

SZTUKA WOJENNA



MILITARNE ASPEKTY ŚRODOWISKA ELEKTRONICZNEGO – PRÓBA REWIZJI ISTNIEJĄCEJ TERMINOLOGII

ppłk dypl. dr inż. Stanisław CZESZEJKO
Dowództwo Generalne Rodzajów Sił Zbrojnych



prof. dr hab. Józef JANCZAK
Akademia Obrony Narodowej

Streszczenie

Coraz bardziej powszechna obecność urządzeń i systemów elektronicznych w życiu człowieka powoduje, że przedstawiciele kilku ostatnich pokoleń podejmują próby opisanie zjawisk zachodzących z ich udziałem. Próby te, podejmowane w celu usystematyzowania postrzegania nowego – w stosunku do istnienia gatunku ludzkiego – „świata” urządzeń i systemów elektronicznych na tle innych aktywności ludzkich, mocno komplikuje fakt jego dynamicznego rozwoju. Autorzy, na bazie bogatego doświadczenia zebranego w ramach wieloletniej pracy związanej z wykorzystaniem urządzeń i systemów elektronicznych, uważają, iż należy opracować nowe podstawy teoretyczne (w tym aparat pojęciowy), bardziej uniwersalne od obecnie istniejących. W niniejszym artykule autorzy proponują wprowadzenie nazwy „środowiska elektronicznego”, będącej synonimem miejsca prowadzenia części działań militarnych, w którym wykorzystuje się urządzenia i systemy elektroniczne. Uzasadniają również w obszerny sposób przyjęty punkt widzenia oraz wykazują zasadność proponowanych zmian.

Słowa kluczowe: sieciocentryczność, świadomość sytuacyjna pola walki, operacje informacyjne.

Wprowadzenie

Istniejące w naturze zjawiska fizyczne związane z silnymi wyładowaniami elektrycznymi w atmosferze, powstające naturalnie, towarzyszące zwykle burzom, były bacznie obserwowane przez ludzi przez kolejne tysiąclecia. Odkryto również szereg zjawisk, którym towarzyszyło zdecydowanie mniej energii elektrycznej, np. powstawanie ładunków elektrostatycznych – tzw. elektryzowanie się. Opisy oddziaływania elektrostatycznego jako jedni z pierwszych pozostawili nam starożytni Grecy. To oni odkryli, że bursztyn (po gr. *elektron*) po potarciu przyciąga drobne przedmioty. Dopiero rozwój nauki w ostatnich kilku stuleciach umożliwił poznanie tych zjawisk powstających w naturze na tyle dobrze, że doprowadził do ich wykorzystywania na potrzeby człowieka. Zaczęto konstruować urządzenia elektryczne i elektroniczne o coraz większym stopniu skomplikowania, na pewnym etapie rozwoju możliwe stało się łączenie ich w różnego rodzaju systemy. Tak oto w nienaturalny, sztuczny sposób wytwarzano prąd, promieniowanie elektromagnetyczne oraz inne efek-

ty fizyczne, które następnie w fizyce¹ opisywano w dziale „elektryczność i magnetyzm”. Oczywiście wojownicza strona natury ludzkiej znalazła zastosowanie dla nowych wynalazków na klasycznym polu walki, i na tym „cichym”, oddalonym nieraz setki kilometrów od linii frontu.

Wraz z rozwojem militarnych urządzeń i systemów elektronicznych tworzono teorię ich wykorzystania, w tym nazewnictwo oraz rozpoczęto uwzględnianie ich obecności w istniejących doktrynach. Oczywiście, aby móc prowadzić działania militarne z ich wykorzystaniem, dokonano pewnych uregulowań. Utworzono wiele pojęć i przedstawiano różne propozycje uregulowania zagadnień z nimi związanych, ale rozbieżności w ich postrzeganiu budzą wciąż wiele wątpliwości. W związku z tym nasuwają się następujące pytania: Czy funkcjonujące uregulowania pozostają nadal aktualne? Czy postrzeganie tej tematyki nie powinno ulec rewizji? Otóż w przeświadczeniu autorów tak.

¹ Istniejący obecnie zakres zainteresowania fizyki ukształtowany został w XIX i na początku XX wieku, wtedy to wyłonił się zasadniczy podział fizyki klasycznej, obejmującej następujące działy: mechanikę, optykę, naukę o ciepłe, elektryczność i magnetyzm (Źródło: <http://pl.wikipedia.org/wiki/Fizyka> – dostęp 31.01.2014 r.).

Czwarty wymiar wojny

W trakcie II wojny światowej działania z wykorzystaniem urządzeń i systemów elektronicznych stały się dość ważnym i powszechnie uznawanym przez dowodzących elementem zabezpieczenia prowadzonych działań bojowych, doczekały się nawet pod jej koniec własnej nazwy. Określono je mianem „wojny radioelektronicznej”, co z punktu widzenia dowódców prowadzących walkę miało swoje racjonalne uzasadnienie – w głównej mierze wykorzystywali oni w niej przecież bezpośrednio fale radiowe (promieniowanie elektromagnetyczne) pochodzące z radiowych urządzeń elektronicznych.

Własne poglądy na ten temat przedstawił brytyjski historyk Michael Howard, w swojej książce pt. *Wojna w dziejach Europy* (w rozdziale VII pt. *Wojny techników*), wydanej w 1976 roku w Wielkiej Brytanii. W jego ocenie już w okresie I wojny światowej powstał, a w czasie II wojny światowej nastąpił dalszy intensywny rozwój nowego „czwartego wymiaru wojny” (po lądowym, morskim i powietrznym)², tj. wojny związanej ówczesnie z rozwojem i wykorzystaniem elektronicznych urządzeń łączności, kryptografii, rozpoznania i walki radioelektronicznej oraz radiolokacji, wykorzystujących głównie promieniowanie elektromagnetyczne. Jak widać Michael Howard, jako historyk i teoretyk, szerzej postrzegał problematykę wykorzystania urządzeń i systemów elektronicznych na potrzeby działań zbrojnych w stosunku do wojskowych pragmatyków z okresu II wojny światowej, gdyż wyraźnie zaakcentował pośród nich obecność urządzeń kryptografii, które nie emitują fal radiowych. Ważny z naszego punktu rozważań jest fakt, iż nie nazwał on owego nowego „czwartego wymiaru wojny”, a jedynie wskazał na jego istnienie.

Spojrzenie M. Howarda na tę złożoną problematykę miało szerokie oddziaływanie. Już na początku lat osiemdziesiątych można znaleźć odzwierciedlenie jego poglądów w polskim piśmiennictwie, w którym spotka się m.in. określenie „czwarty wymiar konfrontacji zbrojnej z przeciwnikiem”³. Znany polski teoretyk wojskowy zajmujący się problematyką rozpoznania i walki elektronicznej (RiWE) oraz walką informacyjną, profesor Leopold Ciborowski, jeszcze pod koniec lat dzie-

więćdziesiątych wskazuje, iż nawet w trakcie pierwszej wojny w rejonie Zatoki Perskiej twierdzono, że walka wkroczyła w „czwarty wymiar”, którym jest przestrzeń elektromagnetyczna⁴.

Naturalnym efektem, będącym reakcją na wskazanie kolejnego wymiaru wojny, były próby jego nazwania. Jedną z takich prób podjął w połowie lat osiemdziesiątych oficer Bundeswehry (SZ RFN) pułkownik Rudolf Grabau. Nie ograniczył się on jedynie do wskazania nazwy dla „czwartego wymiaru wojny” („*fourth dimension of war*”) („spektrum elektromagnetyczne” – „*electromagnetic spectrum*”), lecz przedstawił własny podział wojny na sześć jej wymiarów: odległość (*distance*) – utożsamiającą oddalenie w linii prostej; powierzchnię (*surface area*) (szerokość i głębokość) – utożsamiającą teren; wysokość (*height*) – utożsamiającą przestrzeń poprzez dopełnianie powierzchni; czas (*time*); informacje (*information*); spektrum elektromagnetyczne⁵ (*electromagnetic spectrum*). Wskazał wówczas, że ostatnie trzy czynniki będą mieć decydujący wpływ na charakter przyszłych konfliktów zbrojnych.

Nie jest wykluczone, że przyjęte przez pułkownika Grabau nazewnictwo (spektrum elektromagnetyczne) dla „czwartego wymiaru wojny” M. Howarda jest pewnego rodzaju pokłosiem stosowania w kręgach militarnych różnych państw nazwy „wojny radioelektronicznej”, utożsamianej jednoznacznie z wykorzystaniem fal radiowych. Pewnym wytłumaczeniem poprawności przyjętego przez niego podziału może być fakt, że wymienione wcześniej przez M. Howarda elektroniczne urządzenia kryptografii można umiejscowić w podziale R. Grabau w obszarze informacji.

Środowisko elektromagnetyczne

W specjalistycznym piśmiennictwie polskim funkcjonuje nazwa „środowisko elektromagnetyczne”, które rozumiane jest jako środowisko rozprzestrzeniania się energii elektromagnetycznej⁶. Można też odnaleźć poglądy, w których nasi

⁴ L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, s. 35.

⁵ R. Grabau, *Sechs Dimensionen des Krieges. Versuch einer analytischen Betrachtung*, miesięcznik Soldat und Technik, nr 5, 1985, s. 245.

⁶ W. Scheffs, *Proces oceny przeciwnika w aspekcie elektronicznym*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007, s. 121.

² M. Howard, *Wojna w dziejach Europy*, Ossolineum, Wrocław, 1990, s. 167.

³ H. Piekarski, *Walka radioelektroniczna*, Wydawnictwo MON, Warszawa, 1980, s. 5.

specjaliści twierdzą, że *widmo elektromagnetyczne (obok cyberprzestrzeni) jest kolejnym wymiarem współczesnego pola walki*⁷.

Niektóre źródła wskazują, że w ramach ogólnego podziału prowadzenia walki informacyjnej⁸ wyróżnia się: osobową przestrzeń walki informacyjnej oraz techniczną przestrzeń walki informacyjnej. Podobny podział przyjęto dla rozpoznania⁹, które dzieli się na rozpoznanie: osobowe i techniczne. Ten drugi rodzaj rozpoznania (techniczne) prowadzi się z pomocą specjalistycznych urządzeń, które mogą rozpoznawać i rejestrować efekty i zjawiska w następujących środowiskach: elektromagnetycznym, sprężystym, elektrycznym, magnetycznym oraz chemicznym. Wymienione tu środowiska wymieniane są w obydwu opracowaniach, i tym dotyczącym walki informacyjnej, i tym dotyczącym rozpoznania. W obu wymieniono również oczywiście „środowisko elektromagnetyczne”.

Czy pojęcie „środowiska elektromagnetycznego” można uznać za właściwą nazwę dla „czwartego wymiaru wojny”? Wiele faktów wskazuje na to, że nie. Ale dlaczego?

W rozważaniach na ten temat należy ocenić w pierwszej kolejności źródła powstawania promieniowania elektromagnetycznego. W naturze występuje ich wiele (np. promieniowanie słoneczne, wyładowania atmosferyczne itd.)¹⁰, ale w praktyce na wszystkie naturalne źródła promieniowania elektromagnetycznego człowiek nie potrafi wpływać w taki sposób, by doprowadzić formę ich promieniowania do postaci użytecznej (pożądaną przez niego).

Sytuacja zmieniła się dopiero po odkryciu elektryczności i poznaniu zjawisk fizycznych jej towarzyszących. Wraz z budowaniem coraz większej wiedzy na ten temat możliwe stało się konstruowanie urządzeń elektrycznych i elektronicznych, również tych będących sztucznymi źródłami pro-

mieniowania elektromagnetycznego. W obwodach urządzeń elektrycznych i elektronicznych wytwarzany jest w pierwszej kolejności prąd elektryczny (*electric current*), który jest uporządkowanym (skierowanym) ruchem ładunków elektrycznych (*electric charge*) (dodatnich – np. kationów; lub ujemnych – np. elektronów, anionów). Dopiero poruszający się w ładunek elektryczny wytwarza – w uproszczeniu – pole elektromagnetyczne, a rozchodzące się w przestrzeni otaczającej obwody elektryczne zaburzenia pola elektromagnetycznego to promieniowanie elektromagnetyczne (fale elektromagnetyczne). Urządzeniem do zamiany sygnału elektrycznego na promieniowanie (fale) elektromagnetyczne (i odwrotnie) jest antena.

Należy mieć na uwadze, że jedynie urządzenia elektroniczne są w stanie wytwarzać i przetwarzać skomplikowane sygnały elektryczne użyteczne obecnie dla człowieka (w tym cyfrowe), które mogą być zamieniane na postać pożądanego promieniowania elektromagnetycznego (i odwrotnie). W związku z powyższym widać wyraźnie, że użyteczne promieniowanie elektromagnetyczne jest jedynie skutkiem funkcjonowania urządzeń elektronicznych i nie jest jedynym ich „owocem” wykorzystywanym przez człowieka. Dlatego też – w dużym uproszczeniu – używanie w przeszłości pojęcia „środowiska elektromagnetycznego” miało kiedyś swoje pragmatyczne uzasadnienie, choć niekoniecznie rzeczywiste. Obecnie musimy uwzględnić wszystkie czynniki związane z istnieniem elektroniki, które mają wpływ na naszą ocenę terminologii wykorzystania urządzeń i systemów elektronicznych w taki sposób, by była ona obiektywna i najbardziej odpowiadała panującej rzeczywistości. W dobie wszechobecnych sieci komputerowych innego znaczenia nabrało wykorzystywanie prądu elektrycznego do wytwarzania i przesyłania sygnałów elektrycznych. Dlatego pojęcie „środowisko elektromagnetyczne” nie spełnia wymaganych warunków, aby zyskać miano „czwartego wymiaru wojny”.

Walka elektroniczna

Pojęcie „walka elektroniczna” wywodzi się w prostej linii z pojęcia „walki radioelektronicznej”¹¹, to ostatnie natomiast bezpośrednio z po-

¹¹ W polskiej literaturze przedmiotowej tematyki termin „walka radioelektroniczna” stosowano do 2002 roku [za:

⁷ M. Blach, *Bazy danych elementem skuteczności rozpoznania elektronicznego*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, s. 28.

⁸ L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, s. 112.

⁹ W. Błażejczyk, Gabriel Nowacki, Waldemar Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa, 2002, s. 31.

¹⁰ T. Rybak, *Raport o stanie środowiska w 2010 r. 6. Promieniowanie elektromagnetyczne* (Źródło – dostęp: 24.02.2014 r.: http://www.wios.rzeszow.pl/cms/upload/edit/file/stan_srodowiska_2010/r6.pdf).

jęcia „wojny radioelektronicznej”, jak wcześniej wspomniano, powstałego pod koniec II wojny światowej.

Jedną z ważniejszych pozycji w piśmiennictwie polskim w zakresie opisującym walkę elektroniczną jest praca Leopolda Ciborowskiego z 1993 roku, w której autor bardzo szeroko stosował analizę i modelowanie matematyczne. L. Ciborowski jest typowym przedstawicielem „szkoły”, dla której aparat matematyczny był podstawą wszelkich rozważań naukowych, stąd też we wskazanej pozycji większość hipotez została zweryfikowana z wykorzystaniem metod matematycznych. Już na pierwszych stronach pracy wskazuje on, że *walka elektroniczna zakłóca proces informacyjny przeciwnika (obieg i treść informacji) w sferze elektromagnetycznej*¹², co jednoznacznie charakteryzuje zakres jej działania. Przedstawia również podział rozpoznania ogólnego na¹³: rozpoznanie osobowe i rozpoznanie elektroniczne (podział rozpoznania ogólnego w późniejszych latach ulega przekształceniu i zawiera obecnie¹⁴: rozpoznanie osobowe i rozpoznanie techniczne).

Warto zapoznać się także z definicjami różnych reprezentantów SZ RP, przedstawionych chronologicznie, definiujących interesujący nas obszar działań militarnych jako:

Walka radioelektroniczna¹⁵ (wg AON – 1994 r.) – to całokształt przedsięwzięć i działań wojsk, które wykorzystując energię elektromagnetyczną, zmierzają do rozpoznania i zdeorganizowania systemów radioelektronicznych przeciwnika oraz zapewnienia warunków stabilnej pracy systemom wojsk własnych.

Walka elektroniczna¹⁶ (wg AON – 2000 r.) – to zespół przedsięwzięć i działań wyspecjalizowanych sił, sprzężonych ze sobą organizacyjnie i funkcjonalnie, których celem jest rozpoznanie i dezorganizacja systemów (środków) elektronicznych przeciwnika oraz zapewnienie warunków

do stabilnej pracy analogicznym systemom (środkom) wojsk własnych. Obejmuje ono rozpoznanie, obezwładnianie i obronę radioelektroniczną, realizowane z wykorzystaniem promieniowania energii elektromagnetycznej, w tym wywoływania zmian środowiska elektromagnetycznego oraz wzbudzenia silnych impulsów elektromagnetycznych.

Walka elektroniczna¹⁷ (wg SG WP – 2003 r.) – działania militarne polegające na rozpoznawaniu źródeł emisji elektromagnetycznej oraz dezorganizowaniu pracy systemów elektronicznych przeciwnika wykorzystujących energię elektromagnetyczną, w tym energię wiązkową, przy jednoczesnym zapewnieniu warunków ich efektywnego użycia przez wojska własne.

Warto również zapoznać się z poglądami (definicjami) naszych sojuszników, którzy odgrywają wiodącą rolę w dziedzinie walki elektronicznej i w związku z tym niejednokrotnie kreują pojęcia obowiązujące w Sojuszu. Oto kilka przykładów, przedstawionych również chronologicznie:

Walka elektroniczna¹⁸ (wg USA – 1999 r.) – to każde działanie militarne wiążące się z użyciem energii elektromagnetycznej lub wiązkowej, prowadzone dla kontroli spektrum elektromagnetycznego lub atakowania przeciwnika.

Walka elektroniczna¹⁹ (wg USA – 2010 r.) – działalność militarna obejmująca użycie energii elektromagnetycznej i wiązkowej w celu kontroli spektrum elektromagnetycznego lub ataku prowadzonego przeciwko przeciwnikowi.

Pomimo jednoznaczności zakreslenia obszaru działania we wszystkich wskazanych definicjach i większości twierdzeń nt. „walki elektronicznej”, niektórzy autorzy postrzegają jednak walkę elektroniczną nieco szerzej.

W swojej pracy studyjnej z roku 2001 pracownik AON płk dr inż. Józef Janczak wymienia w ramach rozpoznania elektronicznego następu-

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

¹² L. Ciborowski, *Rozpoznanie i Walka Elektroniczna*, AON, Warszawa 1993, s. 13.

¹³ Ibidem, s. 58.

¹⁴ W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa 2002, s. 29.

¹⁵ Z. Magnucki (red.), *Walka radioelektroniczna w SZ RP*, AON, Warszawa 1994, s. 11.

¹⁶ Z. Dubrawski, *Walka radioelektroniczna prowadzona przez SP. Studium operacyjne*, AON, Warszawa 2000, s. 39, 56.

¹⁷ *Walka elektroniczna*, Sztab Generalny WP, Warszawa, 2003 (Szt. Gen. 1549/2003), Załącznik C – Słownik terminów definicji i skrótów.

¹⁸ R. Szypra, *Militarne operacje informacyjne*, AON, Warszawa, 2003, s. 108 (tłumaczenie z: AFDD 2-5.1: *Electronic Warfare*, Washington D.C., 1999).

¹⁹ Oryginalna wersja językowa: *Electronic Warfare – military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 52 [wskazano tam, że definicja zaczerpnięta została z: *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms*, USA].

jące elementy²⁰: rozpoznanie radioelektroniczne; rozpoznanie radiolokacyjne; rozpoznanie informatyczne; rozpoznanie optoelektroniczne; rozpoznanie czujnikowe. Podobnie przedstawił on podział zakłóceń aktywnych, które wg jego poglądów składają się z²¹: zakłóceń radiowych; zakłóceń radiolokacyjnych; zakłóceń radionawigacyjnych; zakłóceń optoelektronicznych; zakłóceń informatycznych. Autor ten wskazuje również, że działania militarne w ramach walki elektronicznej prowadzone są na specyficznym „elektronicznym polu walki”, które można określić mianem „środowiska elektromagnetycznego” (dotyczącego środowisk elektronicznych promieniujących i odbierających energię elektromagnetyczną)²². Poglądy J. Janczaka wyraźnie kierują się w stronę szerszego postrzegania problematyki wykorzystania urządzeń i systemów elektronicznych w działaniach militarnych, czego dowodem niech będzie włączenie w tą tematykę również obszaru informatyki.

W niektórych źródłach przedstawia się podział rozpoznania technicznego wg kryterium wyróżnialności²³, jakim jest „środowisko nośników danych”, i dzieli się je na: rozpoznanie elektromagnetyczne; rozpoznanie czujnikowe (prowadzone w środowisku: akustycznym, elektrycznym, magnetycznym oraz chemicznym); rozpoznanie informatyczne (związane z techniką komputerową i jej otoczeniem, w tym monitorowanie promieniowania z monitora lub jego części zewnętrznych – np. połączeń kablowych).

Dwaj inni oficerowie – pracownicy AON, płk dr inż. Marian Łokociejewski oraz płk dr inż. Waldemar Scheffs, w swojej pracy z roku 2005 wskazują, że prowadzenie walki elektronicznej nie powinno ograniczać się jedynie do przestrzeni elektromagnetycznej, lecz należy rozszerzyć jej oddziaływanie na inne urządzenia elektroniczne (w tym na te niewykorzystujące energii elektromagnetycznej)²⁴. Według autorów takie podejście umożliwia rozszerzenie walki elektronicznej na oddziaływanie kinetyczne (ogniowe) z wykorzystaniem pocisków samonaprowadzających się na

systemy elektroniczne oraz umożliwia szersze spojrzenie na obronę elektroniczną, w tym systemów informatycznych. Swoją poglądy uzasadniają tym, że gdyby ograniczać się do prowadzenia działań militarnych w przestrzeni elektromagnetycznej, należałoby pozostać przy wykorzystywaniu nazwy „walka radioelektroniczna” jako bardziej adekwatnej.

Dalsze rozważania w podobnym kierunku prowadził w pracach naukowych płk Waldemar Scheffs, który w swoim wystąpieniu podczas międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” w 2008 roku przedstawił, że oprócz przestrzeni elektromagnetycznej można wyróżnić inne środowiska, w których prowadzi się walkę elektroniczną. Zaliczył on wówczas do nich: przestrzeń działania systemów informatycznych, przestrzeń akustyczną, pole magnetyczne²⁵.

Reasumując rozważania nt. walki elektronicznej, należy zauważyć, że zgodnie z regułami nazewnictwa pojęcie „walka” wymaga dodania wyrazu uzupełniającego, który związany będzie z identyfikacją sfery, w której jest, była lub będzie ona prowadzona. Natomiast identyfikacja przedmiotu walki decyduje nie o jej nazewnictwie, ale o doborze narzędzi do jej prowadzenia i sposobów ich wykorzystywania w konkretnym działaniu²⁶. W związku z tym, że nie wszystkie działania związane z wykorzystaniem urządzeń i systemów elektronicznych są walką, nie możemy po prostu poszerzyć pojęcia „walka elektroniczna” na cały obszar działań militarnych z wykorzystaniem urządzeń i systemów elektronicznych. Dlatego należy kontynuować poszukiwania bardziej adekwatnego systemu pojęć, związanego z przedmiotową tematyką.

Walka informacyjna

Innym interesującym nas tutaj rodzajem walki, który zdefiniowano na potrzeby prowadzenia działań militarnych (i nie tylko) jest walka informacyjna. Należy zauważyć, że choć może nie występowała ona pod taką nazwą wcześniej, to pro-

²⁰ J. Janczak, *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, AON, Warszawa, 2001, s. 17.

²¹ Ibidem, s. 131.

²² Ibidem, s. 203.

²³ W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa, 2002, s. 32, 36.

²⁴ M. Łokociejewski, W. Scheffs, *Walka elektroniczna w operacji i walce*, AON, Warszawa, 2005, s. 10.

²⁵ W. Scheffs, *Założenia walki elektronicznej w środowisku sieciocentrycznym*, [w:] materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, s. 113.

²⁶ L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, s. 69.

wadzone ją „od zarania dziejów” ludzkości, czego potwierdzenie można odnaleźć na przykład w wybitnym dziele starożytnego myśliciela i stratega Sun Zi. Skonstruowane przez człowieka urządzenia i systemy elektroniczne stały się tylko narzędziem w prowadzeniu walki tego rodzaju, choć odgrywają w niej coraz większą rolę.

Leopold Ciborowski w swojej pracy z końca lat dziewięćdziesiątych nt. walki informacyjnej, podobnie jak w innych pracach, stosuje również szeroko pojęcia i aparat matematyczny do uzasadnienia swych poglądów. Wskazuje wręcz, że większą precyzję interpretacji w tym obszarze zapewnia słownictwo cybernetyczne i matematyczne²⁷. Przedstawia nam też części składowe walki informacyjnej, wyodrębnione w USA w 1994 roku, na które składają się²⁸: walka elektroniczna, działania psychologiczne oraz walka informatyczna. Wskazuje też na przykładzie poglądów byłego oficera SP USA płk. rez. D. Camptena, który rozszerzył zakres walki informacyjnej na sferę pozamilitarną²⁹, że w USA jej pojmowanie ewaluowało w dość krótkim czasie.

Wcześniejsze poglądy amerykańskie można odnaleźć w doktrynie NATO z 2009 roku³⁰, gdzie w skład Operacji Informacyjnych (*Information Operations – IO*) prowadzonych przez Sojusz obok innych czynników wchodzi m.in. jednocześnie dwa najważniejsze rodzaje działań związanych z wykorzystaniem urządzeń i systemów elektronicznych, tj. walka elektroniczna (*Electronic Warfare – EW*) oraz działania w sieciach informatycznych (*Computer Network Operations – CNO*).

Natomiast już w 2011 roku widać wyraźną różnicę amerykańskich poglądów w stosunku do poprzednio prezentowanych. W dokumentach dotyczących bezpieczeństwa państwa wskazuje się, że operacje Informacyjne (*Information Operations – IO*) prowadzi się równolegle z działaniami w sieciach informatycznych (*Computer Network Operations – CNO*) oraz z walką elektroniczną (*Electronic Warfare – EW*). Wszystkie te rodzaje działań, choć nie są jedynymi, są w USA równoważnymi sobie narzędziami polityki bezpieczeństwa państwa w obszarze elementu potęgi narodowej USA o nazwie „Informacja”, który jest

jednym z wielu elementów tworzących potęgę narodową Stanów Zjednoczonych³¹.

Jak widać na powyższych przykładach, brak jest konsekwencji w umiejscowieniu dwóch najważniejszych rodzajów działań z wykorzystaniem urządzeń i systemów elektronicznych (tj. *EW* i *CNO*), ta rozbieżność świadczy o braku jednolitych poglądów na tę tematykę oraz ciągłym poszukiwaniu i kształtowaniu się poglądów w tym obszarze. Widać tu też złożoność tej problematyki i próby poszukiwania własnych (jak widać na amerykańskim przykładzie), nieraz rozbieżnych w stosunku do Sojuszu, rozwiązań tej problematyki.

Przy rozpatrywaniu wykorzystywania urządzeń i systemów elektronicznych poruszono tematykę walki informacyjnej, mimo że są one jedynie narzędziem wykorzystywanym do jej prowadzenia. Większość dostępnych definicji walki i operacji informacyjnych, ujętych w amerykańskich dokumentach normatywnych z 1995 roku, z 1996 roku, z 1998 roku, z 2009 roku oraz NATO-wskich z 2008 roku i z 2010 roku nie opisuje relacji (zależności) pomiędzy walką informacyjną a urządzeniami i systemami elektronicznymi (walką elektroniczną oraz cyberprzestrzenią).

Nie mniej jednak można się zetknąć z poglądami, które próbują w pewien sposób interpretować walkę informacyjną jako „czwarty wymiar wojny” M. Howarda. Otóż w 1995 roku Martin Libicki, pracownik *National Defence University* w Waszyngtonie, podzielił operacje informacyjne na 7 form (elementów)³²: wojna w zakresie dowodzenia i kontroli (*C2W – Command and Control War*); wojna wywiadowczo-rozpoznawcza (*Intelligence-Based War*); wojna elektroniczna (*Electronic War*); wojna hakerska (*Hacker War*); wojna o informacje ekonomiczne (*Economic Information War*); wojna cybernetyczna lub sieciowa (*Cyber or Net War*); operacje psychologiczne (*Psychological Operations*). Możemy odnaleźć tu prawie wszystkie obszary wykorzystania urządzeń i systemów elektronicznych, ale należy mieć cały czas na uwadze, że nie są one jedynymi elementami tych operacji.

³¹ Materiały z kursu pt. *Special Operations Forces Integration Course* przeprowadzonego w Akademii Obrony Narodowej w dn. 21–25.03.2011 r. przez przedstawicieli m.in. *Joint Special Operations University* z USA, s. 2.

³² A. Nowak, *Założenia dla perspektywnego systemu rozpoznania*, AON, Warszawa, 2004, s. 65 (z: Martin Libicki, *What is Information Warfare*, Washington, 1995).

²⁷ Ibidem, s. 95.

²⁸ Ibidem, s. 37.

²⁹ Ibidem, s. 39.

³⁰ *Połączona sojusznicza doktryna operacji informacyjnych (AJP-3.10)*, Agencja Standaryzacji NATO (NSA), 2009, pkt 0126, pkt. 0129.

Prowadząc rozważania w zakresie walki informacyjnej, można mieć przez moment wrażenie, że pretendują one do miana „czwartego wymiaru wojny” wg M. Howarda. Obszary wykorzystywania urządzeń i systemów elektronicznych nie są jedynymi elementami wykorzystywanymi do prowadzenia operacji informacyjnych, wchodzą w ich skład również działania psychologiczne (operacje psychologiczne). Dlatego pojęcie „walka informacyjna” nie jest właściwe do opisywania działań z wykorzystaniem urządzeń i systemów elektronicznych, tj. nie może być nazywana „czwartym wymiarem wojny”.

Przestrzeń cybernetyczna – cyberprzestrzeń

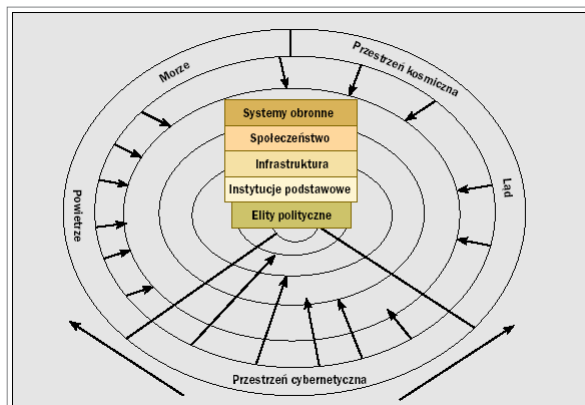
Pojęciem, które od pewnego czasu wykorzystuje się na potrzeby prowadzenia działań militarnych, jest cyberprzestrzeń. Jego wykorzystywanie w terminologii militarnej ściśle wiąże się z konstruowaniem przez człowieka urządzeń i systemów elektronicznych służących do transmisji danych i informacji – sieci komputerowych (teleinformatycznych).

Już w wystąpieniu byłego sekretarza obrony USA Franka Carlucci z 1988 roku można odnaleźć jednoznaczny ocenę wpływu rozwoju elektroniki na zdolność bojową. Wskazał, że w niedalekiej przyszłości „inteligentna technika rażenia celów, zintegrowana informatycznie z automatycznymi procesami zbierania i przetwarzania informacji, stanowić będzie w niedalekiej przyszłości najważniejszy komponent ewentualnego pola walki”³³.

Na początku lat dziewięćdziesiątych pułkownik John A. Warden z Sił Powietrznych Stanów Zjednoczonych w teorii strategicznego paraliżu ujął działania w nowej przestrzeni, nazwanej przez niego przestrzenią cybernetyczną, która obejmowała również działania w sieciach komputerowych. Warden postrzegał nieprzyjaciela jako system systemów, istotę jego systemowego podejścia stanowi model pięciu kręgów: elity polityczne (sprawujące ogólne kierownictwo); instytucje podstawowe (transponujące energię z jednego kręgu do drugiego); infrastruktura; społeczeństwo (ludzie); systemy obronne. Według Wardena każdą

organizację (np. państwo, firmę, wojsko, organizację terrorystyczną, gang przestępczy, itp.) należy traktować jak strukturę składającą się z systemu pięciu wzajemnie powiązanych kręgów (wskazanych powyżej), składających się na całość i pełniących założone dla nich funkcje³⁴.

Każdy z kręgów Wardena funkcjonuje w pięciu „wymiarach” (rysunek nr 1), na które składają się następujące elementy: morze; ląd; powietrze; przestrzeń kosmiczna; przestrzeń cybernetyczna (zwana również cyberprzestrzenią).



Źródło: P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 375.

Rys. 1. Wardenowski model pięciu wymiarów

Z opracowanego przez niego tzw. „Modelu Wardena” wynika, że umiejscowienie w nim przestrzeni cybernetycznej potwierdza uznanie istnienia kolejnego wymiaru walki (tu w kolejności piątego ze względu na ujętą przez niego przestrzeń kosmiczną)³⁵. Można wnioskować, że chociaż nie odniósł się on w żaden sposób do podziału dokonanego przez Howarda M. Friedmana³⁶, to jego „czwarty wymiar wojny” w dużym uproszczeniu nazwał po prostu „przestrzenią cybernetyczną”.

Poglądy Wardena znalazły odzwierciedlenie w oficjalnych amerykańskich poglądach na prowadzenie działań militarnych. Przykładem niech będzie przyjęta w 2004 roku Narodowa Strategia

³⁴ M. Vego, *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona nr 2, Warszawa 2009, s. 185.

³⁵ P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, w: *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 374.

³⁶ H.M. Friedman, *Securities Regulation in Cyberspace*, Aspen 2005.

³³ L. Ciborowski, *Nowe systemy i środki walki oraz kierunki ich rozwoju w SZ państw obcych*, AON, Warszawa 1993, s. 13.

Militarna, wg której Siły Zbrojne USA muszą posiadać zdolność do prowadzenia operacji na lądzie, na morzu, w powietrzu, w kosmosie i w cyberprzestrzeni, i które razem tworzą przestrzeń walki³⁷. Równoległe do takiego ujmowania podziału przestrzeni walki, w innych amerykańskich dokumentach (np. *Joint Publication (JP) 3-0* w dziale „Operacje Połączone”) wskazuje się, że „środowisko operacyjne” składa się z domeny: lądowej, morskiej, powietrznej, kosmicznej oraz środowiska informacyjnego³⁸. Przy ostatnim podziale podkreśla się, że traktowanie cyberprzestrzeni jako domeny stanowi podstawę do rozumienia i definiowania jej miejsca w operacjach militarnych. Na podstawie przytoczonych przykładów wyraźnie rysuje się pewnego rodzaju brak spójności w pojmowaniu przez amerykańskich teoretyków znaczenia i umiejscowienia cyberprzestrzeni w działaniach militarnych.

Biorąc pod uwagę naturalną ewolucję pojęcia cyberprzestrzeni od czasów ogłoszenia teorii Wardena, aby ocenić co obecnie w pojęciu naszych amerykańskich i brytyjskich sojuszników ono oznacza (obejmuje), należy poddać analizie kilka definicji związanych z tym pojęciem. Oto przykładowe (dostępne) definicje:

Cyberprzestrzeń³⁹ (wg *NATO* – 2007/2008 r.) – cyfrowy świat, stworzony przez komputery i sieci komputerowe, w którym współistnieją ze sobą ludzie i komputery, i który obejmuje wszystkie aspekty działalności w sieci komputerowej.

Cyberprzestrzeń⁴⁰ (wg W. Brytanii – 2009 r.) – obejmuje wszystkie formy cyfrowych sieciowych aktywności, które prowadzone są w cyfrowych sieciach lub osiągane są z wykorzystaniem cyfrowych sieci.

³⁷ *National Military Strategy for Cyberspace Operations – NMS-CO*, Joint Chiefs of Staff, Waszyngton 2006, s. 3.

³⁸ *National Military Strategy for Cyberspace Operations – NMS-CO*, Joint Chiefs of Staff, Waszyngton 2006, s. 3.

³⁹ *AC/322(SC/2-NC3TS)L(2007)0002*, Definicje Związane z Cyberwojną, 11.04.2007 r.; *MC 571 – Koncepcja NATO w zakresie Cyberobronności*, 21.02.2008 r. [w: *NATO Bi-SC Informator Operacji Informacyjnych v.1*, Allied Command Transformation, Norfolk 2010, s. 84].

⁴⁰ Oryginalna wersja językowa: Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks. *Cyber Security Strategy of the United Kingdom – safety, security and resilience In cyber space*, The Parliamentary Bookshop, Londyn 2009, s. 7.

Cyberprzestrzeń⁴¹ (wg USA – 2010 r.) – jest globalną domeną zawartą w środowisku informacyjnym, składającą się z niezależnej sieci informacyjnej opartej na infrastrukturze technologicznej, zawierającej Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery.

Integracja operacji cybernetycznych z innymi domenami⁴² (wg USA – 2010 r.) – istotą tego procesu jest pozyskanie możliwości poszerzania zdolności pochodzących z pozostałych, poszczególnych domen w celu uzyskania unikalnych efektów, tzw. „efektów decyzyjnych”. Wykorzystanie cyberprzestrzeni ewaluowało, obecny stan jego rozwoju stanowi potencjał, który umożliwia rozwiązywanie problemów nowymi metodami, co pozwala realizować zakładane narodowe cele. Obecnie wszystkie domeny działań militarnych są silnie powiązane poprzez cyberprzestrzeń (rysunek 2 przedstawia relacje pomiędzy domenami w ramach procesu integracji operacji cybernetycznych z innymi domenami)⁴³, co należy uwzględnić w rozważaniach prowadzonych nt. współczesnych działań militarnych⁴⁴.

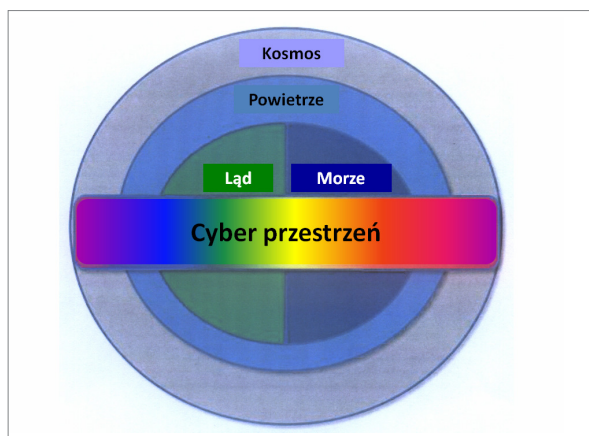
Najnowsze polskie poglądy definiujące pojęcie cyberprzestrzeni pokrywają się zasadniczo z poglądami amerykańskimi i brytyjskimi, a sformułowane są następująco:

⁴¹ Oryginalna wersja językowa: Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 51 [definicja zaczerpnięta z: *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, USA*].

⁴² *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 19.

⁴³ *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 20.

⁴⁴ Oryginalna wersja językowa: As the use of cyberspace continues to evolve, Airmen will determine new ways to solve problems to meet national objectives. The core of cross-domain integration is the ability to leverage capabilities from different domains to create unique – and often „decisive” – effects. The figure portrays the relationship among the operational domains, all domains are interconnected via cyberspace operations. *Cyberspace Operations (DD 3-12)*, Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010, s. 19 (wskazano, że taki sposób pojmowania zaczerpnięto z: Convertino Sebastian, *Flying and Fighting in Cyberspace*, lipiec 2007, Air University, s. 11).



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

Rys. 2. Zależności pomiędzy domenami operacyjnymi w trakcie działań wojennych wg teoretyków SP USA

Cyberprzestrzeń⁴⁵ (JW 3984 – 2013 rok) – miejsce składające się z komputerów, urządzeń teleinformatycznych, współzależnych sieci telekomunikacyjnych i wszelkich mediów cyfrowych, w którym realizowane są procesy informacyjne.

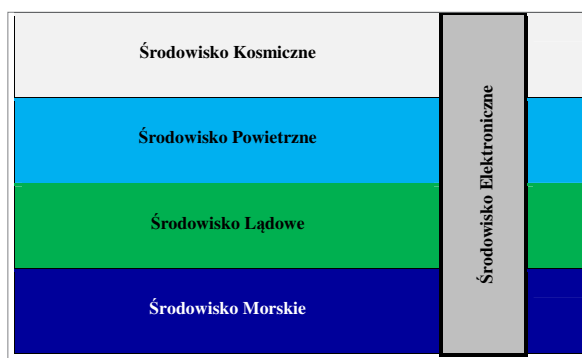
Po zapoznaniu się ze stosunkowo obszernym materiałem pojęciowym dotyczącym cyberprzestrzeni nasuwa się nadal zasadnicze pytanie: Czy cyberprzestrzeń jest tym właściwym terminem zasługującym na miano „czwartego wymiaru wojny”? Otóż nie. Ponieważ pomimo wyraźnie zauważalnej ewolucji i poszerzania obszaru oddziaływania cyberprzestrzeni, nadal we wszystkich dokumentach doktrynalnych amerykańskich i sojuszniczych występuje niezależne pojęcie walki elektronicznej (i wszystko co się z tym wiąże), funkcjonujące obok pojęcia cyberprzestrzeni. Świadczy to o tym, że nie wszystkie urządzenia i systemy elektroniczne zostały podporządkowane funkcjonowaniu w cyberprzestrzeni.

Polskie poglądy na wymiary wojny

W rozważania teoretyczne na ten temat włączyli się w ostatnim czasie również polscy oficerowie. Według najnowszych poglądów oficera Sił Powietrznych podpułkownika Stanisława Czeszejko, przedstawionych w artykule w „Przeglądzie

⁴⁵ R. Janczewski, *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym*, [w: materiały po XX Konferencji Naukowej Automatyzacji Dowodzenia 2013], AON, Gdynia–Warszawa, 2013, s. 101.

dzie Sił Powietrznych” z czerwca 2011 roku, cyberprzestrzeń⁴⁶ jest jedynie elementem działań militarnych, który poszerza i współtworzy istniejący już „czwarty wymiar wojny” Howarda (oparty głównie o walkę elektroniczną), któremu nadał nową nazwę: „środowisko elektroniczne”. Przedstawił on również własny, chronologiczny podział wymiarów wojny, nazywając je środowiskami, których kolejność przedstawił następująco: środowisko lądowe; środowisko morskie; środowisko powietrzne; środowisko elektroniczne; środowisko kosmiczne (rysunek 3)⁴⁷. Również w swojej pracy końcowej z czerwca 2011, opracowanej w trakcie Podyplomowych Studiów Operacyjno-Strategicznych w AON, S. Czeszejko kwalifikuje do działań w środowisku elektronicznym działania z wykorzystaniem energii elektromagnetycznej, działania w cyberprzestrzeni (sieciach komputerowych) oraz inne działania z wykorzystaniem urządzeń i systemów elektronicznych. Do działań w środowisku elektronicznym kwalifikuje on również różne interakcje pomiędzy środowiskiem elektronicznym a pozostałymi środowiskami (np. wykrywanie radarem obiektów powietrznych)⁴⁸.



Źródło: S. Czeszejko, *Działania elektroniczne, a świadomość sytuacyjna pola walki*, [w: materiały po XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa 2011, s. 18).

Rys. 3. Umiejscowienie Środowiska Elektronicznego

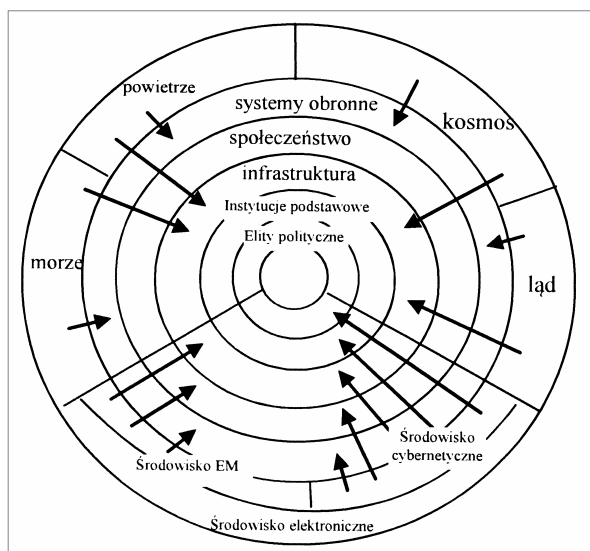
⁴⁶ S. Czeszejko, *Konflikty ery informacyjnej*, Przegląd Sił Powietrznych nr 6, Warszawa, 2011, s. 9.

⁴⁷ S. Czeszejko, *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa, 2011, s. 123.

⁴⁸ S. Czeszejko, *Działania elektroniczne, a świadomość sytuacyjna pola walki*, [w: materiały po XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, s. 11.

Ocenia też, że taki podział wpłynie pozytywnie na podniesienie efektywności wykorzystania urządzeń i systemów elektronicznych (ich synergii) na współczesnym polu walki, w tym na podniesienie świadomości sytuacyjnej pola walki. Ponadto wskazuje on, że urządzenia i systemy elektroniczne są wyróżnikiem oraz wspólnym mianownikiem dla działań militarnych prowadzonych w środowisku elektronicznym.

Oficer Akademii Obrony Narodowej pułkownik Waldemar Scheffs w swoim wystąpieniu w trakcie Konferencji Naukowej Automatyzacji Dowodzenia w październiku 2011 roku proponuje unowocześnienie „Modelu Wardena” poprzez zastąpienie pojęcia przestrzeni cybernetycznej określeniem „środowisko elektroniczne” (zmiana nazwy). Dodatkowo proponuje on podział piątego kręgu tego modelu na dwie części (rysunek 4): obszar środowiska elektromagnetycznego i obszar środowiska cybernetycznego⁴⁹, co jest w gruncie rzeczy potwierdzeniem poglądów jego polskiego kolegi.



Źródło: W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [w: materiały po XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011], Journal of KONBiN, No 3 (19), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, s. 127).

Rys. 4. Zmodernizowany model oddziaływania w J. Wardena

⁴⁹ W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [w: materiały po XIX Konferencji Naukowej Automatyzacji Dowodzenia 2011], Journal of KONBiN, No 3 (19), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, s. 127.

Sieciocentryczność

Kolejnym pojęciem, które w pewnym zakresie ma związek z wykorzystywaniem urządzeń i systemów elektronicznych, jest pojęcie sieciocentryczności. Autorami pierwszej definicji sieciocentryczności byli J. Garstka, D. Alberts i F. Stein, których uważa się za jednych z prekursorów tej koncepcji. W największym skrócie opiera się ona na skupianiu siły, która może być wygenerowana poprzez efektywne połączenia (sieciowanie) elementów ugrupowania bojowego⁵⁰ (w tym z wykorzystaniem urządzeń i systemów elektronicznych, głównie łączności i teleinformatyki). Autorzy uważają również, że zaistniała konieczność odejścia od używania pojęcia „pole walki” na rzecz określenia „środowisko walki sieciocentrycznej” jako „przestrzeni realizacji zadań”. W przestrzeni tego rodzaju nie będzie występować wyraźna granica pomiędzy walczącymi żołnierzami a ludnością cywilną. W związku z powyższym walkę sieciocentryczną należy traktować jako element szerszej definiowanej walki informacyjnej⁵¹.

Należy mieć na uwadze, że dość swobodnie używa się obecnie nazwy „środowisko”, nie podając jego definicji. Ogólny sens używanego w określonym kontekście pojęcia jest zrozumiały. Niemniej jednak, by nazewnictwo precyzyjnie oddawało istotę danego pojęcia, potrzebny jest jednoznaczny system zdefiniowanych pojęć.

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

Sieciocentryczność⁵² (wg AON – 2007 r.) – w ujęciu informatycznym (systemowym) – to integracja z innymi systemami (fuzja informacji), prowadząca do utworzenia jednego wspólnego systemu (nadsystemu).

⁵⁰ J.J. Garstka, D.S. Alberts, F.P. Stein, Network Centric Warfare, DoD C4ISR Cooperative Research Program, Washington D.C., 2000, s. 88 [w: S. Zajas (red. nauk.), *Studium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa, 2009, s. 21].

⁵¹ S. Zajas (red. nauk.), *Studium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa, 2009, s. 21.

⁵² M. Żukowski, *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007, s. 70.

Środowisko sieciocentryczne⁵³ (wg AON – 2008 r.) – zespół czynników wynikających z głębokich przemian w wyposażeniu wojsk oraz połączeniu sieciowym wszystkich uczestniczących w działaniach sił, od żołnierza, pojazdu do najwyższych szczebli włącznie. Stwarzając określone warunki, które wpływają na zachodzące w działaniach wojsk (innych uczestników) zjawiska, sprzężenia i interakcje, determinują charakter dowodzenia i sposób prowadzenia działań, nadając im nowe specyficzne cechy.

Środowisko sieciocentryczne⁵⁴ (wg AON – 2013 r.) – środowisko zaawansowanych systemów wspomagania procesów informacyjno-decyzyjnych wykorzystywane na potrzeby sił zbrojnych. Powstanie i rozwój koncepcji prowadzenia działań w środowisku sieciocentrycznym wymuszone zostały przemianami zachodzącymi w świecie technologii informatycznych oraz wzrostem znaczenia informacji jako czynnika odgrywającego niezwykle rolę we współczesnych konfliktach zbrojnych.

Sieciocentryczność jako nowa idea prowadzenia działań bojowych, jak można zaobserwować w ostatnich latach, znajduje się jeszcze na etapie koncepcyjnym⁵⁵. Oceniając sieciocentryczność, mając na uwadze interesujące nas wykorzystanie urządzeń i systemów elektronicznych, można ocenić, że działania sieciocentryczne swoim znaczeniem najbardziej zbliżone są do walki informacyjnej. Należy zauważyć, że zasadnicza różnica polega na tym, iż sieciocentryczność opiera się w głównej mierze na wykorzystaniu urządzeń i systemów elektronicznych z obszaru łączności i teleinformatyki.

Umiejscowienie „środka ciężkości” na najważniejszych aspektach walki informacyjnej polega na tym, że urządzenia i systemy elektroniczne są głównie źródłami informacji, natomiast w działaniach sieciocentrycznych ich głównym zadaniem jest elektroniczne „spinięcie” wszystkich ele-

mentów ugrupowania bojowego w całość, z czego „wojsko czerpie dodatkową siłę”. Niemniej jednak w obu wypadkach zasadniczym przedmiotem działania jest informacja, a nie urządzenia i systemy elektroniczne.

Wszystko wskazuje na to, że w pierwszym etapie swego (jeszcze nie nazwanego) istnienia (rozwoju) sieciocentryczność była: walką informacyjną opartą o wykorzystanie środków łączności i wspierania procesów związanych ze zdobywaniem informacji; oraz jej przetwarzaniem i dystrybucją (w obu przypadkach niejednokrotnie poprzez niezależne od siebie wykorzystanie komputerów). Dopiero połączenie tych dwóch nurtów rozwojowych w jedno rozwiązanie systemowe stworzyło warunki do utworzenia koncepcji sieciocentryczności.

Sieciocentryczność w żaden sposób nie pretenduje do „czwartego wymiaru wojny”, ponieważ jej głównym celem jest umożliwienie osiągnięcia większej synergii działań militarnych całości wojsk, prowadzonych we wszystkich wymiarach jednocześnie, a nie prowadzenie działań w nowym, „czwartym wymiarze wojny”.

Przeźren czy środowisko?

Wykorzystywanie pojęcia przestrzeni w naukach wojskowych wzięło swój początek w okresie, w którym szeroko posługiwano się analizą i modelowaniem matematycznym. Typowym przedstawicielem „szkoły”, dla której aparat matematyczny był podstawą wszelkich rozważań naukowych, a z którym można zetknąć się jeszcze w militarnym piśmiennictwie polskim, jest Leopold Ciborowski. W swoich pracach szeroko stosuje pojęcia i aparat matematyczny do uzasadnienia swych poglądów, wskazuje, że większą precyzję interpretacji zapewnia słownictwo cybernetyczne i matematyczne⁵⁶. Również większość swoich hipotez zweryfikował z wykorzystaniem metod matematycznych, w których „przeźren” funkcjonuje jako typowe pojęcie „aparatu matematycznego”. Wyróżnia również pojęcie „środowiska”, ale jego znaczenie nie jest powiązane z matematyką. Oto definicje interesujących nas pojęć, sformułowane przez profesora Ciborowskiego:

⁵³ J. Posobiec, *Dowodzenie w środowisku sieciocentrycznym*, Rozprawa habilitacyjna, Zeszyty Naukowe, AON, Warszawa, 2008, s. 52.

⁵⁴ K. Frącik, *Proces dowodzenia jako zasadniczy komponent systemu dowodzenia w uwarunkowaniach środowiska zaawansowanych systemów wspomagania procesów informacyjno-decyzyjnych*, [w: materiały po XX Konferencji Naukowej Automatyzacji Dowodzenia 2013], AON, Gdynia–Warszawa, 2013, s. 24.

⁵⁵ S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, s. 69.

⁵⁶ L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999, s. 95.

Przestrzeń⁵⁷ – zbiór dowolnych przedmiotów (liczb, stanów układu, wektorów itp.), między którymi zostały ustalone pewne relacje natury geometrycznej bądź abstrakcyjnej.

Środowisko walki (sfera walki)⁵⁸ – jest otoczeniem przedmiotu walki, gdzie jest on zlokalizowany. Stosownie do warunków panujących w otoczeniu należy wyodrębnić tylko takie narzędzia walki, które nadawać się będą do wykorzystania w tym środowisku (w tej sferze).

Jak widać na przykładzie definicji sformułowanych przez L. Ciborowskiego, „przestrzeń” jest typowym pojęciem matematycznym, wykorzystywanym do weryfikacji hipotez z wykorzystaniem metod matematycznych, jego wykorzystanie na potrzeby militarne nie do końca jest uzasadnione.

Natomiast definicja „środowiska” walki jest bardziej uniwersalna i pozostaje na użytek prowadzonych tu rozważań jak najbardziej użyteczna. Ale należy zapoznać się i ocenić ogólne definicje środowiska, podawane przez różne źródła, gdzie środowisko to:

- ogół elementów otoczenia⁵⁹;
- ogół wszystkich czynników otoczenia (ożywionych i nieożywionych), mniej więcej jednolitych na danym terenie, oddziałujących na organizmy żywe, ulegającym zmianom pod wpływem tych organizmów⁶⁰;
- 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 zaliczone⁶¹.

Analizując powyższe definicje przestrzeni oraz środowiska, autorzy doszli do wniosku, że właściwszym pojęciem definiującym otoczenie prowadzenia działań militarnych będzie określenie „środowisko” (lądowe, morskie, powietrzne, elektroniczne oraz kosmiczne).

Definicja środowiska elektronicznego

W tłumaczeniu książki Alfreda Price pt. *Narzędzia mroku. Historia walki radioelektronicznej 1939–1945*, wydanej w 1967 roku, w tłumaczeniu „Słowa wstępnego” autorstwa Roberta Cockburna można odnaleźć określenie „środowisko elektroniczne”⁶², które autor utożsamia z funkcjonowaniem systemów radiolokacyjnych oraz radiowych. Takie pojęcie spotyka się w angielskojęzycznych opracowaniach, również współcześnie.

Przykładem współczesnego zastosowania na użytek militarny takiego sformułowania jest „Program rozwoju Marynarki Wojennej USA” z 2003 roku⁶³, gdzie w podrozdziale pt. „Pocisk AGM-88E AARGM”, na stronie 123 użyto sformułowania „electronic environment”⁶⁴, które w tłumaczeniu oznacza ni mniej, ni więcej „środowisko elektroniczne”.

W związku z faktem, że pojęcie „środowisko” jest obecnie dość powszechnie stosowane i jest bardziej pasującym określeniem dla otoczenia prowadzonych działań militarnych, autorzy niniejszego opracowania proponują następujące definicje:

Środowisko elektroniczne⁶⁵ (środowisko prowadzenia działań elektronicznych) – jest otoczeniem sygnałów elektrycznych oraz pochodzącego od nich promieniowania elektromagnetycznego (przedmiotów walki lub przedmiotów działań w środowisku elektronicznym), w którym można je wykorzystywać oraz na nie oddziaływać. Narzędziami oddziaływania (walki) w tym środowisku będą urządzenia i systemy elektroniczne (głównie militarne), które nadawać się będą do wykorzystania w tym środowisku.

⁶² A. Price, *Narzędzia mroku. Historia walki radioelektronicznej 1939–1945*, Wydawnictwo Dolnośląskie, Wrocław, 2006, s. 9.

⁶³ *Roczny raport w zakresie kierowania, testów operacyjnych oraz rozwoju pt. FY 2003*, Ministerstwo Obrony Narodowej USA, 2003, s. 123.

⁶⁴ “The target sets must emulate the threat system in physical appearance as well as in the **electronic environment**”.

⁶⁵ Tłumaczenie: Electronic environment (environment of the electronic activity) – a surrounding of electric signals and electromagnetic radiation produced by them (all of them are the warfare objects). In this environment the signals can be used and affected. In the electronic environment the warfare tools (combat tools) mean the electronic devices and systems (mainly of military character), which are able to operate in this particular environment.

⁵⁷ Ibidem, s. 8.

⁵⁸ Ibidem, s. 99, 100.

⁵⁹ J. Bralczyk, *Słownik 100 tysięcy słów*, PWN, Warszawa, 2005, s. 829.

⁶⁰ S. Dubisz, *Uniwersalny słownik języka polskiego*, PWN, Warszawa, 2003, s. 731.

⁶¹ B. Kaczorowski, *Wielka encyklopedia PWN – T. 27*, PWN, Warszawa, 2005, s. 47.

Urządzenia i systemy elektroniczne⁶⁶ – to zasadnicze elementy środowiska elektronicznego, które należy rozumieć jako zbiór elementów nieożywionych powstałych w wyniku działalności człowieka, występujących w określonym umiejscowieniu, pomiędzy którymi mogą istnieć wzajemne powiązania oraz mogą występować wzajemne oddziaływania, mogą one również pozostawać we wzajemnej zależności – stosownie do panujących warunków.

Specyfiką środowiska elektronicznego jest fakt, że prowadzone w nim działania mogą wchodzić w interakcję z innymi środowiskami walki, np. narzędzia walki lub szerzej: narzędzia działań w środowisku elektronicznym (urządzenia i systemy elektroniczne) mogą być niszczone z wykorzystaniem narzędzi walki przynależnymi naturalnie do innych środowisk (np. niszczenie ogniem dział czołgowych). Innym przykładem jest wykrywanie obiektów powietrznych z wykorzystywaniem promieniowania elektromagnetycznego odbitego od ich powierzchni pokrycia zewnętrznego, gdzie zachodzi interakcja pomiędzy przedmiotem walki środowiska elektronicznego (wypromieniowanego sygnału elektromagnetycznego, a następnie odbiór jego odbitej formy, tzw. „echa”) a środowiskiem powietrznym (obiekt powietrzny unoszący się w powietrzu).

W aspekcie powyższego autorzy proponują, z uwagi na potrzebę ujednoczenia specjalistycznej terminologii w obszarze wykorzystania urządzeń i systemów elektronicznych, podział działań militarnych według nowego wzorca, jako prowadzonych w poszczególnych środowiskach oraz proponują szerokie praktyczne zastosowanie tego podziału. Wskazują również na możliwość powszechnego wykorzystania przedstawionych definicji „środowiska elektronicznego” oraz definicji „urządzeń i systemów elektronicznych”. Analiza istniejącego aparatu pojęciowego, głęboko zakorzenionego w świadomości specjalistów, oraz jego weryfikacja nie była zadaniem łatwym. Wymagała długotrwałej obserwacji, konfrontacji zebranych spostrzeżeń z innymi specjalistami, budowy własnego podejścia do badań i autorskiego opracowania uzyskanych wyników. „Narzędzia” pojęciowe,

⁶⁶ Tłumaczenie: Electronic devices and systems – key elements of the electronic environment, which should be understood as a set of unanimated elements emerging as a result of human activity and which exist in a concrete place. They can be interrelated and influence each other. Also, a mutual dependence among them is possible – in accordance with the existing conditions.

których dostarczają autorzy, mogą pełnić funkcję systematyzowania podejścia do tematyki oraz mogą ułatwić dalsze tworzenie rozwiązań systemowych w rozważanej tematyce.

Podsumowanie

Jak wskazują niektórzy specjaliści na przykładzie działań sieciocentrycznych⁶⁷, rozbieżność terminologiczna jest cechą charakterystyczną dla polskojęzycznej literatury przedmiotu. Zdaniem autorów jest to cecha charakteryzująca również literaturę innych państw. Ale jest to cecha charakterystyczna dla wysoce dynamicznie zmieniającej się dziedziny, jaką jest rozwój urządzeń i systemów elektronicznych oraz ich zastosowania do prowadzenia działań militarnych. Przekłada się to pośrednio na zmiany sposobów walki z ich użyciem, które mają bezpośredni wpływ na zasady walki (np. walki elektronicznej), te natomiast są częścią składową zasad sztuki wojennej. Nie pozostaje to niezauważone, również dla polskich specjalistów, S. Markiewicz opisuje to w swojej pracy⁶⁸, zaznacza również przy tym wyraźnie, że Z. Galewski wskazuje na fakt weryfikacji reguł prowadzenia tego rodzaju walki w trakcie prowadzonych konfliktów zbrojnych⁶⁹. Ale należy pamiętać, że nie same zasady sztuki wojennej, nawet najnowocześniejsze, a umiejętne ich zastosowanie w walce może doprowadzić do pokonania przeciwnika.

W interdyscyplinarny charakter działań w środowisku elektronicznym wpisuje się szereg dziedzin, dyscyplin i specjalności naukowych, a ich systemowe i kompleksowe postrzeganie pozwala na ich pełne zrozumienie. Uwzględnianie w rozważaniach aspektów techniki oraz technologii dotyczących urządzeń i systemów elektronicznych, pozwala na dogłębne zbadanie następstw przyczynowo-skutko-

⁶⁷ J. Janczak, *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007, s. 23.

⁶⁸ S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, s. 64.

⁶⁹ Z. Galewski, *Czynniki powodzenia we współczesnej walce*, Warszawa, 1986, s. 152 [za:] Szymon Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, s. 64.

wych w tej dziedzinie, które determinują również stosowaną na jej użytek terminologię.

Pomimo rozwijania różnych teorii i będących ich konsekwencją rozwiązań systemowych w zakresie wykorzystania urządzeń i systemów elektronicznych oraz ich wpływu na działania militarne, należy pamiętać, że istota zadań poszczególnych rodzajów wojsk w przyszłych operacjach pozostanie taka sama, może zostać ona jedynie nieznacznie zmodyfikowana w zależności od warunków, jakie będą towarzyszyć realizacji stojących przed nimi zadań. Na pewno zmieniać się będzie sposób realizacji zadań, co wynikać będzie ze zmian dotyczących ogólnych założeń prowadzenia walki.

Bibliografia

Pozycje/Wydawnictwa zwarte:

- Blach M., *Bazy danych elementem skuteczności rozpoznania elektronicznego*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, ISBN 978-83-7523-055-0.
- Błażejczyk W., Nowacki G., Scheffs W., *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa 2002.
- Bralczyk J., *Słownik 100 tysięcy słów*, PWN, Warszawa 2005, ISBN 83-01-14509-9.
- Ciborowski L., *Nowe systemy i środki walki oraz kierunki ich rozwoju w SZ państw obcych*, AON, Warszawa 1993.
- Ciborowski L., *Rozpoznanie i Walka Elektroniczna*, AON, Warszawa 1993.
- Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999, ISBN 83-88089-00-5.
- Czeszejko S., *Działania elektroniczne, a świadomość sytuacyjna pola walki*, [w: materiały po XIX Konferencji Naukowej Automatykacji Dowodzenia 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa 2011, ISSN 1895-8281.
- Czeszejko S., *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa 2011.
- Czeszejko S., *Konflikty ery informacyjnej*, Przegląd Sił Powietrznych nr 6, Warszawa 2011, ISSN 1897-8444.
- Dubisz S., *Uniwersalny słownik języka polskiego*, PWN, Warszawa 2003, ISBN 83-01-13868-8.
- Dubrawski Z., *Walka radioelektroniczna prowadzona przez SP. Studium operacyjne*, AON, Warszawa 2000.
- Dymanowski K., Groszek Z., *Walka radioelektroniczna w działaniach SP we współczesnych konfliktach zbrojnych*, AON, Warszawa 2008.
- Grabau R., *Sechs Dimisionen des Kriges. Versuch einer analytischen Betrachtung*, miesięcznik Soldat und Technik nr 5, nr 6, nr 7, 1985.
- Howard M., *Wojna w dziejach Europy*, Ossolineum, Wrocław 2007, ISBN 978-83-0404-865-2.
- Janczak J., *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, AON, Warszawa 2001.
- Janczak J., *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007, ISBN 978-83-7523-002-4.
- Janczewski R., *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym*, [w: materiały po XX Konferencji Naukowej Automatykacji Dowodzenia 2013 pt. *Automatykacja Dowodzenia SZ RP w środowisku sieciocentrycznym*], AON, Gdynia–Warszawa 2013, ISBN 978-83-930150-3-0.
- Kaczorowski B., *Wielka encyklopedia PWN – T. 27*, PWN, Warszawa 2005, ISBN 83-01143-62-2.
- Lokociejewski M., Scheffs W., *Walka elektroniczna w operacji i walce*, AON, Warszawa 2005.
- Magnucki Z. [red.], *Walka radioelektroniczna w SZ RP*, AON, Warszawa 1994.
- Malasiewicz K., *Czynniki domeny kognitywnej w planowaniu działań*, [w: materiały po XX Konferencji Naukowej Automatykacji Dowodzenia 2013 pt. *Automatykacja Dowodzenia SZ RP w środowisku sieciocentrycznym*], AON, Gdynia–Warszawa 2013, ISBN 978-83-930150-3-0.
- Markiewicz S., *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, ISBN 978-83-7523-055-0.
- Nowak A., *Założenia dla perspektywicznego systemu rozpoznania*, AON, Warszawa 2004.
- Piekarski H., *Walka radioelektroniczna*, Wydawnictwo MON, Warszawa 1980, ISBN 83-11-06520-9.
- Posobiec J., *Dowodzenie w środowisku sieciocentrycznym*, Rozprawa habilitacyjna, Zeszyty Naukowe, AON, Warszawa 2008.
- Price A., *Narzędzia mroku. Historia walki radioelektronicznej 1939–1945*, Wydawnictwo Dolnośląskie, Wrocław 2006, ISBN 978-83-7384-473-5.
- Scheffs W., *Automatykacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [w: materiały po XIX Konferencji Naukowej Automatykacji Dowodzenia 2011], Journal of KONBiN, No 3 (19), Instytut Techniczny Wojsk Lotniczych, Warszawa 2011, ISSN 1895-8281.
- Scheffs W., *Proces oceny przeciwnika w aspekcie elektronicznym*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007.
- Scheffs W., *Założenia walki elektronicznej w środowisku sieciocentrycznym*, [w: materiały po międzynarodowej konferencji naukowej nt. „Walka elektroniczna w działaniach sieciocentrycznych” – 2008], AON, 2008, ISBN 978-83-7523-055-0.

- Sienkiewicz P., *Wizje i modele wojny informacyjnej. w: Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Tom 1, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2004, ISBN 83-89388-32-4.
- Szpyra R., *Militarne operacje informacyjne*, AON, Warszawa 2003, ISBN 83-89423-40-5.
- Vego M., *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona nr 2, Warszawa 2009, ISSN 1897-7065.
- Zajas S. (red. nauk.), *Studium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa 2009, ISBN 978-83-7523-063-5.
- Żukowski M., *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych*, [w: materiały po międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych” – 2006], AON, 2007, ISBN 978-83-7523-002-4.
- Czasopisma i mat. konferencyjne/Artykuły:**
- Materiały z kursu „*Special Operations Forces Integration Course*” przeprowadzonego w AON w dn. 21–25.03.2011 r. przez przedstawicieli m.in. *Joint Special Operations University*.
- Dokumenty normatywne i operacyjne, raporty:**
- Cyber Security Strategy of the United Kingdom – safety, security and resilience In cyber space, The Parliamentary Bookshop, Londyn, 2009.
- Cyberspace Operations (DD 3-12), Centrum Rozwoju Doktryn i Edukacji Sił Powietrznych USA, 2010.
- National Military Strategy for Cyberspace Operations – NMS-CO, Joint Chiefs of Staff, Waszyngton, 2006.
- NATO Bi-SC Informator Operacji Informacyjnych v.1, Allied Command Transformation, Norfolk, 2010.
- Połączona sojusznicza doktryna operacji informacyjnych (AJP-3.10), Agencja Standaryzacji NATO (NSA), 2009.
- Roczny raport w zakresie kierowania, testów operacyjnych oraz rozwoju pt. FY 2003, Ministerstwo Obrony Narodowej USA, 2003.
- Walka elektroniczna, Sztab Generalny WP, Warszawa, 2003 (Szt. Gen. 1549/2003).
- Strony internetowe/Publikacje i adresy internetowe:**
- <http://pl.wikipedia.org>
- Rybak T., Raport o stanie środowiska w 2010 r. 6. Promieniowanie elektromagnetyczne (Źródło – dostęp w 24.02.2014 r.: http://www.wios.rzeszow.pl/cms/upload/edit/file/stan_srodowiska_2010/r6.pdf).

MILITARY ASPECTS OF ELECTRONIC ENVIRONMENT - AN ATTEMPT TO REVISE THE EXISTING TERMINOLOGY

Abstract

The increasingly widespread presence of electronic equipment and systems in human life has led representatives of several human generations to attempt to describe this phenomena. These efforts, undertaken in order to systematise the perception of the new - in relation to the existence of the human species - 'world' of devices and electronic systems on a background of other human activities, are greatly complicated by dynamic developments. The authors, based on extensive experience gained in the context of many years of work involving the use of electronic equipment and systems, believe that it is necessary to develop a new theoretical basis (including conceptual apparatus), more versatile than currently existing ones. In this article, they propose to introduce the term 'electronic environment', which is synonymous with the place for conducting part of military action, which uses electronic devices and systems. They also justify the adopted point of view in a comprehensive manner and demonstrate the merits of the proposed changes.

Key words: network-centric operations, situational awareness, information operations.

Introduction

Physical phenomena existing in nature associated with strong lightning in the atmosphere, occurring naturally and usually associated with storms, were closely watched by people for millennia. A number of phenomena, accompanied by far less electricity, for example electrostatic charging - so-called 'static electricity' were also

discovered. Ancient Greeks were the first to give us descriptions of electrostatic interactions. They discovered that amber (*elektron* in Greek) attracted small items when rubbed. It was the development of science over the last few centuries that enabled us to get to know these phenomena arising in nature so well that it led to their use for human needs. The construction of increasingly complicated electrical and electronic equipment began. At

a certain stage of development, it became possible to combine them in different types of systems. Electricity, electromagnetic radiation and other physical effects were produced in an unnatural, artificial way, which were described in the section *Electricity and magnetism* in physics¹. Of course the militant side of human nature has been using new inventions on the classic field of battle and the 'silent' one, sometimes hundreds of kilometres away from the front lines.

With the development of military electronic equipment and systems, the theory of using them was created, including its naming, as well as existing doctrines taking their presence into account. Of course, there had to be some legislation to be able to conduct military operations with them. Many terms were created and various concepts raised to regulate the issues, but the differences in their perception still give rise to many doubts. Therefore, the following questions arise: Can the current regulations remain valid? Should the perception of this subject be revised? In the conviction of the authors it should.

The fourth dimension of war

During World War II, the use of electronic equipment and systems became quite important and widely recognised by commanders as an element of securing conducted combat operations. In the end, they were given their own name. They were called 'radioelectronic war' which, from the point of view of commanders leading the battle, had its rational justification - essentially they have been directly using radio waves (electromagnetic radiation) coming from radio electronic devices.

The British historian, Michael Howard, presented his own views on this subject in his book *The war in the history of Europe* (in Chapter VII: *War of technicians*) published in 1976 in Great Britain. In his opinion, the new 'fourth dimension of war' (after land, sea and air)¹ had been created during World War I and developed intensively during World War II, meaning war related at that time to the development and use of electronic communication devices, cryptography, reconnaissance and radioelectronic warfare as well as radiolocation, mainly using electromagnetic

radiation. It can be seen that Michael Howard, as a historian and theorist, perceived the problems of using electronic equipment and systems for the purpose of military actions wider than military pragmatists from the period of World War II, because he clearly emphasised the presence of cryptography devices that do not emit radio waves. The fact that he did not name this a new 'fourth dimension of war', and only pointed to its existence, is important from our point of view.

The view of M. Howard on these complex issues had a broad impact. In the early 1980s, a reflection of his views can already be found in Polish literature, which uses, among other things, the term 'fourth dimension of armed confrontation with the enemy'². The well-known Polish military theorist, professor Leopold Ciborowski, who deals with the issues of reconnaissance and electronic warfare (REW) as well as information warfare, had already claimed in the late 1990s that even during the first war in the Persian Gulf region the confrontation had entered a 'fourth dimension' which is electromagnetic space³.

The natural effect in a response to an indication of another dimension of warfare is an attempt to name it. One such attempt was made in the mid-1980s by Bundeswehr officer (German Armed Forces), Colonel Rudolf Grabau. He did not confine himself only to indicating the name of the 'fourth dimension of war' ('electromagnetic spectrum') but presented his own division of the war in six dimensions: distance - equating distance in a straight line; surface area (width and depth) - identifying the area; height - equating space through the completion of the surface; time; information; the electromagnetic spectrum. He then pointed out that the last three factors would have a decisive influence on the character of future armed conflicts.

It cannot be ruled out that the terminology adopted by Colonel Grabau (the electromagnetic spectrum) for M. Howard's 'fourth dimension war' is a kind of aftermath of usage in military circles of different countries of the name 'radioelectronic war' unequivocally equated with the use of radio waves. Some explanation for the correctness of the division adopted by him may be that, as mentioned

² H. Piekarski, *Walka radioelektroniczna*, Wydawnictwo MON, Warszawa, 1980, p. 5.

³ L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, p. 35.

¹ M. Howard, *Wojna w dziejach Europy*, Ossolineum, Wrocław, 1990, p. 167.

earlier by M. Howard, electronic devices in cryptography can be placed in a division of Grabau's in the 'information' area.

Electromagnetic environment

In specialist Polish literature, the term 'electromagnetic environment' is defined as an environment in which electromagnetic energy is spreading⁴. One can also find works in which our experts say that *the electromagnetic spectrum (next to cyberspace) is another dimension of the modern battlefield*⁵.

Some sources indicate that within the general division of information warfare the following can be distinguished within the general division of information warfare⁷: personal space combat and technical space of information warfare. A similar division was adopted for reconnaissance, which is divided into: personal and technical reconnaissance. This second type of reconnaissance (technical) is carried out with the aid of specialised equipment that can detect and record the effects and phenomena in the following environments: electromagnetic, elastic, electric, magnetic, and chemical. These environments are pointed out in both studies, the one on information warfare and the one on reconnaissance. In both studies, of course, 'electromagnetic environment' is also mentioned.

Can the term 'electromagnetic environment' be considered as the correct name for the 'fourth dimension of war'? Many facts indicate that it is not. But why?

While considering this issue, the source of electromagnetic radiation should be assessed in the first instance. In nature, there are many (e.g. sunlight, lightning, etc.)⁶, but in practice man cannot influence all the natural sources of electromagnetic radiation in such a manner

to generate radiation in a form useful to him (desirable).

The situation changed only after the discovery of electricity and the understanding of physical phenomena accompanying it. Along with gaining more and more knowledge on the subject, it became possible to construct electrical and electronic equipment, including those being artificial sources of electromagnetic radiation. In the circuits of electrical and electronic equipment, first the electric current is produced, which is an ordered (directed) motion of electric charges (positive - e.g. cations, or negative - e.g. electrons, anions). Only a moving electrical charge creates - to simplify - an electromagnetic field, while disturbances in the electromagnetic field emanating in the space surrounding the electrical circuits are the electromagnetic radiation (electromagnetic waves). The device that converts electrical signals into electromagnetic radiation (waves) and vice versa is the antenna.

It should be noted that only electronic equipment is able to produce and process the complex electrical signals useful for humans (including digital ones), which can be converted to the desired form of electromagnetic radiation (and vice versa).

Accordingly, it is clear that useful electromagnetic radiation is only the consequence of the operation of electronic devices and it is not its only 'fruit' for man's use. Therefore - to put it simply - the notion of 'electromagnetic environment' in the past once had its pragmatic justification, but it was not necessarily real. Nowadays we have to take into account all the factors related to the existence of electronics that have an impact on our assessment of the terminology for electronic equipment and systems being used, in such a way that it is objective and must correspond to the prevailing reality. In the age of ubiquitous computer networks, another meaning is assigned to the use of electric current for generation and transmission of electrical signals. Therefore, the concept of 'electromagnetic environment' does not meet the conditions for gaining the title of 'fourth dimension of war'.

Electronic warfare

The term 'electronic warfare' originates in a straight line from the notion of 'radioelectronic

⁴ W. Scheffs, *Proces oceny przeciwnika w aspekcie elektrycznym*, [in: publication after the international scientific conference „Sieci teleinformatyczne w działaniach sieciocentrycznych” - 2006], AON, 2007, p. 121.

⁵ M. Blach, *Bazy danych elementem skuteczności rozpoznania elektronicznego*, [in: publication after the international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych” - 2008], AON, 2008, p. 28.

⁶ T. Rybak, *Raport o stanie środowiska w 2010* chapter 6. *Promieniowanie elektromagnetyczne* (Source: access on 24 February 2014: http://www.wios.rzeszow.pl/cms/upload/edit/file/stan_srodowiska_2010/r6.pdf).

warfare⁷, while the latter directly from the notion of ‘radioelectronic war’, as previously mentioned, formed at the end of World War II.

One of the most important publications in Polish literature in the field of electronic warfare is Leopold Ciborowski’s of 1993, in which the author widely used the analysis and mathematical modelling. L. Ciborowski is a typical representative of the ‘school’ for which the mathematical apparatus was the basis of all scientific considerations; hence, in the indicated publication, the majority of hypotheses have been verified using mathematical methods. In the very first pages of the work he points out that ‘electronic warfare interferes with an opponent’s information process (circulation and content of the information) in the electromagnetic field⁸, which characterises the scope of its activities. It also presents division of general reconnaissance:⁹ personal and electronic reconnaissance (division of general reconnaissance has been transformed in later years and now includes¹⁰: personal and technical reconnaissance).

It is worth becoming familiar with the definitions of various representatives of the Polish Armed Forces, presented chronologically, defining the interesting area of military actions as:

Radioelectronic warfare¹¹ (by National Defence University - 1994) - all projects and activities of the army that aim at using electromagnetic energy to identify and disrupt the enemy’s electronic systems and to ensure stable conditions for one’s own troop operations.

Electronic warfare¹² (by NDU - 2000.) – a set of projects and activities of specialised forces, coupled together organisationally and functionally, whose aim is to identify and disrupt electronic systems (means) of an adversary and ensuring conditions for stable operation of corresponding

systems (measures) of one’s own troops. It includes reconnaissance, overpowering and radioelectronic defence, implemented using electromagnetic energy radiation, including invoking changes in the electromagnetic environment as well as creating strong electromagnetic impulses.

Electronic warfare¹³ (by General Staff of Polish Armed Forces - 2003). - military action involving the identification of sources of electromagnetic emissions and disrupting the enemy’s electronic systems using electromagnetic energy, including energy-beam, while ensuring conditions for their effective use by one’s own army.

It is also worth becoming familiar with the views (definitions) of our allies who play a leading role in the field of electronic warfare, and, therefore, often create concepts in force within the Alliance. Here are some examples, also presented chronologically:

Electronic warfare¹⁴ (according to the USA - 1999) - any military activity involving the use of electromagnetic and directed energy used to control the electromagnetic spectrum or to attack the enemy.

Electronic warfare¹⁵ (according to the USA - 2010) - military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

Despite the unequivocality of the area of action in all these definitions and most theorems concerning ‘electronic warfare’, some authors perceive electronic warfare slightly more broadly.

In his work of 2001, the NDU employee, Col. PhD Eng. Józef Janczak mentions the following elements within the framework of electronic intelligence:¹⁶ radioelectronic reconnaissance; radiolocation reconnaissance; information reconnaissance; optoelectronic reconnaissance; sensor reconnaissance. Similarly, he presented a division of active interference, which, according

⁷ Polish literature used the term ‘radioelectronic warfare’ until 2002 [as stated in: Karol Dymański, Zbigniew Groszek, *Walka radioelektroniczna w działaniach SP we współczesnych konfliktach zbrojnych*, AON, Warszawa, 2008, p. 5].

⁸ L. Ciborowski, *Rozpoznanie i Walka Elektroniczna*, AON, Warszawa, 1993, p. 13.

⁹ Ibidem, p. 58

¹⁰ W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa, 2002, p. 29.

¹¹ Z. Magnucki [edited by], *Walka radioelektroniczna w SZ RP*, AON, Warszawa, 1994, p. 11.

¹² Z. Dubrawski, *Walka radioelektroniczna prowadzona przez SP. Studium operacyjne*, AON, Warszawa, 2000, p. 39, p. 56.

¹³ *Walka elektroniczna*, General Staff of Polish Armed Forces, Warszawa, 2003 (Szt. Gen. 1549/2003), appendix C – Glossary of terms, definitions and abbreviations.

¹⁴ AFDD 2-5.1: *Electronic Warfare*, Washington D.C., 1999.

¹⁵ *Cyberspace Operations (DD 3-12)*, Center for Doctrine Development and Education of the US Air Force, 2010, p. 52 [it should be noted that the definition is quoted from: *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms*, USA].

¹⁶ J. Janczak, *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, AON, Warszawa, 2001, p. 17.

to his views, consists of:¹⁷ radio interference; radiolocation interference; interference of radio navigation; optoelectronic interference; computer science distortion. This author also indicates that military actions in the context of electronic warfare are conducted on a specific 'electronic battlefield' that can be called 'electromagnetic environment' (concerning electronic means of radiating and receiving electromagnetic energy)¹⁸. The views of J. Janczak clearly lead towards a broader perception of the problems of using electronic equipment and systems in military actions, as evidenced even by the inclusion of computer science topics in the area.

Some sources present a separation of technical reconnaissance according to the criterion of distinctiveness¹⁹, which is the 'environment of data carriers', and they are divided into: electromagnetic reconnaissance; sensor reconnaissance (maintained in acoustic, electric, magnetic and chemical environments); information reconnaissance (related to computer technology and its environment, including observing radiation from a monitor or external parts - for example, cable connections).

Two other officers - employees of the National Defence University, Col. PhD Eng. Marian Łokociejewski and Colonel PhD Waldemar Scheffs, in their work of 2005, indicate that the conduct of electronic warfare should not be limited only to the area of electromagnetics, but must extend its influence to other electronic devices (including those not using electromagnetic energy)²⁰. According to the authors, this approach allows the extension of electronic warfare on the kinetic impact (fire) using missiles homing on electronic systems and enables greater insight into electronic defence, including information technology systems. They justify their views with the notion that, if the conduct of military operations is limited to electromagnetic space, the term 'radioelectronic warfare' should remain in use as a more adequate name.

Further considerations in a similar direction were carried out in scientific papers written by

¹⁷ Ibidem, p. 131.

¹⁸ Ibidem, p. 203.

¹⁹ W. Błażejczyk, G. Nowacki, W. Scheffs, *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa, 2002, p. 32, p. 36.

²⁰ M. Łokociejewski, Waldemar Scheffs, *Walka elektroniczna w operacji i walce*, AON, Warszawa, 2005, p. 10.

Col. Waldemar Scheffs, who in his speech at an international scientific conference on electronic warfare in network-centric operations in 2008 said that, in addition to the electromagnetic space, different environments can be pointed out in which fighting is carried out electronically. He then named them: IT systems space, acoustic space, magnetic field²¹.

Summing up such considerations on electronic warfare, it should be noted that, in accordance with the rules of naming, the concept of warfare requires the addition of a complementary term which will be related to the identification of the sphere in which it is, has been or will be conducted. The identification of the subject of battle determines not its nomenclature, but the selection of tools for its conduct and methods of their use in concrete action²². In view of the fact that not all activities associated with the use of electronic equipment and systems are warfare, we cannot simply expand the notion of 'electronic warfare' on the entire area of military operations with the use of electronic equipment and systems. Therefore, the search for a more adequate system of concepts associated with the subject topic should continue.

Information Warfare

Another interesting kind of struggle that was defined for the purpose of conducting military operations (and not only) is information warfare. It should be noted that, although it was not performed under that name before, it has been carried out 'since the dawn of time', confirmation of which can be found, for example, in the outstanding work of the ancient thinker and strategist, Sun Zi. Devices and electronic systems designed by human beings have become a mere tool in conducting this kind of combat, although they play an increasingly leading role.

In his 1990s work on Information warfare, as well as other works, Leopold Ciborowski also widely used terms and mathematical concepts to justify his views. He even indicates that more precise interpretation in this area is provided by

²¹ W. Scheffs, *Założenia walki elektronicznej w środowisku sieciocentrycznym*, [in: publication after the international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych” - 2008], AON, 2008, p. 113.

²² L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, p. 69.

cybernetic and mathematic vocabulary²³. He presents key components of the information warfare, identified in the US in 1994, consisting of²⁴: electronic warfare, psychological measures and IT warfare. Using the example of the views of the former military officer of the American Air Forces, Colonel Res. D. Campten, who extended the scope of information warfare to the non-military sphere²⁵, he also points out that its understanding evolved in a relatively short period of time in the US.

Early American views can be found in the NATO doctrine of 2009²⁶, where the Information Operations (IO) conducted by the Alliance, in addition to other factors, included the two most important types of activities related to the use of electronic devices and systems, namely Electronic Warfare (EW) and Computer Network Operations (CNO).

In 2011, a clear difference of views in the US could be seen, compared to these previously mentioned. Documents concerning national security point out that the Information Operations are carried out in parallel with activities in Computer Network Operations and Electronic Warfare. All of these types of activities, although they are not the only ones conducted in the US, are equivalent to each state's security policy tools in the area of the US national power element called 'Information,' which is one of many elements forming the national power of the United States²⁷.

As shown in the above-mentioned examples, there is no consistency in the location of the two main types of operations with the use of electronic equipment and systems (EW and CNO); this discrepancy proves the absence of uniformed views on this subject matter and the constant search for ideas in this area and the shaping of them. This also shows the complexity of the matter and the search to find their own solutions to these problems (as seen in the US, for example), sometimes divergent in relation to the Alliance.

²³ Ibidem, p. 95.

²⁴ Ibidem, p. 37.

²⁵ Ibidem, p. 39.

²⁶ *Joint Allied Doctrine for Information Operations (AJP-3.10)*, NATO Standardization Agency, 2009, section 0126, section 0129.

²⁷ Handbook from *Special Operations Forces Integration Course* held in NDU Warsaw on 21-25 March 2011 by representatives of Joint Special Operations University from USA, p. 2.

While considering the use of electronic equipment and systems, the subject of information warfare has been raised, even though they are only a tool used for its conduct. Most of the available definitions of information warfare and operations included in the American normative documents of 1995, 1996, 1998, 2009 and NATO documents of 2008 and 2010 did not describe the relationship (dependencies) between information warfare and devices or electronic systems (electronic warfare and cyberspace).

Nevertheless, views can be encountered that try to in some way interpret information warfare as M. Howard's 'fourth dimension of war'. In 1995, Martin Libicki, an employee of the National Defence University in Washington, DC, divided information operations into 7 forms (elements)²⁸: C2W - Command and Control War, Intelligence-Based War, Electronic War, Hacker War, Economic Information War, Cyber or Net War and Psychological Operations. Almost all areas where electronic equipment and systems are used can be found here, but we must be constantly aware that they are not the only elements of these operations.

Thinking about information warfare for a moment, one can have the impression that it aspires to become M. Howard's 'fourth dimension of war'. Areas where electronic equipment and systems are used are not the only components used to conduct information operations, since they are also composed of psychological operations. Therefore, the concept of 'information warfare' is not correct for describing activities with the use of electronic equipment and systems, which means it cannot be called the 'fourth dimension of war'.

Cyberspace

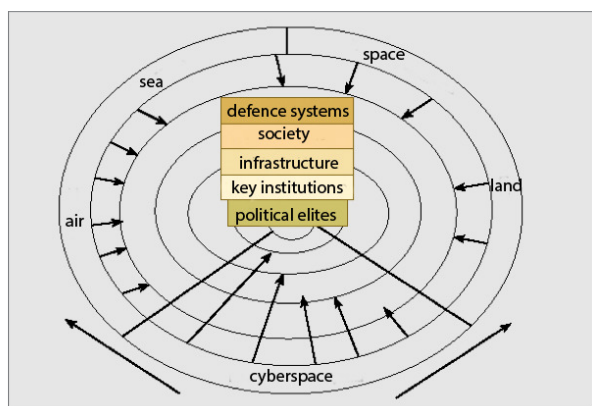
Cyberspace is a concept that, for some time, has been used for the purpose of conducting military operations. Its use in military terminology is closely associated with constructing man-made electronic equipment and systems used for transmission of data and information - computer networks (ICT).

²⁸ M. Libicki, *What is Information Warfare*, Washington, 1995 (quote via Andrzej Nowak, *Założenia dla perspektywicznego systemu rozpoznania*, AON, Warszawa, 2004, p. 65).

In the former US Secretary of Defence, Frank Carlucci's speech in 1988, an unequivocal assessment can already be found of the impact of electronics development on fighting capacity. He pointed out that in the near future, a 'smart technique of target destruction, integrated via informatics with automated processes for collecting and processing information, will be the most important component of any battlefield'²⁹.

In the early 1990s, Colonel John A. Warden of the US Air Force placed action in a new space that he called 'cybernetic space' in the theory of strategic paralysis, which also included operations in computer networks. Warden saw the enemy as a system of systems; the essence of his systemic approach is a model of five circles: the political elites (exercising general control); key institutions (transposing energy from one circle to another); infrastructure; society (people); and defence systems. According to Warden, any organisation (for example: state, company, army, terrorist organisation, criminal gang, etc.) should be considered as a structure consisting of a system of five interconnected circles (mentioned above), which constitute a whole and fulfill the functions established for them³⁰.

Each of Warden's circles operates in five 'dimensions' (Figure 1), which include the following elements: sea, land, air, space and cyberspace.



Source: P. Sienkiewicz, *Wizje i modele wojny informacyjnej*. in: *Spoleczeństwo informacyjne – wizja czy rzeczywistość?*, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, p. 375.

Figure 1. Warden's model of five dimensions

²⁹ L. Ciborowski, *Nowe systemy i środki walki oraz kierunki ich rozwoju w SZ państw obcych*, AON, Warszawa, 1993, p. 13.

³⁰ M. Vego, *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona no. 2, Warszawa, 2009, p. 185.

The so-called Warden's Model indicates that the location in cyberspace confirms the recognition of the existence of another dimension of warfare (here in fifth place because of space being noted by him)³¹. It can be concluded that, although he did not in any way refer to the division made by Howard M. Friedman³², his 'fourth dimension of war' was very simply called 'cybernetic space'.

Warden's views were reflected in the official US position on the conduct of military operations. The example is set by the National Military Strategy, adopted in 2004, according to which the US Armed Forces must have the ability to conduct operations on land, at sea, in the air, in space and in cyberspace, and which together form a warfare area³³.

Parallel to this recognition of the allocation of a warfare area, other US documents (for example Joint Publication (JP) 3-0 in the section 'Combined Operations') indicate that the 'operating environment' consists of the following domains: land, sea, air, space, and information environment³⁴. The last division emphasises that treating cyberspace as a domain provides a basis for understanding and defining its place in military operations. The above examples clearly expose a kind of lack of consistency in the understanding, meaning and location of cyberspace in military actions by American theorists.

Taking into account the natural evolution of the concept of cyberspace since the announcement of Warden's theory, and to assess what the concept of our American and British allies currently is, several definitions associated with this concept must be analysed. Here are some exemplary (available) definitions:

Cyberspace³⁵ (according to NATO - 2007/2008) – a digital world created by computers and computer networks, in which people and

³¹ P. Sienkiewicz, *Wizje i modele wojny informacyjnej*. w: *Spoleczeństwo informacyjne – wizja czy rzeczywistość?*, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, p. 374.

³² H.M. Friedman, *Securities Regulation in Cyberspace*, Aspen, 2005.

³³ *National Military Strategy for Cyberspace Operations – NMS-CO*, Joint Chiefs of Staff, Washington, 2006, p. 3.

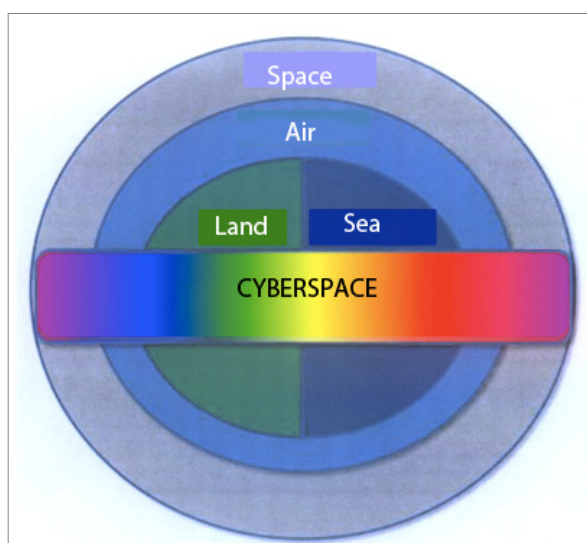
³⁴ *National Military Strategy for Cyberspace Operations – NMS-CO*, Joint Chiefs of Staff, Washington, 2006, p. 3.

³⁵ *AC/322(SC/2-NC3TS)L(2007)0002*, Definitions concerning cyberwar, 11 April 2007; *MC 571 – NATO Cyber Defence Policy*, 21 February 2008 [in: *NATO Bi-SC Directory of Information Operations v.1*, Allied Command Transformation, Norfolk, 2010, p. 84].

computers coexist, and which covers all aspects of working in the network.

Cyberspace³⁶ (according to the UK - 2009) - encompasses all forms of networked, digital activities, this includes the content of and actions conducted through digital networks.

Cyberspace³⁷ (according to the USA - 2010) - a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.



Source: Cyberspace Operations (DD 3-12), Center for Doctrine Development and Education of the US Air Force, 2010, p. 20.

Figure 2. The relationships between operational domains during the war by US Air Force theoreticians

Integration of cyber operations with other domains³⁸ (according to the USA - 2010) - the essence of this process is to achieve the ability to expand the capacity from other domains in order to achieve unique effects, the so-called 'Effect of decision-making'. As the use of cyberspace continues to evolve, Airmen will determine new ways to solve problems to meet national objectives.

³⁶ *Cyber Security Strategy of the United Kingdom – safety, security and resilience In cyber space*, The Parliamentary Bookshop, London, 2009, p. 7.

³⁷ *Cyberspace Operations (DD 3-12)*, Center for Doctrine Development and Education of the US Air Force, 2010, p. 51 [definition via: *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, USA*].

³⁸ *Cyberspace Operations (DD 3-12)*, Center for Doctrine Development and Education of the US Air Force, 2010, p. 19.

The core of cross-domain integration is the ability to leverage capabilities from different domains to create unique – and often 'decisive' – effects. The diagram below portrays the relationship among the operational domains, all domains are interconnected via cyberspace operations³⁹, which should be taken into account in the considerations of modern warfare⁴⁰. Recent Polish views that define cyberspace overlap substantially with American and British views, and are worded as follows:

Cyberspace⁴¹ (military unit 3984 - 2013) - a place consisting of computers, telecommunication devices, joint telecommunications networks, and any digital media, in which information processes are implemented.

Upon getting to know the relatively large conceptual material concerning cyberspace, the fundamental question remains: is cyberspace the correct term, does it deserve to be called the 'fourth dimension of war'? Well, no. Despite the clearly noticeable evolution and broadening of the impact area of cyberspace, all doctrinal American and allied documents continue to use the independent notion of electronic warfare (and everything that goes with it), operating alongside the cyberspace term. This shows that not all devices and electronic systems have been subordinated to the functioning of cyberspace.

Polish views on the dimensions of war

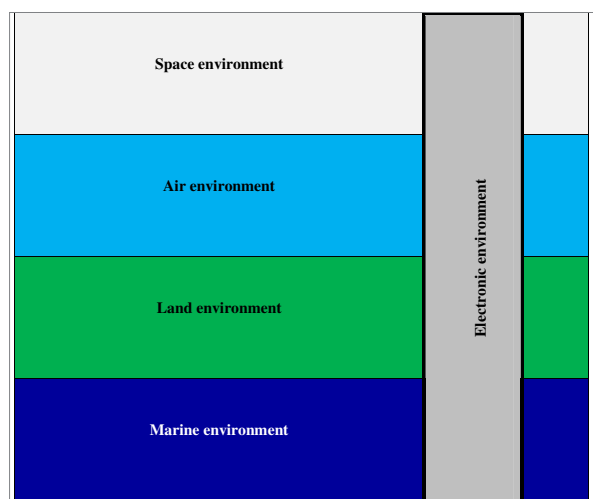
Recently, Polish officers have also joined in the theoretical considerations on this subject. According to the latest views of Air Force officer Lieutenant Colonel Stanisław Czeszejko, which were presented in an article in 'Air Force

³⁹ *Cyberspace Operations (DD 3-12)*, Center for Doctrine Development and Education of the US Air Force, 2010, p. 20.

⁴⁰ *Cyberspace Operations (DD 3-12)*, Center for Doctrine Development and Education of the US Air Force, 2010, p. 20, it is pointed out that this way of thinking is borrowed from: Convertino Sebastian, *Flying and Fighting in Cyberspace*, July 2007, Air University, p. 11.

⁴¹ R. Janczewski, *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym*, [in: materials after 20th scientific conference Automatyzacja Dowodzenia 2013], AON, Gdynia-Warszawa, 2013, p. 101.

Review' of June 2011, cyberspace⁴² is only a part of military operations, expanding and co-creating the existing 'fourth dimension of war' (based mainly on electronic warfare). He has given it a new name: 'the electronic environment'. He also presented its own chronological division of the dimensions of war, calling them environments. He set their sequence as follows: land environment; marine environment; air environment; electronic environment; space environment (Figure 3)⁴³. Also, in his work from the end of June 2011, developed during the course of Postgraduate Operational and Strategic Studies in NDU, S. Czeszejko qualifies activities using electromagnetic energy, activities in cyberspace (computer networks) and other activities with the use of electronic devices and systems as activities in the electronic environment. The activities in the electronic environment also include various interactions between the electronic environment and other environments (for example radar detection of aircrafts)⁴⁴. He also estimates that

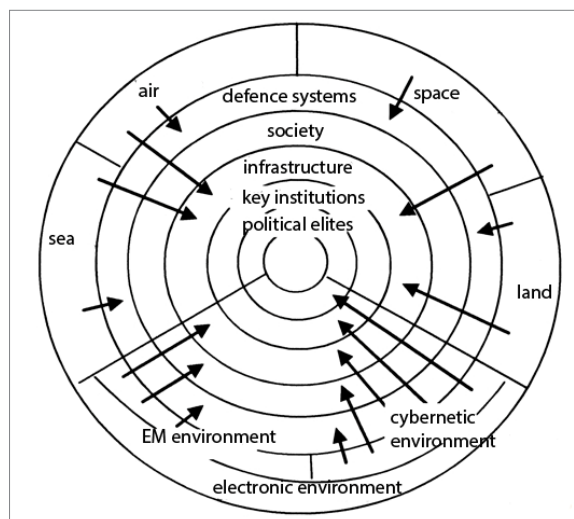


Source: S. Czeszejko, electronic activities and situational awareness of the battlefield [materials after 19th academic conference on automation in command, 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, p. 18.

Figure 3. The location of the electronic environment

this division will contribute positively to increase the efficiency of the use of electronic equipment and systems (their synergy) on the modern battlefield, including increasing the situational awareness of the battlefield. He indicates, as well, that the equipment and electronic systems are the distinguishing element and the common denominator for military operations conducted in the electronic environment.

Colonel Waldemar Scheffs, Officer of the National Defence University, in his speech during the academic conference on automation in command in October 2011, proposed modernising Warden's Model by replacing the notion of cyberspace with the term 'electronic environment' (to change the name). In addition, he proposed dividing the fifth circle of this model into two parts (Figure 4): the area of the electromagnetic environment and the area of cyber environment⁴⁵, which is, in fact, a confirmation of the views of his Polish colleague.



Source: W. Scheffs, *Automatyzacja działań urzędów elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [materials after 19th academic conference on automation in command, 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, p. 127.

Figure 4. The modernised version of J. Warden's interaction model

⁴² S. Czeszejko, *Konflikty ery informacyjnej*, Przegląd Sił Powietrznych nr 6, Warszawa, 2011, p. 9.

⁴³ S. Czeszejko, *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa, 2011, p. 123.

⁴⁴ S. Czeszejko, *Działania elektroniczne, a świadomość sytuacyjna pola walki*, [materials after 19th academic conference Automatyzacja Dowodzenia, 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, p. 11).

⁴⁵ W. Scheffs, *Automatyzacja działań urzędów elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [materials after 19th academic conference on automation in command, 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, p. 127).

Netcentricity

Another concept, which to some extent is related to the use of electronic equipment and systems, is the concept of netcentricity. The authors of the first definition of netcentricity were J. Garstka, D. Alberts and F. Stein, who are considered to be one of the forerunners of this concept. In short, it is based on concentrating power that can be generated through effective connections (networking) of military group elements⁴⁶ (including the use of electronic equipment and systems, mainly communication and ICT). The authors also believe that there was a need to move away from using the term 'battlefield' in favour of the term 'the environment' as 'the area of task execution'. In this kind of area, there will not be a clear boundary between soldiers and civilians. Therefore, netcentric warfare should be considered a part of the broader defined information warfare⁴⁷.

It should be kept in mind that this term is being used quite freely these days, while not giving its definition. The general sense of the concept used in the specific context is understandable. Nevertheless, a clear system of defined terms is needed for the name to accurately capture the essence of the concept.

Let us analyse available definitions related to netcentricity, including netcentric environment:

Netcentricity⁴⁸ (by NDU - 2007) - in terms of information technology (systemic) – it is integration with other systems (fusion of information) leading to the establishment of a common system (supersystem).

Network-centric environment⁴⁹ (by NDU - 2008) - a combination of factors resulting from profound changes in the military equipment and network connection of all forces participating in the activities, from soldier to vehicle to the highest echelons. By creating specific conditions that affect the phenomena and interactions taking place in the activities of the

army (other participants), it determines the nature of the command and the conduct of activities, giving them new specific features.

Network-centric environment⁵⁰ (by NDU - 2013) - Environment of advanced assistance systems for information and decision-making processes used in the armed forces. The introduction and development of the concept of operations in the network-centric environment have been forced by the changes taking place in the world of information technology and the increasing importance of information as a factor that plays a unique role in contemporary armed conflicts.

Netcentricity as a new concept of warfare, which could be observed during recent years, is still in the conceptual stage⁵¹. To assess netcentricity, bearing in mind the use of electronic equipment and systems, it can be estimated that network-centric activities in their meaning are most similar to information warfare. It should be noted that the main difference lies in the fact that netcentricity relies mainly on the use of electronic equipment and systems from the area of communications and IT.

The location of the 'centre of gravity' on the most important aspects of information warfare lies in the fact that the devices and electronic systems are mainly sources of information, while the main purpose of network-centric activities is being an electronic 'spin' to all elements that perform combat together, from which the 'military draws additional force'. However, in both cases the principal object of operation is information and not electronic devices and systems.

Everything indicates that in the first stage of its (not yet named) existence (development), netcentricity was: information warfare based on the use of means of communication and process support associated with getting information; as well as its processing and distribution (both often by independent use of computers). It was a combination of these two trends of development

⁴⁶ J.J. Garstka, D.S. Alberts, F.P. Stein, *Network-centric Warfare*, DoD C4ISR Cooperative Research Program, Washington D.C., 2000, p. 88.

⁴⁷ S. Zajas (edited by), *Stadium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa, 2009, p. 21.

⁴⁸ M. Żukowski, *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych*, [in: materials from scientific conference: „Sieci teleinformatyczne w działaniach sieciocentrycznych” - 2006], AON, 2007, p. 70.

⁴⁹ J. Posobiec, *Dowodzenie w środowisku sieciocentrycznym*, habilitation dissertation, Zeszyty Naukowe, AON, Warszawa, 2008, p. 52.

⁵⁰ K. Frącik, *Proces dowodzenia jako zasadniczy komponent systemu dowodzenia w uwarunkowaniach środowiska zaawansowanych systemów wspomagania procesów informacyjno-decyzyjnych*, [in: material after 20th scientific conference Automatyżacja Dowodzenia 2013], AON, Gdynia-Warszawa, 2013, p. 24.

⁵¹ S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [in: materials after international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych”], AON, 2008, p. 69.

in one systemic solution that created the conditions for the creation of the concept of netcentricity.

Netcentricity in no way claims to be the 'fourth dimension of war', because its main purpose is to enable the achievement of greater synergy of military operations carried out in all dimensions simultaneously, rather than carrying out activities in a new 'fourth dimension of war'.

Space or environment?

Using the concept of space in military science has its origin in the period during which analysis and mathematical modelling were extensively used. A typical representative of the 'school' for whom the mathematical apparatus was the basis of all scientific considerations, and which can still be found in Polish military literature, is Leopold Ciborowski. In his works he widely used mathematical concepts and, to justify his views, he indicates that more precise interpretation is provided by cybernetic and mathematical vocabulary⁵². He also verified most of his hypotheses using mathematical methods, in which the 'space' functions as a typical notion of 'mathematical apparatus'. He also distinguishes the concept of 'environment' but its meaning is not related to mathematics. Here are the definitions of the interesting concepts formulated by Professor Ciborowski:

Space⁵³ - a set of any objects (numbers, system states, vectors, etc.), among which some relations of geometric or abstract nature were established.

Warfare environment (the area of warfare)⁵⁴ - is the area around the subject of warfare in which it is located. According to the environmental conditions, only such weapons should be included which are suitable for use in this environment (in this area).

As seen in the example of the definition formulated by L. Ciborowski, 'space' is a typical mathematical concept used to test hypotheses using mathematical methods, while its use for military purposes is not entirely justified.

In contrast, the definition of 'environment' of warfare is more versatile and is fit for the

foregoing considerations, being the most useful. Nevertheless, one should read and evaluate the general definitions of the environment given by various sources where the environment is:

- 'Entirety of elements in the surrounding area';⁵⁵

- 'Entirety of all factors in the environment (animate and inanimate), more or less uniform in a given area, affecting living organisms, undergoing changes under the influence of these organisms';⁵⁶

- 'Fulfillment of highlighted system for whole area, which is the set of all objects (and their attributes and the relationship between these attributes) that, due to the adoption of the criteria of belonging to the system, have not been included in it'⁵⁷.

By analysing these definitions of space and the environment, the authors concluded that a more appropriate term for defining the area of conducting military operations would be 'environment' (land, marine, air, electronic and cosmic).

The definition of electronic environment

In the edition of the book by Alfred Price called 'Tools of Darkness: The history of warfare in 1939-1945' published in 1967, the 'foreword' by Robert Cockburn includes the term 'electronic environment'⁵⁸, which the author identifies with the operation of radar and radio systems. This term can be found in English-language publications even today.

An example of the modern use of such wording for military purposes is 'The development of the US Navy' from 2003⁵⁹, where in a subsection 'The missile AGM-88E AARGM' on page 123 the expression 'electronic environment'⁶⁰ is used.

⁵⁵ J. Brańczyk, *Słownik 100 tysięcy słów*, PWN, Warszawa, 2005, p. 829.

⁵⁶ S. Dubisz, *Uniwersalny słownik języka polskiego*, PWN, Warszawa, 2003, p. 731.

⁵⁷ B. Kaczorowski, *Wielka encyklopedia PWN - T. 27*, PWN, Warszawa, 2005, p. 47.

⁵⁸ A. Price, *Narzędzia mroku. Historia walki radioelektronicznej 1939-1945*, Wydawnictwo Dolnośląskie, Wrocław, 2006, p. 9.

⁵⁹ *Annual report on management, operational testing and development FY 2003*, United States Department of Defense, 2003, p. 123.

⁶⁰ *The target sets must emulate the threat system in physical appearance as well as in the electronic environment*".

⁵² L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, p. 95.

⁵³ *Ibidem*, p. 8.

⁵⁴ *Ibidem*, pp. 99-100.

Due to the fact that the term 'environment' is now fairly widely used and is a better term for the area where military actions are led, the authors of this study suggest the following definitions:

Electronic environment (environment of electronic activity) – the surroundings of electric signals and electromagnetic radiation produced by them (all of them are warfare objects). In this environment, the signals can be used and affected. In the electronic environment, the warfare tools (combat tools) mean the electronic devices and systems (mainly of military character) which are able to operate in this particular environment.

Electronic devices and systems – key elements of the electronic environment, which should be understood as a set of unanimated elements emerging as a result of human activity and which exist in a concrete place. They can be interrelated and influence each other. Also, a mutual dependence among them is possible – in accordance with the existing conditions.

The specificity of the electronic environment is the fact that activities carried out in it may interact with other warfare environments, for example weapons or, more broadly, tools for operations in an electronic environment (devices and electronic systems) may be destroyed with the use of tools naturally belonging to other environments (for example (destruction with tank fire). Another example is the detection of airborne objects with the use of electromagnetic radiation reflected from the surface of their external covering, where there is an interaction between the object of combat from the electronic environment (radiated electromagnetic signal and reception of its reflected form, the so-called 'echo'), and the air environment (aircrafts floating in the air).

Taking into consideration the need to unify the specialist terminology in the area of using electronic devices and systems, the authors suggest the division of military operations in accordance with the new approach, as conducted in different environments, and offer a wide practical application of this division. They also point to the possibility of widespread use of provided definitions of 'electronic environment' and the definition of 'electronic equipment and systems'. The analysis of the existing conceptual apparatus, deeply rooted in the minds of professionals, as well as its verification, was not an easy task. It required long-term observation, confrontation of

collected insights with other specialists, building one's own approach to research and creating an original description of achieved results. Conceptual 'Tools', provided by the authors, can act as way of structuring the approach to the subject, and can facilitate the further development of system solutions and are a topic under consideration.

Summary

Some experts use netcentric operations⁶¹ as an example to indicate the divergence in terminology, characteristic for Polish-language literature. According to the authors, this is a feature specific to the literature of other countries as well. It is, though, characteristic of a highly dynamically changing field, which is the development of electronic equipment and systems and their usage in conducting military operations. This indirectly translates to changing the way we fight when using them, which has a direct impact on the rules of engagement (for example electronic warfare); these, however, are part of the principles of the art of war. It does not remain unnoticed, by Polish specialists too and S. Markiewicz describes it in his work⁶². At the same time, he also clearly stressed that Z. Galewski points out that verification of rules for this kind of warfare happen in the course of armed conflict⁶³. It has to be kept in mind that these are not only the rules of military art, even the most modern, but their skilful usage in combat can lead to defeating the enemy.

The interdisciplinary nature of the activities in the electronic environment fits into a number of areas of scientific disciplines and specialties, and systemic and comprehensive perception of them allows their full understanding. Including aspects of technology related to electronic equipment

⁶¹ J. Janczak, *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [in: materials after international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych”], AON, 2008, p. 23].

⁶² S. Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [in: materials after international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych”], AON, 2008, p. 64.

⁶³ Z. Galewski, *Czynniki powodzenia we współczesnej walce*, Warszawa, 1986, p. 152 [quote via: Szymon Markiewicz, *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [in: materials after international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych”], AON, 2008, p. 64].

and systems in considerations allows for in-depth examination of cause-and-effect consequences in this area, which is also used to determine the use of its terminology.

Despite the development of various theories and system solutions concerning use of electronic equipment and systems, which are their consequence, as well as their impact on military operations, it should be remembered that the essence of tasks of different types of forces in future operations will remain the same, and it may be only slightly modified depending on the conditions that will accompany the implementation of the tasks facing them. The way the tasks are fulfilled will change for sure, and will result from changes in the general assumptions of warfare.

Bibliography

Books:

- Blach M., *Bazy danych elementem skuteczności rozpoznania elektronicznego*, [in: publication after the international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych”] AON 2008, ISBN 978-83-7523-055-0.
- Błażejczyk W., Nowacki G., Scheffs W., *Radiolokacja w wojskach lądowych wschodnich sąsiadów RP. Studium teoretyczne*, AON, Warszawa, 2002.
- Bralczyk J., *Słownik 100 tysięcy słów*, PWN, Warszawa, 2005, ISBN 83-01-14509-9.
- Ciborowski L., *Nowe systemy i środki walki oraz kierunki ich rozwoju w SZ państw obcych*, AON, Warszawa, 1993.
- Ciborowski L., *Rozpoznanie i Walka Elektroniczna*, AON, Warszawa, 1993.
- Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń, 1999, ISBN 83-88089-00-5.
- Czeszejko S., *Działania elektroniczne, a świadomość sytuacyjna pola walki*, [in: materials after 19th scientific conference Automatyżacja Dowodzenia 2011], Journal of KONBiN, No 2 (18), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, ISSN 1895-8281.
- Czeszejko S., *Działania elektroniczne w NATO i Siłach Zbrojnych Rzeczypospolitej Polskiej – próba kategoryzacji*, AON, Warszawa, 2011.
- Czeszejko S., *Konflikty ery informacyjnej*, Przegląd Sił Powietrznych nr 6, Warszawa, 2011, ISSN 1897-8444.
- Dubisz S., *Uniwersalny słownik języka polskiego*, PWN, Warszawa, 2003, ISBN 83-01-13868-8.
- Dubrawski Z., *Walka radioelektroniczna prowadzona przez SP. Studium operacyjne*, AON, Warszawa, 2000.
- Dymanowski K., Groszek Z., *Walka radioelektroniczna w działaniach SP we współczesnych konfliktach zbrojnych*, AON, Warszawa, 2008.
- Grabau R., *Sechs Dimisionen des Kriges. Versuch einer analitischen Betrachtung*, Soldat und Technik journal no. 5, 6, 7, 1985.
- Howard M., *Wojna w dziejach Europy*, Ossolineum, Wrocław, 2007, ISBN 978-83-0404-865-2.
- Janczak J., *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, AON, Warszawa, 2001.
- Janczak J., *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [in: materials after international scientific conference „Sieci teleinformatyczne w działaniach sieciocentrycznych” - 2006], AON, 2007, ISBN 978-83-7523-002-4.
- Janczewski R., *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym*, [in: materials after 20th scientific conference Automatyżacja Dowodzenia 2013 *Automatyżacja Dowodzenia SZ RP w środowisku sieciocentrycznym*], AON, Gdynia-Warszawa, 2013, ISBN 978-83-930150-3-0.
- Kaczorowski B., *Wielka encyklopedia PWN - T. 27*, PWN, Warszawa, 2005. ISBN 83-01143-62-2.
- Łokociejewski M., Scheffs Waldemar, *Walka elektroniczna w operacji i walce*, AON, Warszawa, 2005.
- Magnucki Z. [red.], *Walka radioelektroniczna w SZ RP*, AON, Warszawa, 1994.
- Malasiewicz K., *Czynniki domeny kognitywnej w planowaniu działań*, [in: materials after 20th scientific conference Automatyżacja Dowodzenia 2013 *Automatyżacja Dowodzenia SZ RP w środowisku sieciocentrycznym*], AON, Gdynia-Warszawa, 2013, 2013, ISBN 978-83-930150-3-0.
- Markiewicz S., *Zasady walki elektronicznej w działaniach sieciocentrycznych*, [in: materials after scientific conference „Walka elektroniczna w działaniach sieciocentrycznych” - 2008], AON, 2008, ISBN 978-83-7523-055-0.
- Nowak A., *Założenia dla perspektywicznego systemu rozpoznania*, AON, Warszawa, 2004.
- Piekarski H., *Walka radioelektroniczna*, Wydawnictwo MON, Warszawa, 1980, ISBN 83-11-06520-9.
- Posobiec J., *Dowodzenie w środowisku sieciocentrycznym*, habilitation dissertation, Zeszyty Naukowe, AON, Warszawa, 2008.
- Price A., *Narzędzia mroku. Historia walki radioelektronicznej 1939-1945*, Wydawnictwo Dolnośląskie, Wrocław, 2006, ISBN 978-83-7384-473-5.
- Scheffs W., *Automatyżacja działań urzędzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, [w: materials after 19th scientific conference Automatyżacja Dowodzenia 2011], Journal of KONBiN, No 3 (19), Instytut Techniczny Wojsk Lotniczych, Warszawa, 2011, ISSN 1895-8281.

- Scheffs W., *Proces oceny przeciwnika w aspekcie elektronicznym*, [in: materials after international scientific conference „Sieci teleinformatyczne w działaniach sieciocentrycznych” - 2006], AON, 2007.
- Scheffs W., *Założenia walki elektronicznej w środowisku sieciocentrycznym*, [in: materials after international scientific conference „Walka elektroniczna w działaniach sieciocentrycznych” - 2008], AON, 2008, ISBN 978-83-7523-055-0.
- Sienkiewicz P., *Wizje i modele wojny informacyjnej. w: Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Vol. 1, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2004, ISBN 83-89388-32-4.
- Szpyra R., *Militarne operacje informacyjne*, AON, Warszawa, 2003, ISBN 83-89423-40-5.
- Vego M., *Systemowe kontra klasyczne podejście do działań bojowych*, Kwartalnik Bellona no 2, Warszawa, 2009, ISSN 1897-7065.
- Zajas S. (edited by), *Studium przyszłości Sił Powietrznych. Kierunki rozwoju do 2025 roku*, AON, Warszawa, 2009, ISBN 978-83-7523-063-5.
- Żukowski M., *Ochrona kryptograficzna informacji w działaniach sieciocentrycznych*, [in: materials after international scientific conference „Sieci teleinformatyczne w działaniach sieciocentrycznych” - 2006], AON, 2007, ISBN 978-83-7523-002-4.

Journals:

- Handbook from Special Operations Forces Integration Course held in NDU Warsaw on 21-25 March 2011 by representatives of Joint Special Operations University from USA

Documents, reports:

- Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space, The Parliamentary Bookshop, Londyn, 2009.
- Cyberspace Operations (DD 3-12), Center for Doctrine Development and Education of the US Air Force, 2010.
- National Military Strategy for Cyberspace Operations – NMS-CO, Joint Chiefs of Staff, Washington, 2006.
- NATO Bi-SC Directory of Information Operations v.1, Allied Command Transformation, Norfolk, 2010.
- Joint Allied Doctrine for Information Operations (AJP-3.10), NATO Standardization Agency, 2009.
- Annual report on management, operational testing and development FY 2003, United States Department of Defense, 2003
- Walka elektroniczna, Sztab Generalny WP, Warszawa, 2003 (Szt. Gen. 1549/2003).

Websites:

- wikipedia.org
- Rybak T., Raport o stanie środowiska w 2010 chapter 6. Promieniowanie elektromagnetyczne (Source: access on 24 February 2014: http://www.wios.rzeszow.pl/cms/upload/edit/file/stan_srodowiska_2010/r6.pdf).