4

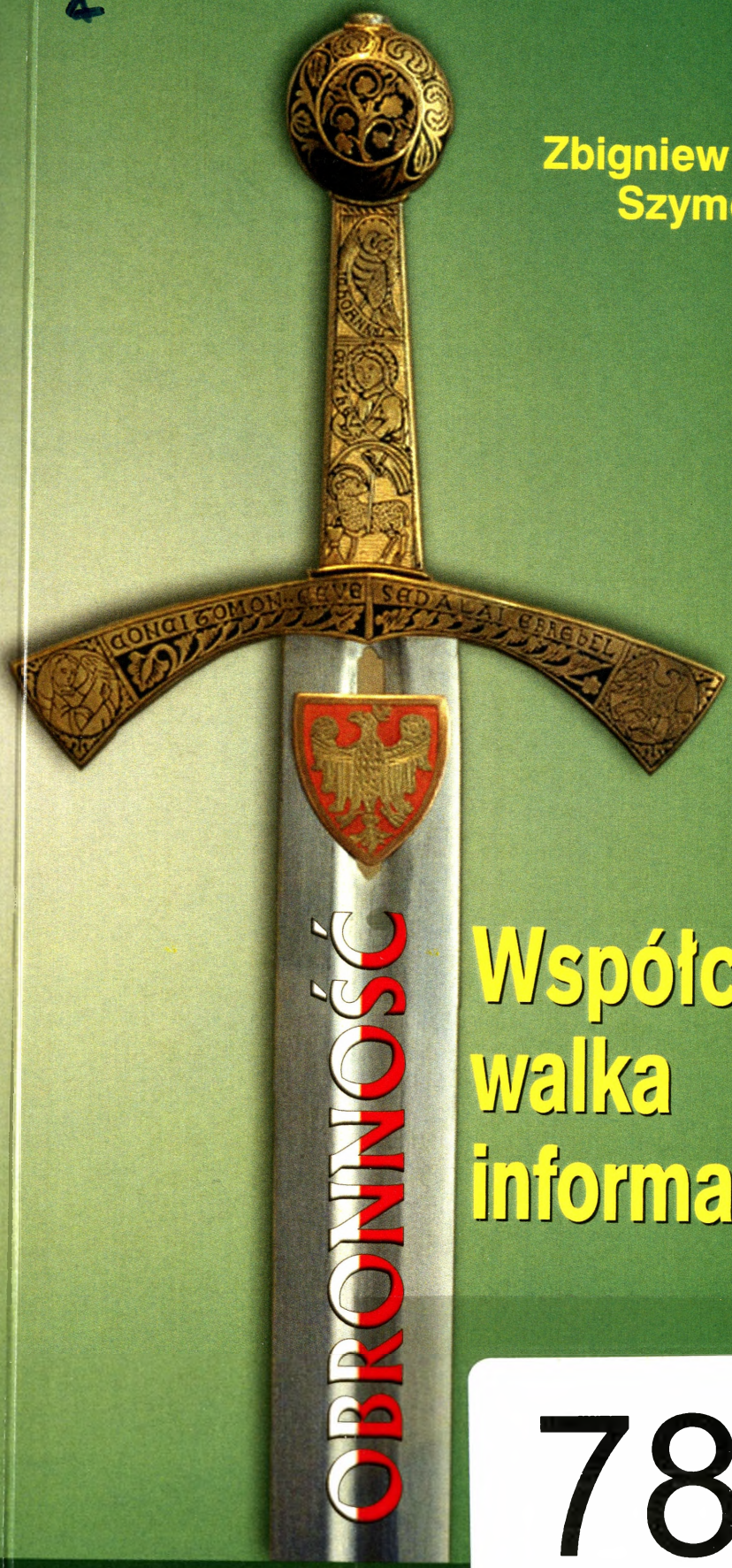
Zbigniew Modrzejewski
Szymon Markiewicz

Współczesna walka informacyjna

OBRONNOŚĆ

AKADEMIA OBRONY NARODOWEJ

Zbigniew Modrzejewski
Szymon Markiewicz



OBRONNOŚĆ

Współczesna walka informacyjna

AKADEMIA

Współczesna walka informacyjna

AKADEMIA OBRONY NARODOWEJ

Zbigniew Modrzejewski
Szymon Markiewicz

Współczesna walka informacyjna

WARSZAWA 2016

Recenzenci
płk prof. dr hab. Marek Wrzosek
płk dr hab. inż. Waldemar Kawka

Zespół autorski
ppłk dr Zbigniew Modrzejewski – wstęp, rozdział 1 i 2, zakończenie
ppłk dr Szymon Markiewicz – rozdział 3

Opracowanie redakcyjne i korekta
Joanna Adamiec-Siemiątkowska

Projekt okładki
Genowefa Majchrowska

Redakcja techniczna i skład
Małgorzata Gawłowska

ISBN 978-83-7523-513-5

Sygn. AON 6410/16

Skład, druk i oprawa: Wydawnictwo Akademii Obrony Narodowej
00-910 Warszawa, al. gen. A. Chruściela 103, tel. 261-814-055, tel./faks 261-813-752
e-mail: wydawnictwo@aon.edu.pl
Zam. nr 857/16

Spis treści

Wstęp

Współcześnie nie trzeba już chyba nikogo przekonywać, że informacja odgrywa kluczową rolę zarówno w sektorze cywilnym, jak i wojskowym. W opinii ekspertów wojskowych informacja jest zasadniczym przedmiotem walki informacyjnej.

Prawie każdy środek bojowy na polu walki jest wyposażony w urządzenia odbierające, przetwarzające i przekazujące informacje. Pozbawienie przeciwnika tych zdolności może być główną przyczyną jego porażki.

Uwarunkowania współcześnie prowadzonych w sferze informacji działań oraz tempo zmian wielu czynników mających bezpośredni wpływ na ich prowadzenie powodują konieczność przedstawienia stanu obecnego tych przedsięwzięć oraz określenia kierunków dalszych zmian.

Analiza istoty konfliktów pozwala na określenie ich podmiotu, którym niezmiennie pozostaje człowiek będący głównym użytkownikiem informacji.

Rozwój środków komunikacji masowej miał znaczący wpływ na rozwój walki informacyjnej. Osiągnięcia technologiczne stosowane na rynku cywilnym są wykorzystywane z powodzeniem przez sferę militarną. Powstały dzięki temu nowe możliwości w zakresie manipulowania świadomością człowieka oraz prowadzenia walki elektronicznej, dezinformacji oraz oddziaływania na środki elektroniczne przeciwnika przez atakowanie i obezwładnianie posiadanych przez niego nośników informacji.

Amerykańska Rada Wywiadu Narodowego (*National Intelligence Council* – NIC) opracowała długoterminową analizę pt. *Global Trends 2025. A Transformed World* (*Globalne Trendy 2025. Świat przekształcony*), w której zawarła przewidywania służb wywiadu co do przyszłości świata do 2025 roku. Zdaniem amerykańskiego wywiadu działania wojenne w 2025 roku będą charakteryzować cztery zasadnicze trendy.

Pierwszy to newralgiczne znaczenie informacji – zaawansowane technologie informatyczne polepszą precyzyjność broni, wzmocnią celność i nawigację, podniosą jakość dowództwa i kontrolę oraz zwiększą użycie sztucznej inteligencji i robotów. Rosnąca rola technologii informatycznych wzmocni znaczenie informacji i uczyni ją podstawowym celem przyszłych konfliktów. Do 2025 roku

niektóre państwa prawdopodobnie rozwiną broń zaprojektowaną do niszczenia i unieszkodliwiania informacji, czujników, sieci i systemów komunikacyjnych, włączając antysatelity, częstotliwości radiowe i broń laserową.

Drugim trendem jest ewolucja potencjału niesymetrycznych działań wojennych – rozprzestrzenianie się nowoczesnej lekkiej broni precyzyjnej oraz technologii informatycznych i komunikacyjnych w dużym stopniu zwiększą możliwości niesymetrycznych aktorów do organizowania, koordynowania i przeprowadzania rozproszonych operacji.

Kolejnym kierunkiem jest rosnące znaczenie pozamilitarnych aspektów działań wojennych. Oznacza to, że w ciągu najbliższych dwudziestu lat dominującą rolę będą odgrywać cybernetyczne, ekonomiczne, surowcowe, psychologiczne i informacyjne aspekty konfliktu. Aktorzy podejmować będą działania medialne w celu zdominowania 24-godzinnego przekazu i manipulacji opinią publiczną, aby uzyskać jej poparcie.

Ostatni, ale nie mniej ważny, trend stanowi ekspansja i eskalacja poza tradycyjne pola walki konfliktów, których powstrzymywanie w przyszłości będzie trudniejsze. Zaawansowane możliwości broni takiej, jak broń precyzyjna, broń dalekiego zasięgu, proliferacja BMR, rozwój nowych form działań wojennych (cybernetyczne, kosmiczne) będą prowadzić do eskalacji i ekspansji konfliktów przez państwowych i niepaństwowych aktorów poza tradycyjne pola walki[1].

Uznanie informacji za zasób strategiczny zarówno w wymiarze militarnym, jak i pozamilitarnym, spowodowało powstanie kategorii walki informacyjnej. Walki, w której informacja traktowana jest z jednej strony jako broń, zaś z drugiej – jako cel ataku.

Walka informacyjna towarzyszyła zawsze walce zbrojnej. W tej sferze odgrywała szczególną rolę niezależnie od tego, czy była tak formalnie nazywana, czy też nie. W historii wojen trudno znaleźć przykład, w którym strona przegrana w walce informacyjnej zdołała odnieść zwycięstwo w walce zbrojnej[2].

Synteza wniosków z doświadczeń zarówno odległych w czasie, jak i współczesnych konfliktów zbrojnych (szczególnie działań militarnych na terenie byłej Jugosławii, w Iraku i w Afganistanie), wskazuje, że walka informacyjna była prowadzona od zawsze. Jednak wraz z rozwojem cywilizacyjnym w sferze informacyjnej stwarzane są nowe możliwości w zakresie jej prowadzenia.

1 *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA*, Vis-a-vis Etiuda, Kraków 2010, s. 195–196.

2 L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999, s. 10.

1. Walka informacyjna – identyfikacja znaczeniowa terminu

Powstanie kategorii walki informacyjnej związane jest bezpośrednio z uznaniem informacji za zasób strategiczny organizacji i traktowanie jej zarówno jako broń oraz jako cel ataku. Pojawienie się pojęcia walki informacyjnej dopiero pod koniec XX wieku związane jest bez wątpienia z rewolucją informacyjną w zakresie technologii pozyskiwania, przetwarzania i wykorzystania informacji.

Sam termin po raz pierwszy został użyty w latach 90-tych XX wieku. W 1994 roku w strukturze Narodowego Uniwersytetu Obrony Stanów Zjednoczonych w Waszyngtonie powstała Szkoła Strategii i Walki Informacyjnej. W tym samym roku Winn Schwartau opublikował książkę na temat walki informacyjnej, w której definiował ją jako działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też jako zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[1].

Walka w sferze informacyjnej nie jest zatem zjawiskiem nowym i zawsze towarzyszyła walce zbrojnej, w której wyodrębniano trzy elementarne czynniki: ruch, rażenie oraz właśnie informację. Informacja jest niematerialnym czynnikiem spinającym pozostałe elementy walki zbrojnej w zharmonizowaną całość starcia zbrojnego[2]. W tej funkcji przejawia się w dowodzeniu, a przez rozpoznanie, maskowanie, dezinformowanie, walkę radioelektroniczną itp. jest również czynnikiem bezpośredniego oddziaływania na przeciwnika[3].

1 Por. P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005, s. 132.

2 S. Koziej, *Czynniki walki zbrojnej*, „Zeszyty Naukowe AON" 1993, nr 4, s. 57–62.

3 Por. S. Koziej, *Teoria sztuki wojennej*, wyd. 2, Bellona, Warszawa 2011, s. 110.

1.1. Desygnaty pojęć walka i informacja

W strukturze pojęcia walki informacyjnej zasadniczym determinantem rzutującym na całokształt przedmiotu myślowego jest wyraz „walka", zaś „informacja" jest elementem uzupełniającym.

Ciekawy pogląd na zagadnienie walki w sensie ogólnoprakseologicznym przedstawił T. Kotarbiński, zdaniem którego walka to „wszelkie działanie przynajmniej dwupodmiotowe (przy założeniu, że i zespół może być podmiotem), gdzie jeden przynajmniej z podmiotów przeszkadza drugiemu"[4]. A zatem oba podmioty nie tylko dążą obiektywnie do celów niezgodnych, lecz także wiedzą o tym i liczą się w budowaniu swoich planów działania z działaniami strony przeciwnej. Zdaniem autora przypadek wzajemnego, obiektywnego i zarazem świadomego przeszkadzania jest najciekawszy, gdyż wtedy obie strony zmuszają się wzajemnie do pokonywania trudności, a więc pośrednio do usprawniania techniki działania.

Oczywiście prakseologia nie ogranicza pojęcia „walka" jedynie do wrogiego starcia o motywacji nieżyczliwej dla przeciwnika. Walką jest również współzawodnictwo w pracy, czy współzawodnictwo sportowe (np. walka bokserska, czy mecz piłkarski).

Walka to kooperacja negatywna przynajmniej dwóch sprawców, spośród których każdy stara się osiągnąć cel niezgodny z celem drugiego, przy czym wie o działaniu przeciwnika i przeciwdziała mu[5].

Walka to zbrojne starcie dwóch przeciwstawnych stron (od pojedynczego żołnierza do związku taktycznego włącznie), dążących do osiągnięcia różnych, niezgodnych celów, zadań, zamierzeń, usiłujących siłą, przede wszystkim zbrojnie, oraz podstępem przeszkodzić sobie wzajemnie (rozbić, zniszczyć, obezwładnić)[6].

Walka to zespół bojów oddziałów i pododdziałów, prowadzonych zgodnie z zamiarem dowódcy taktycznego i pod jego bezpośrednim dowództwem, dla osiągnięcia celu operacyjnego (celów taktycznych)[7].

Walka zatem zarówno w ujęciu T. Kotarbińskiego, jak i z punktu widzenia cybernetyki, utożsamiana jest z wzajemną kooperacją negatywną. Są to wszel-

4 T. Kotarbiński, *Traktat o dobrej robocie*, wyd. 3, popr. i uzup., Ossolineum, Wrocław–Warszawa–Kraków 1965, s. 239.

5 T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław–Warszawa–Kraków–Gdańsk 1978, s. 267.

6 *Leksykon wiedzy wojskowej*, MON, Warszawa 1979, s. 472.

7 M. Huzarski, J. Wołejszo (red. nauk.), *Leksykon obronności. Polska i Europa*, Bellona, Warszawa 2014, s. 38.

kie działania zbiorowe, w których biorą udział przynajmniej dwa układy, przy czym jeden z nich przeszkadza drugiemu.

Termin, który ściśle wiąże się z pojęciem walki i stanowi niejako jego rozwinięcie to walka zbrojna.

Walka to całokształt przedsięwzięć realizowanych w czasie działań wojennych przez siły zbrojne przy użyciu broni[8].

Walka zbrojna to rodzaj walki polegający na prowadzeniu działań, których celem jest zniszczenie (obezwładnienie) przeciwnika przy wykorzystaniu broni. Może być prowadzona na lądzie (walka lądowa), w powietrzu (walka powietrzna) i na morzu (walka morska). Ze względu na skalę zjawiska może występować na szczeblu strategicznym jako kampania, operacyjnym jako bitwa lub operacja oraz taktycznym jako walka (bój)[9].

Walka zbrojna to podstawowa forma zbrojnych działań wojennych. Bezpośrednie starcie zgrupowań wojsk, wzajemne destrukcyjne oddziaływanie za pomocą posiadanych środków rażenia oraz fizyczne i psychiczne obezwładnianie przeciwnika jako przeszkody na drodze do celu[10].

Najczęściej w opinii ekspertów zasadniczym przedmiotem walki informacyjnej jest informacja. Dlatego też w opinii zespołu autorskiego należy wyjaśnić ten termin dla zrozumienia istoty walki informacyjnej.

W potocznym rozumieniu informacja jest zwykle utożsamiana z przedmiotami myślowymi, odzwierciedlającymi wszelkie wiadomości, wieści, nowiny lub rzeczy zakomunikowane[11].

Zgodnie z zapisami encyklopedycznymi informacja to każdy czynnik zmniejszający stopień niewiedzy (nieokreśloności) o badanym zjawisku, umożliwiający człowiekowi, organizmowi żywemu lub urządzeniu automatycznemu polepszenie znajomości otoczenia i w sprawniejszy sposób przeprowadzenia celowego działania; źródłem informacji są odbierane wiadomości, a miarą informacji jest ilość informacji[12].

K. Kolegowicz uważa, że potocznie pojęcie informacji kojarzy się z takimi określeniami, jak wiedza, dane, wiadomość. Jest to duże uproszczenie, ponie-

8 *Leksykon...*, dz. cyt., s. 474.

9 *Regulamin działań wojsk lądowych*, DWLąd., Warszawa 2008, s. 21.

10 M. Huzarski, J. Wołejszo (red. nauk.), *Leksykon...*, dz. cyt., s. 38.

11 W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980, s. 429.

12 *Encyklopedia powszechna PWN*, t. 2, PWN, Warszawa 1974, s. 281.

waż dopiero po transformacji danych i wiadomości oraz nadaniu im konkretnych cech charakterystycznych stają się one informacjami[13].

J. Penc podaje, że w rozumieniu nauki o zarządzaniu informacja oznacza wiedzę potrzebną do określenia i realizacji zadań służących do osiągnięcia celów organizacji, a ściślej: właściwość wiadomości lub sygnału polegającą na zmniejszaniu nieokreśloności lub niepewności co do stanu albo dalszego rozwoju sytuacji, której ta wiadomość dotyczy.

Informację zdefiniowano również na potrzeby wojska, gdzie oznacza ona „nieprzetworzone fakty opisane w dowolny sposób i powiązane z innymi cząstkowymi informacjami, które poddane analizie przez sztabowe komórki rozpoznawcze tworzą wiadomości rozpoznawcze. Pozyskane (zdobyte) informacje powinny być wartościowe z punktu widzenia ich użyteczności, wiarygodności, aktualności i kompletności zawartych w sobie treści"[14].

Informacja zatem składa się z pojedynczego faktu lub grupy faktów (danych), które zostały pozyskane (zdobyte) przez potencjał rozpoznawczy i stanowi ona opis zaistniałego stanu rzeczy w określonym czasie i przestrzeni.

Zdaniem L. Ciborowskiego informacja to bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia itp.), który w jego przekonaniu (świadomości) kojarzy się jakoś z tym bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują ludzką wyobraźnię do działania. Jej istnienie jest relatywnie związane z istnieniem człowieka i jego umysłem[15].

W celu ukazania złożoności terminu „informacja" w tabeli 1 przedstawiono kilka definicji tego pojęcia.

Zdaniem P. Sienkiewicza obecnie o rezultatach zmagań wojennych informacja decydować będzie w stopniu porównywalnym z tradycyjnym stosunkiem sił, efektywnością systemów dowodzenia, kierowania, łączności, rozpoznania i walki radioelektronicznej[16].

13 K. Kolegowicz, *Wartość informacji a koszty jej przechowywania i ochrony* [w:] R. Borowiecki, M. Kwieciński (red.), *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (wybrane problemy teorii i praktyki)*, Kantor Wydawniczy Zakamycze, Kraków 2003.

14 *Doktryna Rozpoznanie wojskowe D/2*, Szt. Gen., Warszawa 2013, s. 14.

15 L. Ciborowski, *Walka...*, dz. cyt., s. 185–186.

16 P. Sienkiewicz, *Informatyczne wspomaganie dowodzenia*, „Myśl Wojskowa" 1993, nr 1.

Tabela 1

Porównanie definicji informacji

Autor i tytuł publikacji	Definicja
C.E. Shannon, *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana 1949.	Informacją jest to wszystko, co nie jest ani energią, ani masą, czyli jest zasilaniem – jest to każde rozpoznanie stanu układu, odróżnialnego od innego stanu układu.
L. Couffignal, *Les machines a penser*, Les Editions de Minuit, Paris 1964.	Informacja to zespół nośnika i semantyki, gdzie semantyka jest efektem psychicznym informacji, a nośnik jest zjawiskiem fizycznym skojarzonym z semantyką w celu utworzenia informacji. Przy tłumaczeniu tekstu z jednego języka na inny, informacje zawarte w tekście początkowym pozostają takie same, chociaż zmieniła się ich forma.
M. Mazur, *Jakościowa teoria informacji*, WNT, Warszawa 1970.	Informacja to transformacja jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji.
Henryk Greniewski, *Sprawy wszystkie i jeszcze inne (o logice i cybernetyce)*, KiW, Warszawa 1970.	W języku potocznym wyraz „informacja" używany jest zwykle w ten sposób, że spełnione są trzy warunki poniższe: – każda informacja jest wiadomością o czymś, – informację uzyskuje tylko człowiek (przez obserwację lub czynność umysłową), – informację przekazuje tylko człowiek człowiekowi. Natomiast w cybernetyce używa się pojęcia informacji w rozumieniu dużo szerszym. Uogólnienie pojęcia informacji – etap I Nie tylko każda wiadomość, lecz również każda decyzja, każdy nakaz, zakaz, zalecenie, sugestia jest informacją. Uogólnienie pojęcia informacji – etap II Przez „informację" będziemy odtąd rozumieli: – wszelkie uzyskiwanie danych nie tylko przez człowieka, lecz również przez dowolną istotę żywą, organ człowieka lub innej istoty żywej, a także przez maszynę lub jej organ, – wszelkie przekazywanie danych między ludźmi, istotami żywymi i maszynami (ewentualnie organami istot żywych lub maszyn).
Encyklopedia organizacji i zarządzania, PWE, Warszawa 1982.	Pojęcie podstawowe nie w pełni zdefiniowane z uwagi na jego pierwotny, elementarny charakter. Wszystkie dotychczasowe próby definiowania go uważa się powszechnie za niezadowalające, a co najwyżej za ukazujące tylko niektóre aspekty (...).

Autor i tytuł publikacji	Definicja
Leksykon zarządzania, Difin, Warszawa 2004.	Informacja to przeanalizowana i przetworzona do postaci zrozumiałej dla odbiorcy wiadomość (dana, sygnał), która powiadamia go o sytuacji i ma dla niego wartość w procesie decyzyjnym. Informacja jest pojęciem węższym niż dana, zawiera bowiem tylko te fakty i liczby, które są przedstawione w formie zrozumiałej dla odbiorcy, dotyczą obszaru zainteresowań odbiorcy, posiadają wartość dla odbiorcy, nie powielają zasobów posiadanej wiedzy (...).
N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, The M.I.T. Press and John Wiley & Sons, Inc., New York–London 1961.	Informacja to nazwa treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy do niego swoje zmysły.
E. Niedzielska (red.), *Informatyka ekonomiczna*, AE we Wrocławiu, Wrocław 1998.	Informacja jest specyficznym dobrem niematerialnym, które w miarę postępu gospodarczego oraz rozwoju środków i form komunikowania się społecznego nabiera coraz większego znaczenia, przeobrażając oblicze wielu tradycyjnie zorganizowanych gospodarek świata.

Opracowanie własne.

1.2. Walka informacyjna, wojna informacyjna i operacje informacyjne

W obszarze terminologicznym dotyczącym walki informacyjnej, traktuje się ją niekiedy jako synonim takich pojęć, jak operacje informacyjne lub wojna informacyjna. Jednak w opinii autora jest to błąd, gdyż o ile walka i operacje informacyjne odnoszą się głównie do działań prowadzonych w czasie kryzysu i konfliktu i mogą być prowadzone w czasie pokoju, to wojna informacyjna, jak wskazuje sam termin, może być prowadzona wyłącznie w czasie wojny.

Zdaniem wspomnianego już P. Sienkiewicza walką informacyjną (*information warfare*, *infowar*) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych)[17].

17 P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] L. Haber (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość*, BG AGH, Kraków 2003, s. 375.

W opinii L. Ciborowskiego walka informacja jest kooperacją negatywną wzajemną, przynajmniej dwupodmiotową, realizowaną w sferach zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistycznej strony drugiej. Istotą walki informacyjnej w działaniach zbrojnych jest stwarzanie sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych, przy jednoczesnej obronie przed tym samym wojsk własnych. Jest ona ukierunkowana na dezorientowanie przeciwnika co do sytuacji na polu walki, komplikowanie jego warunków działania i w efekcie tego na zmuszanie go do podejmowania błędnych decyzji i chybionych reakcji[18].

Walkę informacyjną postrzega się jako działania informacyjne prowadzone podczas kryzysu i konfliktu po to, aby osiągnąć lub promować określone cele w stosunku do zdefiniowanego przeciwnika lub przeciwników[19].

W tabeli 2 przedstawiono kilka przykładów definicji pojęcia walki informacyjnej.

Jak podkreślają P. Sienkiewicz i H. Świeboda, nie istnieje jedna, uzgodniona definicja walki informacyjnej, jednak w większości proponowanych rozwinięć tego terminu występują wspólne treści. Wszystkie one sprowadzają się do postrzegania walki informacyjnej jako konfliktu, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią, obejmującym jednocześnie fizyczne niszczenie infrastruktury wykorzystywanej przez przeciwnika do działań operacyjnych. Obecnie słusznie uważa się, że *cyberwar*, *infowar,* walka informacyjna, cyberterroryzm, *netwar,* wojownicy informacyjni, dominacja informacyjna, obrona w cyberprzestrzeni (*cyberspace defence*) czy chaos informacyjny to tylko synonimy, dotyczące tego samego, ale bardzo szerokiego, pojęcia wojny ery informacyjnej (*information age warfare*)[20].

18 L. Ciborowski, *Walka...*, dz. cyt., s. 187.

19 G.J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Wydawnictwo Naukowo-Techniczne, Warszawa 2004, s. 240.

20 P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 80.

Tabela 2

Porównanie definicji walki informacyjnej

Autor i tytuł publikacji	Definicja
M. Libicki, *What is Information Warfare?*, NDU, Washington 1995.	Walka informacyjna jako samodzielna technika prowadzenia wojny nie istnieje. Istnieje natomiast kilka oddzielnych form walki informacyjnej, z których każda pretenduje do bycia ogólniejszą koncepcją. Obecnie można wyróżnić siedem form walki informacyjnej – konfliktu, który zawiera ochronę, manipulację, degradację lub uniemożliwienie dostępu do informacji.
Joint Publication 3-13, Joint Doctrine for Information Operations, Joint Chiefs of Staff, Washington 1998.	Walka informacyjna to działania informacyjne prowadzone w czasie kryzysu lub konfliktu dla osiągnięcia pożądanych celów w relacjach z przeciwnikiem lub wsparcia działań prowadzących do tych celów.
R. Stark, *Future Warfare: Information Superiority through Info War*, School of Advanced Military Studies, Leavenworth 2000.	Walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią.
G. Nowacki, *Współczesne poglądy na prowadzenie walki informacyjnej*, AON, Warszawa 2001.	Walka informacyjna jest to kooperacja negatywna wzajemna w sferze rozpoznania (zdobywania informacji), zakłócania informacyjnego i obrony informacyjnej. Gdzie każdemu działaniu jednego podukładu tej walki jest przyporządkowane działanie antagonistyczne dwóch pozostałych podukładów strony przeciwnej.
P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość*, Haber L. (red.), Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003.	Walką informacyjną (*information warfare, infowar*) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych).

Opracowanie własne.

Zdaniem P. Sienkiewicza istotą walki informacyjnej jest:

– zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych,

– zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych[21].

21 P. Sienkiewicz, *Wizje...*, dz. cyt., s. 375.

Analizując kwestie walki informacyjnej, B. Balcerowicz zauważa, że może być ona zjawiskiem autonomicznym, komponentem wspierającym działania militarne bądź głównym, wspieranym działaniami militarnymi[22].

Zgodnie z przyjętą w NATO definicją walka informacyjna to działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego, z zamiarem promowania określonego celu politycznego lub wojskowego, w odniesieniu do wskazanego przeciwnika lub przeciwników. Jej elementami wykonawczymi są operacje informacyjne dotyczące działań wspierających, wyselekcjonowane cele polityczne i wojskowe, podejmowane z zamiarem wpłynięcia na decydentów i polegające na oddziaływaniu na procesy informacyjne atakowanej strony, procesy oparte na informacji oraz systemy dowodzenia łączności i rozpoznania, przy równoczesnym zapewnieniu odpowiedniej ochrony własnemu systemowi informacyjnemu. Aktywne formy operacji informacyjnych obejmują szereg działań z zakresu rozpoznania wojskowego, bezpieczeństwa informacji, działań psychologicznych, dezinformacji, walki elektronicznej oraz niszczenia fizycznego wybranych elementów systemów informacyjnych przeciwnika[23].

D.E. Denning używa pojęcia wojny informacyjnej, aby określić działania, których celem jest zdobycie lub wykorzystanie zasobów informacyjnych[24]. Na wojnę informacyjną składają się zatem ofensywne i defensywne działania skierowane przeciw zasobom informacyjnym.

Zdaniem autorów publikacji *Zintegrowane prowadzenie operacji informacyjno-psychologicznych w ramach narodowych i sojuszniczych działań połączonych* wojna informacyjna jest jednym z podstawowych przedsięwzięć, polegającym na użyciu różnorodnych środków do uzyskania przewagi informacyjnej w ogóle. Pojęcie wojen informacyjnych dotyczy kwestii użycia środków elektronicznych, jak i przedsięwzięć obejmujących wszelkie działania zmierzające do naruszenia systemów informacyjnych podczas wojny, kryzysu i pokoju[25].

22 B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Wydawnictwo Naukowe Scholar, Warszawa 2010, s. 179.

23 M. Wrzosek, *Dezinformacja - skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2, s. 18.

24 D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, s. 23.

25 P. Biskup, R. Zając, M. Kuszmider, E. Chomicz, *Zintegrowane prowadzenie operacji informacyjno-psychologicznych w ramach narodowych i sojuszniczych działań połączonych – praca studyjna GZPS-P5*, Warszawa 2005 [za:] K. Rokiciński, B. Pac, *Operacje informacyjne w działaniach militarnych*, Akademia Marynarki Wojennej, Gdynia 2010, s. 21.

Amerykańskie Kolegium Połączonych Szefów Sztabów w dokumencie *Joint Doctrine for Command and Control Warfare* (*C2W*) zdefiniował wojnę informacyjną jako działania podjęte w celu osiągnięcia dominacji informacyjnej przez wpływ na informacje przeciwnika, jego czynności oparte na informacji, systemy informacyjne oraz sieci komputerowe. Jako elementy walki informacyjnej można zatem wskazać: destrukcję fizyczną, operacje bezpieczeństwa, operacje psychologiczne, sabotaż i walkę elektroniczną.

Wojna informacyjna jest bez wątpienia pojęciem szerszym od walki informacyjnej. Jak zauważa R. Szpyra, wojna jest kategorią obejmującą wszystkie formy walki, jednak jej istnienie zależy od uznania – w przeciwieństwie do walki istniejącej obiektywnie[26].

Kolejnym terminem ściśle związanym z tematem tej pracy jest pojęcie operacji informacyjnych.

Problematyka operacji informacyjnych była i jest *sensu stricto* dostrzegana w wielu państwach na świecie. Jednak prekursorami w zakresie prób zdefiniowania tego tego termniu są Amerykanie. Początków tego zjawiska należy szukać prawdopodobnie w 1996 roku, kiedy Amerykanie uznali, że dotychczas używane pojęcie walki informacyjnej stało się nieadekwatne, gdyż szereg przedsięwzięć sfery informacyjnej prowadzonych jest w czasie pokoju i nie da się ich uznać za walkę. Walka jest zaś istotą działań bojowych, w której jeden z podmiotów przeciwdziała drugiemu oraz dąży do osiągnięcia przeciwstawnego celu[27].

Dlatego też postanowiono znaleźć inny termin odzwierciedlający całe spektrum przedsięwzięć w sferze informacyjnej. Uznano, że najodpowiedniejszym będzie przyjęcie ogólnej nazwy „operacje informacyjne" (*information operations*)[28]. Termin ten został zdefiniowany w *Połączonej doktrynie operacji informacyjnych*, według której operacje informacyjne to działania skierowane przeciw informacjom i systemom informacyjnym przeciwnika, przy jednoczesnym wykorzystaniu i obronie własnych informacji i systemów informacyjnych. Operacje informacyjne wymagają ścisłej i ciągłej integracji sił, środków, zasobów oraz działań ofensywnych i defensywnych, jak również

26 Zob. R. Szpyra, *Militarne...*, dz. cyt., s. 65.
27 Zob. *Regulamin działań...*, dz. cyt., s. 19.
28 Zob. R. Szpyra, *Militarne...*, dz. cyt., s. 92.

odpowiedniego współdziałania systemu dowodzenia i kierowania z wywiadem i rozpoznaniem[29].

Według NATO operacje informacyjne to funkcja militarna mająca na celu dostarczenie sugestii i porad oraz zapewniająca koordynację wojskowych działań informacyjnych w taki sposób, aby kreować pożądane efekty odnoszące się do woli, zrozumienia oraz fizycznych możliwości przeciwników, potencjalnych przeciwników lub innych ugrupowań pozostających w rejonie odpowiedzialności dowódcy. Należy podkreślić, że komórka operacji informacyjnych ma pełnić funkcję koordynującą, a nie funkcję dowodzenia. Działania informacyjne zaś to przedsięwzięcia ukierunkowane na wpływanie na informację i/lub na systemy informacyjne. Mogą być prowadzone przez jakiegokolwiek gracza i zawierają środki przeciwdziałania[30].

Doktryna działań połączonych zalicza operacje informacyjne do głównych funkcji połączonych[31]. Definiuje je jako skoordynowane i zsynchronizowane działania podejmowane w celu uzyskania pożądanego wpływu na wolę, sposób myślenia i możliwości strony przeciwnej, potencjalnych przeciwników i innych grup określonych przez NAC[32], wspierając ogólne cele NATO przez wpływanie na ich informacje, systemy i procesy oparte na informacjach. Jednocześnie NATO wykorzystuje i chroni własne informacje, systemy i procesy informacyjne.

INFOOPS (*information operations*) obejmują zintegrowane zastosowanie szeregu metod i technik do osiągania określonych efektów we wspieraniu działań. INFOOPS występują na wszystkich poziomach operacji Sojuszu i będą prowadzone w całym obszarze operacyjnym NATO, w oparciu o polityczne wytyczne NAC i zgodne ze strategią informacyjną Sojuszu. INFOOPS mają także na celu ochronę procesu podejmowania decyzji i taktyki NATO przed istniejącymi i potencjalnymi wpływami zewnętrznymi[33].

29 *Joint Doctrine for Information Operations, JP 3-13*, Joint Chiefs of Staff, 9 October 1998, s. I-9.

30 Z. Modrzejewski, *Operacje...*, dz. cyt., s. 11.

31 Zgodnie z doktryną dowódca przy określaniu zdolności niezbędnych do osiągnięcia przez siły połączone powinien rozważyć przede wszystkim funkcje połączone, do których zalicza się, oprócz operacji informacyjnych, następujące funkcje: dowodzenie i kierowanie, wywiad-rozpoznanie, planowanie, manewr i środki ogniowe, wybór celów i środków ich niszczenia, ochronę sił, współpracę cywilno-wojskową, informowanie publiczne i ciągłość działań.

32 *North Atlantic Council* – Rada Północnoatlantycka.

33 *Doktryna Działań Połączonych D/01 (C)*, Szt. Gen. WP, Warszawa 2009, s. 100.

Zdaniem autorów koncepcji komunikacji strategicznej operacje informacyjne to przedsięwzięcia ukierunkowane na analizowanie, planowanie, ocenę oraz integrowanie działań informacyjnych, których celem jest oddziaływanie na informacje i systemy informacyjne po to, aby tworzyć pożądane efekty (rezultaty) w sferze woli działania, zrozumienia sytuacji i zdolności do prowadzenia działań przez zaaprobowane obiekty oddziaływania (audytoria) w ramach osiągania celów prowadzonej operacji[34].

W obowiązującym *Regulaminie działań wojsk lądowych* znajduje się natomiast definicja działań informacyjnych, według której są to przedsięwzięcia, których celem jest wpływanie na postrzeganie (poglądy) i nastawienie określonych jednostek i grup, prowadzące do zachowań korzystnych z własnego punktu widzenia. To przedsięwzięcia mające wpływ na podejmowanie decyzji politycznych i wojskowych przez oddziaływanie na informację, podstawowe procesy informacyjne oraz systemy dowodzenia, kierowania, łączności i informatyki przeciwnika, a także chroniące własne informacje, procesy i systemy informacyjne[35].

Zasadnicza różnica pomiędzy operacjami informacyjnymi a działaniami informacyjnymi polega na tym, że termin „operacje informacyjne" odnosi się do funkcji militarnej jako doradzania dowódcy i koordynowania działalności różnych elementów w celu osiągnięcia założonego przez dowódcę celu informacyjnego, natomiast działania informacyjne są przedsięwzięciami, które wykonywane są przez dowolne siły (pododdział zmechanizowany, taktyczny zespół wsparcia psychologicznego, środki walki elektronicznej) z zamiarem wpływania na informację lub systemy informacyjne.

1.3. Zasady walki informacyjnej

Planowanie i prowadzenie walki informacyjnej powinno zostać oparte na określonych zasadach. Zasady te będą również kształtowały sposób integracji walki informacyjnej z procesem połączonego targetingu i ukierunkowywały sposób, w jaki działania informacyjne będą wspierały działania militarne komponentu lądowego.

Zdaniem L. Ciborowskiego można przyjąć, że szeroko rozumiane zasady: centralizacji, kompleksowości, spójności, wiarygodności, nieszablonowości,

34 *Koncepcja komunikacji strategicznej w Siłach Zbrojnych RP*, CDiS SZ, Bydgoszcz 2013, s. 14.

35 *Regulamin działań...*, dz. cyt., s. 325.

skrytości, terminowości, ciągłości i elastyczności są tymi, które powinny być przestrzegane w każdej formie i przestrzeni walki informacyjnej[36].

Najbardziej aktualne publikacje z zakresu operacji informacyjnych eksponują nieco inne zasady. Zgodnie z zapisami doktrynalnymi do zasad tych należą: podejście do działań oparte na efektach, wytyczne dowódcy i osobiste zaangażowanie, ścisła koordynacja i kolejność, dokładne rozpoznanie, wkład do połączonego targetingu, scentralizowane planowanie i zdecentralizowane wykonanie, wczesne zaangażowanie i terminowe przygotowanie, ciągłość, monitorowanie i ocena[37].

W obowiązującym *Regulaminie działań wojsk lądowych* możemy znaleźć inny zestaw zasad, które częściowo pokrywają się z przytoczonymi powyżej. Zgodnie z zapisami tej publikacji do zasad działań informacyjnych zalicza się: wytyczne dowódcy, koordynację, terminowe i dokładne rozpoznanie, punkt ciężkości, centralne planowanie, targeting, terminowość, elastyczność oraz analizę efektywności oddziaływania[38].

Zasada „wytyczne dowódcy" oznacza, że dowódca dowodzi i nadzoruje także wszystkie działania z zakresu działań informacyjnych włącznie ze strukturą procesu podejmowania decyzji. Dlatego też jego zamiar będzie również definiował cel działań informacyjnych. Cel ten musi określać stan końcowy.

Koordynacja jest warunkiem niezbędnym do osiągnięcia efektu synergii operacji informacyjnych. Działania informacyjne muszą być zintegrowane w całej strukturze dowodzenia. Wszystkie elementy działań informacyjnych muszą być skoordynowane i zsynchronizowane z innymi działaniami tak, by nie wpływały na siebie negatywnie.

Komórki INFOOPS nie posiadają dostatecznych możliwości gromadzenia i analizy informacji i w tym zakresie ściśle współpracują z komórkami rozpoznawczymi podczas planowania i realizacji operacji informacyjnych. Dlatego też bardzo ważną zasadą jest terminowe i dokładne rozpoznanie. Działania informacyjne muszą być wspierane terminowymi i dokładnymi informacjami o wszystkich stronach konfliktu, a także o podmiotach neutralnych, które mogą wpływać na realizację zadania. Rozpoznanie przez dostarczanie danych i wniosków powinno kształtować podłoże operacyjne, wspomagając ocenę dowódcy.

36 Zob. L. Ciborowski, *Walka...*, dz. cyt., s. 94.

37 *Allied Joint Doctrine for Information Operations AJP-3.10*, NSA, November 2009, s. 1-5–1-6.

38 *Regulamin działań...*, dz. cyt., s. 327–328.

Działania informacyjne, podobnie jak każde inne działania, muszą mieć określony punkt ciężkości. Powinny koncentrować się na punkcie ciężkości przeciwnika, który jest określany w drodze analizy jego działań. Jednocześnie dowódca musi identyfikować swój własny punkt ciężkości i zapewnić mu odpowiedni poziom ochrony.

Zasada centralnego planowania oznacza centralne planowanie i zdecentralizowane wykonanie działań informacyjnych na niższych poziomach. Jednakże dla niektórych działań wymagane będzie scentralizowane koordynowanie (np. dezinformowanie), kiedy wszystkie elementy sił własnych muszą trzymać się jednorodnego planu.

Targeting umożliwia najefektywniejsze użycie posiadanych sił i środków do prowadzenia działań informacyjnych. W działaniach informacyjnych sporządza się długą i zróżnicowaną listę potencjalnych celów działań informacyjnych, która dotyczy szerokiego grona uczestników działań zarówno wewnątrz, jak i na zewnątrz rejonu (obszaru) prowadzonych działań.

Zasada terminowości oznacza, że planowanie działań informacyjnych musi rozpocząć się z wyprzedzeniem szczególnie tam, gdzie kształtowanie opinii jest kluczem do sukcesu, ponieważ zarówno planowanie, jak i wykonanie wymagają czasu, a rezultaty mogą pojawić się znacznie później. W związku z tym wytyczne (priorytety) jako część procesu planowania muszą być określone w pierwszej kolejności. Defensywne działania informacyjne wymagają znacznie więcej przygotowań, szczególnie dla systemu łączności i informatyki, ponieważ te przedsięwzięcia muszą być wbudowane w koncepcję prowadzonych działań i tworzyć podłoże ich prowadzenia. Ponadto dowódca, biorąc pod uwagę zasadnicze wymagania informacyjne, może sprecyzować dla komórki rozpoznawczej dodatkowe potrzeby informacyjne.

Równie ważną zasadą w działaniach informacyjnych jest elastyczność. Celem działań informacyjnych jest wpływanie na podejmujących decyzje, ich percepcję oraz procedury i potencjał systemu dowodzenia. Szczególnie percepcja jest podatna na oddziaływanie. Plan działań informacyjnych musi być elastyczny i zawierać wystarczająco skuteczne działania, by reagować na różne wydarzenia, a w szczególności wykorzystywać nagłe zmiany w nastrojach społecznych.

Działania informacyjne, podobnie jak inne działania, podlegają analizie efektywności oddziaływania. Efektywność działań informacyjnych zależy od ciągłej oceny skutków, zarówno krótkoterminowych, jak i długoterminowych, oraz od wzajemnie ze sobą powiązanych działań, ukierunkowanych na osią-

gnięcie określonego celu. Dokonanie analizy efektywności oddziaływania jest możliwe dzięki pozyskiwaniu informacji ze wszystkich dostępnych źródeł.

Niedocenienie przez władze zasad walki informacyjnej prowadzi bezpośrednio do osiągania przez terrorystów zakładanych przez nich celów. Widać to wyraźnie nie tylko w czasie konfliktów zbrojnych, jak np. w Iraku czy Afganistanie, lecz także w społeczeństwach zachodnich. Najjaskrawszym przykładem są konsekwencje zamachu w Madrycie 11 marca 2004 roku, który doprowadził do zmian politycznych w Hiszpanii (partia rządząca straciła władzę) i w rezultacie wycofania z Iraku pododdziałów hiszpańskich[39].

Nieumiejętnie realizowana polityka informacyjna prowadzi do spadku poparcia społecznego dla polityki rządu w zakresie zwalczania terroryzmu, do oskarżania rządzących o łamanie praw człowieka, naruszanie prawa do prywatności czy nawet o zapędy autorytarne. Można zatem uznać, że w przypadku zamachu w Madrycie powstała asymetria konfliktu także na płaszczyźnie walki informacyjnej. O ile bowiem kampania terrorystyczna została zaplanowana i przeprowadzona jako kampania wpływu społecznego, osiągając zakładane cele, o tyle rządy albo nie podjęły odpowiedniej kontrkampanii dążącej do uzyskania przewagi informacyjnej, albo też reagowały w sposób nieudolny[40].

1.4. Narzędzia walki informacyjnej

Do narzędzi walki informacyjnej komponentu lądowego zaliczane są współcześnie metody, narzędzia i techniki powszechnienie wykorzystywane w operacjach informacyjnych. Narzędzia te w literaturze przedmiotu nazywane są również elementami operacji informacyjnych. Zgodnie z zapisami doktrynalnymi do elementów tych należą: niszczenie fizyczne, operacje psychologiczne, bezpieczeństwo operacji, bezpieczeństwo informacji, walka elektroniczna, dezinformacja, rozpoznanie, współpraca cywilno-wojskowa, sprawy publiczne, zaangażowanie kluczowych przywódców, postawa, wizerunek i profil sił oraz operacje w sieciach komputerowych.

Niszczenie to uderzenie wykonane w celu pozbawienia zdolności bojowej kluczowych komponentów (sił i środków) systemu dowodzenia, łączności,

39 Zob. B. Dobek-Ostrowska, M. Kuś (red.), *Hiszpania: media masowe i wybory w obliczu terroryzmu*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2007.

40 Zob. B. Bolechów, *Terroryzm. Aktorzy, statyści, widownie*, PWN, Warszawa 2010, s. 207 i nast.

informatyki i rozpoznania przeciwnika (*Command, Control, Communication, Computers and Intelligence* – w skrócie C4I).

Można wyróżnić dwa główne aspekty zastosowania niszczenia fizycznego. Pierwszy realizowany jest przez atak na system dowodzenia i kierowania przeciwnika. W tym przypadku niszczenie fizyczne odgrywa znaczącą rolę we wpływaniu na zrozumienie sytuacji przez przeciwnika i jego sposób działania (wolę). Drugi realizowany jest przez fizyczne niszczenie infrastruktury militarnej przeciwnika, co znacząco oddziałuje psychologicznie (wpływa bezpośrednio na morale i postawę żołnierzy przeciwnika).

Przygotowanie niszczenia fizycznego podlega koordynacji w czasie procesu wyboru celów i środków ich niszczenia bądź obezwładniania. Priorytety w zakresie zasobów i celów są określane przez dowódcę z odpowiednim wyprzedzeniem, aby możliwe było dokonanie właściwego przydziału środków do operacji. Po wydaniu przez dowódcę wytycznych, stanowiących część procesu planowania, wyznacza się cele oraz określa się zadania i priorytety. Fizyczne niszczenie może być uwarunkowane zasięgiem systemów uzbrojenia. Decydując się na niszczenie fizyczne, należy mieć na uwadze, że nadmierne zniszczenia i niepotrzebne ofiary przyniosą przeciwny efekt i zostaną potępione przez opinię publiczną. Dowódca powinien rozważyć i zbilansować potencjalny negatywny rezultat tych działań (np. efekty wtórne i konieczność odbudowy) wobec spodziewanych korzyści[41].

Do jednych z najważniejszych zdolności, ale i narzędzi, którymi mogą posługiwać się operacje informacyjne, należą bez wątpienia operacje psychologiczne.

Według doktryny działania psychologiczne stanowią zespół planowych przedsięwzięć realizowanych w czasie pokoju, kryzysu i wojny, skierowanych do wrogich, przyjaznych lub neutralnych odbiorców. Zadaniem tych działań jest wpływanie na postawy i zachowania odbiorcy oraz osiągnięcie pożądanych z punktu widzenia prowadzącego celów politycznych i wojskowych[42].

Do zasadniczych celów operacji psychologicznych zalicza się:

– osłabienie woli działania i agresywnych zamiarów przeciwnych lub potencjalnie przeciwnych obiektów oddziaływania,

– wzmocnienie zaangażowania i wsparcia ze strony przyjaznych obiektów oddziaływania,

41 Z. Modrzejewski, *Operacje...*, dz. cyt., s. 69–70.

42 *Operacje psychologiczne DD/3.10.1(A)*, Szt. Gen. WP, Warszawa 2010, s. 10.

– pozyskanie poparcia i współpracy ze strony środowisk niezaangażowanych lub niezdecydowanych.

Operacje psychologiczne stanowią już dziś nieodzowny element wszystkich operacji na arenie działań. Są one realizowane zarówno na obszarze kraju, jak i poza jego granicami, jako integralna część kompleksowego wysiłku operacyjnego, wspomagającego realizację głównego zadania w obrębie prowadzonych działań sił własnych – narodowych lub w składzie sojuszniczych (wielonarodowych), czy też połączonych operacji wojskowych. Dowódcy na wszystkich poziomach dowodzenia realizują przedsięwzięcia operacji psychologicznych w celu wywołania lub utrwalenia pożądanych zachowań określonych odbiorców, do których można zaliczyć żołnierzy i ludność zarówno przeciwnika, jak i państwa sojuszniczego czy neutralnego.

Narodowa doktryna określa siedem zasadniczych zadań w zakresie działań psychologicznych[43]:

– osłabienie morale przeciwnika (obiektu oddziaływania) oraz obniżanie jego zdolności i możliwości bojowych,

– wzmacnianie postaw przyjaznych (utrwalanie postaw neutralnych) grup i środowisk niezaangażowanych bezpośrednio w konflikt,

– pozyskiwanie poparcia oraz współpracy ze strony środowisk niezdecydowanych i neutralnych,

– uczestniczenie w przedsięwzięciach związanych z maskowaniem operacyjnym i bezpieczeństwem operacji,

– zbieranie, gromadzenie, analizowanie, przetwarzanie oraz rozpowszechnianie niezbędnych danych o przeciwniku i obszarze działań w ramach zintegrowanego systemu rozpoznania,

– wspieranie i współudział w przedsięwzięciach realizowanych przez państwowe oraz wojskowe struktury i komórki informacyjne w zakresie przeciwdziałania operacjom psychologicznym przeciwnika w okresie wojny, kryzysu i pokoju,

– rozwijanie i doskonalenie własnej oraz sojuszniczej bazy danych informacyjnych, a także metodologii planowania i prowadzenia działań psychologicznych.

Bezpieczeństwo operacji (*Operations Security* – OPSEC) to proces zapewniający odpowiedni poziom ochrony operacji lub działań wojskowych, realizowany za pomocą środków pasywnych lub aktywnych w celu uniemożliwie-

43 Tamże, s. 11.

nia przeciwnikowi dostępu do szczególnie ważnych informacji, dotyczących rozmieszczenia, możliwości i zamiarów wojsk własnych[44]. Głównym zadaniem OPSEC jest zidentyfikowanie i ochrona informacji, które są niezbędne do uzyskania powodzenia kampanii i są opisane jako istotne elementy własnej informacji (*Essential Elements of Friendly Information* – EEFI). OPSEC ma na celu utajnienie własnych EEFI przed decydentami przeciwnika i przez to wpłynięcie na postrzeganie przez nich sytuacji. EEFI muszą być chronione przez cały cykl ich funkcjonowania i w całym zakresie działań. W celu zapewnienia bezpieczeństwa EEFI należy – przez zastosowanie kombinacji różnych (pasywnych i aktywnych) technik – wpływać na wolę, zrozumienie sytuacji i możliwości przeciwnika.

Zapewnienie bezpieczeństwa operacji należy do obowiązków dowódcy, który korzysta ze wsparcia komórki operacyjnej wspomaganej przez inne komórki sztabu (przede wszystkim przez komórkę rozpoznawczą). Komórka operacyjna odpowiada w sztabie za całościowe monitorowanie i składanie meldunków w zakresie bezpieczeństwa działań. Podczas tego procesu przeprowadza się identyfikację najważniejszych informacji oraz analizę własnych akcji, które towarzyszą działaniom militarnym i innym.

Można wyodrębnić trzy główne cele stosowania przedsięwzięć bezpieczeństwa działań:

– identyfikacja tych akcji, które można obserwować przez systemy wywiadowcze przeciwnika,

– określanie informacji częściowych, które obce systemy rozpoznania mogą zebrać, zinterpretować i złożyć w całość, aby uzyskać najważniejsze informacje we właściwym czasie,

– wybór i zastosowanie środków, które wyeliminują lub zredukują do akceptowalnego poziomu słabości własnych działań wobec przeciwnika.

Terminem bezpośrednio związanym z bezpieczeństwem operacji jest bezpieczeństwo informacyjne.

Każda organizacja przetwarza dane uważane przez siebie za wrażliwe, a więc takie, które powinny podlegać ochronie zgodnie z literą prawa i których ochrony wymaga żywotny interes organizacji. W pewnych przypadkach chroni się wyłącznie dane osobowe, w innych są to dodatkowo informacje

44 *AAP-6, Słownik terminów i definicji NATO*, Agencja Standaryzacyjna NATO, 3 kwietnia 2013, s. 299.

niejawne, handlowe czy technologiczne. Każda organizacja powinna określić, które informacje wymagają największej ochrony.

Zgodnie z zapisami doktrynalnymi bezpieczeństwo informacji ma na celu zapewnienie systemom i sieciom teleinformatycznym oraz informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach takich cech, jak: dostępność, integralność, autentyczność, poufność i niezaprzeczalność[45].

Zgodnie z doktryną operacji informacyjnych *AJP-3.10* bezpieczeństwo informacyjne (*Information Security* – INFOSEC) stanowi część bezpieczeństwa operacji. Celem INFOSEC jest ochrona informacji (zgromadzonych, przetwarzanych i przesyłanych), jak również własnych systemów. INFOSEC to szereg przedsięwzięć, które są stosowane rutynowo, na bazie zasad bezpieczeństwa odnoszących się do ochrony informacji. Operacje informacyjne wyznaczają kierunek stosowania i wykorzystania środków bezpieczeństwa informacyjnego w celu ochrony własnych decydentów przed INFOOPS przeciwnika oraz uniemożliwienia mu dostępu do własnych informacji, a także zwiększenia możliwości stosowania dezinformacji.

Definicję bezpieczeństwa informacyjnego można znaleźć ponadto w normach odnoszących się do tej problematyki. W normie PN-ISO/IEC 27001:2007 określono, że bezpieczeństwo informacji to zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[46].

Należy przy tym uwzględnić szereg uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim to, że[47]:

– informacja stanowi zasób strategiczny państwa,

– informacja i wynikająca z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym,

– szeroko rozumiany sektor informacyjny generuje znaczną część dochodu narodowego,

45 *Doktryna systemów łączności i informatyki Sił Zbrojnych RP D/6*, CDiS SZ, Bydgoszcz 2013, s. 20.

46 *PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, PKN, Warszawa 2007, s. 9.

47 K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Difin, Warszawa 2012, s. 18.

– procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione od systemów przetwarzania i przesyłania informacji,

– zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych,

– rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej,

– technologie informatyczne stały się istotnym elementem funkcjonowania sił zbrojnych,

– media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. na drodze dezinformacji.

Z kolei Piotr Bączek wśród podstawowych zagrożeń dla bezpieczeństwa informacyjnego państwa wymienia[48]:

– nieuprawnione ujawnienia informacji,
– naruszenia przez władze praw obywatelskich,
– asymetrię w międzynarodowej wymianie informacji,
– działalność grup świadomie manipulujących przekazem informacji,
– niekontrolowany rozwój technologii bioinformatycznych,
– przestępczość komputerową,
– cyberterroryzm,
– samą walkę informacyjną,
– zagrożenia asymetryczne,
– szpiegostwo.

Bezpieczeństwo informacji oznacza zatem ochronę własności intelektualnej wypracowanej w danej instytucji. Obecnie można mówić nawet o uzależnieniu wszystkich aspektów działania instytucji od skomputeryzowanych systemów informacyjnych.

Bezpieczeństwo informacji nie jest stanem niezmiennym, nie można go również osiągnąć dzięki jednorazowej akcji, lecz wymaga działania długofalowego. Dlatego też nieustannie należy analizować zagrożenia dla systemu informacyjnego, weryfikować skuteczność wprowadzonych zabezpieczeń i stosować innowacyjne środki bezpieczeństwa.

Kolejnym narzędziem walki informacyjnej jest walka elektroniczna, która zostanie szczegółowo opisana w Rozdziale 3 niniejszego opracowania.

48 P. Bączek, *Zagrożenia*..., dz. cyt., s. 85–86.

Narzędziem walki informacyjnej jest również dezinformacja. Zgodnie z zapisami regulaminowymi dezinformacja to stwarzanie fałszywego obrazu sytuacji taktycznej nacierającemu, przez co skłania się go do błędnego wyboru głównego kierunku natarcia i rozmieszczenia sił oraz środków w niewłaściwym miejscu. Wprowadzenie w błąd co do kierunku i czasu kontrataku powoduje, że przeciwnik rozmieszcza swoje odwody daleko od miejsc pozwalających na skuteczną reakcję[49].

Według niektórych poglądów dezinformacja to przekazywanie fałszywej informacji wprowadzającej w błąd odbiorcę. Zakłada się, że nieprawdziwa informacja będzie przekazywana najczęściej po to, aby uzyskać określone efekty, wynikające z niewiedzy osoby lub instytucji będącej obiektem dezinformacji. Nie można także wykluczyć, że dezinformacja wystąpi w sposób niezamierzony jako błąd w rozumieniu treści informacyjnej lub jej zniekształcenia (np. w czasie transmisji radiowej).

Przykładem takiej niezamierzonej dezinformacji jest rewelacyjny program radiowy przygotowany przez Orsona Wellesa w 1938 roku. Reżyser adaptował wówczas *Wojnę światów* Herberta George'a Wellsa na słuchowisko, nadając mu formę relacji z wydarzeń. Słuchacze zaś odebrali audycję jako rzeczywisty reportaż z inwazji Marsjan na Ziemię, co wywołało panikę wśród mieszkańców New Jersey. Niewłaściwie odebrane informacje radiowe, zniekształcone przez słuchaczy, spowodowały wiele zamieszania w codziennym życiu mieszkańców stanu. Sugestywny dźwięk i wiarygodna narracja wywołały reakcję nieprzewidzianą przez twórców słuchowiska.

Zdaniem V. Volkoffa dezinformacja może być rozumiana w wąskim i szerszym znaczeniu. W wąskim znaczeniu mieści się ona pomiędzy wprowadzaniem w błąd a wywieraniem wpływu. W opinii autora wprowadzanie w błąd jest czynnością jednorazową, związaną z konkretnym zadaniem, wykorzystuje różne środki i zmierza do wmówienia określonych rzeczy wybranym osobom. Dezinformacja natomiast prowadzona jest w sposób systematyczny, fachowy, zawsze za pośrednictwem środków masowego przekazu i jest skierowana do opinii publicznej, a nie do sztabów krajów – obiektów działań[50]. Volkoff twierdzi ponadto, że wprowadzanie w błąd jest techniką, dezinformacja – doktryną[51].

49 *Regulamin działań...*, dz. cyt., s. 31.
50 V. Volkoff, *Dezinformacja - oręż wojny*, Delikon, Warszawa 1991, s. 8.
51 Tamże, s. 11.

Najistotniejszym z punktu widzenia sił zbrojnych i obronności państwa obszarem dezinformacji jest dezinformacja wojskowa (*Military Deception* – MILDEC). Ze względu na zakres, rolę, charakter i treść można jej dokonać na wszystkich poziomach dowodzenia, czyli zarówno w skali strategicznej, operacyjnej, jak i taktycznej.

Na poziomie strategicznym dezinformacja realizowana jest w celu wprowadzenia przeciwnika w błąd co do czasu, miejsca, potencjału i zamiaru działania na najwyższym szczeblu dowodzenia. W operacjach połączonych działania dezinformacyjne mogą być planowane na poziomie narodowym lub w obszarze działań. Na poziomie operacyjnym dezinformacja to przedsięwzięcia i środki wprowadzające w błąd przeciwnika w zakresie sposobu prowadzenia operacji. Może być zawarta w strategicznym planie dezinformacji. Z kolei na poziomie taktycznym obejmuje ona całość przedsięwzięć i środków mających na celu wprowadzenie przeciwnika w błąd na lądzie, morzu oraz w powietrzu.

Do celów szczegółowych dezinformacji można zaliczyć:

- wywołanie zaskoczenia,
- zapewnienie bezpieczeństwa działań,
- umożliwienie swobody działania dowódcom,
- wprowadzenie w błąd przeciwnika,
- zminimalizowanie strat własnych oraz ograniczenie czasu działania i poziomu wykorzystania sił i środków.

Najogólniej rzecz ujmując, obiektami dezinformacji są: przeciwnik, wojska własne oraz otoczenie, które stanowi płaszczyznę kontaktów obu stron.

Można wyodrębnić dwa rodzaje działań dezinformacyjnych: ofensywne i defensywne. Podział ten wynika raczej z celu, dla jakiego konkretne siły i środki zostają wykorzystane, niż z natury zastosowanych środków. Niektóre z nich mogą być używane tak ofensywnie, jak i defensywnie[52].

Działania dezinformacyjne dostarczają przeciwnikowi w określony sposób tylko takich informacji, które spowodują podjęcie przez niego błędnych decyzji lub zakłócą proces podejmowania decyzji. Są to przedsięwzięcia zmierzające do zmylenia przeciwnika przez manipulację, zniekształcanie lub tworzenie (fałszowanie) faktów, co prowadzi do uznania zdarzenia symulowanego za prawdziwe i w rezultacie wywołuje u nieprzyjaciela reakcję niekorzystną dla jego własnych interesów. Prowadzenie działań dezinformacyjnych nie jest

52 *Regulamin działań...*, dz. cyt., s. 334–335.

procederem nowym. Już od czasów powstania i rozwoju pierwszych form zorganizowanych społeczności ich przywódcy lub dowódcy formacji zbrojnych stosowali dezinformację w celu wprowadzenia przeciwników w błąd. Nie używano jednak pojęcia dezinformacji, lecz posługiwano się terminami „fortel" lub „podstęp". Za prekursorów stosowania podstępu powszechnie uważa się Greków, którzy wykorzystali konia trojańskiego, aby zmylić obrońców Troi.

W opinii historyków wojskowości to Sun Tzu, na podstawie doświadczeń z wojen przełomu VI i V wieku p.n.e., jako pierwszy dokonał analizy przedsięwzięć dezinformacyjnych. W swoim sławnym traktacie *Sztuka wojny* pisał, że „wojna jest sztuką wprowadzania wroga w błąd, (...) strategia wojny polega na przebiegłości i stwarzaniu złudzeń. Dlatego, jeśli jesteś do czegoś zdolny, udawaj niezręcznego, jeśli jesteś aktywny, stwarzaj pozory bierności. Jeśli jesteś blisko, stwórz pozory dużej odległości, jeśli uwierzą, że jesteś daleko, znajdź się niespodziewanie blisko. Staraj się wprowadzić wroga w błąd, stwórz dezorganizację w jego armii i dopiero wtedy uderzaj"[53].

Bardzo ważną rolę w operacjach informacyjnych odgrywa kolejne narzędzie, jakim jest rozpoznanie. Skuteczne militarne operacje informacyjne muszą opierać się na efektywnym wsparciu rozpoznawczym i wywiadowczym. Kluczowe znaczenie w tych operacjach mają wiadomości rozpoznawcze rozpowszechniane przez komórki rozpoznawcze. Wynika to z tego, że komórki INFOOPS nie posiadają dostatecznych możliwości gromadzenia oraz analizy informacji i dlatego ściśle współpracują w tym zakresie z komórkami rozpoznawczymi w ramach planowania i realizacji operacji informacyjnych.

Według obowiązującej doktryny[54] rozpoznanie wspiera pięć dziedzin operacji informacyjnych: bezpieczeństwo operacji, operacje psychologiczne, dezinformację, walkę radioelektroniczną i niszczenie fizyczne. Pozwala zidentyfikować słabe strony przeciwnika oraz określić cele i obiekty dla wyżej wymienionych dziedzin operacji informacyjnych.

Wsparcie bezpieczeństwa operacji wyraża się w identyfikacji słabych i silnych stron przeciwnika oraz w ocenie zamiarów i prawdopodobnej taktyki przeciwnika, które można wykorzystać do opracowania planu ochrony wojsk. Ponadto rozpoznanie wykrywa środki rozpoznania przeciwnika, umożliwiając tym samym podjęcie działań zapobiegających wykryciu istotnych elementów ugrupowania wojsk własnych.

53 Sun Tzu, *Sztuka wojny*, wyd. 2, Helion, Gliwice 2008.

54 *Doktryna rozpoznanie Wojskowe D-2(A)*, Warszawa 2015.

Rozpoznanie dostarcza informacji na temat nastawienia społeczności przeciwnika, a także jej etnicznego i kulturowego charakteru, co umożliwia odpowiednie zaplanowanie i prowadzenie operacji psychologicznych. Ponadto rozpoznanie identyfikuje odpowiednie obiekty oddziaływania operacji psychologicznych, a następnie ocenia efekty przeprowadzonych operacji psychologicznych.

Wsparcie działań dezinformacyjnych przez rozpoznanie przejawia się we wskazywaniu obiektów do dezinformowania, a następnie w przeprowadzeniu oceny efektów realizowanego planu dezinformowania.

Rozpoznanie prowadzi kompleksową analizę systemów dowodzenia przeciwnika oraz identyfikuje kluczowe cele dla ofensywnej walki radioelektronicznej. Oprócz tego rozpoznanie określa i ocenia zagrożenie wykrycia własnych systemów przez przeciwnika.

W przypadku wsparcia niszczenia fizycznego rozpoznanie, przez działanie sił i środków oraz stosowanie procedur rozpoznawczego przygotowania pola walki, dostarcza ofensywnym środkom rażenia danych do wyboru celów (targeting), a następnie, wykorzystując procedury prowadzenia oceny strat i zniszczeń bojowych (BDA), informuje o ewentualnej konieczności powtórnego rażenia.

Współpracę cywilno-wojskową (*Civil-Military Cooperation* – CIMIC) oraz informowanie opinii publicznej zaliczono w *Regulaminie działań wojsk lądowych* do komponentów związanych z INFOOPS, ale nie wchodzących w ich skład. Zgodnie z zapisami doktrynalnymi współpraca cywilno-wojskowa to zespół przedsięwzięć obejmujący koordynację i współdziałanie pomiędzy dowódcą wojskowym, a podmiotami cywilnymi, przez które rozumie się ludność cywilną, władze lokalne oraz organizacje międzynarodowe, rządowe i pozarządowe, działające w obszarach ich kompetencji i odpowiedzialności[55].

Dowódca ponosi odpowiedzialność za uwzględnienie czynników socjalnych, politycznych, kulturowych, religijnych, ekonomicznych, środowiskowych i humanitarnych w planowaniu i prowadzeniu operacji. Ponadto powinien on brać pod uwagę obecność w rejonie działania organizacji międzynarodowych, rządowych i pozarządowych, kierujących się swoimi celami, posiadających własne metody działania i odmienne oceny sytuacji.

55 *Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP DD/9*, Szt. Gen. WP, Warszawa 2004, s. 1–2.

CIMIC jest integralną częścią operacji wspierającą realizację zadań sił zbrojnych, zmierzających do osiągnięcia założonego celu tej operacji.

Podstawowym zadaniem personelu struktur CIMIC jest wspieranie dowódcy, przygotowywanie i przedstawianie ocen dotyczących tej współpracy, inicjowanie działań wspierających plan operacji oraz utrzymywanie niezbędnych relacji łącznikowych w rejonie prowadzonych działań. Ponadto przygotowuje on ocenę sytuacji w rejonie z punktu widzenia współpracy cywilno-wojskowej. Dowódcy na podstawie tej opinii stawiają związane z nią wymagania, np. wyrażają konieczność rozwinięcia sił CIMIC w rejonie prowadzonych działań dodatkowych w celu realizacji zadań bezpośredniego wsparcia misji. Wszyscy żołnierze biorący udział w operacji realizują w pewnym stopniu zadania w obrębie współpracy cywilno-wojskowej.

Współpraca cywilno-wojskowa w sposób zinstytucjonalizowany została wykorzystana po raz pierwszy w Bośni i Hercegowinie przez wojska NATO. CIMIC odgrywała na tym obszarze istotną rolę w operacjach prowadzonych przez Siły Implementacyjne NATO (IFOR) oraz Siły Stabilizacyjne NATO (SFOR), będąc integralnym elementem działalności na wszystkich szczeblach dowodzenia, a także podmiotem planowania oraz szkolenia[56]. Współpracę cywilno-wojskową w czasie operacji pokojowej w Bośni i Hercegowinie nawiązano na podstawie podpisanego 14 grudnia 1995 roku w Paryżu *Porozumienia w sprawie wojskowych aspektów ustanowienia pokoju na terenach Bośni i Hercegowiny* (*Dayton Peace Agreement*).

Kolejny narzędziem, które postało w odpowiedzi na wyzwania współczesnego świata są sprawy publiczne (*Public Affairs* – PA).

Bezpowrotnie minęły czasy, w których sztabowcy musieli koncentrować się jedynie na aspekcie militarnym prowadzonych działań. Obecnie bardzo istotna, a może nawet najważniejsza, jest opinia publiczna[57].

U progu XXI wieku szybkość przepływu informacji i rola jej oddziaływania na otoczenie stały się bardzo istotne. Umiejętne wykorzystywanie i znajomość narzędzi komunikacji przyczynia się zatem do lepszego zrozumienia misji wojska oraz zdobycia w społeczeństwie wsparcia dla realizacji założonych celów.

56 A. Miller, *Rola i zadania CIMIC w operacjach na Bałkanach*, „Zeszyty Naukowe AON" 2012, nr 4, s. 372.

57 Zob. R. Czulda, *Media a sukces operacji zbrojnej*, „Przegląd Wojsk Lądowych" 2008, nr 9, s. 52.

Sprawy publiczne stanowią bezpośrednie wsparcie dla celów militarnych, przeciwdziałając dezinformacji ze strony przeciwnika i jednocześnie zniechęcając go od działania. Jednakże wysiłki PA i INFOOPS koncentrują się na innych odbiorcach i różnią się pod względem zakresu oraz celu działania. Dlatego też przez cały czas i na wszystkich szczeblach – w celu zagwarantowania zgodności komunikatów wydawanych przez stronę militarną do zewnętrznych odbiorców oraz promowania efektywności i zaufania do prowadzonych działań – należy zapewnić koordynację pomiędzy PA i INFOOPS.

Celem PA jest ochrona wiarygodności NATO oraz promocja szeroko pojętego zrozumienia dla działań NATO, a tym samym pozyskanie poparcia dla działań militarnych. Militarne PA NATO to funkcja odpowiedzialna za promowanie militarnych celów NATO wśród odbiorców przede wszystkim po to, żeby wzmocnić świadomość i zrozumienie militarnych założeń Sojuszu. Obejmuje planowanie i realizację kontaktów z mediami oraz relacje wewnętrzne i zewnętrzne. Ważnym czynnikiem wszelkich działań militarnych jest przekazywanie głównych tez i komunikatów do mediów, przy jednoczesnym zapewnieniu jasnego i pełnego zrozumienia działań oraz z zachowaniem OPSEC. Chociaż *public affairs* skupiają się głównie na potrzebie właściwego informowania i kształcenia odbiorców, co skutkuje uzyskaniem poparcia społecznego dla NATO, ich wpływ jest dużo większy. Dlatego też istotne jest, aby personel PA i INFOOPS ściśle współpracował z mediami, zapewniając dostarczenie skoordynowanej wiadomości do wybranych odbiorców. Jako że doniesienia medialne mają wpływ na wszystkie zaangażowane strony, szczególną uwagę należy zwrócić na działające w rejonie operacji media miejscowe i regionalne oraz inne media, które mają wpływ na ludność. Podczas gdy PA i INFOOPS mają innych odbiorców i inne kanały przekazywania informacji, to jednak niezbędna jest koordynacja przekazywanych treści oraz czasu ich dostarczania. Efektywne PA umożliwiają dowódcy swobodę działania i wspierają INFOOPS w przeciwdziałaniu propagandzie przeciwnika, przedstawiając prawdę o działaniach operacyjnych przy zachowaniu odpowiedniego ich bezpieczeństwa. Wiarygodność rzeczników PA jako źródeł terminowej i wiarygodnej informacji nie może zostać narażona. W żadnym wypadku nie można podawać mediom fałszywych informacji. Aby uniknąć kreowania fałszywego

wrażenia, że media w jakikolwiek sposób są manipulowane, należy nakreślić wyraźny podział między działalnością PA i INFOOPS[58].

We współczesnych operacjach zwraca się coraz większą uwagę na kolejne narzędzie, jakim jest zaangażowanie kluczowych przywódców. Operacje w Iraku i Afganistanie pokazały, że ciągłe ich zaangażowanie na każdym poziomie wpływa na zachowanie, postawę i percepcję obiektów oddziaływania. Tego typu aktywność powinna być spójna merytorycznie, dostosowana kulturowo, wiarygodna, dopasowana do realiów oraz celowa.

Zaangażowanie kluczowych przywódców (*Key Leader Engagements* – KLE) to termin określający osobiste interakcje między dowództwem jednostki, a kluczowymi przywódcami i liderami społeczności lokalnej. KLE jest metodą budowania stosunków ze społeczeństwem i osobami wpływowymi (przywódcami, dowódcami, decydentami) reprezentującymi obiekty oddziaływania w rejonie operacji. Celem tych kontaktów jest zmiana zachowania (podejmowanych decyzji, polityki) decydentów (obiektów oddziaływania), zgodna z zakładanym stanem końcowym operacji. Decydentami (obiektami oddziaływania) mogą być przywódcy lokalnych społeczności (formalni i nieformalni), przywódcy religijni, przedstawiciele środowiska akademickiego itp. Istotnym elementem zaangażowania o tym charakterze jest zidentyfikowanie wszystkich kluczowych podmiotów funkcjonujących w obszarze zainteresowania i istniejących między nimi relacji. Po zidentyfikowaniu przywódców należy przeanalizować charakterystykę ich osobowości, przyjęty styl przywództwa (dowodzenia), poziom i zakres ambicji, motywy działania, cele (krótko- i długoterminowe), aktualnie prezentowane postawy, zależności (powiązania), profile psychologiczne i biografie. Stanowi to podstawę do zaplanowania adekwatnych działań informacyjnych, czyli opracowania planu zaangażowania kluczowych przywódców.

Operacje w sieciach komputerowych (*Computer Network Operations* – CNO) to ostatni z rozpatrywanych elementów operacji informacyjnych.

Oprócz roli, jaką odgrywają technologie w zwiększaniu możliwości dostępu do mediów, występuje też stale zwiększająca się zależność od technologii informacyjnej (*Information Technology* – IT). Technologia informacyjna stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie, związane ze zbieraniem, przetwarzaniem, przesyłaniem,

58 Z. Modrzejewski, *Operacje* ..., dz. cyt., s. 112.

przechowywaniem, zabezpieczaniem i prezentowaniem informacji. Dostarcza ona użytkownikowi narzędzi, za pomocą których może on pozyskiwać informacje, selekcjonować je, analizować, przetwarzać, gromadzić, zarządzać nimi i przekazywać je innym ludziom.

Systemy informatyczne „przenikają" społeczeństwo. Tworzą również rdzeń większości systemów wojskowych, a w szczególności systemów wsparcia dowodzenia oraz wspierających działania wywiadowcze i rozpoznawcze. Wzrost zaufania do technologii informacyjnej stwarza nowe możliwości, które mogą zostać wykorzystane, ale jednocześnie kreuje pewne słabości, które należy zdefiniować. Technologia dostarcza ponadto nowych narzędzi bezpośredniego dostępu do informacji przez Internet. Informacja taka może być przyjmowana bez koniecznego zrozumienia jej znaczenia i źródła, w niektórych przypadkach wzbudzając szczególne zaufanie, zwłaszcza w społeczeństwach bez wolnej prasy. Internet jest używany w celu rozpowszechniania i rozsyłania różnych informacji i opinii, włączając w to różnego rodzaju pogłoski, z szybkością niepojętą jeszcze kilka lat temu. Internet jest nieograniczonym i nieuregulowanym środkiem przekazu o zasięgu globalnym, który może być wykorzystywany przez przeciwnika zarówno do rozpowszechniania jego komunikatów, jak również jako środek służący do atakowania systemów sił własnych lub otwarte źródło rozpoznania.

Możliwości i skuteczność CNO są proporcjonalne do uzależnienia przeciwnika od technologii informacyjnej.

Działania te obejmują trzy zintegrowane elementy:

- atak w sieciach informatycznych (*Computer Network Attack* – CNA),
- penetrację sieci informatycznych (*Computer Network Exploitation* – CNE),
- obronę sieci informatycznych (*Computer Network Defence* – CND).

Atak w sieciach informatycznych spowodowany jest niedoskonałościami oprogramowania, nośników danych i sprzętu komputerowego, które pozwalają na zaatakowanie ich przez zastosowanie złośliwych kodów, takich jak wirusy, lub przez subtelniejszą manipulację danymi, zmianę charakterystyki pracy urządzeń lub ściąganie zawartych w nich informacji. Możliwości te zwiększają się przez rosnące zastosowanie nielegalnego oprogramowania w systemach militarnych.

Penetracja sieci informatycznych wspiera INFOOPS przez możliwość dotarcia do informacji o komputerach i sieciach informatycznych oraz przez uzyskanie dostępu do przechowywanych w nich informacji, a także dzięki możliwości korzystania z tych informacji, komputerów/sieci informatycznych.

Celem obrony sieci informatycznych jest obrona przed atakami i penetracją sieci informatycznych. CND to działania podejmowane w celu ochrony przed zakłóceniami, dezinformacją, degradacją lub zniszczeniem informacji zawartych w komputerach lub sieciach informatycznych, lub też samych komputerów i sieci. Są one zatem konieczne, aby móc utrzymać własne zdolności decyzyjne. Podczas tych działań używa się monitoringu i techniki ochrony przed penetracją tak, aby wykryć, scharakteryzować i odpowiedzieć na atak, powstrzymując działania przeciwnika i w razie konieczności podejmując działania naprawcze.

Należy w tym miejscu podkreślić, że narzędzia walki informacyjnej są dostępne nie tylko państwowym siłom zbrojnym, lecz także podmiotom pozapaństwowym (np. organizacjom terrorystycznym), zorganizowanym grupom przestępczym czy też pojedynczym obywatelom[59].

Nowym narzędziem w walce informacyjnej stał się Internet. Pod wieloma względami sieć staje się efektywniejszym środkiem przekazu niż prasa tradycyjna, radio czy telewizja. Z jednej strony sieć zapewnia dostęp do najbardziej wykształconej, a więc opiniotwórczej części odbiorców, z drugiej – przekaz internetowy zapewnia możliwość samodzielnej i nieskrępowanej konstrukcji jego treści, która nie podlega przecież tzw. obróbce redakcyjnej ze strony dziennikarzy przygotowujących materiał (np. eliminujących treści ciągle jeszcze uznawane za zbyt drastyczne). Terroryści zyskali zatem nowe, niejako własne medium, uniezależniając się od mediów oficjalnych. Stanowi to niebywałe wzmocnienie ich przekazu, zwłaszcza że media tradycyjne bez wątpienia powtórzą i dodatkowo nagłośnią przekaz internetowy[60].

Akt terrorystyczny jest ponadto aktem medialnym, a immanentną jego cechą jest opinia publiczna. Aby spełnił on swoją rolę, musi być szokujący, ponieważ tylko w ten sposób można przyciągnąć uwagę opinii publicznej i wywołać zakładany efekt zastraszenia[61].

59 M. Marciniak, *Prawdy i mity o chińskich hakerach*, „ComputerWorld" z 19.10.2011, http://www.computerworld.pl [dostęp: 19.04.2012].

60 Na temat wykorzystania Internetu przez terrorystów powstało już wiele publikacji, m.in.: T. Płudowski (red.), *Terrorism, Media, Society*, Wydawnictwo Adam Marszałek, Toruń 2006; M. Legiędź-Gałuszka, *Obraz terroryzmu w mediach masowych: informacja, perswazja, aksjologia* [w:] K. Kowalczyk, W. Wróblewski (red.), *Oblicza współczesnego terroryzmu*, Toruń 2006; K. Liedel, S. Mocek, *Terroryzm w medialnym obrazie świata*, Trio, Warszawa 2010.

61 T. Aleksandrowicz, *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 30.

Media są dla terrorystów przede wszystkim środkiem rozpowszechniania propagandy, którą można podzielić na kilka komponentów pozostających we wzajemnej zależności[62]:

- oddziaływanie na międzynarodową opinię publiczną,
- poszerzanie stref wpływów,
- rekrutacja członków i sympatyków,
- inspirowanie działań członków i sympatyków,
- przyciąganie uwagi władz,
- budowanie własnego, pozytywnego wizerunku,
- deprecjonowanie przeciwnika,
- wywoływanie poczucia permanentnego zagrożenia,
- osłabianie postawy moralnej społeczeństwa,
- indoktrynacja światopoglądowo-religijna,
- legitymizacja istnienia i działania.

W literaturze przedmiotu można spotkać również inny zestaw elementów i narzędzi walki informacyjnej.

Według Ł. Kamieńskiego do elementów walki informacyjnej można zaliczyć: destrukcję fizyczną, operacje bezpieczeństwa, operacje psychologiczne, sabotaż i walkę elektroniczną.

Do narzędzi walki informacyjnej można natomiast włączyć[63]:

- dyplomację,
- propagandę,
- kampanie psychologiczne,
- działania wpływające na procesy polityczne lub kulturowe,
- dezinformację, manipulowanie lokalnymi mediami,
- infiltrację sieci komputerowych i baz danych.

Konkludując, na podstawie literatury przedmiotu można stwierdzić, że pojęcie „walki informacyjnej" jest różnie interpretowane. Bardzo często w literaturze przedmiotu jest ono zamiennie używane z terminami: „wojna informacyjna" i „operacje informacyjne".

Postęp naukowo-techniczny w dziedzinie elektroniki i informatyki spowodował zmianę charakteru walki informacyjnej przez przeniesienie fizycznych przedsięwzięć z nią związanych do sfery cybernetycznej.

62 P. Wojtunik, *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, s. 23, www.bbn.gov.pl/download/1/1967/zeszyt9wojtunik.pdf [dostęp: 22.02.2015].

63 Zob. K. Liedel, P. Piasecka, *Wojna cybernetyczna - wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1/17, s. 22–23.

Walka informacyjna będzie zatem prowadzona w globalnym środowisku informacyjnym ze względu na nasycenie pola walki nowoczesnymi technologiami elektronicznymi. W nowoczesnej walce informacyjnej głównymi środkami rażenia stały się narzędzia informatyczne i urządzenia, za pomocą których można oddziaływać na wojskowe i cywilne systemy komputerowe przeciwnika w celu zakłócenia lub całkowitego uniemożliwienia ich użytkowania.

Walka informacyjna, podobnie jak wszelkie działania zbrojne, prowadzona jest na określonych zasadach. Zasady te kształtują sposób integracji walki informacyjnej z procesem połączonego targetingu i ukierunkowują sposób, w jaki wspiera ona działania militarne komponentu lądowego.

Literatura wyróżnia różne komponenty walki informacyjnej, zwane niekiedy jej narzędziami. Elementy walki informacyjnej mają zastosowanie we wszystkich operacjach prowadzonych przez komponent lądowy w zakresie planowania, dowodzenia i wsparcia jego działań. Zastosowanie tych elementów (narzędzi) może w krótkim czasie doprowadzić do zniszczenia lub obezwładnienia systemu dowodzenia całego komponentu lądowego lub jego poszczególnych struktur organizacyjnych.

Należy w tym miejscu podkreślić, że walkę informacyjną można prowadzić samodzielnie, to znaczy bez stosowania tradycyjnych sposobów działania i środków bojowych, jak również w połączeniu z nimi.

2. Współczesny wymiar walki informacyjnej

Zdaniem wielu specjalistów kluczową rolę, zarówno w sektorze cywilnym, jak i militarnym odgrywa informacja. Obecnie mamy do czynienia ze zjawiskiem, które niekiedy jest nazywane rewolucją informacyjną, polegającym na połączeniu informatyki i telekomunikacji, co skutkuje powstaniem złożonych systemów teleinformatycznych.

Z wojskowego punktu widzenia, biorąc pod uwagę rolę, jaką odgrywa uzyskanie tzw. przewagi informacyjnej nad przeciwnikiem, skutkuje to tym, że niemalże każdy środek bojowy musi odbierać, przetwarzać i przekazywać setki informacji, dotyczących prowadzonej operacji militarnej. Uszkodzenie jednego z komponentów zastosowanej technologii informacyjnej wystarcza, aby poważnie zakłócić działanie całego systemu. Oznacza to, że współczesna technologia wojskowa jest całkowicie zależna od systemów informatycznych, co naraża ją na ataki z innej, nieznanej dotąd strony – ze strony cyberprzestrzeni. To uzależnienie wojska od informacji wiąże się również z zagadnieniem wpływu sektora cywilnego na działalność w obszarze informacji.

W przeszłości to przede wszystkim armia na własne potrzeby rozwijała technologie, które następnie były wykorzystywane przez prywatną część gospodarki (tak np. było z Internetem). Obecnie wojsko korzysta z nowoczesnych wynalazków naukowców cywilnych, którzy pracują dla prywatnych przedsiębiorstw, ponieważ przemysł militarny został wyprzedzony przez przemysł cywilny w zakresie stosowania nowych rozwiązań technicznych. Doprowadziło to jednak do znacznego uzależnienia informatycznego współczesnych armii od prywatnych przedsiębiorstw. Z kolei zacieranie się granicy między sektorem cywilnym i wojskowym spowodowało, że obrona przed atakami na systemy informatyczne stała się trudniejsza, gdyż państwo nie jest w stanie tych systemów efektywnie kontrolować. Rozwój systemów informatycznych spowodował znaczne skrócenie czasu prowadzenia operacji, szybsze namierzanie celów i zwiększenie bezpieczeństwa żołnierzy. O znaczeniu tych elementów we współczesnych wojnach może świadczyć fakt, że obecnie w nawigację satelitarną wyposażane są niemal wszystkie jednostki armii amerykańskiej.

Dążenie do wspomnianej już przewagi informacyjnej wymusza z kolei stosowanie nowoczesnych, zintegrowanych systemów, które w sposób kompleksowy zbierają dane z całego pola walki. Podczas wojny w Afganistanie i w Iraku rolę tę spełniały różnego rodzaju satelity, które dostarczały dokładny obraz celów ataków. Prowadziło to do stworzenia swoistego „systemu systemów", który łączył w sobie zdolność ciągłego zbierania informacji (w czasie rzeczywistym i bez względu na np. warunki pogodowe) z możliwością szybkiego podejmowania decyzji, która dociera do odbiorcy niemal w tej samej chwili, w której została podjęta. Rewolucyjność tych rozwiązań polega na możliwości rozwiania clausewitzowskiej „mgły wojny", która dotąd oznaczała, że na wojnie wszystko jest niepewne i trudne do przewidzenia.

Problemem, jaki wciąż pozostaje w kontekście wymiany informacji, jest brak należytej standaryzacji systemów wykorzystywanych przez różne rodzaje sił zbrojnych, co powoduje, że często układy te nie są zdolne do efektywnej komunikacji między sobą.

Rewolucja informacyjna wpływa także poważnie na taktykę i organizację armii. Współczesne wojny wymagają ścisłej współpracy rożnych rodzajów sił zbrojnych, co wiąże się z koniecznością wytworzenie owego informacyjnego „systemu systemów", który koordynuje przepływ informacji między wojskami lądowymi, lotnictwem, marynarką wojenną itd.

Zacierają się ponadto różnice między poszczególnymi rodzajami sił zbrojnych, gdyż w każdym z nich powstają formacje, które teoretycznie powinny przynależeć do innej części armii, np. lotnictwo marynarki wojennej, piechota morska itp. Jest to spowodowane wymogami współczesnych doktryn wojennych – chociażby tzw. bitwy powietrzno-lądowej, która zakłada skoordynowany atak na cele przeciwnika sił powietrznych i wojsk lądowych.

2.1. Uwarunkowania prowadzenia współczesnej walki informacyjnej

2.1.1. Globalizacja

XXI wiek przyniósł szereg wyzwań oraz znaczne przyspieszenie procesu określanego mianem globalizacji. Oprócz czynników politycznych i ekonomicznych to rewolucja w sferze informacyjnej miała istotny wpływ na przebieg owego procesu.

Zdaniem zespołu autorskiego czynnikami wpływającymi na proces globalizacji są między innymi:

– polityczny nacisk na wzrost poziomu życia, szczególnie przez rosnące aspiracje globalnej klasy średniej liczącej już obecnie ponad 2 mld ludzi,

– intensyfikacja przepływu informacji oraz dalsze upowszechnienie demokracji,

– poprawa jakości polityki makroekonomicznej,

– wzrost liczby transakcji handlowych i inwestycji w skali światowej (sprzeciw wobec dalszej liberalizacji handlu ze strony grup interesów i niektórych rządów nie podważą zasadniczo podstawowej tendencji do wzrostu handlu światowego),

– upowszechnienie technologii informacyjnej w krajach rozwiniętych gospodarczo (chociaż związane z tym korzyści zaczną odczuwać w zróżnicowanej mierze również inne kraje, przy czym wiele z nich nie zdoła spełnić warunków skutecznego spożytkowania technologii informacyjnej: wysokiego poziomu edukacji, odpowiednio rozwiniętej infrastruktury i właściwej polityki regulacyjnej),

– wzrost dynamiki sektora prywatnego, szczególnie w wielu krajach „wschodzących rynków", stymulowanej deregulacją i prywatyzacją w Europie i Japonii, wzrost konkurencji, upowszechnienie „najlepszych praktyk w gospodarce" dzięki rewolucji informacyjnej.

Potężnym czynnikiem sprzyjającym globalizacji jest ujednolicenie wzorców konsumpcji, stylów życia i technologii. Można łatwo zaobserwować, że coraz większe rzesze ludzi prowadzą coraz bardziej zbliżony styl życia, mają podobne aspiracje konsumpcyjne i zawodowe, podobnie się odżywiają, ubierają, spędzają wolny czas, oglądają te same spektakle telewizyjne, czytają te same lub podobne artykuły w prasie, podobne zagadnienia poruszane są w szkołach, na uniwersytetach i kursach doskonalenia zawodowego. Ludzie poszukują tych samych dóbr, usług i wartości.

Globalizacja zgodnie z zapisami encyklopedycznymi są to charakterystyczne i dominujące w końcu XX i na początku XXI wieku tendencje w światowej ekonomii, polityce, demografii, życiu społecznym i kulturze, polegające na rozprzestrzenianiu się analogicznych zjawisk, niezależnie od kontekstu geograficznego i stopnia gospodarczego zaawansowania danego regionu[1].

1 *Encyklopedia PWN*, http://encyklopedia.pwn.pl/haslo/3905881/globalizacja.html [dostęp: 15.01.2015].

W zależności od dyscypliny naukowej reprezentowanej przez badaczy zajmujących się globalizacją można dostrzec interpretacje nadające globalizacji charakter ekonomiczny, socjologiczny, polityczny, kulturowy lub techniczny[2].

G. Kołodko definiuje globalizację jako historyczny proces liberalizacji i postępującej w ślad za nią integracji funkcjonujących dotychczas w pewnym odosobnieniu rynków kapitału, towarów i siły roboczej w jeden współzależny rynek światowy[3].

Termin „globalizacja" ma co najmniej trzy znaczenia:

- odnosi się do procesu umiędzynarodowienia stosunków społecznych,
- oznacza nową fazę modernizacji i rozwoju kapitalizmu z naciskiem na stosunki międzynarodowe,
- określa nowe tendencje w rozwoju kultury.

Można wyodrębnić szereg przyczyn globalizacji, a do najważniejszych z nich należą:

- postęp technologiczny wyrażający się elastycznością oraz innowacyjnością produkcji, zróżnicowaniem odmian produktów, skróceniem cyklu życia produktów, większymi możliwościami poszerzenia kręgu potencjalnych klientów, wzrostem kosztów w sferze badań i rozwoju, koniecznością szybkiego wprowadzania produktów na rynek i wzrostem sprzedaży,
- postęp telekomunikacyjny przejawiający się łatwością dostępu do informacji, poszerzeniem zbioru dostępnych informacji, skróceniem czasu wymiany informacji, skróceniem czasu i obniżeniem kosztów transportu, przyśpieszeniem procesów decyzyjnych, zmniejszeniem znaczenia lokalizacji źródeł transportu oraz mobilnością zasobów i kontrahentów,
- procesy integracji politycznej, czyli redukcja barier międzynarodowej wymiany handlowej, standaryzacja technologiczna, standaryzacja prawna, instytucje ponadnarodowe, zmniejszenie kosztów wymiany handlowej, jednolite standardy techniczne oraz normy prawne, możliwość uczestniczenia w ponadnarodowych projektach.

Globalizacja to bardzo szeroki i złożony proces, mający wpływ na wszystkie sfery naszego życia. Oznacza kształtowanie nowego typu powiązań między przedsiębiorstwami, państwami i społeczeństwami, w którym wydarzenia,

2 A. Muller, *Globalizacja – mit czy rzeczywistość?* [w:] *Globalizacja od A do Z*, E. Czarny (red.), NBP, Warszawa 2004, s. 37.

3 G.W. Kołodko, *Polska z globalizacją w tle. Instytucjonalne i polityczne aspekty rozwoju gospodarczego*, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 2007, s. 28.

decyzje i działania występujące w jednej części świata mają znaczące konsekwencje dla pojedynczych ludzi i całych społeczeństw w odległych częściach globu. Obszarami globalizacji są finanse, rynki, konkurencyjne strategie, technologia, badania i rozwój wiedzy, modele konsumpcji i style życia, regulacje prawne, a także obraz ujednoliconego świata. Globalizacja zapewnia korzyści wynikające przede wszystkim z rozszerzania skali produkcji i przedłużania cykli życia produktów.

Z efektami globalizacji mamy do czynienia w życiu codziennym na każdym kroku. Jej przejawem jest chociażby dostęp do produktów z całego świata, np. samochodów czy telefonów komórkowych. W czasie podróży zagranicznych mamy dostęp do tych samych produktów co w kraju, np. możemy obejrzeć najnowszą premierę filmu w kinie, iść do restauracji *Hard Rock Cafe*[4] lub napić się *Coca Coli*[5].

Globalizacja umożliwia nam integrację oraz ułatwia komunikację z innymi ludźmi, przyczynia się także do zmniejszania wrogości wśród narodów, co zapewne redukuje ryzyko doprowadzenia do wojen czy konfliktów. Globalizacja jest procesem międzynarodowym, który nie przebiega linearnie. Jednak pozytywne nastawienie lat dziewięćdziesiątych XX wieku, zostało zastąpione bardziej wyważonymi, czy wręcz krytycznymi sądami odnośnie do tego zjawiska we współczesnych stosunkach międzynarodowych.

Wśród negatywnych cech globalizacji jej przeciwnicy wymieniają[6]:

– zagrożenie suwerenności państw ze strony instytucji finansowych oraz korporacji międzynarodowych,
– niebezpieczeństwo degradacji środowiska naturalnego,
– możliwość zaniku ekonomicznej niezależności społeczeństw,
– pogłębienie przepaści między bogatymi a biednymi.

Globalizacji podlega oczywiście także bezpieczeństwo. Mówiąc o współczesnym bezpieczeństwie światowym, mamy na myśli zjawiska i procesy bezpieczeństwa dotykające całą ludzkość, obejmujące w różny sposób całą kulę ziemską, angażujące decydujących graczy na arenie światowej i większość innych podmiotów międzynarodowych.

4 Obecnie działa 175 restauracji *Hard Rock Cafe* w 52 krajach świata, m.in. w Kuwejcie, Szwecji i w Polsce.

5 *The Coca-Cola Company* jest największą firmą produkującą napoje na świecie. Działa na ponad 200 rynkach i ma w swojej ofercie ponad 3000 produktów.

6 *Polski problem globalizacji Europy*, http://www.bryk.pl [dostęp: 9.02.2015].

Z punktu widzenia bezpieczeństwa międzynarodowego globalizacja prowadzi do rozprzestrzeniania zjawisk zarówno korzystnych, jak i niekorzystnych. Tworzy warunki sprzyjające przeciwstawianiu się jednym zagrożeniom, ale równocześnie poszerza zasięg lokalnych zagrożeń oraz rodzi zupełnie nowe. Globalizacja zmienia środowisko bezpieczeństwa, nie eliminując z niego sporów, konfliktów czy kryzysów. Nadaje im jedynie nową jakość, inny charakter[7].

Jak zauważa R. Kuźniar, globalizacja w znacznym stopniu modyfikuje podstawowe parametry porządku międzynarodowego. Prowadzi do osłabienia nie tylko ochronnej funkcji granic państwowych, ale także władzy państwa nad własnym terytorium i ludnością, która je zamieszkuje. Kuźniar wskazuje równocześnie na fakt, że globalizacja sprzyja proliferacji i wzrostowi znaczenia pozarządowych uczestników stosunków międzynarodowych. Jest to spostrzeżenie szczególnie istotne w kontekście omawianego zagrożenia dla bezpieczeństwa narodowego i międzynarodowego, jakim jest terroryzm. Jak podkreśla R. Kuźniar, w odniesieniu do sytuacji bezpieczeństwa globalizacja ułatwia jednocześnie przestępczą lub wręcz zbrodniczą działalność międzynarodowym związkom kryminalnym, trudniącym się przemytem ludzi, broni, narkotyków, czy siatkom terrorystycznym w rodzaju najgroźniejszej ze znanych w historii najnowszej – Al-Kaidy. To właśnie tacy aktorzy pozapaństwowi uważani są za największe zagrożenie dla bezpieczeństwa narodowego i międzynarodowego[8].

Globalizacja i rozluźnienie rygorów po zimnej wojnie stworzyły warunki sprzyjające uaktywnieniu się terroryzmu międzynarodowego. Usamodzielnione i pozbawione ograniczeń wynikających z bipolarnego podziału świata organizacje i grupy terrorystyczne zintensyfikowały swoją aktywność. Zaczęły stawać się samodzielnymi strategicznymi graczami na arenie międzynarodowej. Środkami, które sprzyjają działalności grup terrorystycznych i ułatwiają je, są: rewolucja informatyczna, liberalizacja przepływów kapitałowych oraz możliwość dostępu do środków masowego rażenia związana z otwartością społeczeństw demokratycznych. Globalna sieć terrorystyczna może dyktować państwom narodowym swoje warunki, dezorganizować prace organizacji

7 *Wpływ globalizacji i regionalizacji na bezpieczeństwo międzynarodowe*, http://stosunki-miedzynarodowe.pl [dostęp: 15.01.2015].

8 R. Kuźniar, *Niebezpieczeństwa nowego paradygmatu bezpieczeństwa* [w:] R. Kuźniar, Z. Lachowski (red.), *Bezpieczeństwo międzynarodowe czasu przemian: zagrożenia – koncepcje – instytucje*, Warszawa 2003, s. 210.

międzynarodowych, wprowadzać chaos w życiu społecznym oraz stwarzać zagrożenia ekologiczne.

Podsumowując, globalizacja jest bardzo szerokim i złożonym procesem, mającym wpływ na wszystkie sfery naszego życia, w którym wydarzenia, decyzje i działania występujące w jednej części świata mają znaczące konsekwencje dla pojedynczych ludzi oraz całych społeczeństw nawet w odległych częściach globu.

2.1.2. Asymetria współczesnego świata

Równolegle z procesem globalizacji zachodzi zjawisko określane mianem asymetrii współczesnego świata, które również może być źródłem nowych rodzajów zagrożeń bezpieczeństwa międzynarodowego.

B. Balcerowicz uważa, że postępujący proces globalizacji oprócz widocznych pożytków rozwoju cywilizacyjnego, czy wzrostu dobrobytu, przynosi również skutki negatywne dla społeczności międzynarodowej, które manifestują się m.in. w postaci asymetrii gospodarczej, technologicznej, społecznej i kulturowej. Asymetria w tym ujęciu mieści się nie tylko w obszarze możliwych misji i zdolności wojskowych, lecz także tkwi w obszarze całych organizacji oraz w ich otoczeniu, odnosi się do państw, sojuszy, makrosystemów, do asymetrii aktualnego ładu światowego[9].

Zdaniem S. Kozieja asymetryzacja jest jedną z najbardziej charakterystycznych cech współczesnego środowiska bezpieczeństwa. Na scenie międzynarodowej pojawiają się i rozwijają podmioty radykalnie różniące się od klasycznych podmiotów stosunków międzynarodowych, jakimi są państwa i tworzone przez nie organizacje. Różnice te wyrażają się zarówno w samej istocie (państwa i nie-państwa), jak i w ich potencjałach, organizacji, celach, motywach oraz sposobach działania. Konfrontacyjne asymetryczne relacje między klasycznymi i nowymi (postklasycznymi) podmiotami są dzisiaj w wymiarze globalnym źródłem większych zagrożeń niż relacje między symetrycznymi mocarstwami lub blokami państw, które determinowały bezpieczeństwo światowe przez ostatnie wieki, a zwłaszcza w XX wieku[10].

W ostatnich latach, w polskiej i zagranicznej literaturze wojskowej można zauważyć wzmożone zainteresowanie pojęciem asymetrii współczesne-

9 B. Balcerowicz, *Pokój i „nie-pokój" na progu XXI wieku*, Bellona, Warszawa 2002, s. 162.

10 S. Koziej, *Triada globalnych zagrożeń asymetrycznych: konsekwencja proliferacji terroryzmu, broni nuklearnej i technologii rakietowych*, www.bbn.gov.pl [dostęp: 9.02.2015].

go świata i dyskusję wokół niego. Wpływa to niewątpliwie na rozwój nauk o obronności i bezpieczeństwie oraz stanowi podstawę do rozwiązania wielu zidentyfikowanych problemów.

Etymologicznie słowo „asymetria" wywodzi się z języka greckiego i oznacza naruszenie lub brak symetrii, różnicę między rzeczami, zjawiskami itp. Synonimami tego pojęcia jest m.in. niesymetryczność, nieregularność, nierównowaga, odmienność, nieproporcjonalność itp.

Zgodnie ze zapisem *Słownika języka polskiego* asymetria oznacza „brak równowagi w danym układzie przestrzennym lub relacjach, dominację wartości, zachowań, środków, danych itp. pewnego typu; asymetryczność"[11].

Zdaniem T. Szubrychta pojęcie to w odniesieniu do działań militarnych jest pojmowane odmiennie w zależności od kontekstu lub płaszczyzny odniesienia[12].

Asymetria rozumiana jest jako odmienność i nieprzystawalność, która może dotyczyć rozmaitych zjawisk, zazwyczaj jednak pojęcie to stosuje się do opisu i charakterystyki aktualnych, przyszłych bądź potencjalnych konfliktów zbrojnych – ich kształtu, sposobów prowadzenia działań przez zaangażowane strony, wykorzystywanych środków, celów i stopnia zaangażowania w dany konflikt, wreszcie wartości i norm, którymi kierują się strony. Można stwierdzić, że obecnie przez asymetrię rozumie się m.in.: odmienną taktykę walki (m.in. nieuczciwą walkę), oddziaływanie na wrażliwe (słabe) punkty, walkę informacyjną, zmagania informacyjne w sferze opinii publicznej oraz groźbę lub wykorzystanie broni masowego rażenia[13].

J.S. Nye opisuje asymetrię w perspektywie konfliktów międzynarodowych jako sytuację, w której państwa lub podmioty znajdujące się w opozycji do siebie dysponują niezrównoważonymi potencjałami. Powszechnie za konflikt asymetryczny uważa się wojnę prowadzoną przez USA przeciw Al-Kaidzie[14].

11 http://sjp.pl/asymetria [dostęp: 8.09.2014].

12 T. Szubrycht, *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, „Zeszyty Naukowe AMW" 2006, nr 1, s. 141.

13 Zob. P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, AON, Warszawa 2003, s. 11.

14 J.S. Nye, *Konflikty międzynarodowe. Wprowadzenie do teorii i historii*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009, s. 391.

Asymetria w dziejach wojskowości znana jest od czasów biblijnego pojedynku Dawida z Goliatem, jednak gruntowne badania nad zjawiskiem asymetrii rozpoczęły się w USA po zakończeniu wojny w Wietnamie[15].

Specjaliści zajmujący się kwestiami porażki wojsk amerykańskich w wojnie wietnamskiej doszli do wniosku, że w trakcie jej trwania uwzględniano w stopniu niedostatecznym wpływ niematerialnej przewagi pomiędzy przeciwnikami. Zwrócono wówczas uwagę na zróżnicowany poziom zaangażowania stron w konflikt i wynikającej z tego determinacji w jego prowadzeniu. Duża część badaczy doszła do wniosku, że znaczny wpływ na jego wynik miał też zakres i charakter realizowanych interesów, którym ten konflikt miał służyć. Powyższe badania doprowadziły do tego, że w amerykańskiej strategii pojawiło się pojęcie konfliktu asymetrycznego. Termin ten wówczas pojmowano inaczej niż współcześnie, odnosił się bowiem do wszelkiego rodzaju konfliktów zbrojnych, w których przynajmniej na początku jedna ze stron dysponowała znaczną przewagą materialną.

Podsumowując, pojęcie asymetrii (asymetryczności) na gruncie wojskowym odnosi się do sytuacji, w której mamy do czynienia z nieprzystawalnością, odmiennością czy też nieproporcjonalnością obiektów będących przedmiotem porównania[16]. O asymetrii można mówić również w warunkach, w których nie występują tradycyjnie pojmowane linie frontów, klasyczne bitwy, czy żołnierze przestrzegający zasad prowadzenia walki i spełniający prawne warunki kombatanta.

Na bazie terminu „asymetria" powstało wiele innych pojęć takich, jak: przeciwnik asymetryczny, zagrożenia asymetryczne, konflikt asymetryczny, wojna asymetryczna, działania asymetryczne, asymetryczne metody walki itp.

W przypadku operacji informacyjnych ważne jest określenie przeciwnika, który w literaturze przedmiotu nazywany jest przeciwnikiem asymetrycznym. Zdaniem ekspertów wojskowych to globalizacja wygenerowała nowy typ przeciwnika, określanego mianem przeciwnika asymetrycznego[17].

Przeciwnik asymetryczny nie posiada własnego państwa, a więc nie może być podmiotem prawa międzynarodowego, a tym samym, w znaczeniu prawnym, stroną konfliktu.

15 J. Lasota, *Asymetria w walce zbrojnej*, AON, Warszawa 2014, s. 7.

16 Por. M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Polski Instytut Spraw Międzynarodowych, Warszawa 2007, s. 33.

17 K. Rokiciński, B. Pac, *Operacje...*, dz. cyt., s. 38.

W sferze militarnej przeciwnika asymetrycznego można zdefiniować następująco:

- nie jest stroną w świetle prawa międzynarodowego,
- uczestnicy walki nie mają statusu kombatanta,
- obszar prowadzenia działań nie jest określony,
- prowadzi działania za pomocą wszystkich dostępnych środków[18].

Przeciwnik asymetryczny dąży zazwyczaj do takiego rozegrania konfliktu, aby druga strona nie zdecydowała się na wykorzystanie swojej przewagi nawet wtedy, gdy jest to wykonalne taktycznie oraz technicznie.

Ze względu na cel oraz sferę działania można wyróżnić dwie kategorie przeciwnika asymetrycznego: militarną i pozamilitarną.

Celem militarnego przeciwnika asymetrycznego jest dążenie do osiągnięcia celu z zastosowaniem walki zbrojnej. Natomiast celem niemilitarnego przeciwnika asymetrycznego jest dążenie do osiągnięcia celu przy pomocy środków innych niż militarne.

Kategorię pozamilitarną można następnie podzielić na aspekty – polityczny, ideologiczny, ekonomiczny i socjalny[19] – które są wykorzystywane w następujący sposób:

- aspekt polityczny – do osiągnięcia celu politycznego;
- aspekt ideologiczny – do narzucenia określonych idei lub wiary (bardzo często sposób siłowy);
- aspekt ekonomiczny – do uzyskania maksymalnych zysków z prowadzonych przedsięwzięć (zarówno sposobami legalnymi, jaki nielegalnymi);
- aspekt socjalny – do poprawy swojego statusu przez zmianę rejonu zamieszkania (pobytu).

Kolejny terminem istotny dla dalszych rozważań to „zagrożenia asymetryczne".

Zagrożenia asymetryczne dotyczą zarówno sfery militarnej, jak i niemilitarnej. Obejmują myślenie, organizowanie i działanie odmienne od przeciwnika, w tym wykorzystywanie wszelkiego rodzaju różnic szeroko pojmowanych potencjałów stron.

Ich celem jest maksymalizacja własnej przewagi przy jednoczesnym wykorzystaniu słabości przeciwnika dla uzyskania dominacji lub większej swobody

18 Tamże, s. 39.
19 Tamże, s. 40.

operacyjnej[20]. Posiadane przez państwa zachodnie uzbrojenie oraz umiejętności żołnierzy nie przystają do nowych asymetrycznych wyzwań bezpieczeństwa międzynarodowego i wewnętrznego. Trudno jest bowiem walczyć z przeciwnikiem „wtopionym" w społeczeństwo danego państwa, niestanowiącym żadnego widocznego zagrożenia aż do czasu samego ataku; atakującego cele niewojskowe przy użyciu niekonwencjonalnych metod. Koszty walki z takim przeciwnikiem (materialne, społeczne, propagandowe) są niewspółmiernie wysokie w stosunku do efektów.

Współczesne zagrożenia asymetryczne związane są z istnieniem terroryzmu międzynarodowego, niekontrolowanym rozprzestrzenianiem broni masowego rażenia i zorganizowaną przestępczością międzynarodową. Wielu badaczy przedmiotu rozszerza tę listę o dodatkowe elementy w postaci chociażby zagrożenia ze strony państw upadłych czy konfliktów regionalnych i wewnętrznych, walkę informacyjną, czy wykorzystanie broni psychotronicznej i geofizycznej.

Zagrożenia asymetryczne stwarza zazwyczaj strona, która dążąc do konfrontacji, nie jest zdolna przeciwstawić się przeciwnikowi w sposób symetryczny, z użyciem takich samych lub podobnych środków walki.

Miejsce państw we współczesnych wojnach zajmują podmioty i struktury niepaństwowe. Potencjałowi militarnemu państwa przeciwstawiony zostaje niewspółmiernie mniejszy potencjał owych podmiotów. Ten najbardziej widoczny element, charakteryzujący współczesne wojny, a także inne przesłanki zarówno natury prawnej, jak i strukturalnej oraz funkcjonalnej, wskazują na potrzebę zredefiniowania wojen klasycznych i wskazania istoty nowych konfliktów zbrojnych XXI wieku – konfliktów asymetrycznych.

Termin „konflikt asymetryczny" pojawił się zdaniem K. Piątkowskiego w literaturze fachowej w USA w latach 90. ubiegłego wieku.

Określono nim taki konflikt zbrojny, w którym: „państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja, środki walki i metody działania nie mieszczą się w konwencjonalnym pojęciu wojny. (...) Wojna asymetryczna nie zna pojęcia pola walki, frontu, odbywa się w rozproszeniu bez zachowania ciągłości geograficznej i chronologicznej"[21].

Współcześnie koncepcja konfliktów asymetrycznych, która została sformułowana na podstawie doświadczeń wojny wietnamskiej oraz innych ma-

20 T. Szubrycht, *Analiza podobieństw...*, dz. cyt., s. 144.

21 K. Piątkowski, *Wojna nowego typu?*, „Polska w Europie" marzec 2002, nr 1, s. 23–24.

łych wojen, pokazała, że pojęcie asymetrii wiąże się nie tylko z samą różnicą możliwości bojowych (materialnych i niematerialnych) przeciwników biorących udział w konflikcie, ale także z będącą przeważnie jej wynikiem odmiennością wykorzystania metod i technik walki. Można obecnie stwierdzić, że nie tylko sam fakt istnienia nierównowagi potencjałów i możliwości bojowych ma decydujące znaczenie i wystarcza by uznać konflikt za asymetryczny, lecz to, że działania prowadzone są w nieprzystający do siebie sposób[22].

W konflikcie asymetrycznym przeciwnik relatywnie słabszy, niezdolny do uzyskania militarnego zwycięstwa, będzie próbował wywalczyć przewagę na płaszczyznach pozamilitarnych. Skutkuje to użyciem strategii, metod i technik walki nakierowanych na jak największe oddziaływanie psychologiczne, aby zastraszyć, a w konsekwencji zniechęcić społeczeństwo oponenta do prowadzenia konfliktu.

Kolejnym terminem ściśle związanym z rozpatrywaną problematyką są działania asymetryczne.

Zgodnie z definicją zawartą w *Regulaminie działań wojsk lądowych*, działania asymetryczne to działania, w których strona przeciwna nie jest zdefiniowana lub jej zdefiniowanie nie jest wystarczające do zastosowania regularnych form walki. Występują one, gdy strona przeciwna znacząco różni się poziomem technologicznym, kulturowym (systemem wartości), a angażowane siły i środki są niewspółmierne do rozmachu prowadzonych działań[23].

Ponadto w *Regulaminie...* w podziale działań taktycznych, stosując kryterium znaczenia i charakteru, wyodrębniono nową kategorię – działania asymetryczne. Do tego rodzaju działań zaliczono działania specjalne, antyterrorystyczne, przeciwdywersyjne i nieregularne[24].

Działania asymetryczne są rozumiane również jako wykorzystywanie pewnego rodzaju odmienności do uzyskania przewagi nad przeciwnikiem lub też bardziej precyzyjnie: działanie, organizowanie się i myślenie odmienne od przeciwnika w celu maksymalizacji swoich własnych atutów i wykorzystania słabości przeciwnika dla przejęcia inicjatywy[25].

Zdaniem P. Gawliczka i J. Pawłowskiego typowe działania asymetryczne mogą być podejmowane w okresach zwiększonego napięcia, organizowania

22 J. Lasota, *Asymetria...*, dz. cyt., s. 18.

23 *Regulamin działań...*, dz. cyt., s. 409.

24 Tamże, s. 13.

25 S. Metz, D. V. Johnson II, *Asymmetry and U.S. Asymmetry and U.S. Military strategy*, http://www.strategicstudiesinstitute.army.mil [dostęp: 12.08.2010].

ataków terrorystycznych, w wojnach partyzanckich i w otwartych konfliktach i polegają na:

– wprowadzaniu w wybranym czasie zamieszania lub obezwładnianiu kluczowych elementów infrastruktury cywilnej lub wojskowej przeciwnika,

– uniemożliwianiu (opóźnianiu) przeciwnikowi rozwinięcia jego wojsk w okresie otwartego konfliktu,

– zrywaniu interoperacyjności w celu utrudnienia prowadzenia działań koalicyjnych,

– osłabianiu skuteczności wojskowej przeciwnika, zwłaszcza przez ograniczanie możliwości użycia techniki przed prowadzeniem działań bojowych i w ich trakcie,

– zwiększaniu kosztów operacji w wymiarze politycznym oraz zaangażowaniu zasobów ludzkich i materiałowych,

– ograniczaniu tempa prowadzenia operacji,

– uniemożliwianiu przeciwnikowi osiągnięcia przewagi informacyjnej i prawidłowej oceny sytuacji bojowej,

– osłabianiu poparcia politycznego udzielanego przeciwnikowi przez jego sojuszników[26].

Najlepszym przykładem takich działań asymetrycznych były zamachy w Stanach Zjednoczonych 11 września 2001 roku na Światowe Centrum Handlu (*World Trade Center*).

Działania asymetryczne są najskuteczniejsze, gdy uzyskany efekt ma wymiar strategiczny, niezależnie od poziomu konfrontacji i skali podejmowanych przedsięwzięć. Z samej zasady asymetryczności wynika, że działania te są optymalne w sytuacjach, w których przedsięwzięcia o charakterze taktycznym czy operacyjnym dają efekt strategiczny[27].

Działania asymetryczne są więc nową kategorią walki, gdyż obejmują nie tylko komponent militarny, ale także w znaczącej części dotyczą ludności cywilnej (np. w zakresie nielegalnej imigracji, zorganizowanej przestępczości) nie w odniesieniu do określonego obszaru, ale w skali globalnej. Tym samym działania asymetryczne można zdefiniować jako zespół przedsięwzięć natury politycznej, militarnej, ideologicznej i ekonomicznej, których cel osiągany

26 P. Gawliczek, J. Pawłowski, *Zagrożenia…*, dz. cyt., s. 41.

27 K. Pająk, *Możliwości użycia okrętów podwodnych w konfliktach hybrydowych i asymetrycznych* [w:] W. Sokała, B. Zapała (red. nauk.), *Asymetryczność i hybrydowość – stare armie wobec nowych konfliktów*, Biuro Bezpieczeństwa Narodowego, s. 53, www.bbn.gov.pl [dostęp: 16.01.2015].

jest przez przeciwnika asymetrycznego w skali globalnej, z reguły metodami i środkami niekonwencjonalnymi z punktu widzenia prawa oraz społeczności międzynarodowej[28].

Doświadczenia z misji w Iraku oraz w Afganistanie wskazują, że klasyczne operacje militarne przeprowadzone nawet za pomocą najnowocześniejszego sprzętu nie są w stanie zagwarantować pokonania przeciwnika stosującego nietypowe, asymetryczne metody i środki walki.

Podsumowując, współczesne zagrożenia i konflikty różnią się znacznie od tych, jakie występowały nawet w nieodległej przeszłości. Rozpad bipolarnego, zimnowojennego świata i postępująca globalizacja zmieniły charakter środowiska bezpieczeństwa. Dzisiejsze armie muszą mierzyć się z nowymi wyzwaniami i zagrożeniami, w tym ryzykiem o charakterze asymetrycznym.

2.1.3. Sieciocentryczność

Walka informacyjna w sferze militarnej zyskuje coraz większe znaczenie wobec realizacji w praktyce (w czasie wojny irackiej w 2003 roku) koncepcji wojny (walki) sieciocentrycznej (*Network Centric Warfare* – NCW).

Sieciocentryzm definiowany jest jako doktryna militarna (teoria wojny) powstała w erze informacyjnej, poszukująca sposobów zamiany przewagi informacyjnej na przewagę w walce przez tworzenie sieci dobrze poinformowanych, rozproszonych geograficzne zgrupowań różnych rodzajów sił zbrojnych, pozwalających na nowe formy zachowań organizacyjnych[29].

Sieciocentryczność traktowana jest jako podejście do tworzenia zdolności do prowadzenia działań przez wszelkie zaangażowane siły, w których sieć (lub sieci) odgrywa rolę zasadniczą. Stanowi również uogólnione sformułowanie szerokiego spektrum problematyki sieciocentrycznej.

Dążenie do zwiększenia potencjału wyrażanego siłą bojową wojsk w sposób pozwalający dominować nad przeciwnikiem w informacyjnym XXI wieku materializowane jest w koncepcji działań sieciocentrycznych, którą w zgodnej opinii wielu teoretyków i praktyków wojskowych trudno jest jednoznacznie zdefiniować[30].

28 K. Rokiciński, B. Pac, *Operacje* ..., dz. cyt., s. 45.

29 K. Rudziński, *Zagrożenia sieciocentryczne*, prezentacja w AON, Warszawa 2006.

30 Szer. J. Kręcikij, *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" 2006, nr 4, s. 128.

Podstawowe założenia przyszłych koncepcji sieciocentrycznych zwarte zostały w artykule opublikowanym w 1998 roku przez wiceadmirała A. K. Cebrowskiego oraz J. Garstkę pt. *Network Centric Warfare: Its Origins and Future*[31].

Według jednego z twórców tej koncepcji – J. Garstki – jej podstawą jest założenie zwiększenia efektywności działań przez połączenie w globalną strukturę sieciową wszystkich jej składników, tj. ośrodków decyzyjnych, sensorów i efektorów. Ma to spowodować, że pomimo dużego ich rozśrodkowania, uzyska się zsynchronizowaną czasowo i przestrzennie „świadomość sytuacyjną" wszystkich uczestników sieci. Oznacza to, że teoretycznie tę samą informację powinien posiadać każdy element w systemie[32].

Taka zdolność do współużytkowania, współdzielenia informacji tworzących wspólną sytuację operacyjną dzięki efektywnym systemom dowodzenia i kontroli (C2) daje możliwość działania z niezwykłą efektywnością oraz pozwala wykorzystać efekt synergii, w wyniku transformacji tradycyjnych systemów walki i dowodzenia zgodnie z założeniami i zasadami koncepcji walki sieciocentrycznej.

W ocenie M. Huzarskiego w literaturze przedmiotu spotkać można wiele prób definiowania działań sieciocentrycznych, które traktuje on raczej jako opisy i wyjaśnienia zawierające elementy określające istotę tych działań[33], niż faktyczną interpretację interesującego nas terminu. Potwierdzeniem tego są inne licznie funkcjonujące w literaturze przedmiotu terminy i pojęcia bliskoznaczne, wykorzystywane do wyjaśnienia istoty zjawisk, zależności i sprzężeń związanych z działaniami sieciocentrycznymi.

Złożoność działań o charakterze sieciocentrycznym przyczynia się do zróżnicowanego podejścia i identyfikacji elementów współtworzących środowisko sieciocentryczne.

Według M. Huzarskiego na obecnym poziomie rozwoju teorii sieciocentrycznych można wyróżnić cztery takie wzajemnie przenikające się poziomy[34]:

– poziom zamiaru – czyli cele, które należy osiągnąć, decyzje, jakie trzeba podjąć,

31 A. Cebrowski, J. Garstka, *Network Centric Warfare – Its Origins and Future*, US Naval Institute Proceedings, Annapolis, January 1998.

32 K. Rokiciński, B. Pac, *Operacje* ..., dz. cyt., s. 52.

33 M. Huzarski, *Istota wojny (walki) sieciocentrycznej*, „Zeszyty Naukowe AON" 2007, nr 3, s. 22.

34 Tamże, s. 23.

– poziom działań człowieka – to sposób dowodzenia zależny od poziomu wiedzy, zasad i organizacji dowodzenia, umiejętności, doświadczenia,

– poziom systemu – czyli zaawansowane wspomaganie procesów informacyjno-decyzyjnych, narzędzia teleinformatyczne do współtworzenia środowiska sieciocentrycznego,

– poziom materialny – to sensory, platformy uzbrojenia, środki walki, inne zasoby niezbędne do prowadzenia działań o charakterze sieciocentrycznym.

Wymienione poziomy tworzą sprzężone ze sobą elementy wojny sieciocentrycznej, określające w istocie model jej sieciocentrycznej architektury, który może być wykorzystany zarówno w działaniach koalicyjnych (sojuszniczych), jak i narodowych[35].

Sieciocentryczne środowisko tworzy nową jakość w dowodzeniu, a wielowymiarowość i złożoność zjawisk oraz specyficzne właściwości przyczyniają się do niejednoznacznego podziału przestrzeni egzemplifikujących działania sieciocentryczne. Podkreślić również należy, że nie ma w tym względzie jednolitej zgodności wśród ekspertów i znawców zagadnień sieciocentrycznych. Przeprowadzone analizy i oceny wskazują, że działania te są obecne we wszystkich wymiarach: szerokości, wysokość i głębokości pola walki. Ponadto rozciągają się również na przestrzeń elektromagnetyczną oraz tzw. przestrzeń informacyjną.

Istota koncepcji sieciocentrycznej wskazuje, że kwestią podstawową dla prowadzenia działań sieciocentrycznych jest spięcie całości sił i środków w jedną sieć informacyjną dającą dodatkowo możliwość wymiany, przetwarzania, udostępniania i przechowywania informacji.

W opinii wielu specjalistów koncepcja wojny sieciocentrycznej może zostać zrealizowana tylko wtedy, gdy możliwe będzie stworzenie odpowiedniej infrastruktury sieciowej, tzw. Globalnej Sieci Informacyjnej (*Global Information Grid* – GIG).

Autorzy publikacji *The Implementation of Network – Centric Warfare* do zasad działań sieciocentrycznych zaliczają[36]:

– dążenie do zdobycia przewagi informacyjnej (wyższość informacyjna),

– dostęp do zasobów informacji spełniającej określone wymagania i pochodzącej z różnorodnych źródeł, zgodnie z potrzebami i specyfiką określonego poziomu (szczebla) dowodzenia (każdego rodzaju sił zbrojnych i wojsk),

35 B. Smólski, *Wpływ nowych technologii na przebieg i wyniki operacji „Iracka wolność"* [w:] *Operacja „Iracka wolność"*, AON, Warszawa 2003, s. 113–114.

36 J. Kręcikij, *Istota działań sieciocentrycznych...*, dz. cyt., s. 130.

– szybkość dowodzenia wyrażająca się w szybkich cyklach dowodzenia,
– samosynchronizację,
– nielinearne pole walki (przestrzeń działań),
– rozproszenie sił (rozumiane bardziej jako przeciwstawienie się fizycznemu i geograficznemu zmasowania sił i środków),
– masowe użycie sensorów,
– wykorzystywanie okazji,
– zmniejszenie różnic pomiędzy poszczególnymi poziomami działań zbrojnych oraz zacieranie granic pomiędzy uczestniczącymi w działaniach rodzajami sił zbrojnych i wojsk.

Podsumowując, działania sieciocentryczne najczęściej przedstawia się jako bazującą na przewadze informacyjnej koncepcję prowadzenia współczesnych operacji, według której następuje wzrost siły bojowej przez połączenie w sieć informacyjną sensorów, decydentów i systemów walki dla osiągnięcia wymiernych efektów.

2.2. Walka informacyjna we współczesnych konfliktach zbrojnych

Walka informacyjna towarzyszyła zawsze walce zbrojnej. W tej sferze pełniła szczególnie ważną funkcję, niezależnie od tego, czy była tak formalnie nazywana, czy też nie. W historii wojen trudno znaleźć przykład, aby strona przegrana w walce informacyjnej zdołała osiągnąć zwycięstwo w walce zbrojnej[37].

Bardzo dużą rolę w walce informacyjnej odgrywają media. Konflikt w Wietnamie był jednym z pierwszych, który doczekał się tak szerokiej oprawy medialnej. Do Wietnamu pojechało 464 przedstawicieli mediów (w tym 179 dziennikarzy z USA), którzy relacjonowali przebieg konfliktu. Jednak, jak zauważa L. Ryżewski, reporterów było ok. 60, pozostałe osoby stanowiły zaś personel techniczny, były to również żony korespondentów[38]. W większości byli to reprezentanci mediów amerykańskich. Ponieważ korespondenci nie znali na ogół języka, zwyczajów i przebywali w Wietnamie stosunkowo krótko, relacje w głównej mierze sprowadzały się do prezentowania standardowych obrazów, ukazujących amerykańskich żołnierzy w czasie prowadzenia

37 L. Ciborowski, *Walka...*, dz. cyt., s. 10.

38 L. Ryżewski, *Obraz komunistycznej ofensywy w amerykańskich mediach*, „Studia Medioznawcze" 2009, nr 1, s. 46.

działań, uzupełnionych komentarzem, często opartym na doniesieniach agencyjnych.

Wojna w Wietnamie była pierwszym konfliktem, podczas którego nie obowiązywała oficjalna cenzura wojskowa. Reporterzy akredytowani przy oddziałach amerykańskich mogli udać się wszędzie i pisać, o czym chcieli. Musieli jednakże przestrzegać zasad dotyczących piętnastu kategorii informacji, które musiały być zatwierdzone przez Dowództwo Wsparcia Wojskowego w Wietnamie (*Military Assistance Command Vietnam* – MACV)[39], a dotyczyły m.in. ruchów wojsk, czy liczby zabitych i rannych. Łamiącym te zasady dziennikarzom groziło anulowanie lub zawieszenie akredytacji.

Podstawowym narzędziem walki informacyjnej w Wietnamie były działania psychologiczne. Obejmowały one wszystkie dziedziny życia społeczeństwa wietnamskiego, jednak główne działania skierowano przeciwko siłom Frontu Wyzwolenia Narodowego (FWN). Metody prowadzenia tych działań były różnorodne i zależały od obiektu oddziaływania, planowanych celów, sytuacji militarnej i posiadanych sił.

W Wietnamie amerykańskie działania psychologiczne stanowiły integralną część działań specjalnych. Łączono je ściśle z działaniami bojowymi, a ich celem było pozyskanie przychylności społeczeństwa dla rządu sajgońskiego oraz zastraszenie ludności współpracującej z partyzantami przy jednoczesnym zapewnieniu pomocy dla wszystkich wyznających odmienny niż komunistyczny światopogląd.

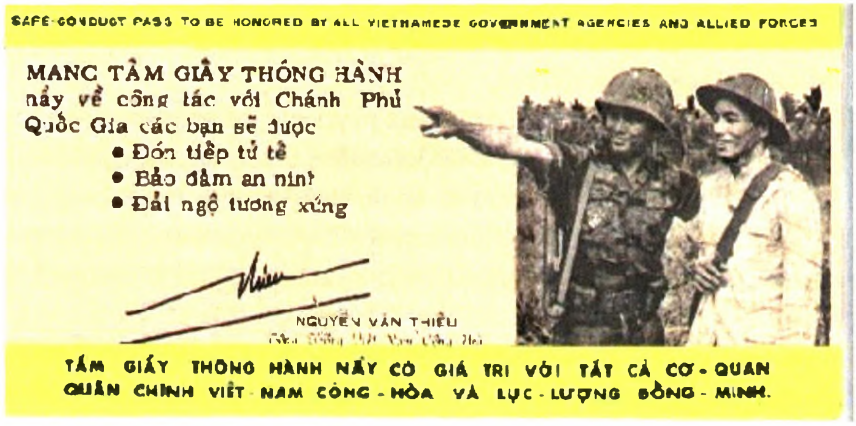
Komponent lądowy w bezpośredniej strefie działań bojowych prowadził działania psychologiczne w sposób zdecentralizowany. Głównym elementem działań psychologicznych wspierającym wojska walczące była kompania wyposażona w urządzenia głośnikowe montowane na samochodach, transporterach i śmigłowcach. Na prowincji działania psychologiczne prowadziły grupy w składzie 40–60 osób, po jednej w każdym okręgu wojskowym. Kompanie działań psychologicznych działały na tyłach sił partyzanckich i na tyłach wojsk własnych. Ich działalność polegała na rozpowszechnianiu materiałów propagandowych środkami technicznymi za pomocą radiofonii publicznej i specjalnych nadajników radiowych pracujących na określonej częstotliwości.

39 Zadaniem MACV było wspieranie Armii Republiki Wietnamu. Dowództwo miało instruktorów z Sił Specjalnych Armii Stanów Zjednoczonych (Zielone Berety) oraz personel z Centralnej Agencji Wywiadowczej (CIA).

W tym celu ludności cywilnej rozdawano miniaturowe odbiorniki jednozakresowe.

W latach 1965–1972 rząd południowowietnamski we współdziałaniu z Połączoną Agencją Stanów Zjednoczonych ds. Publicznych (*Joint United States Public Affairs Office* – JUSPAO) odniósł duże sukcesy dzięki stosowaniu przepustek do „powrotu", rozpowszechnianych na całym terytorium Południowego Wietnamu oraz wzdłuż drogi Ho Chi Mina. Na pierwszej stronie ulotka zawierała emblemat sztandaru południowowietnamskiego w otoczeniu sześciu sztandarów państw sojuszniczych oraz napis: „Przepustka ta jest honorowana przez administrację rządu wietnamskiego oraz siły zbrojne państw sojuszniczych"[40].

Tekst był zredagowany w językach angielskim, koreańskim i tajlandzkim. Na odwrocie przepustka zawierała apel w języku wietnamskim zredagowany przez prezydenta Nguyena Van Thieu.



Źródło: htpp://www.psywarrior.com/viet.html [dostęp: 4.04.2002].

Rys. 1. Ulotka z tekstem zredagowanym przez prezydenta Nguyena Van Thieu

Ciekawym rozwiązaniem było zastosowanie ulotek-kalendarzyków, ulotek-poradników oraz torebek z prezentami i zabawkami[41].

Niekiedy wraz z ulotkami zrzucano papierosy, pastę do zębów, zabawki dla dzieci oraz odbiorniki jednozakresowe do odbioru audycji nadawanych z Sajgonu.

40 Z. Modrzejewski, *Operacje psychologiczne w konfliktach po II wojnie światowej*, AON, Warszawa 2002, s. 29.

41 Z okazji Dnia Dziecka w 1967 roku samoloty zrzuciły około 15 tys. plastikowych torebek z zabawkami i słodyczami.

Nawoływanie żołnierzy Północnego Wietnamu i Frontu Wyzwolenia Narodowego do dezercji i przechodzenia na stronę rządu sajgońskiego stanowiło jeden z podstawowych celów operacji psychologicznych sojuszników. „Przyłączenie" lub „powrót" stanowiły oficjalne pojęcia dla określenia dezercji z szeregów komunistycznych.

Aby złamać ducha bojowego partyzantów oraz pozbawić ich oparcia wśród społeczeństwa wietnamskiego stosowano najczęściej dwie zasadnicze metody: zastraszanie i propagandę pozyskującą. Efekty zastraszania osiągano poprzez systematyczne prowadzenie operacji psychologicznych oraz działań z udziałem lotnictwa, broni ciężkiej, rakiet, napalmu i innych środków rażenia. Stałe nękanie partyzantów, utrzymywanie ich w ciągłym napięciu i niepewności miało doprowadzić do osłabienia morale, załamania chęci do walki, masowych dezercji, rozkładu dyscypliny, a nawet wywołania chorób psychicznych. Efekty propagandy pozyskującej planowano osiągnąć przez ciągłe wskazywanie partyzantom „dobrodziejstw", jakie ich czekają po przejściu na stronę amerykańską. W propagandzie tej eksponowano czynnik materialny. Każdy partyzant po przejściu z bronią w ręku na stronę amerykańską otrzymywał odpowiednią ilość pieniędzy w zależności od rodzaju posiadanej broni.

Wojska amerykańskie stosowały różne sposoby i środki działań psychologicznych, np. w rejonach zamieszkałych przez ludność niepiśmienną preferowano przekaz ustny. Usiłowano zastraszyć ludność oddziaływaniem na jej instynkt samozachowawczy. Zrzucano ulotki z asem pikowym (wśród miejscowej ludności panowało przekonanie, że as przynosi nieszczęście temu, kto go znajdzie) oraz wykorzystywano urządzenia imitujące krzyk sowy (krzyk sowy zapowiada bliską śmierć). Ponadto ustalono cennik, w którym określono, jaką wartość mają poszczególne rodzaje wiadomości o wojskach partyzanckich przekazanych dla Amerykanów.

Najbardziej rozpowszechnionymi i najczęściej stosowanymi sposobami psychologicznego oddziaływania na partyzantów były ulotki i audycje elektroakustyczne. Ulotki propagandowe rozpowszechniano w rejonach kontrolowanych przez partyzantów, w domniemanych rejonach koncentracji, a także w miejscach przypuszczalnego obozowania w dżungli. Szczególną aktywność prowadzenia akcji ulotkowych można było zauważyć podczas akcji ofensywnych, w czasie których zrzucano miliony ulotek.

Podczas wojny w Wietnamie jednostki działań psychologicznych rozpowszechniały ok. 60 milionów ulotek miesięcznie. Zrzucano je z samolotu Lockheed C-130 Hercules, który zabierał jednorazowo 11 milionów ulotek w zasobnikach po 75 tysięcy sztuk. Zasobniki te wyposażono w spadochrony,

które otwierały się na określonej wysokości. Stwierdzono, że najlepszy format ulotki, umożliwiający dogodne jej spadanie ku ziemi ruchem wirowym, to rozmiar 18 x 9 cm[42].

Amerykanie starali się również podważyć zaufanie ludności cywilnej Wietnamu Północnego do obowiązujących w państwie środków płatniczych. Rozpowszechniano w tym celu miliony kopii biletu bankowego wartości jednego donga. Na pierwszej stronie zamieszczono następujący tekst:

„Wraz z przedłużającą się wojną pieniądz coraz bardziej traci na wartości i można za niego kupić coraz mniej towarów. Ceny towarów będą systematycznie wzrastać. Wasze oszczędności staną się bezwartościowymi kawałkami papierów".

Na odwrocie zaś:

„Strzeżcie się kolejnej reformy pieniędzy, podobnej do tej z roku 1959. Możecie stracić cały Wasz dobytek, owoce Waszego potu i łez"[43].

Duży sukces uzyskiwały ulotki odwołujące się do uczuć rodzinnych Wietnamczyków lub ich wierzeń religijnych i przesądów. Inne ulotki podawały wskazówki jak organizować grupową lub indywidualną dezercję. Jedną z takich ulotek wydrukowano w sierpniu 1968 roku w liczbie 46 milionów sztuk. Zawierała ona gwarancję bezpieczeństwa, otrzymania wyżywienia i ubrania, nagrody za przyniesioną broń, obietnicę przeszkolenia zawodowego, powrotu do rodziny i opieki lekarskiej. Na rewersie tej ulotki można było przeczytać następujące pouczenia:

1. Przyłączcie się do każdego organu cywilnego lub wojskowego rządu Wietnamu Płd. lub do jego sojuszników;

2. Przyłączcie się do nas bez względu na porę dnia i nocy;

3. Zanim przyjdziecie do nas, ukryjcie dobrze Waszą broń, a za wskazanie tego miejsca otrzymacie nagrodę;

4. Jeżeli jest to możliwe, przychodźcie z ulotką. Nawet jeśli jej nie macie, nie wahajcie się przed tym krokiem[44].

Do prowadzenia walki w eterze rząd południowowietnamski korzystał z nadajnika o mocy 10 kW, który obejmował swoim zasięgiem cały Wietnam Południowy i Północny oraz południowe rejony Chin. W 1967 roku czas emisji wynosił 12 godzin na dobę. W 1970 r. wzrósł do 46 godzin (na różnych czę-

42 Z. Modrzejewski, *Operacje psychologiczne...*, dz. cyt., s. 32.

43 A. Podkowski, *Rodzaje działań psychologicznych na polu walki*, „Zeszyty Naukowe AON" 1997, nr 1, s. 137.

44 Tamże, s. 138.

stotliwościach) z tym, że 54% programu stanowiła muzyka pop. Dezerterzy z Wietnamu Północnego potwierdzali, że słuchali tego rodzaju programów radiowych, ponieważ muzyka pop była tam zabroniona jako dekadencka i burżuazyjna. Od czasu do czasu rozgłośnia nadawała wietnamską muzykę ludową przeplataną wiadomościami politycznymi nadawanymi w odstępach jednogodzinnych.

Głos Ameryki emitował 17-godzinny program przeznaczony dla mieszkańców Wietnamu Południowego, składający się z wiadomości, komentarzy i muzyki. W latach 1967–1971 czas emisji programów Głosu Ameryki na różnych częstotliwościach potrojono.

W dniu 15 sierpnia 1966 roku południowokoreańska rozgłośnia Wolna Azja rozpoczęła nadawanie własnych programów. Rozgłośnia radiowa o mocy 500 kW obejmowała swoim zasięgiem Koreę Północną, Chiny, Wietnam Północny i Południowy. Z informacji prasowych napływających z Hanoi na początku 1971 roku wynikało, że władze lokalne ostro zareagowały (aż do kar więzienia włącznie) na słuchanie przez ludność cywilną audycji rozgłośni południowowietnamskiej i amerykańskiej.

Często stosowanym sposobem oddziaływania psychologicznego na partyzantów było nadawanie audycji przy pomocy rozgłośni elektroakustycznych dużej i średniej mocy. Rozgłośnie montowano na czołgach, samochodach pancernych i śmigłowcach, a wykorzystywano podczas akcji psychologicznych przeciwko partyzantom w wypadku ich okrążenia na małym obszarze. Posługując się nimi, dowódcy sajgońscy i amerykańscy nadawali wezwania do zaprzestania walki, apele, odezwy i ostrzeżenia. Prowadząc tego rodzaju akcje psychologiczne, posługiwano się różnymi treściami. Aby wywołać przerażenie i strach, szczególnie w nocy, z taśm magnetofonowych odtwarzano przeraźliwe jęki, płacz matki i dziecka, buddyjską muzykę pogrzebową, czy odgłosy dzikich zwierząt. W audycjach tych wykorzystywano także często dezerterów i zbiegów, którzy nawoływali swych kolegów do pójścia w ich ślady[45].

Akcje psychologiczne, których obiektem była ludność cywilna Wietnamu Południowego, były realizowane pod hasłem „zdobyć serca i umysły narodu wietnamskiego". Stosowano różne formy działań psychologicznych; obok akcji ulotkowych w większym zakresie wykorzystywano rozgłośnie radiowe oraz inne środki masowego przekazu. Wychodząc z założenia, że najskuteczniejszą formą oddziaływania psychologicznego jest żywe słowo, Amerykanie organi-

45 Z. Modrzejewski, *Operacje psychologiczne...*, dz. cyt., s. 34.

zowali specjalne mieszane grupy propagandowe, które odpowiednio przygotowane i wyekwipowane udawały się w teren, aby prowadzić agitację wśród ludności wiejskiej.

Podsumowując, należy stwierdzić, że w ciągu całej wojny w Wietnamie stosowano trzy rodzaje oddziaływania psychologicznego na przeciwnika:

- przy użyciu materiałów drukowanych,
- za pomocą radia,
- przez rozgłośnie elektroakustyczne.

Z powodów obiektywnych nie miało sensu wówczas wykorzystywanie telewizji. Jednak w latach późniejszych jej możliwości oddziaływania zostały w pełni docenione (zwłaszcza w koncepcjach oddziaływania na ludność na terenach okupowanych oraz wobec jeńców wojennych w obozach).

Kolejnym konfliktem zbrojnym, w którym walka informacyjna miała duże znaczenie, jest I wojna w Zatoce Perskiej. Konflikt ten jest powszechnie nazywany „pierwszą wojną informacyjną" lub „wojną telewizyjną". Zdaniem ekspertów od czasów tej wojny rozstrzygająca przewaga informacyjna traktowana jest jako istota współczesnych koncepcji prowadzenia operacji informacyjnych.

Przebieg działań wojennych w rejonie Zatoki Perskiej zweryfikował wiele teoretycznych rozwiązań prowadzonych wcześniej w ciszy gabinetów, a sprawdzonych jedynie na symulatorach komputerowych, czy w ramach ćwiczeń poligonowych.

Podobnej weryfikacji nie uniknęła również amerykańska koncepcja prowadzenia operacji psychologicznych. Okazało się, że siły specjalne, w tym komórki operacji psychologicznych, mogą z powodzeniem prowadzić działania i odegrać znaczącą rolę w konfliktach o wysokiej, średniej, jak i niskiej intensywności. Są to bowiem siły zdolne do działania kompleksowego w rejonie konfliktu, przyczyniając się tym samym do maksymalizacji militarnego sukcesu, a zarazem minimalizacji kosztów.

Przed rozpoczęciem wojny amerykańska 4. Grupa Działań Psychologicznych, której obszarem operacyjnym jest Bliski Wschód, wzięła udział w ćwiczeniach pod kryptonimem „Bright Star" i „Desert Flag", których celem było przygotowanie personelu do działania w nowych warunkach. Generał N. Schwarzkopf wyznaczył grupie zadanie zbierania i analizowania danych dotyczących wartości moralno-bojowych żołnierzy irackich, sytuacji poli-

tycznej i nastrojów społeczeństw państw arabskich na tle udziału USA w konflikcie na Bliskim Wschodzie[46].

Po irackiej agresji na Kuwejt w dniu 2 sierpnia 1990 roku pododdziały działań psychologicznych przemieszczono w rejon Zatoki Perskiej. Centrum dowodzenia rozmieszczono w Rijadzie. Zadaniem elementów działań psychologicznych było pozyskanie ludności sojuszników arabskich dla planów amerykańskich, w tym przede wszystkim niezbyt przychylnej ludności Arabii Saudyjskiej.

Bardzo ważnym przedsięwzięciem realizowanym w pierwszej kolejności przez specjalistów PSYOPS było „usprawiedliwienie" interwencji.

W tym celu starano się udowodnić, że:

– możliwość rozwiązania konfliktu na drodze politycznej została już wyczerpana i dlatego konieczna jest interwencja militarna,

– państwa koalicji antyirackiej są jedynymi obrońcami prawa międzynarodowego,

– celem interwencji jest zapobieżenie w przyszłości takim sytuacjom, w których jakiekolwiek silniejsze państwo podejmie próbę podporządkowania sobie słabszego państwa wbrew postanowieniom prawa międzynarodowego,

– głównym motywem działania koalicji jest moralny obowiązek udzielania pomocy ofierze agresji, niezależnie od tego, kto jest agresorem.

4. Grupa Działań Psychologicznych zdobywała dane o armii irackiej przy współpracy z CIA oraz europejskimi i azjatyckimi pracownikami kontraktowymi, którzy wykonując różne prace na terenie Iraku, mogli dostarczyć wstępnych danych o nastrojach wśród ludności i żołnierzy.

Następnie, wykorzystując fakt złamania irackich kodów szyfrowych, personel działań psychologicznych mógł analizować przechwytywane dane oraz przygotować własne dezinformowanie na czas działań bojowych.

Amerykańscy specjaliści wojskowi uznali, że doświadczenia zebrane podczas wojny w Wietnamie uda się zastosować w obecnej sytuacji militarnej i dlatego też nie widzieli potrzeby zmiany form i metod oddziaływania psychologicznego. Stosowano zatem ulotki i audycje radiowe nawołujące żołnierzy przeciwnika do dezercji i ukazujące bezsens prowadzonych działań wojennych. Jednocześnie starano się pozyskać ludność cywilną Iraku i arabskich sojuszników Stanów Zjednoczonych dla prowadzonej przez nich polityki.

46 M. Kwiecień, *Działania psychologiczne Armii Stanów Zjednoczonych*, „Przegląd Wojsk Lądowych" 1997, nr 11, s. 54.

W pasie przygranicznym rozrzucono ulotki w języku arabskim mające osłabić wolę walki żołnierzy irackich oraz sugerujące kierunki przyszłych ataków i maskujące rzeczywiste zamiary głównodowodzącego.

Jedna z pomyślnie przeprowadzonych akcji psychologicznych polegała na dezinformacji przeciwnika. Ulotki zatytułowane „Fala", zapowiadające rzekomy desant Marines, zostały włożone do butelek, które następnie zakorkowano i wrzucono do morza. Dotarły one do wschodniego wybrzeża Kuwejtu. Akcja ta została przeprowadzona na kilka dni przed rozpoczęciem działań lądowych. Jej celem było wprowadzenie w błąd irackiej obrony i spowodowanie przegrupowania wojsk irackich w niewłaściwym kierunku[47].

Z chwilą rozpoczęcia działań zbrojnych przeciwko Irakowi prace personelu operacji psychologicznych zostały ukierunkowane na osłabienie wartości moralno-bojowych żołnierzy Saddama Husajna, obniżenia ich woli walki, a w konsekwencji nakłonienie do dezercji i poddania się.

Kształtowano przekonanie, że Saddam Husajn jest dyktatorem, szaleńcem i mordercą, którego można porównać rzekomo tylko z Hitlerem, wojska koalicji mają wyraźną przewagę pod względem technologicznym i taktycznym, strona iracka dopuszcza się naruszania prawa międzynarodowego w Kuwejcie, przestępstw wobec ludności, grabieży mienia itp.[48]

Akcje ulotkowe przeprowadzane były permanentnie i uwzględniały w swojej treści zmieniającą się sytuację militarną po masowych bombardowaniach oraz zmianę w nastrojach żołnierzy irackich przejawiającą się m.in. w zwiększonej liczbie dezercji.

Według danych Pentagonu w czasie od 30 grudnia 1990 roku do 28 lutego 1991 roku rozrzucono nad terytorium irackim ponad 29 milionów ulotek (1,5 ulotki na statystycznego mieszkańca lub 50 ulotek na statystycznego żołnierza irackiego).

Badania przeprowadzone przez 13. Batalion PSYOP wykazały, że około 98% irackich jeńców widziało te ulotki, 88% uwierzyło w to, co było w nich napisane, a 70% przyznało, że ulotki pomogły im w podjęciu decyzji o kapitulacji lub przejściu na stronę sprzymierzonych.

47 S. Sikora, *Działania psychologiczne w operacji „Pustynna Burza"*, „Wojsko i Wychowanie" 1993, nr 4, s. 81.

48 J. Biziewski, *Pustynna Burza*, cz. 2, Altair, Warszawa 1994, s. 70–71.

Źródło: http://www.geocities.com/Pentagon/1012/links.html [dostęp: 4.04.2002].

Rys. 2. Ulotka o treści: „Pozostanie tutaj oznacza śmierć"

Działania psychologiczne komponentu lądowego były wspierane przez komponent powietrzny. Ulotki przenoszono za pomocą samolotów B-52 Stratofortress, F-16 Fighting Falcon, F/A-18 Hornet i samolotów transportowych MC-130 Hercules. Samoloty bojowe zrzucały bomby propagandowe M-129E1, natomiast MC-130 Hercules miał podwieszane zasobniki z ulotkami (całe pakiety pod klapą rufową). Ponadto wykorzystywano haubice kal. 155 mm oraz zrzucano butelki na wybrzeżu morskim (w okresie poprzedzającym otwarty konflikt)[49].

Nie mniej znaczące były działania zespołów rozgłośni elektroakustycznych. Rozgłośnie wykorzystywano głównie z ziemi, ale montowano je również na śmigłowcach.

Na kilka dni przed planowanym rozpoczęciem bitwy lądowej zauważono irackie jednostki w odległości 60 mil od pozycji 101 Dywizji Powietrznodesantowej, która miała odegrać kluczową rolę, atakując z powietrza.

Każda brygada 101 Dywizji posiadała zespół rozgłośni elektroakustycznych, jednak obszar, na którym znajdowały się wojska irackie, był poza zasięgiem ich działania. Do wykonania tego zadania stworzono doraźnie zespół, którego dowódcą został oficer 9. Batalionu PSYOP – kpt. Thomas Wright. W skład zespołu kapitana Wrighta weszli również dwaj podoficerowie: sierż. sztab. Jensen, znający biegle język arabski, oraz posiadający ogromne

49 P. Lemanowicz, I. Boguszewicz, *Działania psychologiczne w Zatoce Perskiej*, „Wojsko i Wychowanie" 1996, nr 10, s. 83.

doświadczenie sierż. sztab. Fivel. Kpt. Wright opracował projekt ulotki, który następnie został poddany obróbce językowej przez językoznawców.

Po dotarciu nad pozycje irackie rozrzucono ulotki, a następnie przez megafony nawoływano żołnierzy irackich do poddania się. Po stwierdzeniu, że nadawanie jest zakłócane przez silnik śmigłowca, postanowiono wylądować poza zasięgiem rażenia lekkiej broni maszynowej i z ziemi prowadzić dalsze działania. Wynik prowadzonej akcji był zdumiewający – aż 420 Irakijczyków oddało się do niewoli.

Po wyeliminowaniu irackich radiostacji natychmiast rozpoczęto nadawanie na tych samych falach audycji opracowanych przez specjalistów amerykańskich. Przez satelitę nadawano w języku arabskim nie tylko audycje informacyjne i wiadomości z frontu, ale także modlitwy z Koranu oraz wypowiedzi dobrze traktowanych jeńców wojennych. Zaznaczyć w tym miejscu należy, że niektóre audycje były przygotowywane jeszcze przed wybuchem konfliktu. Audycje radiowe nadawano z intensywnością 18 godzin na dobę, wykorzystując do tego celu stacjonarne przekaźniki naziemne na terytorium Arabii Saudyjskiej i Turcji oraz zamontowany na pokładzie samolotu retranslator Volant Solo.

Zarówno audycje radiowe, jak również ulotki amerykańskie, nawoływały żołnierzy irackich do dezercji. Jednocześnie deklarowano dobre warunki traktowania, bezpieczeństwo, opiekę medyczną i wyżywienie, co dla skrajnie wyczerpanego psychicznie i fizycznie żołnierza irackiego miało duże znaczenie. W nadziei na zaspokojenie głodu, z ulotkami w rękach, poddawali się oni wojskom sojuszniczym, nie zważając na funkcjonujący w ich armii kategoryczny, zagrożony karą śmierci zakaz ich posiadania. Głos zabierali w tych audycjach wzięci do niewoli żołnierze lub dezerterzy, którzy zwracając się do konkretnych kolegów i dowódców, uwiarygodniali te audycje.

Jeden z uczestników wojny w rejonie Zatoki Perskiej – pułkownik Layton G. Dunbar – dowodzący 4. Grupą Operacji Psychologicznych stwierdził, że prawie 3/4 dezerterów irackich przyznało, że do ucieczki skłoniły ich audycje radiowe i ulotki.

Duży wpływ na morale armii irackiej miała forma przekazu wiadomości o działaniach militarnych, jaką w środkach masowego przekazu stosowali Amerykanie. Prezentowano wyłącznie spektakularne sukcesy, dodatkowo je koloryzując. Miało to wpłynąć na osłabienie politycznego poparcia dla Iraku ze strony niektórych państw arabskich, a także utwierdzić w sojuszu arabskich partnerów USA.

Amerykanie z inspiracji specjalistów operacji psychologicznych zadbali również o należyte podkreślenie militarnego udziału ich sojuszników. Mimo

że procentowo lotnictwo arabskie stanowiło tylko drobną część powietrznej armady, specjalnie zorganizowano, a następnie propagandowo nagłośniono zestrzelenie przez saudyjskiego pilota F-15 dwóch maszyn Mirage F-1 irackich sił powietrznych. Aby oba te samoloty weszły w celownik pilota saudyjskiego, kilka maszyn amerykańskich wykonało coś w rodzaju pościgu. Manewr ten wywołał wrażenie, jakoby w powietrzu walczyli Arabowie z Arabami.

Propagandowe nagłośnienie zwycięstw powietrznych spowodowało taką destrukcję postawy pilotów irackich, że zaczęli masowo uciekać na najlepszych maszynach do Iranu, odsłaniając w ten sposób całkowicie przestrzeń powietrzną nad Irakiem.

Wobec braku rzeczywistego obrazu wartości moralno-bojowych Gwardii Republikańskiej, znajdującej się w drugim rzucie ugrupowania armii irackiej, za radą specjalistów PSYOPS do złamania, jak się spodziewano, wysokiego morale, użyto bombowców B-52, które prowadziły dywanowe naloty na ich pozycje.

Każdy z samolotów mógł zrzucić do 30 ton bomb. Taka bomba powodowała krater o średnicy 17 metrów, a jej odłamki raziły w promieniu 400 metrów. Po kilku nalotach żołnierze dostawali szału, cierpieli na bezsenność, nie byli zdolni do prowadzenia walki.

Dowództwo alianckie, decydując się na masowe użycie samolotów B-52, chciało doprowadzić do psychicznego załamania armii irackiej, a przy okazji także ludności cywilnej, licząc, że ta z kolei wywoła w Bagdadzie zamieszki i może spowodować upadek Saddama.

Znaczny efekt psychologiczny, osłabiający armię iracką, uzyskano przez podzielenie przestrzeni powietrznej Iraku na sektory, w których bez przerwy znajdowały się samoloty bojowe strzelające do wszystkiego, co mogło być celem wojskowym.

Amerykańscy piloci dostali rozkaz atakowania tylko wyznaczonych obiektów: „Mieli oni surowy zakaz atakowania dzielnic mieszkaniowych, a zwłaszcza meczetów. Zbyt wielkie ofiary w ludziach, a co gorsza, zniszczenie miejsc świętych dla wyznawców Proroka mogły wywołać oburzenie w świecie arabskim i być propagandowo wykorzystane przez Saddama”[50].

Szczególną uwagę zwrócono na wyrzutnie rakietowe Scud, zwłaszcza znajdujące się w zachodnich rejonach Iraku, gdyż z tego obszaru można je było

50 R. Bielecki, *Pustynna Burza*, Bellona, Warszawa 1991, s. 83.

skierować na terytorium Izraela. Irackiemu dyktatorowi zależało na jak najszybszym wciągnięciu Izraela do tego konfliktu.

Poza wykorzystaniem sił powietrznych, podjęto również akcję obezwładniania załóg wyrzutni Scud przez psychologiczne wytworzenie poczucia ciągłego zagrożenia z powietrza. Samoloty B-52, dyżurujące w powietrzu (dzięki samolotom tankowania powietrznego) nad potencjalnym terenem rozmieszczenia wyrzutni, były w ciągłej gotowości do zniszczenia wyrzutni rakiet Scud.

Stosowano również inne metody. Aby umożliwić Marines bezpieczne przejście przez pola minowe, należało obezwładnić batalion iracki, który bronił tego przejścia. W tym celu wykorzystano elementy działań psychologicznych. Najpierw rozrzucono ulotki ostrzegające przed bombardowaniem wielkimi bombami BLU-82, a następnie żeby potwierdzić tę informację, zbombardowano taką bronią pozycje irackie.

Dla wzmocnienia efektu pozycje te zbombardowano w nocy. Wybuch do złudzenia przypominał eksplozję nuklearną. W dalszej kolejności powtórzono zrzucanie ulotek, zapowiadających dalsze bombardowania BLU-82. Przerażeni żołnierze iraccy wraz z dowódcą batalionu, sztabem, oficerem wywiadu, dysponującym mapami pól minowych, przebiegli przez granicę i oddali się do niewoli. Umożliwiło to wykonanie przejść w polach minowych, gdy rozpoczęła się operacja lądowa.

Głównym założeniem specjalistów operacji psychologicznych, wynikającym zresztą ze strategii użycia sił, było ścisłe współdziałanie z innymi rodzajami wojsk w celu maksymalizacji ich wysiłku bojowego. Przykładem może być współpraca w maskowaniu operacyjnym planowanego uderzenia z kierunku południowo-zachodniego z głębokim okrążeniem armii irackiej.

Ukryć trzeba było przesunięcie XVIII i VII Korpusu, tj. około 200 tysięcy ludzi, z całym zaopatrzeniem na odległość 300 mil, w terenie pustynnym, po jednej drodze. Prócz samobieżnego sprzętu bojowego trzeba było zgromadzić do przerzutu ludzi i sprzętu 4,5 tysiąca ciężarówek. W celu zachowania manewru w tajemnicy podjęto wielostronne działania dezinformujące z udziałem komórek walki psychologicznej. Prowadzenie dezinformacji radiowej o koncentracji Marines na morzu w pobliżu wybrzeża Kuwejtu i próbie desantów z morza, a także ulotkowe bombardowanie jednostek irackich broniących dostępu do brzegów, odniosło skutek. Uderzenie z południowego zachodu było zupełnym zaskoczeniem.

Zachodnie służby specjalne przeprowadziły także interesującą operację psychologiczną skierowaną do ludności Iraku. Przerzuciły one na terytorium Iraku tysiące prostych odbiorników tranzystorowych umożliwiających słu-

chanie koalicyjnych rozgłośni radiowych, komunikatów, komentarzy, wypowiedzi i apeli[51].

W treściach powyżej wspomnianych audycji posługiwano się najczęściej następującymi argumentami:

- przewaga sprzymierzonych jest ogromna, a wręcz miażdżąca,
- komunikaty irackie o sytuacji militarnej są celowo fałszowane,
- jest to wojna, która doprowadzi do masowych zniszczeń, których jedyną przyczyną są ambicje Saddama Husajna. W tym czasie Husajn schroni swoją rodzinę wraz z całym majątkiem poza granicami kraju,
- jedynym rozsądnym działaniem umożliwiającym przeżycie jest zaniechanie oporu.

Ta sama operacja skierowana była również do irackich żołnierzy, a jej skutki przerosły oczekiwania sprzymierzonych.

Jako przykład należy tu podać, że: „(...) czterech z pięciu jeńców regularnie słuchało audycji radiostacji Głos Zatoki – przygotowanych przez specjalistów psychologicznych sił zbrojnych USA. Wpływ tej radiostacji był tak poważny, że zabroniono im posiadać przy sobie radioodbiorników"[52].

Dowódcy iraccy konfiskowali swoim żołnierzom osobiste radia, gdyż wiedzieli, jaki skutek mogą przynieść amerykańskie audycje propagandowe.

Od stycznia 1991 roku sześć ukrytych stacji radiowych rozpoczęło nadawanie programu „Głos Zatoki". Rozgłośnia ta od 1 kwietnia 1991 roku nadawała stale ponad 210 godzin programu na żywo i 330 godzin retransmitowanych. Podczas działania tych stacji zrealizowano łącznie 189 operacji psychologicznych. Wiadomości te przekazywane były również czasie kampanii lądowej przez głośniki umieszczone w samochodach i helikopterach.

Amerykańskie grupy PSYOP współdziałały z żołnierzami saudyjskimi, egipskimi i kuwejckimi, którzy wnieśli niezbędną znajomość języka, kultury i mentalności przeciwnika.

Siły koalicji wykorzystały również taśmę wideo pt.: *Nations of the World Take a Stand*, ukazującą potęgę wojsk koalicyjnych. Taśma ta została rozprowadzona na całym Środkowym Wschodzie, a ponad 200 kopii trafiło także do Bagdadu.

51 P. Lemanowicz, I. Boguszewicz, *Działania psychologiczne...*, dz. cyt., s. 81–82.

52 A. Podkowski, *Działania psychologiczno-propagandowe w walce zbrojnej*, AON, Warszawa 1993, s. 39.

Należy pamiętać, że działania psychologiczne prowadziła również strona iracka. Przykładem takich działań może być pokazanie 20 stycznia 1991 roku przez telewizję iracką siedmiu mężczyzn w mundurach wojskowych z zawiązanymi oczami. Trzech miało być pilotami amerykańskimi, dwóch brytyjskimi, jeden włoskim i jeden kuwejckim. Piloci oprócz podania swych nazwisk i stopni wojskowych, dodawali też, prawdopodobnie pod przymusem, że „Stany Zjednoczone nie miały racji, kiedy zaatakowały pokojowy naród Iraku"[53].

Podobnie jak sprzymierzeni, strona iracka w pierwszej kolejności usprawiedliwiła przeprowadzoną już inwazję. W tym celu przekonywano, że:

– Kuwejt jest państwem zabezpieczającym brytyjskie interesy, powstałym w procesie dekolonizacji z terytoriów należących historycznie do Iraku,

– Kuwejtczycy są narodem uciskanym, a więc inwazja jest „wojną wyzwoleńczą",

– Irak nadal będzie żył w nędzy, podczas gdy warstwy rządzące w Kuwejcie opływają we wszelkiego rodzaju dobra ze sprzedaży bogactw należących faktycznie do Iraku.

Propaganda iracka koncentrowała się przede wszystkim na próbach wywołania wrogości wobec antyirackiej koalicji. Starano się wykorzystać rezultaty działań militarnych wojsk sprzymierzonych jako skierowane głównie przeciwko ludności cywilnej. Eksponowano zniszczenia obiektów, straty, zabitych. Upowszechniano skutki nałożonego embarga – brak żywności i lekarstw.

Usiłowano również wykorzystać wątki religijne. Przedstawiano Irak jako jedyne państwo islamu zdecydowane stanąć naprzeciw zachodniego świata. Sugerowano połączenie się z Iranem w wojnie religijnej.

Ponadto obok apelowania do opinii światowej, aby powstrzymać „niczym nieuzasadnioną agresję Busha" i „bezlitosne bombardowanie irackiej ludności cywilnej" Saddam Husajn groził, że spowoduje olbrzymie straty wśród sprzymierzonych przez wykorzystanie „żywych tarcz" z jeńców wojennych oraz przez użycie broni chemicznej[54].

Za najważniejszy z postawionych sobie przez Irak celów propagandowych uznać należy dążenie do wytworzenia w narodach państw arabskich uczestniczących w walce negatywnego nastawienia do tego uczestnictwa. Wykorzystano argumenty nacjonalistyczno-religijne o świętej wojnie (dżihadzie), nawoływano do arabskiej jedności przeciwko Zachodowi, wykorzystywano

53 J. Biziewski, *Pustynna...*, dz. cyt., s. 90.

54 Tamże, s. 112.

wzajemne powiązania elit duchownych islamu, wreszcie usiłowano tworzyć złudzenie, że możliwe jest utworzenie na terenach Kuwejtu państwa palestyńskiego. Upowszechniano mit o niezłomności narodu irackiego i jego armii.

Można z całą pewnością stwierdzić, że znaczenie działań psychologicznych zostało docenione przez obydwie strony konfliktu.

Działania psychologiczne prowadzone przez Amerykanów można podzielić na działania główne dla osiągnięcia celów zasadniczych oraz towarzyszące, które miały wspierać osiąganie celów głównych, dezinformować, ośmieszać, wyszydzać i nakłaniać do postaw pasywnych oraz dezercji. Odegrały one niebagatelną i pozytywną rolę, ułatwiając działania bojowe wojsk sprzymierzonych, zwłaszcza amerykańskich. Zmasowane oddziaływanie psychologiczne, w połączeniu z efektywnymi działaniami lotnictwa, spowodowały znaczący spadek morale wojsk irackich.

W działaniach psychologicznych na polu walki zastosowano wszystkie dostępne ówcześnie środki, a mianowicie: środki radiowe, materiały ulotne (dominujące i jednocześnie najskuteczniejsze) oraz rozgłośnie elektroakustyczne.

O sukcesie, jaki odniosła kampania psychologiczna w operacji „Desert Storm", mogą świadczyć następujące dane: ponad 17 tysięcy żołnierzy irackich uciekło do Arabii Saudyjskiej i Turcji, a ponad 44% zdezerterowało.

Po zakończeniu wojny przeprowadzono badania na grupie 250 jeńców i stwierdzono, że 98% z nich widziało ulotki, 58% słyszało audycje radiowe, a 34% – audycje nadawane przez głośniki. Żołnierze uznali informacje za wiarygodne: 88% powiedziało, że uwierzyli ulotkom, 46% – audycjom radiowym, a 18% – audycjom nadawanym przez głośniki. Jeńcy mówili także, że na ich decyzje o poddaniu się lub ucieczce miały wpływ przekazane wiadomości. Wzięty do niewoli generał powiedział, że „drugim po bombardowaniu największym zagrożeniem dla morale żołnierzy były ulotki z operacjami psychologicznymi"[55].

D.E. Denning, przedstawiając w swojej książce krótką historię I wojny w Zatoce Perskiej, pokazała kilka rodzajów wojny informacyjnej, takich jak: zakłócenia pracy komputerów, szpiedzy, satelity szpiegowskie, podsłuch, kamery obserwacyjne, broń elektroniczną, fizyczne niszczenie urządzeń komunikacyjnych, fałszowanie dokumentów, manipulowanie percepcją, operacje psychologiczne i wprowadzanie wirusów komputerowych. Jednak autorka

55 D.E. Denning, *Wojna informacyjna...*, dz. cyt., s. 8.

wskazuje, że są jeszcze inne formy wojny informacyjnej (wykradanie tajemnic, wkraczanie w sferę prywatności, fałszowanie poczty elektronicznej), które niekiedy są nieetyczne lub nielegalne, a w pewnych okolicznościach są przestępstwem[56].

Najważniejszym wnioskiem wynikającym z konfliktu nad Zatoką Perską jest konieczność utrzymywania i ciągłego doskonalenia jednostek działań psychologicznych. Przy bardzo niskich kosztach utrzymania osiąga się bardzo dużą efektywność wsparcia operacji wojsk własnych. Fachowe przygotowanie specjalistów, odpowiedni ich dobór oraz szeroki rozmach działań wsparty dostępem do najnowszych osiągnięć technicznych może przynieść wymierne korzyści na polu walki. Świadczy to o tym, że we współczesnych działaniach wojennych niewspółmiernie wzrasta rola informacji, działań psychologicznych i mediów masowych.

Operacje psychologiczne odgrywały zasadniczą rolę w operacjach informacyjnych, a także w innych konfliktach zbrojnych, w tym również z udziałem polskich żołnierzy (np. Irak, Afganistan).

Jednakże kluczowe cele operacji psychologicznych we wszystkich tych konfliktach były podobne. Można do nich zaliczyć osłabienie woli działania i agresywnych zamiarów przeciwnika, wzmocnienie zaangażowania i wsparcia ze strony przyjaznych obiektów oddziaływania oraz pozyskanie poparcia i współpracy ze strony środowisk niezaangażowanych lub niezdecydowanych.

Podsumowując, operacje psychologiczne są jednym z podstawowych składowych szeroko rozumianej walki informacyjnej prowadzonej przez komponent lądowy.

Drugim narzędziem często wykorzystywanym w walce informacyjnej jest dezinformacja.

Ciekawym przykładem dezinformacji jest operacja przeprowadzona przez Karola Schulmeistera, szefa ochrony Bonapartego, który posługując się fałszywymi dokumentami dotarł w 1805 roku do Wiednia, utrzymując, że został wydalony z kraju za szpiegostwo przeciwko Cesarzowi Francuzów. Przekazał on dowództwu armii austriackiej wiadomości, jakie ponoć zebrał o stanie wojsk napoleońskich oraz o nastrojach wśród ludności francuskiej, popierając swoje słowa spreparowanymi wydrukami gazet francuskich z artykułami wymierzonymi w Napoleona oraz sfałszowaną korespondencją przedstawicieli elit francuskich. Plan operacyjny trzeciej koalicji antyfrancuskiej przewidy-

56 Tamże, s. 11.

wał, że Anglia zaatakuje Francję od strony morza, natomiast Austria i Rosja rozbiją siły Napoleona na lądzie. Austria rozpoczęła więc ofensywę na lądzie, nie czekając na Rosjan. Pod Ulm, gdzie stacjonowali Austriacy, doszło do bitwy, przed którą Shulmaistrowi, już jako członkowi austriackiego sztabu, udało się przekonać dowódców austriackich, że mają przed sobą słabe siły francuskie. Tymczasem armia napoleońska oskrzydliła przeciwnika, w międzyczasie Schulmeister zniknął, a Austriakom w obliczu klęski pozostała jedynie kapitulacja[57].

Szczególnie wiele miejsca poświęcono w literaturze działaniom dezinformacyjnym realizowanym podczas drugiej wojny światowej. Działania te prowadziły wszystkie zaangażowane strony. Powszechnie znane i godne uwagi są m.in. plany działań dezinformacyjnych o kryptonimie „Bertram" i „Overlord" jako przykłady kunsztu planowania i realizacji tego typu działań prowadzonych na dużą skalę.

Dezinformacja i maskowanie, ze względu na otwartą, pustynną przestrzeń, miały duże znaczenie w przygotowaniach wojsk alianckich dowodzonych przez gen. Claude'a Auchinlecka do ofensywy w listopadzie 1941 roku („Crusader"), która miała wyprzeć wojska włosko-niemieckie z Egiptu. W trakcie przygotowania przełomowej bitwy pod El-Alamein (Al-Alamajn) w październiku 1942 roku po raz pierwszy opracowano kompleksowy plan dezinformacji o kryptonimie „Bertram", obejmujący też szereg akcji pomocniczych („Diamond", „Brian", „Munassib", „Martello", „Murrayfield" i „Meltingpot"). Celem planu „Bertram" było utrzymywanie przeciwnika w przekonaniu, że alianci nie przygotowują się do ofensywy, a gdy będzie to już niemożliwe do ukrycia – zmylenie co do czasu oraz miejsca ataku. Maskowanie ruchów wojsk oraz masy uzbrojenia, amunicji i wszelkiego rodzaju zaopatrzenia nastręczało wiele trudności. W samym tylko rejonie El-Alamein zgromadzono 2000 ton materiałów pędnych, 600 ton żywności, 400 ton części zamiennych. Natomiast w rejonie El Imayid – 3000 ton paliwa, 600 ton sprzętu technicznego i części zamiennych. Jednak przy pomocy wielkiej liczby różnego rodzaju makiet: czołgów, dział, samochodów ciężarowych, a nawet sztucznych linii rurociągowych, zasugerowano niemieckiemu dowództwu, że główne zgrupowania wojsk znajdują się na południowym skrzydle. Zaskakujące uderzenie

57 *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów*, http://www.defence24.pl/299734,wojna-informacyjna-jako-skuteczne-narzedzie-destabilizacji-panstw-i-rzadow-raport [dostęp: 3.02.2016].

wojsk alianckich, dokonane na północnym odcinku frontu, zakończyło się pełnym powodzeniem. Sukces działań dezinformacyjnych w okresie bitwy pod El Alamein przeszedł najśmielsze oczekiwania, chociaż przyczyniły się też do niego błędy niemieckiego rozpoznania lotniczego i wywiadu. Wzięty do niewoli niemiecki dowódca wojsk pancernych – gen. Wilhelm von Thoma, potwierdził, że największą koncentrację wojsk alianckich stwierdzono na południu, a więc tam, gdzie faktycznie była ona tylko pozorowana.

Ogromnym sukcesem aliantów była dezinformacja towarzysząca lądowaniu aliantów w Normandii. Operacja „Overlord", czyli sforsowanie kanału La Manche i desant wojsk alianckich w Normandii, były najbardziej złożoną i skomplikowaną akcją drugiej wojny światowej. Przygotowania do niej rozpoczęły się dwa lata wcześniej, w kwietniu 1942 roku, gdy w ramach operacji „Bolero" rozpoczęto długofalowy proces przerzutu wojsk amerykańskich do Wielkiej Brytanii. Następnie w lipcu 1943 roku opracowano misterny plan dezinformacji o kryptonimie „Jael", który pod koniec roku przemianowano na „Bodyguard". Jego celem było zdezorientowanie Hitlera i podsunięcie mu mylących informacji o zamiarach aliantów. „Bodyguard" podzielono na 39 planów, które rozpracowano na setki przedsięwzięć pozoracyjno-dezinformacyjnych.

Prawdziwym sukcesem radzieckiej dezinformacji w czasie tej wojny były działania przeprowadzone w czasie bitwy o Stalingrad. Podczas gdy Niemcy starali się jesienią i zimą 1942 roku opanować miasto, Rosjanie udawali przygotowania do ofensywy zimowej w centrum teatru pod Moskwą. W połączeniu z upartą obroną Stalingradu dało to Niemcom fałszywe poczucie bezpieczeństwa i przekonanie, że Rosjanie nie zamierzają atakować ich skrzydeł na południowym teatrze działań. Radziecka dezinformacja umożliwiła zamaskowanie ruchu i koncentracji 300 tys. żołnierzy, 1 tys. czołgów i 5 tys. dział, co doprowadziło do okrążenia niemieckiej 6 Armii pod Stalingradem. Warto zauważyć, że umiejętne radzieckie maskowanie było na tyle skuteczne, że Niemcy wysłali 12 dywizji do Grupy Armii „Środek", choć początkowo były one przeznaczone do wsparcia ich walk pod Stalingradem i na Kaukazie.

Dezinformacja była stosowana również podczas wojen w Zatoce Perskiej. Powszechnie znany jest fakt z czasów I wojny w Zatoce Perskiej, gdy sprzymierzeni uszkodzili irackie wojskowe systemy komputerowe za pomocą wirusa komputerowego, który trafił do Iraku w drukarkach. Fakt ten został szczegółowo przedstawiony w telewizyjnym programie sieci ABC pt. *Nightline*. Poprzedziła go informacja w *US News & World Report*. Według autorów programu rząd Stanów Zjednoczonych za cel działania wirusa obrał iracką obronę powietrzną. Kilka tygodni przed operacją „Pustynna Burza" zarażony

wirusem chip komputerowy zainstalowano w drukarce igłowej, którą montowano we Francji i wysłano do Iraku przez Amman w Jordanii. Wirus ten według opinii ekspertów powstał w Narodowej Agencji Bezpieczeństwa (NSA), a zainstalowała go Centralna Agencja Wywiadowcza (CIA). W efekcie pracy wirus unieruchomił prawdopodobnie system operacyjny Windows i główne komputery sterujące działaniem systemów obrony powietrznej[58]. W tym przypadku manipulacji poddano system komputerowy, zmieniając jego właściwości i czyniąc bezużytecznym w dalszej eksploatacji.

Równie ważne było to, że siły koalicji przez manipulację częstotliwością fal elektromagnetycznych zneutralizowały lub zniszczyły najważniejsze systemy informacyjne Iraku. Antyradiacyjne pociski wystrzelone z helikopterów i samolotów w pierwszych chwilach operacji „Pustynna Burza" obezwładniły iracką sieć obrony powietrznej. Wstążki z włókna węglowego uwalniane z pocisków Tomahawk nad irackimi rozdzielniami energetycznymi powodowały zwarcia, przejściowe zakłócenia i wyłączenie znacznych fragmentów sieci energetycznych.

Kolejnym ciekawym przykładem dezinformacji z tej wojny jest wyciek do prasy planów inwazji amerykańskiej.

Opracowany przez gen. Schwarzkopfa plan ataku przewidywał długotrwałe uderzenie lotnicze, po którym miała przyjść faza lądowa. W czasie 42 dób pierwszego etapu zadano ogromne straty infrastrukturze cywilnej państwa, w tym transportowej, ośrodkom kierowania i dowodzenia, obiektom stacjonarnym sił zbrojnych, wreszcie wojskom operacyjnym. Plany dotyczące ataku lądowego były utrzymywanie w ścisłej tajemnicy. Jednak tuż przed przyjętym terminem „Newsweek" wydrukował mapę, która prawie bezbłędnie odtwarzała zamierzenia amerykańskich sztabów. Schwarzkopf był przerażony. Ówczesny przewodniczący Kolegium Połączonych Szefów Sztabów Sił Zbrojnych Stanów Zjednoczonych – gen. Colin Powell – uspokajał go, pokazując dziesiątki innych map publikowanych przez gorzej poinformowane gazety. Stwierdził, że to plotki, które zadziałają na korzyść Amerykanów. Z szumu informacyjnego nie da się bowiem wyłowić żadnych wiarygodnych danych. Zresztą nawet ta historia nie musi być prawdziwa[59].

58 Zob. D. E. Denning, *Wojna...*, dz. cyt.

59 J. Wiśnicki, *Ochrona wojsk w operacji*, „Raport, Wojsko, Technika, Obronność" 2014, nr 7, s. 56–57.

Strona iracka też stosowała dezinformację, wykorzystując do tego przede wszystkim makiety sprzętu bojowego. Działania lotnictwa amerykańskiego trwały dłużej niż zakładało naczelne dowództwo. Przyczynami takiego stanu rzeczy były zarówno złe warunki atmosferyczne, jak i prowadzone przez Irakijczyków działania mające na celu zamaskowanie i ukrycie pozycji. Część bomb i rakiet spadła na umiejętnie przygotowane makiety czołgów i pojazdów, część czołgów i stanowisk artylerii była dobrze okopana i przemyślnie ukryta, a przez to trudna do zlokalizowania z powietrza. W dodatku wojska irackie podpaliły ropę wlaną do rowów przeciwczołgowych, a silny gryzący dym znacznie utrudnił pilotom identyfikację celów, wiele ataków było więc niedokładnych. Jednak mimo tych wszystkich przeszkód zmasowane naloty sił sojuszu coraz bardziej dawały się we znaki wojskom irackim i zadawały im potężne straty.

Już w okresie przygotowawczym do II wojny w Iraku możemy zaobserwować wykorzystanie dezinformacji jako narzędzia walki informacyjnej przez Amerykanów. Długo po tym, jak okazało się, że front północny nie zostanie otwarty z powodu nieuzyskania zgody od rządu Turcji na przegrupowanie przez terytorium tego państwa wojsk amerykańskich (wiedzieli o tym o wiele wcześniej niż zostało to oficjalnie ogłoszone), Amerykanie utrzymywali całą dywizję w tym samym rejonie. Uważali, że przez walkę informacyjną mogą wpływać na reżim Husajna, wprowadzając w błąd wywiad przeciwnika co do swoich zamiarów. Chcieli, aby władze irackie uważały, że wprowadzenie tych sił od północy jest możliwe, a nawet wielce prawdopodobne oraz, że zgoda Turcji to tylko kwestia czasu. Dążyli do stworzenia atmosfery niepewności w umysłach dowódców i planistów irackich. Dzięki temu 13 dywizji irackich było utrzymywanych w północnej części Iraku w gotowości do odparcia ewentualnych działań zaczepnych z tego kierunku. W ten sposób uniemożliwiono użycie tych znacznych sił na kierunku południowym. Dodatkowo umożliwiło to dokładne rozpoznanie rozmieszczenia tych dywizji. Kiedy rozpoczynały jakikolwiek ruch, stawały się obiektami rażenia sił powietrznych[60].

Była to typowa dezinformacja, która doprowadziła do tego, że znaczne siły irackie w pierwszych dniach działań pozostawały bezużyteczne na północy kraju.

60 J. Joniak, A. Polak, *Wojny w Zatoce Perskiej aspekty operacyjne*, AON, Warszawa 2011, s. 38.

2.3. Rosyjska wojna informacyjna XXI wieku

Rosja definiuje wojnę informacyjną jako oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, które mogą być stosowane jako swoista broń informacyjna. Działania te skierowane są nie tylko przeciw siłom zbrojnym, ale przede wszystkim ukierunkowane są na całe społeczeństwo oraz jego świadomość, a także na aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomikę danego państwa. Wojna informacyjna może mieć na celu przygotowanie, w założonej perspektywie czasowej, zbrojnej interwencji mogącej mieć charakter typowych działań wojennych między państwami, bądź też realizowanej jako wojna hybrydowa[61]. Takie podejście do wojny informacyjnej mogliśmy zaobserwować przed zajęciem Krymu, gdy Rosjanie przez media przygotowywali sobie grunt do swoich późniejszych działań.

W 2000 roku wydano oficjalny dokument pt. *Doktryna Bezpieczeństwa Informacyjnego Federacji Rosyjskiej*, określający podstawowe cele, koncepcje działania, szanse i zagrożenia państwa rosyjskiego w sferze informacji. Władze Rosji traktują przede wszystkim bezpieczeństwo informacyjne, w tym bezpieczeństwo w cyberprzestrzeni, jako podstawę całego bezpieczeństwa państwa, jak również jako podstawowe narzędzie do osiągania celów politycznych. Bardzo charakterystyczne jest to, że z punktu widzenia władz rosyjskich walkę informacyjną powinno się stosować przede wszystkim w celu osiągnięcia efektu psychologicznego.

Taka taktyka i takie podejście nie jest niczym nowym i ma w Rosji bardzo długą tradycję. Istnieje nawet specjalny termin w języku rosyjskim na określenie tego typu działań – *maskirovka*, który można przetłumaczyć jako oszustwo, podstęp, manipulacje. *Maskirovka* była, jest i będzie stosowana przez władze rosyjskie, gdyż stanowi niezwykle efektywne narzędzie oddziaływania szczególnie na zagraniczną opinię publiczną (a także na własne społeczeństwo). Należy podkreślić, że walka informacyjna polegająca na manipulacji, propagandzie i dezinformacji nie narodziła się wraz z powstaniem Internetu. Cyberprzestrzeń dała po prostu nowe, bardzo efektywne metody stosowania tych działań. Wracając do *Doktryny*, jako jedno z największych zagrożeń dla bezpieczeństwa informacyjnego Rosji wskazano wpływ podmiotów

61 *Wojna informacyjna jako skuteczne...*, dz. cyt.

zagranicznych, w tym mediów zagranicznych, które dążą do niekorzystnego przedstawiania wizerunku Rosji i działań podejmowanych przez to państwo. Przed takim zagrożeniem władze rosyjskie przestrzegają i zamierzają się bronić. W tym kontekście Rosjanie mogą stosować defensywne, jak i ofensywne metody walki informacyjnej, także w cyberprzestrzeni. Wykorzystanie tzw. trolli (prowokatorów internetowych), czy ujawnianie tajnych rozmów między decydentami mogą być doskonałymi przykładami takich metod.

Poza odniesieniem się do oficjalnych koncepcji i strategii działań rosyjskich, należy także przywołać doświadczenia z niedalekiej przeszłości. Powszechnie znane są wydarzenia, jakie miały miejsce podczas konfliktu w Gruzji czy w Estonii. Powiedzieć należy, że nigdy ostatecznie nie udowodniono winy rosyjskiej w ich kontekście, jednak ogólne przekonanie jest takie, że to właśnie Rosjanie stali za cyberatakami, jakie miały miejsce w tych państwach. To pozwala sądzić, że Rosjanie będą aktywni w cyberprzestrzeni także podczas konfliktu z Ukrainą.

Paleta możliwości działania w cyberprzestrzeni jest bardzo szeroka, nie da się więc wymienić wszystkich sposobów działania z uwagi na ich olbrzymi potencjał i różnorodność. W tym przypadku chodzi raczej o pokazanie pewnego mechanizmu. Wspomniane ujawnienie rozmów zachodnich dyplomatów, którzy mówili o trudnej sytuacji na Ukrainie i podawali informacje o tym, że snajperzy oddawali strzały do demonstrujących oraz władz, mogą być stosowane w celu negatywnego oddziaływania na wizerunek liderów. Oczywiście efektem ma być tutaj ich dyskredytacja (zarówno w oczach zagranicznej opinii publicznej, jak i społeczeństwa Ukrainy), podważenie zaufania, wzbudzenie niepokoju. Cyberprzestrzeń jest doskonałym narzędziem do prowadzenia tego typu działań.

Jednocześnie walka informacyjna w cyberprzestrzeni poza celami psychologicznymi może spełniać także inne funkcje. Można skierować ją nie tyle na samą treść informacji i jej zniekształcanie, ale na komunikację *sensu stricto* oraz na przekazywanie informacji. Przykładem są doniesienia medialne o zablokowaniu telefonów komórkowych członków ukraińskiego parlamentu. System telekomunikacyjny został rzekomo zaatakowany przez armię rosyjską. Może mieć miejsce kontrola przepływu informacji, utrudnianie dostępu do stron internetowych oraz portali społecznościowych (często używanych do działań organizacyjnych).

W skrajnej formie cyberataki mogą zostać użyte do uszkodzenia czy też sparaliżowania elementów ukraińskiej infrastruktury, także krytycznej. Informacja o pojawieniu się wirusa *Snake*, który prawdopodobnie daje możliwość

przejęcia pełnej kontroli nad atakowanym systemem, może być spełnieniem tego czarnego scenariusza. W końcu, jeśli dojdzie do otwartego konfliktu militarnego, ataki mogą zostać skierowane na systemy teleinformatyczne armii ukraińskiej. Konsekwencje tych działań mogą być dużo poważniejsze niż te, jakie niesie za sobą walka psychologiczna.

Obecny kryzys na Ukrainie stał się największym rosyjskim polem cyberwojny od czasów cyberataków na Estonię w 2007 i Gruzję w 2008 roku.

Początek wojny informacyjnej przeciwko Ukrainie na przełomie 2003 i 2004 roku miał na celu powstrzymanie „pomarańczowej dżumy" zagrażającej koncepcji geopolitycznej budowy Eurazji. Celem tymczasowym było wsparcie obozu Janukowycza, aż do jego zwycięstwa w wyborach prezydenckich w 2010 roku.

Wojnę informacyjną na pełną skalę Rosjanie zastosowali podczas Euromajdanu w Kijowie. Celem wojny informacyjnej wymierzonej w Ukrainę było zdestabilizowanie państwa ukraińskiego. Główny ciężar walki spoczywał na dywersji ideologicznej, politycznej i socjokulturowej. Głównym adresatem oddziaływań była ludność Krymu i wschodniej Ukrainy. Ofiarami wojny informacyjnej stała się najpierw ludność Krymu, potem wschodniej Ukrainy, a następnie społeczeństwo rosyjskie. Analiza wydarzeń na Krymie potwierdziła zastosowanie przez Rosję elementów wojny w cyberprzestrzeni, które z powodzeniem i w coraz większym stopniu towarzyszą rosyjskim działaniom konwencjonalnym.

Pierwsze cyberataki za pomocą DDoS (*Distributed Denial of Service*), których autorem z bardzo dużym prawdopodobieństwem była rosyjska agenda informatyczna *Russian Business Network,* odnotowano w Estonii (2007) i w Gruzji (2008). Celem tych ataków było przede wszystkim zablokowanie usług internetowych, takich jak np. usługi bankowe oraz sparaliżowanie systemu informatycznego administracji państwowej.

W dniu 9 marca 2014 roku dokonano cyberataku na ukraińskie systemy teleinformatyczne, w którym posłużono się najbardziej zaawansowanymi atakami z grupy APT (*Advanced Persistent Threat).* Atak tego typu łączy w sobie różne narzędzia: socjotechniczne, programistyczne itp. Ataki te przeprowadzają zazwyczaj zorganizowane grupy dysponujące znacznym budżetem oraz czasem pozwalającym na zinfiltrowanie konkretnego celu ataku (instytucji, firmy), a następnie precyzyjnego przeprowadzenia ataku, którego celem może być kradzież strategicznych informacji lub uszkodzenie (zniszczenie) systemu komputerowego.

Do tej pory w rządowych ukraińskich systemach informatycznych wykryto szereg mniej groźnych tzw. robaków i przede wszystkim bardzo groźnego wirusa *Snake*, którego funkcja nie jest jeszcze do końca znana, ponieważ jest on zdolny m.in. do hibernacji i pozostawania całkowicie nieaktywnym przez długi okres, co bardzo utrudnia jego wykrycie. Uważa się, że *Snake* został zaimplementowany przed laty i był wykorzystywany do tej pory jako narzędzie szpiegowskie, by w marcu 2014 roku posłużyć m.in. do zaburzenia pracy systemów informatycznych, kradzieży informacji, blokowania oraz zagłuszania ukraińskich telefonów rządowych.

Według danych podanych przez brytyjski koncern zbrojeniowy *BAE System*, zajmujący się również zagadnieniami bezpieczeństwa cybernetycznego, *Snake* po raz pierwszy pojawił się w 2006 roku. Jednak od roku 2013 zachowuje się coraz agresywniej. Do tej pory odnotowano 58 przypadków działania tego wirusa, z czego aż 44 w 2013 roku. Zdaniem ekspertów *BAE Systems*, *Snake* bardzo przypomina strukturę wirusa *Stuxnet*, który zaatakował irańskie placówki nuklearne. Potwierdzają oni również, że *Snake* jest najprawdopodobniej produktem rosyjskim wspomnianej już wcześniej agendy informatycznej *Russian Business Network,* ponieważ jego operatorzy działają według czasu moskiewskiego, a w kodzie wirusa znaleziono fragmenty tekstu po rosyjsku.

Według ekspertów INSS[62] Rosji udało się przejąć kontrolę niemal nad wszystkimi ukraińskimi stronami rządowymi oraz monitorować łącza internetowe i linie telefoniczne jeszcze przed zajęciem Krymu. Z kolei rosyjskie siły specjalne fizycznie zniszczyły wszystkie istotne systemy łączności ostatecznie odcinając półwysep od Ukrainy.

Jak wiadomo cyberszpiegostwo jest integralną częścią strategii wojskowej i polityki zagranicznej Rosji wobec m.in. krajów byłego Związku Radzieckiego. Eksperci z INSS podają, że Rosja posiada znaczne możliwości dostępu do systemów dyplomatycznych, rządowych i wojskowych od czasów upadku ZSRR. Daje jej to ogromną przewagę w przewidywaniu taktyki i możliwych działań swoich sąsiadów.

BBC donosiła, że największy wojskowy cyberatak został zrealizowany przez rosyjskie GRU na siłach zbrojnych Ukrainy. Według ukraińskich organów ścigania ataki te spowodowały zerwanie łączy komunikacyjnych niemal wszystkich sił ukraińskich. Cyberataki zostały również skierowane na rządowe strony internetowe oraz serwisy społecznościowe. Analogiczny zestaw działań

62 *Institute for National Security Studies.*

miał miejsce w czasie wojny z Gruzją, co według ekspertów z INSS świadczy o starannym zaplanowaniu z góry operacji na Krymie. Szef Służby Bezpieczeństwa Ukrainy, Wałentyn Naływajczenko, przyznał, że zneutralizowano systemy łączności członków ukraińskiego rządu oraz zakłócono komunikację między agencjami rządowymi.

Były oficer CIA, Marty Martin, uważa, że Rosjanie mogą przeprowadzić dużo ostrzejsze ataki cybernetyczne w przypadku eskalacji obecnego konfliktu. Jednak zdaniem ekspertów nikt na świecie (w tym CIA) nie jest w stanie ocenić rzeczywistych możliwości Rosji w kwestii prowadzenia cyberwojny. Dla zachodnich agencji wywiadowczych dużym problemem pozostaje identyfikacja przyjaciel–wróg, ponieważ zarówno Rosjanie, jak i Ukraińcy posługują się bardzo podobnym językiem i często dokonują ataków z podobnych adresów IP.

Według dyrektora firmy *CrowdStrike*, zajmującej się cyberbezpieczeństwem, Dmitrija Alperowicza, na Ukrainie nie zaobserwowano dużej ilości cyberataków i kontroli cyberprzestrzeni podczas kryzysu krymskiego. Alperowicz zauważa również, że pomimo, iż zarówno ukraińscy, jak i rosyjscy hakerzy posiadają podobne umiejętności, to różnica w ich zapleczach technologicznych jest ogromna.

Rosjanie w czasie przeprowadzania cyberataków na Ukrainie wykorzystali doświadczenia zdobyte podczas wcześniejszych ataków na Estonię i Gruzję, ale nie uniknęli pozostawienia „odcisków palców" prowadzących do rosyjskich źródeł. Jednak dzisiejsze wojny cybernetyczne wyraźnie różnią się od klasycznych konfliktów, co zdecydowanie ogranicza możliwości reagowania. Brak skutecznych międzynarodowych narzędzi prawnych oraz doktryny cyberbezpieczeństwa może doprowadzić nawet do konieczności fizycznej konfrontacji[63].

Warto podkreślić, że działaniom wojskowym od samego początku konfliktu towarzyszy otwarta wojna psychologiczno-informacyjna. Media zasypywane są informacjami mającymi wywołać efekt tzw. szumu informacyjnego, który w konsekwencji doprowadza do całkowitej dezinformacji. Wszelkie niejasności w kwestii aktualnego stanu posiadania i podejmowanych działań obie strony tłumaczą na swoją korzyść, przy czym częściej potwierdzenie znajdują informacje ukraińskie. Najbardziej jaskrawym przykładem celowej dezinformacji stanowiło przekazanie 3 marca 2014 roku przez Interfaks-Ukraina

63 *Ukraina polem cyberwojny: warunki dyktuje Moskwa*, http://www.defence24.pl [dostęp: 19.01.2015].

(z powołaniem się na źródło w ukraińskim resorcie obrony) informacji o ultimatum wystosowanym przez dowództwo Floty Czarnomorskiej do blokowanych na Krymie jednostek armii ukraińskiej. Zgodnie z ultimatum, jeśli do godziny 5 rano 4 marca jednostki te by się nie poddały, jednostki rosyjskie miały rozpocząć szturm na wszystkie obiekty znajdujące się pod ich kontrolą. Informacja ta została zdementowana przez stronę rosyjską. Nie można wykluczyć, że wpłynęło to na stanowiska stron w trakcie debaty w Radzie Bezpieczeństwa ONZ, mającej miejsce również 3 marca 2014 roku.

Pierwszą ofiarą wojny jest zawsze prawda. Doskonale można to zaobserwować na przykładzie Ukrainy, gdzie obiektywne sprawozdanie czy reportaż jest prawdziwą rzadkością.

Potwierdza to sytuacja, jaka miała miejsce w położonym na wschodzie Ukrainy miasteczku Ługańsk. Strona rosyjska przedstawiła wydarzenia w następujący sposób: w jednym z parków leżą porozrzucane, metalowe odpryski. Premier separatystycznej Ługańskiej Republiki Ludowej, Wasilij Nikitin oraz pewien dziennikarz zbierają je z ziemi i uważnie oglądają. „Zostały znalezione niedaleko poplamionego krwią samochodu" – mówi Nikitin. Dla niego jest to dowód na użycie przez ukraińską armię w walce przeciwko separatystom bomb rozpryskowych. „Zginęło osiem osób" – dodaje. Państwowa telewizja podaje natomiast zupełnie inną wersję wydarzeń, twierdząc, że miał miejsce wypadek. Według niej to separatyści odpalili rakietę na ukraiński samolot i przypadkowo uderzyli w budynek miejscowej administracji, będącej w rękach rebeliantów. Rodion Mirosznik, dziennikarz pracujący od dwudziestu pięciu lat dla regionalnej stacji telewizyjnej obwodu ługańskiego mówi, że to czysta propaganda: „Wypadek! To oczywiste kłamstwo! Dziś na Ukrainie to norma" – komentuje.

Dostęp do rzetelnych informacji dotyczących konfliktu graniczy na Ukrainie z cudem. Największa stacja informacyjna, 5 Kanał TV, należy do wybranego na prezydenta biznesmena i miliardera Petra Poroszenki. Także inne ponadregionalne stacje informacyjne są w prywatnych rękach. Według Mirosznika wiele z nich jest stronniczych, ponieważ nie dopuszczają do głosu rebeliantów. Twierdzi również, że jego szefowie w Kijowie próbują wywierać wpływ na sposób relacjonowania wydarzeń na Ukrainie: nakazuje się im nazywanie bojowników „separatystami" lub „terrorystami", w żadnym wypadku nie „bojownikami o wolność". Mimo to jego praca nie spotyka się z negatywnym odzewem ze strony mieszkańców Ługańska, których doprowadzają do szału korespondenci państwowych rozgłośni: „Ludzie na nich wrzeszczą, zdarzają się nawet pobicia" – mówi Mirosznik. Niektóre stacje zmuszone są

nawet do wycofywania swoich korespondentów: „Nie powinno tak być, ale to rezultat propagandy. Ludzie orientują się, że to, co pokazuje telewizja, nie ma nic wspólnego z prawdą" – dodaje.

Lidiya Huzhva, która jest reżyserką, ale podczas rewolucji z własnej inicjatywy, bez wynagrodzenia, filmowała na małej kamerze i puszczała w obieg za pośrednictwem Internetu to, co działo się na Majdanie, Krymie, na wschodzie Ukrainy, ma inne zdanie. Mimo niebezpieczeństwa towarzyszy jednostce ukraińskiej armii jako reporterka. Nie przeszkadza jej, że staje po stronie rządu w Kijowie. „Jesteśmy jak Fox News. Mam swoje zdanie i je wypowiadam. Nie twierdzę, że mam monopol na prawdę" – tłumaczy. Dowodzi, że najwięcej propagandy można znaleźć w rosyjskich mediach: „Ostatnio pokazywano zdjęcie zabitego chłopca, rzekomo ofiary ataku sił rządowych. W rzeczywistości fotografia została zrobiona w Syrii przed dwoma laty" – mówi Huzhva. Według niej manipulacja rosyjskich mediów miała miejsce również w przypadku zdjęcia Tatarów krymskich, którzy stali w kolejce przed lokalami wyborczymi podczas referendum rozstrzygającym o statusie Krymu. „Czysta propaganda" – mówi. I dodaje: „Byłam tam. To była grupa trzydziestu Tatarów wysłanych z jednego lokalu do drugiego, by pokazać, jak Tatarzy wspierali referendum".

Lidiya Huzhva mówi jeszcze, że od czasu rewolucji na Majdanie ukraińskie dziennikarstwo stało się wiarygodniejsze. Kiedy chodzi o interpretację wydarzeń, dziennikarze poruszają się na cienkiej granicy między legitymizacją, a dyskredytacją różnych punktów widzenia. Ukraińscy dziennikarze po obu stronach barykady uwięzieni są w okowach wojny informacyjnej[64].

Kolejnym ciekawym przykładem walki informacyjnej prowadzonej za pośrednictwem mediów jest sposób przedstawiania wizyty prezydenta Ukrainy Petra Poroszenki w Polsce. Według rosyjskich mediów Polacy manifestowali przeciwko wizycie ukraińskiej głowy państwa. Rzecz w tym, że *news* od początku do końca został ukartowany na potrzeby wewnętrznej propagandy.

„W Warszawie przed gmachem Sejmu odbywa się demonstracja protestacyjna przeciwko wizycie Poroszenki" – czytamy na stronie internetowej agencji informacyjnej Ria Novosti. Z kolei depesza agencji ITAR-TASS opisuje, jak rzekome tłumy manifestantów wyrażały sprzeciw wobec polityki Poroszenki, którego uważają za głównego winowajcę śmierci tysięcy ludzi na Ukrainie, a także destabilizacji tego państwa. Agencja przytacza ich komentarze, jakoby

64 *Wojna informacyjna na Ukrainie*, http://www.rp.pl/artykul/1117754.html [dostęp: 18.01.2015].

nie życzyli sobie jego obecności w naszym kraju, ponieważ jest tu *persona non grata*.

Taką wersję wydarzeń powieliło kilka innych rosyjskich mediów, wszystkie zbiegły się w czasie z wizytą prezydenta Poroszenki w Polsce. Rzecz w tym, że zdjęcia ilustrujące wspomniane publikacje – widzimy na nich tłumy ludzi z polskimi flagami – ukazują członków marszu zorganizowanego 13 grudnia 2014 roku przez Prawo i Sprawiedliwość. Zdjęcie pochodzi z twitterowego konta Ewy Kędzierskiej, byłej sekretarz Parlamentarnego Zespołu na rzecz Tybetu. Natomiast w tekście Ria Novosti sytuacja jest jeszcze bardziej kuriozalna, bowiem zamieszczona fotografia przedstawia uczestników Marszu Niepodległości z 11 listopada 2013 roku. Tyle, że nawet tutaj nie są oni pod Sejmem, a na Placu Unii Lubelskiej, co zresztą jest widoczne w podpisie zdjęcia.

ВЕСЬ МИР

0

Жители Варшавы протестуют против визита Порошенко в Польшу

Поляки вышли на митинг к зданию польского парламента, где через некоторое время президент Украины должен выступить с речью

2014/12/17 16:12

Варшава, 17 декабря. Жители Варшавы протестуют против визита президента Украины Петра Порошенко в Польшу, передают СМИ

Поляки вышли на митинг к зданию польского парламента, где через некоторое время Порошенко должен выступить с речью

Źródło: *Polacy protestowali przeciwko wizycie Poroszenki? Rosyjskie media okłamują obywateli*, http://swiat.newsweek.pl [dostęp: 17.12.2014].

Rys. 3. „Protest przeciwko wizycie Poroszenki w Polsce"

Fakty są jednak inne. Otóż pod Sejmem w czasie wizyty Poroszenki rzeczywiście pojawili się manifestanci. Jednak nie stawili się w tysiącach czy nawet setkach, a w grupie zaledwie kilkunastu osób związanych z Obozem Wielkiej Polski. Na filmie z tej demonstracji widzimy, że zebrani mają ze sobą flagę Polski i samozwańczych ukraińskich republik, a także flagę syryjską i sztandar w barwach tzw. wstążki gieorgijewskiej (to jeden z symboli rebeliantów na Ukrainie). Przez megafon wygłaszają też przemówienia nieprzychylne prezydentowi Poroszence.

Propaganda ta ma służyć najprawdopodobniej pokazaniu Rosjanom, że obywatele Zachodu wcale nie odwracają się od nich i od Rosji, a wręcz ich popierają. To rządy i politycy zachodni są kreowane w przekazach prokremlowskich mediów na wrogich Federacji[65].

Zdaniem analityków Rządowego Centrum Bezpieczeństwa, Rosja przekształca realny konflikt ukraińsko-rosyjski w konflikt ideologiczny z Zachodem.

W rosyjskiej teorii i praktyce oddziaływania informacyjnego nagminnie wykorzystywana jest retoryka socjotechniki. Socjotechnice służy aparat pojęciowy. Zawiera on mnóstwo pojęć w rodzaju „broń informacyjna", „broń cywilizacyjna", „informacyjny specnaz", „informacyjne wojska", „wojna informacyjna" (a także: psychologiczna, ideologiczna, cywilizacyjna, jądrowa, tj. rozważania o możliwościach użycia taktycznej broni jądrowej przeciwko Ukrainie, Europie, Ameryce itp.). Te zmilitaryzowane pojęcia kształtują postawy konfrontacyjne oraz narzucają własnej i światowej opinii kremlowski zmanipulowany obraz świata: „Zachód wydał Rosji wojnę informacyjną"; „Przedstawia Rosjan jako agresorów, tymczasem na Ukrainie trwają czystki etniczne Rosjan".

Eksperci i politolodzy próbują uchwycić główne cechy tej wojny na przykładzie agresji informacyjnej przeciwko Ukrainie, dostosowując je do istniejących teorii wojen oraz próbując określić jej fronty i główne parametry. Wyodrębniają oni cechy informacyjnej agresji Rosji, takie jak brak jednej linii frontu, przestrzeń informacyjna jako główne pole walki, brak formalnego wypowiedzenia wojny, a także zacieranie różnic między okresem wojny i pokoju, maskowanie celów i oficjalnego zaangażowania militarnego, angażowanie do walki szerokich grup społeczeństwa.

65 *Polacy protestowali przeciwko wizycie Poroszenki? Rosyjskie media okłamują obywateli*, http://swiat.newsweek.pl [dostęp: 17.12.2014].

Rosyjski teoretyk Siergiej Rastorgujew z Instytutu Problemów Bezpieczeństwa Informacyjnego Uniwersytetu Łomonosowa w wywiadzie dla tygodnika „Litieraturnaja Gazieta" (23.10.2013) zrównał cele wojny informacyjnej i innych rodzajów wojen: wszystkie toczą się o zasoby innych państw (w przypadku wojen informacyjnych – o zasoby społeczne). „Kluczem do tych zasobów są elity i media przeciwnika. Ważnym czynnikiem jest posiadanie wśród tych elit i mediów niezbędnej masy agentów wpływu, których agresor rekrutuje spośród osób o egoistycznym bądź niewolniczym światopoglądzie". Autor zwraca uwagę, że „strategia wojny informacyjnej zawsze łączy mnóstwo powiązanych wzajemnie taktycznych operacji informacyjnych. Globalny cel tych operacji nie zawsze jest widoczny"[66].

Podsumowując, współczesna walka informacyjna uwarunkowana jest szeregiem czynników mających zasadniczy wpływ na jej planowanie, organizowanie i prowadzenie. Do najważniejszych czynników należy: globalizacja, prowadzenie działań zgodnie z koncepcją sieciocentryczności oraz asymetria współczesnego świata przejawiająca się nowymi zagrożeniami oraz nowym, często trudnym do ustalenia przeciwnikiem, zwanym przeciwnikiem asymetrycznym.

Zmieniająca się sytuacja bezpieczeństwa globalnego spowodowała zmianę nastawienia opinii światowej z oczekiwanej konfrontacji supermocarstw w kierunku bardziej kompleksowych interakcji poszczególnych państw i innych uczestników konfliktu. Globalizacja i zmagania o źródła surowców w połączeniu z ideologicznymi, religijnymi i kulturowymi różnicami przyczyniają się do zachwiania równowagi sił, w wyniku czego następuje wzrost zagrożenia stanu bezpieczeństwa, wpływając na destabilizację wielu rejonów świata. Jednocześnie dokonuje się rewolucja informacyjna otwierająca nową epokę narzędzi informatycznych, wspierających procesy decyzyjne, do których zalicza się powszechny już Internet i telefonię komórkową. To stosunkowo nowe środowisko informacyjne obejmuje swoim zakresem wszelkie informacje, użytkowników i systemy umożliwiające przetwarzanie danych. Do kategorii użytkowników środowiska informacyjnego zalicza się liderów i decydentów, jak również pojedynczych uczestników, a także całe organizacje i ich struktury. Systemy informacyjne obejmują materiały i urządzenia wykorzystywa-

66 Opracowano na podstawie: J. Darczewska, *Rosja zbroi się do wojny informacyjnej z Zachodem*, Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa, październik–grudzień 2014, nr 9, s. 3–8.

ne do zbierania, przetwarzania i rozpowszechniania informacji. Środowisko informacyjne stanowi zasadniczą przestrzeń procesu decyzyjnego, ponieważ w jego obszarze ludzie i systemy prowadzą obserwację oraz analizę, podejmują decyzje oraz zarządzają informacją.

Kluczowe znaczenie dla rozwoju walki informacyjnej miała I wojna w Zatoce Perskiej. Po zakończeniu tej wojny wiele krajów zaczęło przywiązywać większą uwagę do działań prowadzonych w obszarze walki informacyjnej. Rezultatem prowadzenia walki informacyjnej będzie dezorganizacja funkcjonowania elementów infrastruktury przeciwnika, a w szczególności ośrodków kierowania i dowodzenia, stanowisk startowych rakiet i ogniowych artylerii, lotnisk, portów morskich, systemów łączności i informatyki, składów amunicji itp. Celem będą systemy informacyjne, a w szczególności nośniki danych. Dlatego też tak dużą rolę odgrywa zabezpieczenie własnych systemów przed oddziaływaniem walki informacyjnej prowadzonej przez stronę przeciwną.

Na podstawie analizy literatury można wnioskować, że w nowoczesnych konfliktach zbrojnych pierwszą fazą działań będzie zdobycie panowania w eterze, drugą – wywalczenie i utrzymanie przewagi w powietrzu, a dopiero trzecią fazą prowadzenie działań przez komponent lądowy.

Według innego scenariusza przyszły konflikt zbrojny może przebiegać tylko w dwóch fazach:

– faza I – wywalczenie panowania w eterze,

– faza II – jednoczesne uderzenie powietrzno-lądowe (a więc połączenie w jedną fazę, drugiej i trzeciej fazy pierwszego scenariusza).

Konflikt we wschodniej części Ukrainy pokazał, że Rosja prowadzi walkę informacyjną ukierunkowaną zarówno na społeczeństwo nie tylko ukraińskie oraz innych państw (w szczególności państw zachodnich i byłych republik radzieckich), ale także własne. Celem rosyjskiej wojny informacyjnej jest podporządkowanie elit i społeczeństwa własnego i krajów obcych w sposób dla nich niezauważalny, przy wykorzystaniu tajnych i jawnych kanałów, oddziaływania psychologicznego, neuropsychologicznego, dezinformacji, dywersji ideologicznej i politycznej. Wojna informacyjna jest narzędziem geopolityki stosowanej, a więc metody prowadzenia polityki międzynarodowej, opartej na determinizmie geograficznym. Rosyjska geopolityka stosowana postrzega relacje państw w kategorii konfliktu interesów, nieustannej rywalizacji o wpływy i ekspansję. Walka informacyjna (sieciowa, psychologiczno-informacyjna) umożliwia

osiągnięcie celów w polityce wewnętrznej, międzynarodowej, regionalnej, a także ma zapewnić przewagę geopolityczną.

Konflikt na Ukrainie stał się prawdziwym polem walki informacyjnej, a główną rolę odgrywają w niej media. Konflikt ten ukazał wciąż rosnącą rolę cyberprzestrzeni, która stała się nie mniej ważnym polem toczonej wojny, niż działania prowadzone na lądzie, w wodzie i w powietrzu.

3. Rola i miejsce walki elektronicznej w prowadzeniu walki informacyjnej

Minione wojny wykazały, że w warunkach, w których technika, a w szczególności technika radioelektroniczna, decyduje o efektywności działań wojskowych, aktywne oddziaływanie na nią w celu zmniejszenia stopnia jej sprawności ma kluczowe znaczenie. Wszyscy są świadomi, że prowadzenie walki informacyjnej, a w jej obrębie zakłócanie obiegu informacji, odcięcie dowództwa i sztabu jako organu kierującego od jej źródeł, wprowadzanie do obiegu fałszywych danych lub opóźnianie przepływu wiadomości dezorganizuje pracę systemów dowodzenia do tego stopnia, że wykorzystanie wojsk, uzbrojenia i techniki bojowej może się stać nieskuteczne, opóźnione, a czasem wręcz niemożliwe. Oczywiście w tym aspekcie aktywne, celowe oddziaływanie na czynne środki i systemy dowodzenia wojskami i kierowania środkami walki przeciwnika nabiera priorytetowego znaczenia.

Wprowadzanie do uzbrojenia wojsk nowych, coraz doskonalszych i złożonych systemów radioelektronicznych i środków walki oraz sukcesy w działaniach zbrojnych możliwe do osiągnięcia w rezultacie efektywnej walki elektronicznej stanowią główną przyczynę podjęcia w ostatnich latach, na niespotykaną dotąd skalę, prac naukowo-badawczych i rozwojowych w zakresie techniki walki elektronicznej oraz doskonalenia form i metod jej organizacji oraz prowadzenia podczas działań zbrojnych. Wysiłek badawczy podejmowany jest w niemal wszystkich państwach świata.

Doskonalenie i unowocześnianie współczesnego systemu walki elektronicznej realizuje się według opracowanych programów rozwojowych, niestety w ograniczonym zakresie dotyczy to SZ RP[1].

1 Por. *Priorytetowe zadania modernizacji technicznej sił zbrojnych Rzeczypospolitej Polskiej w ramach programów operacyjnych*, Uchwała Nr 123 Rady Ministrów z dnia 23 czerwca 2014 r., Monitor Polski, poz. 558.

Nowoczesne państwa nieprzerwanie prowadzą systematyczne badania mające na celu techniczne doskonalenie i przyśpieszenie opracowania nowych środków walki elektronicznej oraz wypracowanie najefektywniejszych sposobów ich wykorzystania w walce, z uwzględnieniem zadań i właściwości działań poszczególnych rodzajów sił zbrojnych i rodzajów wojsk[2]. Stale też i coraz intensywniej prowadzone są badania naukowe i prace konstrukcyjno-techniczne. Działalność sztabów nastawiona jest na opracowanie nowoczesnej struktury organizacyjno-funkcjonalnej systemu walki elektronicznej dla całości sił zbrojnych. Tworzone są nowe wyspecjalizowane jednostki walki elektronicznej.

Walka elektroniczna traktowana jest jako integralna część działań zbrojnych, część potencjału militarnego państwa oraz rodzaj działań, który w aktywnej, ofensywnej formie i w bardzo szerokim zakresie rozpoczyna się przed konfliktem, a nasila się z chwilą wybuchu wojny (prowadzenia działań), przed lub równocześnie z wykonaniem zmasowanych uderzeń klasycznymi środkami rażenia. Przestrzeń rozchodzenia się fal elektromagnetycznych należy do wszystkich. Walka elektroniczna nie jest więc ograniczona ani czasem, ani przestrzenią i nie istnieją dla niej żadne granice państwowe, co determinuje jej przydatność w prowadzeniu walki informacyjnej.

3.1. Ogólne cechy walki elektronicznej wpływające na prowadzenie walki informacyjnej

Walka elektroniczna nie zawsze rozpoczyna się z chwilą wybuchu konfliktu zbrojnego lub wytworzenia się na świecie stanu napięcia międzynarodowego i nie kończy się w momencie zakończenia tego konfliktu czy złagodzenia stanu napięcia. W tych okresach zwiększa się jedynie jej zakres i intensywność. Wynika z tego, że walka elektroniczna prowadzona jest również dziś, w czasie pokoju, nieprzerwanie, na różną skalę, z różnym nasileniem, przy zastosowaniu różnych metod i środków. Intensywność przedsięwzięć walki elektronicznej zależy od aktualnej sytuacji politycznej i militarnej we współczesnym świecie.

2 Por. K. Dymanowski, *Zmiany w koncepcji walki elektronicznej NATO*, „Przegląd Sił Powietrznych" 2009, nr 11.

Walka elektroniczna w okresie pokoju ma charakter pasywny. Jej wysiłek skierowany jest przede wszystkim na wykonanie rozpoznania elektronicznego (w terminologii anglojęzycznej nazywanego zwiadem elektronicznym), rozpoznania środków, obiektów i systemów radioelektronicznych przeciwnika oraz na przygotowanie własnych sił zbrojnych do prowadzenia aktywnych działań radioelektronicznych na wypadek powstania konfliktu zbrojnego.

W założeniach doktrynalnych wiodących państw NATO podkreśla się, że dokładne dane o środkach i systemach radioelektronicznych przeciwnika zawsze należy zdobywać wszelkimi dostępnymi sposobami i środkami. Dewiza ta w praktyce realizowana jest od zakończenia drugiej wojny światowej, często z naruszeniem suwerenności państwowej i nieliczeniem się z prowokacyjnym i niebezpiecznym dla pokoju charakterem tych przedsięwzięć.

W okresie wojny, w toku działań zbrojnych, walka elektroniczna ma wybitnie aktywny i ofensywny charakter. Obejmuje rozpoznanie oraz obezwładnianie środków i obiektów radioelektronicznych ogniem i zakłóceniami. Traktowana jest jako zorganizowane starcie zbrojne z techniką radioelektroniczną przeciwnika, która znajduje zastosowanie na obszarze jego państwa w systemach rozpoznania, zarządzania i kierowania, powiadamiania i ostrzegania, jak również z tą jego techniką, która wykorzystywana jest na obszarze działań zbrojnych, w systemach dowodzenia wojskami i kierowania środkami walki poszczególnych rodzajów sił zbrojnych i rodzajów wojsk.

Wysokie wartości techniczne nowoczesnych środków rozpoznania, dywersji i zakłóceń elektronicznych oraz bardzo duże nasycenie nimi wojsk sprawiają, że walka elektroniczna prowadzona podczas działań zbrojnych charakteryzuje się zdecydowanym, aktywnym, ofensywnym i zmasowanym oddziaływaniem radioelektronicznym na różne systemy dowodzenia wojskami i kierowania środkami walki. Cechuje ją również rozmach przestrzenny, znaczne głębokości rozpoznania i obezwładniania elektronicznego oraz możliwość wykonania zmasowanych i ściśle zsynchronizowanych z ogniowymi uderzeń radioelektronicznych.

Wymienione założenia znajdują odbicie w obowiązujących w siłach zbrojnych NATO zasadach taktyki prowadzenia aktywnych działań elektronicznych. Wypracowano je w ciągu ostatnich kilkudziesięciu lat i poddano wszechstronnym praktycznym próbom. Przewiduje się, że w czasie wojny aktywne i ofensywne działania będą prowadzone kompleksowo, w sposób skoordynowany, wszystkimi dostępnymi środkami elektronicznymi, w skali strategicznej, operacyjnej i taktycznej. Dla osiągnięcia celów strategicznych wykonywane będą zadania w zakresie wywiadu i rozpoznania elektronicznego

oraz obezwładniania zakłóceniami środków i systemów radioelektronicznych obrony powietrznej, kierowania środkami walki, radionawigacji dalekiego i bliskiego zasięgu, jak również łączności państwowej i sił zbrojnych strategiczno-operacyjnego przeznaczenia.

Osiągnięcie celów operacyjnych i taktycznych można uzyskać przez stałe i intensywne rozpoznawanie oraz obezwładnianie zakłóceniami środków wykorzystywanych w systemach radiolokacyjnych, radionawigacyjnych i łączności wojsk lądowych oraz lotnictwa. Jak dowodzą doświadczenia z współczesnych konfliktów militarnych, w pierwszej kolejności obezwładnione zostają środki i systemy radioelektroniczne wojsk rakietowych i artylerii, obrony powietrznej i lotnictwa.

W walce i operacji, przy uwzględnieniu ich ogólnego celu, przewiduje się organizowanie walki elektronicznej z takim wyliczeniem, aby jak najszybciej, zwłaszcza na decydujących etapach działań, uniemożliwić przeciwnikowi dowodzenie wojskami i kierowanie środkami walki, szczególnie w strefie taktycznej, a tym samym stworzyć korzystne warunki do wykonania zadań przez wojska własne oraz osiągnięcia sukcesu taktyczno-operacyjnego i zrealizowania celu operacji.

W wykonaniu tych zadań będą uczestniczyć wszystkie rodzaje sił zbrojnych oraz wojsk, wykonując zadania stosowne do posiadanego etatowego uzbrojenia oraz wyposażenia w radioelektroniczne środki walki. Zasadnicze zadania w zakresie aktywnego radioelektronicznego oddziaływania wykonywać będą oddziały i pododdziały rozpoznania, zakłóceń i dezinformacji elektronicznej, o różnej strukturze organizacyjnej, przeznaczeniu, wyposażeniu i możliwościach, pozostające w dyspozycji dowództw i sztabów rodzajów sił zbrojnych oraz w dyspozycji dowództw i sztabów ogólnowojskowych związków operacyjnych i taktycznych.

Walka elektroniczna realizowana w obrębie walki informacyjnej obejmuje różne przedsięwzięcia i działania wojsk związane z zastosowaniem odpowiednich sił i środków, metod i sposobów, mających na celu rozpoznanie oraz aktywne zwalczanie środków i systemów radioelektronicznych przeciwnika, z równoczesnym zapewnieniem stabilności pracy i odporności na zakłócenia analogicznym środkom i systemom radioelektronicznym wojsk własnych. Z powyższego wynika, że w działaniach zbrojnych, w walce i operacji, ma ona do spełnienia dwa główne, kompleksowe zadania:

– zwalczanie elektronicznie za pomocą zakłóceniowej energii elektromagnetycznej oraz broni wiązkowej, czynnych środków i systemów radioelektronicznych przeciwnika, w celu dezorganizacji dowodzenia wojskami i kie-

rowania środkami walki, a poprzez to obniżenie efektywności użycia środków bojowych oraz skuteczności działań lotnictwa, wojsk rakietowych i artylerii, zgrupowań wojsk pancernych i zmechanizowanych, desantów, sił i środków obrony powietrznej oraz sił morskich,

– zabezpieczenie środków i systemów radioelektronicznych wojsk własnych przed oddziaływaniem radioelektronicznym przeciwnika w celu zapewnienia ciągłości i operatywności dowodzenia wojskami i kierowania środkami walki, a tym samym zachowanie żywotności i zdolności bojowych wojsk.

Efektywne wykonanie pierwszego zadania prowadzi do rozproszenia wysiłku operacyjnego i taktycznego wojsk przeciwnika wskutek znacznego utrudnienia, a nawet pozbawienia dowództw i sztabów możliwości koordynowania działań poszczególnych rodzajów sił zbrojnych oraz wojsk, jak również poszczególnych związków operacyjnych i taktycznych. Może to powodować opóźnienia, a w skrajnych przypadkach nawet uniemożliwić zastosowanie środków rażenia.

Skuteczne zdezorganizowanie pracy radioelektronicznych systemów kierowania i sterowania środkami ogniowymi pozbawia przeciwnika możliwości terminowego ich użycia, powoduje wcześniejsze lub późniejsze, w stosunku do planowanego, działanie ładunków wybuchowych głowic rakiet, bomb lotniczych, pocisków kierowanych itp. Utrudnia lub uniemożliwia adwersarzowi wykonanie celnych uderzeń na wojska znajdujące się w rejonach stałej dyslokacji, podczas ich przegrupowania, w rejonach ześrodkowania i wyjściowych oraz na wojska rozwinięte i walczące na obszarze działań zbrojnych, w wyznaczonych im obszarach, pasach i rejonach.

Wykonanie drugiego zadania w warunkach radioelektronicznego oddziaływania przeciwnika umożliwia zachowanie ciągłości i operatywności dowodzenia własnymi wojskami, a w rezultacie terminowe ich użycie na wyznaczonych kierunkach operacyjnych, zgodnie z decyzjami dowódców, a także zachowanie ścisłego współdziałania i wykonanie zarówno skutecznych uderzeń wszystkimi środkami bojowymi, jak i planowanych zadań przez wszystkie rodzaje wojsk.

Między wymienionymi głównymi zadaniami istnieje ścisła współzależność. Wymaga ona kompleksowego i systemowego ujmowania walki elektronicznej, przede wszystkim ścisłego koordynowania i łączenia przedsięwzięć zakłócania i dezinformacji elektronicznej z uderzeniami wojsk, z uderzeniami ogniowymi wojsk rakietowych i artylerii oraz lotnictwa, jak również z przedsięwzięciami zabezpieczającymi własne wojska i systemy dowodzenia przed aktywnym oddziaływaniem radioelektronicznym przeciwnika. Wymaga także

wyjątkowo wysokiej, kunsztownej, taktyczno-operacyjnej i technicznej umiejętności określania newralgicznych miejsc w systemach dowodzenia wojskami, kierowania środkami rażenia, rozpoznania i walki elektronicznej przeciwnika, jak również niezawodnych, choć prostych w swoim zamiarze, sposobów działania oraz umiejętnego, wręcz mistrzowskiego, wykorzystywania własnej, coraz doskonalszej techniki elektronicznej, którą powszechnie wprowadza się do wojsk.

Jednoznacznie sformułowane cele i zadania wykazują, że współczesna walka elektroniczna, podobnie jak każda klasyczna walka zbrojna, obejmuje dwie formy działań[3]: ofensywną, która w tym wypadku polega na rozpoznaniu i obezwładnianiu elektronicznym, ściśle skoordynowanym z obezwładnianiem środkami rażenia, oraz defensywną, polegającą na kompleksowym wykonaniu wielu przedsięwzięć zapewniających ciągłą i efektywną pracę własnych środków i systemów radioelektronicznych. Obie te formy wzajemnie się uzupełniają, a ich jednoczesne zastosowanie stanowi istotę współczesnej walki elektronicznej. Od ich jakości i sposobu wykonania zależy uzyskanie przewagi informacyjnej. Dlatego muszą one być jednakowo dokładnie zaplanowane i zorganizowane, stosownie do aktualnej sytuacji strategiczno-operacyjnej i taktycznej, sytuacji radioelektronicznej oraz decyzji dowódców, określających zadania i sposób działania poszczególnych rodzajów wojsk.

Na podstawie analizy dokumentów sojuszniczych można wnioskować, że walka elektroniczna stanowi szeroko rozbudowany system i obejmuje[4]:

– rozpoznanie elektroniczne prowadzone wszystkimi dostępnymi siłami i środkami w ramach jednolitego systemu strategiczno-operacyjnego i taktycznego rozpoznania wojskowego, w ścisłym współdziałaniu z innymi rodzajami rozpoznania,

– przeciwdziałanie elektroniczne obejmujące stosowanie różnego rodzaju aktywnych i pasywnych zakłóceń, dezinformacji elektronicznej (mylenia) oraz niszczenia urządzeń elektronicznych. Do tych celów wykorzystywane są jedno- i wielozadaniowe stacje zakłócające i dywersyjne oraz środki pasywne zakłóceń elektronicznych (maskowania), a także, w wiodących państwach świata, broń wiązkowa (laserowa, mikrofalowa),

3 *Walka elektroniczna*, MON SG WP, Warszawa 2003, s. 7.

4 W terminologii angielskiej występują określenia: ESM – *Electronic Warfare Support Measures*, ECM – *Electronic Countermeasures*, EPM – *Electronic Protective Measures*.

– obrona elektroniczna polegająca na wykonaniu szeregu przedsięwzięć organizacyjno-technicznych oraz na kontroli radioelektronicznej, w celu zapewnienia stabilności pracy różnych systemów dowodzenia i kierowania środkami walki własnych wojsk.

W związku z szybkim rozwojem nowoczesnych środków walki, a zwłaszcza rakiet i lotnictwa, w teorii wojskowości, w całokształcie zadań walki elektronicznej uwzględnia się również zagadnienia niszczenia ogniem zasadniczych środków i obiektów elektronicznych przeciwnika, głównie systemów rozpoznania radiotechnicznego wykorzystywanego w obronie powietrznej państwa. Do uzbrojenia lotnictwa wprowadza się od kilku lat coraz doskonalsze rakiety przeciwradiolokacyjne, przeznaczone przede wszystkim do niszczenia stacji radiolokacyjnych pracujących w systemie obrony powietrznej oraz rakiety samonaprowadzające się na źródła promieniowania elektromagnetycznego. O wysokiej efektywności tego typu środków walki świadczy wartość prawdopodobieństwa trafienia stacji radiolokacyjnej za pomocą tego typu rakiet, która wynosi 0,7–0,8.

3.2. Rozpoznanie elektroniczne jako element walki informacyjnej

Rozpoznanie elektroniczne w terminologii anglojęzycznej określa się mianem ESM (*Electronic Warfare Support Measures*), które doktrynalnie oznacza pasywną formę zdobywania informacji o obiektach elektronicznych przeciwnika promieniujących energię EM, przez ich poszukiwanie, przechwytywanie, śledzenie, namierzanie oraz analizę[5]. Jako element systemu rozpoznania wojskowego określane jest jako rozpoznanie radioelektroniczne (ang. *Signals Intelligence* – SIGINT). Termin ten definiuje się podobnie, a mianowicie jako potencjał rozpoznawczy oraz proces pozyskiwania danych i informacji rozpoznawczych o obiektach elektronicznych przeciwnika promieniujących energię elektromagnetyczną[6].

Jako element działań informacyjnych rozpoznanie elektroniczne prowadzone jest stale, bez względu na istniejącą sytuację polityczno-militarną, warunki atmosferyczne, czas, miejsce oraz położenie wojsk.

5 *Walka elektroniczna...*, dz. cyt., s. 8.
6 *Doktryna Rozpoznanie...*, dz. cyt., s. 12.

W ciągu następujących po sobie czynności rozpoznania elektronicznego pozyskane fakty (dane wejściowe) o obiektach promieniujących energię elektromagnetyczną stają się informacjami rozpoznawczymi, a jako takie stanowią podstawę do analizy operacyjnej i technicznej. Wytworzone na ich podstawie wiadomości są wykorzystywane przede wszystkim do oceny sytuacji militarnej w procesie dowodzenia (rozpoznanie sytuacyjne). Informacje techniczne o wykorzystywanych przez przeciwnika sygnałach wykorzystywane są do określenia parametrów technicznych i przedsięwzięć organizacyjnych niezbędnych do przeprowadzenia skutecznego przeciwdziałania elektronicznego (rozpoznanie celów elektronicznych). Stanowią również podstawę do organizowania obrony elektronicznej, a także koordynacji kolejnych zadań rozpoznawczych.

Rozpoznanie sytuacyjne i rozpoznanie celów elektronicznych podlegają wszelkim regułom i zasadom obowiązującym w procesie działalności rozpoznawczej, do których zalicza się[7]: centralne kierowanie, terminowość, efektywne wykorzystanie, obiektywność, dostępność, dyspozycyjność, bezpieczeństwo oraz systematyczność.

W czasie prowadzenia walki informacyjnej rozpoznanie elektroniczne może służyć do wskazywania kierunków i rejonów zwiększonej aktywności elektronicznej przeciwnika, określenia położenia jego wojsk i obiektów, stanowiąc podstawę do dokładnego ich zidentyfikowania i lokalizacji z wykorzystaniem innych środków rozpoznania.

Rozpoznanie radioelektroniczne dzieli się na rozpoznanie radiowe i rozpoznanie elektroniczne.

Rozpoznanie radiowe (ang. *Communications Intelligence* – COMINT) to potencjał rozpoznawczy oraz proces pozyskiwania danych i informacji rozpoznawczych z systemów komunikacyjnych (łączności i transmisji danych) przechwyconych przez innych odbiorców niż tych, do których są one adresowane.

Rozpoznanie elektroniczne (ang. *Electronic Intelligence* – ELINT) to potencjał rozpoznawczy oraz proces pozyskiwania danych i informacji rozpoznawczych z systemów niekomunikacyjnych przechwyconych przez innych odbiorców niż tych, do których są one adresowane. Informacje rozpoznawcze pozyskiwane są w procesie analizy takich sygnałów, jak: sygnały wytwarzane przez radary, systemy naprowadzania rakiet, lasery, urządzenia emitujące promieniowanie podczerwone i inne promieniujące energię elektromagnetyczną.

7 Szerzej w: *Doktryna Rozpoznanie...*, dz. cyt., s. 21–22.

Rozpoznanie radioelektroniczne stanowi jeden z najważniejszych sposobów zdobywania informacji w systemie rozpoznania wojskowego i w systemie walki elektronicznej. Współczesne potęgi militarne dla potrzeb swoich sił zbrojnych organizują globalny system rozpoznania radioelektronicznego, w obrębie którego prowadzi się nieprzerwanie, w okresie pokoju, kryzysu i wojny, rozpoznanie strategiczne oraz, w okresie działań zbrojnych, rozpoznanie operacyjne i taktyczne.

Na podstawie analizy dostępnych informacji specjalistycznych można wnioskować, że radioelektroniczne rozpoznanie strategiczne obejmuje swoim zakresem działalność różnych wywiadów radioelektronicznych oraz rozpoznanie satelitarne, powietrzne, morskie i naziemne. Prowadzone jest na bardzo dalekie odległości i ma na celu zebranie informacji i ustalenie danych o najważniejszych obiektach gospodarczych, politycznych i militarnych przeciwnika, które mogą mieć istotne znaczenie w wypadku powstania konfliktu zbrojnego. W czasie wojny jego celem prawdopodobnie będzie potwierdzenie danych uzyskanych w okresie pokoju oraz wykrywanie kierunków i miejsc przemieszczania się wojsk, jak również zmian dyslokacji ważnych obiektów radioelektronicznych.

Elektroniczne rozpoznanie operacyjne i taktyczne, które prowadzi się w celu zabezpieczenia działań zbrojnych, realizowane jest różnorodnymi siłami i środkami rozpoznania wojskowego oraz siłami i środkami walki elektronicznej. Obejmuje ono elektroniczne rozpoznanie powietrzne, morskie i naziemne.

Najogólniej rzecz ujmując, rozpoznanie elektroniczne prowadzone podczas rozpoznania strategicznego, operacyjnego i taktycznego zapewnia zdobycie możliwie pełnych informacji o obiektach, wojskach oraz systemach radioelektronicznych przeciwnika. W jego ramach stosowane są różne techniki rozpoznania (radiowe, radiolokacyjne, laserowe, optoelektroniczne itp.). Na podstawie przebiegu konfliktów militarnych w Iraku i byłej Jugosławii można postawić tezę, że rozpoznanie i kontrola promieniowania elektromagnetycznego, szczególnie pasm częstotliwości radiowych i radiolokacyjnych, umożliwia neutralizację systemów radiolokacyjnych wroga i penetrację jego obszaru powietrznego oraz chroni przed podobną akcją podjętą przez przeciwnika. Umożliwia także dowództwom i sztabom przekazywanie rozkazów oraz zakłócanie tego ważnego procesu realizowanego przez drugą stronę konfliktu.

Ze względu na ogromne możliwości uzyskiwania różnorodnych danych rozpoznawczych rozpoznanie elektroniczne traktowane jest jako jeden z ważniejszych rodzajów rozpoznania wojskowego. Zapewnia bowiem dużą szybkość otrzymywania danych o wojskach przeciwnika, jego uzbrojeniu,

możliwościach oraz o środkach i systemach radioelektronicznych; umożliwia określenie przynależności wykorzystywanych przez przeciwnika środków i urządzeń radioelektronicznych, ich częstotliwości roboczych, rodzajów pracy, mocy promieniowania anten radioelektronicznych urządzeń nadawczych oraz miejsc i rejonów dyslokacji, z dokładnością rzadko pozwalającą na skuteczne ich niszczenie ogniem, jak również efektywne obezwładnianie zakłóceniami elektronicznymi.

Na podstawie zdobytych informacji ustala się typy, liczbę, parametry techniczne i zasady wykorzystywania środków radioelektronicznych. Określa się charakterystyki i struktury organizacyjne systemów rozpoznania radiolokacyjnego, radionawigacji oraz metody i system kierowania i naprowadzania środków walki, jak również liczbę i gęstość rozmieszczenia źródeł promieniowania elektromagnetycznego i tym samym nasycenie poszczególnych rejonów i poszczególnych kierunków strategiczno-operacyjnych i taktycznych środkami i urządzeniami radioelektronicznymi.

Rozpoznaniu radioelektronicznemu podlegają obecnie wszystkie środki łączności radiowej, radioliniowej (zakresu metrowego, decymetrowego, troposferyczne, jonosferyczne) i łączności satelitarnej oraz różnego typu stacje radiolokacyjne, radionawigacyjne i inne środki radioelektroniczne specjalnego przeznaczenia.

Informacje uzyskiwane na potrzeby walki informacyjnej dzięki rozpoznaniu radioelektronicznemu pozwalają określić rozmieszczenie wojsk, lotnisk, baz i składów wojskowych, stanowisk startowych rakiet, stanowisk dowodzenia i węzłów łączności. Rozpoznanie radioelektroniczne dostarcza także innych niezbędnych danych o położeniu, stanie bojowym i możliwościach sił zbrojnych przeciwnika; pozwala również wykryć przygotowania jego sił zbrojnych do wojny.

Dzięki możliwościom technicznym współczesnych środków i urządzeń rozpoznawczych rozpoznanie elektroniczne może być prowadzone na dużą głębokość niezależnie od pory roku i doby oraz warunków meteorologicznych. Uzyskanie wymaganej głębokości rozpoznania zależy od prawidłowego doboru środków rozpoznania oraz ich rozmieszczenia w terenie, stosownie do położenia wojsk przeciwnika i prawdopodobnych kierunków ich działań, jak również odpowiednio do rozpoznawanych obiektów i możliwości technicznych wykorzystywanych środków.

Przedmiotem rozpoznania elektronicznego są sygnały i emisje elektromagnetyczne urządzeń radioelektronicznych: samolotów, okrętów i okrętów podwodnych, wojsk rozmieszczonych w terenie, baz rakietowych oraz baz innych

rodzajów uzbrojenia. Prowadzony jest również nasłuch dyplomatycznych, państwowych i wojskowych relacji łączności radioliniowej i troposferycznej. Takie przedsięwzięcia realizują wyspecjalizowane jednostki radioelektroniczne przewidziane do wsparcia działań bojowych.

Rozpoznanie satelitarne traktowane jest przez specjalistów wiodących potęg militarnych jako najważniejszy rodzaj rozpoznania zarówno w okresie pokoju, jak i wojny. Podczas rozpoznania satelitarnego, oprócz rozpoznania obrazowego, stosuje się w szerokim zakresie rozpoznanie radioelektroniczne. W stosunku do celów i realizowanych zadań rozpoznania modelowane są orbity satelitów rozpoznawczych najczęściej w taki sposób, aby cyklicznie, w określonych interwałach czasowych zlokalizować i ustalić aktualną sytuację militarną i radioelektroniczną na obszarach zainteresowania. Do prowadzenia rozpoznania satelitarnego wykorzystuje się sztuczne satelity Ziemi. Zadaniem rozpoznania satelitarnego jest wykrycie środków i obiektów systemu obrony powietrznej, rejonów dyslokacji stanowisk startowych rakiet, obiektów systemu dowodzenia i naprowadzania lotnictwa, obiektów stacjonarnych i polowych systemów łączności satelitarnej, łączności strategiczno-operacyjnego przeznaczenia oraz systemów rozpoznania radiolokacyjnego i radionawigacji.

Na potrzeby prowadzenia walki informacyjnej rozbudowywane zostają także radioelektroniczne systemy wykrywania i śledzenia satelitów. Proces wykrycia, identyfikacji i oceny obiektu satelitarnego wymaga jednak wielkiej dokładności i dużej szybkości działania całego systemu rozpoznawczego.

W systemie wykrywania i śledzenia satelitów wykorzystuje się specjalne stacje rozpoznawcze, wyposażone w przyrządy optyczne, urządzenia laserowe oraz różnorodną aparaturę radioelektroniczną. Stacje rozpoznawcze wchodzą w skład specjalnych ośrodków i punktów (posterunków) rozpoznania satelitarnego.

Lotnicze rozpoznanie radioelektroniczne prowadzone jest w okresie pokoju, kryzysu i wojny. Do tego celu wykorzystuje się samoloty rozpoznawcze i samoloty walki elektronicznej wyposażone w wysokiej jakości urządzenia radioelektroniczne umożliwiające wykrywanie i śledzenie pracy środków radioelektronicznych w zakresie fal metrowych, decymetrowych i centymetrowych. Są to urządzenia przechwytywania radiowego, rozpoznania radiolokacyjnego, analizy emisji elektromagnetycznych, stacje radiolokacyjne, urządzenia optoelektroniczne itp. Celem wykonywanych lotów rozpoznawczych jest określenie położenia wojsk, dyslokacji obiektów radioelektronicznych (stacji radiolokacyjnych radionawigacyjnych i środków łączności zarówno stacjonarnych, jak i polowych), ustalenie ich parametrów taktyczno-technicznych oraz

nasłuch i rejestrowanie przekazywanych informacji za pomocą różnych metod, sposobów i technicznych środków.

Do zadań rozpoznania radioelektronicznego wykorzystuje się samoloty rozpoznawcze, na których zamontowane są uniwersalne i panoramiczne stacje radiolokacyjne, stacje radiolokacyjne obserwacji bocznej oraz urządzenia rozpoznania radiowego.

Samoloty wyposażone w najnowocześniejsze środki rozpoznania radioelektronicznego wykonują w czasie pokoju loty rozpoznawcze w różne części globu. Bardzo intensywnie prowadzone są loty w różnych przedziałach czasowych wzdłuż granic państw należących do stref zainteresowania[8]. Celem wykonywanych lotów jest określenie miejsc dyslokacji wojskowych obiektów radioelektronicznych (stacji radiolokacyjnych i środków łączności – stacjonarnych i polowych), ustalenie ich parametrów taktyczno-technicznych oraz nasłuch i rejestrowanie informacji przekazywanych w czynnych relacjach łączności.

Dzięki posiadanym siłom i środkom rozpoznania radioelektronicznego lotnictwo może prowadzić rozpoznanie radiowe w zakresie krótkofalowym na głębokość 1000–4000 km, a w zakresie ultrakrótkofalowym radiowe i radiolokacyjne na głębokość 300–400 km. Wykorzystywane w systemie rozpoznania samolotowe rozpoznawcze stacje radiolokacyjne mają dużą zdolność rozróżniania obiektów i mogą prowadzić rozpoznanie poza strefą zasięgu aktywnych środków obrony przeciwlotniczej. Podczas lotów na małych, średnich i dużych wysokościach zapewniają możliwość rozróżniania celów stacjonarnych i ruchomych. Tego rodzaju stacje radiolokacyjne znajdują zastosowanie również na bezpilotowych samolotach rozpoznawczych, których przelot odbywa się według wcześniej ustalonego programu lub według komend przekazywanych z ziemi.

Jak wskazują doświadczenia płynące z współczesnych konfliktów zbrojnych, podczas działań zbrojnych realizuje się prowadzenie rozpoznania taktycznego przez lotnictwo przed rozpoczęciem działań oraz w ich toku w celu określenia i ustalenia parametrów taktyczno-technicznych, przeznaczenia, rozmieszczenia oraz stopnia odporności na zakłócenia środków i urządzeń radioelektronicznych wojsk przeciwnika. Na podstawie uzyskanych danych wytyczane są zadania i określana jest taktyka działania samolotów wyposażonych w środki zakłócające.

8 Por. http://www.tvp.info/17449694/niespotykana-skala-aktywnosci-rosyjskiego-lotnictwa-nad-europa-nato-zaniepokojone [dostęp: 15.11.2014].

Zadaniem rozpoznania radioelektronicznego prowadzonego podczas wykonywania zadań bojowych przez lotnictwo jest również uprzedzenie pilotów o wejściu w strefę rozpoznania radiolokacyjnego środków OPL oraz określenie rejonów rozmieszczenia środków radiolokacyjnych stanowiących największe niebezpieczeństwo dla samolotów; ustalenie potrzeb, zakresu i sposobów stosowania zakłóceń elektronicznych (aktywnych i pasywnych) oraz zdecydowanie o konieczności wykonania niezbędnego manewru samolotów w powietrzu oraz wskazywania samolotom bojowym celów radioelektronicznych, które podlegają obezwładnieniu (niszczeniu) rakietami typu „powietrze–ziemia" oraz rakietami przeciwradiolokacyjnymi (samonaprowadzającymi się na źródło promieniowania energii elektromagnetycznej – stacja radiolokacyjna, radiostacja itp.).

Tego rodzaju taktykę rozpoznania radioelektronicznego zaczęto stosować podczas wojny w Wietnamie i na Bliskim Wschodzie, a kontynuowano w I i II wojnie w Iraku, w byłej Jugosławii oraz w konflikcie na terytorium Libii. Uogólniając, rozpoznanie przed rozpoczęciem lotów bojowych prowadziły samoloty rozpoznawcze wyposażone w stacje pracujące w zakresach częstotliwości: 30–4125 MHz i 1000–10750 MHz. Za pomocą tych urządzeń wykrywano środki radioelektroniczne, określano ich parametry techniczne, miejsca rozmieszczenia i zapewniano wskazywanie celów środkom ogniowym i zakłócającym znajdującym się w składzie grup uderzeniowych lotnictwa.

Morskie rozpoznanie radioelektroniczne w okresie pokoju, kryzysu i wojny prowadzone jest na głównych morskich szlakach komunikacyjnych i wzdłuż granic wód terytorialnych państw będących w zainteresowaniu rozpoznawczym. Do tego celu wykorzystuje się specjalne okręty nawodne i podwodne wyposażone w liczne urządzenia radioelektroniczne, które umożliwiają śledzenie pracy środków i obiektów radioelektronicznych z odległości kilkudziesięciu, a nawet kilkuset kilometrów od brzegu. W okresie pokoju okręty wyposażone w środki rozpoznania radioelektronicznego wykonują najczęściej rejsy pojedyncze, które często trwają około dwóch tygodni. Okręty rozpoznania elektronicznego nieprzerwanie prowadzą rozpoznanie radioelektroniczne. Bardzo często okręty te w sposób zamierzony wchodzą na wody terytorialne państw, aby sprowokować pracę środków radioelektronicznych w systemie sił zbrojnych, w szczególności systemów rozpoznania i dowodzenia marynarki

wojennej[9]. Również w akwenie Morza Bałtyckiego wykorzystywane są różnego typu okręty rozpoznania radioelektronicznego.

Oprócz specjalnych okrętów w systemie rozpoznania radioelektronicznego przewiduje się używanie okrętów wyposażonych w znaczną liczbę środków rozpoznania i zakłóceń elektronicznych oraz lotnictwa pokładowego sił morskich, w którego składzie znajdują się eskadry rozpoznania i zakłóceń elektronicznych.

Na okrętach bojowych, w zależności od ich typu i przeznaczenia, mogą się także znajdować co najmniej trzy stacje rozpoznania radiolokacyjnego, stacje rozpoznania radiowego, namierniki radiowe, stacje zakłócające oraz stacje imitujące obiekty nawodne. Wyposażenie to wykorzystywane jest w walce informacyjnej do tworzenia świadomości sytuacyjnej oraz tworzenia obrazu pozornego dla systemów rozpoznania elektronicznego przeciwnika.

Naziemne rozpoznanie radioelektroniczne prowadzone jest w ogólnowojskowym systemie rozpoznania oraz w systemie walki elektronicznej. W każdym systemie rozpoznawczym wojsk wykorzystuje się stacjonarne i polowe środki rozpoznawcze. Polowe środki rozpoznawcze znajdują się w wyposażeniu jednostek wojsk pancernych i zmechanizowanych oraz w wyposażeniu specjalnych jednostek rozpoznania oraz jednostek walki elektronicznej.

W stacjonarnym systemie rozpoznania radioelektronicznego wykorzystuje się stacje i posterunki rozpoznawcze, które w zależności od poziomu kompletności i rodzaju wyposażenia, mogą przechwytywać emisje elektromagnetyczne i prowadzić nasłuch radiowy na głębokość ponad 2000 km na falach długich, średnich i krótkich.

Polowy system rozpoznania radioelektronicznego rozwijają specjalne jednostki rozpoznania i walki elektronicznej. Wyposażone są one w środki i urządzenia radioelektroniczne, które umożliwiają prowadzenie rozpoznania radiowego w zakresie fal średnich, krótkich i ultrakrótkich oraz rozpoznania systemów radiolokacyjnych (radiotechnicznego).

Jednostki rozpoznania radioelektronicznego wojsk lądowych mają zasadniczo możliwość prowadzenia rozpoznania radiowego w zakresie fal średnich i krótkich na głębokość 1000 km i więcej, w zakresie fal UKF metrowych do

9 Por. http://wiadomosci.onet.pl/swiat/tajemnicza-operacja-wojskowa-u-wybrzezy-szwecji-zatonal-rosyjski-okret-podwodny/8bh1x [dostęp: 20.11.2014], http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosyjski-okret-szpiegowski-pod-nosem-usa,402937.html [dostęp: 20.14.2014].

80 km, w zakresie fal UKF decymetrowych do 60 km, w zakresie fal centymetrowych do 40 km[10].

Z dużą dozą prawdopodobieństwa można założyć, że obecnie, w okresie pokoju, wszystkie jednostki rozpoznawcze prowadzą nieprzerwane rozpoznanie radiowe, radiotechniczne i namierzanie radiowe. Są w stałej gotowości bojowej. Intensywność działań tych pododdziałów wzrasta w okresach napięć w sytuacji międzynarodowej.

Oprócz tych rodzajów rozpoznania w systemie rozpoznawczym wojsk lądowych szczególnie dużo uwagi poświęca się radioelektronicznemu rozpoznaniu i obserwacji pola walki. Mając to na względzie, do uzbrojenia oddziałów i pododdziałów wojsk pancernych i zmechanizowanych wprowadzono znaczną liczbę stacji radiolokacyjnych obserwacji pola walki, które umożliwiają wykrywanie celów naziemnych (czołgi, transportery opancerzone, samochody, ludzie itp.). Wiele z nich przeznacza się do rozpoznawania obiektów poruszających się nocą i w warunkach ograniczonej widoczności.

W wojskach lądowych do prowadzeniu tego rodzaju rozpoznania wykorzystuje się stacje o różnych możliwościach taktyczno-technicznych. Można je podzielić na cztery podstawowe grupy: stacje dalekiego rozpoznania o zasięgu wykrywania do 20 km; średniego – do 18 km; małego – do 10 km i bliskiego – do 3–5 km.

W systemie rozpoznania wojsk lądowych do prowadzenia rozpoznania i obserwacji pola walki przewiduje się również wykorzystywanie radioelektronicznych środków telewizyjnych. W zależności od charakteru rozwiązywanych zadań i warunków ich użycia środki i urządzenia telewizyjne instalowane są na bezpilotowych środkach rozpoznawczych, w samolotach i śmigłowcach, w czołgach i transporterach opancerzonych. Tego rodzaju środki montuje się również na okrętach nawodnych i podwodnych oraz na satelitach rozpoznawczych.

Obecnie do prowadzenia rozpoznania wykorzystuje się różne systemy obrazowe. Zwykle sygnały obrazu z ziemi, powietrza i z morza przekazywane są do specjalnie urządzonych odbiorczych stacji rozwiniętych na punktach dowodzenia szczebla strategicznego, operacyjnego i taktycznego. W zależności od odległości między elementem rozpoznawczym, a stacją odbiorczą sygnały mogą być przekazywane w bezpośredniej relacji łączności lub przez jedną czy kilka stacji retranslacyjnych.

10 Zasięg rozpoznania zależy m.in. od częstotliwości sygnału (długości fali), mocy nadajnika, zysku kierunkowego anteny nadawczej i odbiorczej, wysokości posadowienia anten oraz warunków rozprzestrzeniania się fali elektromagnetycznej.

W działaniach bojowych stosuje się także artyleryjskie rozpoznanie radiotechniczne, które może zdobywać informacje o obiektach przeciwnika przy wykorzystaniu specjalnych rozpoznawczych stacji radiolokacyjnych. Polowe stacje radiolokacyjne rozpoznania artyleryjskiego mogą rozpoznać naziemne środki na głębokość 20–30 km od linii styczności wojsk[11].

W radioelektronicznym podsystemie rozpoznawczym szerokie zastosowanie znajduje również technika pracująca w podczerwieni i technika laserowa. Tego rodzaju środki i urządzenia umożliwiają obserwację pola walki w warunkach ograniczonej widoczności, a nawet całkowitej ciemności. Zapewniają one wykrywanie obiektów na podstawie ich własnego promieniowania cieplnego, naprowadzania pocisków na cel i sterowanie środkami bojowymi. Elektroniczno-optyczne przyrządy noktowizyjne pozwalają prowadzić obserwację, ogień oraz kierować czołgami, transporterami opancerzonymi i samochodami w nocy. Pracują one głównie na zasadzie wykorzystania odbitych od obiektu promieni cieplnych o długości fali do 2 mikronów.

W grupie laserowych środków rozpoznawczych w coraz szerszym zakresie wykorzystuje się różnego typu dalmierze, urządzenia podświetlania celów, urządzenia rozpoznania, naprowadzania pocisków przeciwpancernych, bomb lotniczych i różnego typu rakiet.

Dalmierze laserowe, które znajdują się w wyposażeniu etatowym czołgów, transporterów opancerzonych, samolotów i śmigłowców są w porównaniu z urządzeniami optycznymi i radiolokacyjnymi dokładniejsze w określaniu współrzędnych celu, a także mniejsze i łatwiejsze do transportu. Zasada ich działania jest analogiczna jak dalmierzy radiolokacyjnych. Różnią się tylko zakresem częstotliwości. Pracują w zakresie promieni świetlnych i podczerwonych i umożliwiają dokładne określenie odległości od obiektów.

Zakres i możliwości techniczne rozpoznania elektronicznego, choć przedstawione jedynie w bardzo ogólnym zarysie, dowodzą, że we współczesnym systemie walki informacyjnej odgrywa ono jedną z priorytetowych ról. Jego organizacją zajmują się organy służb specjalnych, organy rozpoznania wojsk oraz organy walki elektronicznej sztabów sił zbrojnych i rodzajów wojsk, związków operacyjnych i taktycznych. Organom tym podporządkowane są specjalne jednostki rozpoznania elektronicznego wykonujące zadania w systemie rozpoznania satelitarnego, lotniczego, morskiego i lądowego.

11 Por. http://dziennikzbrojny.pl/artykuly/art,5,23,3423,wojska-ladowe,wyposazenie,radar-rozpoznania-artyleryjskiego-liwiec [dostęp: 15.10.2014].

3.3. Przeciwdziałanie elektroniczne jako element walki informacyjnej

Przeciwdziałanie elektroniczne, w anglojęzycznej literaturze określane jako ECM (*Electronic Countermeasures*), definiowane jest jako zespół skoordynowanych przedsięwzięć, ukierunkowanych na dezorganizację pracy systemów oraz urządzeń elektronicznych przeciwnika, funkcjonujących w środowisku elektromagnetycznym[12].

Przeciwdziałanie elektroniczne jako element walki informacyjnej ma za zadanie uniemożliwić lub znacząco ograniczyć efektywność wykorzystania przestrzeni elektromagnetycznej przez przeciwnika. Prowadzenie tych działań wpływa na obniżenie sprawności systemów dowodzenia, rozpoznania i kierowania środkami walki strony przeciwnej. Może być ono realizowane w formie aktywnej lub pasywnej. Forma aktywna polega na wypromieniowaniu przez urządzenie nadawcze zakłócającej lub neutralizującej energii elektromagnetycznej na częstotliwościach lub w paśmie pracy odpowiednich urządzeń odbiorczych przeciwnika. Do tego celu mogą być wykorzystywane urządzenia stacjonarne, polowe (mobilne) oraz nadajniki jednorazowego użytku, odznaczające się różnorodnymi parametrami taktyczno-technicznymi, dostosowanymi do konkretnych środków i systemów elektronicznych, na które mają oddziaływać. Forma pasywna polega na wtórnym wypromieniowaniu (odpromieniowaniu, odbijaniu i rozpraszaniu) lub obniżeniu mocy energii elektromagnetycznej, w tym jej wchłanianiu, przez środki niebędące jej generatorami, w sposób zamierzony, w celu zmylenia, odwrócenia uwagi lub oszukania przeciwnika i jego systemów elektronicznych.

W ramach przeciwdziałania elektronicznego prowadzone są następujące działania: zakłócanie elektroniczne, pozorowanie elektroniczne oraz neutralizacja elektroniczna.

Zakłócanie elektroniczne polega na celowym (rozmyślnym) promieniowaniu energii elektromagnetycznej powodującej obniżenie efektywności użycia odbiorczych urządzeń (systemów) elektronicznych wykorzystywanych przez przeciwnika i jest aktywną formą przeciwdziałania elektronicznego. Wnosi ono do urządzeń elektronicznych dodatkowe wartości energetyczne o strukturze zbliżonej do sygnałów użytecznych, które powodują dezorganizację ich

12 *Walka elektroniczna*..., dz. cyt., s. 9.

pracy. Tak rozumiane zakłócanie elektroniczne wkomponowuje się w teorię walki informacyjnej jako składowa zakłócania informacyjnego[13].

Drugim przedsięwzięciem realizowanym w obrębie przeciwdziałania elektronicznego jest neutralizacja elektroniczna, która polega na celowym użyciu energii elektromagnetycznej o dużej gęstości, powodującej uszkodzenie lub zniszczenie podzespołów elektronicznych sprzętu bojowego, wykorzystywanego głównie w procesie dowodzenia i łączności, kierowania uzbrojeniem, nawigacji i rozpoznania.

Ostatnim przedsięwzięciem przeciwdziałania jest pozorowanie elektroniczne. Stanowi ono kompleks przedsięwzięć organizacyjnych i technicznych mających na celu wprowadzanie w błąd przeciwnika (głównie środków rozpoznania elektronicznego). Działania te mogą przyjąć formę aktywną lub pasywną. Polegają na sztucznym tworzeniu „obrazu" (obiektu, czynności itp.) zbliżonego do rzeczywistego przez promieniowanie, odbijanie lub tłumienie energii elektromagnetycznej. Sygnały przekazywane wraz z treściami informacyjnymi powinny wytworzyć u przeciwnika przekonanie o sytuacji nieistniejącej w rzeczywistości. Odbierający nie powinien zorientować się, że sygnały są spreparowane lub zmodyfikowane i uznać przekazaną treść za prawdziwą. Pozorowanie elektroniczne osiąga się przez tworzenie obiektów pozornych, stosowanie manewru pozornego środkami lub energią elektromagnetyczną oraz pozornych przedsięwzięć organizacyjnych, a także przez deformowanie obiektów rzeczywistych dla rozpoznawczych urządzeń elektronicznych przeciwnika.

Uogólniając, przeciwdziałanie elektroniczne obejmuje wszelkie środki i sposoby mające na celu uniemożliwienie przeciwnikowi wykorzystania jego środków i systemów elektronicznych. Uważane jest ono za zasadniczy element aktywnej i ofensywnej walki elektronicznej. Stanowi zasadniczo zespół przedsięwzięć ukierunkowanych na wytwarzanie różnorodnych zakłóceń w pracy środków radioelektronicznych przeciwnika. Zakłócenia te znajdują zastosowanie w systemach łączności radiowej i radioliniowej, radiolokacji, radionawigacji, naprowadzania rakiet, kierowania różnymi środkami walki itp.

W procesie przeciwdziałania realizuje się również zadania dezinformacji radiowej i maskowania przeciwradiolokacyjnego obiektów przez promieniowanie wtórne, zniekształcanie sygnałów, pochłanianie lub odbijanie energii elektromagnetycznej, imitację pracy środków radioelektronicznych oraz przekazywanie celowo fałszywych informacji.

13 Por. J. Janczak, *Zakłócanie informacyjne*, AON, Warszawa 2001.

Do przeciwdziałania elektronicznego służą różnego typu stacje zakłócające (stacjonarne i polowe) oraz stacje pokładowe montowane na samolotach, śmigłowcach, bezzałogowych statkach powietrznych i okrętach.

W systemie przeciwdziałania elektronicznego wykorzystuje się także różnego typu nadajniki zakłócające jednorazowego użytku. Na obszar zajmowany przez wojska ewentualnego przeciwnika mają być one wystrzeliwane za pomocą rakiet, artylerii, zrzucane z samolotów i śmigłowców oraz ustawiane ręcznie przez grupy specjalne, przede wszystkim w rejonie jego stanowisk dowodzenia, węzłów łączności i w rejony dyslokacji innych obiektów elektronicznych.

Analizując trendy technologiczne w konstrukcjach militarnych, można przypuszczać, że w działaniach zbrojnych będą wykorzystywane:

– naziemne stacje zakłóceń łączności radiowej, radioliniowej, stacje zakłóceń radiolokacyjnych i systemów pozycjonowania,

– naziemne stacje zakłóceń zapalników radiowych (zbliżeniowych) rakiet, bomb lotniczych, pocisków artyleryjskich oraz stacje zakłócające pokładową aparaturę radionawigacyjną,

– samolotowe i okrętowe stacje zakłóceń systemów radiolokacyjnych i łączności obrony powietrznej lotnictwa oraz wojsk lądowych,

– nadajniki zakłócające jednorazowego użytku o niewielkich gabarytach i stosunkowo małej mocy, od kilku do kilkudziesięciu watów.

Moc większości naziemnych stacji zakłócających jest stosunkowo duża i wynosi w zależności od rodzaju stacji kilkadziesiąt, kilkaset, a nawet kilka tysięcy watów. Wszystkie stacje są zuniwersalizowane. Wyposażono je w układy automatycznego poszukiwania środków radioelektronicznych przeciwnika.

Działanie środków zakłóceń elektronicznych jest integrowane z działaniem innej aparatury elektronicznej, przede wszystkim rozpoznawczej. Dąży się do wyposażenia wojsk w urządzeniu wielofunkcyjne, zdolne do wytwarzania różnego rodzaju zakłóceń oraz wykonywania jednocześnie kilku zadań przeciwko różnym systemom radioelektronicznym przeciwnika.

W celu skutecznego zakłócania środków i systemów radioelektronicznych przeciwnika bez narażania na zakłócenia własnych środków przewiduje się wykorzystanie znacznej liczby różnego typu nadajników zakłócających jednorazowego użytku. Mają one być zrzucane z samolotów (za pomocą automatów lub spadochronów) lub wystrzeliwane za pomocą rakiet i pocisków artyleryjskich. Tego rodzaju nadajniki zrzucano już z samolotów w czasie wojny w Wietnamie. Włączały się one automatycznie po zetknięciu z ziemią i zakłócały łączność radiową oraz pracę stacji radiolokacyjnych.

Zakłócanie pracy radiowych zapalników zbliżeniowych realizowane jest za pomocą specjalnych automatycznych stacji, które odbierają sygnały radiowych zapalników zbliżających się rakiet, bomb lotniczych, pocisków itp. i retransmitują je z większą mocą do danego środka rażenia, powodując w ten sposób wcześniejsze zadziałanie zapalnika, a tym samym wybuch rakiety, bomby czy pocisku.

Zakłócanie, stanowiące zasadniczy sposób przeciwdziałania elektronicznego, traktowane jest w nowoczesnych armiach jako niezmiernie ważny element walki elektronicznej, który uzupełnia niszczenie obiektów radioelektronicznych przeciwnika środkami rażenia. Analizując cele walki informacyjnej, można wywnioskować, że zakłócanie elektroniczne będzie prowadzone równocześnie w skali strategicznej, operacyjnej i taktycznej.

W skali strategicznej zakłócanie elektroniczne może przyjąć formę zmasowanego, aktywnego i ofensywnego oddziaływania radioelektronicznego, które zapoczątkuje działania zbrojne. Wykonywane ono będzie zwykle w celu stworzenia odpowiednich warunków do uderzeń siłami lotnictwa i przejścia wojsk lądowych do operacji zaczepnej. Stosowanie tej formy działań elektronicznych pozwala na uzyskanie przewagi elektronicznej (uniemożliwienie przeciwnikowi dostępu do spektrum EM[14]) w całym obszarze działań wojennych lub w jego części, obejmującej główne operacyjne kierunki działania wojsk.

Aktywne i zmasowane oddziaływanie radioelektroniczne będzie prawdopodobnie prowadzone kompleksowo, różnymi środkami technicznymi, za pomocą różnego rodzaju zakłóceń, dywersji oraz dezinformacji, a także przy wykorzystaniu broni wiązkowej. Można z dużym prawdopodobieństwem przyjąć, że w ramach operacji informacyjnych będzie ono wykonywane równocześnie z lądu, powietrza (Kosmosu) i morza na ważne, wyselekcjonowane obiekty i systemy radioelektroniczne rodzajów sił zbrojnych i rodzajów wojsk kilku szczebli dowodzenia jednocześnie. Działania te będą zwykle ściśle łączone z działaniami demonstracyjnymi, a następnie z faktycznym działaniem wojsk lądowych, uderzeniami wojsk rakietowych i artylerii, lotnictwa i sił morskich.

Z uwagi na zakres zadań oraz dużą ilość angażowanych sił i środków walki elektronicznej zmasowane oddziaływanie elektroniczne jest domeną planowania i organizowania walki elektronicznej na szczeblu strategicznym, dla osiągnięcia celów strategiczno-operacyjnych.

14 Por. K. Dymanowski, *Uniemożliwienie dostępu do spektrum elektromagnetycznego*, „Przegląd Sił Powietrznych" 2012, nr 1.

Operacje informacyjne obejmują swoim zakresem dwie formy oddziaływania na środki i systemy dowodzenia wojskami i kierowania środkami walki przeciwnika: zmasowane, nękające zakłócenia elektroniczne (zaporowe, dalekiego zasięgu, długotrwałe i bardzo silne[15]) na wyselekcjonowane ważne obiekty i systemy elektroniczne przeciwnika, z jednoczesnym stosowaniem dywersji i rozpowszechnianiem fałszywych informacji, oraz zmasowany atak elektroniczny na wybranych kierunkach działania.

Nękające oddziaływanie zakłóceniami ma na celu uśpienie czujności, rozproszenie uwagi i zmęczenie załóg dyżurnych określonych środków i obiektów w systemach elektronicznych przeciwnika, wprowadzenie w błąd oraz wymuszenie określonych reakcji ze strony dowództw i sztabów oraz podjęcie przez nich decyzji o znaczeniu strategiczno-operacyjnym.

Zakłócenia elektroniczne przewiduje się wykonywać wszystkimi posiadanymi środkami zakłócającymi i dywersyjnymi, w sposób zmasowany i dużą mocą – na głównych kierunkach operacyjnych, w celu okresowego uniemożliwienia przeciwnikowi dowodzenia wojskami i kierowania środkami walki oraz w celu uzyskania zaskoczenia i dominacji w spektrum elektromagnetycznym w wyznaczonej części obszaru działań zbrojnych.

Dla osiągnięcia celów strategiczno-operacyjnych przed rozpoczęciem konfliktu wojskowego i w trakcie jego trwania konieczne jest oddziaływanie dezinformacyjne zakłóceniami na obiekty i systemy elektroniczne obrony powietrznej, systemy kierowania i naprowadzania rakiet, na środki lotniczej i morskiej radionawigacji dalekiego i bliskiego zasięgu oraz na systemy łączności państwowej i wojskowej do szczebla operacyjnego przeciwnika.

Natomiast dla osiągnięcia celów operacyjno-taktycznych z chwilą przejścia do działań zbrojnych nieodzowne jest skupienie wysiłków oddziaływania elektronicznego na zakłócaniu środków i systemów radiolokacyjnych, radionawigacyjnych, łączności radiowej i radioliniowej zgrupowań uderzeniowych wojsk pancernych i zmechanizowanych, wojsk rakietowych i artylerii, lotnictwa i obrony powietrznej przeciwnika, przede wszystkim w strefie taktycznej i na głównych kierunkach działań wojsk.

Jak wskazują doświadczenia z ćwiczeń grupowych realizowanych w czasie studiów i kursów realizowanych w Akademii Obrony Narodowej, do najważniejszych zadań przeciwdziałania elektronicznego można zaliczyć:

15 Nazewnictwo zakłóceń użyto zgodnie z: *Walka elektroniczna* ..., dz. cyt., s. 34.

– zakłócanie pracy środków i relacji łączności radiowej i radioliniowej systemów dowodzenia wojskami i kierowania środkami walki oraz naprowadzania i radionawigacji lotnictwa,

– zakłócanie pracy pokładowych środków radiolokacyjnych (radiolokacyjne celowniki bombowe), radionawigacyjnych oraz łączności radiowej dowodzenia i naprowadzania lotnictwa przeciwnika,

– prowadzenie dezinformacji w systemach łączności i w innych systemach elektronicznych przeciwnika wykorzystywanych do dowodzenia wojskami i kierowania środkami walki oraz do naprowadzania i radionawigacji lotnictwa,

– zdalne detonowanie zakłóceniami elektronicznymi zapalników rakiet, pocisków i bomb lotniczych wyposażonych w radioelektroniczne zapalniki lub zdalnie sterowanych za pomocą fal radiowych,

– mylenie środków walki (rakiety, pociski, bomby) naprowadzających się na cel przy wykorzystaniu energii elektromagnetycznej.

Największą efektywność przeciwdziałania elektronicznego osiąga się przez kompleksowe wykonywanie różnego rodzaju zakłóceń w stosunku do najważniejszych środków i obiektów elektronicznych przeciwnika w sposób zmasowany, niespodziewany, na głównych kierunkach i w decydujących etapach działań bojowych. Wychodząc z tych założeń, na głównych kierunkach działań wojsk zasadne jest rozwinięcie większej ilości sił i środków rozpoznania i zakłóceń elektronicznych. Jest to niezbędne do wyeliminowania z przestrzeni walki ważnych środków elektronicznych przeciwnika i tym samym do stworzenia dogodnych warunków dla działań głównych zgrupowań wojsk lądowych i lotnictwa.

Przyjmuje się, że podczas walki informacyjnej obezwładnianie zakłóceniami elektronicznymi przy jednoczesnym stosowaniu dezinformacji powinno być wykonywane w sposób skoncentrowany, dużą mocą promieniowania energii elektromagnetycznej. Swoim zasięgiem powinno ono obejmować stanowiska dowodzenia, węzły łączności i ośrodki retranslacyjne, posterunki naprowadzania i powiadamiania oraz inne środki i obiekty elektroniczne jednocześnie dwóch albo trzech szczebli dowodzenia. Ponadto, w działaniach bojowych obezwładnianie zakłóceniami elektronicznym ma być ściśle skoordynowane z uderzeniami ogniowymi i działaniami wojsk pierwszego i drugiego rzutu, ponieważ tylko wówczas może ono doprowadzić do częściowej lub całkowitej dezorganizacji dowodzenia wojskami i kierowania środkami walki przeciwnika, a więc również stworzyć korzystne warunki do prowadzenia działań głównych sił wojsk lądowych, lotnictwa i desantów.

Odpowiednio zorganizowane i planowo prowadzone zakłócanie elektroniczne pozwala zdezorganizować pracę dużej liczby środków kilku systemów elektronicznych jednocześnie na bliskich, dalekich i bardzo dalekich odległościach.

Wynika to przede wszystkim z tego, że wraz z rozwojem techniki bojowej, a w szczególności środków elektronicznych, znacznie zwiększyły się możliwości obezwładniania zakłóceniami elektronicznymi. Należy jednak zaznaczyć, że stosując zakłócanie elektroniczne, nie zadaje się przeciwnikowi bezpośrednich strat materialnych, lecz dezorganizuje pracę jego środków i systemów wykorzystujących w swojej działalności energię elektromagnetyczną, pozbawiając go w ten sposób możliwości wymiany informacji. To z kolei uniemożliwia skoordynowane i operatywne dowodzenie wojskami i kierowanie środkami walki, co w następstwie może prowadzić do znacznych strat materialnych w sile żywej i sprzęcie bojowym. W rezultacie na określonych etapach działań bojowych może przyczynić się do uzyskania znacznej przewagi ogólnej nad przeciwnikiem.

Według teoretyków zajmujących się teorią nauk o obronności zakłócenia elektroniczne powinny być ściśle skoordynowane ze wsparciem ogniowym (wojsk rakietowych i artylerii, lotnictwa) oraz z działaniami głównych sił uderzeniowych wojsk pancernych i zmechanizowanych, desantów, grup uderzeniowych lotnictwa i sił morskich, jak również z osłoną ogniową realizowaną w czasie obrony powietrznej wojsk i obiektów.

O skuteczności zakłóceń elektronicznych prowadzonych w działaniach zbrojnych w ramach walki informacyjnej decyduje kilka czynników: przede wszystkim liczba i rodzaj posiadanych sił i środków rozpoznania oraz zakłóceń elektronicznych, ich parametry taktyczno-techniczne, stopień zautomatyzowania procesów rozpoznawczo-zakłóceniowych i zdalnego sterowania, rozmieszczenie sił i środków rozpoznania i zakłóceń, ich podporządkowanie organizacyjno-operacyjne, zdolności bojowe i taktyka ich użycia w walce i operacji.

Środki rozpoznania, zakłóceń i dezinformacji elektronicznej stosowane w celu uzyskania powodzenia w aktywnym oddziaływaniu elektronicznym oraz siły i środki walki elektronicznej powinny działać w ugrupowaniu bojowym związków taktycznych i oddziałów pierwszego rzutu, gdyż takie połączenie daje najpewniejsze i najwieksze rezultaty. W natarciu powinny one większość sił skierować na główne kierunki w celu osłabienia oporu broniących się wojsk, w obronie natomiast powinny oddziaływać na prawdopodobnych kierunkach głównego uderzenia przeciwnika z zadaniem obniżenia jego siły uderzeniowej.

Wnioski z ćwiczeń Pierścień (edycji 12, 13 i 14) realizowanych w Akademii Obrony Narodowej wskazują, że w działaniach bojowych lotnictwa taktycznego głównym celem realizowanych przedsięwzięć walki elektronicznej powinno być stworzenie korzystnych warunków do szybkiego przełamania obrony powietrznej przeciwnika. Siły i środki wydzielane do zakłócania środków radioelektronicznych systemu obrony powietrznej przeciwnika (stacji radiolokacyjnych i środków łączności) mogą wyprzedzać działania grup uderzeniowych lotnictwa lub działać w ugrupowaniu bojowym tych grup do strefy rażenia środków ogniowych obrony powietrznej strony przeciwnej. Taką taktykę działania lotniczych sił i środków walki elektronicznej stosowano w czasie wojny w Wietnamie, na Bliskim Wschodzie oraz w Zatoce Perskiej i na Bałkanach.

W wojnie wietnamskiej[16] amerykańskie lotnictwo wykorzystywało środki walki elektronicznej przede wszystkim do obezwładniania zakłóceniami środków radioelektronicznych systemów kierowania rakietami przeciwlotniczymi, lotnictwem myśliwskim, artylerią przeciwlotniczą, a także dla utrudnienia pracy lub wprowadzenia w błąd środków rozpoznania radiolokacyjnego systemu obrony powietrznej. Do tego celu używano środków zakłócających znajdujących się w samolotach grup uderzeniowych oraz specjalnych samolotów do walki elektronicznej wyposażonych w stacje zakłócające, a także w dipole odbijające i pułapki radiolokacyjne oraz pułapki pracujące na podczerwień. Lotnictwo taktyczne było zawsze wspierane przez samoloty grupy sił walki elektronicznej, przeznaczone przede wszystkim do obezwładniania zakłóceniami systemu rozpoznania radiolokacyjnego obrony powietrznej.

W wojnie na Bliskim Wschodzie[17] przed działaniem lotniczych grup uderzeniowych zwykle wykonywały swoje zadania siły i środki walki elektronicznej. Kilka minut przed uderzeniami grup lotniczych zakłócano środki radioelektroniczne obrony powietrznej państw arabskich, wykonywano uderzenia rakietami na wyselekcjonowane obiekty radioelektroniczne jednostek obrony powietrznej i baz lotnictwa myśliwskiego, a zakłócanie elektroniczne prowadzono za pomocą samolotów i śmigłowców walki elektronicznej, najczęściej ze stref nad terytorium opanowanym przez wojska izraelskie.

16 Por. V. Grankin, *Środki wojny radioelektronicznej i ich zastosowanie w wojnach lokalnych*, „Przegląd informacyjny ASG WP" 1972, nr 5, 38–45.

17 Tamże.

W przypadku osłony elektronicznej działań lotnictwa dużo uwagi poświęca się od niedawna zagadnieniu stosowania biernych (pasywnych) zakłóceń elektronicznych, wytwarzanych w stosunku do stacji radiolokacyjnych systemu obrony powietrznej przeciwnika za pomocą dipoli odbijających. Do zrzutu dipoli z samolotów używa się rakiet i wyrzutni dipoli o napędzie elektromechanicznym, pneumatycznym i pirotechnicznym. Ponadto urządzenia te pozwalają zrzucać pułapki na podczerwień (termiczne).

W systemie obrony elektronicznej wojsk lądowych szerokie zastosowanie mają różnego rodzaju odbijacze kątowe, maski i ekrany przeciwradiolokacyjne oraz pokrycia interferencyjne, które działają przede wszystkim przeciwko środkom rozpoznania radiolokacyjnego samolotów przeciwnika.

3.4. Obrona elektroniczna jako element walki informacyjnej

Obrona elektroniczna (w anglojęzycznej literaturze określana jako *Electronic Protective Measures* – EPM) stanowi zespół przedsięwzięć organizacyjno-technicznych zapewniających stabilną pracę własnym środkom i systemom elektronicznym podczas prowadzonej przez przeciwnika walki elektronicznej oraz w warunkach intensywnego użycia środków elektronicznych wojsk własnych[18]. Ukierunkowana jest na ochronę elektroniczną własnych środków i systemów dowodzenia wojskami i kierowania środkami walki przed przeciwdziałaniem i rozpoznaniem elektronicznym przeciwnika.

Obrona elektroniczna to forma walki elektronicznej, która zapewnia skuteczne wykorzystanie własnych środków radioelektronicznych w warunkach oddziaływania zakłóceniami i bronią wiązkową strony przeciwnej. Swoim zakresem obejmuje ona kompleks przedsięwzięć technicznych i taktyczno-organizacyjnych mających na celu ukrycie własnych środków i systemów radioelektronicznych przed rozpoznaniem elektronicznym przeciwnika, obniżenie skutków jego zakłóceń elektronicznych, uniknięcie uderzenia broni samonaprowadzającej na źródła promieniowania elektromagnetycznego, a także zapewnienie kompatybilności elektromagnetycznej.

Analiza rozwiązań teoretycznych i doświadczenie nabyte w pracy w jednostce radioelektronicznej pozwalają na wyciągniecie wniosku, że ukrywanie środków radioelektronicznych przed rozpoznaniem przeciwnika może zawierać

18 *Walka elektroniczna...*, dz. cyt., s. 10.

następujące elementy: maskowanie elektroniczne, kontrolę promieniowania elektromagnetycznego własnych środków elektronicznych, stosowanie środków pozoracji i mylenia elektronicznego, a także zapewnienie skrytości dowodzenia wojskami.

Skutki zakłóceń elektronicznych można zmniejszyć, wykrywając te zakłócenia i stosując przedsięwzięcia w celu zwiększenia trwałości i odporności własnych środków i systemów radioelektronicznych na zakłócenia przeciwnika.

Przedsięwzięcia techniczne w zakresie obrony elektronicznej wdrażane są do techniki wojskowej. Do konstrukcji urządzeń elektronicznych wprowadza się różne nowoczesne elementy, które pozwalają w jak największym stopniu eliminować ujemny wpływ zakłóceń. Najczęściej rozszerza się zakres częstotliwości roboczych oraz wbudowuje filtry przeciwzakłóceniowe.

Jak pokazują rozwiązania proceduralne, zadania w zakresie obrony elektronicznej realizuje się na każdym szczeblu dowodzenia, we wszystkich rodzajach sił zbrojnych i rodzajach wojsk. Za ich organizację odpowiedzialni są wszyscy dowódcy i sztaby dysponujące środkami radioelektronicznymi. Organizację, treść zadań oraz sposób ich wykonania wyszczególnia się w dokumentach bojowych określających działania wojsk. Można stwierdzić, że brak realizacji właściwych przedsięwzięć obrony elektronicznej może w znacznym stopniu wpłynąć na jakość prowadzonych działań bojowych i zmniejszyć efekty organizowanego przez wojska obezwładniania ogniowego oraz elektronicznego, a niekiedy nawet całkowicie je zniweczyć.

Przedsięwzięcia obrony elektronicznej realizowane są przez wojska w systemach łączności, we wszystkich zorganizowanych i czynnych systemach rozpoznania elektronicznego oraz radiolokacyjnych, radionawigacyjnych i sterowania środkami walki. Powinno się je przeprowadzać w ścisłym powiązaniu z niszczeniem środków rozpoznania i przeciwdziałania przeciwnika.

Realizację przedsięwzięć organizacyjnych i technicznych obrony elektronicznej dostosowuje się do rodzaju funkcji i zadań oraz właściwości działania poszczególnych środków i systemów radioelektronicznych, ich możliwości techniczno-eksploatacyjnych oraz do przestrzennego rozmieszczania eksploatowanych środków i elementów. Dąży się do tego, aby wszystkie wykonywane czynności, zarówno organizacyjne, jak i techniczne, zapewniły skrytość i ciągłość pracy własnych środków i systemów radioelektronicznych, co uzyskuje się m.in. przez eliminowanie lub skuteczne osłabianie aktywnego oddziaływania elektronicznego przeciwnika.

Potrzeby te uzasadnia się tym, że używany w wojskach sprzęt radioelektroniczny (radiowy, radioliniowy) nie jest w pełni odporny na zakłócenia. Analiza odporności łączności radiowej i radioliniowej wykazała, że najwrażliwsze

na zakłócenia są relacje łączności radiowej krótkofalowej na falach przyziemnych i odbitych od jonosfery o małym natężeniu pola elektromagnetycznego, a zwłaszcza środki łączności cyfrowej. Najmniej wrażliwe na zakłócenia są analogowe środki radiowe łączności fonicznej.

Ochronę własnych środków i systemów radioelektronicznych można zapewnić przez niszczenie wykrytych stacji zakłócających oraz nadajników zakłócających jednorazowego użytku zrzucanych lub wystrzeliwanych przez przeciwnika w rejony stanowisk dowodzenia, węzłów łączności i innych obiektów radioelektronicznych, jak również przez realizację kompleksowych przedsięwzięć obronnych o charakterze organizacyjno-technicznym.

Środki i systemy łączności przewiduje się chronić przed zakłóceniami elektronicznymi, podejmując na każdym szczeblu dowodzenia wiele przedsięwzięć organizacyjnych i technicznych obrony elektronicznej. Za najważniejsze przedsięwzięcia organizacyjne uważa się przydział dla relacji łączności częstotliwości roboczych, zapasowych i rezerwowych, tworzenie dublujących, rezerwowych i utajnionych kanałów łączności, wykorzystywanie okrężnych kanałów łączności i odpowiednio zorganizowanych punktów retransmisyjnych (siatkowy system łączności) oraz przekazywanie ważnych informacji jednocześnie na kilku różnych częstotliwościach lub w kilku różnych kanałach łączności.

Za najważniejsze przedsięwzięcia techniczne uważa się stosowanie:

- urządzeń przeciwzakłóceniowych,
- urządzeń automatycznego zdalnego przestrajania stacji,
- urządzeń tzw. szybkiej łączności,
- anten kierunkowych,
- odbioru informacji w wąskim paśmie przepuszczania częstotliwości odbiornika,
- odbioru informacji na kilku urządzeniach odbiorczych oddalonych od siebie,
- zmianę rodzajów pracy (modulacja, manipulacja),
- okresową zmianę polaryzacji anten.

Ochronę środków i systemów radiolokacyjnych w ramach obrony elektronicznej można zapewnić m.in. przez:

- wykorzystywanie stacji radiolokacyjnych o różnych parametrach technicznych,
- odstrajanie się od zakłóceń za pomocą aparatury przeciwzakłóceniowej,
- wprowadzenie ograniczeń pracy stacji radiolokacyjnych,
- unikanie zbędnego promieniowania energii elektromagnetycznej,
- wykorzystywanie właściwości naturalnych osłon terenowych.

Innym sposobem utrudniającym zakłócanie jest stosowanie wielu różnych stacji radiolokacyjnych o zsynchronizowanych sygnałach. Tego typu sieć radiolokacyjna mogłaby pracować mimo zakłóceń oraz wprowadzać w błąd system naprowadzający w rakietach przeciwradiolokacyjnych przeciwnika.

Obronę przed dezinformacją radiową może zapewnić zwiększenie czujności obsługi i załóg poszczególnych środków radioelektronicznych, umiejętność odróżniania pracy środków łączności przeciwnika od własnych, stałe sprawdzanie tożsamości korespondentów, ścisła kontrola treści odbieranych informacji oraz stosowanie technicznych urządzeń utajniających.

Podsumowując, zasady organizacji i prowadzenia walki elektronicznej stanowią uogólnienie doświadczeń wojennych. W zakresie prowadzenia walki informacyjnej można do nich zaliczyć:

- koncentrowanie wysiłków aktywnego i ofensywnego oddziaływania elektronicznego w odpowiednim miejscu i czasie na rozstrzygających kierunkach w stosunku do najważniejszych obiektów radioelektronicznych przeciwnika;
- kompleksowe oddziaływanie radioelektroniczne na środki dowodzenia wojskami przeciwnika przy pomocy nowoczesnego sprzętu rozpoznania, zakłóceń, dezinformacji (mylenia) oraz różnych form i metod prowadzenia aktywnych działań elektronicznych;
- konsekwentne dążenie do uzyskania zaskoczenia elektronicznego, aby w krótkim czasie osiągnąć zasadniczy cel walki elektronicznej – dominację w spektrum elektromagnetycznym;
- aktywne i ciągłe oddziaływanie elektroniczne na najważniejsze środki i systemy dowodzenia i kierowania środkami walki przeciwnika na głównych kierunkach działań wojsk i w decydujących etapach walki.

Częściową lub całkowitą dezorganizację dowodzenia wojskami i kierowania środkami walki przeciwnika można osiągnąć, przeciwstawiając mu lepsze techniczne uzbrojenie radioelektroniczne i większą ilość sił i środków walki elektronicznej, jak również nieprzerwanie oddziałując ofensywnie na jego radioelektroniczne systemy dowodzenia.

Ogromne nasycenie wojsk środkami radioelektronicznymi o różnym stopniu efektywności działania oraz różnorodność organizowanych i eksploatowanych w wojskach systemów radioelektronicznych świadczą o tym, że rola walki elektronicznej znacząco wzrosła w warunkach współczesnej walki informacyjnej.

Aktywne i ofensywne działania elektroniczne powinny być prowadzone na każdym szczeblu, w każdej operacji i na każdym kierunku operacyjnym, z koncentracją wysiłków sił i środków walki elektronicznej. W walce elektro-

nicznej wymagane jest ześrodkowywanie działań elektronicznych na najważniejszych kierunkach, jednocześnie w czasie i w przestrzeni, szybko i zdecydowanie, w ścisłej koordynacji z uderzeniami ogniowymi i działaniami wojsk. Odpowiednie ześrodkowanie wysiłku działań elektronicznych pozwala najracjonalniej i najefektywniej wykorzystać posiadany potencjał sił i środków walki elektronicznej.

W toku prowadzenia walki informacyjnej koncentrowanie wysiłków rozpoznania i przeciwdziałania elektronicznego wymaga doskonałej znajomości używanych w wojskach technicznych środków radioelektronicznych, zasad i właściwości ich eksploatacji oraz zasad organizacji i działania systemów dowodzenia wojskami oraz kierowania środkami walki przeciwnika, a także szczegółowej oceny sytuacji radioelektronicznej w przestrzeni walki, racjonalnego prognozowania zamiarów przeciwnika i odpowiedniego wyboru obiektów radioelektronicznych do obezwładnienia ogniowego i elektronicznego.

Kompleksowość oddziaływania elektronicznego powinna być ściśle przestrzegana podczas realizacji zadań rozpoznania, przeciwdziałania i obrony elektronicznej. Taka potrzeba wynika ze ścisłej współzależności, jaka istnieje między wszystkimi elementami walki elektronicznej. Umiejętne skorygowanie wszystkich przedsięwzięć oraz konsekwentna ich realizacja w czasie działań zbrojnych jest podstawowym warunkiem uzyskania powodzenia w prowadzeniu walki informacyjnej w działaniach militarnych.

W rozpoznaniu za nieodzowne uważa się zdobywanie danych o środkach, obiektach i systemach radioelektronicznych przeciwnika wszystkimi posiadanymi siłami i środkami rozpoznania elektronicznego. Zasadne jest ścisłe łączenie wysiłków potencjału rozpoznania elektronicznego z wysiłkami potencjału zakłóceń elektronicznych. Niezmiernie ważną rolę odgrywa również organizowanie wszechstronnego i stabilnego współdziałania elementów poszczególnych systemów rozpoznawczych z siłami i środkami obezwładniania ogniowego i elektronicznego.

W celu efektywnego wykonania zadań zakłócania elektronicznego zasadne jest kompleksowe wykorzystywanie różnorakich środków zakłócających, zdolnych do dezorganizowania pracy i działania jednocześnie kilku różnych systemów łączności przeciwnika, stosowanie różnego rodzaju zakłóceń oraz dezinformacji radiowej w różnych zakresach częstotliwości w stosunku do relacji łączności kilku szczebli dowodzenia jednocześnie. Nieodzowne jest też stosowanie w sposób kompleksowy naziemnych i powietrznych środków rozpoznania i zakłóceń elektronicznych oraz różnego typu nadajników zakłócających jednorazowego użytku.

Podczas prowadzenia walki informacyjnej związki taktyczne powinny posiadać takie wyposażenie do walki elektronicznej, aby były zdolne do zdezorganizowania pracy systemów łączności szczebla taktycznego wojsk lądowych przeciwnika. W dyspozycji związków operacyjnych natomiast powinny znajdować się takie siły i środki walki elektronicznej, które byłyby zdolne do wsparcia elektronicznego działań związków taktycznych oraz do efektywnego dezorganizowania pracy różnorakich systemów radioelektronicznych operacyjnego przeznaczenia wojsk lądowych, lotnictwa i sił morskich ewentualnego przeciwnika.

Zaskoczenie w walce elektronicnej można osiągnąć przez użycie większej liczby technicznych środków, zastosowanie nowych i nieznanych stronie przeciwnej urządzeń radioelektronicznych oraz rozpoczęcie i wykonanie w sposób nagły i nieoczekiwany zmasowanego obezwładniania elektronicznego w połączeniu z rażeniem ogniowym. Celem zaskoczenia elektronicznego powinno być nagłe sparaliżowanie w szerokim zakresie normalnego funkcjonowania systemów radioelektronicznych przeciwnika, a tym samym pozbawienie go możliwości dowodzenia wojskami i kierowania środkami walki, uniemożliwienie szybkiego i skutecznego działania jego wojskom, lotnictwu i środkom rażenia; stworzenie korzystnych warunków do działań własnych wojsk oraz uzyskania powodzenia przy minimalnych stratach.

Zjawiska towarzyszące zaskoczeniu umożliwiają uzyskanie przewagi i panowania w eterze. Zaskakujące, zmasowane obezwładnianie elektroniczne (w połączeniu z oddziaływaniem ogniowym), atak i uderzenia radioelektroniczne wykonywane z dużą mocą i różnymi środkami mogą przerwać dowodzenie wojskami przeciwnika, zdezorientować dowództwa oraz zmusić je do bezplanowego działania. Mogą zatem wytworzyć bardzo trudną i skomplikowaną sytuację, a tym samym już w początkowym okresie działań zbrojnych zadecydować o sukcesie.

Zaskoczenie radioelektroniczne może być także osiągnięte dzięki wprowadzeniu przeciwnika w błąd przez odpowiednio zorganizowane maskowanie wojsk i obiektów radioelektronicznych, dezinformację i pozorację elektroniczną, skrytość przygotowań do wykonania zadań zakłóceń elektronicznych.

Powodzenie w walce informacyjnej osiągnie ta strona, której oddziaływanie elektroniczne, prowadzone w ścisłej koordynacji z ogniem i uderzeniem wojsk, pod każdym względem będzie przemyślane i celowe, aktywne i zdecydowane, która będzie miała inicjatywę, narzucała przeciwnikowi swoją wolę, uprzedzała go w ofensywnych działaniach elektronicznych.

Przemyślane i celowe oddziaływanie elektroniczne polega na ścisłym powiązaniu i zgodności zadań rozpoznania, zakłóceń i dezinformacji elektronicznej z zamiarem prowadzenia działań bojowych, z zadaniami wojsk oraz na ścisłym skoordynowaniu wszystkich przedsięwzięć walki elektronicznej z uderzeniami ogniowymi wojsk rakietowych, artylerii i lotnictwa.

Na efektywność prowadzenia walki informacyjnej wpływa terminowość i szybkość oddziaływania elektronicznego na środki i systemy radioelektroniczne przeciwnika. Problem ten jest już szczegółowo rozpatrywany przy opracowywaniu wymagań taktycznotechnicznych dla wszystkich środków walki elektronicznej, a w szczególności dla środków rozpoznania i zakłóceń elektronicznych. Równie wnikliwie jest rozważany przy ustalaniu koncepcji strukturalno-funkcjonalnej systemu walki elektronicznej i wypracowywaniu taktyki działania wszystkich sił i środków wykorzystywanych w tym systemie. Terminowe i szybkie, a jednocześnie rozważne i zdecydowane oddziaływanie elektroniczne ma szczególnie duże znaczenie wtedy, kiedy czas determinuje ostateczne jego efekty.

Właściwości pracy oraz specyficzne cechy środków radioelektronicznych wykorzystywanych w systemach dowodzenia wojskami, kierowania środkami walki, naprowadzania i radionawigacji nakazują, aby czas od momentu wykrycia środka radioelektronicznego przeciwnika lub emitowanego w eter sygnału (informacji) do chwili zareagowania aktywnymi, skutecznymi zakłóceniami był bardzo krótki. W większości wypadków po wykryciu pracujących środków radioelektronicznych lub relacji łączności reakcja zakłóceniami powinna być natychmiastowa.

Ważnym elementem w walce elektronicznej jest manewr radioelektroniczny siłami i środkami dowodzenia wojsk, wykonywany w ramach obrony elektronicznej. Ma on na celu zmniejszenie efektywności rozpoznania, zakłóceń i dezinformacji elektronicznej w systemach dowodzenia wojsk własnych.

Zakończenie

Termin „walka informacyjna" jest bardzo pojemny i obejmuje elementy konfliktu zbrojnego, konfliktów asymetrycznych, protestów społecznych i przestępczości, działań politycznych i propagandowych, a nawet działań frustratów i wandali. Jednakże wszystkie te przejawy ludzkiej aktywności można sprowadzić do wspólnego mianownika: istnienia konfliktu rozstrzyganego za pomocą informacji traktowanej jako broń skierowana przeciwko zasobom informacyjnym strony przeciwnej przy jednoczesnej obronie własnych zasobów informacyjnych.

Na przykładzie pierwszej wojny w Zatoce Perskiej można wnioskować, że prowadzenie operacji psychologicznych jest jednym z kluczowych narzędzi walki informacyjnej. Konflikt ten dowiódł, że o odniesieniu sukcesu w walce zbrojnej decyduje w głównej mierze walka informacyjna. Walka ta jest prowadzona niekiedy na długo przed rozpoczęciem działań zbrojnych. Szczególne miejsce poświęcono walce informacyjnej w aktualnie trwającym konflikcie na Ukrainie, wskazując ją jako przykład walki informacyjnej XXI wieku.

W warunkach współczesnej walki informacyjnej wzrasta rola walki elektronicznej. Spowodowane jest to ogromnym nasyceniem pola walki środkami radioelektronicznymi o różnym stopniu efektywności działania oraz różnorodność organizowanych i eksploatowanych w wojskach systemów radioelektronicznych. Walka elektroniczna ma szerokie zastosowanie w operacjach militarnych. Wykorzystując siły i środki walki elektronicznej można osiągnąć efekty negatywne dla przeciwnika, ograniczające lub uniemożliwiające użycie przez niego własnych środków elektronicznych. Walka elektroniczna wspiera swoimi działaniami również inne działania prowadzone w ramach walki informacyjnej, a w szczególności działania dezinformacyjne i operacje psychologiczne.

Bibliografia

A. Publikacje zwarte

1. *AAP-6, Słownik terminów i definicji NATO*, Agencja Standaryzacyjna NATO, 3 kwietnia 2013.
2. Aleksandrowicz T., *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
3. *Allied Joint Doctrine for Information Operations AJP-3.10*, NSA, November 2009.
4. Balcerowicz B., *Pokój i „nie-pokój" na progu XXI wieku*, Bellona, Warszawa 2002.
5. Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Wydawnictwo Naukowe Scholar, Warszawa 2010.
6. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005.
7. Bielecki R., *Pustynna Burza*, Bellona, Warszawa 1991.
8. Biziewski J., *Pustynna Burza*, cz. 2, Altair, Warszawa 1994,
9. Bolechów B., *Terroryzm. Aktorzy, statyści, widownie*, PWN, Warszawa 2010.
10. Borowiecki R., Kwieciński M. (red.), *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (wybrane problemy teorii i praktyki)*, Kantor Wydawniczy Zakamycze, Kraków 2003.
11. Brzeski R., *Wojna informacyjna – wojna nowej generacji*, Antyk, Warszawa 2014.
12. Cebrowski A., Garstka J., *Network Centric Warfare – Its Origins and Future*, US Naval Institute Proceedings, Annapolis, January 1998.
13. Ciborowski L., *Walka informacyjna*, Adam Marszałek, Toruń 2001.
14. Czarny E. (red.), *Globalizacja od a do Z*, NBP, Warszawa 2004.
15. Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.

16. Dobek-Ostrowska B., Kuś M. (red.), *Hiszpania: media masowe i wybory w obliczu terroryzmu*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2007.
17. *Doktryna Działań Połączonych D/01 (C)*, Szt. Gen. WP, Warszawa 2009.
18. *Doktryna Rozpoznanie wojskowe D/2*, Szt. Gen., Warszawa 2013.
19. *Doktryna systemów łączności i informatyki Sił Zbrojnych RP D/6*, CDiS SZ, Bydgoszcz 2013.
20. *Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP DD/9*, Szt. Gen. WP, Warszawa 2004.
21. *Encyklopedia powszechna PWN*, t. 2, PWN, Warszawa 1974.
22. Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, AON, Warszawa 2003.
23. Haber L. (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość*, BG AGH, Kraków 2004.
24. Huzarski M., Wołejszo J. (red. nauk.), *Leksykon obronności. Polska i Europa*, Bellona, Warszawa 2014.
25. Janczak J., *Współczesne koncepcje walki informacyjnej*, AON, Warszawa 2002.
26. Janczak J., *Zakłócanie informacyjne*, AON, Warszawa 2001.
27. *Joint Doctrine for Information Operations*, *JP 3-13*, Joint Chiefs of Staff, 9 October 1998.
28. Joniak J., Polak A., *Wojny w Zatoce Perskiej aspekty operacyjne*, AON, Warszawa 2011.
29. Kołodko G.W., *Polska z globalizacją w tle. Instytucjonalne i polityczne aspekty rozwoju gospodarczego*, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 2007.
30. *Koncepcja komunikacji strategicznej w Siłach Zbrojnych RP*, CDiS SZ, Bydgoszcz 2013.
31. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980.
32. Kotarbiński T., *Traktat o dobrej robocie*, wyd. 3, popr. i uzupeł., Ossolineum, Wrocław – Warszawa – Kraków 1965.
33. Kowalczyk K., Wróblewski W. (red.), *Oblicza współczesnego terroryzmu*, Toruń 2006.
34. Koziej S., *Teoria sztuki wojennej*, wyd. 2, Bellona, Warszawa 2011.
35. Kuźniar R., Lachowski Z. (red.), *Bezpieczeństwo międzynarodowe czasu przemian: zagrożenia – koncepcje – instytucje*, Warszawa 2003.
36. Madej M., Terlikowski M. (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
37. Lasota J., *Asymetria w walce zbrojnej*, AON, Warszawa 2014.

38. *Leksykon wiedzy wojskowej*, MON, Warszawa 1979.
39. Liedel K., Mocek S., *Terroryzm w medialnym obrazie świata*, Trio, Warszawa 2010.
40. Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Difin, Warszawa 2012.
41. Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Polski Instytut Spraw Międzynarodowych, Warszawa 2007.
42. Modrzejewski Z., *Operacje psychologiczne w konfliktach po II wojnie światowej*, AON, Warszawa 2002.
43. Modrzejewski Z., *Operacje informacyjne*, AON, Warszawa 2015.
44. Nowacki G., *Współczesne poglądy na prowadzenie walki informacyjnej*, AON, Warszawa 2001.
45. Nye J.S., *Konflikty międzynarodowe. Wprowadzenie do teorii i historii*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.
46. *Operacja „Iracka wolność"*, AON, Warszawa 2003.
47. *Operacje psychologiczne DD/3.10.1(A)*, Szt. Gen. WP, Warszawa 2010.
48. Płudowski T. (red.), *Terrorism, Media, Society*, Adam Marszałek, Toruń 2006.
49. *PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, PKN, Warszawa 2007.
50. Podkowski A., *Działania psychologiczno-propagandowe w walce zbrojnej*, AON, Warszawa 1993.
51. *Priorytetowe zadania modernizacji technicznej sił zbrojnych Rzeczypospolitej Polskiej w ramach programów operacyjnych*, Uchwała Nr 123 Rady Ministrów z dnia 23 czerwca 2014 r., Monitor Polski, poz. 558.
52. Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław – Warszawa – Kraków – Gdańsk 1978.
53. Rattray G.J., *Wojna strategiczna w cyberprzestrzeni*, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
54. Rokiciński K., Pac B., *Operacje informacyjne w działaniach militarnych*, Akademia Marynarki Wojennej, Gdynia 2010.
55. Rudziński K., *Zagrożenia sieciocentryczne*, prezentacja w AON, Warszawa 2006.
56. Sun Tzu, *Sztuka wojny*, wyd. 2, Helion, Gliwice 2008.
57. Szpyra R., *Militarne operacje informacyjne*, AON, Warszawa 2003.
58. *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA*, Vis-a-vis Etiuda, Kraków 2010.

59. *Walka elektroniczna*, MON, Warszawa 2003.
60. Volkoff V., *Dezinformacja - oręż wojny*, Delikon, Warszawa 1991.
61. Wrzosek M., *Dezinformacja jako komponent operacji informacyjnych*, AON, Warszawa 2005.

B. Artykuły

1. Chojnacki Z., Dymanowski K., Molenda J., *Operacje militarne w cyberprzestrzeni*, „Kwartalnik Bellona" 2007, nr 1.
2. Czulda R., *Media a sukces operacji zbrojnej*, „Przegląd Wojsk Lądowych" 2008, nr 9.
3. Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku*, „Punkt widzenia" nr 42, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2014.
4. Darczewska J., *Rosja zbroi się do wojny informacyjnej z Zachodem*, „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa", październik-grudzień 2014, nr 9.
5. *Doktryna systemów łączności i informatyki Sił Zbrojnych RP D/6*, CDiS SZ, Bydgoszcz 2013.
6. Dymanowski K., *Uniemożliwienie dostępu do spektrum elektromagnetycznego*, „Przegląd Sił Powietrznych" 2012, nr 1.
7. Dymanowski K., *Zmiany w koncepcji walki elektronicznej NATO*, „Przegląd Sił Powietrznych" 2009, nr 11.
8. Gałązka M., *Zasady prowadzenia walki informacyjnej*, „Kwartalnik Bellona" 2007, nr 1.
9. Grankin V., *Środki wojny radioelektronicznej i ich zastosowanie w wojnach lokalnych*, „Przegląd informacyjny ASG WP" 1972, nr 5.
10. Huzarski M., *Istota wojny (walki) sieciocentrycznej*, „Zeszyty Naukowe AON" 2007, nr 3.
11. Koziej S., *Czynniki walki zbrojnej*, „Zeszyty Naukowe AON" 1993, nr 4.
12. Kręcikij J., *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" 2006, nr 4.
13. Kwiecień M., *Działania psychologiczne Armii Stanów Zjednoczonych*, „Przegląd Wojsk Lądowych" 1997, nr 11.
14. Lemanowicz P., Boguszewicz I., *Działania psychologiczne w Zatoce Perskiej*, „Wojsko i Wychowanie" 1996, nr 10.
15. Liedel K., Piasecka P., *Wojna cybernetyczna - wyzwania XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1/17.

16. Miller A., *Rola i zadania CIMIC w operacjach na Bałkanach*, „Zeszyty Naukowe AON" 2012, nr 4.
17. Piątkowski K., *Wojna nowego typu?*, „Polska w Europie" marzec 2002, nr 1.
18. Podkowski A., *Rodzaje działań psychologicznych na polu walki*, „Zeszyty Naukowe AON" 1997, nr 1.
19. *Rosja zbroi się do „wojny informacyjnej" z Zachodem*, „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa" październik–grudzień 2014, nr 9.
20. Ryżewski L., *Obraz komunistycznej ofensywy w amerykańskich mediach*, „Studia Medioznawcze" 2009, nr 1.
21. Sienkiewicz P., *Informatyczne wspomaganie dowodzenia*, „Myśl Wojskowa" 1993, nr 1.
22. Sikora S., *Działania psychologiczne w operacji „Pustynna Burza"*, „Wojsko i Wychowanie" 1993, nr 4.
23. Szubrycht T., *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, „Zeszyty Naukowe AMW" 2006, nr 1.
24. Wiśnicki J., *Ochrona wojsk w operacji*, „Raport, Wojsko, Technika, Obronność" 2014, nr 7.
25. Wrzosek M., *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2.

C. Strony internetowe

1. *Encyklopedia PWN*, http://encyklopedia.pwn.pl/haslo/3905881/globalizacja.html [dostęp: 15.01.2015].
2. Kossecki J., *Totalna wojna informacyjna XX wieku a II RP*, Kielce 1997, socjocybernetyka.files.wordpress.com/.../totalna-wojna-informacyjna.pdf [dostęp: 1.01.2015].
3. Koziej S., *Triada globalnych zagrożeń asymetrycznych: konsekwencja proliferacji terroryzmu, broni nuklearnej i technologii rakietowych*, www.bbn.gov.pl [dostęp: 9.02.2015].
4. Lekowski M., *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*, www.bbn.gov.pl/download/1/8617/265-283MaciejLekowski.pdf [dostęp: 10.01.2015].
5. Marciniak M., *Prawdy i mity o chińskich hakerach*, „Computer World" z 19.10.2011, http://www.computerworld.pl [dostęp: 19.04.2012].
6. Metz S., Johnson II D.V., *Asymmetry and U.S. Asymmetry and U.S. Military strategy*, http://www.strategicstudiesinstitute.army.mil [dostęp: 12.08.2010].

7. Pachucki J., *Rosyjska wojna informacyjna w kontekście aneksji Krymu*, http://www.debata.olsztyn.pl/wiadomoci/polska/3646-rosyjska-wojna-informacyjna-w-kontekscie-aneksji-krymu-kafelek.html [dostęp: 2.01.2015].
8. *Polacy protestowali przeciwko wizycie Poroszenki? Rosyjskie media okłamują obywateli*, http://swiat.newsweek.pl [dostęp: 17.12.2014].
9. Polski problem globalizacji Europy, http://www.bryk.pl [dostęp: 9.02.2015].
10. *Rosja zbroi się do „wojny informacyjnej" z zachodem*, „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa", październik–grudzień 2014, nr 9, rcb.gov.pl/wp-content/uploads/biuletyn/9.pdf [dostęp: 14.01.2015].
11. Sokała W., Zapała B. (red. nauk.), *Asymetryczność i hybrydowość – stare armie wobec nowych konfliktów*, Biuro Bezpieczeństwa Narodowego, www.bbn.gov.pl [dostęp: 16.01.2015].
12. *Ukraina polem cyberwojny: warunki dyktuje Moskwa*, http://www.defence24.pl [dostęp: 19.01.2015].
13. *Wojna informacyjna na Ukrainie*, http://www.rp.pl/artykul/1117754.html [dostęp: 18.01.2015].
14. *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów – raport*, http://www.defence24.pl/299734,wojna-informacyjna-jako-skuteczne-narzedzie-destabilizacji-panstw-i-rzadow-raport [dostęp: 3.02.2016].
15. Wojtunik P., *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, www.bbn.gov.pl/download/1/1967/zeszyt9wojtunik.pdf [dostęp: 22.02.2015].
16. *Wpływ globalizacji i regionalizacji na bezpieczeństwo międzynarodowe*, http://stosunki-miedzynarodowe.pl [dostęp: 15.01.2015].
17. www.e-debiuty.byd.pl/file/rznnonhy6wpijz7/PDF/chorobinski.pdf [dostęp: 2.01.2015].
18. http://dziennikzbrojny.pl/artykuly/art,5,23,3423,wojska-ladowe,wyposazenie,radar-rozpoznania-artyleryjskiego-liwiec [dostęp: 15.10.2014].
19. http://sjp.pl/asymetria [dostęp: 8.09.2014].
20. http://wiadomosci.onet.pl/swiat/tajemnicza-operacja-wojskowa-u-wybrzezy-szwecji-zatonal-rosyjski-okret-podwodny/8bh1x [dostęp: 20.11.2014].
21. http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosyjski-okret-szpiegowski-pod-nosem-usa,402937.html [dostęp: 20.14.2014].
22. http://www.tvp.info/17449694/niespotykana-skala-aktywnosci-rosyjskiego-lotnictwa-nad-europa-nato-zaniepokojone [dostęp: 15.11.2014].

Spis rysunków i tabel

Rysunki

Tabele

WYDAWNICTWO

e-mail: wydawnictwo@aon.edu.pl

tel. 261 813 671, tel./fax 261 813 752

KSIĘGARNIA

e-mail: ksiegarnia.akademicka@aon.edu.pl

261 814 608
261 814 055

SKLEP INTERNETOWY

www.ksiegarnia.aon.edu.pl

al. gen. A. Chruściela 103, 00-910 Warszawa

ISBN 978-83-7523-513-5

WYDAWNICTWO
AON