłony prawnej, a także do ich przygotowania edukacyjnego i sprawnościowego do radzenia sobie w czasie katastrof czy też klęsk żywiołowych.

Zagrożenia o charakterze niemilitarnym mogą powodować skutki porównywalne do tych, które niesie ze sobą wojna. Dość ważne stają się również zagrożenia związane z dostawami surowców strategicznych pozyskiwanych w ramach umów międzynarodowych. Nowym zagrożeniem zyskującym coraz większe znaczenie staje się naruszenie systemu finansowego, opartego w większości na bankowości internetowej czy też wszelkiego rodzaju transakcjach wykonywanych w środowisku sieciowym przez wszechobecne próby jego paraliżowania za pośrednictwem wirusów komputerowych czy też penetrowania i fałszowania danych w kluczowych instytucjach państwowych.

Siły zbrojne są zasadniczym narzędziem polityki państwa i od wieków spełniają istotną funkcję w zakresie bezpieczeństwa. Wraz z upływem czasu oraz zachodzącymi zmianami ich rola ewoluowała. Obecnie oczywiście ich zadania do obrony przed agresją zbrojną są pierwszoplanowe, ale częściej są one wykorzystywane jako instrument wsparcia ludności i władz cywilnych w sytuacjach kryzysowych.

Użycie sił zbrojnych, stanowiących zasadniczy element systemu bezpieczeństwa narodowego, traktuje się jako ostateczność. Ograniczenia i możliwości ich wykorzystania w sytuacjach kryzysowych są determinowane obowiązującymi przepisami prawa oraz wynikającymi potrzebami.

Zasadniczym aktem prawnym regulującym zakres zadań oraz kompetencje użycia oddziałów i pododdziałów sił zbrojnych w sytuacjach kryzysowych jest ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Podkreśla się w niej, że siły zbrojne mogą zostać wykorzystane do zwalczania klęsk żywiołowych oraz usuwania ich skutków, w działaniach o charakterze antyterrorystycznym, do ochrony mienia oraz w akcjach poszukiwawczych. Ponadto do ratowania lub ochrony zdrowia i życia ludzkiego, oczyszczania terenów z materiałów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwiania. W ustawie wprost zaznacza się, że siły zbrojne mogą uczestniczyć w zadaniach odnoszących się do zarządzania kryzysowego[2].

Zapisy przytoczonej ustawy znalazły uszczegółowienie w ustawie o zarządzaniu kryzysowym, która jest najważniejszym aktem prawnym odnoszącym się bezpośrednio do omawianej problematyki. Określono w niej warunki, sposób oraz procedurę aktywacji sił zbrojnych do udziału w sytuacji, gdy użycie innych sił i środków jest niemożliwe lub niewystarczające. W myśl zapisów wspomnianej ustawy minister obrony narodowej, na wniosek wojewody, może przekazać do jego dyspozycji siły i środki pozostające w dyspozycji resortu wraz ze skierowaniem ich do wykonywania określonych zadań z zakresu zarządzania kryzysowego[3].

Wykorzystanie potencjału sił zbrojnych jest możliwe również w sytuacji wprowadzenia jednego ze stanów nadzwyczajnych przewidzianych w *Rozdziale XI Konstytucji Rzeczypospolitej Polskiej z 1997 roku*. Do takich zalicza się: stan wojenny (art. 229), stan wyjątkowy (art. 230) oraz stan klęski żywiołowej (art. 232).

Stan wyjątkowy wprowadza prezydent RP na wniosek prezesa Rady Ministrów. Decyzja o użyciu oddziałów i pododdziałów sił zbrojnych ma na celu przywrócenie prawidłowego funkcjonowania państwa w razie naruszenia porządku ustrojowego, konstytucyjnego oraz bezpieczeństwa i porządku publicznego. W ustawie wyraźnie podkreśla się, iż użycie sił zbrojnych na potrzeby stanu wyjątkowego nie powinno zagrozić zdolności do realizacji ich zasadniczej funkcji, która wiąże się z gotowością do obrony terytorium Polski lub sojusznika w wypadku agresji zbrojnej[4].

Następny stan nadzwyczajny wiąże się z wystąpieniem klęski żywiołowej rozumianej jako awaria techniczna lub katastrofa naturalna, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko z zastosowaniem nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji

2 *Ustawa z dnia 21 listopada 1967roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, Dz.U. 1967 nr 44 poz. 220.

3 Art. 18, ust. 1. *Ustawy z dnia 27 kwietnia o zarządzaniu kryzysowym,* Dz.U. 2007 nr 89 poz. 590 z późn. zm.

4 Art. 11. *Ustawy z dnia 21 czerwca 2002 roku o stanie wyjątkowym,* Dz.U. 2002 nr 113 poz. 985.

oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem[5]. W tym wypadku jednym z takich nadzwyczajnych środków może być np. sięgnięcie po pomoc sił zbrojnych. Na wniosek właściwego terytorialnie wojewody minister obrony narodowej może przekazać pododdziały lub oddziały wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieganiem skutkom klęski żywiołowej lub do usuwania jej skutków[6].

Dla sił zbrojnych przewidziano również rolę podmiotu wspierającego inne instytucje systemu zarządzania kryzysowego w sytuacjach, gdy podmiot wiodący nie jest w stanie niezależnie przeciwdziałać zagrożeniu. Przykładem tego rozwiązania są chociażby zapisy ustawy o policji. Założono w niej uproszczenie zasad użycia sił zbrojnych dzięki obniżeniu szczebla decyzyjnego, koniecznego do podjęcia decyzji o udzieleniu wsparcia policji. Pomoc w tym wypadku może być udzielona jedynie w sytuacji wystąpienia poważnego zagrożenia bezpieczeństwa i porządku publicznego bądź dokonania przestępstwa o charakterze terrorystycznym[7]. Biorąc pod uwagę uporządkowany charakter organizacji wojskowej, dowodzenie oddziałami i pododdziałami wydzielonymi do działań w sytuacjach kryzysowych odbywa się na zasadach ustalonych w regulaminach wojskowych i według procedur obowiązujących w siłach zbrojnych.

Podstawowym dokumentem planistycznym, sporządzanym na szczeblu strategicznym i regulującym kwestie wykorzystania oddziałów i pododdziałów sił zbrojnych, jest *Plan zarządzania kryzysowego Ministerstwa Obrony Narodowej*, wprowadzony do użytku na mocy rozkazu szefa Sztabu Generalnego Wojska Polskiego. Określa się w nim gotowość sił i środków, procedury aktywacji, działania systemu dowodzenia i łączności, zasady ujednolicenia oraz organizację zabezpieczenia logistycznego i medycznego. Ujęto w nim także przykłady, które mogą zostać uwzględnione na potrzeby zarządzania kryzysowego. W planach szczegółowych w pierwszej kolejności pod uwagę wzięto zagadnienia uregulowań prawnych w zakresie możliwości udziału sił zbrojnych w poszczególnych sytuacjach kryzysowych, następnie przedstawiono szczegółową charakterystykę zagrożenia, wykaz realizowanych zadań, procedury aktywizacji dostępnych sił i środków oraz zasady współdziałania z innymi podmiotami[8].

ELEMENTY SYSTEMU

Obecnie można zaobserwować poszerzanie zakresu działań realizowanych przez siły zbrojne. Zadania wykonywane w sytuacjach zagrożeń niemilitarnych stawiane są na równi z zadaniami realizowanymi przez siły zbrojne w zakresie bezpieczeństwa militarnego[9]. W *Strategii bezpieczeństwa narodowego RP* zarówno z 2007, jak i z 2014 roku zauważono, że siły zbrojne dysponują potencjałem ludzkim, organizacyjnym oraz sprzętem i wyposażeniem, które mogą być użyte do wspierania instytucji cywilnych podczas wystąpienia nadzwyczajnych zagrożeń.

Zwiększający się zakres zadań dla sił zbrojnych, odnoszący się do zarządzania kryzysowego, w znacznej mierze wynika z:

– przydatności organizacji wojskowej (dyspozycyjność, zdyscyplinowanie, mobilność przestrzennej lokalizacji);

– wzrastającej skali zagrożeń niemilitarnych (obecnie tego typu zagrożenia są równie groźne jak wojny i ich skutki);

– niewydolności organizacyjnej i wykonawczej, zwłaszcza w sytuacjach szczególnych zagrożeń, stałych służb cywilnych, a także z niedostatecznego ich przygotowania do sprostania nagłemu wzrostowi potrzeb ratowniczych, ochronnych, logistycznych, inżynieryjnych i innych w trybie natychmiastowym. Oznacza to, że w sytuacjach szczególnych zagrożeń i potrzeb zachodzi wręcz konieczność wsparcia wojskowego[10].

Unikatowy charakter sił zbrojnych i ich wyposażenie pozwalają na realizację w obszarze zarządzania kryzysowego następujących zadań:

– uczestnictwo w zwalczaniu klęsk żywiołowych i ich skutków;

– współdziałanie z policją w działaniach antyterrorystycznych;

– współudział w monitorowaniu zagrożeń;

– czynności mające na celu ocenę skutków zjawisk zaistniałych w obszarze wystąpienia sytuacji kryzysowej;

– akcje o charakterze ratowniczo-poszukiwawczym;

– ewakuacje poszkodowanej ludności i jej mienia;

– organizowanie tymczasowego zakwaterowania dla ewakuowanej ludności;

– współudział w ochronie mienia na obszarze wystąpienia sytuacji kryzysowej;

– izolacja obszaru oddziaływania sytuacji kryzysowej i miejsca prowadzenia akcji ratowniczej;

– wykonywanie zadań o charakterze ratowniczym, ewakuacyjnym i zabezpieczającym przy obiektach budowlanych i zabytkach;

– prace wymagające specjalistycznego sprzętu lub materiałów wybuchowych znajdujących się w wyposażeniu sił zbrojnych;

5 Art. 3, pkt 1 *Ustawy z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej,* Dz.U. 2002 nr 62 poz. 558.

6 Art. 2, 5, ibidem.

7 *Art. 18* i inne *Ustawy z dnia 6 kwietnia 1990 roku o Policji,* Dz.U. 2011 poz. 1687.

8 W. Lidwa, *Zarządzanie w sytuacjach kryzysowych*, AON, Warszawa 2011, s. 55.

9 G. Sobolewski, *Siły zbrojne RP w zarządzaniu kryzysowym. Aspekt narodowy i międzynarodowy,* Warszawa 2013, s. 111.

10 *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2007 roku,* Warszawa 2007, s. 24.

– likwidacja skażeń chemicznych i biologicznych;
– pomiar i usuwanie skażeń promieniotwórczych;
– wykonywanie napraw i odbudowy infrastruktury technicznej;
– udzielanie pomocy medycznej i wykonywanie zadań sanitarno-epidemiologicznych[11].

Szczególną rolę w sytuacjach kryzysowych odgrywają pododdziały wojsk inżynieryjnych. Jest to rodzaj wojsk składający się z oddziałów i pododdziałów różnych specjalności, przeznaczonych do realizacji zadań w zakresie wsparcia inżynieryjnego działań taktycznych innych rodzajów wojsk. Mogą one być wykorzystane do zadań i prac inżynieryjnych podczas akcji ratowniczych oraz do likwidacji skutków katastrof i klęsk żywiołowych bądź do zapobiegania im w okresie pokoju w ramach zarządzania kryzysowego.

Pododdziały wojsk inżynieryjnych występują we wszystkich rodzajach sił zbrojnych. Ich skład i wyposażenie są stosowne do rodzaju oraz zakresu przewidywanych zadań. Przekrój zadań oddziałów i pododdziałów wojsk inżynieryjnych w sytuacjach kryzysowych może być większy w stosunku do ich liczby i jest zasadniczym czynnikiem uwzględnianym podczas planowania użycia sił w ramach zarządzania kryzysowego, sposobów dowodzenia, ich zabezpieczenia logistycznego, a także współdziałania z podmiotami militarnymi i niemilitarnymi. Jednak ich specjalistyczne wyposażenie sprawia, że są one głównym wykonawcą zadań w wypadku wystąpienia sytuacji kryzysowej na obszarze kraju. Pododdziały, które są przewidziane do działań kryzysowych, to przede wszystkim bataliony ratownictwa inżynieryjnego. Przeznaczone są one do wykonywania zadań ewakuacyjno-ratowniczych oraz związanych z likwidacją skutków wynikających z wystąpienia sytuacji kryzysowych, samodzielnie lub we współdziałaniu z siłami układu pozamilitarnego. Wśród wielu zadań realizowanych przez nie na rzecz szeroko pojętego bezpieczeństwa w sytuacjach kryzysowych należałoby wyróżnić:
– ewakuacyjno-ratownicze, w tym ewakuację ludzi i mienia z terenów zagrożonych i objętych kataklizmem;
– inżynieryjne, związane z odtwarzaniem sprawności obiektów infrastruktury komunikacyjnej w rejonach dotkniętych żywiołem oraz z doraźną naprawą i wzmocnieniem wałów przeciwpowodziowych;
– wykonywanie przepraw mostowych przez przeszkody terenowe z wykorzystaniem mostów towarzyszących oraz przepraw desantowych z zastosowaniem pływających transporterów gąsienicowych (PTS) i łodzi desantowych (ŁD)[12].

Podkreślając zaangażowanie jednostek wojskowych w czasie sytuacji kryzysowych, należy zaznaczyć, iż siły zbrojne są zdolne do zabezpieczenia logistycznego zarówno poszkodowanych, jak i pozostałych służb realizujących zadania w rejonie wystąpienia sytuacji kryzysowych.

Zadania wsparcia logistycznego obejmują między innymi wsparcie sił cywilnych w: dostawach wody i żywności; organizowaniu usług transportowych i tymczasowych miejsc zakwaterowania; organizacji ratownictwa medycznego i przedsięwzięć leczniczo-ewakuacyjnych, sanitarnohigienicznych i przeciwepidemicznych oraz w innych działaniach w zależności od potrzeb ludności cywilnej i podmiotów zaangażowanych w rozwiązywanie sytuacji kryzysowej.

Największą przydatność w początkowym okresie sytuacji kryzysowej mają zestawy żywnościowe zarówno indywidualne, jak i grupowe.

Istotną pomocą może być również wydzielenie przez jednostki wojskowe sprzętu do przygotowania posiłków gorących, przechowywania żywności i jej transportu, do wypieku chleba, podgrzewaczy do wody itp. W organizacji żywienia zbiorowego do przygotowania gorących posiłków mogą być również wykorzystywane należności wojskowe skoncentrowane. Służą one do przygotowania posiłków, gdy brakuje artykułów świeżych.

Organizacja usług transportowych polega przede wszystkim na wydzielaniu środków transportu, pomocy w wykonywaniu prac załadunkowych, organizacji kolumn transportowych, ich pilotowaniu oraz kierowaniu ruchem na drogach dowozu i ewakuacji. Wszystkie jednostki wojskowe dysponują pojazdami samochodowymi, które mogą być wydzielane do realizacji zadań zaopatrzeniowych i ewakuacyjnych na rzecz poszkodowanej ludności. Niektóre jednostki posiadają środki transportu powietrznego, w tym śmigłowce przydatne do wykonywania zadań trans-

SIŁY ZBROJNE SĄ SKUTECZNYM ŚRODKIEM DO SPRAWNEGO DZIAŁANIA W CZASIE POKOJU,

11 Z. Kuśmierek, *Udział wojska w sytuacjach kryzysowych*, „Zeszyty Naukowe Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2014 nr 1, s. 18–19.

12 A. Bartnicki, *Wykorzystanie pododdziałów inżynieryjnych Sił Zbrojnych RP w logistycznym zabezpieczeniu sytuacji kryzysowych*, WAT, Warszawa 2016, s. 136.

portowych, w wypadku gdy sieć kolejowa lub drogowa zostały zniszczone. W aspekcie wsparcia sił cywilnych podczas organizacji zakwaterowania szczególną pomoc mogą udzielić jednostki wojskowe, zapewniając tymczasowe miejsca zakwaterowania na bazie tzw. miasteczek namiotowych. Miasteczka te oprócz odpowiedniej liczby namiotów, stosownego wyposażenia oraz prawidłowego ich rozmieszczenia zapewniają właściwe warunki sanitarnohigieniczne

POZOSTAJĄCYM W CIĄGŁEJ GOTOWOŚCI KRYZYSU ORAZ WOJNY

i przeciwepidemiczne. Infrastrukturę komunalną stanowią: urządzenia dostarczające podstawowe media, czyli energię elektryczną, wodę pitną, ogrzewanie; baza żywnościowa (stołówki, kuchnie, urządzenia do dystrybucji żywności); urządzenia medyczne (przychodnie, apteki); węzły sanitarne; obiekty magazynowe i handlowe.

Wsparcie sił cywilnych podczas organizacji ratownictwa medycznego w sytuacjach kryzysowych polega przede wszystkim na wydzieleniu żołnierzy ratowników medycznych oraz przekazaniu zestawów medycznych do udzielania pomocy przedlekarskiej. Specjalność ratownika posiadają wszyscy żołnierze i pracownicy wojska zajmujący stanowiska pielęgniarek i pielęgniarzy, a ratownika medycznego – wszyscy podoficerowie wojskowej służby zdrowia. Również uprawnienia ratownika, na zasadzie drugiej specjalności, może mieć wielu innych żołnierzy i pracowników wojska, szczególnie w pododdziałach wojsk inżynieryjnych, chemicznych oraz logistycznych.

Do wsparcia sił cywilnych podczas organizacji przedsięwzięć leczniczo-ewakuacyjnych najbardziej są przystosowane pododdziały i oddziały wojskowej służby zdrowia. W przedsięwzięciach tych mogą brać udział plutony medyczne batalionów, kompanie medyczne pułków i brygad czy bataliony medyczne związków operacyjnych. Kompanie samochodów sanitarnych dysponują samochodami sanitarnymi, w których chorzy i ranni mogą być ewakuowani w pozycji leżącej i siedzącej z możliwością udzielenia im pomocy lekarskiej lub wykonywania medycznych czynności ratunkowych.

Do wsparcia sił cywilnych podczas organizacji przedsięwzięć sanitarnohigienicznych jest przygotowany batalion przeciwepidemiczny. W swojej strukturze ma on dziewięć laboratoriów uniwersalnych na samochodach oraz 12 łaźni – dezynfektorów na samochodach.

Wsparcie sił cywilnych podczas organizacji przedsięwzięć przeciwepidemicznych będzie polegać na skierowaniu odpowiednich specjalistów, którzy w zależności od sytuacji będą wykonywać takie zadania, jak: organizowanie ośrodków izolacyjno-terapeutycznych w wypadku stwierdzenia epidemii chorób zakaźnych, prowadzenie rozpoznania sanitarno-epidemicznego, wykonywanie szczepień ochronnych oraz dezynfekcji środków transportu, pomieszczeń kwaterunkowych i wyposażenia terenu. Do dezynfekcji mogą być wykorzystywane środki i sprzęt indywidualny oraz instalacje samochodowe, którymi dysponują pododdziały wojsk chemicznych, takie jak np. instalacja IRS.

PRZYKŁADY

Skutecznym rodzajem sił zbrojnych, mającym zdolności do realizacji zadań wspierania podsystemów ochronnych w zakresie bezpieczeństwa wewnętrznego i pomocy społeczeństwu, są niewątpliwie wojska obrony terytorialnej (WOT). Fundamentalne znaczenie mają specyficzne dla tego rodzaju sił zbrojnych cechy odróżniające je od wojsk operacyjnych takie, jak:

– terytorialność – specyfika działania polega na ich użyciu w stałych rejonach odpowiedzialności (SRO);

– masowość – oddziały i pododdziały są formowane głównie z wykorzystaniem zasobów miejscowych.

Wojska obrony terytorialnej zostały użyte do usuwania skutków klęsk żywiołowych w maju 2019 roku. Żołnierze wspierali lokalne społeczności, terenowe organy administracji państwowej i publicznej oraz służby ratownicze, w szczególności Państwową i Ochotniczą Straż Pożarną. Usuwali skutki trąby powietrznej na Lubelszczyźnie.

Działania rozpoczęto wczesnym popołudniem 21 maja w województwie lubelskim od usuwania skutków trąby powietrznej, która przeszła przez miejscowości w gminach Konopnica i Wojciechów. Po niespełna 4 godz. od wystąpienia kataklizmu działania podjął Zespół Oceny Wsparcia 2 Lubelskiej Brygady OT. Na wniosek wojewody lubelskiego minister obrony narodowej podjął decyzję o skierowaniu w rejon dotknięty kataklizmem blisko 200 żołnierzy z 2 BOT. Do ich głównych zadań należało: wsparcie służb ratowniczych w zapewnieniu przejezdności dróg, usuwanie powalonych drzew na terenach posesji, zabezpieczenie dostaw energii elektrycznej do gospodarstw i instytucji oraz oświetlenie rejonu prowadzenia działań ratowniczych. Działania prowadzono trzy doby. Zakończyły się one 23 maja o godz. 15.00.

Jednocześnie na skutek niekorzystnych zmian pogodowych, w tym głównie długotrwałych i intensywnych opadów, na południu kraju zaczęły wylewać rzeki. Z wnioskami do ministra obrony narodowej o wsparcie sił zbrojnych w usuwaniu skutków powodzi wystąpili wojewodowie: podkarpacki, małopolski, śląski oraz świętokrzyski. Zgodnie z decyzją ministra obrony narodowej do przeciwdziałania powodzi oraz zwalczania jej skutków skierowano sześć zgrupowań zadaniowych, w ramach których było zaangażowanych ponad 1200 żołnierzy WOT. Ich główne zadania obejmowały: wzmacnianie wałów przeciwpowodziowych, zabezpieczanie osunięć, przygotowanie i transport materiałów przeciwpowodziowych, wypompowywanie wody i oświetlanie rejonów działań.

Na Podkarpaciu od 22 do 27 maja 2019 roku bezpośrednio było zaangażowanych ponad 350 żołnierzy 3 Podkarpackiej Brygady OT. W tym samym czasie na terenie Małopolski zadania wykonywało ponad 300 żołnierzy 11 Małopolskiej Brygady OT. Od 22 do 23 maja na Śląsku działania prowadziło ponad 160 żołnierzy 13 Śląskiej Brygady OT. Od 24 do 28 maja na terenie województwa świętokrzyskiego było zaangażowanych ponad 430 żołnierzy z 2 oraz 10 BOT.

W realizację zadań z zakresu zarządzania kryzysowego, które miały na celu wsparcie organów administracji publicznej i służb ratowniczych w usuwaniu skutków zagrożeń, bezpośrednio zaangażowanych w pomoc było 1440 żołnierzy WOT. Działania na terenie pięciu województw prowadziło siedem zgrupowań zadaniowych. Zdecydowaną większość żołnierzy WOT (1179) stanowili żołnierze, których odsetek stawiennictwa w trybie alarmowym wyniósł aż 95%. W trzeciej godzinie od otrzymania sygnału stawiało się 60% alarmowo powołanych żołnierzy. Tak wysokie wskaźniki są na pewno odzwierciedleniem tego, jak poważnie żołnierze OT podchodzą do swoich zadań. Dzięki nim możliwe było znaczne zminimalizowanie skutków powodzi i zniszczeń będących następstwem trąby powietrznej.

Siły i środki WOT od jesieni 2018 roku są włączone do systemu zarządzania kryzysowego resortu obrony narodowej. Procedura ich uruchomienia jest taka sama, jak w wypadku innych rodzajów sił zbrojnych i realizowana zgodnie z ustawą z 26 kwietnia 2007 roku o zarządzaniu kryzysowym, a wydzielone siły są przekazane w podporządkowanie Dowództwa Operacyjnego RSZ .

Należy stwierdzić, że ze względu na swoją terytorialność i masowość pododdziały WOT przejawiają daleko idącą uniwersalność w działaniach niemilitarnych oraz stanowią istotne wsparcie dla władz lokalnych w reagowaniu na skutki klęsk żywiołowych, katastrof czy też wypadków. Funkcjonowanie pododdziałów wojsk obrony terytorialnej znacząco przyczynia się do wzmocnienia roli wsparcia sił zbrojnych w sytuacji wystąpienia klęsk żywiołowych i zwiększenia potencjału sił ratowniczych.

WALKA Z EPIDEMIĄ KORONAWIRUSA

Siły zbrojne wspierają działania, dzięki którym możliwe jest zatrzymanie epidemii koronawirusa oraz łagodzenie jej skutków. We wszystkich województwach działają zgrupowania zadaniowe, które udzielają wsparcia Ministerstwu Zdrowia. Mają one do dyspozycji m.in.: kilkadziesiąt pojazdów sanitarnych i mikrobusów, dezynfekcyjne zespoły zadaniowe, mobilne zespoły medyczne i personel medyczny, kontenerowy szpital polowy we Wrocławiu, wyposażony w 100 łóżek i przeznaczony do kwarantanny oraz udzielania pomocy potrzebującym, a także budynek wyposażony w 200 łóżek do przeprowadzania kwarantanny. W całym kraju działa siedem wojskowych laboratoriów do wykonywania testów na koronawirusa, w tym dwa mobilne. Siły powietrzne w razie potrzeby dysponują samolotami i śmigłowcami do ewakuacji medycznej. Ważne zadanie w tym czasie wykonują pododdziały wojsk chemicznych, które każdego dnia dezynfekują szpitale, domy pomocy społecznej, ulice, przystanki autobusowe oraz zabezpieczają dezynfekcję sprzętu wojskowego. Wśród zadań jest także dezynfekcja cargo, które przylatuje z polskich kontyngentów wojskowych. Swoje zadania mają także podchorążowie, którzy każdego dnia wspierają służby medyczne, a we współpracy z żołnierzami WOT zaspokajają potrzeby osób starszych.

Szczegółowe działania podejmowane przez siły zbrojne w czasie walki z epidemią przedstawia poniższe kalendarium[13]:

- 16 marca – minister obrony narodowej podjął decyzję o zaangażowaniu podchorążych w działania mające na celu powstrzymanie rozprzestrzeniania się koronawirusa. Ich zakres będzie obejmował zaopatrzenie w żywność i leki dla osób potrzebujących, w tym dla osób objętych kwarantanną. Dodatkowo podchorążowie Wojskowej Akademii Technicznej w razie potrzeby będą udzielać wsparcia technicznego administracji oraz samorządom w zakresie uruchamiania usług zdalnych. Na wrocławskim lotnisku rozpoczęła się budowa kontenerowego szpitala polowego, gdzie miały się odbywać konsultacje specjalistyczne i badania diagnostyczne żołnierzy i pracowników wojska powracających z działań poza granicami państwa;
- 17 marca – żołnierze 10 Śląskiej Brygady Obrony Terytorialnej dostarczyli do szpitala w Starachowicach respiratory. Do żołnierzy, którzy od kilku dni wspierali służby na granicach, dołączyli żołnierze 8 Koszalińskiego Pułku Przeciwlotniczego. Wspólnie z funkcjonariuszami Straży Granicznej 60 żołnierzy patrolowało granicę w Świnoujściu;

13 https://www.gov.pl/web/obrona-narodowa/mon-i-wojsko-zaangazowane-w-dzialania-zwiazane-z-zagrozeniem-koronawirusem/. 1.05.2020.

• 18 marca – pracę rozpoczęło mobilne laboratorium rozpoznania biologicznego;

• 19 marca – około 1500 żołnierzy wspierało funkcjonariuszy Straży Granicznej i Policji w ochronie granicy. Zorganizowano pierwsze akcje honorowego krwiodawstwa wśród żołnierzy. Żołnierze 15 Batalionu Saperów rozbudowali zabezpieczenia na granicy polsko-litewskiej. Żołnierze 6 Brygady Powietrznodesantowej razem z żołnierzami 5 Pułku Chemicznego rozwinęli w Gliwicach punkt dekontaminacyjny;

• 28 marca – żołnierze z Grupy Zabezpieczenia Medycznego 10 Brygady Logistycznej rozpoczęli współpracę z Opolskim Centrum Ratownictwa Medycznego;

• 30 marca – na wniosek wojewody śląskiego żołnierze 13 Śląskiej Brygady OT zaczęli wspierać Dom Pomocy Społecznej w Koszęcinie, ewakuując część pacjentów do szpitali. Po zakończonej ewakuacji personelu żołnierze 5 Pułku Chemicznego zdezynfekowali budynek;

• 2 i 3 kwietnia – żołnierze brygad logistycznych przetransportowali z magazynów 1,2 mln maseczek chirurgicznych oraz 9,5 tys. l płynów do dezynfekcji. Materiały zostały dostarczone do 105 szpitali na terenie kraju. Żołnierze 12 Wielkopolskiej Brygady Obrony Terytorialnej zakończyli budowę w Wolicy tymczasowej izby przyjęć dla Wojewódzkiego Specjalistycznego ZZOZ Chorób Płuc i Gruźlicy;

• 4 kwietnia – żołnierze z 1 Brygady Logistycznej dostarczyli maseczki i płyny do dezynfekcji do 49 placówek medycznych w kraju. 21 żołnierzy z 4 Pułku Chemicznego przeprowadziło dezynfekcję szpitala w Wołominie;

• 8 kwietnia – żołnierze brygad logistycznych przetransportowali z magazynów Agencji Rezerw Materiałowych do szpitali w Warszawie, Łańcucie, Starachowicach, Poznaniu i Wrocławiu 37 respiratorów i 54 kardiomonitorów. Żołnierze z 4 Pułku Chemicznego przeprowadzili dezynfekcję pomieszczeń w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Płońsku;

• 12 kwietnia – w odpowiedzi na nowe zachorowania i braki personelu żołnierze 9 Łódzkiej Brygady OT zostali skierowani do bezpośredniej opieki nad pensjonariuszami w Domu Pomocy Społecznej w Drzewnicy koło Opoczna;

• 18 kwietnia – przeprowadzono ewakuację zakażonych pensjonariuszy Domu Pomocy społecznej w Kaliszu. W czynnościach tych uczestniczyło 43 żołnierzy z: 12 Wielkopolskiej Brygady OT, 2 Wojskowego Szpitala Polowego z Wrocławia, 6 Batalionu Chemicznego Sił Powietrznych oraz podchorążowie AWL. Z kolei żołnierze WOT wybudowali kontenerową izbę przyjęć w Szpitalu Wojewódzkim w Poznaniu;

• 21 kwietnia żołnierze z 6 Batalionu Chemicznego przeprowadzili dezynfekcję w Domu Pomocy Społecznej „Polanki" w Gdańsku;

• 22 kwietnia – do Słowenii udali się lekarze z Wojskowego Instytutu Medycznego w celu wymiany wiedzy i doświadczeń w zakresie sposobów i warunków udzielania pomocy ofiarom epidemii SARS-CoV-2 oraz dzielenia się wypracowanymi wzorcami. Pielęgniarki, ratownicy medyczni i kierowcy sanitarek z Grupy Zabezpieczenia Medycznego 10 Brygady Logistycznej przeszli szkolenie specjalistyczne w Opolskim Centrum Ratownictwa Medycznego. Miało ono przygotować żołnierzy do pracy w ramach systemu ratunkowego. Przeszkoleni żołnierze, jeśli zajdzie taka potrzeba, będą wsparciem dla Opolskiego Centrum Ratownictwa Medycznego w czasie np. ewakuacji placówek medycznych lub natychmiastowej relokacji dużej liczby pacjentów;

• 23 kwietnia – 80 żołnierzy przeprowadziło ewakuację pensjonariuszy Domu Opieki Długoterminowej w Kaliszu. Zostali oni przetransportowani do szpitala jednoimiennego w Wolicy koło Kalisza. Również w tym dniu do USA udali się lekarze z Wojskowego Instytutu Medycznego w celu wymiany doświadczeń, prezentacji dobrych praktyk i zintensyfikowania współpracy w dziedzinie doskonalenia sposobów organizacji systemu ochrony zdrowia w walce z epidemią koronawirusa, a także polskich i europejskich osiągnięć w leczeniu chorych z COVID-19;

• 26 kwietnia – żołnierze z 7 Pomorskiej Brygady Obrony Terytorialnej, 3 Flotylli Okrętów oraz 7 Szpitala Marynarki Wojennej wyewakuowali około 70 pensjonariuszy i opiekunów z Domu Seniora w Koleczkowie w województwie pomorskim;

• 30 kwietnia – w Krotoszynie powstał pierwszy wojskowy punkt pobierania wymazów.

Wymienione przedsięwzięcia ilustrują sposób oraz charakter wsparcia sił zbrojnych w sytuacjach kryzysowych. Warto również dodać, iż w walkę z epidemią koronawirusa zaangażowano blisko 10 tys. żołnierzy i pracowników wojska, a także blisko 15 tys. jednostek sprzętu.

WNIOSKI

Przydatność jednostek wojskowych jest ściśle związana z zasadniczą funkcją państwa, która sprowadza się do zapewnienia bezpieczeństwa obywatelom. Koniecznością stają się przedsięwzięcia organizacyjne skierowane na zapobieganie i minimalizowanie skutków wszelkich zagrożeń. Zagrożenia spowodowane siłami natury oraz działalnością człowieka w określonych okolicznościach stanowią ryzyko inicjacji sytuacji kryzysowych, a podejmowane działania w ich obliczu bardzo często odbiegają od tych podejmowanych przez podmioty wykonawcze w systemie bezpieczeństwa narodowego. Siły zbrojne są skutecznym środkiem pozostającym w ciągłej gotowości do sprawnego działania w czasie pokoju, kryzysu oraz wojny. Cecha ta wyraża się gotowością do podejmowania działań skierowanych do wsparcia władz cywilnych i społeczeństwa w obliczu sytuacji kryzysowych. ■

Militarne znaczenie **Podlasia**

SWOBODA DOSTĘPU DO TERYTORIÓW PAŃSTW BAŁTYCKICH JEST ISTOTNA DLA POWODZENIA OPERACJI OBRONNEJ PROWADZONEJ PRZEZ SIŁY NATO.

mjr dypl. SZRP Marcin Wawro

Autor jest zastępcą dowódcy – szefem sztabu batalionu czołgów w 19 Brygadzie Zmechanizowanej.

Sojusz Północnoatlantycki stanowi dzisiaj najważniejszy element bezpieczeństwa międzynarodowego w Europie. Z kolei państwem, które uzurpuje sobie prawo do ustalania porządku w Europie, w szczególności w Europie Wschodniej i Środkowej, jest Federacja Rosyjska. Relacje FR z NATO odgrywają ważną rolę w europejskiej i globalnej polityce bezpieczeństwa. Stosunki obu podmiotów od początku cechowały wzajemna nieufność, narastające sprzeczności, zmiany w podejmowanych decyzjach. Były one i są nadal trudne ze względu na odmienne postrzeganie podstawowych aspektów kwestii bezpieczeństwa w Europie i na świecie. Obecnie relacje NATO – Federacja Rosyjska zostały ograniczone z powodu aneksji Krymu. Współczesne zagrożenia absorbujące uwagę europejskich polityków powodują coraz większy rozdźwięk między Federacją Rosyjską i państwami Sojuszu Północnoatlantyckiego. Rozmach ćwiczeń militarnych sił zbrojnych Rosji skłania do ostrożności, gdyż mogą one przeobrazić się w nieprzewidywalny bieg zdarzeń, których efektem będzie konflikt zbrojny wymierzony w państwa bałtyckie oraz w nasz kraj. Jednym z jego obszarów, który w pierwszej kolejności może odczuć skutki takiego scenariusza wydarzeń, jest Podlasie. Dodatkowo oddziela ono Białoruś od obwodu kaliningradzkiego, w którym zgromadzony potencjał militarny może być użyty w przewidywanych działaniach.

CHARAKTERYSTYKA

Podlasie to część geograficzna naszego kraju i jednocześnie część województwa podlaskiego. Region ten jest położony wzdłuż Niziny Podlaskiej oraz polskiej części Pojezierza Litewskiego. Sąsiaduje z Pojezierzem Mazurskim oraz Niziną Północnomazowiecką i Południowopodlaską. Krajobraz jest urozmaicony, ukształtowany na północy w wyniku zlodowacenia bałtyckiego, na pozostałym obszarze podczas zlodowacenia środkowopolskiego. Najwyższe wzniesienia występują na północy, gdzie dominuje krajobraz pagórkowaty pojezierny. Na terenie województwa leżą fragmenty pierwotnej Puszczy Białowieskiej oraz unikatowe bagna w dolinie Biebrzy i rozlewisk Narwi. W rozległych lasach i puszczach (Puszcze Białowieska, Augustowska, Knyszyńska, Zielona) można spotkać bogactwo unikatowej fauny i flory. Niektóre z nich, jako jedyne w Europie, zachowały swój pierwotny charakter.

POTYCZKI I BOJE

Podlasie ma również bogatą historię militarnych zmagań nie tylko wojska polskiego, lecz także największych mocarstw Europy w czasach epoki napoleońskiej oraz podczas I i II wojny światowej.

Z punktu widzenia rodzimej historii wojskowości teren ten był świadkiem walk partyzanckich w okresie powstania styczniowego w1863 roku, którego największym epizodem był bój pod Siemiatyczami. Stoczona w dniach 6–7 lutego 1863 roku bitwa między wojskami carskimi i oddziałami powstańców zakończyła się zwycięstwem wojsk rosyjskich. Jednym z głównych powodów porażki był brak współdziałania między polskimi dowódcami. Po porażce

Podlasie jest obszarem ważnym dla NATO oraz bezpieczeństwa naszego kraju. Można przypuszczać, że w przypadku potencjalnego konfliktu zbrojnego będzie odgrywało kluczową rolę w dopływie kolejnych sił NATO do państw bałtyckich przez przesmyk suwalski.

TOMASZ NIEZIEŁSKI/PKP PLK

część oddziałów powstańczych powróciła do Królestwa Polskiego, część do Puszczy Białowieskiej. W bitwie poległo 200 powstańców oraz 70 Rosjan.

Przez Podlasie maszerowała również armia napoleońska podczas kampanii przeciwko Rosji w 1812 roku. Wojska generała Reymera przemieszczały się przez Puszczę Knyszyńską. Ich trasa stanowi dzisiaj tzw. szlak napoleoński i jest atrakcją turystyczną.

Podlasie było teatrem działań również w I wojnie światowej. W jego północnej części przebiegał front wschodni. Na terenach Suwalszczyzny i Podlasia setki tysięcy żołnierzy toczyły walki niemniej zacięte i krwawe niż na froncie zachodnim. Na początku 1915 roku dowództwo niemieckie zdecydowało się na wykonanie uderzenia, którego celem było przełamanie frontu we wschodniej części Pojezierza Mazurskiego. Miało ono stworzyć zagrożenie dla rosyjskich linii komunikacyjnych i w konsekwencji doprowadzić do wycofania się armii rosyjskiej z terenów Królestwa Polskiego. Przeciwnikiem niemieckiej 12 Armii była rosyjska 2 Armia dowodzona przez Władimira Smirnowa. W sierpniu 1915 roku Niemcy zajęli Białystok, Grodno i Bielsk, a załamanie się obrony rosyjskiej umożliwiło im także zajęcie twierdzy brzeskiej. Ponadto miała tutaj miejsce tzw. bitwa białostocka stoczona 22 sierpnia 1920 roku w czasie wojny polsko-bolszewickiej między 1 Pułkiem Piechoty Legionów i wycofującymi się spod Warszawy oddziałami 16 i 3 Armii RFSRR.

To również obszar, na którym walczyły oddziały polskie w czasie wojny obronnej 1939 roku. Bój pod Zambrowem, który stoczyła z wojskami niemieckimi 18 Dywizja Piechoty wchodząca w skład SGO „Narew", jest tego najlepszym przykładem.

WSPÓŁCZEŚNIE

Podlasie jest obszarem ważnym dla NATO oraz bezpieczeństwa naszego kraju. Można przypuszczać, że w przypadku potencjalnego konfliktu zbrojnego będzie odgrywało kluczową rolę w dopływie kolejnych sił NATO do państw bałtyckich przez przesmyk suwalski. *Działania na obszarze przesmyku suwalskiego będą zatem zapewne miały charakter operacji osłonowej dla natarcia na terytoriach Estonii i Łotwy (podobnie jak działania zbrojne we wschodniej Ukrainie miały kluczowe znaczenie dla powodzenia całkowitego opanowania Krymu). Cel osłony to nie tylko odcięcie od pomocy. Istotą operacji będzie sprowokowanie konfliktu, którego zakończenie Moskwa obłoży warunkiem zaakceptowania rosyjskich zdobyczy w państwach bałtyckich… Skuteczne odcięcie republik bałtyckich od lądowego łącznika z NATO oznaczałoby porażkę Sojuszu i prawdopodobnie brak możliwości odtworzenia status quo ante. Wynik dla NATO byłby jednoznaczny – Sojusz nie jest w stanie zapewnić skutecznej obrony swym członkom*[1]. Dodatkowo należy zaznaczyć, że w przypadku utraty przesmyku suwalskiego państwa bałtyckie zostaną pozbawione wsparcia NATO. ■

1 L. Kościuk, *Jakoś to nie będzie*, „Niezależny Magazyn Strategiczny PARA BELLUM" 2015 nr 3, s. 12.

Warunki atmosferyczne i teren a relacje łączności radiowej

UMIEJĘTNOŚĆ WŁAŚCIWEGO WYKORZYSTANIA SIŁ I ŚRODKÓW ŁĄCZNOŚCI NA POLU WALKI POWINNA DOTYCZYĆ NIE TYLKO ŻOŁNIERZY KORPUSU WOJSK ŁĄCZNOŚCI I INFORMATYKI.

mjr dypl. SZRP Kamil Organista

Autor jest zastępcą dowódcy – szefem sztabu Batalionu Dowodzenia w 1 Brygadzie Pancernej.

Coraz szybszy rozwój środków walki powoduje powstawanie nowej rzeczywistości, którą G.R. Sullivan i J.M. Dubik w swoim opracowaniu *Land Warfare in the 21st Century* określili *wojskowo-technologiczną rewolucją*[1]. Doświadczenia historyczne, a także wnioski z wojen i konfliktów zbrojnych wskazują, że skuteczna obrona przed siłami przeciwnika, szczególnie w przypadku jego dużej przewagi, będzie możliwa tylko wtedy, gdy zostaną wykorzystane atuty obronne własnego terytorium. Jednymi z nich są warunki terenowe i atmosferyczne. Znaczenie środowiska walki dostrzegł już Sun Tzu, który w swoim dziele *Sztuka wojny* napisał: *Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite*[2]. Znajomość i wykorzystanie terenu jest jednym z zasadniczych atutów w rękach każdego dowódcy, czego potwierdzeniem są przykłady z historii wojen. Bolesław Chocha stwierdził: *Każda rozsądna decyzja taktyczna musi być poparta argumentem terenowym. Każde inne podejście do zagadnienia jest błędne i przynosi szkodę szkoleniu bojowemu wojsk*[3]. Jednak kontrowersje budzi rola i znaczenie środowiska walki przy coraz szybszym tempie rozwoju możliwości taktycznych sprzętu łączności.

ZASADY OGÓLNE

Warunki terenowe naszego kraju mają urozmaicony charakter. W związku z ich dużą różnorodnością związki taktyczne i oddziały (pododdziały), przechodząc do obrony w określonych pasach (rejonach) odpowiedzialności, będą prowadzić walkę w różnych warunkach (terenie). Dlatego też każdy dowódca oraz

1 G.R. Sullivan, J.M. Dubik, *Land Warfare in the 21st Century*, Carlisle Barracks, Pensylwania, US Army War College, 1993, s. 12.
2 Sun Tzu, *Sztuka wojny*, Warszawa 1994, s. 116.
3 B. Chocha, *Rozważania o taktyce*, MON, Warszawa 1982, s. 37.

Główną przeszkodą w codziennym wykorzystywaniu łączności satelitarnej są wysokie koszty usług satelitarnych w porównaniu z kosztami systemów naziemnych.

1.

RAFAŁ MNIEDŁO/11 LDKPANC

oficerowie sztabu muszą opanować umiejętność prawidłowej oceny terenu i jego wpływu na możliwość wykonania otrzymanego zadania. Dotyczy to także analizy warunków prowadzenia działań przez żołnierzy wojsk łączności i informatyki.

W myśl zapisów regulaminowych[4] są organizowane dla wojsk lądowych SZRP z wykorzystaniem dostępnych zakresów częstotliwości radiostacji dwa podstawowe rodzaje sieci radiowej pola walki[5]:

• *sieci radiowe UKF* – przeznaczone do wymiany informacji fonicznych; zakres częstotliwości: 30–87 MHz, zasięg 8–40 km, rodzaj pracy: fonia/dane (modulacja typu FM), moc wyjściowa nadajnika radiostacji: 8–35 W[6];

• *sieci radiowe KF* – zapewniające łączność w odległości przekraczającej zasięg środków UKF na wymaganych trzech poziomach:

– bliski zasięg (22 mile*)* – do 35 km;

– średni zasięg (31 mil) – poziom brygady (35–50 km), niski poziom mocy wyjściowej toru nadawczego (20 W PEP – Peak Evelope Power);

– daleki zasięg (31–186 mil) – poziom dywizji (50–300 km), średni poziom mocy wyjściowej toru nadawczego (150–400 W PEP)[7].

W zależności od sposobu przejścia wojsk do obrony, stopnia rozbudowy sieci łączności oraz stanu łączności radioliniowo-przewodowej środki radiowe są używane w różny sposób. Ze względu na promieniowanie elektromagnetyczne aktywność środków radiowych powinna być ograniczona podczas walki obronnej.

W natarciu natomiast mogą być stosowane bez ograniczeń. Ten rodzaj środków łączności stanowi często jedyną możliwość szybkiej wymiany informacji w czasie działań manewrowych. W rejonach wyjściowych, alarmowych i ześrodkowania obowiązuje zakaz używania środków radiowych na nadawanie. Dopuszcza się możliwość przejścia na nadawanie tylko w wyjątkowych sytuacjach do przekazywania sygnałów alarmowych, na przykład gdy przeciwnik dokonał zmasowanych uderzeń lotnictwa lub użył broni masowego rażenia. W czasie marszu również obowiązuje zakaz stosowania środków radiowych na nadawanie. Jedynie przekazywanie sygnałów dowodzenia w wydzielonych sieciach radiowych UKF oraz w sytuacjach szczególnych w sieciach radiowych KF jest dopuszczalne.

Łączność satelitarna ze względu na globalny zasięg oraz krótki czas instalowania sprzętu ma powszechne zastosowanie w wojskowych systemach łączności na całym świecie. Wojskowe terminale satelitarne wielokrotnie sprawdziły się w pracy w różnych warunkach terenowych, zapewniając łączność i dostępność sieci w ponad 99,7%, niezależnie od istniejącej w danym rejonie infrastruktury telekomunikacyjnej. Środków satelitarnych, takich jak środki radiowe, używa się w zależności od sposobu przejścia wojsk do obrony oraz stopnia rozbudowy i aktualnego stanu łączności radioliniowo-przewodowej. Podczas prowadzenia obrony oraz w rejonach wyjściowych, alarmowych i ześrodkowania środki te stanowią medium transmisyjne dla podsystemów wspomagających proces dowodzenia i kierowania wojskami. W natarciu i w czasie marszu ze względu na duże wymiary terminali satelitarnych wykorzystuje się telefony satelitarne.

W regulaminie działań wojsk lądowych specyficzne środowisko określono jako *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*[8].

Do specyficznych środowisk walki zalicza się: lasy i obszary lesisto-jeziorne, teren górzysty, teren zabudowany (zurbanizowany), wybrzeże morskie oraz przeszkody wodne. Natomiast specyficzne warunki to okres zimy oraz ograniczonej widoczności.

TEREN LESISTY I LESISTO-JEZIORNY

Podczas organizowania łączności w terenie lesistym (lesisto-jeziornym – 29,6% powierzchni naszego kraju)[9] należy zwrócić szczególną uwagę na:

– wybór rejonów rozmieszczenia węzłów łączności oraz samodzielnych grup środków łączności;

– znaczne zmniejszenie zasięgu radiostacji;

– zwiększenie odległości między stanowiskami dowodzenia;

– wzrost niebezpieczeństwa oddziaływania grup dywersyjno-rozpoznawczych przeciwnika na elementy łączności, zwłaszcza na węzły łączności, grupy środków radiowych oraz pojedyncze samodzielnie działające środki radiowe.

Jednym z warunków zapewnienia ciągłej i niezawodnej łączności z przełożonym i podwładnymi jest właściwe rozmieszczenie stanowisk dowodzenia i węzłów łączności. Las o dużej liczbie dróg, polan i przesiek stwarza dogodne warunki do rozmieszczenia środków łączności i jej zapewnienia. W lasach pozbawionych tych elementów lub o ograniczonej liczbie ich występowania utrudnione jest rozwijanie środków i urządzeń łączności, w tym głównie urządzeń antenowych.

Przyjmuje się, *że jednolity masyw leśny zmniejsza zasięg radiostacji pracujących w zakresie 20–50 MHz*

4 *Regulamin działań wojsk lądowych*, sygn. DWLąd wewn. 115/2008, Warszawa 2008, s. 293–306.

5 M. Frączek, *Teleinformatyczne środki dowodzenia*, AON, Warszawa 2012, s. 15.

6 P. Daniluk, *Sieci radiowe pola walki*, AON, Warszawa 2001, s. 18.

7 Ibidem, s. 20.

8 Ibidem, s. 173.

9 Według danych Głównego Urzędu Statystycznego z grudnia 2017 roku, https://www.lasy.gov.pl/pl/nasze-lasy/polskie-lasy/. 12.12.2019.

TABELA 1. SPOSOBY ROZMIESZCZENIA ŚRODKÓW RADIOWYCH W TERENIE LESISTYM

Sposób rozmieszczenia	Wpływ terenu
Na skraju lasu	niekorzystny: łączność niestabilna, należy poszukiwać miejsc najlepszego odbioru sygnałów korespondenta
W głębi lasu	korzystny: łączność jest stabilna, zasięg maleje
Jedna radiostacja w gęstym lesie, druga w terenie otwartym	korzystny: łączność stabilna, zasięg zmaleje od 1,5 raza do 2 razy
Na skraju lasu, grupy drzew i krzewów	niekorzystny: łączność może być niestabilna, należy wykorzystać tzw. wysepki dobrego odbioru
W gęstym wilgotnym, zwłaszcza liściastym lesie	niekorzystny: zasięg łączności może zmniejszyć się 3–4-krotnie w porównaniu z terenem otwartym

Opracowano na podstawie: J. Janczak, *Właściwości organizacji łączności w specyficznych środowiskach i warunkach walki*, Warszawa 2003.

około 2–3-krotnie, a w zakresie 50–88 MHz około 3–4-krotnie[10].

Największy ujemny wpływ na zapewnienie łączności radiowej wywiera rozmieszczenie środków radiowych na polanach lub skraju lasu, ponieważ następuje tam rozproszenie fal, a także występuje dodatkowe tłumienie oraz złożona struktura pola, w wyniku czego natężenie pola elektromagnetycznego ulega znacznym i nagłym zmianom w obrębie kilku metrów. Rozmieszczając środki radiowe, należy dążyć do tego, by znajdowały się one poza granicami lasu. Dla zakresu częstotliwości 20–50 MHz pożądana odległość to 500 m, dla wyższych częstotliwości odległości powinny być większe. Decydujący wpływ poszycia lasu obserwuje się wówczas, gdy korespondujące ze sobą radiostacje umieści się na skraju lasu lub w jego głębi. Należy zatem mieć na uwadze zmniejszenie zasięgu działania środków radiowych pracujących w zakresie fal UKF. Występuje także znaczne osłabienie natężenia pola elektromagnetycznego (do 2,5 raza) przy bardzo wilgotnym podłożu gruntu, przede wszystkim podczas opadów mokrego śniegu lub deszczu.

Lasy liściaste w większym stopniu wpływają negatywnie na rozprzestrzenianie się fal UKF niż lasy iglaste. Stąd też rozmieszczanie środków radiowych w gęstym i wysokim lesie (liściastym) może znacznie ograniczyć zasięg łączności. Jeśli jedna z korespondujących radiostacji UKF znajduje się w gęstym lesie, inna zaś w terenie otwartym, to zasięg w kierunku łączności może się zmniejszyć 1,5–2-krotnie.

W przypadku obfitego deszczu, wiosennych roztopów oraz jesiennego nawilgocenia drzew, gruntu i poszycia leśnego lub rozmieszczenia dwóch korespondujących ze sobą radiostacji w gęstym lesie liściastym następuje dalsze pogorszenie warunków propagacyjnych oraz – co się z tym wiąże – zasięg łączności radiowej może zmniejszyć się nawet czterokrotnie w porównaniu z otwartym terenem. Jeśli środki radiowe, zwłaszcza UKF, rozmieści się na niewielkich polanach, na skraju lasu, w rzadkim lesie lub w grupach drzew i krzewów, to zapewnienie łączności również będzie utrudnione. Na skutek zjawisk interferencji[11] i wielokrotnego odbijania się fal elektromagnetycznych od poszczególnych drzew powstają tzw. wysepki dobrego odbioru korespondenta[12]. W tym celu należy przemieszczać wozy dowodzenia (radiostacje przenośne) co kilka metrów w różnych kierunkach dla uzyskania poprawy warunków odbioru (tab. 1).

Ze względu na rozśrodkowanie elementów ugrupowania, szczególnie na niższych szczeblach organizacyjnych, zostaną zwiększone odległości między stanowiskami dowodzenia i węzłami łączności, co przy zmniejszeniu zasięgu środków radiowych utrudnia lub uniemożliwia utrzymanie bezpośredniej łączności. W takiej sytuacji, w zależności od możliwości i potrzeb, należy rozwijać mobilną grupę dowodzenia (MGD), a na niższych szczeblach dowodzenia – punkty dowódczo-obserwacyjne (PDO). W przypadku łączności satelitarnej zalesienie terenu nie ma wpływu na przesyłany sygnał. Zatem potrzeby dotyczące zapewnienia łączności w terenie lesistym (lesisto-jeziornym) są uzależnione od roli i miejsca pododdziału w ugrupowaniu bojowym wyższego szczebla organizacyjnego oraz utworzonego systemu dowodzenia, sposoby zaś organizacji łączności dyktują warunki terenowe i możliwości taktyczno-techniczne sprzętu oraz zdolności ogniowego i radioelektronicznego oddziaływania przeciwnika na system łączności. Należy stwierdzić, że

10 J. Janczak, M. Marczyk, *Organizacja systemu łączności i informatyki wojsk obrony terytorialnej*, ASzWoj, Warszawa 2018, s. 47.

11 Interferencja fal – fizyczne zjawisko nakładania się (superpozycji) dwóch lub więcej fal, w przypadku którego w różnych punktach przestrzeni następuje wzmacnianie (interferencja konstruktywna) lub osłabianie (interferencja destruktywna) amplitudy fali wypadkowej; https://encyklopedia.pwn.pl/haslo/interferencja-fal;3915082.html/. 12.12.2019, https://encyklopedia.pwn.pl/haslo/interferencja-fal;3915082.html/. 3.10.2019.

12 J. Janczak, M. Marczyk, *Organizacja systemu łączności i informatyki*..., op.cit., s. 48.

TABELA 2. ROZMIESZCZANIE ŚRODKÓW RADIOWYCH W TERENIE GÓRZYSTYM

Sposób rozmieszczenia	Wpływ terenu	
Teren średnio urozmaicony	korzystny	– na wierzchołkach wzniesień i na zboczach od strony korespondentów
	niekorzystny	– u podnóża wzniesień po przeciwnej stronie w stosunku do korespondentów
Wąwozy, okopy	korzystny	– jak najbliżej górnej krawędzi, aby antena była widoczna nad krawędzią (anteny kierunkowe); – w głębokim wąwozie możliwie wysoko i na przeciwległym zboczu do korespondenta
	niekorzystny	– na zboczu wąwozu od strony korespondenta; – na dnie wąwozu

Opracowano na podstawie: J. Janczak, *Właściwości organizacji łączności w specyficznych środowiskach i warunkach walki*, Warszawa 2003.

w tych warunkach zwiększają się potrzeby łączności, w tym współdziałania, co wynika głównie z organizowania dodatkowych elementów ugrupowania bojowego oraz innego ich składu i sposobów działania. Zaspokojenie związanych z tym potrzeb wymaga zmian lub uzupełnienia planów łączności (nowe relacje łączności, skład sieci radiowych), a ich realizacja może być utrudniona.

TEREN GÓRZYSTY

Dużą część południowej powierzchni naszego kraju zajmują pasma górskie (Góry Świętokrzyskie, Sudety, Karpaty – 3,3% powierzchni RP)[13] oraz zwarte masywy górskie. Masywy w zależności od położenia geograficznego i okresu powstania różnią się właściwościami. Na dowodzenie w takich warunkach mają wpływ następujące czynniki:

– konieczność prowadzenia działań bojowych na kilku kierunkach, w wielu przypadkach samodzielnie, oddzielonych od siebie oraz niejednokrotnie na dużych obszarach (dotyczy to działań obronnych);

– wymóg uwzględnienia w planowaniu dodatkowych przedsięwzięć wynikających ze specyfiki działań;

– tworzenie swoistych zgrupowań uderzeniowych, wydzielanie silnych odwodów i odwodów specjalnych, a także oddziałów obejścia;

– ograniczone możliwości wykorzystania w poszczególnych etapach walki niektórych rodzajów wojsk i środków bojowych;

– mała liczba dróg i trudności w poruszaniu się po nich;

– ograniczony zasięg obserwacji pola walki;

– decentralizacja użycia niektórych rodzajów wojsk (inżynieryjnych, artylerii);

– trudności w uzyskiwaniu planowanego tempa oraz w utrzymaniu ciągłości działań w szybko zmieniających się warunkach meteorologicznych;

– problemy z wyborem odpowiednich miejsc na rozmieszczenie stanowisk dowodzenia oraz z przemieszczaniem ich do kolejnych rejonów działania[14].

Działania bojowe prowadzone w terenie górzystym wymagają wykonania przez siły łączności złożonych zadań w niekorzystnych warunkach. Ich realizacja wiąże się ze zorganizowaniem dodatkowych relacji łączności, co wynika ze znacznie większej liczby elementów ugrupowania bojowego. Uzasadnione jest użycie uzupełniających elementów systemu łączności, które nie występują na szczeblu taktycznym, na przykład zaplanowanie pomocniczych węzłów łączności. Posiadanie niezbędnego i odpowiednio rozmieszczonego odwodu sił i środków umożliwia dokonanie manewru nimi na odpowiednie kierunki. Elementy ugrupowania bojowego działające samodzielnie w znacznym oddaleniu od sił głównych muszą być wyposażone w koniecznie potrzebne techniczne środki łączności (typu przenośnego), źródła zasilania oraz części zamienne do urządzeń łączności.

Do czynników wpływających na realizację zadań łączności w terenie górzystym można zaliczyć:

– ekranizujące oddziaływanie gór na rozprzestrzenianie się fal elektromagnetycznych, szczególnie zakresu UKF, a także liczne zakłócenia atmosferyczne występujące powyżej 2000 m n.p.m.;

– specyficzny układ i zmieniający się czas trwania poszczególnych pór roku;

– zmienność warunków atmosferycznych, w tym różnice ciśnienia i temperatury powietrza oraz zawartości w nim pary wodnej;

– dużą liczbę wąwozów, stromych i urwistych stoków, niewielką liczbę dróg ograniczających w znacznym stopniu ruch i manewr;

– powstawanie zawał, lawin śnieżnych lub skalnych;

– występowanie zastojów par środków trujących w dolinach i wąwozach;

– utrudnioną rozbudowę fortyfikacyjną.

13 https://www.gdos.gov.pl/polska-w-liczbach/. 12.12.2019.

14 J. Janczak, M. Marczyk, *Organizacja systemu łączności i informatyki*..., op.cit., s. 50.

Natomiast na realizację zadań łączności w górach w zimie ujemnie wpływają: niska temperatura, pokrywa śnieżna oraz zamiecie i zawieje śnieżne.

Czynniki te wynikające ze specyfiki terenu górzystego mają negatywny wpływ zarówno na funkcjonowanie załóg, jak i środków łączności.

Na pracę załóg w czasie prowadzenia działań bojowych w terenie górzystym największy wpływ mają:

– pokrywa śnieżna,

– trudności z orientacją w terenie,

– różnice temperatury i ciśnienia atmosferycznego.

Góry mają ujemny wpływ na możliwość zapewnienia łączności radiowej zarówno w zakresie UKF, jak i KF. Znajomość zasad rozprzestrzeniania się fal elektromagnetycznych oraz możliwości praktycznego ich wykorzystania pozwalają na znaczne zwiększenie zasięgu łączności. Jeśli na trasie radiowej występują niewielkie pagórki o wysokości porównywalnej z długością fali, to mogą wystąpić znaczne zmiany w natężeniu pola elektromagnetycznego.

W takich sytuacjach mogą pojawić się obszary (rejony), w których natężenie pola elektromagnetycznego może być dostatecznie silne lub bardzo słabe, co uniemożliwi nawiązanie i zapewnienie łączności.

W przypadku gdy na drodze rozprzestrzeniania się fal radiowych występuje wysoka przeszkoda terenowa, wówczas znacznie zmniejsza się za nią natężenie pola elektromagnetycznego. Zmniejszenie to (osłabienie fali) zależy od:

– wymiarów przeszkody oraz jej właściwości elektrycznych (im większa przeszkoda, tym większe osłabienie fali);

– jej kształtu (duże przeszkody w kształcie klina nie wpływają znacząco na pogorszenie propagacji; przeszkoda typu dwugarbnego znacznie osłabia fale radiowe);

– długości fali radiowej (w miarę zwiększania częstotliwości wzrasta osłabienie fali);

– kąta dyfrakcji[15] (im kąt dyfrakcji większy, tym większe jest osłabienie fali radiowej).

Czynnikiem mającym wpływ na jakość łączności radiowej w górach jest możliwość odbioru przez odbiornik, oprócz fali bezpośredniej, również fali odbitej od powierzchni Ziemi. Fala odbita, która dociera do odbiornika w przeciwfazie, może osłabiać natężenie indukowanego sygnału w obwodach wejściowych odbiornika. Różnica faz zależy od stosunku długości linii radiowych – zarówno bezpośredniej, jak i odbitej.

W działaniach bojowych, jeżeli zaplanowany kierunek radiowy nie zapewnia dobrej łączności, należy dokonać zmiany jednej z następujących wielkości: wysokości zawieszenia anteny nadawczej lub odbiorczej, odległości między pracującymi radiostacjami lub częstotliwości pracy w celu osiągnięcia lepszych wyników. Fale radiowe zakresu UKF i KF mają również charakterystyczne właściwości w trakcie rozchodzenia się w wąwozach i lesie. Jeśli węzły łączności zostaną rozmieszczone w wąwozach, jarach czy parowach, to zapewnienie stabilnej łączności wymagać będzie dokonania prawidłowej oceny ich wpływu na zmianę natężenia pola elektromagnetycznego.

Najlepsze warunki do uzyskania stabilnej łączności istnieją wówczas, gdy urządzenia łączności rozmieszcza się na przeciwstokach. Gorsze warunki są w wąwozach, natomiast najgorsze na stokach bliższych korespondentowi ze względu na występowanie cienia radiowego[16], który może powodować zmniejszenie zasięgu 2–3-krotnie (tab. 2).

Z przedstawionych właściwości rozprzestrzeniania się fal radiowych wynikają następujące wnioski:

• *Dla zakresu fal radiowych KF* wpływ terenu na rozprzestrzenianie się fal jest stosunkowo niewielki i przy odległościach rozmieszczenia środków radiowych na szczeblu taktycznym możliwe jest zapewnienie łączności zarówno na fali przyziemnej, jak i przestrzennej.

W celu uzyskania maksymalnych zasięgów łączności należy:

– wybierać na rozwinięcie radiostacji miejsca na obszarach o mokrej glebie*;*

– do pracy na fali przyziemnej wykorzystywać częstotliwości z początku podzakresów*;*

– dążyć do tego, aby przeszkody terenowe na trasie radiowej nie przekraczały wysokości 400 m;

– zapewniając łączność na fali odbitej na dużą odległość, stosować częstotliwości: w dzień 13–30 MHz, w nocy 3–8,5 MHz. Do zapewnienia łączności w czasie wschodu i zachodu słońca wybierać częstotliwości świtu (zmierzchu) 8,5–12 MHz;

– w celu uniknięcia strefy martwej korzystać z anteny promieniowania pionowego.

• *Dla zakresu fal radiowych UKF* w celu zapewnienia łączności w terenie górzystym należy:

– stosować dolną część zakresu UKF;

– radiostacje rozmieszczać na wierzchołkach gór lub na zboczach widocznych od strony korespondenta;

– rozmieszczając radiostacje w wąwozach, należy dążyć do umieszczania ich na zboczach widocznych od strony korespondenta;

– unikać rozmieszczania radiostacji na skraju lasu, wśród pojedynczych drzew i na polanach; w przypadku

15 Kąt zawarty między prostą poprowadzoną od radiostacji do wierzchołka przeszkody a prostą łączącą wierzchołek przeszkody z radiostacją korespondenta; https://pl.wikipedia.org/wiki/Dyfrakcja/. 12.12.2019.

16 *Cień radiowy (shadowing) – zjawisko występujące podczas propagacji fal radiowych, np. w sieciach radiokomunikacyjnych. Polega na stracie mocy sygnału wskutek rozprzestrzeniania wieloma drogami. Gdy pomiędzy nadajnikiem a odbiornikiem pojawia się przeszkoda (np. budynek, drzewo), wówczas fala elektromagnetyczna ulega odbiciom i ugięciom. W efekcie sygnał dociera do odbiornika po różnych drogach i z różnym opóźnieniem. Z uwagi na interferencję poszczególnych ścieżek sygnału, w przestrzeni pojawiają się miejsca, gdzie sygnał ten zanika i jest nie do odebrania*; https://pl.wikipedia.org /wiki/Cie%C5%84_radiowy/. 1.12.2019.

konieczności rozwinięcia radiostacji w takich warunkach, wyboru miejsca należy dokonać na podstawie pomiaru natężenia pola elektromagnetycznego;

– rozwijać radiostacje w gęstym lesie lub w terenie zakrzaczonym;

– wybierać trasy linii radiowych z przeszkodami, których wierzchołki mają jak najmniejszy promień krzywizny (wierzchołki bardziej ostre) i jednocześnie umożliwiają bezpośrednią widoczność wierzchołka z obu punków rozmieszczenia radiostacji;

– dążyć do uzyskania jak najmniejszych kątów dyfrakcji przez rozwijanie radiostacji oddalonych od przeszkody i na niewielkich wzniesieniach o wilgotnym gruncie; najbliższe możliwe rozmieszczenie radiostacji od podnóża przeszkody równe jest dwukrotnej długości przeszkody[17];

– używać anten o polaryzacji pionowej, podniesionych nad ziemią.

Podsumowując, należy stwierdzić, że sprawne zorganizowanie i funkcjonowanie systemu łączności w terenie górzystym musi być poprzedzone właściwym przygotowaniem ludzi i sprzętu do wykonywania zadań w tym specyficznym środowisku.

TEREN ZABUDOWANY

Na prowadzenie działań bojowych w tym terenie wywierają wpływ:

– ograniczone pole ostrzału i obserwacji;

– dobre warunki do organizowania ukrycia i maskowania sił i środków;

– niewielkie możliwości manewru wojsk;

– zwiększone zdolności przenikania i obejścia;

– występowanie ludności cywilnej.

Obok wysokiej i średniej wysokości zwartej zabudowy o konstrukcji żelbetowej i murowanej występuje tu zabudowa niska typu willowego, otoczona terenami zielonymi. Między miejscowościami są także obszary wolne od zabudowy. Rozmieszczenie budynków kanalizuje ruch wojsk i jednocześnie ułatwia organizację łączności.

Specyfiką terenu miejskiego są grupy zwartej zabudowy oddzielone obszarami luźnej, niskiej zabudowy lub pasami zieleni. Teren może być poprzecinany liniami komunikacyjnymi (kolejowymi i drogowymi). Ulice i drogowe arterie komunikacyjne w większości mają twardą nawierzchnię ułatwiającą komunikację i jednocześnie utrudniającą maskowanie kablowych linii łączności.

Z punktu widzenia zapewnienia łączności najbardziej niekorzystne są obszary o zwartej, wysokiej i średniej zabudowie oraz rejony przemysłowe. Szczególnie niekorzystne są budowle o konstrukcji metalowej i żelbetonowej oraz metalowe elewacje i pokrycia dachów, gdyż pochłaniają one energię fal elektromagnetycznych oraz powodują ich załamywanie i rozproszenie. W wyniku tych zjawisk powstają strefy tzw. cienia radiowego, którego następstwem jest znaczne ograniczenie zasięgu łączności radiowej i radiotelefonicznej. W tej sytuacji wybór odpowiednich rejonów rozwinięcia węzłów łączności czy środków łączności będzie miał szczególnie istotne znaczenie zarówno z punktu widzenia możliwości rozmieszczenia ich elementów, jak i zapewnienia łączności, zwłaszcza z użyciem środków radiowych i radioliniowych. Do miejsc zapewniających możliwości rozwijania węzłów łączności można zaliczyć skwery, place, parki lub zabudowę typu willowego. Przy wyborze rejonów należy brać pod uwagę wrażliwość węzłów łączności na ogniowe oddziaływanie przeciwnika. Teren zabudowany ułatwia przenikanie grup dywersyjno-rozpoznawczych w głąb ugrupowania wojsk własnych. Tym samym przeciwnik ma większe możliwości przechwytywania, jak również ogniowego oddziaływania na elementy węzłów łączności.

Przedstawione właściwości i uwarunkowania obligują do stosowania następujących rozwiązań organizacyjno-technicznych w zakresie łączności radiowej i radiotelefonicznej:

– organizowanie łączności w kierunkach radiowych;

– tworzenie podstawowych relacji łączności radiowej w zakresie KF (HF), który jest mniej wrażliwy na destrukcyjny wpływ właściwości terenu zabudowanego;

– przydzielanie częstotliwości roboczych dla relacji radiowych UKF (VHF) w dolnym paśmie zakresu;

– rozwijanie radiostacji doręcznych, plecakowych na dachach lub najwyższych kondygnacjach budynków;

– rozmieszczanie wozów dowodzenia i aparatowni z dala od budynków w stosunku do korespondentów, najlepiej na skwerach, w parkach lub w rejonach o niskiej zabudowie;

– unikanie rozmieszczania radiostacji wewnątrz lub w pobliżu dużych metalowych obiektów (hale fabryczne, wysokie budynki z metalowymi konstrukcjami lub metalową elewacją);

– stosowanie stałych punktów retransmisyjnych, rozmieszczając je na najwyższych piętrach budynków i innych budowli.

Po przeanalizowaniu wymienionych uwarunkowań należy stwierdzić, że obszary zabudowane nie sprzyjają organizacji łączności radiowej. Dlatego też znajomość ich specyfiki oraz wpływu na nią jest jednym z podstawowych warunków zapewnienia trwałej i ciągłej łączności walczącym pododdziałom, oddziałom i związkom taktycznym.

Rozwiązaniem mogą być systemy łączności radiowej, głównie HF, wykorzystujące promieniowanie pod odpowiednim kątem do jonosfery w dobrze dobranym zakresie częstotliwości roboczej opierającym się na propagacji fali typu NVIS *(near-vertical incidence skywave),* gdyż nie mają strefy martwej. Teren nie wpływa na zanik sygnału. Także poziom sygnału odbieranego nie zmienia się wraz z dystansem, dzięki czemu nie ma potrzeby wybierania rejonów do rozmieszczania środków radiowych. Zatem użytkowanie przez pododd-

17 J. Janczak, *Właściwości organizacji łączności w specyficznych środowiskach i warunkach walki*, Warszawa 2003, s. 63.

działy dowodzenia techniki propagacji wykorzystującej promieniowanie pionowe w zakresie fal krótkich (NVIS) staje się kluczowym sposobem uzyskania pewnej i niezawodnej łączności[18].

KIERUNKI ZMIAN

Wojska lądowe są zasadniczym rodzajem sił zbrojnych realizującym zadania w okresie pokoju, kryzysu i wojny. Jest to przyczynkiem do tego, aby w ich wyposażeniu znajdowały się nowoczesne środki teleinformatyczne, czyli radiostacje oraz wozy dowodzenia, dowódczo-sztabowe lub dowódczo-bojowe. Pełnią one dwie podstawowe funkcje, czyli:

– przekazywania informacji między elementami (osobami funkcyjnymi lub komórkami funkcjonalnymi) systemu dowodzenia;

– wspomagania przetwarzania informacji w procesie dowodzenia.

Dodatkowo wymaga się, by wozy dowodzenia zapewniały zdolność do kierowania środkami walki. Powinny również chronić obsługi oraz osoby funkcyjne przed skutkami rażenia ogniowego przeciwnika. W odniesieniu do oczekiwań systemu łączności wybrana platforma wozu dowodzenia powinna być wyposażona w nowoczesne technologie, które pozwalają na:

– projektowanie, konstruowanie i budowanie nowych środków zapewniających bezpieczeństwo obsług zgodnie z potrzebami;

– zautomatyzowanie procesów rozpoznania i dowodzenia, głównie przez analizę danych we wskazanych rejonach działań w czasie rzeczywistym i w każdych warunkach atmosferycznych;

– zwiększenie mobilności, a także skuteczności działania pododdziałów;

– zapewnienie szybkości oraz trwałości wymiany informacji między różnymi poziomami dowodzenia w trakcie wykonywania zadań;

– skrócenie czasu niezbędnego na podjęcie decyzji stosownie do potrzeb, co staje się warunkiem koniecznym do wykonania zadania, a tym samym właściwego użycia posiadanych sił i środków;

– w razie konieczności na prowadzenie walki (wozy dowódczo-bojowe – WDB).

Wojska lądowe powinny podjąć decyzje dotyczące wyboru dwóch lub większej liczby uniwersalnych platform kołowych oraz gąsienicowych, na których bazie zostaną zbudowane wozy dowodzenia wspierające pracę dowódców i ich sztabów. Konieczność transformacji w tej dziedzinie wynika z faktu, że stopniowo kończą się resursy techniczne eksploatowanych wozów dowodzenia na podwoziach UAZ, BWP-1, MTLB, ZWD-3. Ponadto firmy oferujące swoje produkty wycofują przestarzałe rozwiązania (generacje sprzętu) i nie prowadzą serwisu oraz sprzedaży części zamiennych. Wskazane czynniki i uwarunkowania stwarzają problemową sytuację oraz są podstawą do dalszych rozważań na ten temat. Należy również uwzględnić fakt, że nowoczesne środki łączności i informatyki zastępują urządzenia starszej generacji, a wzrost ich wydajności pozwala na zwiększenie zakresu usług.

Sieć teleinformatyczna pododdziałów wojsk lądowych powinna być siecią cyfrową zbudowaną z najnowszych urządzeń. System łączności musi być ujednolicony. Różnice w wyposażeniu i sposobie jego organizowania są powodem wielu dyskusji. Pożądanym trendem w rozwoju systemu jest sukcesywne dążenie do transformacji obecnej struktury sieci teleinformatycznej. Środki satelitarne w połączeniu z cyfrowymi radioliniami systemu MPCŁU Storczyk oraz radiostacjami UKF i KF (Harris, F@lcon, PR4G) nowej generacji umożliwiają budowę niezawodnych systemów łączności zapewniających wachlarz usług teleinformatycznych na poziomie taktycznym. Warto podkreślić, że zdecydowano się na szersze wykorzystanie systemów satelitarnych, zwłaszcza w czasie ćwiczeń i treningów oraz w operacjach wsparcia pokoju. Wciąż zwiększa się zapotrzebowanie na coraz większą mobilność, przepływność i bezpieczeństwo sieci teleinformatycznych, a także występuje wzrost zapotrzebowania na szerokość pasma w usługach transmisji danych zarówno w zakresie integrowania mobilnych i stacjonarnych sieci teleinformatycznych, jak i dostępu do internetu. Samodzielność działań poszczególnych zgrupowań, zwłaszcza w wymiarze sieciocentrycznym, powoduje, że zdolne są do operowania na każdym wskazanym obszarze, a poszczególni żołnierze mogą realizować zadania decydujące o ich powodzeniu.

Główną przeszkodą w codziennym wykorzystywaniu łączności satelitarnej są wysokie koszty usług satelitarnych w porównaniu z kosztami systemów naziemnych. Koszt systemu satelitarnego jest większy o około 50–70% od kosztów systemów naziemnych[19]. Innymi barierami ograniczającymi możliwości korzystania z łączności satelitarnej są m.in.: brak wystarczających szkoleń dla żołnierzy; brak doświadczenia w posługiwaniu się techniką satelitarną; problemy związane z pozyskaniem cyfrowych map terenu. Zdolność do zastosowania łączności satelitarnej do szybkiego i nieograniczonego zasięgiem przesyłu informacji kreuje poczucie przewagi informacyjnej, co tym samym zwiększa skuteczność prowadzonych operacji.

Spełnienie wymagań stawianych systemowi łączności wiąże się z koniecznością zapewnienia odpowiednio wysokiego poziomu wiarygodności i bezpieczeństwa przy jednoczesnym spełnieniu warunku dotyczącego szybkości wymiany informacji. Równie ważny jest odpowiedni poziom interoperacyjności narodowych systemów telekomunikacyjnych z systemami państw koalicyjnych. ■

18 W. Jabłoński, *Taktyczna łączność radiowa*, „Przegląd Sił Zbrojnych" 2020 nr 1, s. 108–113.

19 T. Wałek, *System łączności jako ważny element zarządzania kryzysowego*, „Kultura Bezpieczeństwa, Nauka – Praktyka – Refleksje" 2013 nr 14, s. 233.

Infrastruktura komunikacyjna wykorzystywana **przez siły zbrojne**

SZYBKOŚĆ PRZEMIESZCZANIA SIĘ KOLUMN MARSZOWYCH ODDZIAŁÓW I PODODDZIAŁÓW ZALEŻY OD STANU DRÓG ORAZ WŁAŚCIWEJ ORGANIZACJI SYSTEMÓW KOMUNIKACYJNYCH KRAJU ZAPEWNIAJĄCYCH SPRAWNE WYKONYWANIE ZADAŃ BOJOWYCH.

mgr Karol Romanowski

Autor jest samodzielnym referentem ds. łączności i informatyki w Sekcji Technicznej Oddziału Zabezpieczenia Dowództwa Garnizonu Warszawa.

W literaturze przedmiotu występuje pojęcie *infrastruktura transportowa.* Obejmuje ona sieci drogowe i kolejowe oraz żeglugi śródlądowej, autostrady morskie, porty żeglugi morskiej i śródlądowej, a także porty lotnicze. W potocznym ujęciu wymienione elementy są określane jako infrastruktura komunikacyjna. W *Słowniku języka polskiego* infrastruktura to *urządzenia i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki*[1]. Ponadto wyróżnia się podział na infrastrukturę ekonomiczną oraz infrastrukturę społeczną. Natomiast środki publicznego transportu zbiorowego dzieli się na transport kolejowy, samochodowy, lotniczy i rurociągowy oraz żeglugę śródlądową i morską.

PODSTAWY PRAWNE

Wyróżnia się trzy stany gotowości obronnej państwa, czyli: stałą gotowość obronną (czasu pokoju), gotowość obronną podczas kryzysu oraz gotowość obronną czasu wojny. W każdym z nich siły zbrojne wykorzystują elementy infrastruktury komunikacyjnej zgodnie ze swoimi potrzebami. Stanowi o tym ustawa z 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. W artykule szóstym stwierdzono, że Rada Ministrów wyznacza podmioty odpowiedzialne za warunki i sposób przygotowania oraz wykorzystania transportu morskiego, kolejowego, samochodowego, lotniczego i żeglugi śródlądowej oraz infrastruktury drogowej i kolejowej na potrzeby obronne państwa, a także ich ochrony w czasie wojny[2]. Z kolei zgodnie z rozporządzeniem Rady Ministrów z 3 lutego 2004 roku w sprawie warunków i sposobu przygotowania i wykorzystania transportu na potrzeby obronne państwa określono zakres obowiązków poszczególnych ministrów z tym związanych[3]. W paragrafie 23. określono zadania dotyczące przygotowania infrastruktury drogowej, które sprowadzają się do:

1 *Słownik języka polskiego*, https://sjp.pwn.pl/slowniki/infrastruktura/. 11.11.2020.

2 *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, Dz.U. 1967 nr 44 poz. 220.

3 *Rozporządzenie Rady Ministrów z dnia 3 lutego 2004 r. w sprawie warunków i sposobu przygotowania i wykorzystania transportu na potrzeby obronne państwa, a także jego ochrony w czasie wojny, oraz właściwości organów w tych sprawach*, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20040340294/. 12.11.2020.

Rozwój infrastruktury komunikacyjnej, która może służyć siłom zbrojnym, jest dość istotny, ponieważ wszelkie manewry oddziałami, by zostały wykonane szybko, muszą odbywać się po drogach lub z wykorzystaniem lotnisk bądź szlaków kolejowych.

MARIAN KLUCZYŃSKI

• przygotowania określonych dróg publicznych do eksploatacji w czasie wojny;
• sukcesywnej budowy objazdów wytypowanych miast i węzłów drogowych, eliminowania jednopoziomowych skrzyżowań dróg publicznych z liniami kolejowymi o dużej częstotliwości ruchu, a także utrzymania istniejących dojazdów i bezkolizyjnych skrzyżowań w gotowości eksploatacyjnej;
• budowy dublujących się mostów drogowych w rejonach ustalonych przez ministra obrony narodowej;
• przygotowania i utrzymania dróg dojazdowych zapewniających funkcjonowanie:
– przepraw przez przeszkody wodne,
– rejonów przeładunkowych,
– przeładowni polowych,
– baz zaopatrywania sił zbrojnych;
• budowy i utrzymania drogowych przejść granicznych przewidywanych do wykorzystania przez Siły Zbrojne RP i wojska sojusznicze zgodnie z umowami międzynarodowymi;
• budowy i modernizacji drogowych odcinków lotniskowych na trasach określonych przez ministra obrony narodowej.

Przygotowanie transportu kolejowego obejmuje:
• ustalenie potrzeb przewozowych oraz wymagań techniczno-obronnych w tym zakresie;
• przygotowanie niezbędnej ilości i różnych rodzajów taboru kolejowego specjalnie utrzymywanego dla zapewnienia przewozów na rzecz sił zbrojnych podczas podwyższania gotowości obronnej państwa oraz w czasie wojny;
• zapewnienie niezbędnej liczby cystern kolejowych;
• współpracę i wzajemne świadczenie usług przez przedsiębiorców podczas realizacji przewozów i osłony technicznej oraz wykorzystania posiadanych środków trakcyjnych do organizowania trakcji zastępczej na zelektryfikowanych liniach kolejowych znaczenia obronnego;
• realizowanie przedsięwzięć organizacyjnych zapewniających sprawne przejęcie z państw sąsiednich taboru kolejowego;
• organizacyjne przygotowanie do użycia eksploatowanego taboru kolejowego w poszczególnych stanach gotowości obronnej państwa i w czasie wojny;
• gromadzenie oraz utrzymywanie wyposażenia i urządzeń przeznaczonych do przystosowania wagonów krytych towarowych do przewozu ludzi w transportach wojskowych i ewakuacyjnych;
• wprowadzanie ograniczeń przewozowych oraz określanie priorytetu przewozów poszczególnych rodzajów ładunków;

• wprowadzanie uproszczonego zamawiania przez przewoźników rozkładu jazdy dla przesyłek priorytetowych.

Natomiast przygotowanie żeglugi śródlądowej i śródlądowych dróg polega na:

• sformowaniu określonych jednostek zmilitaryzowanych przeznaczonych do realizacji zadań przeprawowych oraz na gromadzeniu środków do zorganizowania i uruchomienia przepraw promowych lub mostowych w czasie podwyższania gotowości obronnej państwa oraz w czasie wojny;

• przygotowaniu niezbędnych budowli wodnych w rejonach planowanych przepraw promowych lub mostowych;

• osłonie technicznej śródlądowych dróg wodnych;

• zgromadzeniu niezbędnej liczby statków;

• świadczeniu usług przewozowych.

W paragrafie 12. określono zakres przygotowania transportu morskiego, czyli:

• przygotowanie statków, a także infrastruktury portowej do zapewnienia przyjęcia, rozładunku i załadunku oraz przeładunków i przewozów morskich;

• zorganizowanie przewozów i przeładunków morskich;

• zabezpieczenie nawigacyjno-hydrograficzne i ratownictwo morskie;

• kontrolę żeglugi morskiej;

• formowanie jednostek zmilitaryzowanych;

• zorganizowanie remontu okrętów i statków;

• zorganizowanie obrony cywilnej i ochrony obiektów oraz kierowania gospodarką morską;

• odtwarzanie infrastruktury portowej i innych obiektów gospodarki morskiej;

• planowanie i organizację świadczenia usług transportowych.

Natomiast paragraf 19. zawiera ustalenia dotyczące przygotowania transportu lotniczego, czyli:

• zapewnienia siłom zbrojnym niezbędnej liczby statków powietrznych;

• przygotowania i utrzymania ustalonych przez ministra obrony narodowej lotnisk oraz urządzeń i zaplecza technicznego przewidzianych do wykorzystania w czasie wojny na potrzeby sił zbrojnych i dla innych celów związanych z działaniem lotnictwa cywilnego w tym okresie;

• koncentracji i przekazania statków powietrznych oraz lotnisk, a także urządzeń i zaplecza technicznego lotnictwa wraz z personelem obsługującym, będących w posiadaniu jednostek organizacyjnych lotnictwa, nieprzewidywanych do militaryzacji i użycia przez siły zbrojne;

• utworzenia organizacyjnych rozwiązań dotyczących ograniczenia lub zawieszenia podczas podwyższania gotowości obronnej państwa ruchu lotniczego cywilnych statków powietrznych oraz podporządkowania przestrzeni powietrznej wymogom operacyjnym lotnictwa wojskowego.

Na podstawie rozporządzenia Rady Ministrów z 27 czerwca 2012 roku określono warunki oraz sposób przygotowania i wykorzystania podmiotów leczniczych na potrzeby obronne państwa. Dotyczą one przede wszystkim planowania i realizacji następujących zadań: *zwiększenia liczby łóżek bazy szpitalnej i zmiany jej profilu; tworzenia zastępczych miejsc szpitalnych; wykonywania ambulatoryjnych świadczeń zdrowotnych; określenia sposobu zabezpieczenia potrzeb kadrowych oraz wskaźników zatrudnienia w podmiotach leczniczych; wykorzystania jednostek organizacyjnych publicznej służby krwi; określenia sposobu zabezpieczenia sanitarno-epidemiologicznego; określenia sposobu postępowania w przypadku wystąpienia zdarzenia radiacyjnego; określenia sposobu realizacji świadczeń na potrzeby jednostek podległych lub nadzorowanych przez Ministra Obrony Narodowej i ministra właściwego do spraw wewnętrznych oraz na potrzeby Szefa Agencji Bezpieczeństwa Wewnętrznego; określenia sposobu i zakresu prowadzenia ewidencji i sprawozdawczości medycznej w warunkach masowego napływu poszkodowanych, rannych i chorych; określenia sposobu realizacji świadczeń na rzecz podmiotów leczniczych realizujących zadania obronne*[4].

Możliwości wykorzystania infrastruktury państwa przez siły zbrojne zostały poddane szczegółowej analizie w *Doktrynie logistycznej Sił Zbrojnych RP D-4 (B)* oraz w *Doktrynie DD-4.5 (B) o wsparciu przez państwo gospodarza*. W rozdziale siódmym pierwszego dokumentu *Obszary powiązane z systemem funkcjonalnym logistyki Sił Zbrojnych RP* określono osiem czynników mających związek z omawianym zagadnieniem. Są to:

– narodowy system zarządzania informacją logistyczną;

– wsparcie przez kontrahentów zewnętrznych;

– budżet i finanse prowadzonych operacji;

– gospodarcze ogniwa obronne podsystemu pozamilitarnego;

– współpraca cywilno-wojskowa;

– ochrona środowiska;

– pochówek poległych i zmarłych;

– organizacja obiektów przetrzymywania jeńców[5].

Na szczególną uwagę zasługuje zapis dotyczący wsparcia przez kontrahentów zewnętrznych (CSO), które stanowi uzupełnienie wojskowego potencjału logistycznego. Kontraktowanie dostaw zaopatrzenia i usług jest ważnym źródłem wsparcia logi-

4 *Rozporządzenie Rady Ministrów z dnia 27 czerwca 2012 r. w sprawie warunków i sposobu przygotowania oraz wykorzystania podmiotów leczniczych na potrzeby obronne państwa oraz właściwości organów w tych sprawach*, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20120000741/O/D20120741.pdf/. 12.11.2020.

5 *Doktryna logistyczna Sił Zbrojnych RP D-4 (B),* wersja 2, Bydgoszcz 2019, s. 169.

stycznego działań. Kolejnym elementem godnym uwagi są gospodarcze ogniwa obronne podsystemu pozamilitarnego. Warto przytoczyć definicję podsystemu pozamilitarnego, który *tworzą niewchodzące w skład sił zbrojnych ogniwa wykonawcze administracji publicznej, inne instytucje państwowe, a także przedsiębiorcy i stowarzyszenia, na które nakładane są zadania lub którym zleca się wykonywanie zadań na rzecz obronności*[6].W podrozdziale o przedsiębiorcach działających w ramach przemysłowego potencjału obronnego znajduje się zapis o podstawowych ich zadaniach, czyli:

– *pozyskiwanie lub budowa obiektów oraz ich użytkowanie*;

– *przystosowanie obiektów już istniejących do realizacji zadań obronnych równolegle z ich użytkowaniem zgodnie z zasadniczym przeznaczeniem*[7].

W trakcie planowania budowy obiektów infrastruktury wyróżnia się cztery podstawowe czynniki, które muszą zostać uwzględnione, czyli:

– *dostosowanie parametrów technicznych infrastruktury transportowej do wymagań sił zbrojnych (np. w zakresie budowy drogowych odcinków lotniskowych, przystosowania sieci transportowej do przewozu ładunków o zwiększonych gabarytach lub masie, organizacji zapasowych rejonów budowy punktów przeprawowych);*

– *przystosowanie portów morskich i lotniczych do przyjęcia statków oraz samolotów będących w wyposażeniu państw NATO (np. w zakresie możliwości technicznych dotyczących przyjęcia, obsługi oraz uzupełnienia płynów eksploatacyjnych);*

– *zapewnienie wymaganych systemów łączności (np. w zakresie łączności niejawnej, stabilności połączeń, dublowania systemów)*;

– *wykorzystanie obiektów przez wojska Sojuszu*[8].

Ostatnim obszarem powiązanym z systemem funkcjonalnym logistyki sił zbrojnych jest współpraca cywilno-wojskowa (*Civil-Military Coopearation* – CIMIC). Jest to *zespół przedsięwzięć obejmujących koordynację i współdziałanie między dowódcą wojskowym a lokalnymi podmiotami cywilnymi, do których zalicza się: ludność cywilną; władze lokalne działające w obszarach swoich kompetencji i odpowiedzialności; organizacje rządowe, pozarządowe i międzynarodowe*[9]. Ponadto komórki współpracy cywilno-wojskowej wykonują zadania w procesie zawierania kontraktów z kontrahentami zewnętrznymi. Działania te obejmują:

1) *włączanie personelu komórek logistyki w skład grup rekonesansowych kierowanych do obszaru planowanej operacji z zadaniem*:

– *gromadzenia informacji o zasobach lokalnych*;

– *wykonania wstępnej oceny stanu zasobów i infrastruktury lokalnej*;

– *ustalenia mechanizmów koordynacji działań z przedstawicielami władz i organizacji państwa-gospodarza*;

2) *informowanie personelu komórek logistyki o stanie i możliwościach*:

– *gospodarki państwa-gospodarza*;

– *infrastruktury lokalnej*;

– *lokalnego systemu opieki zdrowotnej*;

– *lokalnych systemów łączności*;

3) *zapewnienie personelowi komórek logistyki dostępu do określonych szczebli władz państwa-gospodarza*[10].

POTENCJAŁ

W naszym kraju są realizowane kompleksowe przedsięwzięcia na rzecz rozbudowy infrastruktury transportowej oraz poprawy jej stanu technicznego, a także bezpieczeństwa. Infrastruktura transportowa wpływa na efektywne funkcjonowanie sił zbrojnych oraz rozwój gospodarki państwa. Dlatego też przewiduje się dalsze zwiększanie przewozu osób, jak również towarów. Na podstawie wyników analizy możliwości korzystania z infrastruktury komunikacyjnej przedstawię potencjał, jakim dysponujemy. W tabeli 1 i 2 zaprezentowano dane Głównego Urzędu Statystycznego z lat 2017 i 2018 odnoszące się do przewozu ładunków oraz pasażerów.

Analizując transport samochodowy, należy uwzględnić aktualny stan najważniejszych dróg w Polsce, mianowicie autostrad. Łączna ich długość według stanu w dniu 31 grudnia 2018 roku wynosiła 1637 km. Z kolei długość dróg ekspresowych (dróg szybkiego ruchu) to 2077 km.

Również informacje o stacjach paliwowych są istotne, gdyż zarówno podczas przemieszczania, jak i prowadzenia działań mogą służyć oddziałom sił zbrojnych. Może jednak wykorzystać je także potencjalny przeciwnik.

Jeżeli zaś chodzi o transport lotniczy, funkcjonuje obecnie w kraju 12 cywilnych portów lotniczych. Są to: Warszawa-Okęcie (WAW); Modlin (WMI); Wrocław (WRO); Poznań-Ławica (POZ); Kraków-Balice (KRK); Katowice-Pyrzowice (KTW); Łódź-Lublinek (LCJ); Gdańsk-Rębiechowo (GDN); Bydgoszcz (BZG); Rzeszów-Jasionka (RZE); Szczecin (SZZ) i Zielona Góra (IEG).

Największym, mającym status głównego lotniska, jest Port Lotniczy im. Fryderyka Chopina w Warszawie. Pozostałe działają na zasadzie portów regionalnych, stanowiąc lotniska pomocnicze dla Okęcia. Porty lotnicze mogą być używane przez siły

6 Ibidem, s. 181.
7 Ibidem, s. 186.
8 Ibidem, s. 187.
9 Ibidem, s. 188.
10 Ibidem, s. 189.

TABELA 1. PRZEWOZY ŁADUNKÓW W LATACH 2017–2018

Wyszczególnienie	2017	2018
	w tysiącach ton	
Transport kolejowy	239 501	249 260
Transport samochodowy	1 747 266	1 873 022
Transport rurociągowy	52 393	55 287
Transport morski	8254	9149
Śródlądowy transport wodny	5777	5107
Transport lotniczy	53	63
OGÓŁEM	2 053 244	2 191 889

Opracowano na podstawie: *Przewozy ładunków i pasażerów w 2018 r.*, GUS, Warszawa 2019, s. 1.

TABELA 2. PRZEWOZY PASAŻERÓW W LATACH 2017–2018

Wyszczególnienie	2017	2018
	w tysiącach osób	
Transport kolejowy	303 001	309 722
Transport samochodowy	378 610	336 511
Transport morski	1459	1535
Śródlądowy transport wodny	1262	1395
Transport lotniczy	11 846	11 258
OGÓŁEM	696 178	660 421

Opracowano na podstawie: *Przewozy ładunków i pasażerów w 2018 r.*, GUS, Warszawa 2019, s. 5.

zbrojne jako lotniska zapasowe lub do serwisowania sprzętu, tankowania czy też awaryjnego lądowania. Nie bez znaczenia jest również cała infrastruktura stanowiąca zaplecze portów lotniczych, czyli hotele i dogodne połączenia, między innymi trasy szybkiego ruchu.

W odniesieniu zaś do transportu morskiego na naszym wybrzeżu funkcjonuje 13 portów morskich w: Gdańsku, Gdyni, Szczecinie, Świnoujściu, Elblągu, Darłowie, Dziwnowie, Kołobrzegu, Policach, Stepnicy, Ustce i Władysławowie.

Śródlądowe drogi wodne również mogą zostać wykorzystane przez siły zbrojne. Jednak ze względu na długi czas przemieszczania się nimi może to być środek transportu użytkowany jedynie w sytuacjach wyjątkowych.

Rozwój infrastruktury komunikacyjnej, która może służyć siłom zbrojnym, jest dość istotny, ponieważ wszelkie manewry oddziałami, by zostały wykonane szybko, muszą odbywać się po drogach lub z wykorzystaniem lotnisk bądź szlaków kolejowych. O tym, w jaki sposób oddziały i pododdziały będą się przemieszczać, decyduje Szefostwo Transportu i Ruchu Wojsk – Centrum Koordynacji Ruchu Wojsk, planujące w czasie pokoju sposób korzystania z sieci transportowej kraju. Właśnie ta instytucja planuje i koordynuje przemieszczanie wojsk własnych i sojuszniczych na obszarze kraju. Fakt stopniowego zwiększania potencjału infrastruktury komunikacyjnej wpływa na wzrost możliwości jej użycia przez siły i środki sił zbrojnych. ■

Sprostać **wyzwaniom**

POTRZEBA MONITOROWANIA ORAZ WYMÓG ZNAJOMOŚCI BIEŻĄCYCH POTRZEB POSZCZEGÓLNYCH JEDNOSTEK WOJSKOWYCH WYMUSIŁY WPROWADZENIE SYSTEMÓW UŁATWIAJĄCYCH ZARZĄDZANIE POSIADANYMI ZASOBAMI.

mjr Adrian Matyla

Autor jest szefem Sekcji Informatyki w Centrum Szkolenia Logistyki.

Rewolucja technologiczna w dziedzinie systemów komputerowych i teleinformatycznych dotyka każdego z nas w coraz większym stopniu. Uwidacznia się to w działaniu wszystkich komórek organizacyjnych poszczególnych jednostek wojskowych niezależnie od specyfiki ich działania. W działalności służbowej wykorzystujemy wiele systemów, aplikacji i urządzeń teleinformatycznych. Za tym wszystkim stoją ludzie, którzy odpowiadają za wdrażanie, administrowanie, konfigurację i aktualizowanie systemów oraz zapewnianie sprawności i stabilności działania zarówno urządzeń, jak i sieci oraz systemów informatycznych i teleinformatycznych.

OFERTA

Centrum Szkolenia Logistyki już na etapie formowania liczyło się z koniecznością przygotowania kadr realizujących zadania z zastosowaniem logistycznych systemów informatycznych. Zapoczątkowało to proces szkolenia wykładowców – specjalistów z tej dziedziny, by możliwe było wdrożenie do oferty szkoleniowej kursów przygotowujących do opanowania programów wykorzystywanych w logistyce.

Początkowo oferta szkoleniowa obejmowała trzy kursy. Jednak rozwój systemów teleinformatycznych używanych w logistyce generował dodatkowe potrzeby i stymulował rozbudowę oferty szkoleniowej (rys.).

W 2021 roku wdrożono trzy nowe oraz zawieszono prowadzenie trzech dotychczasowych kursów. Obecnie kształcimy specjalistów logistyki na takich kursach, jak:

- *Planowanie i sprawozdawczość logistyczna LOGREP oraz zarządzanie zasobami logistycznymi z wykorzystaniem systemu informatycznego LOGFAS*;
- *Indeksacja wyrobów w systemie Jednolitego Indeksu Materiałowego (JIM)*;
- *Zastosowanie technologii kodów kreskowych w logistyce Sił Zbrojnych RP*;
- *Kurs podstawowy z realizacji procesów logistycznych w wojskowym oddziale gospodarczym z wykorzystaniem ZWSI RON*;
- *Kurs doskonalący z realizacji procesów logistycznych w wojskowym oddziale gospodarczym z wykorzystaniem ZWSI RON*;
- *Wsparcie eksploatacji SpW z wykorzystaniem ZWSI RON*;
- *Wykorzystanie modułu PZM ZWSI RON służby mundurowej w wojskowym oddziale gospodarczym*;
- *Monitorowanie eksploatacji sprzętu wojskowego z wykorzystaniem ZWSI RON*.

Natomiast w roku 2022 przewidziano wprowadzenie do oferty Centrum siedmiu nowych kursów (tab.).

Z przedstawionych informacji wynika, że w ciagu ostatnich dziesięciu lat oferta szkoleniowa przygotowująca do korzystania z logistycznych systemów informatycznych została zwiększona o 600%.

DZIAŁALNOŚĆ

Analizując program kursów, można zauważyć, że dotyczą one kilku głównych obszarów. Pierwszy z nich to szkolenia na temat Zintegrowanego Wieloszczeblowego Systemu Informatycznego Resortu Obrony Narodowej (ZWSI RON). Z roku na rok jest on coraz częściej wykorzystywany do informatyzacji kolejnych dziedzin działalności służb logistycznych, generując potrzebę odpowiedniego przygotowania ich personelu, jak również konieczność dostosowania oferty doocze-

RYS. DYNAMIKA ZMIAN LICZBY KURSÓW DOTYCZĄCYCH LOGISTYCZNYCH SYSTEMÓW INFORMATYCZNYCH W OFERCIE CSLOG

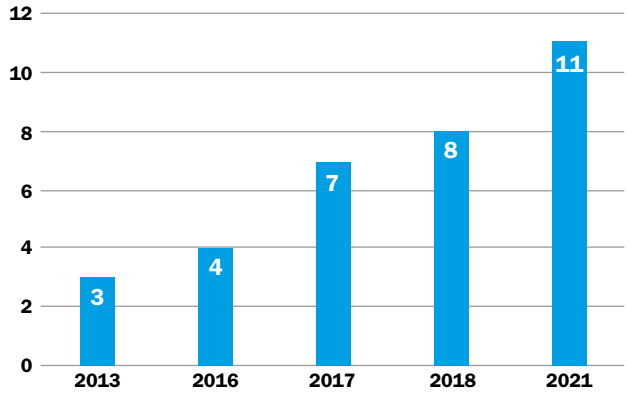


TABELA. KURSY PRZEWIDZIANE DO WDROŻENIA W ROKU 2022

Lp.	Temat kursu	Czas trwania
1	*Obsługa modułu EWM ZWSI RON rozszerzonej gospodarki magazynowej*	4 dni
2	*Wykorzystanie modułu PZM ZWSI RON w magazynie służby mundurowej wojskowego oddziału gospodarczego*	3 dni
3	*Operacyjne wykorzystanie SI LOGFAS dla oficerów sztabu i logistyki*	5 dni
4	*Logistic Functional Area Services (LOGFAS) Fundamentals & Basic Data Operator*	5 dni
5	*Allied Deployment and Movements System (ADAMS) Basic Operator*	5 dni
6	*Coalition Reception, Staging and Onward Movement (CORSOM) Operator*	5 dni
7	*Effective Visible Execution (EVE) Operator*	5 dni

Opracowanie własne (2).

kiwań dowódców. Centrum poza kursami związanymi z modułami przeznaczonymi dla konkretnej branży proponuje również kursy na temat realizacji procesów logistycznych w wojskowych oddziałach gospodarczych. Szkolenie jest prowadzone na kursach podstawowym i doskonalącym. Przy czym na poziomie podstawowym jest przeznaczone dla jednorodnych grup z poszczególnych służb. Zawansowany natomiast obejmuje bardziej skomplikowane i rzadziej realizowane w codziennej działalności służbowej procesy logistyczne.

Kolejny obszar odnosi się do Logistics Functional Area Services (LOGFAS). Ma on coraz większe znaczenie jako sojuszniczy system informatyczny wspierający procesy logistyczne realizowane w ramach ćwiczeń czy też operacji NATO. Umożliwia współpracę wielonarodową oraz wymianę informacji z sojusznikami podczas planowania i wykonywania zadań logistycznych. Na rok 2021 przewidziano budowę zdolności sił zbrojnych do jego wykorzystania w większym zakresie. Dlatego też od przyszłego roku w Centrum Szkolenia Logistyki będą prowadzone przez wykładowców z NATO Communications and Information Academy szkolenia z zakresu transportu i ruchu wojsk. Będą w nich uczestniczyć wytypowane osoby funkcyjne reprezentujące różne instytucje i jednostki Sił Zbrojnych RP.

Trzeci obszar działalności szkoleniowej dotyczy kursów związanych z podsystemem monitorowania przesyłek (PMP). Szkolenia na ten temat prowadzono dla operatorów PMP praktycznie od 2013 roku. Następnie w 2017 roku wzbogacono ofertę o kolejne kursy przeznaczone dla dyspozytorów i służb dyżurnych oraz dla administratorów lokalnych węzłów podsystemu monitorowania przesyłek. Obecnie kursy te zostały zawieszone ze względu na modernizację tego podsystemu. Po jej zakończeniu kursy z pewnością zostaną przywrócone i odpowiednio dostosowane do potrzeb.

Na pozostałych kursach poświęconych wykorzystaniu logistycznych systemów informatycznych omawiane są zagadnienia indeksacji wyrobów w systemie Jednolitego Indeksu Materiałowego oraz zastosowania technologii kodów kreskowych w logistyce sił zbrojnych. Na uwagę zasługuje fakt, że w dobie pandemii kursy dotyczące indeksacji wyrobów odbywają się zdalnie bez konieczności wizyty w Centrum. Dotyczy to zarówno części teoretycznej, jak i praktycznej.

Rozszerzanie oferty szkoleniowej, a także wdrażanie nowych systemów generuje potrzebę tworzenia struktur, które sprostają związanym z tym zadaniom. Przy czym wykonywanie ich na odpowiednim poziomie jest procesem czasochłonnym i skomplikowanym, gdyż priorytetem jest jakość, by zapewnić dowódcom jednostek warunki umożliwiające realizację zadań oraz efektywne funkcjonowanie w obszarze logistyki.

Mimo że są to procesy złożone i czasochłonne, wymagające zaangażowania wielu osób, to jednak nasza wiedza, bagaż doświadczeń oraz świadomość znaczenia i gotowość uczestniczenia w nich powodują, że dobrze realizujemy stojące przed nami zadania. ■

Zasady przewozu towarów niebezpiecznych **transportem drogowym**

ABY WYKLUCZYĆ LUB OGRANICZYĆ RYZYKO WYPADKU ORAZ EWENTUALNYCH SZKÓD, NALEŻY STOSOWAĆ W PRAKTYCE PRZEPISY, KTÓRE ZAPOBIEGAJĄ TAKIM INCYDENTOM.

Dariusz Turek

Autor jest specjalistą w Cyklu Eksploatacji Centrum Szkolenia Logistyki.

Dotyczą one transportu tego rodzaju towarów jednostką transportową po drogach publicznych lub po innych drogach ogólnodostępnych z uwzględnieniem wymaganych postojów oraz czynności z nimi związanych. Podstawowymi aktami prawnymi odnoszącymi się do przewozu towarów niebezpiecznych są między innymi umowa o międzynarodowym przewozie drogowym towarów niebezpiecznych ADR[1] oraz ustawa o przewozie towarów niebezpiecznych[2]. Umowa ADR podlega aktualizacji w cyklu dwuletnim. Przystąpiło do niej dotychczas 50 państw. Większość stanowią kraje europejskie. Ponadto podpisały ją państwa azjatyckie: Azerbejdżan, Kazachstan, Tadżykistan, Turcja oraz afrykańskie: Tunezja i Maroko.

WYMAGANIA

Każda jednostka wojskowa (przedsiębiorstwo) dokonująca załadunku, rozładunku lub przewozu towarów niebezpiecznych powinna wyznaczyć co najmniej jednego doradcę do zapewnienia bezpieczeństwa w transporcie towarów niebezpiecznych, odpowiedzialnego za wsparcie działań zapobiegających zagrożeniom dla osób, mienia i środowiska. Zgodnie z punktem 1.8.3.3 umowy ADR głównym zadaniem doradcy, przy zachowaniu odpowiedzialności kierującego przedsiębiorstwem, powinno być dążenie – z zastosowaniem wszystkich niezbędnych środków oraz w granicach określonych zakresem działalności przedsiębiorstwa – do ułatwienia realizacji omawianego przedsięwzięcia zgodnie z odpowiednimi wymaganiami i w możliwie najbezpieczniejszy sposób.

Osoby uczestniczące w transporcie spełniającym wymagania umowy ADR muszą ukończyć odpowiednie szkolenie. Kierowca jednostki transportowej powinien mieć zaświadczenie ADR o przeszkoleniu dopuszczającym do uczestniczenia w danym rodzaju przewozów. Dotyczy to kierowców przewożących: towary niebezpieczne w opakowaniach (nazywanych również sztukami przesyłki) z wyłączeniem materiałów wybuchowych oraz promieniotwórczych; towary niebezpieczne w cysternach; materiały klasy 1 (materiały wybuchowe)

1 Dz.U. 2019 poz. 769, z późn. zm.

2 *Ustawa o przewozie towarów niebezpiecznych*, Dz.U. 2020.0.154/. 7.04.2021. Stan prawny aktualny na dzień: 19.04.2021 r.

1.

ARKADIUSZ DWULATEK
COMBAT CAMERA DORSZ

OSOBY UCZESTNICZĄCE W TRANSPORCIE SPEŁNIAJĄCYM WYMAGANIA ADR MUSZĄ UKOŃCZYĆ ODPOWIEDNIE SZKOLENIE. KIEROWCA POWINIEN MIEĆ ZAŚWIADCZENIE ADR O PRZESZKOLENIU DOPUSZCZAJĄCYM DO UCZESTNICZENIA W DANYM RODZAJU PRZEWOZÓW.

oraz klasy 7 (materiały promieniotwórcze) – fot. 1. Ci ostatni powinny zaliczyć dodatkowe kursy specjalistyczne obejmujące odpowiednie zagadnienia. Członkowie załogi jednostki transportowej, którzy nie są kierowcami i nie mają uprawnień ADR oraz świadectwa doradcy, muszą odbyć szkolenie dla osób zaangażowanych w przewóz towarów niebezpiecznych zgodnie z działem 1.3 umowy ADR oraz artykułem 14 ustawy o przewozie towarów niebezpiecznych.

PODSTAWOWE ZASADY

Podczas transportu towarów niebezpiecznych jednostce transportowej niezbędne są odpowiednie dokumenty. Głównym jest dokument przewozowy spełniający wymagania umowy ADR. Dodatkowe to: instrukcje pisemne, dokument tożsamości kierowcy z fotografią, świadectwo dopuszczenia jednostki transportowej do wykonywania przewozu towarów niebezpiecznych oraz zaświadczenie o przeszkoleniu kierowcy.

Sztuka przesyłki transportowana zgodnie z umową ADR musi spełniać odpowiednie wymagania dotyczące oznakowania oraz konstrukcji. Konieczne jest podanie numeru UN przewożonego materiału niebezpiecznego, jak również użycie nalepki ostrzegawczej w kolorze czerwonym.

W przypadku materiałów wybuchowych, promieniotwórczych oraz gazów dodatkowo na sztuce przesyłki musi być umieszczona prawidłowa nazwa przewozowa w kolorze pomarańczowym (fot. 2). Oznakowanie musi być dobrze widoczne i czytelne oraz wykonane z trwałych materiałów odpornych na oddziaływanie warunków atmosferycznych. Opakowanie zastosowane do przewozu materiałów niebezpiecznych powinno być wyposażone w certyfikat w kolorze niebieskim, zatwierdzony przez właściwe władze. W przypadku opakowań zbiorczych, oprócz wskazanych na fotografii 2 informacji, musi być naniesiony napis „Opakowanie zbiorcze".

Jednostka transportowa, która przewozi towary niebezpieczne w sztukach przesyłki, powinna być wyposażona w dwie prostokątne tablice barwy pomarańczowej umieszczone z jej przodu i z tyłu w płaszczyźnie pionowej. Tablice te muszą być zamontowane w taki sposób, aby były dobrze widoczne, co pokazano na rysunku rys. 1.

Pojazdy przewożące materiały wybuchowe klasy 1 w sztukach przesyłki powinny być oznakowane z przodu i z tyłu tablicą barwy pomarańczowej oraz

ARCH. AUTORA

2.

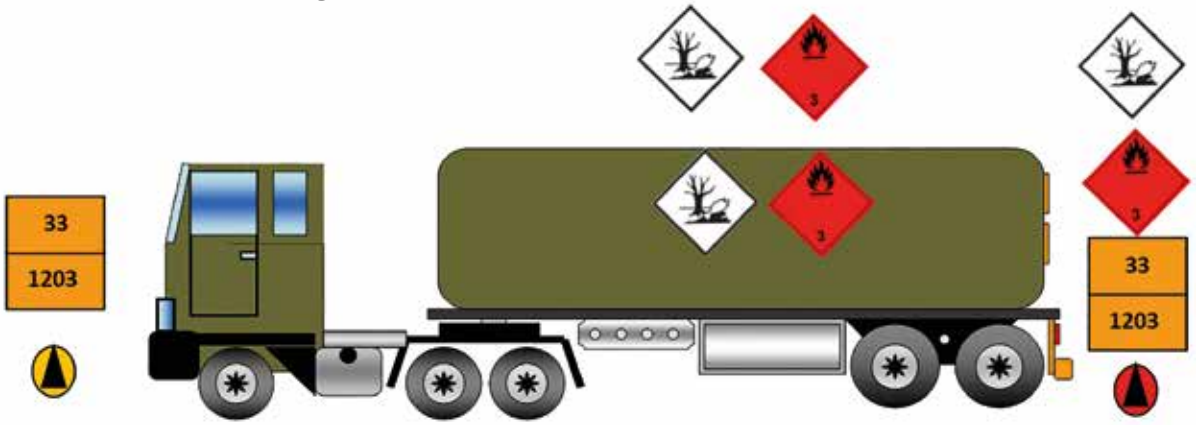
Oznakowanie przesyłki towarów niebezpiecznych

RYS. 1. OZNAKOWANIE POJAZDU PRZEWOŻĄCEGO TOWARY NIEBEZPIECZNE

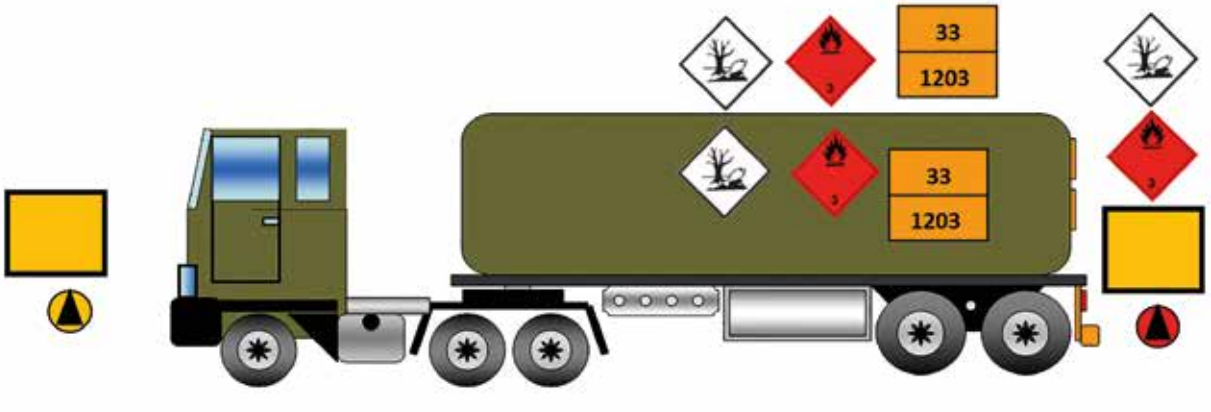
RYS. 2. OZNAKOWANIE POJAZDU PRZEWOŻĄCEGO MATERIAŁY WYBUCHOWE KLASY 1

Opracowanie własne (2).

RYS. 3. OZNAKOWANIE ŚRODKA TRANSPORTU (CYSTERNY) PRZEWOŻĄCEGO MATERIAŁ NIEBEZPIECZNY



RYS. 4. INNY SPOSÓB OZNAKOWANIA POJAZDU PRZEWOŻĄCEGO MATERIAŁ NIEBEZPIECZNY



na obu bokach i z tyłu nalepką (nalepkami) ostrzegawczą wymaganą w przypadku transportu danego materiału (rys. 2).

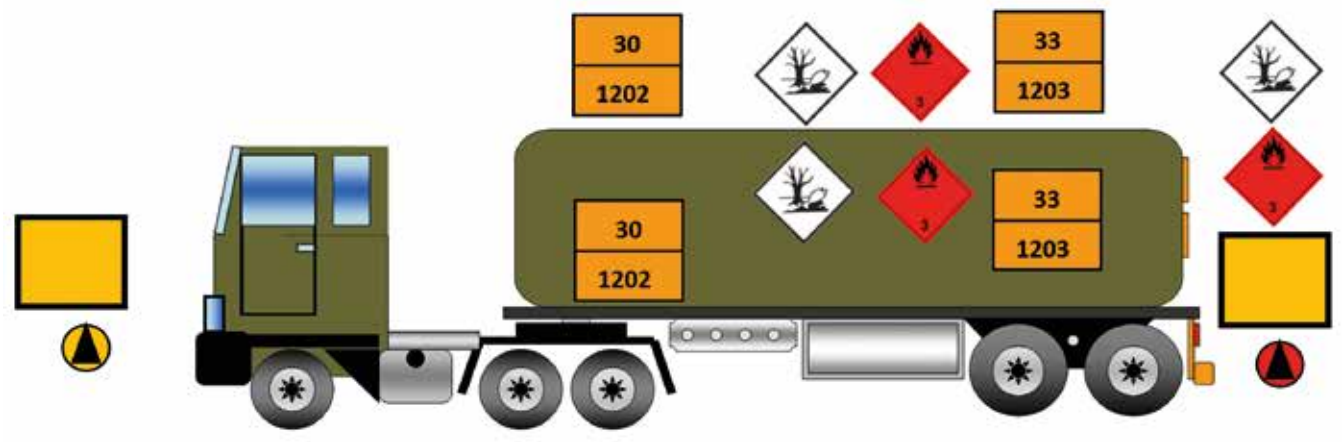
Jeżeli w pojeździe są przewożone materiały wybuchowe należące do dwóch lub więcej grup zgodności, to na nalepkach nie umieszcza się liter grup zgodności. Pojazdy, w których przewozi się materiały i przedmioty należące do różnych podklas, muszą być wyposażone w nalepki odpowiadające podklasie o najwyższym zagrożeniu według następującej kolejności: 1.1; 1.5; 1.2; 1.3; 1.6; 1.4.

Środek transportu przewożący jeden materiał niebezpieczny w cysternach lub luzem powinien być oznakowany z przodu i z tyłu tablicą barwy pomarańczowej zawierającą numer UN oraz numer rozpoznawczy zagrożenia, a także nalepkami ostrzegawczymi umieszczonymi na obu bokach oraz z tyłu pojazdu (rys. 3).

Jednostka może być również oznakowana z przodu i z tyłu tablicą pomarańczową gładką oraz na obu bokach tablicą z numerem UN i numerem rozpoznawczym zagrożenia (rys. 4).

Pojazd cysterna przewożący różne materiały (cysterna wielokomorowa) powinien być wyposażony w gładkie tablice bez numerów umieszczone z przodu i z tyłu jednostki transportowej. Dodatkowo na

RYS. 5. OZNAKOWANIE POJAZDU CYSTERNY PRZEWOŻĄCEGO RÓŻNE MATERIAŁY NIEBEZPIECZNE



Opracowanie własne (3).

pojeździe należy umieścić tablice z numerami UN oraz z numerem rozpoznawczym zagrożenia. Ponadto cysterna musi być oznakowana nalepkami ostrzegawczymi dotyczącymi przewożonego materiału (rys. 5).

Jeżeli materiał został rozładowany, a jednostka transportowa jest odgazowana i oczyszczona, oznakowanie powinno być zdjęte lub zakryte. Pokrowiec zasłaniający tablice powinien być wykonany z materiału zapewniającego co najmniej piętnastominutową odporność na oddziaływanie ognia.

Jednostki transportowe przewożące materiały niebezpieczne powinny być wyposażone w odpowiednią ilość środka gaśniczego w zależności od dopuszczalnej masy całkowitej zespołu pojazdów. Gaśnice muszą być wyposażone w plombę potwierdzającą, że nie były używane. Ponadto powinny być umieszczone na nich informacje o terminie następnej kontroli lub dopuszczalnym okresie użytkowania. Dodatkowym wyposażeniem podczas transportu jest tak zwana skrzynka ADR zawierająca: klin pod koło dla każdego pojazdu, dwa stojące znaki ostrzegawcze, płyn do płukania oczu, kamizelkę ostrzegawczą, przenośne urządzenia oświetleniowe (latarka), parę rękawic ochronnych, ochronę oczu (okulary ochronne), maskę ucieczkową, łopatę, osłonę otworów kanalizacyjnych oraz pojemnik do zbierania pozostałości.

OFERTA

Warto zaznaczyć, że wspomniane kursy można ukończyć w Centrum Szkolenia Logistyki. Oferowane są następujące ich rodzaje: kurs początkowy dla kierowców przewożących towary niebezpieczne w cysternach oraz towary klasy 1 (10 dni szkoleniowych); kurs doskonalący dla kierowców przewożących towary niebezpieczne w cysternach i towary klasy 1 (5 dni szkoleniowych); kurs początkowy dla kandydatów na doradców do spraw bezpieczeństwa w transporcie drogowym towarów niebezpiecznych (10 dni szkoleniowych); kurs doskonalący dla doradców do spraw bezpieczeństwa w transporcie drogowym towarów niebezpiecznych (5 dni szkoleniowych); kurs początkowy (i doskonalący) dla doradców do spraw bezpieczeństwa przewozu towarów niebezpiecznych transportem kolejowym (RID) (10 dni szkoleniowych); kurs dla doradców do spraw bezpieczeństwa przewozu towarów niebezpiecznych transportem lotniczym (ICAO/IT – kat. 6) (4 dni szkoleniowe) oraz kurs dla doradców do spraw bezpieczeństwa przewozu towarów niebezpiecznych transportem morskim (IMDG).

* * *

Zaprezentowane zasady przewozu towarów niebezpiecznych transportem drogowym stanowią jedynie niewielki procent całości przepisów dotyczących tego zagadnienia zgodnie z umową ADR. Należy jednak pamiętać, że przepisy wspomnianej umowy podlegają aktualizacji, dlatego szukając szczegółowych informacji, warto upewnić się, czy wskazany przepis nadal obowiązuje. ■

Nowa jakość w konfliktach zbrojnych

MUSIMY SIĘ PRZYZWYCZAIĆ DO FAKTU, ŻE OBRAZ WSPÓŁCZESNEGO KONFLIKTU LOKALNEGO BĘDZIE POKAZEM KOLEJNYCH, NOWYCH ROZWIĄZAŃ PLATFORM BEZZAŁOGOWYCH.

płk dypl. rez. nawig. inż. Józef M. Brzezina

Autor jest ekspertem w Biurze Projektów Lotniczych PGZ SA.

Jednym z istotnych czynników obecności bezzałogowych statków powietrznych (BSP) w rejonach konfliktów jest wypracowywanie nowych sposobów wykorzystania coraz liczniejszej floty tych uniwersalnych systemów. Wiadomo, że wielu producentów tego sprzętu nie ma zbyt dużo okazji do sprawdzenia, jak ich produkty są wykorzystywane w walce i jakie przyjąć kierunki ich rozwoju. Tym bardziej informacje przekazywane za pośrednictwem mediów z miejsc, gdzie dochodzi do starć z udziałem BSP, mogą być zmanipulowane lub też zawierać dużą dozę przekłamań. W tych trudnych warunkach politycznych, potęgowanych jeszcze skutkami pandemii, duży nacisk w toczonych konfliktach położono na użycie lotnictwa, a także nowych typów BSP, które mają teraz jeszcze większą szansę na zainteresowanie potencjalnych klientów. To głównie takie miejsca stwarzają okazję do sprawdzenia wielu nowych koncepcji i użycia różnego typu zdalnie sterowanych systemów powietrznych przeznaczonych do militarnego ich zastosowania.

KIERUNKI ROZWOJU

Z analizy sposobów wykorzystania platform bezzałogowych w rejonach konfliktów wynika, że ich uczestnicy walory tego sprzętu, oprócz zdolności do prowadzenia rozpoznania, umiejętnie połączyli z innymi istotnymi w tych warunkach systemami rażenia i walki elektronicznej (tab.). Można się pokusić o określenie ogólnych trendów zastosowania platform bezzałogowych, do których należą:

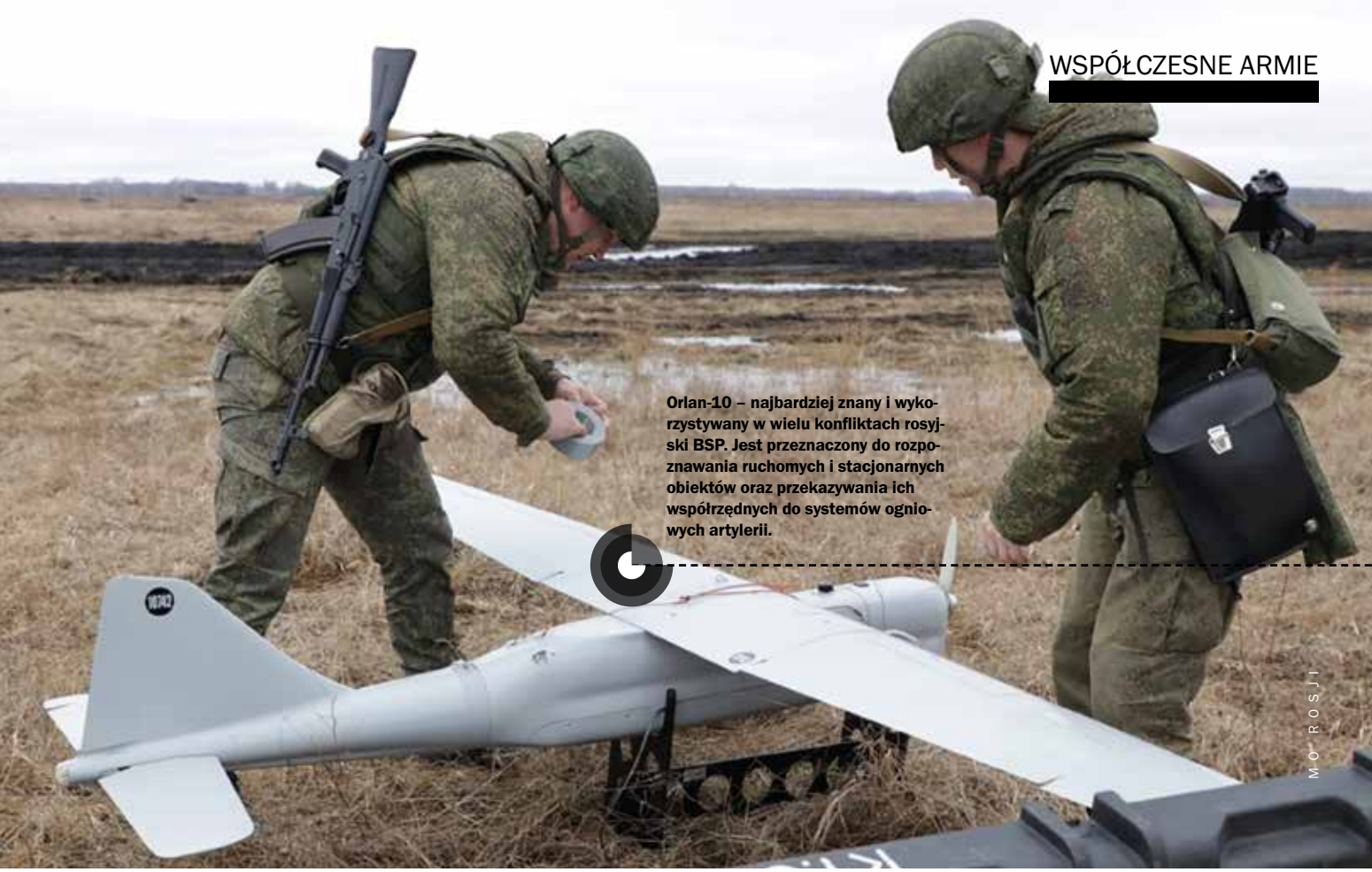
– użycie dobrze znanych od wielu lat drogich i zaawansowanych technologicznie BSP, produkowanych głównie w Stanach Zjednoczonych, Chinach i Izraelu. Liczba oraz lista tego typu zaawansowanych platform stale się powiększa;

– wykorzystywanie prostszych i tańszych BSP w połączeniu z wieloma powietrznymi i naziemnymi systemami, zdolnymi do precyzyjnego oddziaływania za ich pośrednictwem na przeciwnika prowadzącego działania na lądzie;

– stosowanie tanich platform bezzałogowych do wykonywania powietrznych misji grupowych zwanych rojami.

Z dzisiejszej perspektywy trudno uwierzyć, że tego typu działania były już dobrze znane kilka dziesiątek lat temu. Jednym z przykładów, o którym należałoby wspomnieć, to zastosowanie w dolinie Bekaa przez siły zbrojne Izraela podczas konfliktu libańskiego w 1982 roku jednocześnie wielu niedużych, różnych typów BSP. Skutecznie przeprowadzono wtedy grupowe działania pozoracyjne i demonstracyjne, które miały istotny wpływ na przebieg operacji lotniczej, złożonej głównie z załogowych samolotów bojowych. Izraelczycy nauczeni doświadczeniami płynącymi z wojny Yom Kippur (1973 rok) odnieśli w tym konflikcie spektakularne zwycięstwo.

Bezzałogowe statki powietrzne zostały wykorzystane w kompleksowy i niekonwencjonalny, jak na tamten okres, sposób. Mini-BSP Mastiff, Scout, Chucar i Samson służyły w głównej mierze do wykrywania oraz zwalczania syryjskich pododdziałów rakiet przeciwlotniczych. Dodatkowo, bardzo często wykorzystywano je do patrolowania strefy przygranicznej. Współcześnie można stwierdzić, że na liderów nowo-



Orlan-10 – najbardziej znany i wykorzystywany w wielu konfliktach rosyjski BSP. Jest przeznaczony do rozpoznawania ruchomych i stacjonarnych obiektów oraz przekazywania ich współrzędnych do systemów ogniowych artylerii.

MO ROSJI

czesnego zastosowania BSP w konfliktach zbrojnych o znaczeniu lokalnym i międzynarodowym wyrosły trzy państwa: Turcja, Iran oraz Federacja Rosyjska, które duży nacisk położyły na rozwój swoich platform bezzałogowych.

Wpływ na tę ocenę miały decyzje, które podjęto znacznie wcześniej, bo już co najmniej dekadę temu. Dróg było wiele, a najprostszą było powielenie koncepcji rozwoju systemów BSP realizowanych w innych państwach. Wystarczyło zakupić flotę kilku typów BSP, jak to robił w ostatnich latach np. Azerbejdżan, lub krok po kroku budować złożony z wielu elementów własny autorski program, jak miało to miejsce w wypadku tych trzech wymienionych państw.

BUDOWANIE ZDOLNOŚCI

Rosja na początku swojej drogi kupiła pewną liczbę gotowych egzemplarzy BSP (Searcher Mk II, Bird Eye 400 i I-View MK-150) oraz licencje w Izraelu i Austrii (S-100). Jednak już na kolejnym etapie zbudowała mocne fundamenty własnego programu, opartego na prostych i odpornych na trudne warunki platformach. Rosjanie nie postawili na długotrwałe i wymagające dużego wysiłku budowanie uzbrojonych ciężkich bojowych BSP, zaliczanych do kategorii średnia wysokość oraz duża długotrwałość lotu. Jednak ich koncepcja, polegająca na wykorzystaniu posiadanej floty lżejszych i prostszych BSP w połączeniu z bezpośrednią współpracą z naziemnymi środkami rażenia, przynosi dobre efekty.

Do realizacji zadań stosuje się rozpoznawcze bezzałogowe statki powietrzne, które wykrywają i śledzą wybrane cele, mające w danym czasie wpływ na sytuację taktyczną na polu walki. System jest w stanie określić ich dokładne współrzędne i przekazać te informacje w czasie zbliżonym do rzeczywistego bezpośrednio do baterii artylerii. Artylerzyści zaś mogą zniszczyć rozpoznany za pośrednictwem sensorów BSP cel przeciwnika. Atak jest wykonywany z wykorzystaniem standardowych pocisków lub kierowanych za pomocą lasera. Wskaźnik laserowy znajduje się na pokładzie rozpoznawczego BSP i oświetla cel dla naziemnych środków rażenia.

Koncepcja systemu rozpoznawczo-uderzeniowego polega na użyciu lasera, który emituje wiązkę, oznaczając *migotaniem* wcześniej rozpoznany przez operatora BSP cel, zakwalifikowany przez dowódcę komponentu lądowego jako opłacalny do zniszczenia. Cel dla artylerii jest wskazywany przez operatora BSP bezpośrednio ze stanowiska sterowania i kontroli misji za pomocą lasera pokładowego w momencie, kiedy pocisk się do niego zbliża i wymaga on korekcji trajektorii lotu, tak by osiągnąć bezpośrednie trafienie.

Podobno sześciocalowa półaktywna głowica laserowa pocisku kalibru 122 mm Krasnopol (podobna do amerykańskiego pocisku Copperhead) zwykle wymaga 30-sekundowego oświetlenia celu (bliżej celu załączała się półaktywna laserowa głowica naprowadzania). Pocisk Krasnopol jest standardową bronią w arsenale rosyjskiej samobieżnej haubicoarmaty 2S19 Msta-S kalibru 152 mm i może być również wystrzelony przez starsze haubice samobieżne, np. 2S3 Akacja, stosowane przez armię syryjską. Siły rosyjskie testują również nowsze pociski, które wymagają mniej

czasu do precyzyjnego prowadzenia pocisku w fazie końcowej.

Według producenta amunicji, Biura Konstrukcyjnego Przyrządów im Akademika A. Sziponowa (KBP) z Tuły, sprzęt do tego typu zadań o masie 4,2 kg został przetestowany na BSP pionowego startu i lądowania Katran. W oświadczeniu firmy czytamy: *Kierowana amunicja artyleryjska stanowi sposób na utrzymanie i pomnożenie roli systemów artyleryjskich w obecnej fazie rozwoju uzbrojenia, co wymaga większej mobilności, krótszego czasu reakcji i mniejszego zużycia amunicji. Zautomatyzowany system rozpoznawczo-uderzeniowy wykorzystujący BSP może zapewnić wyeliminowanie wielu ważnych dla przebiegu walki celów przy wykorzystaniu amunicji kierowanej na znaczne odległości*.

Wydaje się, że armia rosyjska z wielu powodów preferuje mniejszy i tańszy system rozpoznawczo-uderzeniowy od większych i uzbrojonych bojowych BSP. Mały, nieuzbrojony BSP jest trudniejszy do wykrycia i zestrzelenia przez przeciwnika. Co więcej, jest znacznie tańszy, łatwiejszy w budowie i utrzymaniu, a ponadto oferuje dłuższy czas przebywania w powietrzu.

Rosyjskie Ministerstwo Obrony po przetestowaniu kilku typów BSP do realizacji zadań w nowej roli jako najbardziej odpowiedni do produkcji w dużej liczbie uznało Orlan-30. Producent charakteryzuje platformę jako kolejną wersję Orlan-10 – rozpoznawczego BSP (fot.) sprawdzonego podczas działań bojowych we wschodniej Ukrainie i w Syrii. Jest to obecnie najpopularniejszy rosyjski BSP używany w Syrii i podkreśla się, że jest on przeznaczony do rozpoznawania ruchomych i stacjonarnych obiektów oraz przekazywania ich współrzędnych do systemów ognia artylerii.

Jeszcze w 2019 roku Orlan-30 przeszedł państwowe testy akceptacyjne. Zgodnie z oświadczeniem Ministerstwa Obrony duża liczba tych platform w nowej wersji miała wejść do służby od 2020 roku. Platforma powietrzna o masie około 30 kg wykonuje lot z prędkością 150 km/h i może być używana do wysokości 4500 m. Nowy BSP może realizować misję przez ponad 5 godzin w odległości do 300 km od miejsca startu. Oprócz wskazywania celów do rażenia pociskami Krasnopol może także wskazywać cele dla pocisków Smelchak wystrzeliwanych z moździerzy kalibru 240 mm Tulipan, a także dla bomb serii KAB-500/1500.

Ostatnio Federacja Rosyjska zanotowała pierwsze sukcesy dotyczące coraz powszechniej stosowanej na polu walki amunicji krążącej. Producent m.in. rosyjskich platform bezzałogowych ZALA AERO, będący częścią firmy Kałasznikow wchodzącej w skład koncernu Rostec, zakończył testy bezzałogowych precyzyjnych systemów uderzeniowych typu Lanciet. Jest to nowa, inteligentna broń, która może samodzielnie zlokalizować i zniszczyć cel. Platforma została wyposażona w łącze transmitujące obraz w czasie rzeczywistym i pozwalające potwierdzić trafienie w wybrany cel.

Platforma ta miała swoją premierę podczas forum „Armija-2019". BSP Lanciet zawiera moduły odpowiedzialne za rozpoznanie, komunikację, nawigację, a także precyzyjny środek uderzeniowy. Jest w stanie niszczyć cele w powietrzu, na lądzie i morzu. Jego zasięg wynosi do 40 km, a jego maksymalna masa startowa to 12 kg.

Nasz wschodni sąsiad nie zapomniał również o większych BSP. W połowie 2019 roku poinformowano o przeprowadzeniu pierwszego lotu testowego ciężkiego, bojowego BSP S-70 Ochotnik (Łowca), opracowanego przez Biuro Projektowe Suchoja. Oblot nowej platformy przeprowadzono na wysokości około 600 m pod kontrolą operatora znajdującego się na ziemi. Zakończył się on pomyślnym lądowaniem.

Jak poinformowało Ministerstwo Obrony Federacji Rosyjskiej, BSP S-70 Ochotnik został zbudowany w układzie latającego skrzydła z wykorzystaniem specjalnych materiałów i powłok, które mają za zadanie zmniejszyć jego powierzchnię skutecznego odbicia. Ma to uczynić go trudno wykrywalnym dla radarów.

Dodatkowo platforma ma być wyposażona w różnego typu nowoczesne systemy rozpoznawcze oraz dwie komory uzbrojenia, w których będzie można pomieścić do 2000 kg kierowanego i niekierowanego uzbrojenia. Pierwszy lot testowy oznaczał wstęp do dalszych, kluczowych badań i testów nowej konstrukcji, która wpisuje się w ambitny plan rozwoju rosyjskich zdolności w dziedzinie opracowywania i produkowania własnych BSP, w tym również ich ciężkich i uzbrojonych wersji.

TURECKIE DĄŻENIA

Ten kraj z dużą determinacją opracował własny program rozwoju floty bojowych BSP. Prace rozpoczęto prawie dekadę temu. Powoli, krok po kroku, budowano elementy systemu potrzebnego do stworzenia liczącej się floty bezzałogowej, na wzór tego, co udało się parę lat wcześniej uzyskać w Iranie.

Ze względu na konflikt z kurdyjskim ruchem separatystycznym PKK (Partia Pracujących Kurdystanu) Turcy mieli czas, aby podczas działań związanych ze zwalczaniem tego ruchu doskonalić swoje możliwości z zakresu budowy platform bezzałogowych. Amerykański zakaz używania platform bezzałogowych w tym konflikcie korzystnie wpłynął na odważne decyzje podejmowane w Turcji. Polityka USA, ograniczająca sprzedaż technologii uzbrojonych BSP Turcji z obawy, że zostanie ona wykorzystana w celu wspierania walk z Kurdami, stała się kluczową dla rozwoju krajowego programu BSP. Do 2007 roku tureckie siły zbrojne nie miały złudzeń co do tego, co mogą pozyskać od Amerykanów. Ci zgadzali się jedynie na wysyłanie nad terytorium tego państwa swoich uzbrojonych BSP MQ-1 Predator. Turcy byli rozczarowani słabą wydajnością izraelskich BSP, które pozyskali wiele lat temu (Heron i Harpy). W tej sytuacji nie mieli wyboru i zaczęli rozwijać swój własny autorski program, który po latach robi spore wrażenie.

W Europie w tym czasie żadne z państw należących do NATO nie dokonało tak znaczącego postępu w tej

TABELA. INCYDENTY Z UDZIAŁEM BSP WYKONUJĄCYMI MISJE BOJOWE NAD SYRIĄ ORAZ SĄSIEDNIMI PAŃSTWAMI OD POCZĄTKU 2017 ROKU

Rok 2017			
Data	Wydarzenie	Klasa	Państwo
23.01	Rosjanie utracili BSP Orłan-10 w rejonie miejscowości Homs	taktyczny	Syria/Federacja Rosyjska
24.01	Strona rosyjska utraciła mini-BSP Granat 4	taktyczny	Syria/Federacja Rosyjska
3.03	Rosjanie utracili BSP Orłan-10 w rejonie m. Hama (przyczyna techniczna)	taktyczny	Syria/Federacja Rosyjska
19.03	Strona izraelska utraciła w Syrii (rejon m. Quneitra) mini-BSP Skylark I (według strony izraelskiej utrata kontroli operatora BSP, według rebeliantów izraelski BSP został zestrzelony)	taktyczny	Izrael/Syria
9.04	Prawdopodobnie nad Syrią zestrzelono z wykorzystaniem systemu rakietowo-artyleryjskiego Pancyr S1 izraelski BSP Heron w rejonie m. Tartus	MALE (Medium Altitude Long Endurance)	Izrael/Syria
20.05	Prawdopodobnie zestrzelono za pomocą systemu Pancyr S1 kolejny izraelski BSP typu Heron w rejonie m. Tartus	MALE	Izrael/Syria
27.05	System Pancyr S1 osłaniający bazę Tartus brał udział w zestrzeleniu taktycznego BSP RQ-21B BlackJack	taktyczny	Syria/Stany Zjednoczone
6.06	Syryjski samolot załogowy MiG 23 MLD zestrzelił jordański BSP Falco	taktyczny	Jordania/Syria
8.06	Irański BBSP Shahed 129 zaatakował rakietami powietrze–ziemia pozycje amerykańskich sił specjalnych w rejonie Al-Tant. Został zestrzelony przez samolot F-15 E Strike Eagle	BBSP (bojowy BSP)	Syria/Iran/Stany Zjednoczone
20.06	Samolot F-15 E Strike Eagle zestrzelił irański BBSP Shahed 129	BBSP	Syria/Iran/Stany Zjednoczone
6.07	Prawdopodobnie nad Syrią zestrzelono za pomocą systemu Pancyr S1 izraelski BSP Heron w rejonie m. Masyaf	MALE	Izrael/Syria
18.09	Izraelczycy zestrzelili irański BSP wykorzystując przeciwlotniczy pocisk kierowany MIM 104D wystrzelony z systemu Patriot	taktyczny	Izrael/Syria
wrzesień	Doszło do próby uderzenia z użyciem BSP na rosyjską przeprawę mostową na rzece Eufrat. BSP atak wykonały bombami improwizowanymi. Rosjanie nie ponieśli strat	BBSP	tzw. Państwo Islamskie/Syria
12.12	Atak brytyjskiego MQ-9 Reaper na grupę ekstremistów tzw. Państwa Islamskiego. Użyto rakiety przeciwpancernej AGM-114	BBSP, MALE	Syria/Wielka Brytania
Rok 2018			
10. 01	W rejonie Wzgórz Golan granicę przekroczył irański BSP Shahed 171 (przypominający RQ-170), który po wykryciu przez naziemne środki radiolokacyjne został zestrzelony przez śmigłowiec AH-64D pociskiem AGM-114K	taktyczny	Izrael/Iran
12.01	W Syrii w rejonie północno-wschodniej Hamy został zestrzelony rosyjski rozpoznawczy BSP Forepost. Platformę zestrzelili bojownicy islamistycznego ugrupowania Nour-al.-Din al.-Zenki	taktyczny	Federacja Rosyjska
10.02	W syryjskiej prowincji Deir ez-Zor sfilmowano udany atak BBSP MQ-9 Reaper na czołg. Pojazd został zniszczony	BBSP/MALE	Syria/Stany Zjednoczone
12.02	Turecki TB2 Bayraktar został zestrzelony przez Kurdów koło wioski Qude w rejonie Afrin	MALE	Turcja/Syria
3.03	W Syrii strona rosyjska utraciła BSP Eleron 3 SW w rejonie m. Hama	taktyczny	Syria/Federacja Rosyjska

4.03	W pobliżu granicy syryjskiej iraccy żołnierze zestrzelili BSP Skywalker X8 należący do tzw. Państwa Islamskiego	mini-BSP	Irak/tzw. Państwo Islamskie
6.03	W Syrii w pobliżu miejscowości Lataminah Rosjanie utracili BSP T23E Eleron-3SW (n/b 216). Spadł on na teren kontrolowany przez rebelianckie ugrupowanie Jaysh al-Izza	taktyczny	Syria
22.03	Syryjscy rebelianci z ugrupowania Jaysh al-Izza zestrzelili rosyjski rozpoznawczy BSP Orłan-10. Z opublikowanego filmu wynika, że po odstrzeleniu skrzydła operator chciał ratować maszynę, wypuszczając spadochron do lądowania, ale uszkodzony BSP ostatecznie zerwał się i roztrzaskał o ziemię.	taktyczny	Syria/Federacja Rosyjska
27.03	Nad miejscowością Bosra w południowej Syrii rebelianckie ugrupowanie FSA zestrzeliło mini-BSP produkcji rosyjskiej Granat-4	taktyczny BSP	Federacja Rosyjska/ Syria
29.04	W Libii znaleziono BSP używany wyłącznie przez rosyjski Specnaz	taktyczny	Libia/Federacja Rosyjska
15.05	W rejonie miejscowości Bare w irackim Kurdystanie rozbił się turecki BSP najprawdopodobniej TB2 Bayraktar	BBSP	Turcja
28.06	Wieczorem w syryjskiej prowincji Hama w ręce rebeliantów wpadł rosyjski rozpoznawczy BSP Orłan-10. Aparat był kompletny i nie wyglądał na to, że był uszkodzony od ostrzału	taktyczny	Syria/Federacja Rosyjska
17.08	W pobliżu bazy lotniczej w Benina odnaleziono rozpoznawczy BSP produkcji chińskiej pionowego startu SD-60B Sea Cavalery. Do jego zestrzelenia przyznają się bojówki sprzyjające LNA	BSP (pionowego startu i lądowania)	Libia
20.09	W rejonie Ain Zara, na południe od Trypolisu, wojska GNA zestrzeliły rozpoznawczy rosyjski BSP Orłan-10. Rząd GNA utrzymuje, że należał on do wojsk LNA. Tymczasem Orłan-10 chętnie jest używany przez rosyjskie wojska specjalne	taktyczny	Libia/Federacja Rosyjska
28.09	Para samolotów F-16 należąca do tureckich sił powietrznych zestrzeliła niezidentyfikowany BSP nad turecką prowincją Kilis graniczącą z Syrią	taktyczny BSP	Turcja
31.12	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
Rok 2020			
22.01	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
28.01	W rejonie na wschód od Misraty wojska podległe rządowi GNA zestrzeliły należącego do ZEA bojowego BSP WingLoong (produkcji chińskiej), który wspierał wojska LNA. Wśród szczątków platformy były widoczne punkty podwieszenia uzbrojenia wraz z fragmentami chińskiego pocisku LJ-7	BBSP	ZEA/Chiny
30.01	Na południe od Trypolisu odnaleziono szczątki rosyjskiego BSP Orlan-10. Jego zestrzelenie przypisują sobie wojska podległe GNA, które zidentyfikowały BSP jako należący do ZEA	taktyczny	Libia/ZEA
25.02	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
25.02	Tureckie lotnictwo straciło w rejonie m. Dadikh BSP Anka-S. Turecki BBSP był uzbrojony w pociski kierowane MAM-L	MALE	Turcja/Syria
26.02	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
28.02	Wojska LNA zestrzeliły dwa tureckie bojowe BSP TB2 Bayraktar (przy czym co do prawidłowości identyfikacji szczątków spod Trypolisu można mieć wątpliwości)	BBSP	Libia/Turcja
29.02	Od pocisku z tureckiego BSP zginęło dwóch generałów, pułkownik i kilku oficerów niższej rangi, którzy zostali zabici podczas odprawy w m. Zarbach	BBSP	Turcja/Syria
1.03	Na teren kontrolowany przez rebeliantów spadł turecki BSP Anka-S	MALE	Turcja/Syria
2.03	W rejonie Jabal al-Zawiya rozbił się wspierający działania wojsk rządowych BSP Ababil AB.3. Do jego zestrzelenia przyznali się syryjscy rebelianci z dżihadystycznego ugrupowania Hayat Tahrir al-Sham	BBSP	Iran/Syria
2.03	Syryjskie siły rządowe zestrzeliły turecki BSP TB2 Bayraktar. Rozbił się on w okolicy Kfardael, w zachodniej części prowincji Aleppo. Według Syryjczyków został trafiony przeciwlotniczym pociskiem rakietowym wystrzelonym z zestawu Buk-M2	BBSP	Turcja/Syria
4.03	Syryjska obrona przeciwlotnicza zestrzeliła turecki BSP TB2 Bayraktar	BBSP	Turcja/Syria
5.03	W okolicy Darat Izza rebelianci zestrzelili irański BSP Ababil AB.3. Dokonano tego rakietą Stinger	BBSP	Iran/Syria
10.03	W Turcji tuż po starcie z położonej przy granicy syryjskiej bazy Batman rozbił się BBSP TB2 Bayraktar. Jako przyczynę podano awarię techniczną	BBSP	Turcja/Syria

10.03	Syryjskie rebelianckie ugrupowanie NSA (New Syrian Army) poinformowało o zestrzeleniu rosyjskiego rozpoznawczego BSP Orlan-10, który spadł w rejonie miejscowości Suluk w północnej części prowincji Rakka. Mogło dojść do naturalnego lub sztucznego zakłócenia sygnału (na tym terenie operują amerykańskie oddziały specjalne z odpowiednim wyposażeniem WRE) lub awarii innego typu	taktyczny BSP	Syria/Federacja Rosyjska
31.03	Wojska LNA zestrzeliły dwa tureckie bojowe BSP TB2 Bayraktar (Misrata i Al-Tawaisha pod Trypolisem)	BBSP	Libia/Turcja
5.04	W pobliżu m. Tathuna w Libii w wyniku ataku tureckiego BSP TB2 Bayraktar został zniszczony samolot transportowy An-32, który wylądował z zapasami dla wojsk LNA. Nic nie wiadomo o losie załogi	BBSP	Libia/Turcja
11.04	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
17.04	Wojska LNA zestrzeliły dwa tureckie bojowe BSP TB2 Bayraktar	BBSP	Libia/Turcja
18.04	Wojska LNA zestrzeliły turecki bojowy BSP TB2 Bayraktar	BBSP	Libia/Turcja
19.04	Wojska LNA zestrzeliły w Libii w okolicy m. Abu Grein bojowy chiński BSP WingLoong II, należący do ZEA, które wspierają siły LNA. Wszystko wskazuje na to, że doszło do omyłkowego zestrzelenia sojuszniczej maszyny. Wbrew oczywistym dowodom rzecznik LNA informował, że jest to turecki BSP Anka-S o zbliżonym układzie konstrukcyjnym	BBSP	Libia/ZEA

Opracowanie własne.

dziedzinie. Dlatego też nasi sojusznicy wciąż są uzależnieni od decyzji dwóch dominujących w świecie zachodnim producentów uzbrojonych BSP, tj. USA i Izraela. Nawet Wielka Brytania, budując dobrze oceniany i wszechstronny system Watchkeeper, nie zdecydowała się na uzbrojenie swoich BSP i od 2007 roku korzysta z dziesięciu MQ-9 zakupionych w USA.

W 2009 roku Turcy założyli firmę lotniczą Baykar, która opracowała bojowy BSP średniego zasięgu TB2 Bayraktar. Jest to platforma, która może spędzić 24 godziny w powietrzu. BSP jest tani, łatwy do wykonania i dobrze przygotowany do realizacji swoich zadań. To nie wszystko. Podziw wzbudza szeroki wybór wyposażenia, który czyni z tej platformy groźny środek przeznaczony do wykonywania precyzyjnych ataków. To przede wszystkim pociski Smart Micro Munition MAM-L, mała kierowana bomba przeciwpancerna o zasięgu około 10 km z bardzo dokładnym systemem nawigacji laserowo-GPS, który kieruje nią do celu z dokładnością do metra. Turcja już w zeszłym roku sprzedała Ukrainie 12 egzemplarzy tego typu BSP i trzy mobilne centra dowodzenia za 69 mln dolarów. Należy przyjąć, że za jeden bezzałogowy statek powietrzny TB2 zapłacono mniej niż 6 mln dolarów. Jest to około jedna trzecia kosztów przeznaczonych na bardzo podobne platformy wykorzystywane przez siły zbrojne USA, czyli BBSP MQ-9 Reaper, które są sprzedawane jedynie zaakceptowanym przez Kongres sojusznikom USA za około 16 mln dolarów za sztukę.

W ubiegłym roku prezydent Turcji podpisał rozporządzenie o przyznaniu dodatkowych funduszy na rozwój tureckich bezzałogowych statków powietrznych. *Dekret 1506* ma umożliwić Turcji uniezależnienie się od zewnętrznych dostawców oraz eksport własnych rozwiązań technicznych. Wartość przyznanych prezydenckim rozporządzeniem środków to 600 mln lir (ponad 105 mln dolarów). Mają one mieć postać nie tylko dopłat bezpośrednich, lecz także ubezpieczeń, zwolnień z podatków czy zwrotów cła.

Fundusze zostały przyznane na dalszy rozwój dwóch ważnych dla obronności Turcji systemów: Bayraktar TB2 i Akinci. Obie konstrukcje bezzałogowe są uzbrojonymi BSP klasy średni pułap i duża długotrwałość lotu MALE (Akinci bywa określany jako MALE/HALE – *Medium Altitude/High Altitude Long Endurance*). BBSP TB2 może wykonywać lot do wysokości 7200 m, BBSP Akinci – 12 km. Obydwie maszyny mogą przebywać w powietrzu przez 24 godziny.

BBSP TB2 jest już w pełni operacyjny. Był już używany bojowo, np. w Libii oraz Syrii. BBSP Akinci, rozwijany wespół z Ukrainą, jest z kolei większy (20 m rozpiętości skrzydeł wobec 12 m TB2 oraz 12 m długości kadłuba Akinci wobec 6,5 m TB2). Pociągnęło to za sobą konieczność zastosowania dwóch turbowałowych silników dla większego BSP.

Obydwa BBSP mają możliwość przenoszenia szerokiej gamy środków bojowych, w tym pocisków rakietowych Cirit oraz lekkich bomb kierowanych MAM-L i MAM-C. BSP Akinci ma też mieć możliwość przenoszenia kierowanych i niekierowanych wersji bomb typu Mk.81 i Mk.82, a według planów również pocisków manewrujących Roketsan SOM (turk.: Satha Atılan Orta, ang. Stand Off Missile). Co nie mniej ważne, oba typy BBSP będą dostosowane do przenoszenia systemów rozpoznawczych ELINT/SIGINT (ELectronical INTelligence/SIGnal INTelligence).

Jak wynika z zaprezentowanych przykładów rozwoju konstrukcji platform bezzałogowych, należałoby się zastanowić, jaką drogą mają pójść nasze siły zbrojne? Czy zdecydować się zakup tych środków walki za granicą, uzależniając się coraz bardziej od niepewności regularnych dostaw części zamiennych, czy wykorzystać możliwości rodzimego przemysłu, który z pewnością jest w stanie zaspokoić ich potrzeby. ■

Współpraca cywilno-wojskowa a zagrożenia asymetryczne

WSPÓŁCZESNE KONFLIKTY ZBROJNE CHARAKTERYZUJĄ SIĘ TYM, ŻE DZIĘKI SZEROKIEMU DOSTĘPOWI DO ŚRODOWISKA INFORMACYJNEGO ZNACZENIE LUDNOŚCI CYWILNEJ W ICH PROWADZENIU SIĘ ZWIĘKSZA.

ppłk Tomasz Kowal

Autor jest w dyspozycji dowódcy 12 Brygady Obrony Terytorialnej.

W ciągu dziesięciu lat od rozpoczęcia interwencji w Afganistanie do 2011 roku siły sojusznicze zaangażowane w operację „Trwała wolność" (*Enduring Freedom*) oraz ISAF przeznaczyły nieproporcjonalnie duże środki, próbując sprostać wyzwaniom stawianym przez przeciwnika prowadzącego tzw. wojnę pchły. Ocenia się, że na początku 2012 roku w walkę z rebeliantami było zaangażowanych około 432 tys. żołnierzy i funkcjonariuszy. W tym 130 tys. żołnierzy NATO, 300 tys. żołnierzy i funkcjonariuszy Afgańskich Sił Bezpieczeństwa i 12 tys. Afgańczyków uczestniczących w programie Afgan Local Police[1].

Stany Zjednoczone ponadto przeznaczały około 100 mld dolarów rocznie na sfinansowanie zarówno prowadzonej operacji, jak i wdrażanie projektów rozwojowych. Siły przeciwnika określano na około 20–40 tys. bojowników (relacja 11 do 1 po stronie sił przeciwrebelianckich), a środki finansowe szacowano na równowartość 100–200 mln dolarów rocznie (relacja 500 do 1 na korzyść rebeliantów).

Miarą skuteczności podejmowanych działań są dane udostępnione przez amerykański Departament Obrony w dokumencie *Addendum to SIGAR's January 2018 Quarterly Report to the United States Congress.* Wynika z nich, że administracja afgańska kontroluje 55,8% z ogólnej liczby dystryktów 407 dystryktów identyfikowanych przez dowództwo operacji „Resolut Support", talibowie – 14%, a 30% jest uznawanych za obszary sporne. Przedstawione dane wskazują na skalę wyzwań stwarzanych przez zagrożenia asymetryczne. Niezależnie od wielkości tego zjawiska, celowe jest podkreślenie znaczenia ludności cywilnej w wysiłkach zmierzających do ich neutralizacji. Skuteczne przeciwdziałanie zagrożeniom asymetrycznym wymaga zrozumienia, że społeczeństwo ma wymiar krytyczny.

ZAKRES POJĘCIOWY

Zgodnie z definicją przedstawioną w *Doktrynie działań połączonych D/01 (C)*, zagrożenia asymetryczne są definiowane jako *zagrożenia wynikające*

1 *Afgan Local Police* – lokalne afgańskie siły samoobrony tworzone zgodnie ze strukturą plemienną (milicja plemienna). Formowana i szkolona przez *Combined Forces Special Operations Component Command – Afghanistan* (CFSOCC-A) celem obrony własnych miejscowości przed atakami rebeliantów oraz umożliwienia afgańskiej policji przejścia do działań ofensywnych.

ADAM ROIK
COMBAT CAMERA DORSZ

ZMIANĘ W PODEJŚCIU DO LUDNOŚCI CYWILNEJ W KONFLIKTACH ZBROJNYCH PRZYNIESIE OPRACOWANA PRZEZ NATO ALLIED COMMAND TRANSFORMATION KONCEPCJA OCHRONY LUDNOŚCI CYWILNEJ (*CONCEPT FOR THE PROTECTION OF CIVILIANS*).

z możliwości zastosowania różnych środków i metod w celu osiągnięcia lub neutralizacji silnych punktów przeciwnika, wykorzystując jednocześnie jego słabości, w celu uzyskania niewspółmiernych wyników[2]. W myśl tej definicji zagrożenie asymetryczne polega głównie na[3]:

– *naturze przeciwnika, który może być trudny do rozpoznania, odróżnienia, identyfikacji i zaatakowania lub nawet podjęcia negocjacji;*

– *odmiennym charakterze ideałów, kultury i/lub celów przeciwnika, które mogą być sprzeczne z wartościami, priorytetami prawnymi, moralnymi ograniczeniami członków Sojuszu;*

– *niekonwencjonalnych metodach, które może zastosować przeciwnik w celu przeciwstawienia się przewadze jakościowej i ilościowej*.

W tym samym dokumencie podkreśla się prawdopodobieństwo coraz większego angażowania sił zbrojnych w zwalczanie zagrożeń asymetrycznych oraz sił stosujących terror zarówno w wymiarze wewnętrznym, jak i poza granicami własnego państwa.

Podobną w treści definicję zagrożeń asymetrycznych można znaleźć w amerykańskim podręczniku wojsk specjalnych, dotyczącym działań niekonwencjonalnych FM 3-05.130 (*Army Special Operations Forces Unconventional Warfare*). Zwraca się w nim uwagę na wykorzystanie różnic, które wynikają z odmiennych struktur organizacyjnych, stosowanych środków walki, zdolności oraz akceptowanych przez różne strony wartości oraz norm moralnych i etycznych[4].

Pochodnymi definicji zagrożeń asymetrycznych będą objaśnienia terminu *konflikt asymetryczny*. W wymienionym dokumencie określa się, że w konflikcie tego typu potencjały przeciwnych stron nie są lustrzanym odbiciem, a strona słabsza (niezdolna do odniesienia zwycięstwa w konfrontacji konwencjonalnej) jest zmuszona szukać powodzenia swoich działań przez zastosowanie metod eksploatujących słabości przeciwnika.

Bardzo ciekawą i jednocześnie zwięzłą w swojej treści definicję autorstwa dr. Roda Thorntona przed-

2 *Doktryna działań połączonych D/01 (C)*, Warszawa 2009, Szkol. 213/2009, s. C-8.

3 Ibidem, s. 21.

4 *Army Special Operations Forces Unconventional Warfare FM 3-05.130*, 30.09.2008, s. Glossary-9.

stawiono w opracowaniu *Russian New Generation Warfare Handbook*, stworzonym przez Asymmetric Warfare Group Armii Stanów Zjednoczonych. Aby uniknąć niewłaściwego zrozumienia jej znaczenia, zostanie tu zacytowana w oryginale: […] *asymmetric warfare is violent action undertaken by the "have-nots" against the "haves" whereby the have-nots, by the state or sub-state actors, seek to generate profound effects – at all levels of warfare (however defined), from the tactical to strategic – by employing their own specific relative advantages against the vulnerabilities of much stronger opponents. Often this will mean that the weak will use the methods that lie outside the "norms" of warfare, methods that are radically different*[5].

Warto też zaznaczyć, że asymetryczność nie zawsze oznacza nierówność. Przykład zaangażowania Sił Zbrojnych Federacji Rosyjskiej w konflikt na Ukrainie dowodzi, że asymetryczne metody walki mogą być stosowane również przez stronę silniejszą. Można zatem założyć, że działania podejmowane w celu zwalczania zagrożeń asymetrycznych (pokonania przeciwnika w konflikcie asymetrycznym) to bardzo ogólne w swoim znaczeniu pojęcie, opisujące pełen zakres środków mogących mieć charakter polityczny, ekonomiczny, militarny lub działań informacyjnych. Zazwyczaj będą one stosowane jako kombinacja kilku lub, jak w wypadku afgańskim, wszystkich czynników.

Działania przeciwrebelianckie w *Doktrynie AJP-3.4.4* (*Allied Joint Doctrine for Counterinsurgency* – COIN) przedstawiono jako miejsce konfrontacji z przeciwnikiem stosującym asymetryczne metody walki.

ŚRODOWISKO CYWILNE

W *Doktrynie prowadzenia operacji połączonych D-3 (B)* środowisko operacyjne jest zdefiniowane jako *zbiór warunków, okoliczności i czynników wpływających na wykorzystanie zdolności i decyzje dowódcy*[6]. Zestawiając tę definicję z uwarunkowaniami, w jakich prowadzone są konflikty zbrojne, można stwierdzić, że pozyskanie wsparcia ludności cywilnej (zwłaszcza kontroli nad nią) jest jednym z zasadniczych czynników warunkujących uzyskanie powodzenia. Dla przeciwnika stosującego strategię asymetryczną prawdziwe będzie stwierdzenie, że środkiem ciężkości działań jest ludność cywilna, a obszarem jej prowadzenia – środowisko cywilne.

Posłużę się przykładem afgańskich talibów, których intensywność działań powinna odpowiedzieć na pytanie: *dlaczego skuteczne przeciwdziałanie zagrożeniom asymetrycznym (w tym prowadzenie operacji przeciwrebelianckich) powinno być koncentrowane na społeczeństwie*[7]. Do tych czynników należy zaliczyć następujące:

– ugrupowanie rebelianckie wymaga relacji z ludnością cywilną zachowującą się w pożądany przez nie sposób (wynikający m.in. z wspólnej ideologii, wspólnoty kulturowej itp.). Będzie się ona charakteryzować biernym przyzwoleniem na prowadzenie działań, nieudzielaniem informacji o własnej aktywności, podatnością na oddziaływanie informacyjne. Brak tego czynnika może mieć konsekwencje w postaci zaniku aktywności rebeliantów lub jej niezaistnienia;

– w przeciwieństwie do rebeliantów, którzy osiągnęli wysoki poziom mobilności (przeciwnik *jest płynny*), dla lokalnych społeczności charakterystyczny jest osiadły, dowiązany do własnych osad tryb życia (ludność *jest stała*), dlatego kontrola społeczeństwa – przez afgańską administrację i siły bezpieczeństwa wspierane przez siły sojusznicze – jest osiągalna, a całkowita neutralizacja aktywności przeciwnika – niemożliwa;

– wysoki poziom mobilności przeciwnika oraz jego związek z ludnością cywilną rejonu, w którym prowadzi działania, wpływa na jego zdolność do kontroli poziomu własnych strat. Całkowita, fizyczna eliminacja przeciwnika, w przypadku koncentracji działań wyłącznie na rebeliantach, jest dla sił walczących z zagrożeniem asymetrycznym nieosiągalna (*enemy-centric approach*);

– charakterystyczne dla rejonów objętych aktywnością rebeliantów jest występowanie wielu grup przeciwnika, które różnią się od siebie pod względem potencjału, struktur organizacyjnych i motywacji działań. W ujęciu ogólnym społeczeństwo będzie jednorodne, stąd wniosek, że przeciwnik może nie zostać poprawnie zidentyfikowany. Poznanie ludności cywilnej (w tym czynników eksploatowanych przez rebeliantów celem uzyskania wsparcia prowadzonych działań) jest wykonalne.

Dlatego też efektywne przeciwdziałanie współczesnym zagrożeniom asymetrycznym zakłada uznanie znaczenia środowiska cywilnego jako czynnika kluczowego dla osiągnięcia powodzenia. Znaczenie tego środowiska wymaga uzupełnienia o stwierdzenie zawarte w opracowanej w CIMIC Centre of Excellence (Haga, Holandia) *Doktrynie współpracy cywilno-wojskowej* (*Allied Joint Doctrine for Civil-Military Cooperation* – AJP- 3.19), zgodnie z którym każdy atak powoduje efekt w środowisku cywilnym[8]. Mimo że jest ono przedstawione w części opisującej współpracę cywilno-wojskową (*Civil- Military Cooperation* – CIMIC) w środowisku działań powietrznych, dostrzegalna jest prawdziwość tego stwierdzenia dla aktywności we wszystkich domenach pola walki.

5 *Russian New Generation Warfare Handbook,* Asymmetric Warfare Group, December 2016, s. 3–4.

6 *Doktryna prowadzenia operacji połączonych D-3(B),* Bydgoszcz 2015, Szkol. 918/2015, Słownik-11.

7 D. Kilcullen, *Counterinsurgency*, Nowy Jork 2010, Oxford University Press, s. 7–10

8 *Allied Joint Doctrine for Civil-Military Cooperation AJP-3.19, Edition A Version 1*, November 2018, s. 3–7.

Definicja zamieszczona w *AJP-3.19* określa CIMIC jako zestaw zdolności integralnych z działaniami podejmowanymi dla osiągnięcia zakładanych celów operacji i umożliwiająca dowództwom NATO efektywne uczestnictwo w szerokim spectrum interakcji cywilno-wojskowej (*civil-military interaction*) z różnorodnymi podmiotami pozawojskowymi.

W związku z tym współpraca cywilno-wojskowa w operacji sił Sojuszu Północnoatlantyckiego w Islamskiej Republice Afganistanu wynikała z następujących czynników: specyfiki środowiska operacyjnego oraz rodzaju prowadzonej operacji (z uwzględnieniem jej społeczno-centrycznego imperatywu).

Skuteczna realizacja współpracy cywilno-wojskowej w przeciwdziałaniu zagrożeniom asymetrycznym wymagała spełnienia trzech podstawowych funkcji[9]:

– działalności łącznikowej między siłami własnymi a środowiskiem cywilnym,

– wsparcia sił własnych

– wsparcia podmiotów pozawojskowych i środowiska cywilnego.

Francuska publikacja *Doctrine for counterinsurgency at the tactical level* charakteryzuje współpracę cywilno-wojskową w operacji przeciwrebelianckiej jako *uczestnictwo w izolowaniu rebeliantów od ludności cywilnej celem pozbawienia przeciwnika źródła nowych rekrutów, zasobów, informacji rozpoznawczych i wiarygodności, a jednocześnie rozwinięcia lepszych relacji między środowiskiem cywilnym a wojskami własnymi*[10]. Definicja ta w sposób właściwy wpisuje się w warunki konfliktu afgańskiego. Podkreślenia wymaga fakt, iż siłą napędową przeciwnika jest głównie słabość instytucji państwowych, będąca efektem ich niezdolności do zapewnienia ludności jej podstawowych potrzeb (zwłaszcza potrzeby poczucia bezpieczeństwa i zdolności do rozstrzygania konfliktów). Dążąc do osiągnięcia tego celu, będzie on próbował utrzymać efektywność władz afgańskich na możliwie najniższym poziomie, wprowadzając jednocześnie własne, *nielegalne* struktury bezpieczeństwa, administrację i sądownictwo.

OBSZARY ODDZIAŁYWANIA

Obszerność problematyki zagrożeń asymetrycznych powoduje brak możliwości kompleksowego zdefiniowania ich środka ciężkości. Przykładem niech będzie tzw. Państwo Islamskie (ISIS), które wykorzystuje w swoich działaniach asymetryczne metody walki. Na przestrzeni ostatnich lat w opracowaniach dotyczących tego zagadnienia dominowały następujące poglądy:

– potencjał militarny organizacji – definiowany jako siła wysoce zmotywowana, mająca doświadczenie wyniesione z walki, konieczna do utrzymania i kontroli zajętych obszarów oraz nadania im cech państwowości. Wsparcie udzielane przez ludność cywilną powinno być tu identyfikowane jako *critical vulnerability* i traktowane jako czynnik kluczowy w pokonaniu ISIS;

– ideologia – rozumiana jako czynnik generujący napływ bojowników, określający ich wolę walki oraz powodujący, że ludność kontrolowanych obszarów będzie poddawała się kontroli organizacji i udzielała jej niezbędnego wsparcia (sunnici w Iraku i Syrii);

– efektywne działania informacyjne, których skuteczności dowodzi choćby upadek Mosulu w czerwcu 2014 roku. Należy jednak zaznaczyć, że jednym z najważniejszych obiektów oddziaływania informacyjnego ISIS jest sunnicka ludność Iraku i Syrii, a opresyjne stanowisko rządów w Bagdadzie i Damaszku w stosunku do sunnitów oraz ich marginalizacja były eksploatowane celem zdobycia sojuszników wspierających aktywność *armii kalifatu*, pozyskania informacji wywiadowczych i rozpoznawczych oraz prowadzenia działań nieregularnych na zapleczu przeciwnika;

– ludność sunnicka w Iraku i Syrii – przyszły (lub aktualny) środek ciężkości, określony na podstawie obserwacji tendencji rozwojowych organizacji oraz jej prawdopodobnych zdolności rezyliencyjnych, prowadzących ISIS do klasycznych działań rebelianckich (*insurgency*).

Przecięcie relacji między społecznościami sunnickimi a organizacją ISIS w dużym stopniu ograniczyłoby jej możliwości działania lub nawet doprowadziłoby do jej zaniku.

Pozyskanie wsparcia ludności cywilnej (w szczególności kontroli nad nią) jest zatem czynnikiem warunkującym osiągnięcie powodzenia. Potwierdzeniem tego założenia są wnioski z wojny domowej w Syrii. Zdaniem redaktora Łukasza Wójcika, autora artykułu poświęconego tematyce sytuacji ludności cywilnej w konflikcie syryjskim, *przyłączenie się do konfliktu Iranu, Arabii Saudyjskiej, USA, Rosji i ostatnio Turcji sprawiło, że wszelkie klasyczne teorie o wojnie domowej nie mają tu już zastosowania. Zniknęły znane z „układu zamkniętego czynniki, które by tę wojnę tonowały i sprzyjały jej zakończeniu – jak na przykład zależność od miejscowej ludności. W izolowanej wojnie domowej nie można wygrać bez jej poparcia, zarówno politycznego, jak i logistycznego. Cywile dają schronienie, żywność, dlatego warto o nią dbać*[11]. W swojej publikacji powołuje się on na opinię amerykańskiego politologa Patricka H. Regana, zgodnie z którą *dopóki wojna domowa toczy się w izolacji, koniec nie*

9 Ibidem, s. 2–7.

10 *Doctrine for counterinsurgency at the tactical level*, April 2010, s. 62.

11 Ł. Wójcik, *Niech się wypali*, https://www.polityka.pl/tygodnikpolityka/swiat/1674406,1,syrie-nalezaloby-zostawic-samej-sobie-w-przeciwnym-razie-wojna-nigdy-sie-nie-skonczy.read/. 6.09.2016.

EFEKTYWNE PRZECIWDZIAŁANIE ZAGROŻENIOM **ŚRODOWISKA CYWILNEGO** JAKO CZYNNIKA

może być odległy, gdyż strony wyczerpują swój potencjał i dochodzi najczęściej do „pokoju przez wycieńczenie" („peace by exhaustion")[12].

KONFLIKT UKRAIŃSKI

W opinii dr. Adama Pomorskiego wojna hybrydowa na Ukrainie jest praktyczną realizacją głównych założeń rosyjskiej doktryny wojennej, w myśl której zasadniczym jest *osiąganie celów na terytorium przeciwnika przez próby zarządzania stymulowanym przez Rosję konfliktem wewnętrznym. Generowanie chaosu informacyjnego i społecznego aż do krwawych wojen domowych i rebelii na skalę makrospołeczną*[13].

W wypadku konfliktu w Donbasie kluczowe dla jego powodzenia wydają się być dwa czynniki, a mianowicie:

– ciągłość wsparcia udzielanego separatystom przez Federację Rosyjską;

– wsparcie ludności cywilnej (opinia publiczna) dla Donieckiej i Ługańskiej Republiki Ludowej.

Z uwagi na sytuację wewnętrzną państwa ukraińskiego przerwanie relacji przedstawionej w pierwszym punkcie jest na chwilę obecną niewykonalne. Przy założeniu, że celem rządu w Kijowie jest odzyskanie terytorium na wschodzie kraju, bardziej optymistyczna wydaje się być perspektywa zmian przekonań społecznych. Wymaga to jednak zastosowania skoncentrowanej na ludności (społeczno-centrycznej) operacji przeciwrebelianckiej. Jej głównymi założeniami – liniami działania (*Line of Operation* – LoO), mogłyby przykładowo być:

– stabilizacja polityczna – obejmująca poważne zmiany w regionie (w tym przedsięwzięcia antykorupcyjne oraz zgodne z porozumieniem *Mińsk II* wycofanie ciężkiego sprzętu z rejonu walk), prowadzone w celu udowodnienia społeczności międzynarodowej i ludności Donbasu zaangażowanie rządu ukraińskiego w rozwiązanie konfliktu, uznanie akceptowalnego poziomu autonomii regionu połączone z powrotem przedstawicieli legalnej administracji i zanegowaniem argumentu separatystów o jej niezainteresowaniu problemami regionu. W rezultacie ludność cywilna powinna nabrać przekonania o odpowiedzialności za przemoc liderów separatystów oraz destrukcyjnym wpływie Federacji Rosyjskiej na sytuację społeczną;

– progresja ekonomiczna – mająca na celu wyrównanie poziomu życia ludności cywilnej po obu stronach linii rozgraniczenia (w tym wzrost wynagrodzeń, reforma emerytalna, wsparcie przemysłu – głównego źródła dochodu – w Donbasie, obniżenie cen żywności do poziomu po stronie ukraińskiej, wzrost możliwości zatrudnienia). Przedsięwzięcia te powinny być traktowane jako mające największy potencjał zmiany opinii o władzach w Kijowie;

– rozwój gospodarczy i rekonstrukcja infrastruktury – zwiększenie pomocy międzynarodowej i krajowej dla regionu z jednoczesnym wzrostem jakości sprawowania administracji. Szybkie wdrożenie projektów rozwojowych dałoby potencjał do zapoczątkowania procesu odbudowy relacji społeczności Donbasu z administracją ukraińską oraz wzmocnienie jej pozytywnego odbioru w rejonie konfliktu. Tempo realizacji projektów będzie mierzalnym wskaźnikiem zaangażowania rządu w Kijowie;

– zaangażowanie militarne – skoncentrowane na izolacji separatystycznych zdolności do dowodzenia i kierowania własnymi siłami, koordynowaniu ich działań z wspierającymi elementami rosyjskimi oraz administrowaniu kontrolowanym obszarem.

Każde z wymienionych założeń powinno być wsparte agresywnymi działaniami informacyjnymi, które podkreślałyby jedność społeczeństwa ukraińskiego, wspólną historię, destrukcyjny wpływ Federacji Rosyjskiej i separatystów na stabilizację społeczną w regionie. Wszystkie te czynniki uwzględniają kluczową rolę ludności cywilnej, a celem strategicznym będzie odtworzenie integralności terytorialnej państwa ukraińskiego.

W tak zdefiniowanych przedsięwzięciach zadania elementów CIMIC mogą być wykorzystywane do:

– zwiększenia świadomości sytuacyjnej dzięki dostarczeniu analizy i oceny środowiska cywilnego i podmiotów pozawojskowych;

– zapewnienia dowódcom ukraińskim prowadzącym operację przeciwrebeliancką efektywnego wsparcia w interakcji cywilno-wojskowej;

– wsparcia administracji ukraińskiej w odbudowie relacji z ludnością cywilną Donbasu;

– koordynacji aktywności podmiotów rozwojowych (w tym również organizacji międzynarodowych, rządowych i pozarządowych oraz sektora prywatnego);

12 Ibidem.

13 A. Szostkiewicz, *Rosja nad Nilem*, https://www.polityka.pl/tygodnikpolityka/swiat/1742754,1,czwarte-wcielenie-putina.read/. 27.03.2018.

– aktywnego udziału w prowadzeniu efektywnych działań informacyjnych.

TENDENCJE ZMIAN

Zmiany w środowisku operacyjnym, w szczególności wzrost znaczenia środowiska cywilnego oraz funkcji przestrzeni informacyjnej dla rozwiązywania konfliktów, wpływają na tendencje rozwojowe w dziedzinie współpracy cywilno-wojskowej. Można do nich zaliczyć między innymi: rozwój doktrynalny, strukturalny oraz wynikający z nowego ujęcia ochrony ludności cywilnej w konfliktach zbrojnych.

ASYMETRYCZNYM ZAKŁADA UZNANIE ZNACZENIA KLUCZOWEGO DLA OSIĄGNIĘCIA POWODZENIA

Przedstawiona w artykule nowa definicja współpracy cywilno-wojskowej wskazuje na zdolności adaptacyjne personelu CIMIC do wymagań złożonego środowiska operacyjnego. Ich materializacją jest również dokument *Allied Joint Doctrine for Civil-Military Cooperation AJP-3.19*[14].

W publikacji zakłada się, że NATO może być konfrontowane z przeciwnikiem działającym w sposób nieprzewidywalny i innowacyjny, wykorzystującym różne metody walki, w tym takie, które nie są zawarte w granicach międzynarodowego prawa humanitarnego konfliktów zbrojnych czy ogólnie akceptowanych norm moralnych i etycznych. Autorzy dokumentu zakładają ponadto, że potencjalny przeciwnik, angażując się w działania nieregularne i asymetryczne, może wykorzystywać podmioty pozawojskowe celem maksymalizacji efektów podejmowanych przez siebie działań oraz osiągania własnych celów. Prowadzona przez niego aktywność w bezpośredniej relacji z ludnością cywilną będzie miała poważne konsekwencje dla sił NATO. Ich przykładem może być utrudniona poprawna identyfikacja przeciwnika (zwłaszcza takiego, który walczy w obszarach zurbanizowanych, wśród grup społecznych wspierających jego aktywność), prowadząca do niezamierzonych strat wśród ludności cywilnej (*collateral damage*). Skuteczna realizacja zadań i osiąganie zakładanych celów operacyjnych będą wymagały wysokiej świadomości sytuacyjnej i szczegółowego zrozumienia sytuacji operacyjnej (w tym kontekstu społecznego, dynamiki konfliktu oraz identyfikacji podmiotów pozawojskowych pomocnych w rozwiązywaniu konfliktów[15].

Potwierdzeniem wpływu środowiska cywilnego na prowadzenie działań jest przedstawienie współpracy cywilno-wojskowej jako funkcji połączonej. Tradycyjnie CIMIC jest wiązany z operacjami prowadzonymi na lądzie. Jako funkcja połączona może mieć zastosowanie także w środowisku morskim i powietrznym. Z uwagi na zdolność umożliwiającą sprawne uczestnictwo w interakcji cywilno-wojskowej, CIMIC jest wskazywany również jako narzędzie mające potencjał do poruszania się wśród podmiotów aktywnych w przestrzeni kosmicznej i cyberprzestrzeni[16].

Również w *AJP-3.19* znacznie poszerza się znaczenie elementów środowiska cywilnego, zmieniając funkcjonujące dotychczas pojęcie *podmioty cywilne* na *podmioty pozawojskowe*. Celem utrzymania pojemności tego terminu nie podaje się precyzyjnej jego definicji. Zbiór podmiotów pozawojskowych zawiera w sobie (lecz nie jest nimi ograniczony) następujące elementy:

– organizacje międzynarodowe (*International Organizations*),

– Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężyca (*International Red Cross* and *Red Crescent Movement*),

– organizacje pozarządowe (*non governmental organizations*),

– organizacje rządowe (*governmental organizations*),

– organizacje przestrzegania porządku prawnego (*law enforcement agencies*),

– organizacje obrony cywilnej (*civil defence organizations*),

– podmioty lokalne i administracja lokalna (*local actors and authorities*),

– sektor prywatny (*private sector*).

Doktryna identyfikuje tzw. *cross-cutting topics*, czyli charakterystyczne dla środowisk operacyjnych obszary, które mogą wpływać na prowadzone działa-

14 *AJP-3.19* jest trzecią od 2003 roku doktryną współpracy cywilno-wojskowej. Przyjmuje się, że pierwsza z nich, *AJP-9*, powstała na podstawie doświadczeń zebranych w trakcie interwencji Sojuszu Północnoatlantyckiego w Bośni i Kosowie. Jej kolejna edycja. – *AJP-3.4.9* – została opublikowana w 2013 roku i zawiera wyraźny wpływ operacji w Republice Iraku oraz Islamskiej Republice Afganistanu; w *AJP-3.19* jest dostrzegalna analiza środowisk operacyjnych w Syrii, Libii i na Ukrainie, kryzysu uchodźczego na południowej flance NATO, zagrożenia terrorystycznego w Europie oraz coraz mocniej obecnych przestrzeni kosmicznej i cybernetycznej.

15 *Allied Joint Doctrine for Civil – Military Cooperation AJP-3.19...*, op.cit., s. 1–2.

16 Ibidem, s. 3-9–3-10.

nia w różnoraki sposób, ale pozostają – z uwagi na poziom skomplikowania i cechy charakterystyczne – poza strefą wyłącznie wojskowego zakresu odpowiedzialności. Zgodnie z treścią dokumentu należą do nich[17]:

– ochrona ludności cywilnej (*protection of civilians*),

– ochrona i bezpieczeństwo kobiet (*women, peace and security*),

– uczestnictwo dzieci w konfliktach zbrojnych (*children and armed conflict*),

– ochrona dóbr kulturowych (*cultural property protection*),

– działania wzmacniające administrację i przedsięwzięcia antykorupcyjne (*building integrity*).

Przygotowując swoje siły zbrojne do wymogów zmiennego i złożonego środowiska operacyjnego, wybrane państwa NATO podjęły próby dostosowania swoich struktur do efektywnej realizacji zadań z zakresu oddziaływania niekinetycznego. Przykładem mogą tu być brytyjska 77 Brygada i amerykańskie jednostki SFAB (*Security Force Assistance Brigade*).

77 Brygada jest jednostką sformowaną w 2015 roku (w ramach koncepcji *Army 2020*), której obszarem odpowiedzialności jest *non – lethal warfare*. Jest ona przeznaczona do wsparcia misji stabilizacyjnych. W opinii byłego ministra obrony Wielkiej Brytanii Marka Francois jednostka została sformowana z połączenia istniejących i rozwijających się zdolności celem umożliwienia skutecznej odpowiedzi na wyzwania współczesnych konfliktów. Zapewnia ona możliwość oddziaływania na przeciwnika w sposób inny niż kinetyczny. Następczyni Marka Francois, Penny Morduant, stwierdziła, że jednostka wykorzystuje kombinację sojuszniczych i brytyjskich doktryn, włączając w nią obszary dotyczące współpracy cywilno-wojskowej, wsparcie bezpieczeństwa, operacje stabilizacyjne, działania informacyjne, wsparcie pokoju i pomoc humanitarną.

Można założyć, że takie ujęcie jest pochodną obserwacji współczesnych środowisk operacyjnych, analiz konfliktów zbrojnych, a w szczególności relacji występującej w trójkącie: ludność cywilna–przeciwnik–środowisko informacyjne. Stąd wniosek, że środowisko cywilne i obszar działań informacyjnych w analizie aktywności przeciwnika w środowisku informacyjnym nie powinny być traktowane rozdzielnie.

W skład tej jednostki wchodzą następujące elementy:

– *The Defence Cultural Specialist Unit* (DCSU) – wsparcie procesu planistycznego przez dostarczenie behawioralnej analizy podmiotów środowiska operacyjnego, potencjalnych odbiorców prowadzonych działań informacyjnych oraz przeciwnika. Dostarcza szczegółowej informacji o motywacjach, narracji i przekonaniach wymienionych grup oraz o możliwych opcjach wsparcia własnych działań informacyjnych. Wśród zadań elementu znajduje się również doradztwo kulturowe i lingwistyczne;

– *Task Group* – wsparcie w postaci dywizyjnych, brygadowych (*Division/Brigade Information Activity & Outreach Cell*), batalionowych (*Information Activity & Outreach Team*) elementów działań informacyjnych oraz współpracy cywilno-wojskowej (*Tactical Engagement Team*). Ponadto w składzie Task Group znajduje się zespół walki informacyjnej (*Information Warfare Team*), zapewniający wsparcie na szczeblu armii i resortu obrony, oraz zespół szkoleniowo-doradczy (*Training and Advisory Team*), ukierunkowany na rozwijanie zdolności do prowadzenia działań informacyjnych w elementach strukturalnych brytyjskich sił zbrojnych;

– *Digital Operations Group* (*Digi Ops*) – zapewnienie specjalistycznych zdolności umożliwiających oddziaływanie przez cyfrowe kanały komunikacyjne;

– *Operational Media and Communication Group* – dostarczenie zespołów *Combat Camera* oraz oficerów zdolnych do prowadzenia ekspertyz środowiska medialnego celem wsparcia komunikacji strategicznej;

– *Outreach Group* – zapewnienie specjalistów w wybranych obszarach wiedzy, użytecznych we wsparciu: współpracy cywilno-wojskowej, ochrony dóbr kulturowych, bezpieczeństwa ludności cywilnej oraz działań stabilizacyjnych i odbudowy;

– *The Staff Corps* – specjaliści (oficerowie rezerwy) w zakresie doradztwa ekonomicznego, finansowego oraz politycznego.

Prawdopodobną zmianę w podejściu do ludności cywilnej w konfliktach zbrojnych przyniesie opracowana przez NATO Allied Command Transformation *Koncepcja ochrony ludności cywilnej* (*Concept for the Protection of Civilians*). Konsekwencją zatwierdzenia i opublikowania tego dokumentu powinny być zmiany w systemie szkolenia elementów CIMIC oraz zwiększenie zdolności do prowadzenia współpracy cywilno-wojskowej oddziałów i związków taktycznych. Ma to zostać osiągnięte dzięki stworzeniu modelu ułatwiającego zrozumienie głównych zasad ochrony ludności cywilnej. Tak pojmowana koncepcja ma przedstawić specyfikę ochrony ludności w konfliktach zbrojnych oraz dostarczyć dowódcom użytecznych wskazówek w trakcie planowania i prowadzenia operacji.

Podstawą stworzenia *Koncepcji…* jest założenie, że ochrona ludności cywilnej w trakcie konfliktu zbrojnego nie powinna być prowadzona wyłącznie z powodów moralnych, prawnych i politycznych, lecz również jako środek skutecznie wspierający osiągnięcie powodzenia w działaniu. Dlatego też

17 Ibidem, s. B-1.

w przedsięwzięciach podejmowanych celem zapewnienia tejże ochrony znaczenie prymarne ma zrozumienie unikatowych cech określonych społeczności obecnych w środowisku operacyjnym. Wśród nich są wymienione: kultura, historia, demografia, czynniki decydujące o ich sile i słabościach. Ponadto w operacjach reagowania kryzysowego (*NATO non – article 5 crisis response operations*) istotne również będzie zdefiniowanie źródeł niestabilności (*sources of instability*) oraz przyczyn konfliktu (*drivers of conflict*)[18].

Ochrona ludności cywilnej zawiera w sobie wszelkie działania podejmowane w celu uniknięcia i zminimalizowania negatywnych skutków, które mogą powstać w środowisku cywilnym w efekcie działań własnych, oraz działania ukierunkowane na ochronę przed przemocą (lub zagrożeniem jej użycia) przez pozostałych uczestników działań zbrojnych. W ich skład wchodzi szeroki zakres aktywności (z użyciem siły włącznie) stosowanych jako środki zapobiegające, odstraszające, uprzedzające oraz wykorzystywane w reakcji na zaistniałą sytuację, w której ludność cywilna ucierpiała lub jest zagrożona przemocą.

Proponowany model *Koncepcji…* podkreśla konieczność holistycznego zrozumienia środowiska cywilnego w celu stworzenia świadomości na poziomie strategicznym we wszystkich domenach pola walki oraz identyfikacji zagrożeń, wrażliwości, mocnych stron i odporności (*resilience*) ludności cywilnej. Jest to możliwe dzięki wykorzystaniu trzech różnych, ale jednocześnie współzależnych perspektyw, takich jak[19]:

– mitygowanie cierpienia (szkód powstałych w rezultacie działań militarnych (*Mitigate Harm* – MH);

– zapewnienie dostępu do podstawowych potrzeb egzystencjalnych (*Facilitate Access To Basic Needs* – FABN);

– uczestnictwo w zapewnieniu bezpiecznego środowiska operacyjnego (*Contribute to a Safe and Secure Environment* – C-SASE).

Wymienione czynniki mają pomóc w informowaniu, które jest elementem procesu planowania, jak również w dostarczaniu konkretnych danych (*Lines of Effort* – LoE) do prowadzenia operacji, by efektywnie zapewnić wielowymiarową naturę zadań związanych z ochroną ludności cywilnej.

Aspekty ochrony ludności cywilnej powinny być postrzegane jako integralna część każdego kryzysu lub konfliktu nawet w wypadku braku wyraźnego mandatu jej ochrony.

Aby osiągnąć zakładane cele operacji, należy umieć sobie radzić z trzema różnymi grupami ludzkimi zaangażowanymi w kryzys (konflikt), czyli: sprawcami przemocy (*Perpetrators of Violence*); ludnością cywilną, w tym osobami i organizacjami zajmującymi się dostarczaniem pomocy (*The Civilians and Aid Workers*), oraz z lokalną administracją (*Government and Institutions*).

WNIOSKI

Przedstawione zjawiska wydają się dowodzić właściwego kierunku zmian w myśleniu o współpracy cywilno-wojskowej. Potwierdzeniem ich efektywności będą analizy aktualnych i przyszłych zaangażowań w rejonach konfliktów. Jednak już teraz można założyć, że są one w większym stopniu przystosowane do wyzwań stawianych przez współczesne środowisko operacyjne.

Niezależnie od tego, czy opisywane zjawiska spowodują zmiany strukturalne w elementach Sił Zbrojnych RP zajmujących się współpracą cywilno-wojskową, warto zwiększyć ich skuteczność w realizacji zadań dzięki:

– integracji szkolenia istniejących elementów CIMIC i działań psychologicznych (PSYOPS) oraz potwierdzeniu uzyskanego poziomu wyszkolenia w ramach wspólnego uczestnictwa w ćwiczeniach;

– prowadzeniu szkolenia ukierunkowanego na zwiększenie możliwości analitycznych zachowania środowiska cywilnego i jego wpływu na sytuację operacyjną;

– relacji wojsk obrony terytorialnej ze środowiskiem cywilnym. Niezbędne jest wyposażenie tego rodzaju sił zbrojnych w zdolności umożliwiające skuteczną realizację zadań współpracy cywilno-wojskowej w czasie pokoju, kryzysu i wojny;

– szkoleniu ukierunkowanemu na zwiększenie świadomości wpływu środowiska cywilnego na prowadzone działania, w tym ochrony ludności cywilnej w konfliktach zbrojnych;

– dążeniu do wsparcia wszystkich dywizji i brygad wojsk operacyjnych[20] i brygad obrony terytorialnej w elementy wsparcia CIMIC i PSYOPS;

– rozpatrywaniu ochrony ludności cywilnej w trakcie planowania i prowadzenia działań nie tylko ze względów prawnych i moralnych, lecz również jako czynnik wspierający osiąganie zakładanych celów operacji;

– właściwemu, z uwagi na coraz wyraźniejszą obecność podmiotów pozawojskowych w środowisku operacyjnym, zwiększaniu zdolności interakcyjnych elementów CIMIC;

– zasadnemu, szerszemu włączaniu podmiotów pozawojskowych we wsparcie w realizacji zadań i osiąganiu zakładanych celów zarówno w trakcie ćwiczeń, jak i poza ich granicami. ■

NATO MOŻE BYĆ KONFRONTOWANE Z PRZECIWNIKIEM DZIAŁAJĄCYM W SPOSÓB NIEPRZEWIDYWALNY I INNOWACYJNY, WYKORZYSTUJĄCYM RÓŻNE METODY WALKI, W TYM TAKIE, KTÓRE NIE SĄ ZAWARTE W GRANICACH MIĘDZYNARODOWEGO PRAWA HUMANITARNEGO KONFLIKTÓW ZBROJNYCH.

18 *Concept for the Protection of Civilians*, April 2018, s. 8.

19 Ibidem, s. 6.

20 Obecnie, w wypadku współpracy cywilno-wojskowej, dotyczy to wyłącznie jednostek posiadających zdolność do przerzutu.

Czołgi w działaniach na rzecz wsparcia pokoju

OBECNIE POWSZECHNY JEST POGLĄD, ŻE WYKORZYSTANIE WOJSK PANCERNYCH W DZIAŁANIACH ASYMETRYCZNYCH, TYM BARDZIEJ W DZIAŁANIACH WSPARCIA POKOJU, JEST NIEEFEKTYWNE.

ppor. mgr Cyprian Kaczmarczyk

Autor jest zastępcą dowódcy kompanii czołgów w 1 Brygadzie Pancernej.

Od kilkudziesięciu lat prym w operacjach pokojowych prowadzonych pod egidą ONZ oraz w działaniach stabilizacyjnych wiedzie piechota zmotoryzowana na kołowych transporterach opancerzonych. Mimo tego ogólnego trendu niektóre państwa zdecydowały się wykorzystać w takich działaniach pododdziały czołgów nie tylko jako projekcję siły oraz czynnik odstraszający, lecz znacznie zwiększyły zdolności obrony i reakcji żołnierzy w przypadkach zagrożenia. Udokumentowane działania pozwalają ocenić techniczne aspekty użycia czołgów w określonych uwarunkowaniach. Przede wszystkim są materiałem do analizy zastosowanych rozwiązań, która pozwoli na zrozumienie ograniczeń w ich wykorzystaniu oraz ułatwi poszukiwanie sposobów zwiększania potencjału bojowego. Przemyślenia zawarte w niniejszym materiale z pewnością nie wzbogacą sposobów użycia czołgów w konflikcie zbrojnym, jednak nie można wykluczyć, że w przyszłości pododdziały te nie zostaną skierowane do działań pokojowych jedynie jako wsparcie i wzmocnienie sił lekkich.

EPIZOD DUŃSKI

Rok 1991 roku to początek rozpadu Socjalistycznej Federalnej Republiki Jugosławii. Jego wynikiem było wiele krwawych konfliktów między federacyjnymi republikami. W 1992 roku Rada Bezpieczeństwa ONZ ustanowiła więc siły ochronne UNPROFOR[1] (*United Nations Protection Force* – Siły Ochronne Organizacji Narodów Zjednoczonych). Ich celem było zahamowanie eskalacji konfliktu, początkowo na terenie Chorwacji, następnie także Bośni i Hercegowiny. Żołnierze ONZ mieli prawo użyć broni jedynie w ramach samoobrony oraz w przypadku ataków na strefy bezpieczeństwa. Mimo to w wyniku starć zginęło 167 członków wspomnianych sił.

W sierpniu 1993 roku parlament Królestwa Danii zadecydował o wysłaniu w te rejony kompanii[2] czołgów Leopard oraz 125 żołnierzy, stanowiących w większości wsparcie techniczno-administracyjne.

W siłach zbrojnych Królestwa Danii w latach dziewięćdziesiątych ubiegłego wieku kompania (szwadron) czołgów składała się z dziesięciu pojazdów: wozu dowódcy kompanii oraz trzech plutonów po trzy załogi. Czołgi, które zamierzano wykorzystać w działaniach, były to Leopardy 1A5DK-1. Towarzyszył im pojazd ewakuacji technicznej Bergepanzer 2 AVLP oraz cztery transportery piechoty M113 APCs.

Leopard 1A5DK-1 to zmodernizowany na potrzeby działań pokojowych czołg Leopard 1A5. Poprzednik Leoparda 2 był czołgiem drugiej generacji wyposażonym w: stabilizację armaty, system kierowania ogniem, system sterowania układem hydrauliki wieży, system ochrony przed BMR, noktowizor kierowcy, wyrzutnie granatów dymnych, ogrzewanie, instalację przeciwpożarową oraz telefon zewnętrzny służący do

1 Misja UNPROFOR rozpoczęła się w lutym 1992 roku, a zakończyła 31 marca 1995 roku w wyniku przekształcenia jej w trzy samodzielne misje: UNPREDEP w Macedonii, UNCRO w Chorwacji oraz UNMIBH w Bośni i Hercegowinie). Zob.: http://www.unic.un.org.pl/misje_pokojowe/unprofor.php/. 15.06.2020.

2 Według nomenklatury duńskiej był to *squadron* – odpowiednik polskiego szwadronu, pododdziału równorzędnego z kompanią. Uwaga: w niektórych siłach zbrojnych *squadron* jest odpowiednikiem polskiego batalionu. Zob.: https://en.wikipedia.org/wiki/Squadron_(army)/. 15.06.2020.

Dysponowanie odwodem w postaci pododdziału czołgów może dać przewagę siłom pokojowym podczas wykonywania mandatowych zadań.

RYS. POZYCJE SIŁ ONZ ORAZ BOSNIAN SERB ARMY (BSA)

Opracowano z użyciem: *Mapcarta,* OpenStreetMap, http://mapcarta.com/. 15.06.2020. Podstawa: *Dokumentar: Operation Bøllebank,* https://www.youtube.com/watch?v=bgHJ6uyCf8g [dostęp: 21.05.2020]; *Bøllebank i erindring,* https://www.youtube.com/watch?v=TtxtssQ401/. 21.05.2020.

komunikacji z towarzyszącą mu piechotą. Napęd stanowił wysokoprężny silnik o mocy 830 KM połączony w jeden moduł ze skrzynią biegów (tzw. *power-pack*). Specjalna konstrukcja układu wydechowego zmniejszała temperaturę spalin przed odprowadzeniem ich na zewnątrz, mieszając z powietrzem służącym do chłodzenia silnika.

Uzbrojenie stanowiła armata kalibru 105 mm oraz dwa karabiny maszynowe MG-3: jeden sprzężony z armatą, drugi umieszczony na wieży jako środek przeciwlotniczy. Zapas amunicji do armaty wynosił 60 nabojów: trzy w wieży oraz 57 w kadłubie. Działonowy dysponował stereoskopowym dalmierzem optycznym (dwie oddalone od siebie głowice optyczne, przez które obserwował teren, zapewniały mu dwa różne obrazy celu nakładane na siebie; odległość była odczytywana z pokręteł regulacyjnych).

Pojazdy Leopard 1A5DK-1, którymi mieli posługiwać się Duńczycy, zostały wyposażone w celownik termowizyjny oraz dalmierz laserowy, układy przeciwwybuchowy i klimatyzacji, pomocniczą jednostkę zasilającą (tzw. APU) oraz sprzężony z armatą reflektor halogenowy. Charakter działań wymusił ponadto białe malowanie wraz z oznakami identyfikacyjnymi o przynależności do sił ONZ. Z dziesięciu czołgów trzy wyposażono w lemiesze, kolejne trzy – ze względu na duże zagrożenie minami – w trały przeciwminowe.

Siły duńskie tworzące tzw. kompanię DANSQN (*Danish Tank Squadron*) z kilkumiesięcznym opóźnieniem, spowodowanym blokadą Serbów[3], pojawiły się w wyznaczonym rejonie działań, tj. w miejscowości Tuzla w Bośni, w lutym 1994 roku. Dwa miesiące później duński kontyngent walczył w ochronie lotniska w rejonie Tuzli z siłami serbskimi. Starcie znane jest jako operacja „Bøllebank" („Hooligan Bashing"). 29 kwietnia około godziny 22.00 serbska artyleria ostrzelała posterunek obserwacyjny Tango 2, w związku z czym podjęto działania zmierzające do jego ochrony.

Do działań skierowano siedem Leopardów (1 i 2 pluton oraz wóz dowódcy kompanii), transporter opancerzony oraz wóz dowodzenia. Trzeci pluton pozostał w odwodzie. Zgodnie z przyjętą procedurą

3 Serbowie zablokowali duńskie siły UNPROFOR w miejscowości Pancevo (okolice Belgradu w Serbii). Zdecydowano się przemieścić je transportem kolejowym przez Węgry i Austrię do Włoch, następnie drogą morską do Splitu, skąd przerzucono do miejscowości Tuzla. Zob. M. Jerchel, *Leopard 1. Main Battle Tank 1965–95*, Osprey Publications, Oxford 1995, https://books.google.pl/books?id=QMPvCwAAQBAJ&printsec=frontcover&hl=pl&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false/. 15.06.2020.

duńskie pojazdy przemieszczające się do oddalonego o 8 km od Tuzli posterunku były oświetlone, co wskazywało na ich przynależność do sił pokojowych. Ponadto na pojazdach umieszczono flagi ONZ. Liczono, że samo pojawienie się czołgów spowoduje przerwanie ostrzału[4], jednak Serbowie zorganizowali na drodze marszu zasadzkę.

Uczestniczyła w niej piechota, trzy czołgi T-55, środki przeciwpancerne i artyleria. Z chwilą gdy siły kompanii DANSQN znalazły się w wioskach Saraci i Kalesija, przeciwnik rozpoczął ostrzał środkami przeciwpancernymi. Wozy obu plutonów zajęły stanowiska ogniowe pod osłoną zabudowań (rys.). Nie wezwano wsparcia lotniczego.

Według relacji duńskich czołgistów celowniki termowizyjne umożliwiały im dokładną obserwację czołgów przeciwnika. Zgodnie z przyjętymi zasadami użycia siły ogień prowadzono jedynie do środków przeciwpancernych. Dwa czołgi dotarły do posterunku obserwacyjnego Tango 2 i tam zajęły stanowiska ogniowe. W tym momencie przeciwnik przerwał ostrzał.

Po upływie 30 min podjęto decyzję o wycofaniu się z wyjątkiem wozów na posterunku obserwacyjnym Tango 2. W czasie wycofywania się plutonu z wioski Kalesija w kierunku Saraci przeciwnik wznowił ostrzał. Rozpoczęła się ponowna wymiana ognia, która zakończyła się w chwili, gdy pocisk wystrzelony z jednego z Leopardów trafił w amunicję składowaną na ziemi. Po stronie duńskiej nie zginął nikt. Starty BSA, w zależności od źródeł, wynosiły od 9 do nawet 150 zabitych[5].

Kolejna potyczka z udziałem Leopardów miała miejsce 25 października 1994 roku[6]. Grupa zadaniowa UNPROFOR w składzie: duński pluton czołgów, szwedzki pluton zmechanizowany, jordański radar rozpoznania artyleryjskiego oraz grupa zabezpieczenia medycznego – została wysłana w rejon miejscowości Gradacac w celu zajęcia posterunku obserwacyjnego opuszczonego przez załogę. Czołgi zostały ostrzelane przez wóz T-55 Bośniacko-Serbskiej Armii (Armia Republiki Serbskiej), który Duńczycy zniszczyli ogniem prowadzonym z dział.

INCYDENT PRIZREŃSKI

Walki między Armią Wyzwolenia Kosowa i policyjnymi oddziałami Serbii i Czarnogóry doprowadziły do kryzysu humanitarnego na obszarze Kosowa. Reakcją ONZ było ustanowienie 12 czerwca 1999 roku funkcjonujących do dziś sił KFOR (*Kosovo Force*). Działający w ramach IFOR (*Implementation Force*) kontyngent niemiecki zadecydował o wykorzystaniu w początkowej fazie działań czołgów Leopard 2A5. I tak 13 czerwca po północy niemieckie siły rozpoczęły zajmowanie miasta Prizren. Wycofywanie się Serbów przebiegało zgodnie z ustaleniami, początkowo w całkowitym porządku, a lokalna ludność albańska była nastawiona przyjaźnie[7] do sił rozjemczych. Kiedy siły pokojowe dotarły do centrum miasta, zostały ostrzelane przez snajperów. Ostrzelano także czołg Leopard 2A5 oraz transporter opancerzony z grupą piechoty. Po chwili do zatrzymanych pojazdów podjechało samochodem dwóch Serbów, którzy otworzyli ogień w kierunku cywilów oraz żołnierzy sił pokojowych. Atak został odparty przy użyciu broni strzeleckiej. Lokalni mieszkańcy pochodzenia albańskiego pomogli siłom pokojowym ustalić stanowisko ogniowe snajpera ukrywającego się w kościele.

WIELE NIEWIADOMYCH

Charakter działań w trakcie operacji wspierania pokoju wymusza na żołnierzach realizację zadań z dokładnym przestrzeganiem ustalonych, niekiedy bardzo rygorystycznych, zasad użycia siły. Wykorzystanie pododdziałów czołgów w tych uwarunkowaniach pozwala na zademonstrowanie wysokiego poziomu wyszkolenia ich załóg, co powinno wpływać na deeskalację agresji i ataków którejś ze stron konfliktu. W razie konieczności odparcia ataku na siły pokojowe czołgi zapewniają dużą przewagę ogniową, a precyzyjny ogień o dużej sile rażenia może ograniczyć straty w cywilnej infrastrukturze w porównaniu z tymi, jakie mogą powstać w wyniku ataku lotniczego. Jednocześnie załogi wozów mają zapewniony duży stopień ochrony.

Konieczność ograniczania strat wśród ludności cywilnej i w infrastrukturze uniemożliwia wykorzystanie pełnych możliwości prowadzenia ognia, nawet z zachowaniem maksymalnej ostrożności. Jednak dysponowanie odwodem w postaci pododdziału czołgów może dać przewagę siłom pokojowym podczas wykonywania mandatowych zadań.

Decyzja o wysłaniu w składzie kontyngentu pododdziałów czołgów to początek trudnych przedsięwzięć logistycznych. Utrzymanie odpowiedniego poziomu gotowości bojowej wymaga zabezpieczenia remontowo-serwisowego i technicznego, zapewnienia materiałów pędnych i smarów oraz środków bojowych, w tym części zamiennych w celu wymiany elementów podlegających okresowej wymianie oraz najczęściej ulegających awarii. Może właśnie procesy logistyczne są powodem niewykorzystywania tego rodzaju wojsk w działaniach pokojowych. ■

4 L. Møller remembers: *Actually, we intended to move up with the tanks because they tend to stop the shooting* [w:] O.K. Hansen, *Operation "Hooligan bashing" – Danish Tanks at War*, http://web.archive.org/web/20140221230137/http://www.milhist.dk/post45/boellebank/boellebank_uk.htm/. 15.06.2020.

5 Ibidem, s. 62.

6 *Yugoslav Events Chronology,* Sept.-Dec. 1994, The University of Texas Arlington, http://www.uta.edu/cpsees/yec-394.txt#prof/. 15.06.2020.

7 S. Philip, *Flowers Turn to Bullets in Prizren: German Troops Kill Attacking Serb,* „The Washington Times (Waszyngton, DC)", 14.06.1999, https://www.highbeam.com/doc/1G1-56766596.html/. 21.05.2020.

Profilowanie kryminalne

TYPOWANIEM SPRAWCÓW PRZESTĘPSTW ZAJMUJE SIĘ CORAZ WIĘKSZA GRUPA OSÓB MAJĄCYCH RÓŻNE UPRAWNIENIA, STOPNIE I TYTUŁY NAUKOWE, W TYM BIEGLI SĄDOWI ORAZ SPECJALIŚCI I FUNKCJONARIUSZE POLICJI.

ppłk dr Zbigniew Nowak

Autor jest szefem Wydziału Prawa Publicznego w Oddziale Prawnym DGRSZ.

Członkowie amerykańskiej Akademii Telewizyjnej 28 lipca 2020 roku ogłosili w Los Angeles nominacje do 72. edycji nagród Emmy. Najwięcej, łącznie bowiem 160, otrzymał jeden z flagowych seriali Netflixa – dwusezonowy *Mindhunter*. Akcja toczy się w Stanach Zjednoczonych pod koniec lat siedemdziesiątych ubiegłego wieku. Dwóch agentów FBI zmienia oblicze kryminologii, badając umysły morderców i niebezpiecznie przybliżając się do poznania istoty bezwzględnego zła. W tym celu przeprowadzają serię rozmów z odsiadującymi wyroki kryminalistami, m.in. z seryjnymi mordercami i gwałcicielami. Postaci agentów inspirowane były pracą prawdziwych agentów Federal Bureau of Investigation: Roberta K. Resslera i Johna E. Douglasa oraz dr Ann Wolbert Burgess – psychiatry współpracującej z FBI, wykładowcy Uniwersytetu w Pensylwanii. Prowadzą oni systematyczną analizę działań i motywacji odbywających karę kryminalistów, aby zrozumieć mechanizmy popychające ich do zbrodni, czyli: *How + Why = Who*.

Polska, Gostynin, Krajowy Ośrodek Zapobiegania Zachowaniom Dyssocjalnym. Wśród kilkudziesięciu osadzonych w tym zamkniętym zakładzie psychiatrycznym jest Leszek Pękalski. Do niedawna przebywał tu Mariusz Trynkiewicz. Pierwszy z nich to największy zbrodniarz w historii powojennej Polski, „wampir z Bytowa": dewiant seksualny, seryjny

Sprawcy zbrodni mają umiejętność manipulowania dowodami, takimi jak ciało ofiary czy miejsce zdarzenia. Może to prowadzić do wysunięcia błędnych wniosków już na wczesnych etapach czynności śledczych.

SHUTTERSTOCK/FER GREGORY

morderca popełniający zbrodnie z motywów urojenionych, seksualnych, gwałciciel, pedofil – nimfofil, nekrofil wykazujący objawy nekrosadyzmu, homoseksualista zawdzięczający swoją dzisiejszą egzystencję katalogowi kar ustanowionych po 1995 roku.

Drugi z nich, „szatan z Piotrkowa", to wybitnie inteligentny egocentryk, jedynak, zabójca czterech chłopców, pedofil, skazywany jeszcze przed ich zamordowaniem w 1988 roku za czyny pedofilne. Trynkiewicz w trakcie przesłuchań wyjaśniał, że wystarczyło mu samo patrzenie na nagich małoletnich, ponieważ było to dla niego *formą rozładowywania emocji* w nim narastających[1]. Dziś odbywa następną karę pozbawienia wolności za kolejne przestępstwa seksualne.

Niezależnie od kontynentów czy państw, co łączy takie osoby? Jakie są okoliczności popełniania przez nich zbrodni będących przedmiotem badań naukowych, tematem seriali, domniemań i poszukiwań?

Elementów wspólnych jest z pewnością wiele, począwszy od samych zbrodni zabójstwa, ich podobieństw i okoliczności modalnych, przez wszelkie odstępstwa od „normy" sprawców, weryfikację ich poczytalności, na wpływie różnorodnych czynników na ich zachowania kończąc, m.in. dzieciństwa, wychowania, patologii, alkoholu. Nieznanego sprawcę czy „zwykłego" gwałciciela, pedofila, czy też „bardziej wyrafinowanego" seryjnego zabójcę trzeba oczywiście znaleźć, co może nastręczać trudności, w szczególności gdy między poszczególnymi aktami zbrodni okres tzw. wyciszenia trwa kilka miesięcy lub lat.

Istotą tej publikacji jest przedstawienie jednej z cech wspólnych, elementu zyskującego na popularności w ostatnich latach, mimo wszystko nie do końca wykorzystywanego przez organy ścigania, być może z powodu braku specjalistów oraz niespopularyzowania wyników badań naukowych w tym zakresie. Elementu, który prowadzi do najważniejszego, kodeksowego celu postępowania przygotowawczego – wykrycia i ujęcia nieznanego dotychczas organom ścigania sprawcy czynu zabronionego. Tym elementem jest profilowanie kryminalne.

JAKO NARZĘDZIE ŚLEDCZE

Profil – widok przedmiotu (zwłaszcza twarzy) z boku; zarys, kontur; sylwetka; przenośnie przekrój, zakres; technicznie: przekrój z boku, obrys. Z łacińskiego profilare – nakreślać; „pro" – naprzód; „filare" – prząść, snuć[2]. Wspomniani agenci Federal Bureau of Investigation definiowali profilowanie jako: *określenie cech sprawcy opierające się na analizie popełnionego przestępstwa, którego wynikiem jest ogólna charakterystyka osoby*[3]. Według innej definicji *profilowanie kryminalne to zbiór operacji realizowanych zazwyczaj w przypadku morderców działających metodycznie lub przestępstw mających charakter seksualny realizowanych, by poznać cechy nieujawnionego przestępcy na podstawie informacji zgromadzonych z miejsca przestępstwa cech wiktymologicznych ofiary, a także wiadomości zdobytych podczas pracy nad tożsamymi sprawami*[4].

Bogdan Lach, pierwszy polski profiler, autor ponad czterystu profili psychologicznych i kryminalistycznych nieznanych sprawców różnych kategorii przestępstw, określa profilowanie jako: *szereg czynności związanych z analizą śladów* […], *które w rezultacie zmierzają do zbudowania logicznej, spójnej i zwięzłej charakterystyki sprawcy*[5].

W ocenie Jana Gołębiowskiego, biegłego sądowego Sądu Okręgowego w Warszawie, wykładowcy Szkoły Wyższej Psychologii Społecznej Uniwersytetu Humanistyczno-Społecznego w Warszawie, założyciela Centrum Psychologii Kryminalnej, jednego z najbardziej znanych polskich profilerów, profilowanie kryminalne to jednak praktyczne, nie zaś teoretyczne, kryminalistyczne i kryminologiczne *narzędzie śledcze, a nie metoda naukowa*[6].

Zgodnie z poglądem profesor Ewy Gruzy, profilowanie psychologiczne znajduje zastosowanie w pracy wykrywczej. Stanowi ono jedną z metod wspomagających proces wykrywczy, w założeniu prowadzącą do wytypowania, a w konsekwencji do identyfikacji sprawcy zdarzenia. Efektem tego procesu jest stworzenie tzw. portretu psychologicznego nieznanego sprawcy i na tej podstawie typowanie polegające na dopasowaniu stworzonego profilu do populacji i wybranie z niej osób pasujących do portretu. Należy zaznaczyć, że nie jest możliwe stworzenie takiego profilu, który umożliwiałby wskazanie konkretnej osoby. Zawsze jest to określenie grupowe, ułatwiające planowanie i podejmowanie działań zarówno procesowych, jak i operacyjnych. Profil zawiera więc cechy probabilistyczne[7]. Wynikiem profilowania jest opinia dotycząca zestawu cech psychologicznych, społecznych i fizycznych tworzących portret nieznanego jeszcze sprawcy.

1 E. Iwanicki, *Proces Szatana*, Łódź 1990, s. 32. Por. E. Żarska, *Łowca. Sprawa Trynkiewicza*, Kraków 2018, s. 183 i nast.

2 *Słownik wyrazów obcych* Władysława Kopalińskiego, Warszawa 1999, s. 414.

3 R.K. Ressler et al., *Crime Classification Manual: A Standard System For Investigating And Classifying Violent Crimes,* Lexington, Mass 1992, s. 82.

4 J. Gołębiowski, K. Grochowska, *Profilowanie kryminalne na potrzeby sądu. Kontrowersje wokół przydatności*, https://www.bibliotekacyfrowa.pl/./publication/58993/. 5 sierpnia 2020.

5 B. Lach, *Profilowanie kryminalistyczne*, Warszawa 2014, s. 12.

6 J. Gołębiowski, *Profilowanie kryminalne,* Łomianki 2017, s. 28.

7 E. Gruza, *Psychologia sądowa dla prawników,* Warszawa 2009, s. 251 i nast.

8 B. Hołyst, *Kryminalistyka,* Warszawa 2010, s. 1166.

Cytując profesora Brunona Hołysta, można stwierdzić, że *sporządzenie profilu psychologicznego jest sztuką, a korzystanie z niego wymaga szczególnych umiejętności, natomiast wykonanie empirycznego profilu sprawcy wiąże się głównie ze zdrowym rozsądkiem i kryminalistyczną starannością, która powinna cechować każdego kryminalistyka, a stosowanie go w praktyce nie wymaga specjalistycznej wiedzy*[8].

W naszym kraju nie ma konkretnej dziedziny nauki o nazwie *profilowanie*. Najbliższe profilowaniu są nauki kryminalistyczne. Tak więc profilowanie kryminalne ani w kraju, ani na świecie nie stanowi odrębnej dziedziny nauki. Jest to specjalność absolutnie multidyscyplinarna, łącząca psychologię, kryminologię, wiktymologię, kryminalistykę, psychiatrię, medycynę sądową i wiele innych dziedzin. Połączenie wszystkich tych nauk ma pomóc w jednym – w odnalezieniu sprawcy przestępstwa[9].

Praca profilera jest żmudna. To analityczna dłubanina. Akta sprawy na biurku to za mało. Nie da się stworzyć profilu zabójcy, nie będąc na miejscu zdarzenia, nie mając dobrej dokumentacji fotograficznej czy wideo, nie rozmawiając z ewentualnymi świadkami, nie obserwując nawet ich zachowań. Zawsze kilka przestępstw dokonanych przez jednego sprawcę daje analitykowi dużo więcej wskazówek dotyczących jego cech indywidualnych, charakteru. Ogólnie rzecz biorąc, jego cech osobowościowych i behawioralnych.

Profilowanie kryminalne zaczyna się na miejscu zbrodni. Policjanci – śledczy oraz technicy – zbierają dane pod swoim kątem, natomiast profiler zwraca uwagę na inne elementy. Ale także, co jest oczywiste, korzysta z wyników pracy organów ściągania: oględzin miejsca zdarzenia i zwłok, ekspertyz, przesłuchań, konfrontacji, opinii innych biegłych. Samodzielnie powinien zbierać dowody, rozmawiać ze wszystkimi osobami (jako pierwszy), umieć nawiązywać kontakt, bacznie obserwować i słuchać. Czerpie z tego, co zbiorą policjanci, ale de facto prowadzi własne śledztwo[10]. W zależności od sytuacji profiler udziela śledczym rad, czasem zawierających proaktywną taktykę, a także strategię przesłuchań, jeżeli sprawca został zatrzymany.

Profilowanie jest narzędziem szczególnie „lubianym" przy poszukiwaniu przestępców seryjnych, w tym głównie sprawców przestępstw na tle seksualnym. Jest wykorzystywane do tworzenia ich portretu psychologicznego, rozumianego jako swoisty moment psychobiograficzny wybrany przez psychologa. Może jednak prowadzić do wykrycia sprawców innych przestępstw, niekoniecznie wyłącznie zabójców czy zabójców seryjnych lub wielokrotnych. W tym „pakiecie" są również sprawy związane z molestowaniem dzieci, z porwaniami, samobójstwami, obscenicznymi telefonami czy też wymuszeniami. Nawet jeżeli podejrzany odpowiada profilowi, nie może to stanowić dowodu bezpośrednio obciążającego go w postępowaniu karnym. Profil jest hipotezą, a wyrok musi opierać się na obiektywnych dowodach i faktach.

Profilowanie nie ma wyznaczonej w polskim prawodawstwie pozycji i ściśle sprecyzowanego miejsca. Jeszcze niedawno było traktowane jedynie jako czynność pozaprocesowa, którą wykorzystywały zwykle operacyjne służby śledcze. Jest prowadzone w ramach czynności operacyjno-rozpoznawczych, jak również podczas postępowania karnego w działaniach procesowych. Wynika z tego, że jako czynność ma dwoistą naturę.

HISTORIA PROFILOWANIA KRYMINALNEGO

Niełatwo określić dokładną datę pojawienia się profilowania, ponieważ podobnie jak inne dziedziny nauki rozwijało się ono stopniowo. W literaturze przedmiotu uznaje się, że jako pierwszy charakterystyki przestępcy dokonał włoski psycholog, antropolog i kryminolog Cesare Lombroso. W 1876 roku opublikował swoje znane dzieło *L'uomo delinquente in rapporto all'antropologia, alla giusprudencia ed alle discipline carcerarie*, w którym na podstawie przeprowadzonych badań porównał cechy sprawców podobnych przestępstw i wyróżnił trzy typy kryminalne:

- urodzeni przestępcy – prymitywni, osoby zdegenerowane;
- przestępcy obłąkani – osoby cierpiące na choroby psychiczne;
- kryminoloidzi – grupa niemająca specyficznej charakterystyki, osoby o predyspozycjach do przejawiania zachowań przestępczych[11].

Co ciekawe, badania antropologiczne kontynuował w XIX wieku niemiecki lekarz psychiatra Ernst Kretschmer, według którego:

- laptosomicy i ascenicy – to osoby wysokie i szczupłe będące drobnymi złodziejami i oszustami;
- atletycy – to osoby o dobrze rozwiniętych mięśniach popełniający przestępstwa gwałtowne;
- pyknicy – to ludzie niscy i korpulentni, otyli, najczęściej powinni być kojarzeni z podstępem, wprowadzaniem w błąd, z oszustwem;

8 B. Hołyst, *Kryminalistyka,* Warszawa 2010, s. 1166.

9 J. Gołębiowski, *Profilowanie*..., op.cit., s. 12.

10 W naszym kraju nie ma takiego zawodu jak profiler, aczkolwiek są organizowane szkolenia z tego zakresu przez Centrum Psychologii Kryminalnej w Warszawie.

11 B. Hołyst, *Cesare Lombroso: jego życie i dzieło* [w:] *Geniusz i obłąkanie*, Warszawa 1987, s. 7–34. Lombroso wskazał 18 charakterystycznych cech. Występowanie przynajmniej pięciu powoduje, że mamy do czynienia z urodzonym mordercą. Są to: asymetryczność twarzy, nadmierna wielkość szczęki lub kości policzkowych, worki w policzkach jak u zwierząt, nienormalne uzębienie, dodatkowy palec, zajęcza warga i inne.

• dysplastycy lub mieszani – to osoby mogące popełniać przestępstwa przeciwko dobrym obyczajom i moralności.

Określany mianem ojca kryminalistyki Hans Gross, austriacki profesor kryminalistyki, sędzia śledczy, kryminolog, założyciel Instytutu Kryminalistycznego w Grazu, mający znaczący wpływ na rozwój profilowania, wprowadził z kolei dwa kolejne istotne terminy charakteryzujące wykorzystanie i tworzenie profilu kryminalnego, tj. kryminologię stosowaną oraz śledztwo kryminalne.

Jeszcze w XIX wieku (w 1888 roku) chirurg George Philips dokonywał w Wielkiej Brytanii oględzin ciał i na tej podstawie wnioskował, że z pewnością istnieje związek między cechami sprawcy a ranami stwierdzonymi u ofiary. W tym samym roku wydano opinię na temat zabójcy z Whitchapel koło Londynu – „Kuby Rozpruwacza", mordercy prawdopodobnie kilkunastu kobiet[12]. Profil psychologiczny sprawcy został opracowany na prośbę szefa Departamentu Dochodzeń Kryminalnych przez psychiatrę i chirurga dr. Thomasa Bonda. Była to pierwsza zanotowana prośba o stworzenie profilu sprawcy, choć nie doprowadziła do schwytania jednego z pierwszych i najbardziej znanych zabójców na świecie.

W 1957 roku kryminolog James Reinhardt używał pojęcia *łańcuchowy morderca*. W 1966 roku, opierając się na wcześniejszych badaniach, John Brophy w swojej publikacji *The Meaning of Murder* użył zwrotu *seryjny morderca*, wprowadzonego do praktyki prawnej przez wspominanego agenta biura federalnego Roberta K. Resslera w roku 1974 (*zabójstwo seryjne*).

W latach 1940–1957 w związku z dużą liczbą zamachów bombowych dokonywanych przez „Szalonego Bombiarza z Nowego Yorku" nowojorskiej policji w poszukiwaniu sprawcy pomagał psychiatra James Brussel. Ten na podstawie akt sprawy, dokumentacji fotograficznej miejsc zdarzeń oraz listów sprawcy stworzył profil Mad Bombera. Zajęło mu to trzy tygodnie, a pół roku później ujęto imigranta polskiego pochodzenia – George'a Metesky'ego. Oto jego opis: *samotnik, bez przyjaciół, małe zainteresowanie kobiet. Nieżonaty, może żyć ze starszą krewną. Czterdzieści do pięćdziesięciu lat. Precyzyjny, czysty i schludny. Słowianin*. Przed sporządzeniem profilu poszukiwania zamachowca trwały ponad 17 lat.

W roku 1969 Howard Teten rozpoczął w Akademii FBI w Quantico profesjonalne badania nad profilowaniem kryminologicznym. Korzystał początkowo ze wskazówek dr. Jamesa Brussela. Rok później prowadził wykłady nt. *Apllied Criminology*. W roku 1972 przyłączył się do niego inny agent FBI Pat Mullany. Teten i Mullany zaczęli budować bazę danych złożoną z wywiadów przeprowadzonych z seryjnymi i gwałtownymi mordercami. W 1974 roku do nowo powstałej jednostki FBI, utworzonej przez Jacka Kirsha – Behavioral Science Unit, dołączył chyba najbardziej znany profiler wszechczasów, wspomniany już Robert K. Ressler[13].

Od roku 1974 FBI mogło pochwalić się wieloma sukcesami w profilowaniu sprawców seryjnych morderstw. Skutecznym narzędziem w poszukiwaniu sprawców morderstw o podłożu seksualnym okazał się program profilowania psychologicznego wprowadzony w 1978 roku przez Wydział Badań nad Zachowaniem Akademii FBI w Quantico (Behavioral Science Unit zmieniono na Investigative Support Unit), powstały przy znaczącym udziale wspomnianych tu Roberta K. Resslera, Johna E. Douglasa oraz dr Ann Wolbert Burgess, co zresztą stało się istotnym elementem scenariusza serialu *Mindhunter*.

PRACA PROFILERA MOŻE PROWADZIĆ JEST PRZYCZYNIENIE SIĘ DO UJĘCIA

Od 1992 roku intensywne badania nad profilowaniem prowadzono pod kierownictwem brytyjskiego profesora psychologii, uznawanego za jednego z najwybitniejszych profilerów w historii, Davida Cantera w ramach Investigative Psychology Research Group na Uniwersytecie Surrey (obecnie University of Liverpool). Stosowane podejście nazwano *profilowaniem geograficznym*. Rola Davida Cantera w tych badaniach jest nie do przecenienia. Nazywany jest czasem nawet ojcem profilowania. On też wprowadził do użycia termin *psychologia śledcza,* używany do określania metody profilowania wypracowanej przez zespół Cantera w Anglii między 1985 a 1992 rokiem. Niektórzy twierdzą, że jest to jedyna właściwa metoda profilowania. W 1985 roku David Canter, profesor psychologii, dostarczył profil w sprawie Johna Duffy'ego – przestępcy podejrzanego o 30 gwałtów i kilka morderstw. Podejście Cantera ma charakter iście akademicki i podparte jest twardą nauką. Nie posługuje się on utworzonymi typologiami, lecz stara się dotrzeć do uniwersalnych mechanizmów rządzących ludzkim zachowaniem.

Autorem powszechniej używanej metody opartej na profilowaniu geograficznym jest Kanadyjczyk dr Kim Rossmo, funkcjonariusz Policji z Vancouver.

12 B. Lach, *Profilowanie...*, op.cit., s. 27–31.

13 I. Brian, *Niezbity dowód – metody wykrywania zbrodni,* Warszawa 2001, s. 50 i nast.

Wyniki swoich badań polegających na poszukiwaniu sprawców z wykorzystaniem mapy przestępstw (gdzie popełniono przestępstwa, gdzie ujawniono zwłoki itp.) opublikował w 1995 roku.

W latach siedemdziesiątych i osiemdziesiątych XX wieku do grona państw korzystających z profilowania kryminalnego dołączyły ZSRR i Polska. W roku 1984 Alexandr Bukhanowsky, rosyjski profesor psychiatrii, został poproszony o sporządzenie profilu „rzeźnika z Rostowa" Adrieja Czikatiły. Bukhanowsky stworzył psychologiczny profil na 65 stronach. Dopiero po pięciu latach od utworzenia profilu seryjnego zabójcy ponad 50 kobiet udało się złapać sprawcę, którego profil idealnie pasował do przedstawionego przez doktora Bukhanowskiego.

Pierwszym praktycznym przykładem profilowania w Polsce był przypadek Zdzisława Marchwickiego – „wampira z Zagłębia", domniemanego mordercy skazanego na karę śmierci za zabójstwo 14 kobiet i usiłowanie zabójstwa kolejnych. Do opracowania profilu psychologicznego sprawcy poproszono w roku 1972 grono specjalistów z dziedziny psychiatrii, psychologii i medycyny sądowej[14]. Wielość dziedzin reprezentowanych przez nich doprowadziła do powstania charakterystyki mordercy zawierającej tak wiele cech, że mógłby to być każdy mężczyzna. O konsultacje w tej sprawie poproszono nawet wspominanego doktora Jamesa Brussela, który specjalnie w tym celu przyleciał do naszego kraju. Winę aresztowanego, oskarżonego i straconego Zdzisława Marchwickiego podaje się do dziś w wątpliwość[15].

Zresztą podobny przypadek skazania być może niewinnej osoby lub skazania za część zbrodni, których nie popełnił, miał miejsce na Śląsku, gdzie w latach dwudziestych XX wieku zatrzymano „rzeźnika" Edwarda Trautmanna podejrzanego o dokonanie ponad 20 morderstw. Głównym argumentem oskarżenia było dopasowanie jego osobowości do dokonanej zbrodni. Profil ten doprowadził jednak do wielkiej pomyłki, ponieważ prawdziwym mordercą okazał się Karl Denke, którego zatrzymano w 1924 roku. Natomiast Trautmann został skazany niewinnie na 12 lat[16].

W 1983 roku w czasie śledztwa oznaczonego kryptonimem „Skorpion" dzięki inicjatywie kpt. Ryszarda Małaszka skorzystano ze specjalnego narzędzia, jakim była ankieta wstępnego opracowania sylwetki psychologicznej mordercy.

W 1986 roku w sprawie zabójstwa kobiety w Dąbrowie Tarnowskiej Instytut Ekspertyz Sądowych im. prof. dr. Jana Sehna w Krakowie stworzył profil, który uznano za pierwszy profesjonalny profil psychologiczny sprawcy. Zresztą Instytut jest najstarszą instytucją w kraju, która chlubi się tym, że tworzyła profile sprawców, badając niewyjaśnione morderstwa na podstawie akt spraw.

Sprawa „inkasenta z Małopolski" była jedną z pierwszych, w których użyto profilu kryminalnego sprawcy[17]. Mimo długiego procesu sądowego oskarżony został uniewinniony, a rzeczywisty sprawca pięciu zabójstw pozostaje nieuchwytny do dziś.

W roku 2017 Jan Gołębiowski przedstawił dane dotyczące wzrostu popularności profilowania kryminalnego. *W roku 2001 w policji sporządzono 15 profili sprawców, które zostały użyte na rzecz śledztwa*, […] *w roku 2002 i 2003 wymienia się już około 29 sporządzonych profili. Raport Psychologa Koordynatora z KGP za rok 2005 podaje liczbę już 45 sporządzonych profili przez wszystkich psychologów policyjnych w kraju. W 2009 roku była ich szczytowa ilość – 86, w 2012 – 78, zaś w 2015 – 45*[18].

Te liczby są jednak znacznie zaniżone. Nie jest znana liczba śledztw, w których wykorzystuje się w ostatnich latach profilowanie kryminalne.

DO EKSCYTUJĄCEGO FINAŁU, JAKIM SPRAWCY ZBRODNI

KREOWANIE PROFILU KRYMINALNEGO

Profilowanie jest czynnością złożoną, dlatego tworzenie profilu powinno być podzielone na kilka etapów:

- pierwszy – to gromadzenie wszystkich informacji, które są niezbędne, aby stworzyć profil nieznanego sprawcy;

14 Psychiatrę prof. Tadeusza Bilikiewicza, prof. Bolesława Popielskiego, prof. Jana Stanisława Kobielę, doc. Tadeusza Hanauska, doc. Władysława Nasiłowskiego, dr. Andrzeja Różyckiego.

15 J. Gołębiowski, *Profilowanie*..., op.cit., s. 46.

16 Por. http://ligas.atspace.com/psychologia/historia_typowania.html/. 3.08.2020.

17 M. Wasiak, *Profilowanie kryminalne i lingwistyka kryminalistyczna jako multidyscyplinarne metody typowania sprawców przestępstw*, «Security, Economy & Law» 11.2/2016, s. 87–88. Por. http://security-economy-law.pl/wp-content/ uploads/2016/11/SEL_11_84-105.pdf/. 29.07.2020.

18 J. Gołębiowski, *Profilowanie*..., op.cit., s. 45 i nast. *Liczby sporządzonych profili kryminalnych powyżej to tylko te sporządzone przez psychologów policyjnych, więc biorąc pod uwagę, że takie profile tworzą też biegli sądowi, liczby te mogą być nawet dwukrotnie większe.*

• drugi – to klasyfikacja i porządkowanie wszystkich zgromadzonych dotychczas informacji, aby podjąć dalsze działania;
• trzeci – to odtwarzanie kolejności wydarzeń na miejscu zbrodni;
• czwarty – to określenie motywacji sprawcy, co nim kierowało, jakie były jego wewnętrzne odczucia podczas dokonywania przestępstwa;
• piąty – to stworzenie profilu nieznanego sprawcy i skontrolowanie go;
• szósty – to już proces aresztowania potencjalnego sprawcy oraz sprawdzenie, czy to faktycznie on dokonał przestępstwa.

Według innego, uproszczonego schematu, tok czynności w procesie budowania profilu można podzielić na trzy etapy: poszukiwanie źródeł informacji, ocena wiarygodności źródeł oraz rekonstrukcja[19].

W kryminalistyce uznaje się, że profil kryminalny powinien odpowiadać przede wszstkim na następujące pytania:
• Czy sprawca i ofiara się znali?
• Jakiego rodzaju była to znajomość?
• Co ich łączyło?
• Czy sprawca znał miejsce, w którym dokonano przestępstwa, i w jaki sposób jest z nim związany?
• Co mogło go motywować do dokonania tego czynu?
• Czy sprawca cierpi na zaburzenia?
• Jakie zachowania sprawca mógł przejawiać w przeszłości?

Doktor Maciej Szaszkiewicz twierdzi, że profilowanie opiera się na trzech filarach. Są to:
– informacje wiktymologiczne,
– dane dotyczące miejsca zdarzenia,
– dane dotyczące czasu zdarzenia: lokalizacji w czasie (kiedy?) i czasu trwania zdarzenia (jak długo?).

Opierając się na wiedzy psychologicznej, zwłaszcza o zachowaniu człowieka, w szczególności o zachowaniu i psychice zabójców, analizuje się dane i stawia hipotezy interpretacyjne. Wychodząc z tych ustaleń, weryfikuje się te hipotezy i dąży do odtworzenia przebiegu zdarzenia. Następnie do odtworzenia sposobu działania sprawcy oraz jego motywacji. Po tym wszystkim ustala się jego cechy. Dochodzi się wtedy do charakterystyki sprawcy, czyli jego profilu.

Istnieje kilka szkół modelowania, kreowania profilu kryminalnego sprawcy[20].

Należy zacząć od modelu profilowania powstałego w Stanach Zjednoczonych, spopularyzowanego przez wspominanych bohaterów serii Netflixa – Roberta K. Resslera, Johna E. Douglasa oraz Ann W. Burgess. Po kilkunastu latach badań i rozmów z seryjnymi mordercami oraz na podstawie zebranych danych opracowano w 1986 roku w FBI wspomniany pierwszy model profilowania *The Criminal – profile – generating proces*. Niedługo potem utworzono bazę gromadzącą dane behawioralne, które wykorzystywano w procesie profilowania sprawców.

Stosując w niej podział dychotomiczny, wyróżniono dwa podstawowe typy przestępców, czyli: przestępca zorganizowany oraz przestępca zdezorganizowany (niezorganizowany).

Podział ten jest najpopularniejszym wstępnym sposobem modelowania profilu nieznanego sprawcy. Klasyfikacja ta opiera się na diagnozach klinicznych. Bazuje na śladach znalezionych w przestrzeni, w której dokonano morderstwa, gdyż właśnie po szczegółowej analizie miejsca zdarzenia można odtworzyć zachowanie sprawcy.

Uznaje się, że przestępstwa popełnione przez sprawców zorganizowanych (działających metodycznie) są wcześniej odpowiednio zaplanowane. Ofiarą jest raczej osoba, której sprawca nie zna, lecz wybiera ją przed dokonaniem przestępstwa. Może ją długotrwale obserwować, nawet dążyć do wcześniejszego kontaktu, do rozmowy. Przy wyborze ofiary zwraca uwagę na jej cechy szczególne. Mogą dotyczyć wyglądu bądź charakteru. Wskazani przestępcy zazwyczaj dokonują zbrodni na tle seksualnym[21]. Zabójca zorganizowany zwykle nie depersonalizuje swojej ofiary. Najczęściej krępuje ją, przejmując nad nią władzę i dokonuje aktów seksualnych z żywą osobą. Często używa samochodu, na przykład do porwania ofiar, a później do przewiezienia i ukrycia zwłok. Przemierza w tym celu nawet znaczną odległość. Zorganizowani zabójcy inscenizują często miejsce zbrodni, chcąc upokorzyć policję, przede wszystkim jednak oddalić podejrzenia od siebie. Po dokonaniu zbrodni zabójca zorganizowany śledzi tok postępowania policji. Może nawet włączyć się do poszukiwań pokrzywdzonego. Pobudza w ten sposób swoje wspomnienia i fantazje, do czego mogą mu służyć zarówno przedmioty osobiste zabrane ofierze, jak i szczegółowe opisywanie czy fotografowanie zwłok i miejsca zbrodni.

Natomiast zdezorganizowani przestępcy żyją zazwyczaj w pojedynkę, nie czują potrzeby kontaktu z ludźmi. Praca, którą sobie wybierają, to taka, w której nie jest potrzebny kontakt z innymi lub jest on ograniczony do minimum. Ich zarobki są zazwyczaj niskie. Problemem dla sprawcy niezorganizowanego jest utrzymanie stałej posady. Ten typ przestępcy w przeciwieństwie do poprzedniego nie zastanawia się nad tym, kto będzie jego ofiarą. Działania podejmuje impulsywnie i spontanicznie. Dokonane zabójstwo nie jest wcześniej dokładnie zaplanowane,

19 E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych,* Warszawa 2011, s. 47 i nast.

20 Na potrzeby artykułu bardziej szczegółowo zostaną przeanalizowane jedynie trzy główne nurty, w tym jeden krajowy.

21 Ciekawy pogląd reprezentuje B. Lach, dokonując analizy przypadków seryjnych morderczyń. W jego ocenie *profilowanie w takich przypadkach wiąże się z większymi trudnościami – kobiety należą do mniejszej grupy zabójców, a dokonując zabójstwa, są zorganizowane, metodyczne, dokładne i spokojne.*

a więc i sprawca nie przejmuje się zbytnio śladami pozostawionymi na miejscu jej popełnienia (na przykład jest w stanie porzucić nawet przedmioty ułatwiające jego osobistą identyfikację)[22]. Zabójca tego typu depersonalizuje ofiary, nie traktuje ich jak istoty ludzkie. Pozbawia przytomności, po czym zakrywa twarz albo wręcz odcina głowę. Zdarzają się bardzo rozległe rany u osób pokrzywdzonych lub rozczłonkowywanie ciała. Sprawca nie używa samochodu, ponieważ najprawdopodobniej stopień jego zaburzenia psychicznego nie pozwala mu na kierowanie pojazdem[23].

Zarówno w przypadku sprawców zorganizowanych, jak i niezorganizowanych należy pamiętać, że ich umiejętności manipulowania dowodami, takimi jak ciało ofiary czy miejsce zdarzenia, mogą prowadzić do wysunięcia błędnych wniosków już na wczesnych etapach czynności śledczych[24]. Istotnym założeniem tego typu profilowania kryminalnego jest także fakt, że ludzkie zachowania są zazwyczaj stałe, tzn. człowiek najczęściej zachowuje się w podobny sposób (np. zbrodnie popełniane przez seryjnych morderców o tym samym stałym schemacie)[25]. Stałość działania i jego powtarzalność nie są jednak kryterium, które należy od początku przyjąć jako pewnik do dalszych rozważań.

Nieco odbiegającą od tego podziału metodę opracowali Roland M. Holmes oraz Stephen T. Holmes, choć bazuje ona w dużej mierze na modelu profilowania FBI. Model Holmesów dzieli sprawców przestępstw na dwie grupy. Jedna z nich to sprawcy zorganizowani socjalni, druga to sprawcy niezorganizowani asocjalni.

Dzielą oni również zabójców na geograficznie stabilnych, czyli popełniających zbrodnie w okolicy miejsca swojego zamieszkania, oraz geograficznie mobilnych, czyli przemieszczających się w celu popełnienia zbrodni.

W 1985 roku wprowadzili podział na zabójców, którzy popełniali zbrodnie o motywach seksualnych. Wyróżnili takie typy, jak:

- wizjonerski – do tego typu należą seryjni zabójcy, którzy mają wizje bądź też słyszą głosy, które „mówią" im, że muszą zabić daną osobę lub grupę osób;
- misjonarski – typ ten nie ma wizji zabójstwa ani nie słyszy głosów, ma natomiast określoną misję do wykonania, świadomy cel polegający na wyeliminowaniu na przykład określonej kategorii ludzi;
- hedoistyczny – to typ zabójcy nastawionego na przyjemność bądź poszukiwanie konkretnych emocji; zabójstwa poprawiają jego samopoczucie bądź dają radość życia;
- nastawiony na siłę i kontrolę – mordercy tego typu czerpią satysfakcję z życia bądź też ze swojej ofiary; najważniejszym elementem jest posiadana władza nad osobą bezbronną[26].

Przedstawiciel i jednocześnie jeden z twórców polskiej szkoły profilowania kryminalnego dr Bogdan Lach używa modelu, który łączy różne metody i korzysta z systemu opracowanego w 1986 roku przez FBI (wspomniany *The Criminal – profile – generating process* oraz *Motivational Model for Sexual Homecide*). Tworząc profil, opiera się on na własnych badaniach i doświadczeniach oraz licznych źródłach wiedzy z tej dziedziny. Wraz ze zdobywaniem nowych informacji, nabywaniem doświadczenia oraz zwiększaniem się możliwości modyfikuje on swój model działania. Często podkreśla, że biegły profiler zmierza w swojej pracy do uzyskania zestawu charakterystycznych cech nieznanego sprawcy przestępstwa dokonanego w danym miejscu i czasie, co pomaga ograniczyć krąg osób będących w zainteresowaniu organów ścigania. Ocena realnej przydatności wytypowanych cech w prowadzonym śledztwie sprowadza się jednak do tego, w jakim stopniu są one konkretne, a więc można przypisać je indywidualnym osobom, a nie ogólnikowe i opisujące duże grupy społeczne[27].

Jego zdaniem, istotne jest także odtworzenie wydarzeń poprzedzających zdarzenie. Model, który stosuje, opiera się w znacznym stopniu na analizie sporządzonego wywiadu wiktymologicznego, to jest ustaleniu dostępności ofiary dla sprawcy oraz faktu, że ofiara miała zaspokoić potrzeby sprawcy. Uważa on bowiem, że *badanie ofiary przestępstwa jest tak samo ważne, jak badanie miejsca zdarzenia i osoby, która ponosi za to odpowiedzialność, gdyż ofiara zawsze stanowi połowę przestępstwa*.

Zwraca przy tym szczególną uwagę na proces motywacyjny. Twierdzi, że *jednym z najważniejszych aspektów charakterystyki sprawców jest proces motywacyjny – fundament działania sprawcy w poszczególnych rodzajach przestępstw. Pojęcie procesu motywacyjnego w przyjętym modelu jest rozumiane jako zjawisko regulacyjne pełniące funkcję sterowania czynnościami sprawcy, które doprowadziły go do określonego działania*[28]. Wskazuje na istotny aspekt profilowania, jakim jest fakt, że model wykorzystywany do sporządzenia profilu kryminalistycznego

22 B. Lach, *Profilowanie...*, op.cit., s. 110–111.

23 M. Niewińska, *Profilowanie nieznanych sprawców zabójstw na podstawie modus operandi*, «E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. E-monografie» 51/2014, http://www.bibliotekacyfrowa.pl/Content/58889 /PDF/12_Magdalena_Niewinska.pdf/. 3.08.2020.

24 J. Konieczny, M. Szostak, *Profilowanie kryminalne,* Warszawa 2011, s. 62–70.

25 J. Gołębiowski, *Profilowanie...*, op.cit., s. 28 i nast.

26 R.M. Holmes, J. de Burger, *Serial murder,* Thousand Oaks CA 1988, s. 56 i nast.

27 A. Gawliński, B. Lach, *Profilowanie kryminalistyczne, Przegląd piśmiennictwa,* RPEiS 2014 nr 76.4, s. 384–385.

28 B. Lach, *Profilowanie...*, op.cit., s. 116–117.

PIOTR BERNABIUK

NIEZNANEGO SPRAWCĘ, TRZEBA OCZYWIŚCIE ZNALEŹĆ, CO MOŻE NASTRĘCZAĆ TRUDNOŚCI, W SZCZEGÓLNOŚCI GDY MIĘDZY POSZCZEGÓLNYMI AKTAMI ZBRODNI OKRES TZW. WYCISZENIA TRWA KILKA MIESIĘCY LUB LAT.

powinien być dostosowany do realiów i możliwości danego państwa.

Proces profilowania kryminalnego ulega w naszym kraju, podobnie jak na świecie, ciągłym przekształceniom, ewolucji, głównie dzięki wykorzystywaniu wyników badań naukowych, sprzętu informatycznego oraz baz danych. Powstają nowe terminy i pojęcia odnoszące się do metod profilowania sprawców, często stosowane zamiennie. Najpopularniejsze z nich to:

- dochodzenie psychologiczne (*investigative psychology*) – wnikliwa obserwacja i analiza przypadków; w psychologii śledczej jako nauce znajduje zastosowanie metodologia nauk społecznych;
- psychodynamiczne profilowanie osobowości (*psychodynamic personality profiling*) – opiera się na psychoanalizie, na poznaniu osobowości oraz charakteru człowieka; zgodnie z tą teorią działania człowieka można przewidzieć i skorygować, uwzględniając jego popędy;
- socjologiczno-psychologiczne profilowanie (*sociopsychological profiling*) – obejmujące charakterystykę potrzeb, pragnień i preferencji sprawcy; jest to połączenie socjologii i psychologii;
- kryminologia stosowana (*applied cryminology*) – opiera się na wiedzy pochodzącej z wszelkich przeprowadzonych czynności śledztwa: od stwierdzenia, czy przestępstwo zostało popełnione, przez zebranie i weryfikację dowodów z miejsca przestępstwa, do zidentyfikowania, zlokalizowania i zatrzymania sprawcy;
- behawioralna analiza dowodów (*behavioral evidence analysis*) – każde przestępstwo jest inne, charakteryzowane przez indywidualny i mało powtarzalny układ czynników;
- kryminologia kliniczna (*clinical psychology*) – stawianie psychologiczno-psychiatrycznej diagnozy sprawców przestępstw, będącej połączeniem kryminologii, psychiatrii i psychologii;
- analiza przestępstwa (*crime scene analysis*) – analiza z wykorzystaniem wszelkich możliwych do-

wodów z miejsca przestępstwa, zabezpieczonych śladów biologicznych, traseologicznych, toksykologicznych, daktyloskopijnych; analiza materiałów operacyjnych; metoda profilowania stosowana przede wszystkim przez FBI;

• rekonstrukcja przestępstwa (*crime scene reconstruction*) – pokazanie i analiza tego, co wydarzyło się w konkretnym czasie i miejscu[29].

Kreowanie profilu kryminalistycznego jest procesem złożonym. Wynik profilowania powinien uwzględniać: wiek, płeć, wykształcenie, status majątkowy, relacje interpersonalne, wcześniejszą karalność, rodzaj zaburzeń psychicznych oraz motywację sprawcy. Na jego powstanie bezpośredni wpływ ma ustalenie motywu zachowania sprawcy oraz sposobu jego działania.

Tak więc niezmiernie istotnym założeniem w procesie tworzenia profilu sprawcy jest zarówno poznanie motywu jego działania (zachowania, motywacji), jak i w ramach tego procesu sposobu działania, tzw. *modus operandi*. Patrząc jednak na ten problem z innej strony, profilowanie kryminalne jest sposobem prowadzącym do poszukiwania motywu popełnienia przestępstwa, do poznania motywacji sprawcy popychającej go do popełniania czynu zabronionego.

MOTYWACJA A *MODUS OPERANDI*

Cechy psychologiczne sprawcy są odzwierciedlone w jego zachowaniu. Dlatego też profiler, opisując go, w pierwszej kolejności dąży do zdefiniowania motywu zachowania. Motywacja jest bowiem bodźcem i przyczyną danego zachowania osoby[30]. Motywację sprawcy ustala się na podstawie analizy.

John Douglas, jeden z najwybitniejszych profilerów ubiegłego wieku, ekspert, konsultant pozycji książkowych i scenariuszy filmowych, kierował się zasadą*:* jeśli zrozumie się motyw, można rozwikłać tajemnicę zbrodni. Przekonywał, że każda zbrodnia ma wiodący motyw, a jeśli profilerowi uda się odkryć, co działo się w umysłach przestępców, którzy ją popełniali, będzie w stanie udzielić odpowiedzi na pytanie, kto zabił. Ustalenie procesów motywacyjnych jest istotne nie tylko na etapie ścigania sprawcy, lecz również może być przydatne w trakcie przesłuchania w celu zastosowania odpowiedniej taktyki[31].

Istnieje wiele przyjętych kategorii motywacji. Poza tym istnieją dziesiątki, jeśli nie setki motywacji prowadzących do zbrodni. W literaturze przedstawiane są cztery fazy przestępstwa, w trakcie których można analizować samego sprawcę i jego motywację prowadzącą do popełnienia czynu zabronionego. Są to:

– pierwsza, przedkryminalna – obejmuje okres przed popełnieniem przestępstwa, a jej głównym przejawem są fantazje sprawcy, które prowadzą do podjęcia decyzji o popełnieniu czynu;

– organizacja sceny przestępstwa – w tej fazie sprawca wybiera ofiarę, miejsce oraz sposób popełnienia morderstwa;

– uprzątniecie sceny przestępstwa – to proces pozbycia się dowodu w postaci ciała ofiary i uprzątnięcia miejsca zbrodni;

– faza postkryminalna – obejmuje zachowanie sprawcy po dokonaniu zbrodni[32].

Biorąc pod uwagę motywację przestępcy, nawet w przypadku tylko zwykłego zabójstwa może to być podział oparty na motywach: rabunkowych, erotycznych, seksualnych (sadyzm seksualny, lubieżność, gwałt na zwłokach), nieporozumienia rodzinnego, porachunków osobistych, a także zlecenia lub innych powodów (istotne są charakterystyczne cechy związków między ofiarą a sprawcą, sprawcami, na przykład zemsta), choćby chuligańskich, nieustalonych, urojeniowych (schizofrenia, paranoja).

Rodzaje motywacji sprawcy można podzielić najprościej na: emocjonalno-urojeniową (urojeniowa, inaczej: patologiczna – poniżej 1% stwierdzonych przypadków), seksualną i ekonomiczną. Przy czym, opierając się na dotychczasowym dorobku psychologii, nie można już mówić o pojedynczym motywie, ponieważ nie występuje nigdy jeden. Obecnie uznaje się, że zazwyczaj jest to złożony zespół różnych motywacji, gdy jeden element może zasadniczo przeważać[33].

Przyjmując ten podział, należy domniemywać – na przykład w stosunku do sprawców zabójstw – jakie typowe elementy mogą budować ich profil psychologiczny. Można zakładać, że sprawca o motywacji emocjonalnej w pierwotnym założeniu będzie chciał tylko rozładować napięcie, a nie zabić. Cechami charakteryzującymi ten typ działania przestępnego jest na przykład odnalezienie zwłok w miejscu popełnienia przestępstwa, które nierzadko jest również miejscem zamieszkania ofiary. Dodatkowo zwłoki niekiedy mają zasłonięte oczy, co może świadczyć o wyrzutach sumienia lub o osobistym stosunku sprawcy do ofiary i emocjonalnym podłożu zabójstwa. Brak innych zmiennych mówiących o tym, że sprawca w jakikolwiek sposób manipulował przy zwłokach, próbując je ukryć lub przemieścić, zdaje się wskazywać, że nie realizował przez zabójstwo innych celów (ekonomicznych czy seksualnych), a także że nie było ono racjonalnie zaplanowane i wykonane. Nie uczynił też niczego, aby ukryć prze-

29 Ibidem, s. 51.

30 Ze względu na temat niniejszego artykułu zagadnienie motywacji sprawcy oraz *modus operandi* zostaną poddane analizie w ogólnym zarysie.

31 B. Lach, *Proces motywacyjny nieznanego sprawcy zabójstwa* [w:] *Problemy współczesnej kryminalistyki,* red. M. Goc, E. Gruza, T. Tomaszewski, t. XII, cz. 2, s. 368 i nast.

32 Por. http://seryjnimordercy-psyche.blogspot.com/p/blog-page_1336.html/. 3.08.2020.

33 M. Całkiewicz, *Modus operandi sprawców zabójstw,* Warszawa 2010, s. 191 i nast.

stępstwo. Zatem próba ukrycia zwłok może oznaczać instrumentalny stosunek sprawcy do popełnionego czynu, chęć uniknięcia odpowiedzialności karnej, a także potwierdzenie kryminalnej jego przeszłości.

Poza sprawcami o motywacji emocjonalnej można wyróżnić tych, których działanie prowadzące do uśmiercenia ofiary miało charakter posiłkowy. Zabójstwo było jedynie środkiem do określonego celu, czy to zaspokojenia seksualnego, czy dokonania przestępstwa przeciwko mieniu. Cechami charakterystycznymi, które odróżniają miejsce zabójstwa o podłożu seksualnym od innych typów motywacji, są przede wszystkim: rozebranie ofiary, niszczenie ubrań, manipulacja przy zwłokach, układanie ich w określony sposób, zabieranie rzeczy osobistych ofiary, które mogłyby później pełnić rolę trofeum lub wyzwalacza wspomnień o popełnionej zbrodni, umieszczanie ciał obcych w zwłokach, ślady spermy, występujące czasem obrażenia genitaliów. Sprawcę motywowanego seksualnie cechuje chłód emocjonalny. Zabójstwo dokonane jest często przez uduszenie prawdopodobnie po to, by sprawca mógł uzyskać więcej wrażeń, utrzymując bliski kontakt z konającą ofiarą.

Pokrzywdzonym jest zazwyczaj kobieta, obca sprawcy, często w wieku do niego zbliżonym. Została wybrana ze względu na określony wygląd lub zajęcie jako element rozbudowanych jego fantazji seksualnych. Typowe zmienne, zwłaszcza te wychodzące poza czynności potrzebne do dokonania przestępstwa, są charakterystyczne dla konkretnego sprawcy. Zebranie ich pozwala zobrazować coś, co można nazwać jego podpisem czy kartą wizytową, po czym można rozpoznać kolejne popełnione przez niego zbrodnie. Ocena podpisu jest istotna, gdyż wśród zabójców o motywacji seksualnej występuje największe prawdopodobieństwo dokonania serii przestępstw.

W porównaniu z pozostałymi podgrupami zabójców sprawcy kierujący się motywacją ekonomiczną stosunkowo najrzadziej wykazywali zaburzenia psychiczne lub problemy z kontrolą własnego zachowania. Wyróżniająca cecha w odniesieniu do nich to brak zachowań koncentrujących się na ofierze, jak w przypadku zabójstw motywowanych seksualnie, oraz przeżywanie silnych emocji związanych z ofiarą, jak w zabójstwach motywowanych emocjonalnie[34].

Jak już wielokrotnie wskazano, istotną cechą podczas tworzenia profilu kryminalistycznego jest określenie *modus operandi*. Metoda profilowania na podstawie sposobu działania najlepiej sprawdza się w sytuacji sprawców seryjnych[35].

Pojęcie sposobu działania wiąże się nierozerwalnie z każdym przejawem aktywności człowieka, z jego zachowaniem. Wszystko, czego dokonuje człowiek, musi przybrać jakąś określoną formę. Ludzie różnią się między sobą wiedzą, doświadczeniem, pomysłowością, temperamentem, zręcznością, umiejętnościami oraz wieloma innymi szczegółami. Właśnie to, co nas różni, powoduje, że te same czynności wykonujemy w różny sposób, zgoła indywidualny, czyli tylko sobie właściwy. Natomiast wielokrotne powtarzanie tych samych czynności powoduje przyzwyczajenie, od którego człowiek rzadko odstępuje. Może ono zacząć dominować u danej osoby, i w efekcie stać się indywidualną cechą jej zachowania, co właśnie prowadzi do konstatacji, że *modus operandi* jest ważny w przypadku przestępstw seryjnych, powtarzalnych.

Już przyjęcie chociażby kryteriów odpowiedniego sposobu przeprowadzenia ataku, miejsca dokonania zbrodni, porzucenia ciała i narzędzi, pozostawienia śladów oraz zachowania się osoby podejrzanej ułatwia ujawnienie sprawcy.

Istotna jest ofiara. Odpowiada ona na pytanie, jakie potrzeby zaspokajał sprawca, dokonując przestępstwa. Profil ofiary pomaga w rekonstrukcji przebiegu zdarzenia, właściwe zaś rozpoczęcie procesu profilowania jest możliwe dopiero po ustaleniu mechanizmu zgonu ofiary oraz charakteru doznanych przez nią obrażeń. Jest to bowiem podstawa odtwarzania zachowania przestępcy.

Wskazane tu przykłady typowych elementów branych pod uwagę podczas profilowania ze względu na stopień ogólności mogą wywołać lekko drwiący uśmiech u osób, które zajmują się sporządzaniem profilu. Wystarczy zastanowić się, w jaki sposób zdefiniować zachowania wspominanego Leszka Pękalskiego – osoby lekko upośledzonej, drapieżnika, któremu zupełnie obojętny był sposób działania, byle tylko zmierzał do seksualnego zaspokojenia. Oto ich opis: […] *ponieważ kobiety miały pogryzione piersi, wykonano silikonowy odlew mordercy ze słabo wykształconą górną trójką. Istniało podejrzenie, że sprawca jest zarażony chorobą weneryczną. Rozesłaliśmy informacje do wszystkich gabinetów stomatologicznych i poradni wenerologicznych. Bez rezultatu. Tymczasem po wielu latach otrzymaliśmy informację z komendy słupskiej, że zatrzymano człowieka, który przyznaje się do tych morderstw. Pękalski, zaznaczając na mapie miejsca, gdzie dokonywał zbrodni, obwiódł kółkiem także nasze miasto. Przywieziony na wizję lokalną dotycząca pierwszej ze spraw wskazał jeszcze dwa inne miejsca. Miejsca zabójstw Moniki i Jolanty.* […] *dziś wiemy, że bardzo lubił się przemieszczać, jeździć z miasta do miasta pozornie bez celu. Mamy w policyjnych aktach jeszcze inne niewyjaśnione do dzisiaj mordy o zbliżonym modus operandi, dlatego istnieje podejrzenie, że Pękalski może być ich sprawcą*[36].

34 B. Hołyst, *Psychologia kryminalistyczna,* Warszawa 2009, s. 1430.

35 M. Całkiewicz, *Modus operandi...,* op.cit., s. 191 i nast.

36 M. Omilianowicz, *Bestia. Studium zła*, Warszawa 2016, s. 72–73.

Profilowanie nie zna granic. Przykłady pochodzą nie tylko z Polski czy Stanów Zjednoczonych. W jaki sposób ujawnić sprawcę wyłącznie jednego zabójstwa, zwłaszcza gdy nie ma już ciała? Issei Sagawa, dziś żwawy 71-latek, to autor poczytnych japońskich nowel, aktor filmów erotycznych, który w 1981 roku jako student literatury angielskiej na Sorbonie zaprosił holenderską koleżankę Renée Hartevelt na kolację połączoną z dyskusją na temat literatury. Następnie ją zastrzelił, zgwałcił jej zwłoki i zjadał je w ciągu dwóch dni.

Zapewne przykład starszego kolegi znany był zabójcy dwójki dzieci, 14-latkowi Sakakibarze Seito, którego Sagawa uczynił bohaterem jednej ze swoich książek. […] *Dzisiaj przeprowadziłem świetny eksperyment, który potwierdził, jak kruche są istoty ludzkie. Wziąłem ze sobą młotek i zaszedłem jakąś dziewczynę od tyłu. Kiedy odwróciła się w moją stronę, uderzyłem ją kilka razy, już nie pamiętam ile. Byłem zbyt podekscytowany, by zapamiętać.* […] *Dzisiaj rano mama powiedziała do mnie: Biedna dziewczynka. Ta zaatakowana dziewczyna zmarła. Nie ma żadnych sygnałów, żeby byli na moim tropie*[37].

Nierzadko jest tak, że z pozoru sytuacja wydaje się oczywista. Nawet jeśli tak jest, to rolą organów ścigania jest dotarcie do prawdy obiektywnej. Dlatego nie można ignorować jakichkolwiek faktów, które mogą podważyć dotychczasowy wynik postępowania i skierować je na inny tor. Dopiero całokształt okoliczności pozwoli na właściwą interpretację. Wszystkie zasady mają na celu pomóc w opisaniu *modus operandi* sprawcy[38].

PODSUMOWANIE

Profilowanie kryminalne, czyli profilowanie psychologiczne, jest czynnością usprawniającą proces wykrywczy. Jednak w niewielkim stopniu znajduje odzwierciedlenie w kompleksowych opracowaniach naukowych na temat tego zagadnienia w naszym kraju[39].

Mimo że praca profilera wygląda fascynująco w serialach i towarzyszą jej emocje, w rzeczywistości oczekuje się od niego, że uczyni cud. W literaturze pojawia się nawet tzw. syndrom CSI. *Efekt* CSI to wiara w nieomylność techniki kryminalistycznej i jej zdolność do rozwiązania wszelkich spraw kryminalnych.

W naszym kraju nie ma kogoś takiego jak zawodowy profiler. Ogromna większość osób wykonujących zadanie profilowania to policjanci, psycholodzy, biegli sądowi i psychiatrzy czy specjaliści, zatem osoby mające odpowiednią wiedzę, doświadczenie i umiejętności.

Każdemu, kto chce zrobić karierę jako profiler, można poradzić, aby:

– skończył studia związane z badaniem psychiki ludzkiej, psychologię, socjologię, antropologię itp., medycynę ze specjalnością psychiatria lub też prawo;

– zdobył doświadczenie, pracując w jednostce związanej z policją i sądownictwem, np. w prokuraturze, urzędzie sądowym, jednostce policyjnej itp.;

– dopiero po zdobyciu wiedzy oraz odpowiedniego doświadczenia ubiegał się o stanowisko profilera[40].

Bartosz W. Wojciechowski na łamach „Palestry" stwierdził, że po wnikliwej lekturze kilku profili można jednak odnieść wrażenie, że do sporządzenia opinii nie jest konieczne posiadanie wykształcenia psychologicznego i specjalnej wiedzy. Wystarczy logiczne myślenie i dokładna lektura kolejnych tomów akt. Poza tym we wcześniejszym fragmencie artykułu wspomina, powołując się na „Journal of Interpersonal Violence", że zgodnie z wynikami badań, aby sporządzić profil psychologiczny, nie trzeba posiadać szczególnej wiedzy, bogatego doświadczenia w pracy śledczej i intuicji. Studenci chemii i rekruci policyjni osiągali znacznie lepsze wyniki w czasie eksperymentów. Tworzyli bowiem pełniejsze, bardziej szczegółowe i trafne profile psychologiczne niż doświadczeni w tworzeniu profili detektywi.

Szanując i przyjmując tę opinię, wywołującą z pewnością satysfakcję wśród osób zaczynających lub planujących swoją karierę jako profiler kryminalny, warto jednak postawić sobie większe wymagania. Choć oczywiście wiedza i duże doświadczenie w zawodzie oraz udział w tworzeniu wielu profili nie gwarantują skuteczności, jaką finalnie jest ujęcie sprawcy czynu zabronionego. Profiler musi być uczciwy wobec samego siebie. Musi zachować obiektywizm, nie może kierować się własnymi wrażeniami, lecz logiką.

Praca profilera – czy to studenta, czy profesora psychiatrii lub medycyny sądowej może prowadzić do ekscytującego finału, jakim jest przyczynienie się do ujęcia sprawcy zbrodni. Każda sprawa, człowiek, sprawca są inni. Zatem i profilowanie ma tę cechę, że dotyczy spraw niepowtarzalnych. Każdy bowiem przypadek jest inny, co skutecznie zapobiega rutynie lub znudzeniu wykonywaną pracą. Im bardziej nietypowa sprawa, im bardziej zawiła motywacja sprawcy, często nie do końca poczytalnego, tym typowanie trudniejsze, uzyskiwane innymi metodami, ale sprawiające większą satysfakcję. Jest to niewątpliwie argument, aby kwestii profilowania kryminalnego przyjrzeć się bliżej i to zarówno w ramach kreowania swojej przyszłości, jak i prowadzenia badań naukowych na ten temat. ■

37 Por. http://kryminalnajaponia.blogspot.com/2018/02/morderstwadzieci-w-kobe-prawdopodobnie.html/. 5.08. 2020.

38 M. Niewińska, *Profilowanie nieznanych*..., op.cit.

39 A. Gawliński, B. Lach, *Profilowanie kryminalistyczne...*, op.cit., s. 384 i nast.

40 J. Gołębiowski, K. Grochowska, *Profilowanie kryminalne na potrzeby sądu. Kontrowersje wokół przydatności*, https://www.biblioteka-cyfrowa.pl /publication/58993/. 5.08. 2020 r., op.cit., https://www.biblioteka cyfrowa.pl/publication/58993/. 5.08.2020.

Dear Readers,

in many publications on future armed conflicts, their authors proclaim that such conflicts will not only be conducted with the use of military potential, but also, if not majorly, with the help of non-military measures aimed at destructing a potential enemy. Conventional activities will be supported by those of intelligence, political, psychological, economic, informational, humanitarian and social nature. At the same time, the use of above-mentioned non-military warfare tools and the use of armed violence indicates that such a war can be qualified as a hybrid war. With all certainty, someday robots will replace soldiers on the future battlefield in performing the most extreme tasks. Cyber soldiers will be used particularly by the land forces, which are most vulnerable to enemy fire, and, in consequence, to battle casualties. Warfare causing too many personnel losses generally does not pave the way to an easy success, and may even make it entirely impossible. Moreover, in the future armed conflicts, a significant role will be played by informational and cyberspace warfare activities.

The above issues will be addressed in the cycle of our articles, where their authors, taking into account current achievements in military technology, make an attempt to forecast the course of armed conflicts. Some interesting conclusions come to mind after reading, particularly if it comes to defense industry capabilities in different countries in the matter of equipping naval and air platforms so they meet challenges of the future battlefield.

The Przegląd Sił Zbrojnych articles explain and interpret cyberspace, and the capabilities both sides of the conflict can have and use. One of the articles explains the meaning of cyberspace in the civil environment, or specifically in communication aviation, and an discusses attempts to regulate this issue as presented in adequate documents of international organizations.

There is also a material explaining the rules for boresighting and calibrating the Beryl carbine with the holographic weapon sight (HWS).

We also present the articles of last-year graduates of the Military Faculty at the War Studies University (ASzWoj), where they discuss some military state security issues, including the significance of certain Polish territories.

Last but not least, there are also articles on: the significance of communication infrastructure in our country for forces redeployment; the transportation of dangerous goods according to the ADR regulations (e.g. designation of cargo and vehicles that carry them); the system solutions about the formation of cybernetic defense forces, which entered into force in the Polish Armed Forces; the use of tanks during peace-keeping activities following the separation of feuding sides of the conflict; and on the evolution of NATO normative documents in the area of civil and military cooperation.

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.



#SZCZEPIMYSIĘ

WWW.GOV.PL/**SZCZEPIMYSIE**

MINISTERSTWO OBRONY NARODOWEJ