Sławomir Sadowski

Cyberprzestrzeń – nowy wymiar wojny?

Abstrakt

W artykule autor skupia się na problemie cyberprzestrzeni jako nowym obszarze wojny. Powstaje pytanie, czy cyberprzestrzeń może być uznawana za nowy wymiar wojny? Według autora, cyberprzestrzeń jest w niewielkim stopniu nowym wymiarem wojny, ponieważ pokrywa tylko fragment spektrum elektromagnetycznego, w którym prowadzone są wrogie działania. Tylko połączenie cyberprzestrzeni z innymi formami radioelektronicznej i elektronicznej interakcji tworzy nowy wymiar wojny, który może być opisany jako cyberelektroniczny wymiar wojny.

Słowa kluczowe: cyberprzestrzeń, wojna, walka elektroniczna, spektrum elektromagnetyczne, wymiary wojny.

Abstract

Cyberspace – a New Dimension in War?

In the article the author focuses on the problem of cyberspace as a new area of the war. It poses the question of whether cyberspace can be considered as a new dimension of war? According to the author cyberspace is hardly a new dimension of war, because it covers only a portion of the electromagnetic spectrum, within which hostilities are conducted. Only a combination of cyberspace with other forms of radio-electronic and electronic interactions create a new dimension of war, which can be described as a cyber-electronic dimension of war.

Keywords: Cyberspace, warfare, electronic warfare, the electromagnetic spectrum, the dimensions of the war.

W naukach politycznych pojęcie wojny rozumiane było przez dwa ostatnie wieki zgodnie z clausewitzowską tezą, że wojna to kontynuacja polityki innymi, tzn. militarnymi środkami. Jednak wojna to także zderzenie potencjałów militarnych, których wielkość w zasadniczym stopniu decyduje o jej wyniku. Wielkość tych wymiarów określa charakter wojny, jej skalę, konieczność zastosowania róż-

nych sił i środków na polu walki, a więc czynników decydujących o wyniku starcia zbrojnego. Pojawia się więc pytanie: Czym i jakie są to wymiary określające środowisko wojny?

Wymiar to wielkość obiektu lub zjawiska możliwa do opisania stosownymi miarami fizycznymi. Pojęcie to odnosi się również do ogólnego znaczenia skali faktu lub zjawiska, a więc w stosunku do wojny może ono mieć wymiar globalny, regionalny, lokalny itp. Pojęcie „wymiar wojny" wprowadził do obiegu naukowego brytyjski historyk Michael Howard w książce pt. *Wojna w dziejach Europy* wydanej w 1976 r., wymieniając wymiary: lądowy, morski i powietrzny oraz zasugerował istnienie czwartego wymiaru, związanego z intensywnym rozwojem i wykorzystaniem w XX wieku elektronicznych urządzeń łączności, kryptografii, rozpoznania i walki radioelektronicznej oraz radiolokacji, wykorzystujących głównie promieniowanie elektromagnetyczne. Howard nie nazwał owego nowego zjawiska wymiarem wojny, a jedynie wskazał na jego istnienie[1]. Postrzegał on wymiary wojny jako obszary jej prowadzenia.

Nieco inaczej potraktował wymiary wojny Rudolf Grabau[2], który wyodrębnił ich sześć, czyli: odległość, wysokość, powierzchnię, czas, informacje, spektrum elektromagnetyczne[3]. Według niego, wymiary wojny to nie tylko obszar jej prowadzenia, ale także czynniki decydujące o charakterze i skali wojen oraz konfliktów zbrojnych. Podkreślał, że szczególną rolę w przyszłych wojnach będą odgrywały trzy ostatnie wymiary: czas, informacje i spektrum elektromagnetyczne. W związku z powyższym w przeszłości, niemal do połowy XIX wieku, można było mówić o wymiarach wojny: odległości, przestrzeni, czasie i informacji, a więc wartościach łatwo wyrażanych za pomocą podstawowych wielkości fizycznych.

Wymiar pierwszy – odległość, rozumiemy jako długość krzywej (odcinka) pomiędzy dwoma punktami. Jednak w odniesieniu do wymiarów wojny bardziej adekwatna jest tzw. odległość Mahalanobisa, rozumiana jako odległość między dwoma punktami w n-wymiarowej przestrzeni, która różnicuje wkład poszczególnych składowych oraz wykorzystuje korelacje między nimi[4]. W dziejach wojen odległość w działaniach strategicznych w zasadzie jest wartością niezmienną,

[1] M. Howard, *Wojna w dziejach Europy*, Wrocław 1990, s. 167.

[2] Rudolf Grabau (ur. 1937 r.), emerytowany pułkownik Bundeswehry, jeden z twórców niemieckich założeń i organizator struktur organizacyjnych sił wojny elektronicznej. W formacjach tych służył w latach 1956-1987. Na emeryturze konsultant z zakresu historii telekomunikacji i radiowego rozpoznania elektronicznego w wielu komercyjnych firmach radioelektronicznych. Autor prac z zakresu wojny radioelektronicznej.

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

[4] A. I. Orlov, *Mahalanobis distance*, "The Encyclopedia of Mathematics", https://www.encyclopediaofmath. org/index.php/Mahalanobis_distance [dostęp: 12.10.2015]

gdyż zarówno współczesne wojny, jak starożytne czy średniowieczne prowadzone były na wielkich odległościach, które różnią się tylko czasem ich pokonywania przez wojska. Natomiast odległości w działaniach taktycznych i pośrednich (operacyjnych) zmieniły się w dziejach bardzo wydatnie. W okresie przedogniowym odległości zamykały się w wielkościach do kilku kilometrów, zaś współcześnie zasięg rakiet taktycznych, operacyjno-taktycznych czy lotnictwa taktycznego wynosi nawet do 1-2 tys. km[5].

Wymiar drugi – wysokość, rozumiany jest jako pionowa odległość jakiegoś punktu względem punktu odniesienia innego niż poziom morza. Wysokość była przez wieki drugorzędnym wymiarem wojny, dopiero pojawienie się lotnictwa i środków rakietowych spowodowało, że działania wojenne zostały wyniesione na pełną wysokość atmosfery ziemskiej, a w niektórych rodzajach działań przeniesione w przestrzeń kosmiczną. Tym samym wysokość stała się wymiarem w znacznym stopniu determinującym czas i sposób prowadzenia działań wojennych.

Przestrzeń to wymiar wyznaczony przez płaszczyznę i pionowy doń odcinek, w której każdemu punktowi odpowiada trójka uporządkowana liczb rzeczywistych, zwanych współrzędnymi. Ten rodzaj przestrzeni określa się mianem przestrzeni euklidesowej[6]. Jednak z wojskowego punktu widzenia równie istotna jest przestrzeń geograficzna i kosmiczna. Pod pojęciem przestrzeni geograficznej rozumie się powierzchnię Ziemi w jej fizycznym i przyrodniczym, złożonym zróżnicowaniu. Za jej umowne granice przyjmuje się najczęściej: dolną, czyli powierzchnię Moho, zaś górną – tropopauzę. Przestrzeń kosmiczna natomiast to strefa poza obszarem ziemskiej atmosfery. Za granicę pomiędzy atmosferą a przestrzenią kosmiczną przyjmuje się umownie wysokość 100 km nad powierzchnią Ziemi, gdzie przebiega linia Kármána[7]. Każda z tych przestrzeni odgrywa inną rolę w działaniach wojennych, aczkolwiek ich realna policzalna funkcja pojawiła się dopiero w XIX wieku, gdy zaistniała konieczność prowadzenia ognia z zakrytych stanowisk ogniowych, nawigowania statkami powietrznymi i okrętami, czy w końcu lotami rakiet.

Kolejny wymiar wojny to czas, kategoria niezwykle trudna do zdefiniowania, wieloznaczna. Generalnie można przyjąć, że czas to skalarna wielkość fizycz-

[5] Szerzej o przemianach taktyki, operacji i strategii w dziejach zob.: *Historia sztuki wojennej od starożytności do czasów współczesnych*, G. Parker (red.), Warszawa 2008; J. Keegan, *Historia wojen*, Warszawa 1998.

[6] O. Leszczak, *Ontologia czasu i przestrzeni w definicjach słownikowych i encyklopedycznych: analiza konceptualna*, „The Peculiarity of Man" 2014, nr 19, s. 15-42.

[7] Przestrzeń kosmiczna charakteryzuje się występowaniem wysokiej próżni, co uniemożliwia rozchodzenie się w niej fal dźwiękowych, a także bardzo utrudnia wymianę cieplną. Mimo że przestrzeń kosmiczną uważa się za strefę zdemilitaryzowana, to jest ona często wykorzystywana przez mocarstwa do rozmieszczania różnych środków zabezpieczania działań wojennych, np. systemów rozpoznawczych, łączności itp. W. Stankiewicz, *Rywalizacja państw w kosmosie*, „Przegląd Politologiczny" 2010, nr 2, s. 110-125.

na określająca kolejność zdarzeń oraz odstępy między zdarzeniami zachodzącymi w tym samym miejscu. Pod pojęciem czasu można rozumieć także: chwilę, punkt na osi czasu, odcinek czasu, trwanie, zbiór wszystkich punktów i okresów czasowych czy też czwartą współrzędną czasoprzestrzeni w teorii względności[8]. Z wojskowego punktu widzenia czas, jako wymiar wojny, ma bardzo różnorodną długość – od ułamków sekund po wieloletnie odcinki czasowe. Czas oznacza także porę roku lub doby.

Informacją nazywamy dane w postaci tekstu, liczb, dźwięków, obrazów itd., dzięki którym zmniejsza się stopień niewiedzy odbiorcy oraz które wnoszą do jego świadomości element nowości. Odbiorcą tych danych może być zarówno człowiek, jak i maszyna, jednak tylko człowiek posiada umiejętność zinterpretowania danych, dzięki czemu stają się one dla niego informacjami. Informacje ważne z wojskowego punktu widzenia to wszystkie dane mogące być przydatne w prowadzeniu wojny, w tym dotyczące:

- sytuacji politycznej, gospodarczej i geostrategicznej, a także ich wzajemnych zależności,
- sił i środków własnych i przeciwnika,
- cech charakterystycznych oraz sytuacji geograficznej, geologicznej, fizycznej, biologicznej, chemicznej i medycznej,
- sposobów postępowania, z uwzględnieniem zasad dowodzenia i działania, przepisów, regulaminów oraz niektórych reakcji automatycznych,
- treści przekazów pisanych, obrazowych lub dźwiękowych (np. rozkazów, meldunków, wiadomości, informacji rozpowszechnianych przez środki masowego przekazu),
- stanu i rozwoju właściwości fizycznych, psychicznych i moralnych,
- cybernetycznych współzależności między informacjami pojedynczymi a dużą ilością danych[9].

Informacje można wykorzystać tylko wtedy, gdy się je posiada do dyspozycji. Właściwość ta w sposób istotny odróżnia informację od takich wymiarów wojny, jak przestrzeń, czas czy spektrum elektromagnetyczne, które mają charakter obiektywny, a więc może je wykorzystać każdy w odpowiadający mu sposób.

Ostatnim, szóstym wymiarem wojny, według Grabaua, jest spektrum elektromagnetyczne. Pojęcie to jest najmłodszym spośród wszystkich wymiarów wojny, a jego źródeł należy szukać na początku XIX wieku wraz z odkryciem różnorodnych fal elektromagnetycznych. Promieniowanie elektromagnetyczne to rozchodzące się w przestrzeni zaburzenie pola elektromagnetycznego. Składowa elektryczna i magnetyczna fali indukują się wzajemnie – zmieniające się pole elektryczne wytwarza zmieniające się pole magnetyczne, a z kolei zmieniające się pole magnetyczne wytwarza zmienne pole elektryczne. Właściwości fal elek-

[8] O. Leszczak, dz. cyt., passim.

[9] R. Grabau, *Sześć wymiarów wojny,* cz. II, „Wojskowy Przegląd Zagraniczny" 1987, nr 2, s. 17-19.

tromagnetycznych zależą od długości fali. Promieniowanie elektromagnetyczne to różnej długości fale: radiowe, mikrofale, podczerwień, światło widzialne, ultrafiolet, promieniowanie rentgenowskie i promieniowanie gamma[10].

Informacje, czas i przestrzeń miały zawsze fundamentalne znaczenie w procesie kierowania wojną, natomiast z całego spektrum elektromagnetycznego wykorzystywano tylko niewielki jego zakres, czyli światło optyczne. Odkrycie kolejnych rodzajów fal elektromagnetycznych pozwoliło na większe ich wykorzystywanie na potrzeby wojny. Początkowo fale elektormagnetyczne stosowano tylko do szybkiego przekazywania meldunków i rozkazów. Od połowy XX wieku w coraz większym zakresie służyły do rozpoznania pola walki, naprowadzania środków bojowych na cel, ostrzegania przed atakiem przeciwnika, sterowania bezzałogowymi środkami bojowymi czy zakłócania przestrzeni elektromagnetycznej przeciwnika. W efekcie wygenerowano nowy obszar konfrontacji zbrojnej, nazwany wojną radioelektroniczną[11].

Po II wojnie światowej ukształtowało się i funkcjonuje nowe pojęcie – walka elektroniczna, które wywodzi się bezpośrednio z pojęcia walki radioelektronicznej, a to natomiast od pojęcia wojny radioelektronicznej. Praktycznie wszystkie dostępne definicje wskazują, że walka elektroniczna ogranicza się do prowadzenia działań militarnych z użyciem energii elektromagnetycznej.

Cyberprzestrzeń jako nowe środowisko wojny

Na początku lat dziewięćdziesiątych pułkownik John A. Warden z Sił Powietrznych Stanów Zjednoczonych w *teorii strategicznego paraliżu* wprowadził nową przestrzenń wojny, którą nazwał cyberprzestrzenią. Według Wardena, każdą organizację (w tym nieprzyjaciela) należy traktować jak strukturę składającą się z systemu pięciu wzajemnie powiązanych kręgów (elity polityczne, instytucje podstawowe, infrastruktura, społeczeństwo, systemy obronne), składających się na całość i pełniących założone dla nich funkcje. Każdy z kręgów Wardena funkcjonuje w pięciu wymiarach, na które składają się następujące elementy: morze, ląd, powietrze, przestrzeń kosmiczna, cyberprzestrzeń[12]. Można wnioskować, że

[10] Fundamentalnymi odkryciami w obszarze promieniowania elektromagnetycznego było odkrycie: w 1800 r. przez Williama Herschela promieniowania cieplnego, w 1801 r. przez Johanna Wilhelma Rittera promieniowania ultrafioletowego, w 1820 r. przez Hansa Christiana Ørsteda pola magnetycznego wytwarzanego przez prąd elektryczny, w 1831 r. przez Michaela Faradaya, że zmienne pole magnetyczne wytwarza pole elektryczne, przez Jamesa Clerka Maxwella w roku 1861 praw elektrodynamiki, w 1895 r. przez Wilhelma Conrada Röntgena promieniowania, nazwanego później rentgenowskim, w 1896 r. Antoine'a Henriego Becquerela promieniowania jądrowego, w 1900 r. przez Paula Villarda promieniowania gamma. A. Januszajtis, *Fale,* Warszawa 1991, passim.

[11] R. Grabau, *Sześć wymiarów wojny – walka o spektrum elektromagnetyczne,* cz. III, „Wojskowy Przegląd Zagraniczny" 1987, nr 2, s. 20.

[12] S. Czeszejko, *Ciągłość śledzenia a ciągłość informacyjna rozpoznania radiolokacyjnego w środowisku elektronicznym,* „Obronność. Zeszyty Naukowe" 2014, nr 4, s. 22-23.

chociaż nie odniósł się on w żaden sposób do podziału dokonanego przez poprzedników, to czwarty wymiar wojny Howarda czy grabauowskie spektrum elektromagnetyczne, nazwał po prostu „cyberprzestrzenią". Poglądy Wardena szybko znalazły odzwierciedlenie w amerykańskich poglądach na prowadzenie działań militarnych.

Pojęcie to upowszechniło się bardzo szybko i współcześnie praktycznie we wszystkich krajach świata definiowane jest w sposób podobny, jak uczynił to Departament Obrony USA, który stwierdza, że cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[13]. Analizę definicji pojęcia cyberprzestrzeń w głównych państwach świata prezentuje Janusz Wasilewski w artykule *Zarys definicyjny cyberprzestrzeni*[14].

W przyjętej w 2003 r. Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni USA zapisano:

> „Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego."[15]

Europejskie pojmowanie cyberprzestrzeni jest bardzo zbliżone do amerykańskiego i Komisja Europejska definiuje ją jako: „Wirtualną przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata[16]". Elementem podstawowym tej definicji stała się „przestrzeń wirtualna". Ta wyodrębniona logicznie (nieistniejąca fizycznie) przestrzeń jest tworzona przez sumę

[13] *Department of Defense Dictionary of Military and Associated Terms 8 November 2010. As Amended Through 15 June 2015,* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf [dostęp: 15.10.2015].

[14] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni,* „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225-234.

[15] *National Strategy to Secure Cyberspace*, Department of Homeland Security, http://www.dhs.gov/national-strategy-secure-cyberspace (dostęp: 1.10.2015).

[16] R. Ottis, P. Lorents, *Cyberspace. Definition and Implications,* Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf [dostęp: 10.10.2015].

zawartych w systemach danych, plików, stron internetowych, aplikacji oraz procesów, do których uzyskuje się dostęp wyłącznie poprzez systemy teleinformatyczne[17]. Brytyjskie pojmowanie cyberprzestrzeni zostało zawarte w *Strategii Cyberbezpieczeństwa Zjednoczonego Królestwa* z 2011 r. i zgodnie z nim:

> „Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują nasz biznes, infrastrukturę oraz wspomagają świadczenie usług. Cyfrowe sieci już dziś podbudowują proces zaopatrywania naszych domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów oraz służą za niezbędne narzędzie biznesowe w całym Zjednoczonym Królestwie. Ich zasięg ustawicznie się powiększa, w miarę jak podłączamy do nich nasze telewizory, konsole do gier, czy nawet urządzenia AGD."[18]

Brytyjczycy poszerzyli pojęcie cyberprzestrzeni i, prócz internetu, włączyli doń inne sieci, niekoniecznie połączone z globalną siecią WWW, na przykład lokalne, wykorzystywane w dużych przedsiębiorstwach. Jest to dosyć oryginalne pojmowanie cyberprzestrzeni, gdyż w innych krajach pojęcie to jest integralnie łączone z internetem, z globalna siecią.

We współczesnym świecie sieci informatyczne tworzące cyberprzestrzeń stanowią istotny element funkcjonowania społeczeństwa w wymiarze gospodarczym, społecznym, politycznym, kulturalnym i praktycznie każdym innym. Naruszenie stabilności w sieci uchodzi za poważne naruszenie bezpieczeństwa indywidualnego oraz zbiorowego. Jednak wiąże się ono ściśle z konstruowaniem przez człowieka urządzeń i systemów elektronicznych, służących do transmisji danych i informacji – sieci komputerowych (teleinformatycznych).

To – oczywiście – z wojskowego punktu widzenia kwestia bardzo ważna, ale czy wyczerpuje w istocie znamiona nowego wymiaru wojny? Gdyby jednak zaakceptować spektrum elektromagnetyczne Grabaua jako nowy wymiar wojny, to niewątpliwie cyberprzestrzeń tylko częściowo wypełnia zakreślony przez niego obszar. Należy także przyjąć, że Amerykanie cyberprzestrzeń postrzegają jako pewien fragment większej, elektronicznej przestrzeni.

Wojna (walka): elektroniczna – informatyczna – cybernetyczna

We wszystkich dokumentach doktrynalnych amerykańskich i NATO nadal występuje pojęcie walki elektronicznej, co świadczy o tym, że nie wszystkie urzą-

[17] J. Wasilewski, dz. cyt., s. 229.

[18] *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [dostęp: 1.10.2015].

dzenia i systemy elektroniczne zostały podporządkowane cyberprzestrzeni. Istotnym elementem współczesnych operacji wojskowych są działania w środowisku elektromagnetycznym. Obejmują one trzy rodzaje działań: atak elektroniczny, obronę elektroniczną i wsparcie elektroniczne. Elektroniczny atak to forma wykorzystania impulsu elektromagnetycznego do zakłócania i uniemożliwienia użycia go przez przeciwnika. Do aktywnych form ataku zalicza się: zagłuszanie, zakłócanie radiowe i uderzeniowe użycie impulsu elektromagnetycznego. Obrona elektroniczna ma na celu ochronę personelu, uzbrojenia i urządzeń przed wszelkimi skutkami wrogiego wykorzystania spektrum elektromagnetycznego przez przeciwnika. Wsparcie elektroniczne polega na pasywnym wykorzystaniu promieniowania elektromagnetycznego dla zdobycia informacji o jednostkach znajdujących się na polu walki lub znalezienia, zidentyfikowania i przechwycenia potencjalnych zagrożeń lub celów. Celem walki elektronicznej jest redukcja przewagi przeciwnika w przestrzeni elektromagnetycznej i uzyskanie w niej przewagi celem swobodnego dostępu do środowiska informacyjnego. Walkę elektroniczną prowadzi się we wszystkich środowiskach wojny i może być ona realizowana w powietrzu, na ziemi i morzu za pomocą systemów załogowych i bezzałogowych[19].

Wojna elektroniczna stanowi istotny element doktryny wojennej wszystkich nowoczesnych armii świata. Mimo że niewątpliwie technologicznie najbardziej zaawansowane są amerykańskie, izraelskie i japońskie systemy walki elektronicznej, to skuteczne instrumenty jej prowadzenia znajdują się także w arsenałach rosyjskim, chińskim i innych posiadających w miarę zaawansowane systemy elektroniczne.

W literaturze pojawia się także pojęcie walka informatyczna, którą również sytuuje się w przestrzeni elektronicznej. Militarny charakter walki informacyjnej definiuje się, jako:

> „zorganizowaną w formę przemocy militarną aktywność zewnętrzną państwa prowadzącą do osiągnięcia określonych celów politycznych, skierowaną na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływających przez nie informacji oraz ochronę własnych systemów informacyjnych przed podobnym działaniem przeciwnika."[20]

W istocie rzeczy mamy tu do czynienia z odmianą walki elektronicznej, odbywającej się w ograniczonej przestrzeni. Należy jednak zaznaczyć, że nie dotyczy to tylko działań w cyberprzestrzeni, gdyż współcześnie transfer informacji wojskowej odbywa się nie tylko poprzez sieć internetową, lecz również tradycyj-

[19] *Electronic Warfare. Joint Publication 3-13.1,* http://fas.org/irp/doddir/dod/jp3-13-1.pdf [dostęp: 10.10.2015].

[20] *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka),* t. I: *Raport z badań*, T. Jemioło, P. Sienkiewicz (red.), Warszawa 2004, s. 75; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku,* „Bezpieczeństwo Narodowe" 2011, nr 1, s. 17.

nie, poprzez niezwykle zaawansowane technologicznie systemy łączności, choćby łączność radiową, emitującą w mikroczasie głęboko zakodowane informacje, czy też łączność kosmiczną. Warto podkreślić, że elementem walki informacyjnej jest też zdolność do zakłócenia systemów sterowania i kierowania środkami bojowymi przeciwnika.

Trzecim pojęciem, które łączy elektromagnetyczny wymiar wojny i cyberprzestrzeń jest niewątpliwie wojna cybernetyczna (cyberkonflikt). Pojęcie to odnosi się do konfliktu angażującego różnorodne systemy ludzi, rzeczy, procesów i postrzegania, które związane są z sieciami komputerowymi, choć niekoniecznie całkowicie skomputeryzowane. Konfliktem cybernetycznym będzie zatem:

> „każdy konflikt, w którym sukces lub porażka są dla większości jego uczestników uzależnione od działań prowadzonych w sieciach komputerowych. W związku z tym tak długo, jak długo Internet pozostanie na tyle otwarty, jak jest dzisiaj, konflikty prowadzone na jakiejkolwiek płaszczyźnie będą podlegały 'cybernetyzacji'. Wynika to z faktu, że obecnie niemal każdy aspekt ludzkiej działalności powiązany jest w jakimś stopniu z działaniem sieci cyfrowych"[21].

Według Krzysztofa Liedla cyberkonflikty można podzielić na:

- aktywizm – niedestrukcyjną działalność, w ramach której internet służy wsparciu prowadzonej kampanii,
- haktywizm – kombinację aktywizmu i działań przestępczych; wykorzystuje on metody hakerskie przeciwko określonym celom w internecie, by zakłócić ich funkcjonowanie, nie powodując przy tym poważnych strat; działalność ta ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócenie uwagi na dany problem,
- cyberterroryzm – politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach realizacji daleko idących politycznych i społecznych działań w szerszym rozumieniu tego słowa; jest to także użycie internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne[22].

Generalnie rzecz biorąc, walka cybernetyczna realizowana jest w sieci internetowej, a więc nie wyczerpuje wymiaru elektromagnetycznego wojny, a tylko może być jednym z elementów działań militarnych.

[21] K. Liedel, P. Piasecka, dz. cyt., s. 17-18; P. Dombrowski, Ch. C. Demchak, *Cyber war, cybered conflict, and the maritime domain*, https://www.usnwc.edu/getatt achment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx [dostęp: 15.10. 2015].

[22] K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 23-24.

Nowy wymiar wojny – cyberprzestrzeń czy spektrum elektromagnetyczne

Ten problem znajduje także odzwierciedlenie w polskiej dyskusji naukowej. Stanisław Czeszejko uważa, że cyberprzestrzeń jest jedynie elementem działań militarnych, który poszerza i współtworzy *czwarty wymiar wojny* Howarda. Wymiar ten nazwał środowiskiem elektronicznym[23]. Jest on również autorem klasyfikacji wymiarów wojny, które określił mianem środowisk: lądowe, morskie, powietrzne, elektroniczne i kosmiczne[24]. Interesujące jest zwłaszcza wprowadzenie kosmicznego wymiaru wojny, który to zgodnie z prawem międzynarodowym jest obszarem o ograniczonych możliwościach prowadzenia działań wojennych.

Mimo że od początku ery kosmicznej interesy wojskowe były jednym z decydujących czynników działalności kosmicznej państw, to jednak starano się ograniczyć zwłaszcza prawo do umieszczania w kosmosie broni masowego rażenie. Jednak siły stacjonujące na globie ziemskim aktywnie wykorzystują i eksploatują satelity o różnorodnych funkcjach i zadaniach. Obiekty te nie są bronią w ścisłym znaczeniu, ponieważ nie stwarzają niebezpieczeństwa bezpośredniego ataku w kosmosie lub z kosmosu. Często stanowią wręcz ogniwo umocnienia stabilności w stosunkach międzynarodowych, jako narodowe środki kontroli umów rozbrojeniowych. Funkcjonowanie systemów satelitarnych jest ściśle powiązane z naziemnymi siłami zbrojnymi państwa. Zgodnie z międzynarodowymi zobowiązaniami państw, ich narodowa satelitarna technika kontroli nie może być przedmiotem napaści, zagłuszania czy innych działań utrudniających prawidłowe funkcjonowanie. Dotyczy to w szczególności systemów wczesnego uprzedzania i nawigacji[25].

Biorąc powyższe pod uwagę, wydaje się, że definiowanie kosmosu jako odrębnego środowiska wojny jest chyba przedwczesne. W istocie rzeczy, mamy bowiem do czynienia praktycznie z poszerzeniem działania niektórych form walki zbrojnej w przestrzeń kosmiczną, ale w dalszym ciągu mamy do czynienia z „ziemskimi" wymiarami wojny.

Z kolei Waldemar Scheffs zaproponował modyfikację *Modelu Wardena* poprzez zastąpienie pojęcia przestrzeni cybernetycznej określeniem środowisko elektroniczne. Dodatkowo dokonał on podziału piątego kręgu na dwie części: obszar

[23] S. Czeszejko, *Konflikty ery informacyjnej*, „Przegląd Sił Powietrznych" 2011, nr 6, s. 9; Tenże, *Ciągłość śledzenia...*, dz. cyt., s. 24.

[24] S. Czeszejko, *Działania elektroniczne a świadomość sytuacyjna pola walki*, „Journal of KONBiN" 2011, nr 2, s. 18.

[25] C. T. Szyjko, *Bezpieczeństwo kosmosu: rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej*, „Portal Stosunki Międzynarodowe", http: //stosunki-miedzynarodowe.pl/bezpieczenstwo/798-bezpieczenstwo-kosmosu-rewizja-zasad-pokojowego-wykorzystnia-przestrzeni-wokolziemskiej [dostęp: 17.10.2015]

środowiska elektromagnetycznego i obszar środowiska cybernetycznego[26]. Ta bardzo interesująca propozycja budzi jednak pewne wątpliwości, gdyż oba te środowiska wzajemnie się uzupełniają i w wielu punktach są zbieżne, a więc raczej tworzą jedno środowisko – wymiar wojny. Powyższe stanowisko znajduje odzwierciedlenie także w Stanach Zjednoczonych. Rick San Miguel w prezentacji *Cyber CoE Doctrine Brief* zaprezentowanej 10 września 2014 r. w *Cyber Centre of Exellence* w Fort Gordon postuluje połączenie działań w cyberprzestrzeni i wojny radioelektronicznej w jeden wspólny obszar (wymiar wojny)[27].

Ten tok myślenia przebija się także w innych państwach, zwłaszcza w Rosji, gdzie działania walki radioelektronicznej są ściśle koordynowane z cyberatakami. Przykładem takiej kooperacji jest wojna z Gruzją 2008 r., kiedy to cyberprzestrzeń i spektrum elektromagnetyczne stanowiły jeden wymiar wojny[28].

* * *

Stosowane w powszechnym obiegu pojęcie cyberprzestrzeń trudno uznać za określenie równoważne z innymi wymiarami wojny, gdyż obejmuje ono tylko pewną część środowiska elektronicznego, w ramach którego prowadzone są działania wojenne. Dopiero połączenie cyberprzestrzeni z innymi formami oddziaływań radioelektronicznych i elektronicznych tworzy nowy wymiar wojny, który można określić jako cyberelektroniczny wymiar wojny. Wydaje się, że pojęciu cyberprzestrzeń, powstałemu w obszarze popkultury i zaadaptowanemu do świata prawdziwych konfliktów, zbyt pochopnie próbowano nadać status wymiaru (odrębnego środowiska) wojny. W istocie cyberprzestrzeń to środowisko będące fragmentem większego wymiaru, którego istotą jest wykorzystanie w działaniach wojennych spektrum elektromagnetycznego w jego wszystkich wielowariantowych przejawach.

Bibliografia

Czeszejko S., *Ciągłość śledzenia a ciągłość informacyjna rozpoznania radiolokacyjnego w środowisku elektronicznym*, „Obronność. Zeszyty Naukowe" 2014, nr 4.

Czeszejko S., *Działania elektroniczne, a świadomość sytuacyjna pola walki*, „Journal of KONBiN" 2011, nr 2.

[26] W. Scheffs, *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, „Journal of KONBiN" 2011, nr 3, s. 127.

[27] http://www.afcea.org/events/augusta/14/documents/T2S3AFCEATechNetBriefDoctrineandLessonsLearned29Jul.pdf [dostęp: 15.10.2015].

[28] *Walka radioelektroniczna w wojnie rosyjsko-gruzińskiej w 2008 r.*, „Portal Militarium.net" http://militarium.net/walka-radioelektroniczna-w-wojnie-rosyjsko-gruzinskiej-w-2008-r/ [dostęp: 16.10.2015].

Czeszejko S., *Konflikty ery informacyjnej*, „Przegląd Sił Powietrznych" 2011, nr 6.
Department of Defense Dictionary of Military and Associated Terms 8 November 2010. As Amended Through 15 June 2015, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
Dombrowski P., Demchak Ch. C., *Cyber war, cybered conflict, and the maritime domain*, https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx.
Electronic Warfare. Joint Publication 3-13.1, http://fas.org/irp/doddir/dod/jp3-13-1.pdf
Grabau R., *Sechs Dimissionen des Krieges. Versuch einer analytischen Betrachtung*, „Soldat und Technik" 1985, nr 5.
Grabau R., *Sześć wymiarów wojny,* cz. I, „Wojskowy Przegląd Zagraniczny" 1987, nr 1.
Grabau R., *Sześć wymiarów wojny,* cz. II, „Wojskowy Przegląd Zagraniczny" 1987, nr 2.
Grabau R., *Sześć wymiarów wojny,* cz. III, „Wojskowy Przegląd Zagraniczny" 1987, nr 3.
Historia sztuki wojennej od starożytności do czasów współczesnych, G. Parker (red.), Warszawa 2008.
Howard M., *Wojna w dziejach Europy*, Wrocław 1990.
Januszajtis A., *Fale,* Warszawa 1991.
Keegan J., *Historia wojen*, Warszawa 1998.
Leszczak O., *Ontologia czasu i przestrzeni w definicjach słownikowych i encyklopedycznych: analiza konceptualna,* „The Peculiarity of Man", 2014, nr 19.
Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010.
Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku,* „Bezpieczeństwo Narodowe" 2011, nr 1.
National Strategy to Secure Cyberspace, Department of Homeland Security, http://www.dhs.gov/national-strategy-secure-cyberspace.
Orlov A. I., *Mahalanobis distance*, "The Encyclopedia of Mathematics", https://www.encyclopediaofmath. org/index.php/Mahalanobis_distance.
Ottis R., Lorents P., *Cyberspace. Definition and Implications,* Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.
San M. R., *Cyber CoE Doctrine Brief,* http://www.afcea.org/events/augusta/14/documents/T2S3AFCEATechNetBriefDoctrineandLessonsLearned29Jul.pdf.
Scheffs W., *Automatyzacja działań urządzeń elektronicznych w środowisku cyberprzestrzeni i walki elektronicznej*, „Journal of KONBiN" 2011, nr 3.
Stankiewicz W., *Rywalizacja państw w kosmosie,* „Przegląd Politologiczny" 2010, nr 2.
Szyjko C. T., *Bezpieczeństwo kosmosu: rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej,* „Portal Stosunki Międzynarodowe", http: //stosunki-miedzynarodowe.pl/bezpieczenstwo/798-bezpieczenstwo-kosmosu-rewizja-zasad-pokojowego-wykorzystnia-przestrzeni-wokolziemskiej.
The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf.
Walka radioelektroniczna w wojnie rosyjsko-gruzińskiej w 2008 r., „Portal Militarium.net" http://militarium.net/walka-radioelektroniczna-w-wojnie-rosyjsko-gruzinskiej-w-2008-r.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni,* „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka), t. I: *Raport z badań*, T. Jemioło, P. Sienkiewicz (red.), Warszawa 2004.