Journal of KONBiN 3(19) 2011
ISSN 1895-8281

THE AUTOMATION OF ELECTRONIC EQUIPMENT IN CYBERSPACE AND ELECTRONIC WARFARE

AUTOMATYZACJA DZIAŁAŃ URZĄDZEŃ ELEKTRONICZNYCH W ŚRODOWISKU CYBERPRZESTRZENI I WALKI ELEKTRONICZNEJ

Waldemar Scheffs

National Defense University, Akademia Obrony Narodowej
w.scheffs @aon.edu.pl

***Abstract**: The rapid technological advancement of IT engineering has given rise to clandestine and intense war in the electromagnetic and IT environment. A signal transmitted simultaneously to a large number of receivers has become a tool to wage this kind of war. The signal itself is devoid of power and mass.*
New technologies have given rise to new potential areas of warfare. Cyberspace is the most telling example of an artificially created environment. This new warfare environment has been claiming an ever larger proportion in the ways of sending and receiving information command, reconnaissance electronic war, among many others. The article mentions topics closely connected with the automation of electrical devices operating under two different conditions: cybernetic and electromagnetic. One dovetails with the other and both could use the same type of equipment, yet their functions differ.

***Keywords:** cybernetic and electromagnetic environment, automation*

***Streszczenie:** Nowe technologie stały się czynnikami, który powodują, że od momentu ich powstania w środowiskach elektromagnetycznym i informacyjnym trwa cicha i intensywna wojna. Narzędziem prowadzenia tej wojny jest informacja przesyłana za pomocą sygnałów do wielu różnych odbiorców. Technologie wykreowały nowe środowiska działań. Środowisko cyberprzestrzeni jest tu przykładem sztucznie stworzonego środowiska walki. Staje się główną płaszczyzną przekazywania informacji w dowodzeniu, rozpoznaniu, walce elektronicznej, artylerii i wielu innych gałęziach działania wojsk. W referacie poruszane są kwestie zawiązane z automatyzacją działania urządzeń elektronicznych pracujących w dwóch różnych środowiskach: informatycznym, (cybernetycznym) i elektromagnetycznym. Oba środowiska pracy zazębiają się i mogą wykorzystywać te same urządzenia, ale ich funkcje są różne.*

***Słowa kluczowe:** środowisko cybernetyczne, elektroniczne, automatyzacja*

1. Wprowadzenie

Rewolucja techniczno-naukowa jaką obserwujemy od połowy XX wieku stała się wyznacznikiem rozwoju wielu działów nauki i gałęzi przemysłu. Tak gwałtowny rozwój świata industrialnego cechuje się szerokim wytwarzaniem i konsumpcją wszelkich dóbr wyprodukowanych przez człowieka i tych eksploatowanych w czystej postaci surowcowej. Urządzenia elektroniczne zdominowały nie tylko życie człowieka ale cały przemysł, którego część wojskowa zajmuje pokaźne miejsce. Aktualnie wielu naukowców skłania się do stwierdzenia, że elektronika i informatyka to nowi członkowie społeczności ludzkiej.
Technika wojskowa z okresu II wojny światowej rozwijała się, jak na tamte czasy szybko. Urządzenia elektroniczne, były bardzo nowoczesne, (lamy elektronowe tj. triody, pentody to bardzo duże osiągnięcia naukowe) ale mające swoje ograniczenia, głównie energetyczne (duża moc zasilania) i gabarytowe . Pierwszy przełom następuje z chwilą opracowania naukowego i w konsekwencji skonstruowania lampy magnetronowej wykorzystywanej w radiolokatorach. Prawdziwa rewolucja techniczna następuje jednak po zakończeniu II wojny światowej. Tranzystor i układ scalony są wyznacznikami wielkiego bumu elektronicznych układów o różnym przeznaczeniu. Wojsko, bardzo szybko dostrzega potęgę elektroniki i silnie wprzęga ją do swoich zastosowań, na początku głównie w lotnictwie i wojskach rakietowych. Jednocześnie nie zapomina o innych rodzajach wojsk i służb. Bardzo szerokie zastosowanie urządzenia elektroniczne znajdują w systemach łączności, rozpoznania, walki elektronicznej, obronie przeciwlotniczej, artylerii. Coraz powszechniej urządzenia elektroniczne stosuje się w pojazdach bojowych (czołgach, wozach opancerzonych lub pojazdach kołowych). Dzisiejsze samoloty w technologii stelth to „latający komputer-robot" sterowany przez człowieka. W niedalekiej przyszłości może na wzór BŚR podobne samoloty będą wykonywały zadania bojowe[1].
Obszar powietrzny to nie jedyny, w którym urządzenia elektroniczne zdominowały działania wojska. Marynarka Wojenna z okrętami nawodnymi i podwodnymi stanowi kolejny przykład metalowych kolosów naszpikowanych urządzeniami sterowania środkami rażenia, dowodzenia, rozpoznania, łączności, walki elektronicznej, kierowania jednostką. Każdy okręt bez względu, czy nawodny, czy podwodny to pływająca twierdza broniąca się samodzielnie lub w grupie, zdolna wykryć, rozpoznać i zniszczyć cel oddalony o wiele kilometrów. Okręty dysponują najnowocześniejszą techniką elektroniczną i informatyczną, stanowią dobitny przykład wykorzystania najnowszych zdobyczy techniki elektronicznej w praktycznych zastosowaniach. Dzisiaj bez urządzeń elektronicznych i starowania komputerami niemożliwe byłyby loty w przestrzeń kosmiczną. Niedawny wylot ostatniego amerykańskiego wahadłowca Atlantis (lipiec 2011) nie kończy ery

[1] Aktualnie bezpilotowe środki lotnicze głównie wykonują zadania rozpoznawcze. Niemniej zdarzają się przypadki przenoszenia przez BŚL pocisków rakietowych i bomb.

podboju kosmosu. Jest tylko zakończeniem pewnego etapu, w którym elektroniczka i informatyka odegrała dominującą rolę.
Nie możemy zapominać także o technice wojskowej na ziemi. Stalowe rumaki to dzisiaj jeżdżące roboty, w których urządzenia elektroniczne stanowią podstawę celnego ognia do wykrytych celów. Załoga zaopatrzona jest najnowocześniejsze zdobycze techniczne umożliwiające pokonanie przeciwnika na odległościach będących poza zasięgiem jego ognia.
Na koniec, a może powinno się wymienić na początku jest człowiek-żołnierz. Dzisiejszy wojownik to może jeszcze nie cyberwojownik, ale jest już na tyle bogato wyposażony w urządzenia elektroniczne, że śmiało można powiedzieć że urządzenia elektroniczne zaczęły dominować w jego wyposażeniu. Pomimo, iż nadal broń osobista jest podstawowym elementem wyposażenia żołnierza to coraz częściej mówi się o terminalach komputerowych pozwalających szybciej dowodzić, przekazać informację, rozpoznać przeciwnika i celnie prowadzić ogień, będąc samemu niewidocznym dla strony przeciwnej.
Wszystkie wymienione zastosowania urządzeń elektronicznych i informatycznych pracują w środowisku elektronicznym, elektromagnetycznym lub informatycznym albo w wszystkich jednocześnie. Wszystkie można rozpoznać i zakłócić energią elektromagnetyczną lub sygnałem niosącym program infekujący system informatyczny. Problemem jest identyfikacja urządzeń tych które pracują dla systemów walki elektronicznej i tych które można wykorzystać w środowisku informatycznym. Urządzenia elektroniczne jako element materii nieożywionej można poddać automatyzacji działania, ale należy wiedzieć, które i w jakiej kolejności oraz na czyją korzyść działają. Tym zagadnieniom poświęcony jest ten artykuł.
Pierwsze dwa rozdziały artykułu dotyczą wykorzystania urządzeń elektronicznych w środowisku elektromagnetycznym używanym przez systemy walki elektronicznej i w środowisku cybernetycznym. Treści tych rozdziałów egzemplifikują możliwości identyfikacji urządzeń elektronicznych możliwych do zastosowań w obu środowiskach będąc tym samym urządzeniem ale spełniającym różną funkcję.

2. Działania w środowisku walki elektronicznej

2.1 Fale elektromagnetyczne środowiskiem walki

Jeszcze stosunkowo niedawno, zakres światła widzialnego, był jedynym z całego widma elektromagnetycznego, z którego człowiek nieświadomie korzystał dzięki oczom, w które wyposażyła go natura. Na polu walki, zakres światła widzialnego początkowo był wykorzystywany do zdobywania informacji przez obserwację (stosowane zresztą do dzisiaj) oraz do przekazywania ustalonych sygnałów świetlnych, dymnych itp. Jednak zarówno te pierwsze, wzrokowe wykorzystanie widma jak i późniejsze środki łączności przewodowej, miały ograniczony zasięg i przywiązywały system transmisji do określonych punktów (urządzenia końcowe) i linii (odcinki przekazu). Dopiero odkrycie fal radiowych umożliwiło późniejsze,

pełne wykorzystanie przestrzeni elektromagnetycznej i doprowadziło do konfrontacji w tym wymiarze.

Elektromagnetyczny wymiar konfrontacji rozpoczął się pod sam koniec XIX wieku z chwilą skonstruowania pierwszych telegrafów i przesłania użytecznych sygnałów drogą radiową. Główne formy wojny w spektrum fal radiowych kształtowały się na początku XX wieku, kiedy technika osiągnęła poziom umożliwiający wykorzystanie radia do celów wojskowych. Prawie jednocześnie z użyciem radia do celów łączności wojskowej, rozpoczęła się walka w przestrzeni elektromagnetycznej. Początkowo walka sprowadzała do przechwytywania i rozszyfrowania informacji przesyłanych drogą radiową oraz wysyłania w eter sygnałów zakłócających emisje przeciwnika.

Wraz z przyspieszonym rozwojem radiokomunikacji, pojawiły się nowe formy tej „niewidzialnej" wojny między innymi takie jak: nowe, różne od poprzednich, metody radioelektronicznego rozpoznania i przeciwdziałania, radiolokacja oraz ofensywna propaganda radiowa.

W okresie międzywojennym ogromny postęp w dziedzinie radioelektroniki, nie znalazł odzwierciedlenia ani w rozwoju technicznych środków walki, ani w doskonaleniu form i metod jej prowadzenia w wymiarze elektromagnetycznym. Tak jak podczas I wojny światowej, główną sferą konfrontacji było rozpoznanie i dezinformacja radiowa, głównie w paśmie KF, to w czasie II Wojny Światowej dopiero po roku 1940, nastąpił gwałtowny rozwój środków i form walki w przestrzeni elektromagnetycznej, po obu stronach frontu.

Alianci, realizując badania w ramach specjalnych programów naukowych i technologicznych, dostarczali wojskom znaczne ilości nowoczesnego sprzętu rozpoznania i zakłóceń, zdolnego do pracy na różnych częstotliwościach oraz do wytwarzania zakłócającej energii elektromagnetycznej o znacznych mocach.

Niemcy i pozostałe państwa osi, w badaniach rozwojowych koncentrowali swoje wysiłki na pracach związanych z obroną przed rozpoznaniem i zakłóceniami. Tą drogą starali się zachować żywotność swoich środków i systemów radioelektronicznych[2].

Po zakończeniu działań II wojny światowej, w pracach nad doskonaleniem techniki i form prowadzenia walki elektronicznej szeroko wykorzystywano doświadczenia wojen lokalnych: Korea (1950-1953), Wietnam (1964-1973), Bliski Wschód (1967, 1973, 1981), działania wojenne o Falklandy - Malwiny (1982), Zatoka Perska (1990-1991), (2001), Jugosławia (1999).

Wymienione konflikty ukształtował jej obecny charakter. Działania w środowisku fal EM ugruntowały swoją dominację zmagań w środowisku powietrznym i morskim a następnie kosmicznym. Takie podejście jest bardzo wyraźnie uwidocznione w zachodnim postrzeganiu wykorzystywania systemów WE. W poglądach wschodnich ówczesnych przeciwników z okresu zimnowojennego, urządzenia elektroniczne wykorzystywano w środowisku lądowym, a dopiero

[2] A. Price, *Narzędzia mroku*, Wydawnictwo Dolnośląskie, Wrocław 2006.

później w powietrznym i morskim. Proporcje instalowania i taktyki wykorzystywania tych urządzeń są widoczne do czasów obecnych. Przyczyn takiego zróżnicowanego podejścia do działalności systemów i urządzeń elektronicznych (w tym głównie WE) należy upatrywać w doświadczeniach wyniesionych z okresu II wojny światowej, gwałtownemu rozwojowi nauki i nowych technologii w państwach zachodnich oraz rozpoczęciu wyścigu zbrojeń, w której armia Stanów Zjednoczonych i pozostałe państwa NATO, dążyli do roli dominującej w świecie i potrzebowali systemów zdolnych do rozpoznawania przeciwnika z bardzo dużych odległości. Do roli dominującego środka rozpoznawczego nadawały się wówczas tylko samoloty dalekiego zasięgu i o rozpoznaniu kosmicznym dopiero myślano. Strategiczne rozpoznanie USA wyznaczyło kierunki rozwoju urządzeń elektronicznych, w tym urządzeń rozpoznawczych i zakłócających. Rozpoznanie na bardzo duże odległości z możliwością jednoczesnego zakłócania a także utrzymywanie łączności w każdym zakątku globu to podstawa rozwoju nowych technik i technologii w budowie i wykorzystaniu urządzeń elektronicznych. Środowisko fal EM stało się oczywistą domeną wyścigu zbrojeń cichej walki.

2.2 Działania systemów walki elektronicznej w środowisku fal elektromagnetycznych

Zgodnie z przyjętymi założeniami doktrynalnymi, konfrontacja w wymiarze środowiska fal elektromagnetycznych jest prowadzona we wszystkich rodzajach działań bojowych i ma powszechny charakter. Główny ciężar tych zmagań spoczywa na wyspecjalizowanych jednostkach, wyposażonych w urządzenia rozpoznania, zakłóceń oraz obrony elektronicznej.

Walka elektroniczna funkcjonuje w środowisku elektromagnetycznym a zatem "obszarem[3] działania WE jest przestrzeń elektromagnetyczna oraz środki radioelektroniczne[4] promieniujące i odbierające energię elektromagnetyczną". Środowisko WE cechuje się: zakresem wykorzystywanego widma fal elektromagnetycznych, gęstością wykorzystywanych częstotliwości, gęstością (mocą) energii EM w przestrzeni, gęstością pracy urządzeń radioelektronicznych (Re) na km^2, rozkładem dyslokacji poszczególnych urządzeń Re w funkcji odległości od linii styczności wojsk, wykazem oraz rozmieszczeniem ważnych obiektów Re (głównie WŁ, posterunki radiolokacyjne, centra rozpoznania RE, stacje zakłóceń, satelity łączności, rozpoznania i radionawigacji itp.).

Walkę elektroniczną prowadzi się w takich samych zakresach częstotliwości jakie wykorzystywane są przez systemy radioelektroniczne wojsk przeciwnika (w tym

[3] W wielu różnych periodykach naukowych otocznie działania urządzeń elektronicznych stanowi tożsame pojęcie jak środowisko działania, w którym rozprzestrzeniają się fale elektromagnetyczne, dlatego w niniejszym artykule przyjęto, ze oba pojęcia będą tożsame.

[4] Mówimy o środkach radioelektronicznych, bowiem tylko one są w zasięgu dostępności energetycznej i fizycznej aktualnych urządzeń rozpoznawczych i zakłócających stanowiących podstawę systemów walki elektronicznej w SZ RP.

łączność, radiolokacje, teledetekcje, radionawigację). Są to pasma od 30kHz do 40GHz (również w paśmie 94 - 108 GHz), podczerwieni, światła widzialnego.
Rozkład dyslokacji poszczególnych urządzeń Re pokazuje w jakich strefach lub na jakich rubieżach względem linii styczności wojsk (lub względem rubieży rozwinięcia środków WE) są usytuowane zasadnicze ilości poszczególnych rodzajów środków Re. Znajomość rozkładu potrzebna jest do określenia skuteczności zakłócania Re z poszczególnych rubieży ich rozwinięcia.
Ponadto w całym środowisku walki prowadzi się wykaz ważnych obiektów Re oraz określa prawdopodobną ich dyslokację. Wykonuje się to dla ukierunkowania rozpoznania, określenia optymalnego czasu ich zakłócania Re, oddziaływania impulsem EM lub rażenia ogniowego.
Celem działań WE w ramach różnych działań operacyjnych i taktycznych wojsk, jest zdobywanie informacji o systemach i środkach elektronicznych wojsk lądowych, lotnictwa uderzeniowego, obrony powietrznej i przeciwlotniczej, siłach morskich, kosmicznych przeciwnika. Dezorganizowaniem pracy systemów dowodzenia wojskami i kierowania (sterowania) środkami walki jest również mylenie systemów rozpoznania.
W wymienionych rodzajach prowadzonej walki, środowisko fal EM zdobywa rolę dominującego środowiska. Można wyróżnić wiele rodzajów systemów uzbrojenia, w których urządzania elektroniczne wspomagające realizację zadań są wiodące:

- systemy dowodzenia i łączności (C2W);
- systemy radiotechniczne;
- systemy kierowania i sterowania uzbrojeniem (rakietami, BSR itp.);
- systemy rozpoznania (np. optoelektronika);
- systemy przełamywania obrony powietrznej (SEAD);
- systemy WE(w tym również impuls EM);
- systemy informatyczne (cybernetyczne);
- systemy nawigacyjne (GPS, Glonass)
- różne wspomagające systemy lotnicze, MW i wojsk lądowych.

W przedstawionym ujęciu urządzenia elektroniczne systemów WE prowadzą nieprzerwanie działania w okresie pokoju, kryzysu i wojny. W poszczególnych okresach zwiększa się jedynie zakres i intensywność działalności elektronicznej o charakterze i znaczeniu militarnym.
Prezentowane ujęcie działań urządzeń elektronicznych WE w siłach zbrojnych RP, jak i całej teorii WE, jej realizacji, odnosi się do ściśle określonych zadań (*task orientem approach*). W okresie pokoju sztaby wojskowe przygotowują się do działań w określonych ramach czasowo przestrzennych. Doświadczenia te przenoszone są na konkretnie rozwiązania w czasie ćwiczeń. Oficerowie (planiści) komórek walki elektronicznej analizują działania przeciwnika, dokonują oceny zagrożenia, planują konkretne przedsięwzięcia, realizują je i sprawdzają efekty (poprzez obiór sygnałów strony przeciwnej z poszczególnych pasm po dokonanych działaniach). Jeżeli działania będą skuteczne to realizują kolejny krok, jak będą nieskuteczne to powtarzają działania lub weryfikują decyzję i kontynuują działania.

Ta ogólna zasada działań i planowania (planuj – realizuj – sprawdzaj – weryfikuj) ukształtowana historycznie znalazła zastosowanie w każdej armii realizującej zadania WE.
Od ośmiu lat w Sojuszu Północnoatlantyckim dyskutowana jest nowa koncepcja działań WE bazująca na uzyskaniu określonych efektów końcowych jeszcze przed tym jak planiści rozpoczną planowanie działań. Nowa koncepcja ukazała się w publikacji z 2008r pod nazwą *NATO Electronic Warfare Policy* (MC 0064/10). Ocenie dowódcy i planiści muszą najpierw określić pożądany efekt prowadzenia walki elektronicznej w środowisku fal elektromagnetycznych oraz wpływ tego efektu na prowadzenie i powodzenie całej operacji połączonej. Zmusza to do nowego, wykraczającego poza dotychczas przyjęte ramy, spojrzenia na proces planowania, przygotowanie i prowadzenia walki elektronicznej.
W startym ujęciu dysponując określonym rodzajem i ilością sprzętu WE określano możliwości oddziaływania na potencjał elektroniczny przeciwnika, zgrubnie tylko szacując efekt. Zakładając powtarzanie działań, aż zaobserwuje się pożądany efekt. W nowym ujęciu zakłada się uzyskany efekt końcowy i do niego dostosowuje się ilość niezbędnego sprzętu, przedsięwzięcia (metody i sposoby działania) i struktury. Jeżeli dany szczebel, siły zbrojne czy państwo nie posiada wystarczającego potencjału WE wspierają go siły Sojuszu Północnoatlantyckiego. Dlatego, nowe ujęcie prowadzenia WE zakłada działania połączone jako podstawę przyszłych działań w środowisku elektromagnetycznym. Wyprzedzając nieco następne podrozdziały można powiedzieć, że stanowią podstawę przyszłych działań w środowisku elektronicznym.

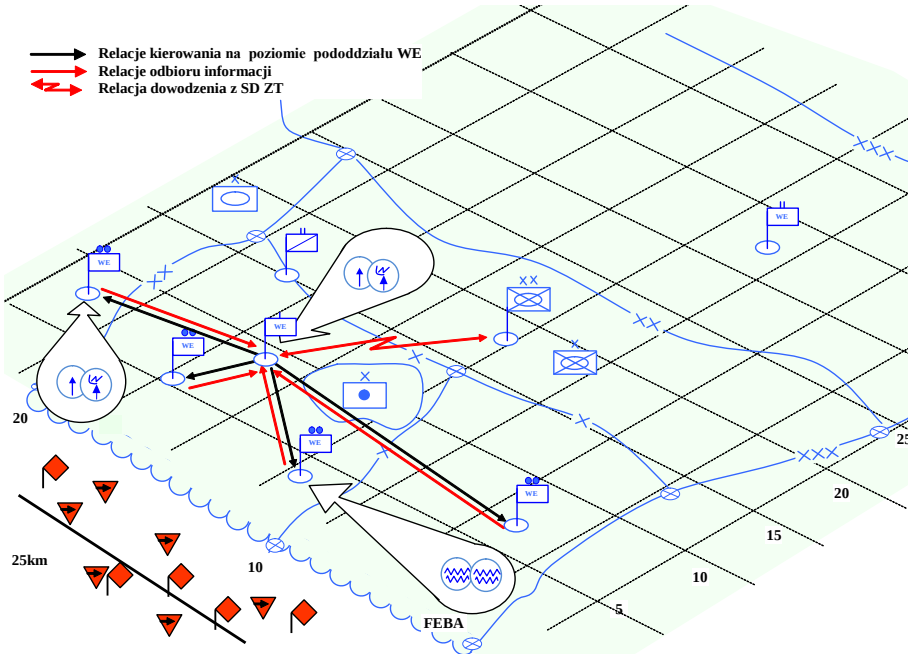
2.3 Automatyzacja działania urządzeń elektronicznych w systemach WE

Automatyzować można: proces analityczny i planistyczny, proces realizacji zadań bojowych przez systemy lub urządzenia elektroniczne oraz proces przekazu informacji do decydenta i odwrotnie. Zachodzi, więc pytanie, czy wszystkie procesy można zautomatyzować? czy wszystkie urządzenia elektroniczne przeznaczone do rozpoznania i zakłócania można spiąć w systemy zautomatyzowane? Najnowsze konstrukcje urządzeń rozpoznawczych i zakłócających już z założenia są półautomatyczne lub w pełni automatyczne (traktowane jako kombajny wielofunkcyjne). Natomiast większy problem występuje gdy staramy się połączyć sprzęt starego parku, aby spełniał wymagania systemów zautomatyzowanych. Niektórych urządzeń nie można zautomatyzować z uwagi na niedostosowanie technologiczne, inne tylko częściowo. Analizy techniczne i finansowe jednoznacznie wskazują, że nieopłacalnym jest budowanie systemów zautomatyzowanych WE w oparciu o stary park sprzętowy. Korzystniejszym rozwiązaniem jest budowa od podstaw nowego systemu z własną myślą techniczną i wkładem własnego przemysłu.
Dla lepszego zrozumienia problemów związanych z automatyzacją urządzeń elektronicznych w środowisku fal EM wykorzystywanych na potrzeby WE należy nieco zapoznać się z ogólnymi właściwościami prowadzenia WE w tym środowisku.

W siłach zbrojnych RP WE prowadzona jest głównie z powierzchni ziemi lub morza, czyli zadania realizowane są w ograniczonej dwuwymiarowej płaszczyźnie (szerokość, głębokość). Obszar powietrzny, mimo, iż jest dostrzegany to został mocno zaniedbany. Możliwości realizacji zadań ograniczają linie rozgraniczenia ZT lub ZO oraz zasięgi łączności pomiędzy poszczególnymi elementami systemu, natomiast głębokość prowadzonej WE ograniczona jest możliwościami odbioru emisji elektromagnetycznych, czyli horyzontem radiowym dla pasm VHF, UHF, SHF, EHF i rozmieszczeniem urządzeń elektronicznych przeciwnika.
Wyposażenie SZ RP w pojedyncze zestawy zautomatyzowanych systemów WE to niewielki procent potrzeb, aby można było przyjąć, iż posiadamy zautomatyzowane systemy WE. Nawet zautomatyzowany system pk. Wołczenica w siłach powietrznych to jeszcze nie automatyzacja WE w SP. Nadal w dużej części pododdziałów walka elektroniczna na poziomie taktycznym i operacyjnym realizowana jest bez żadnej automatyzacji. Cały proces rozpoznania i zakłócania elektronicznego kierowany jest w sposób foniczno-ręczy z SD pododdziału WE. Pozbawia to pododdział, a zarazem dowódcę szczebla taktycznego, szybkiej reakcji na zaistniałe sytuacje elektroniczne na polu walki.
Poziom działań taktycznych charakteryzuje się wysoką dynamiką zachodzących zmian, dlatego bez natychmiastowej reakcji na wykryte źródła i relacje radiowe ZT narażony jest na oddziaływanie elektroniczne przeciwnika. W praktyce nie wszystkie źródła należy natychmiast zakłócać. W niektórych sytuacjach człowiek musi zdecydować o konieczności zakłócania wykrytego źródła elektronicznego lub relacji radiowej. Dlatego, zautomatyzowane systemy dowodzenia i kierowania powinny być także wyposażone w moduł sterowania ręcznego.
Dotychczasowe kierowanie kWE drogą radiową na poziomie taktycznym odbywa się poprzez komendy wydawane z G2 SD ZT (rys.1.). Całością systemu kieruje szef komórki WE a poszczególnymi posterunkami dowodzi dowódca kWE. Informacje z realizacji zadań WE przekazywane są do zespołu analizy i oceny informacji w G2.
Przedstawiony sposób kierowania kWE, bez szybkich i pewnych łączy radiowych bardzo ogranicza możliwość prowadzenia WE (wykrywania, identyfikacji, zakłócania). Podobna sytuacja występuje na poziomie operacyjnym. Brak automatyzacji systemów operacyjnych WE powoduje, iż realizowane zadania rozpoznania i zakłócania, mimo dość znacznych możliwości w paśmie HF, nie są w pełni wykorzystane[5]. Poszczególne pododdziały wyposażone w sprzęt starszego parku technicznego nie zaspokoją potrzeb współczesnego pola walki. Brak zautomatyzowanego systemu kierowania rozpoznaniem i zakłócaniem bardzo często powoduje, iż wykryte relacje radiowe kończą nadawanie zanim rozpocznie się ich zakłócanie. Pododdział zakłóceń HF, mimo, iż może być sterowany

[5] Jedyny system zautomatyzowanego namierzania TIEREK produkcji radzieckiej, zmodyfikowany przez stronę polską, jest już systemem nie spełniającym wymogów współczesnego pola walki. Czas namiaru i zbiór informacji połączony z analizą namierzonej informacji jest zbyt długi, a sprzęt często zawodny.

półautomatycznie, w praktyce częściej wykorzystuje się sposób ręczno-foniczny. Zużycie sprzętu powoduje, iż automatyka zawodzi.



Rys. 1. Ugrupowanie kWE szczebla taktycznego

Receptą na wymienione niedomagania miał być system WE pk. PRZEBIŚNIEG. System wprowadzony na wyposażenie kompanii WE na szczeblu taktycznym. Jest to system w pełni automatyczny wewnętrznie, ale na poziomie pododdziału. Poprawił on znacząco możliwości wykrywania, namierzania i zakłócania, nadal jednak nie osiągnął nakazanej głębokości rozpoznania całego pasa odpowiedzialności rozpoznawczej ZT (50 km), pomimo wyniesienia systemu antenowego na 25 m.

W systemie Przebiśnieg kierowanie poszczególnymi wozami (podsystemami) odbywa się drogą radiową wykorzystując pętlę czasową TDMA z wozu dowodzenia. Można, więc mówić o automatyzacji. Dodatkowo przewidziano możliwość pracy poszczególnych systemów samodzielnie, niezależnie od siebie i agregować informację przechwycone w wozie dowodzenia.

Niedomaganiem systemu Przebiśnieg jest także nierozwiązany problem spójnej wizualizacji wyników rozpoznania i namierzania w wozie dowodzenia kWE. Dowódca widzi na dwóch wskaźnikach dwie różne sytuacje rozpoznania radiowego i radiolokacyjnego, a brak jest weryfikacji danych niezbędnych podczas określenia przynależności operacyjno-taktycznej poszczególnych źródeł.

Natomiast podstawowym mankamentem systemu Przebiśnieg jest brak łączy automatycznego przekazu i kierowania (sterowania) w systemie dowodzenia ZT. Na SD ZT powinny być urządzenie, które umożliwiałyby przekazywanie danych do systemu i odbiór od niego wyników pracy. Element ten należy w trybie pilnym skonstruować i wdrożyć do wojsk lądowych. Wóz automatycznego odbioru i przekazu informacji na SD powinien wykorzystywać istniejące środki łączności np. Storczyk. Bez niego system Przebiśnieg będzie systemem spełniającym jedynie wymagania WE na poziomie pododdziału, a informacyjne dla dowódcy i sztabu dywizji nie będą spływać w czasie rzeczywistym. Podejmowane decyzję będą obarczone niedostatkiem informacyjnym. Dlatego, automatyzacja w pododdziałach WE jest koniecznością.

W przyszłościowych rozwiązaniach systemów WE wojsk lądowych, ale nie tylko, główny nacisk położono na systemy przekazu informacji, uznając, iż o efektywności działania systemów WE decyduje szybkość rozpoznania i przeciwdziałania, a drogą do osiągnięcia tego sukcesu są doskonałe środki przekazu informacji. Przyszłościowy system pk. Kaktus z założenia ma spełnić wymogi natychmiastowego przekazu danych już od elementów rozpoznawczych do decydenta w czasie nieomal rzeczywistym. System Katus oprócz automatyzacji wewnętrznej systemu będzie również wyposażony w moduły automatyzacji zewnętrznej. Poprzez różne rodzaje systemów łączności, głównie radioliniowy system np. Storczyk, przekaz informacji do SD związku operacyjnego lub taktycznego odbywać się będzie z niewielkim opóźnieniem. Taki rozwiązanie organizacyjno-techniczne zapewnia przepływ informacji tekstowej, graficznej i obrazowej z dużą pojemnością i bez strat na jakości. Warunkiem właściwej współpracy z SD jest stanowisko odbioru informacji na SD (lub osobny wóz przekaźnikowy podłączony bezpośrednio do wewnętrznego systemu obiegu informacji). Bez tego stanowiska nawet najlepszy system jest tylko elementem wykonującym zadania w trybie ręcznym, z którego należy odebrać informacje, przetworzyć je i zobrazować, aby dowódca mógł podjąć właściwą decyzję, a czas obiegu informacji jest bardzo długi.

Aktualnie w jednostkach WE SZ RP wiele egzemplarzy sprzętu jest różnych producentów (niemieckich, francuskich, amerykańskich, rosyjskich). Spełniają określone zadania na różnych pasmach częstotliwości. Większość z nich służy do rozpoznania i namierzania źródeł radiowych. Głównym sposobem prowadzonej działalności rozpoznawczej jest poszukiwanie i przechwytywania sygnałów będących w zainteresowaniu jednostek WE. Współcześnie wykorzystywane urządzenia zdolne są do wykrywania większości nadawanych sygnałów, których nośnikiem są fale EM, w każdym paśmie częstotliwości. Przechwytywane sygnały nie zawsze są nadawane przez nadajniki radiowe, często są to sygnały o emisji nieradiowej, trudno identyfikowalnej. Z analizy widmowej takich sygnałów można wnioskować, iż mogą one pochodzić z źródeł: radiolokacyjnych, emisji komputerów, źródeł mikrofalowych itp. Takie sygnały urządzenia rozpoznawcze również przechwycą i namierzą. Podpierając się przykładem systemu Przebiśnieg,

należy zauważyć, iż istnieje możliwość rozpoznawania i namierzania urządzeń elektronicznych, które nie są w obszarze zainteresowania decydentów wojskowych. Możliwości odbiorników pozwalają na odbiór sygnałów do 3 GHz a odbiorników radiolokacyjnych do 18 GHz. Problem jest tylko z ich identyfikacją. Dysponując odpowiednią bazą danych o sygnałach nie niosących informacji można dokonywać identyfikacji tych sygnałów. Dlatego, niektóre urządzenia rozpoznawcze mogą mieć podwójną funkcję. Jedne będą wykorzystywane na potrzeby WE inne mogą służyć jako uniwersale urządzenia rozpoznawcze w zależności od potrzeb ich zastosowania i będą wykorzystywane przez inne jednostki lub organizacje. W innych zastosowaniach niż WE, urządzenia rozpoznawcze (tj. odbiorniki wielofunkcyjne) będą poszukiwały nietypowych sygnałów w różnych pasmach częstotliwości. Dysponując wzorcami z BD, będzie można identyfikacji źródła emisji i je zakłócać. Odrębną funkcją jest już sam proces zakłócania. Urządzenia zakłócające emitują energię wprowadzając entropię informacyjną w urządzeniach odbiorczych przeciwnika lub w określonych pasmach częstotliwości powodując zmianę przeznaczenia informacji lub jej całkowity albo częściowy zanik. Te urządzenia również spełniają podwójną funkcję. Można je wykorzystać w systemie WE, ale także do wnoszenia energii (sygnałów) zniekształcających sygnał właściwy w systemach i sieciach komputerowych. Jeżeli sygnały zniekształcające będą przenosiły dodatkowo programy np. wirusy to takie działanie zakłócające są już domeną działań w środowisku cybernetycznym i można je nazwa walką cybernetyczną.

3. Środowisko cybernetyczne – konteksty terminologiczne

Działania w sieciach informatycznych[6] należy postrzegać przez pryzmat zamian jakie zachodziły i nadal zachodzą w konfliktach militarnych oraz operacji innych niż wojna. Zakończenie zimnowojennych zmagań i koniec dwubiegunowego układu sił na świecie spowodowały nową sytuację polityczną oraz nową sytuacje bezpieczeństwa w skali globalnej. Ostatnie dziesięciolecia wykreowały zagrożenia o jakich wcześniej nie wspominano lub jakich nie było. Skutkiem tych zmian jest niestandardowe użycie sił zbrojnych oraz nowe podejście do planowania, dowodzenia i kierowania, współdziałania, koordynacji wewnątrz sił zbrojnych oraz w kooperacji z siłami sojuszniczymi. Działania te wykreowały także nowe podejście do współdziałania z organizacjami innymi niż wojskowe tj. agencje cywilne udzielające pomoc humanitarną, które często są podporządkowane siłom wojskowym. Całość tych działań spowodowała eskalację nowych form asymetrycznego oddziaływania na wojska własne i przeciwnika. Jest to przykład nowych zagrożeń w sferze działań militarnych. Odejście od ustalonych kanonów sztuki wojennej na działania z zaskoczenia, w wielu miejscach, małymi siłami jednocześnie jest tego objawem. Atak fizyczny, oprócz niewątpliwie oddziaływania ogniowego, znajduje swój upust w innych środowiskach, do których

[6] Przez Lecha Konopkę nazywanych sieciami centrycznymi.

cyberprzestrzeń (czasami nazywana środowiskiem informatycznym) z swoimi sieciami informatycznymi jest predysponowana.
Środowisko cyberprzestrzeni stało się rozwojem mediów przekazu informacji w każdej postaci, od przekazu słownego, drukowanego do obrazowego włącznie (być może w przyszłości holograficznego). Globalne przekazy informacyjne są rewolucją w czasie dostępu do informacji. Środowisko to jest szeroko wykorzystywane przez wojsko. Każda decyzja dowódców może być śledzona na „żywo" w Internecie. Dowódcy i ich wojska stały się niejako zakładnikami środków masowego przekazu, muszą, więc liczyć z tym, że ich bieżąca działalność będzie stale oceniana przez własną oraz światową opinię publiczną. Środowisko cyberprzestrzeni, w którym działają jest ogólnie dostępne dla opinii publicznej żądnej aktualnych informacji z przebiegu działań.
Otwartość na informację uzyskano głównie dzięki szerokiemu rozwojowi sieci Internet. W wielu państwach rozpoczęto definiowanie pojęcia sieci informatycznych. Samo pojęcie jest dość oczywiste, ale zaczęto przyjmować nieco szersze wyobrażenie obejmujące działania w skali globalnej polegające nie tylko na przekazie informacji, ale także gromadzeniu, rozpoznawaniu, zakłócaniu i wykorzystywaniu środowiska informatycznego, stąd powstało wiele definicji pojęcia cyberprzestrzeni. Publikacje dotyczące cyberprzestrzeni ukazują się już od dawna. Wielu autorów podświadomie przyjmuje pojęcie cyberprzestrzeni i szeroko się nim posługuje, często nie zastanawiając się nad jej znaczeniem i zawartością merytoryczną. Dla wielu stało się kluczem wytrychem do prezentacji swoich poglądów.
Opis cyberprzestrzeni niewątpliwie zapoczątkowały pojęcia odnoszące się do sieci informatycznych. Konsekwencją zachodzących przemian było wydanie doktryny przez SZ USA w grudniu 2006 roku pt. Narodowa Militarna Strategia ws. Operacji Cybernetycznych (*National Military Strategy for Cyberspace Operations – NMS-CO*). Opisuje ona domenę cybernetyczną, wymienia zagrożenia i wrażliwe obszary związane z cyberprzestrzenią, stanowi też strategiczną podstawę do dalszych działań w tym obszarze. Amerykańska doktryna wyraża wszechstronne, strategiczne podejście SZ USA do wykorzystania operacji cybernetycznych w celu zapewnienia strategicznej militarnej przewagi Stanów Zjednoczonych w tej domenie. Realizację tego celu ma zapewnić, wg. tej strategii, integracja ofensywnych operacji cybernetycznych z defensywnymi, która potęgowana ma być poprzez zapewnienie specjalistycznego potencjału ludzkiego na potrzeby tej działalności. W publikacji tej podjęto się próby zdefiniowania środowiska cyberprzestrzeni[7].
Cyberprzestrzeń – jest domeną charakteryzującą się wykorzystaniem elektroniki i spektrum elektromagnetycznego w celu gromadzenia, modyfikacji i wymiany

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

danych poprzez systemy sieci oraz towarzyszącej fizycznej infrastruktury[8]. W dokumencie tym przytacza się również starszą definicję cyberprzestrzeni z innego dokumentu (JP 1-02), która sformułowano następująco[9]: cyberprzestrzeń – wyobrażane środowisko w którym informacje w cyfrowej postaci są udostępniane poprzez sieci komputerowe[10].

Na podstawie porównania tych dwóch definicji widać wyraźnie ewolucję pojęcia „cyberprzestrzeni", gdzie w starszej jej wersji udostępnianiu informacji cyfrowych służyć miały jedynie sieci komputerowe, a w nowszej jej wersji do tego celu ma służyć większa gamma urządzeń elektronicznych, sieci i towarzyszącej fizycznej infrastruktury (nie jest ona ograniczona jedynie do sieci komputerowych).

Przedstawione definicje odnoszą się ściśle do już istniejących sieci informatycznych, natomiast na cyberprzestrzeń należy spojrzeć także z punku widzenia wartości społecznych wynikających z ogromnej różnicy, która rysuje się między tradycyjną przestrzenią życia grupowego ludzi, a kontaktami z wykorzystaniem Internetu. Czas i przestrzeń nie ogrywają roli w cyberprzestrzeni, a kontakty interpersonalne jak najbardziej. Obejmują one przedstawicieli różnych kultur, są nieprzerwane, niekontrolowane. Każdy ma wpływ na każdego będąc jednocześnie anonimowym członkiem tej społeczności.

Wspomniano, że cyberprzestrzeń można definiować różnie, można ją traktować jako działalność ludzką z udziałem technologii informacyjno-komunikacyjnych, gdzie obszar działania postrzegany jest przez pryzmat techniki, a nie przez tradycyjną przestrzeń geograficzną. Jak zauważył P. Virilio „jej elementy pozbawione są wymianu rozciągłości, lecz wpisane w specyficzny rodzaj czasowości związanej z procesem błyskawicznego rozpowszechniania. […] Współpracujące ze sobą terminale komputerowe i monitory sprawiają, że podział na „tu" i „tam" nic już nie znaczy[11].

Częste stwierdzenia, że cyberprzestrzeń jest nowym medium przekazu informacji, wzajemnych oddziaływań, za pośrednictwem bitów przenoszonych z prędkością światła jest czymś oczywistym. W podświadomości, intuicyjne odczuwamy, że autorom chodzi o sieci informatyczne a szczególnie o Internet. Cyberprzestrzeń traktowana jest jako byt, wytwór wirtualny (sztuczny stworzony przez człowieka), pozbawiony parametrów geograficznych, niemierzalny i nieograniczony. Jak zauważył Z. Bauman „jej ramy i granice wyznacza poziom aktualnego rozwoju techniki informatycznej i stopień osieciowania świata. W istocie to, co nazywamy odległością wcale nie jest obiektywną bezosobową daną natury fizycznej, lecz

[8] *„**Cyberspace** – a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures".*

[9] Wyd.cyt. *National Military*, ..s. 3.

[10] *Cyberspace – the notional environment in which digitized information as communicated over computer networks".* Zob. S. Czeszejko, Działania elektroniczne w NATO i SZ RP – próba kategoryzacji, AON, Warszawa 2011.

[11] Z Bauman, Globalizacja, Warszawa 2000, s.24.

konstruktem społecznym. […] Wszystkie pozostałe czynniki, za pomocą których zbiorowe tożsamości tworzą się, zyskują odrębność i ją zachowują"[12].
Cyfrowy kontakt partnerów zmienił się pod wpływem powstania cyberprzestrzeni. Zależności interpersonalne nabierają charakteru partnerskiego. Podczas, gdy rozszerzeniu ulega sfera wolności słowa, zanika terytorialność, cyberprzestrzeń stała się medium transferu informacji przy barku jakichkolwiek skutecznej kontroli tego co, kiedy, koś i jak przekazuje. Głównym problemem jest, więc nie nieograniczony przekaz informacji a kontrola przestrzeni wirtualnej. Wiele państw, szczególnie demokratycznych, pragnących kontrolować cyberprzestrzeń napotyka trudności płynące m.in. z równoczesnego obowiązku zapewnienia zasady wolności słowa. Postanowiono, że jeżeli nie można kontrolować cyberprzestrzeni należ minimalizować skutki jej funkcjonowania. Skutki takiej działalności są szczególne widoczne w ograniczeniach dostępu do poszczególnych stron internetowych dla dzieci. Strony z pornografią, przemocą są automatycznie blokowane lub ręcznie przez rozważnych rodziców. Podobne działania stosują różne firmy w stosunku do swoich pracowników a nawet organa państwowe, blokujące dostęp do agresywnych, niepopularnych lub wrogich stron internetowych. W krajach arabskich lub azjatyckich blokady stron (witryn) to czynnik nieomal codzienny. Państwa autorytarne ściśle kontrolują dostęp społeczności do tych informacji, które mają charakter demokratyczny, narodowowyzwoleńczy. Takie działania mogą by skuteczne albowiem stopień osieciowienia w tych państwach jest niewielki (przynajmniej w niektórych).
Cyberprzestrzeń w polskiej literaturze przedmiotu znalazła swoje odzwierciedlenie w oficjalnym dokumencie o nazwie „*Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia"*, wydanym w roku 2009. Jest on wynikiem szeregu inicjatyw podejmowanych w Unii Europejskiej, w których swój udział ma również Polska. Dokument ten stanowi oficjalne podwaliny pod działania prowadzone przez Polskę w obszarze cyberprzestrzeni. Dokument zawiera bardzo prostą definicję cyberprzestrzeni, którą należy rozumieć jako „przestrzeń komunikacyjną tworzoną przez system powiązań internetowych" [13].
Dokument przedstawia m.in. realizatorów przedsięwzięć związanych z działaniami w cyberprzestrzeni, do których należą: MSWiA, ABW, MON, SKW, oraz inne organy administracji publicznej, podmioty prywatne - właścicieli zasobów stanowiących krytyczną infrastrukturę teleinformatyczną państwa.
Z opublikowanego dokumentu wynika, że MON otrzymało swój obszar odpowiedzialności za cyberprzestrzeń. Jako podstawę prawną działania wojska, wskazano dokument „*Decyzję MON nr 375/MON z dn. 29.07.2008 r. w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony*

[12] Z. Bauman, Globalizacja, czyli komu globalizacja, a komu lokalizacja, "Studia socjologiczne", nr 3, 1997
[13] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*, Warszawa, 2009. s.4.

narodowej", co świadczy o wcześniejszych inicjatywach podejmowanych przez wojsko w obszarze cyberprzestrzeni.
Na bazie decyzji rządowych Minister Obrony Narodowej polecił zorganizować Centrum Bezpieczeństwa Cybernetycznego SZ RP, które ma odpowiadać za prowadzenie operacji cyberprzestrzennych szczebla operacyjnego. Specjaliści z tego biura postrzegają działania w cyberprzestrzeni poprzez dostępność i szerokie wykorzystanie fal EM. W ich interpretacji cyberprzestrzeń definiowana jest jako *globalny obszar w obrębie środowiska informacyjnego, składającego się z Internetu, sieci telekomunikacyjnych oraz systemów informatycznych, natomiast operacje w cyberprzestrzeni to osiąganie różnych celów poprzez przestrzeń cybernetyczną. Działania te obejmują operacje zmierzające do pozyskania lub ochrony informacji*[14]: Prezentowane definicje są bardzo zbieżne z poglądami amerykańskimi w tym zakresie.
Ewolucyjnym rozwinięciem działań w środowisku informatycznym są działania w cyberprzestrzeni, a rozwijając problem jeszcze szerzej będą nimi operacje cybernetyczne. Dominującym państwem, wyznaczającym trendy rozwojowe oraz określającym zakres działalności są oczywiście Stany Zjednoczone. Predysponują do roli lidera z uwagi na najlepiej rozwinięta technikę informatyczną na świecie (przynajmniej do chwili obecnej). Dokumentem doktrynalnym DD 3-12 próbują na swój sposób (wg. ich racji stanu) definiować cyberprzestrzeń, rozszerzając pojęcia na operacje cybernetyczne oraz przewagę cybernetyczną.
Na bazie publikowanych i wprowadzanych dokumentów doktrynalnych bardzo wyraźnie można zaobserwować stopniowy charakter rozszerzania cyberprzestrzeni i toczonej za jej pośrednictwem walce na bity.
Najnowsza definicja cyberprzestrzeni wskazuje, że jest to globalna domena zawarta w środowisku informacyjnym, składająca się niezależnej sieci informacyjnej opartej na infrastrukturze technologicznej, zawierającej Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery. Wyraźnie więc widać rozszerzenie pojęcia o domenę zawartą w środowisku informacyjnym[15]. Natomiast operacje cybernetyczne są zdefiniowane jako zastosowanie zdolności cybernetycznych w sytuacji, w której pierwotnym zamiarem jest osiągnięcie własnego celu w cyberprzestrzeni lub poprzez cyberprzestrzeń. Takie operacje zawierają operacje (działania) w sieciach informatycznych oraz wszelkie aktywności w celu oddziaływania i obrony globalnej sieci informacyjnej (*Global Information Grid - GIG*). Konsekwencja wymienionych pojęć jest przewaga cybernetyczna określana jako „operacyjna w cyberprzestrzeni, poprzez cyberprzestrzeń, i ze strony cyberprzestrzeni w celu prowadzenia operacji w danym czasie i w danej domenie, z eliminacją niepożądanych ingerencji"[16].

[14] Materiały robocze Centrum Bezpieczeństwa Cybernetycznego, Białobrzegi, 2011, str. 13.
[15] *Cyberspace Operations* (*DD 3-12*), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, str. 1.
[16] Tamże, str. 2.

4. Korelacja działania urządzeń elektronicznych

Po drugiej wojnie światowej wielu teoretyków wojskowych i cywilnych uważało, że wymiar przyszłych wojen będzie ewoluował w kierunku kosmosu i spektrum elektromagnetycznego. Wyrażane poglądy pozycjonowały środowisko fal EM jako pierwsze środowisko następnej wojny. Dowodów na poparcie tej tezy szukano w historycznym rozwoju środków walki nasyconych elektroniką. Przeniesienie ciężaru walki w wymiar fal EM potwierdzały liczne nowe konstrukcje sprzętu wojskowego w coraz większym stopniu uzależnione od urządzeń elektronicznych. Co bardziej śmiali teoretycy mówili o wojnach elektroniczno-kosmicznych.

Wyrażony pogląd przez historyka brytyjskiego Michaela Howarda[17] w książce pt. „*Wojna w dziejach Europy*" dość sugestywnie ujmuje zagadnienia wojny związanej z rozwojem i wykorzystaniem elektronicznych urządzeń łączności, kryptografii, rozpoznania i walki radioelektronicznej oraz radiolokacji. *(...) Zwycięstwo przypadało ostatecznie tej stronie, która umiała śledzić poruszenia przeciwnika i odczytywać jego szyfry przy jednoczesnym utajnieniu własnych. W II wojnie światowej umożliwiła to technika radarowa oraz umiejętność przechwytywania sygnałów radiowych*[18]."

Można, więc przyjąć fakt, że rozpoczęto już ówcześnie wykorzystywać, nowe środowisko działań militarnych (po lądowym, morskim i powietrznym). Koncepcji podziału działań militarnych i określenie nowych wymiarów wojny lub jej czynników w literaturze przedmiotu można spotkać wiele.

Jeszcze niedawno konfrontacja przebiegała w przestrzeni trójwymiarowej, tak bliskiej zmysłom i wyobraźni ludzkiej. Zmagania na współczesnym polu walki obejmują swym zasięgiem przestrzeń wielowymiarową. Niektórzy teoretycy wojskowi wymieniają aż sześć wymiarów wojny. Do takich przedstawicieli należy płk R. Grabau[19] z armii niemieckiej. Wielowymiarowość wojny prezentuje poprzez wykorzystanie sześciu wymiarów jej prowadzenia. Do pierwszych trzech standardowych zalicza: odległości [Y], powierzchni (szerokość [X] i głębokość [Z]), wysokość [H]. i dodatkowo uwzględnia następne tj: czas, informację oraz spektrum elektromagnetycznego. Właśnie te trzy czynniki mają decydować charakterze przyszłych konfliktów.

Niezależnym potwierdzeniem istnienia takiego podziału („wymiaru") walki[20] jest tzw. „Model Wardena", który został opracowany przez pułkownika Johana Wardena z Sił Powietrznych Stanów Zjednoczonych na początku lat

[17] Sir Michael Howard (ur. 29.11.1922 r.) profesor, brytyjski historyk wojskowości. W swoim czasie był jednym z najbardziej wpływowych Brytyjczyków w obszarze kształtowania badań strategicznych nt. obronności i bezpieczeństwa państwa. Źródło (styczeń 2011 r.): http://en.wikipedia.org/

[18] M Howard, Wojna w dziejach Europy, Ossolineum, Wrocław 1990, s. 167.

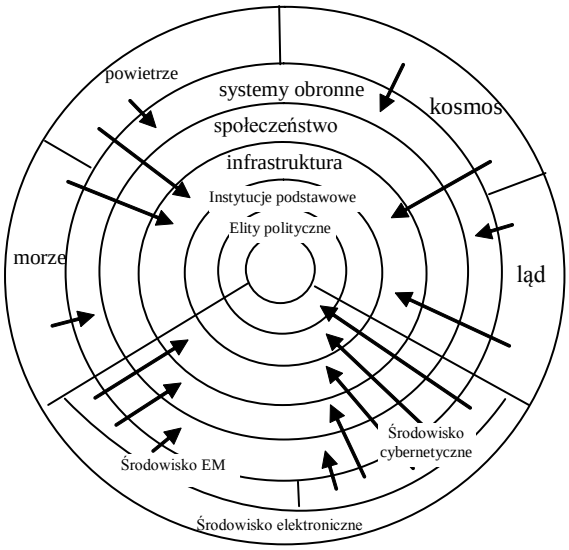
[19] R. Grabau, Sześć wymiarów wojny, WPZ nr.1(173), 2(174), 3(175), Warszawa 1987.

[20] Sienkiewicz P., *Wizje i modele wojny informacyjnej*. w: *Społeczeństwo informacyjne – wizja czy rzeczywistość ?,* Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 374.

dziewięćdziesiątych w jego teorii strategicznego paraliżu. J. Warden postrzegał przeciwnika jako system systemów, istotę jego systemowego podejścia stanowi model pięciu kręgów. Według Wardena każdą organizację (państwo, firmę, wojsko, organizację terrorystyczną, gang przestępczy, itp.) należy traktować jak strukturę składającą się z systemu pięciu wzajemnie powiązanych kręgów, składających się na całość i pełniących założone dla nich funkcje. Ich budowa wygląda w następujący sposób[21]:

- elity polityczne – tj. komponent przywództwa sprawujący ogólne kierownictwo;
- instytucje podstawowe – tj. komponent procesów (wcześniej określany jako *potrzeby organiczne*) transponujący energię z jednego kręgu do drugiego;
- infrastruktura – tj. komponent infrastruktury fizycznej;
- społeczeństwo – tj. komponent ludności;
- systemy obronne – tj. komponent aktorów (wcześniej nazywany *siłami polowymi*) składający się z grup demograficznych.

Każdy z kręgów Wardena funkcjonuje w pięciu „wymiarach", na które składają się następujące obszary działania: morze, ląd, powietrze, przestrzeń kosmiczna, przestrzeń cybernetyczna. Dzisiaj można ten model nieco unowocześnić i wyróżnić działania w środowisku elektronicznym zamiast cybernetycznym. Wówczas piąty krąg podzielić można na dwie części: obszar środowiska elektromagnetycznego i cybernetycznego.



Rys. 4. Zmodernizowany model oddziaływania wg. J. Wardena
Źródło: Opracowanie własne

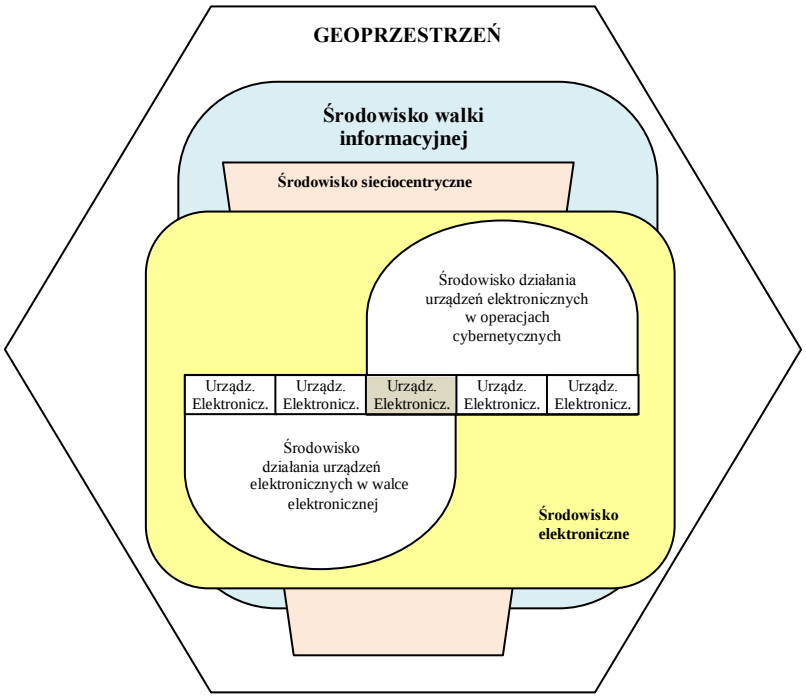
[21] Vego M., *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona nr 2, Warszawa, 2009, str. 185.

Problemy automatyzacji urządzeń i systemów elektronicznych występujące w WE odnoszą się do środowiska fal elektromagnetycznych. Automatyzacja a jednocześnie działanie w innych środowiskach prowadzenia WE np. środowisku informatycznym (lub szerzej cybernetyczne) pozostaje nadal poza zainteresowaniem decydentów wojskowych. Natomiast, wnioski z minionych i trwających konfliktów zbrojnych (Bośnia, Irak, Afganistan), w których udział brały i biorą siły koalicyjne wskazuje, że środowisko informatyczne zaczyna odgrywać coraz większą rolę. Można zadać pytanie, czy urządzenia elektroniczne można wykorzystać do prowadzenia rozpoznania sieci informatycznych? A jeżeli tak to, jakie urządzenia? Czy te same urządzania można wykorzystać do działania w sieciach informatycznych i systemach WE? Czy dla nich istnieje osobne środowisko działania? A może działają w ramach innego, jeszcze nie zdefiniowanego środowiska.

W tradycyjnym rozumieniu pole walki jest zamkniętym geograficznie obszarem, na którym prowadzone są działania bojowe. Pojęcie to samo w sobie zawiera uwarunkowania jego prowadzenia. Aktualnie wprowadzanie nowych środowisk walki do arsenałów środków działania w znacznym stopniu znajdujących się poza obszarem geograficznym powoduje, że pojawiają się nowe uwarunkowania prowadzenia działań, nawet te na najniższym poziomie, zmieniają się radykalnie. Za przykład mogą posłużyć działania w środowisku sieciocentrycznym związane z utrzymaniem ciągłego strumienia informacji od decydenta do sensorów wykonawczych. Zmieniające swoją rolę urządzenia (sensory) o zasięgu globalnym służące realizacji zadań strategicznych na korzyść nawet pojedynczego żołnierza przekazując ciągłym strumieniem informacyjnym niezbędne dane do działania. Innym bardzo jaskrawym przykładem zmieniającego się uwarunkowania pola walki są działania antyterrorystyczne, szczególnie w środowisku sieciocentrycznym. W walce z niezidentyfikowanym przeciwnikiem trudno mówić jest o polu walki. Żadne akcje militarnie nie przynoszą spodziewanych rezultatów. Konflikty asymetryczne nie mają typowego obszaru pola walki. Zarówno przeciwnik jaki i ich prześladowcy są w ciągłym ruchu. Ten kto zdobędzie pierwszy informację o ruchach drugiej stront ten odnosi sukces. Częściej jednak niewidoczny przeciwnik odnosi sukcesy z uwagi, że to on wybiera siły, miejsce i czas akacji.

Odpowiedzią na takie działanie była propozycja nowego pojęcia, zaproponowana przez SZ USA, dotycząca przestrzeni walki (*battlespace*). Ma ona zastąpić dotychczasowe pojęcie pole walki *(battlefield*). W proponowanym ujęciu przestrzeń walki obejmowałaby wszystkie uwarunkowania związane z prowadzeniem działań bojowych na wszystkich szczeblach (strategicznym, operacyjnym, taktycznym), niezależnie od ich geograficznego ulokowania. Przyjęcie takiego podejścia wyraźnie wskazuje, że działania nawet na szczeblu taktycznym uwarunkowane są olbrzymia ilością czynników, których znaczna część jest poza obszarem tradycyjnie geograficznego pola walki, na którym są fizycznie prowadzone działania bojowe. Dają się zauważyć inne środowiska (przestrzenie)

działania. W tradycyjnie zorganizowanych działaniach dowódca z powodu ograniczonych możliwości monitorowania i oceny, a także ograniczonymi możliwościami rozpoznawczymi i łączności nie jest zdolny do właściwego funkcjonowania. Problem ten rozwiązuje zastosowanie sieciocentrycznego podejścia do działań bojowych. Precyzyjnej rzecz ujmując sensory i sieci informatyczne stanowią tu podstawę skutecznego działania. Środowisko informacyjne, elektromagnetyczne a ogólnie rzecz ujmując środowisko elektroniczne stają się dominującym.



Rys. 3. Miejsce środowisk działania urządzeń elektronicznych na tle walki informacyjnej i środowiska sieciocentrycznego
Źródło: Opracowanie własne

Wykorzystanie energii elektromagnetycznej w środowiskach naturalnych (powietrzu, kosmosie i wodzie) oraz wykorzystanie systemów komputerowych w przestrzeni stworzonej przez człowieka (cyberprzestrzeni) ukierunkowały działania militarne na nowe środowisko, w którym elektronika jest dominującym organem. Oczywistym jest, że środki rażenia pozostaną zawsze domena militarnego oddziaływania, ale ich znaczenie może być sprowadzone już tylko do roli odstraszania potencjalnego przeciwnika. Wkroczyliśmy więc w wymiar środowiska elektronicznego. Wspólnym mianownikiem działania w tym środowisku są urządzenia i systemy elektroniczne. Ich rola i funkcje sterują i kontrolują nieomal każde działanie urządzeń wojskowych oraz wspomagają

dowodzenie wojskami. Człowiek jest częścią tego mechanizmu. Kolejnym istotnym wyróżnikiem nowego wymiaru jest możliwość prowadzenia w nim samodzielnych działań militarnych, niezależnych od działań prowadzonych na lądzie, morzu, w powietrzu i kosmosie. To samodzielne prowadzenie działań z wykorzystaniem urządzeń i systemów elektronicznych jednej strony przeciwko analogicznym urządzeniom i systemom strony przeciwnej oznacza wyraźnie, że jesteśmy świadkami powstania nowego środowiska działań, które możemy nazwać środowiskiem elektronicznym. Posługując się ogólnymi definicjami środowiska tj:

- *dopełnienie wyróżnionego systemu do całej przestrzeni, czyli zbiór wszystkich obiektów (wraz z ich atrybutami oraz relacjami między tymi atrybutami), które z uwagi na przyjęte kryteria przynależności do systemu, nie zostały do niego zaliczone*[22]*;*
- *ogół elementów nieożywionych i ożywionych, zarówno naturalnych, jak i powstałych w wyniku działalności człowieka, występujących na określonym obszarze oraz ich wzajemne powiązania, oddziaływania i zależności*[23].

Podjęto się sprecyzowania środowiska działania urządzeń elektronicznych „jako ogół elementów nieożywionych powstałych w wyniku działalności człowieka, występujących w określonym obszarze i przestrzeni, pomiędzy którego elementami istnieją wzajemne powiązania, wzajemne oddziaływania i pozostają one we wzajemnej zależności[24].

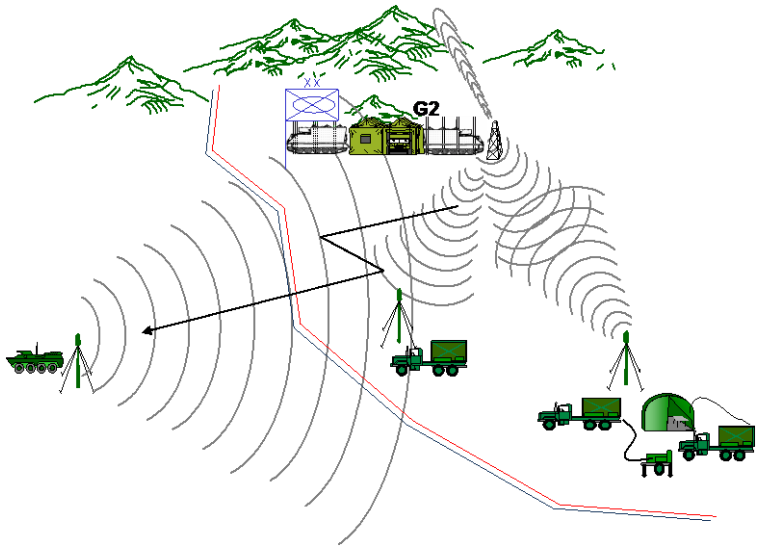
Środowisko elektromagnetyczne zostało już szeroko omówione. Przedstawiono także wybrane problemy związane z automatyzacją urządzeń elektronicznych w tym środowisku, ale problemem jest automatyzacja urządzeń elektronicznych pracujących w innych środowiskach? Nasuwa się, więc kolejne pytanie czy urządzenia elektroniczne pracujące w środowisku cybernetycznym można również automatyzować? Przedstawiono już zakres tego środowiska. Należy się ogólnie zgodzić, że urządzenia elektroniczne pracujące w środowisku cybernetycznym to głównie komputery, ale obok nich także różne urządzenia wspomagające ich pracę. Prowadząc działania w środowisku cyberprzestrzeni mamy do czynienia z tymi samymi rodzajami zadań jakie występują w walce elektronicznej. Jeżeli przymniemy, że systemy (narzędzia) walki cybernetycznej[25] prowadzą rozpoznanie, zakłócanie i obronę to ogólnie są to te same rodzaje zadań.

[22] Kaczorowski B., *Wielka encyklopedia PWN - T. 27*, PWN, Warszawa, 2005, str. 47.
[23] Źródło (styczeń 2011 r.): http://pl.wikipedia.org/
[24] Zob. S. Czeszejko wyd. cyt. s. 13
[25] Walka cybernetyczna jest pojęciem wyróżnionym z uwagi na jednoznaczność pojęć. Jeżeli posługujemy się pojęciem walka elektroniczna i myślimy o działaniach w środowisku fal EM to przez analogię występują działania w środowisku cybernetyczny. Możemy wówczas posługiwać się pojęciem walki cybernetycznej. Nie użyto pojęcia wojny bowiem, jest ono zastrzeżone jest dla działań, w którym strony walczące angażują do walki cały potencjał gospodarczy swoich państw a elity polityczne i społeczeństwo to akceptują. Jak już wcześnie wykazano działania w sieciach informatycznych są częścią działań w walce cybernetycznej.

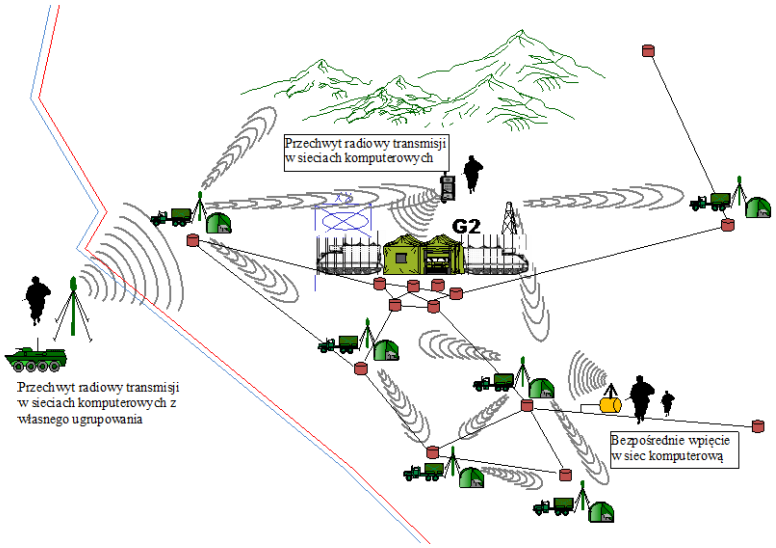
Pytaniem podstawowym jest czy o takim samym charakterze?. Rozpoznanie w walce cybernetycznej ma na celu zdobywanie informacji o ruchu obiektów[26] w sieciach komputerowych, czyli prowadzi poszukiwanie interesujących odbiorcę informacji, przechwytywanie informacji od zidentyfikowanych obiektów, namierzanie interesujących obiektów (źródł) i śledzenie ich. Są to, więc te same rodzaje zadań jakie występują w WE. Zmieniły się tylko częściowo narzędzia służące do ich realizacji. Odbiornik radiowy zastąpiono komputerem, ale z odpowiednim oprogramowaniem. Owo oprogramowanie jest kluczem i podstawową różnicą pomiędzy WE a walką cybernetyczną. Rozpatrując problem dogłębniej przekonamy się, że jest to tylko część problemu, bowiem komputery są wyposażone w urządzenia odbiorczo-nadawcze tj. np. WiFi czy Bluetooth. W związku z tym urządzenie odbiorcze i nadawcze oraz komputer tworzą system nadawczo-odbiorczy. Nie będziemy rozpatrywać możliwości odbiorczych takiego urządzenia, tylko sam fakt odbioru treści przekazywanych informacji. Urządzenia WiFi (poprzez swoje protokoły) pozwalają na zdalne obieranie przekazywanych sygnałów za pośrednictwem fal EM (2,4 Ghz). W takim przypadku możemy mówić, iż urządzenia odbiorcze upodabniają się do urządzeń odbiorczych wykorzystywanych w WE. Konkludując rozpoznanie informatyczne w ramach WE to rozpoznanie radioelektroniczne realizujące zadania poszukiwania źródła emisji, przechwytywania, śledzenia i namierzania sygnałów przesyłanych falami EM. Zmienia się tylko typ rozpoznawanego urządzenia. Natomiast rozpoznanie informatyczne w ramach walki cybernetycznej to poszukiwanie źródeł (obiektów, programów), przechwytywanie ich, śledzenie i namierzanie w sieciach komputerowych i komputerach wykorzystując sygnały prądowe i częściowo fale EM. Drogą wtargnięcia do systemów komputerowych jest spektrum fal EM lub bezpośrednie podłączenie się do sieci.

Zakładając, iż istnieje możliwość prowadzenia rozpoznania RE i informatycznego za pośrednictwem fal EM (w szczególnych przypadkach) można się zastanowić czy jest możliwe skonstruowanie uniwersalnego urządzenia monitorującego sieci komputerowe lub inne urządzenia elektroniczne pracujące na podobnych częstotliwościach, wspólne dla systemów WE i WC. Jeżeli założymy, że prowadzimy WE w mieście to takie urządzenie wydaje się zasadne. Dysponując jednym zdalnie rozkładanym urządzeniem z możliwością odbioru szerokiego spektrum częstotliwości to zarówno na potrzeby WE będzie ono zdolne do odbioru urządzeń elektronicznych będących w zainteresowaniu WE jak i odbioru częstotliwości pracy sieci. Zakładając, iż posiadamy możliwości zdalnego łączenia się z takim urządzeniem możemy w ramach WC z ukrycia podłączyć się do danej sieci.

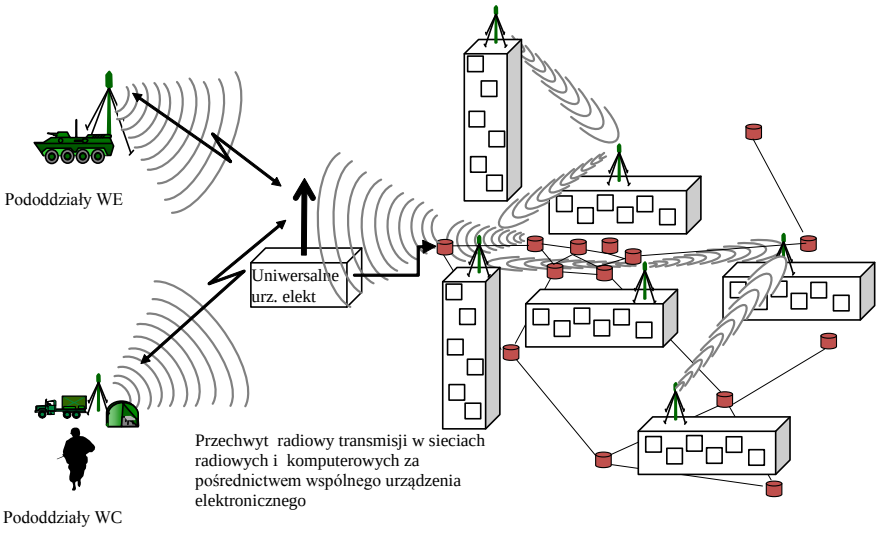
[26] Obiektem w tym znaczeniu jest ktoś lub coś (np. program komputerowy), który celowo wprowadzony do sieci lub komputera realizuje określone zadania (poszukiwanie, śledzenie, niszczenie, infekowanie).



Rys. 4. Idea rozpoznania radioelektronicznego
Źródło: Opracowanie własne



Rys. 5. Idea rozpoznania cybernetycznego
Źródło: Opracowanie własne



Rys. 6. Idea wspólnego urządzenia rozpoznawczego i zakłócającego w walce elektronicznej i cybernetycznej
Źródło: Opracowanie własne

W walce cybernetycznej obok urządzeń elektronicznych, typowych dla WE będą wykorzystywane także urządzenia do procesu zakłócania i obrony cybernetycznej. Zakłócanie w walce cybernetycznej to nic innego jak wprowadzanie do sieci komputerowych programów służących do szpiegowania (zdobywania określonych informacji w poszczególnych sieciach i komputerach różnymi metodami). Ponadto zakłócanie to także wprowadzania programów nastawionych na fizyczne niszczenie zawartości np. baz danych, poprzez ich kasowanie, infekowanie wirusami lub powodowanie przeciążeń napięciowych i konsekwencji powodując destrukcję (przepalenie) części elektronicznych (celowe zdalne przeciążenia procesora, pamięci, karty graficznej). Całość tych procesów może być starowana z oddalonego na odległość komputera. Ogólnie można wyróżnić dwa sposoby wtargnięcia do sieci lub komputerów. Pierwszy złamanie zabezpieczeń i wprowadzanie programów z dowolnego miejsca na świecie, a drugi to fizyczne podłączenie się do sieci będącej przedmiotem zainteresowania. Ponieważ wiele odbiorców stosuje odpowiednie zabezpieczenia sieci i uniemożliwia zdalne włamywanie się do systemów komputerowych od osób zdobywających informacje wymaga się odpowiedniej wiedzy i doświadczenia, co przy obecnym poziomie wykształcenia nie jest problemem. Ponadto dużo większy problem stanowią sieci ulokowanie poza możliwościami fizycznego dotarcia dla zwykłych żołnierzy (cyberwojowników), alternatywą jest wykorzystanie urządzeń uniwersalnych przenoszonych przez siły specjalne i rozstawianych w ugrupowaniu (na terenie) przeciwnika. Takie urządzenie może prowadzić rozpoznanie radioelektroniczne

w tradycyjnym znaczeniu (np. na potrzeby WE) i jednocześnie monitorować obszar terenu w poszukiwaniu pożądanej sieci informatycznej. Jak zostanie zlokalizowana sieć wówczas odpowiednimi programami możliwa będzie realizacja zadań z obszaru walki cybernetycznej.
Uniwersalność urządzeń rozpoznawczych i ich zarządzanie (automatyzowanie) działań podyktowane jest zarówno oszczędnościami finansowymi (mniejsze gabaryty, mniejszy kosz produkcji) oraz masowością, i szerokim spektrum wykorzystania, mniejszą liczba kanałów sterujących urządzeniami rozpoznawczymi (oszczędność). Najlepiej do tej roli predysponują urządzenia czujnikowe spełniające wiele funkcji, od rozpoznawczych poprzez zakłócające do miny pułapki.
Odrębnym problemem są zabezpieczenia sieci komputerowych. Obrona w walce cybernetycznej skupia się głównie na przedsięwzięciach technicznych ochrony komputerów (programy, urządzenia ekranujące, monitujące wtargnięcie do pomieszczeń i komputerów) oraz przedsięwzięcia organizacyjne polegające na takiej organizacji zarządzania siecią aby nikt niepowołany nie miał dostępu do pojedynczej końcówki sieci a szczególnie do serwera, do pomieszczeń do kart identyfikacyjnych itp.
Wspólna automatyzacja urządzeń elektronicznych na potrzeby WE i WC jest możliwa tylko w ograniczonym zakresie i w stosunku do wyspecjalizowanych urządzeń rozpoznawczych. Jak wykazują wnioski i doświadczenia z minionych konfliktów przyszłe środowisko walki sukcesywnie wymusza na nas zmianę filozofii myślenia o przyszłych systemach rozpoznawczych dlatego, proponowane rozwiązanie może stanowić alternatywę dla nowych rozwiązań technicznych.

5. Zakończenie

Ciągła ewolucja poglądów na prowadzenie działań zbrojnych w środowiskach innych niż elektromagnetyczne w wielu armiach oraz permanentna reorganizacja rozpoznania nie sprowadza się tylko do zmian strukturalnych i doktrynalnych. Nowe ukierunkowanie na inne środowiska oznacza, że chodzi o głęboką transformację, która będzie trwać stosunkowo długo, być może ponad 20 lat. Chodzi, bowiem przede wszystkim o zmiany mentalności i koncepcji w problemach działań w sieciach informacyjnych i szerszym spojrzeniu w środowisku działania na urządzenia elektroniczne. Elektroniczny i cybernetyczny wymiar walki staje się powoli faktem. Zmiany taktyki działania, personalne, strukturalne i technologiczne powodują, że już dzisiaj należy podjąć kroki zmierzające do przemyśleń organizacyjnych, funkcjonalnych i konstrukcyjnych wykorzystujących urządzenia elektroniczne zdolnych działać w wielu różnych środowiskach równocześnie. Konstrukcje jednorodnych urządzeń działających stricte w jednym środowisku są drogie, gabarytowo duże i szybko wykrywalne na polu walki. Urządzenia małe, uniwersalne spełniające wiele funkcji będą zdolne do osiągnięcie takiego stopnia doskonałości rozpoznania, by móc

w przyszłości lepiej realizować skomplikowane zadania. Automatyzacja tych urządzeń jest wiec wymogiem i koniecznością.
Zmiany te są, i prawdopodobnie nadal będą, wykonywane w trakcie wypełniania przez wojska różnorodnych zadań (misji). Oznacza to, że równolegle przebiegają (i należy przypuszczać, że nadal będą przebiegać) trzy procesy: udział rozpoznania w operacjach (misjach) z użyciem aktualnego sprzętu rozpoznawczego, przekształcanie systemów do postaci zautomatyzowanych oraz szukanie nowych rozwiązań technicznych. Dlatego zadania, rozpoznawcze, WE, walki cybernetycznej realizowane będą w bardzo skomplikowanych warunkach. Uwzględniając powyższe, można sądzić, że w najbliższych latach w SZ RP nadal dominującym środowiskiem działania urządzeń i systemów WE pozostanie spektrum EM, a automatyzacja działania systemów systematycznie będzie się rozwijać. W środowisku cybernetycznym automatyzacja urządzeń ma ograniczony zasięg, ale rozpatrując trudności w dostępie do wybranych sieci (szczególnie zamkniętych typu LAN) wspólne urządzania elektroniczne (np. czujniki) można rozpatrywać na płaszczyźnie automatyzacji.
Nowe pojęcia związane z środowiskiem elektronicznym są problemem poddanym do ogólnej dyskusji. Weryfikacja ich przydatności powinna nastąpić na drodze rozważań naukowych i po weryfikacji może zostać ujęta w doktrynach i podręcznikach. Te rozważania jeszcze przed nami.
Automatyzacja i miniaturyzacja zmieniają podejście naukowców do problemów rozpoznawania w różnych środowiskach. Jednostki WE już dzisiaj realizują zadnia nie tylko w spektrum fal EM, ale próbują rozszerzyć swoja działalność o inne środowiska. Bez przyszłościowego spojrzenia na całość problematyki rozpoznania, może się okazać, że spektrum fal EM po 50 latach burzliwego rozwoju ustąpi miejsca innemu środowisku, a „my" przegapimy ten moment. Następuje kolejny etap rozwoju ludzkości i kolejna era dominacji, tym razem informatycznej. Powinniśmy być przygotowania na nadchodzące zmiany.

6. Literatura

[1] Bauman Z., *Globalizacja, czyli komu globalizacja, a komu lokalizacja, "Studia socjologiczne*", nr 3, 1997.
[2] Bauman Z, *Globalizacja*, Warszawa 2000.
[3] Bógdał-Brzezinska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* ASPRA-JR, Warszawa 2003.
[4] Czeszejko S. *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji,* AON, Warszawa 2011
[5] *Cyberspace Operations* (*DD 3-12*), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010.
[6] Grabau, *Sześć wymiarów wojny*, WPZ nr 1,2,3, Warszawa, 1987
[7] Howard M, *Wojna w dziejach Europy*, Ossolineum, Wrocław 1990.

[8] Konopka L., *Walka sieciocentryczne sposobem działania sił zbrojnych w przyszłości*, Myśl Wojskowa, nr 2/2006.
[9] *Mały słownik Cybernetyczny*, Wiedza Powszechna, Warszawa 1973.
[10] Materiały robocze Centrum Bezpieczeństwa Cybernetycznego, Białobrzegi, 2011.
[11] *National Military Strategy for Cyberspace Operations – NMS-CO,* Joint Chiefs of Staff, Waszyngton, 2006,
[12] Price A., *Narzędzia mroku*, Wydawnictwo Dolnośląskie, Wrocław 2006
[13] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia,* Warszawa, 2009.
[14] Scheffs W., *Walka elektroniczna w operacji i walce,* AON, Warszawa 2005.
[15] Scheffs W, *Środowisko działania sensorów walki elektronicznej*, ZN AON nr 4/2010
[16] Sienkiewicz P., *Wizje i modele wojny informacyjnej*. w: *Społeczeństwo informacyjne – wizja czy rzeczywistość ?,* Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003.
[17] Vego M., *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona nr 2, Warszawa, 2009.
[18] http://en.wikipedia.org/cybrprzestrzeń

płk dr inż. Waldemar Scheffs, *adiunkt – Kierownik Zakładu Rozpoznani i Walki Elektronicznej Akademii Obrony Narodowej. Absolwent Wyższej Oficerskiej Szkoły Radiotechnicznej w Jeleniej Górze oraz Akademii Obrony Narodowej w Warszawie. W latach 1985-1993 pełnił służbę na rożnych stanowiskach w pułku rozpoznania radioelektronicznego, od 1994r. jest nauczycielem w AON. W 2001 roku obronił rozprawę doktorską w specjalności dowodzenie. Autor podręczników i artykułów z rozpoznania, walki elektronicznej i działań informacyjnych.*