Cyberprzestrzeń – piąty teatr wojny cz. II

Cyberwojna – wyzwanie dla bezpieczeństwa państwa
Wybrane zagadnienia

PIXABAY

LESZEK KLICH

informatyk i programista od wielu lat projektuje bezpieczne rozwiązania informatyczne dla biznesu. Na UKSW pracuje nad dysertacją „Zagrożenia w cyberprzestrzeni jako współczesne wyzwania dla bezpieczeństwa i obronności Rzeczypospolitej Polskiej".

W artykule poruszono wybrane zagadnienia działań w cyberprzestrzeni, które pomimo swojego militarnego charakteru, oddziaływać mogą również na sferę cywilną lub też odwrotnie. Naukowego opisu wymagają pojęcia stosowane przy identyfikacji wybranych zjawisk, głównie ze względu na wiele obowiązujących terminów. Autor podjął próbę wyekstrahowania najważniejszych pojęć terminologicznych: cyberwojny, wojny informacyjnej oraz walki informacyjnej.

Wojna znana jest ludzkości od zarania dziejów. Zawsze walczono o władzę, terytoria, zasoby. Postęp techniczny i cywilizacyjny spowodował wzrost wartości nowych, niematerialnych zasobów, co spowodowało rozwój dodatkowych przyczyn konfliktów. Zmieniające się przyczyny współzawodnictwa i walki zmieniły jednocześnie formę współczesnych wojen. Zmieniła się również jej koncepcja. Z wyłącznie fizycznej formy starcia między państwami, która polegała głównie na skierowaniu do walki jak największej liczby żołnierzy i sprzętu, przygotowania taktycznego i strategicznego dowódców, co umożliwiło tworzenie się warunków starcia w kierunku form hybrydowych, lub też coraz częściej – cyfrowych[1].

W cyberprzestrzeni życie cywilne znajduje się na pierwszej linii, jednak coraz częściej mamy w niej do czynienia z interesami wojska. Obecnie toczące się konflikty międzypaństwowe coraz częściej określa się „cyberwojną", choć obecnie żaden akt cyberprzestępczy nie wywołał jak dotąd zbrojnego konfliktu[2].

Oprócz negatywnej działalności, toczy się tam wszelka inna cyberaktywność, co oznacza, że dane bojowe przemieszczają się wraz z innymi, niegroźnymi danymi, w żaden sposób nie oddziałując na siebie wzajemnie, zaś walka toczy się w ściśle określonych miejscach[3].

Abstract

The article discusses selected issues related to activities in cyberspace that despite their military nature can also affect the civil sphere, or vice versa. A scientific description is required for notions used in identification of selected phenomena, mainly due to many terms in use. The author made an attempt to extract the most important terminological notions: cyberwar, netwar and information warfare.

Terminologia

Cyberwojna to konflikt międzypaństwowy lub globalny, prowadzony przede wszystkim z użyciem technologii informacyjno-komunikacyjnej[4]. W literaturze można jednak spotkać także pojęcie cyberwarfare, które oznacza użycie systemów informatycznych (sprzętu, oprogramowania oraz Internetu) oraz innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzenia ataków na systemy informacyjne i informatyczne przeciwnika[5].

Pojawienie się wielu określeń związanych z wojną w cyberprzestrzeni, jak: „cyberwojna", „wojna sieciowa", „wojna informacyjna", czy „walka sieciocentryczna"[6] spowodowało, że szczególnie w publicystyce terminy te stosowane są w sposób dowolny i niezależny od

1. K. Liedel, P. Piasecka Wojna cybernetyczna – wyzwanie XXI wieku, Bezpieczeństwo Narodowe I-2011, s. 17.
2. C. François Cyberwojna czy cyberpokój?, http://wolnemedia.net/cyberwojna-czy-cyberpokoj (stan na 08.08.2016).
3. B. Józefiak Cyberbezpieczeństwo na szczycie NATO. Jakie priorytety Polski i Sojuszu?, http://www.cyberdefence24.pl/399633,cyberbezpieczenstwo-na-szczycie-nato-jakie-priorytety-polski-i-sojuszu (stan na 16.08.2016).
4. Information – Comunication Technology, ICT.
5. J. Kisielnicki Po drugiej strony mocy, czyli ciemne strony informatyki, Annales Universitatis Mariae Curie-Skłodowska, Vol L,2 – 2016, s. 34.
6. Zob. B. Grenda Sieciocentryczne zarządzanie siłami powietrznymi, AON, Journal of KONBiN 3(19) 2011, s. 5: Od zarania wieków teoretycy sztuki wojennej poszukują odpowiedzi na pytanie, jak skutecznie oddziaływać informacyjnie na przeciwnika dla dezorganizacji jego systemów informacyjnych przy zachowaniu ochrony systemów własnych. Poszukiwania te

ARCH. LESZEK KLICH

zjawiska, którego dotyczą. Tymczasem, ich znaczenie nie jest tożsame, choćby dlatego, że zapobieganie im bądź ich prowadzenie, nie zawsze należy do zadań armii[7].

Jedna z definicji określa cyberwojnę, jako *działania prowadzone przez państwa oraz podmioty niepaństwowe, przy użyciu broni cybernetycznych do penetrowania komputerów lub sieci w celu niszczenia, i/lub fałszowania danych, zakłócania lub uszkodzenia systemów. Działania cyberwojenne dotyczą także stosowania aktów szpiegostwa, przestępstw oraz wojny gospodarczej, lecz mogą również obejmować działania mające na celu wsparcie operacji wojskowych na szczeblu taktycznym i operacyjnym wojny oraz działania mające na celu uzyskanie efektów strategicznych*[8].

Słownik wydawnictwa Oxford University Press z kolei definiuje cyberwojnę, jako wykorzystanie technologii komputerowej do zakłócania działalności innego państwa lub organizacji poprzez zamierzone ataki na systemy komunikacyjne przez inne państwa[9].

Słownik Macmillan Dictionary podaje jednocześnie dwa znaczenia dla zjawiska cyberwojny:, jako rodzaju wojny, w której systemy komputerowe są wykorzystywane w celu niszczenia, bądź uszkadzania wrogich systemów i wykorzystania systemów komputerowych dostarczających informacje dla zyskania przewagi lub zniszczenia zdolności wroga do przekazywania informacji[10].

Mieczysław Bieniek pisał o cyberwojnie, jako o świadomych i celowych działaniach ze strony państw lub organizacji – w tym także terrorystycznych, które mają na celu zakłócenie działania lub zniszczenie struktur zarządzania innego państwa lub organizacji. Celem w tym przypadku jest zredukowanie zdolności obronnych przeciwnika w stopniu uniemożliwiającym skuteczne funkcjonowanie i przeciwdziałanie innym formom działań wojennych. Autor podkreślił jednocześnie konieczność ostrożności w ujmowaniu zjawiska cyberwojny ze względu na wymiar konfliktu, wymagający elastycznego i złożonego podejścia. Działania w cyberprzestrzeni nie muszą być działaniami zbrojnymi, choć skutki dokonanego ataku mogą być równie destrukcyjne jak w przypadku bezpośrednich działań wojennych[11].

Jednym z najpopularniejszych terminów używanych w omawianej materii jest „net war", czyli wojna sieciowa, który może się odnosić także do społecznych konfliktów ideowych, prowadzonych po części poprzez różne formy komunikacji, co dotyczy głównie operacji na szczeblu wojskowym. Obie formy walki koncentrują się ściśle na informacji, zaś ich istotą jest walka o wiedzę na temat: kto co wie, kiedy, gdzie i dlaczego oraz wiedzy na temat swojego przeciwnika[12].

Kluczowym słowem jest w tym przypadku sieć, która we współczesnym dialekcie języka angielskiego oznacza *the network*, czyli sieć (komputerowa), zaś w rzeczywistości chodzi o cyberprzestrzeń. Z militarnego punktu widzenia, cyberprzestrzeń stanowi przestrzeń informacyjną, w której rozwija się operacje strategiczne o charakterze wojskowym i wywiadowczym oraz przestrzeń medialną, dyplomatyczną, ekonomiczną oraz techniczną. Można tu wyodrębnić elementy składowe sieci, dotąd wymieniane oddzielnie, jak: jednostki bojowe, kształtowanie opinii publicznej, wywiad i kontrwywiad, system łączności, obsługa informacyjna, posunięcia dyplomatyczne, procesy społeczne, etnopsychologia, psychologia religijna i kolektywna, źródła finansowania, nauka akademicka, czy innowacje technologiczne. Wymienione elementy tworzone są jako składowe sieci, wzajemnie powiązane i służące wymianie in-

doprowadziły do wypracowania nowej koncepcji walki sieciocentrycznej, która bazuje na nowym sposobie myślenia – myśleniu sieciocentrycznym. Nowa koncepcja walki wykorzystującej informację, zapoczątkowana została w Siłach Zbrojnych Stanów Zjednoczonych w latach 90.

7. R. Ciastoń Piąty element, [w:] Polska Zbrojna, nr 18(811) listopad 2013, s.18.
8. Zob. http://www.academia.edu/8906542/NATO_a_aspekty_bezpieczeństwa_w_cyberprzestrzeni_w_Cyberbezpieczeństwo_jako_podstawa_bezpiecznego_państwa_i_społeczeństwa_w_XXI_wieku_Marek_Górka_red._Adres_wydawniczy_Warszawa_Difin_2014_Szczegóły_s._202-221_ISBN_978-83-7930-334-2.
9. Zob. http://www.oxforddictionaries.com/definition/english/cyberwar (05-05-2015).
10. Zob. http://www.macmillandictionary.com/us/dictionary/american/cyberwar (05-05-2015).
11. Zob. M. Bieniek Cyberprzestrzeń, http://www.cxnews.pl/cyberprzestrzen,644.html (z dnia 01-01-2014).
12. J. Arquilla, D. Ronfeldt Cyberwar is Coming! Comparative Strategy, 12(2) 1993, 141-165.

formacji. Nowa teoria wojny dąży do jednej i wszechogarniającej sieci, zastępującej istniejące dotąd modele i koncepcje wojskowe. Ingeruje przy tym we wspólny system, powodując, że wojna w przyszłości stanie się zjawiskiem sieciowym z działaniami wojennymi charakteryzującymi się różnorodnością procesów sieciowych[13]. W efekcie znaczenie słowa „net war" ujęto bardzo szeroko, zaliczając do tej grupy także środki techniczne.

Wojna w ujęciu klasycznym odnosi się konfliktu międzypaństwowego, jednak w przypadku wojny sieciowej, znaczenie konfliktu nie jest już jednoznaczne, bowiem agresja może być skierowana także przeciwko organizacjom niepaństwowym. Wojna sieciowa może być prowadzona przez państwa oraz ich służby przeciwko wrogom z określonych grup społecznych lub odwrotnie, ale także przez sektor niepaństwowy przeciwko innym sektorom niepaństwowym[14].

Wątpliwości pojawiają się podczas analizy terminu „*information warfare*", ponieważ może być on tłumaczony jako „walka informacyjna", ale także jako „wojna informatyczna". Jednak wojna, jak zauważył R. Szpyra, jest kategorią, która wykorzystuje wszystkie formy walki (zbrojną, informacyjną, ekonomiczną, itp.), zaś postrzeganie takich zjawisk jak „*cyberwar*", „informacyjni wojownicy", „informacyjna dominacja", „obrona w cyberprzestrzeni", czy „chaos informacyjny" są neologizmami, dotyczącymi tego samego zjawiska, lecz w szerszym ujęciu wojny w erze informacyjnej. Współczesna walka informacyjna jest jednym z elementów walki zbrojnej, zaś dopiero postęp technologiczny przyniósł zmiany jakościowe w obrębie zjawiska wojny. Efektem tego jest wzrost różnorodności i typów zagrożeń informacyjnych oraz wzrost kompleksowości, dynamiczny wzrost intensywności działań destrukcyjnych, autonomiczność niektórych form walki informacyjnej, globalizację rynków informacyjnych, powstanie cyberprzestrzeni i nadanie jej rangi jednego z wymiarów walki[15].

Wojna informacyjna jest metodą, która jak zauważa R. Brzeski – obezwładnia przeciwnika informacją, modyfikując postrzeganie rzeczywistości przez społeczeństwa poprzez działania wywiadu z zakresu propagandy i manipulacji. Jednak proces zmian w świadomości społeczeństwa poddawanego tego typu operacjom nie jest natychmiastowy, lecz stopniowy. W znaczeniu militarnym należy uwzględnić zintegrowane wykorzystanie środków operacyjnych: dezinformacji, operacji psychologicznych, walce elektronicznej oraz niszczeniu fizycznym, którego zamierzeniem jest pozbawienie przeciwnika dopływu informacji, degradowania czy wypaczania otrzymywanych danych, a także niszczenia jego zdolności dowodzenia i kontroli. Pierwszą fazą operacji psychologicznych może być demoralizacja, zaś kolejnym – zburzenie obowiązującego od wieków porządku i systemu wartości, zaś w kolejnym etapie – pozbawienie społeczeństwa poczucia własnej godności, zakłamania osiągnięć przodków, wpajanie uczucia ogólnej niemożności, co w konsekwencji ma spowodować zaprzestanie stawiania oporu[16].

Z kolei E. Waltz kieruje definiowanie zjawiska wojny informacyjnej w stronę części technicznej, określając go działaniami podjętymi w celu zachowania integralności i ochrony własnych systemów informatycznych przed eksploracją, uszkodzeniem lub zakłóceniami, przy jednoczesnym uszkadzaniu lub niszczeniu systemów przeciwnika, co uniemożliwić ma przeciwnikowi osiągnięcie przewagi informacyjnej w zakresie stosowania siły[17].

Brak jest jednoznacznej definicji walki informacyjnej, choć w wielu próbach terminologicznych znaleźć można wspólne treści, które ułatwiają postrzeganie tego zjawiska jako konfliktu, w którym informacja staje się jednocześnie zasobem, obiektem ataku oraz bronią[18]. Walka informacyjna to także kształtowanie świadomości społecznej, zaś tego typu operacje stosowane są we wszystkich fazach działań operacji wojskowych[19]. Definicja jednak odnosi się jedynie do działań psychologicznych, nie

13. A. Dugin Wojny sieciowe, http://geopolityka.org/analizy/112-wojny-sieciowe, (08-05-2016).
14. K. Liedel, P. Piasecka Wojna cybernetyczna – wyzwanie XXI wieku, Bezpieczeństwo narodowe, 1-2007, s. 23.
15. M. Madej, M. Terlikowski Bezpieczeństwo teleinformatyczne państwa, PISM 2009, s. 80.
16. Zob. R. Brzeski Wojna informacyjna, http://ojczyzna.pl/ARTYKULY/BRZESKI-R_Wojna-Informacyjna.htm.
17. E. Waltz Information Warfare, Principles and Operations. Norwood: Artech House Boston, London 1998.
18. M. Madej, M. Terlikowski Bezpieczeństwo teleinformatyczne państwa, PISM 2009, s. 80.
19. M. Gałązka Informacja jako broń, Bellona, 4/2009, Ministerstwo Obrony Narodowej, s. 50.

obejmując powszechnych negatywnych działań (np. szpiegowskich), jako czynników powodujących napięcia pomiędzy walczącymi państwami wraz z ujawnianiem tego typu działań. Aktywność państwa w walce informacyjnej służy osiągnięciu określonych celów politycznych i może być skierowana także na niszczenie lub modyfikowanie systemów komunikowania przeciwnika lub przepływających informacji przy jednoczesnej ochronie własnych systemów[20].

Za walkę informacyjną Komitet Wojskowy NATO uważa koordynację działań podejmowanych w celu osiągnięcia pożądanych rezultatów końcowych, takich jak możliwość oddziaływania na przeciwnika, potencjalnego przeciwnika lub na inne grupy społeczne dla osiągnięcia celów prowadzonej misji. Operacje informacyjne stosuje się we wszystkich fazach działań, we wszystkich rodzajach operacji wojskowych oraz na każdym etapie wojny[21].

Pomimo różnic w definicjach walki informacyjnej, dominującą tezą jest wykorzystywanie tego zjawiska zarówno jako wyłącznego sposobu prowadzenia konfliktu, jak i traktowanie go jako jednego z elementów szerszych działań w wymiarze informacyjnym, wraz z towarzyszącymi innym działaniami w sferze fizycznej[22].

Ekspert ds. bezpieczeństwa – Martin Libicki wyszczególnia różne formy walki informacyjnej, zaliczając do nich konflikty w szerszym ujęciu, obejmujące ochronę, manipulację, walkę wywiadowczą polegająca na projektowaniu; ochronie oraz pozbawianiu systemów wyszukujących wiedzę niezbędną do dominacji na polu walki, a także walkę radioelektroniczną (techniki kryptograficzne, wojna psychologiczna, wojny „hakerskie") do atakowania systemów komputerowych. Kolejną formą walki jest ekonomiczna wojna informacyjna, polegająca na blokowaniu informacji lub wpływaniu na ich treści w celu zdobycia przewagi gospodarczej oraz wojnę cybernetyczną, obejmującą wiele futurystycznych scenariuszy.[23]

Istotną bronią informacyjną, kształtującą społeczeństwo jest medialny przekaz propagandowy, tworzony za pomocą podporządkowanych lub tradycyjnych oraz cyfrowych mediów. W konsekwencji pozwala to rządom państw na bagatelizowanie strat własnych przy jednoczesnej multiplikacji strat przeciwnika oraz kreowanie wizerunku wojny sprawiedliwej, cywilizowanej oraz precyzyjnej, która charakteryzuje się niewielkimi stratami w ludziach, co ma na celu uspokojenie opinii publicznej[24].

Idea cyberwojny

Zmiany cywilizacyjne, zmierzające ku cywilizacji informacyjnej, powodują modyfikacje w charakterystyce paradygmatu wojny, pozornie obalając clausewitzowski paradygmat zwycięstwa, które odbywa się poprzez totalne niszczenie. Wynika z tego, że współcześnie wyniszczająca wojna na wielką skalę wydaje się być ujęciem anachronicznym, w którym działania wojenne są w dużym stopniu ograniczone (choć nie przestrzennie), zaś główną strategią rozwiniętych państw staje się minimalizacja strat poprzez zastosowanie inteligentnej broni – w tym narzędzi informacyjnych.

Nadejście współczesnych cyfrowych wojen przewidzieli w 1993 roku John Arquilla i David Ronfeldt, argumentując rozwój tego zjawiska łatwością przeprowadzenia ataków i trudnością ich skutecznego odparcia. W dokumencie *Cyberwar is coming* autorzy ci zawarli ostrzeżenia o konsekwencjach rewolucji informacyjnej, przewidując wzrost znaczenia informacji. Postawili hipotezę, że społeczeństwa przyszłości będą toczyć między sobą konflikty podobnie, jak dzieje się to w przypadku wojen tradycyjnych, gdzie stronami są państwa[25].

Miejscem prowadzenia cyberwojen jest cyberprzestrzeń, określana piątym teatrem wojny. Tego

20. [w:] T. Jemioło, P. Sienkiewicz (red.) Zagrożenia dla bezpieczeństwa informacyjnego państwa Identyfikacja, analiza zagrożeń i ryzyka. Tom I. Raport z badań, Warszawa 2004, s. 74–75.

21. M. Gałązka Informacja jako broń, Bellona, 4/2009, Ministerstwo Obrony Narodowej, s. 51.

22. M. Wrzosek Zagrożenia technologiczne a bezpieczeństwo Europy, Bellona, 3/2012 (670), s. 13.

23. M. C. Libicki What is Information Warfare?, National Defense University, Center for Advanced Concepts and Technology, Washington D.C. August 1995.

24. L. Klich, C. Sochala Bezpieczeństwo informacyjne jako współczesne wyzwania współczesnego państwa – wybrane problemy, Międzynarodowa konferencja: Україна В Процесах Глобального Інформаційного Обміну, Lwów 2016, s. 97.

25. B. Bartoszek Cyberwojna – wojna XXI wieku, http://www.mojeopinie.pl/cyberwojna_wojna_xxi_wieku,3,1215862210 (stan na 09.08.2016).

typu podejście zaproponował John A. Warden w 1995 roku, określając cyberprzestrzeń jako *piąty wymiar walki zbrojnej* – obok lądu, morza, powietrza i przestrzeni kosmicznej. Cechami cyberwojny jest uzyskanie przewagi informacyjnej, niewidzialność przeciwnika, cyberprzestrzeń jako miejsce działania oraz czas – jako czynnik krytyczny[26].

Współczesne społeczeństwa informacyjne, gospodarki państw oparte na wiedzy czy też istnienie informacyjnej cyberprzestrzeni militarnej sugerują, że analogicznie towarzyszyć im powinny wyłącznie wojny informacyjne. Oznacza to, że postrzeganie współczesnych wojen nie odbywa się wyłącznie poprzez działania zbrojne i fizyczną eliminację przeciwnika. Sun Tzu głosił, że odniesienie stu zwycięstw w stu bitwach nie jest szczytem umiejętności. Szczytem umiejętności jest pokonanie przeciwnika bez walki[27]. W przypadku cyberwojen stwierdzenie to teoretycznie oddaje istotę nowoczesnego typu wojny, odnoszącego się do walki bez tradycyjnego oręża oraz braku konieczności unicestwiania życia ludzkiego (lub przynajmniej – minimalizowania strat w ludziach).

Elementy cyberwojny dostrzec można we współczesnych konfliktach zbrojnych, zaś terminologia wojskowa wzbogaciła się o nowe pojęcia określające wojnę przyszłości: wojna informacyjna, wojna cybernetyczna, wojna wirtualna, czy wojna asymetryczna[28]. Terminologia ta trafnie oddaje środowisko cyberwojny, jednak ostatnie z przytoczonych pojęć, choć czasem funkcjonuje w odniesieniu do cyberwojny, jest terminem użytym niefortunnie, bowiem wojna asymetryczna jest pojęciem szerszym od wojny z użyciem technologii informatycznych i może oznaczać także wojnę między regularną armią a rebeliantami, z użyciem środków konwencjonalnych.

Nadużywanie pojęcia „wojna informacyjna" jest powszechne, jednak, jak zauważa P. Daniluk, określenie to wymaga rozpatrywania szeregu poglądów i założeń uwzględniających wiele warunków, które powinny być spełnione[29].

Wojna jest zjawiskiem zbyt złożonym, by je można było ograniczać jedynie do sfery informacyjnej czy technicznej. Występuje zaś równolegle z działaniami informacyjnymi lub też dezinformacyjnymi. Dodatkowo, pomimo wysokiego poziomu technologicznego i globalnego osieciowienia, obecne konflikty toczą się wciąż przy użyciu środków tradycyjnych, przy współudziale środków informacyjnych, ale także coraz powszechniej – informatycznych. W opinii autora, terminów „wojna informacyjna" lub też „cyberwojna" użyć można jednak w celu posiłkowania się w przypadku chęci wydobycia środowiska walki, podobnie jak w przypadku walki lądowej, powietrznej, czy morskiej[30]. Cyberwojna charakteryzuje się asymetrią[31], stąd może stanowić perspektywę dla krajów słabiej rozwiniętych, które w przypadku konwencjonalnej wojny nie mają szans z o wiele silniejszym przeciwnikiem.

Cyberwojna, podobnie jak wojna tradycyjna, oznacza wciąż aktualne clausewitzowskie założenie, że jest ona przedłużeniem i narzędziem polityki, a jednocześnie *aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli*[32].

Działania w cyberprzestrzeni znacznie różnią się od tradycyjnych działań militarnych, stąd nie można polegać na mechanizmach bezpieczeństwa użytych do ochrony w przypadku konfliktu fizycznego. Istota cyberwojny przypomina działania zimnowojenne, w których aktorzy opracowują coraz nowsze metody ofensywne oraz obronne[33], zaś ich cechą jest to, że prowadzenie przez państwa działań informacyjnych przeciwko innym państwom

26. Zob. http://geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku

27. M. Gałązka Informacja jako broń, Bellona, 4/2009, Ministerstwo Obrony Narodowej, s. 50

28. Wojna asymetryczna jest pojęciem szerszym od wojny z użyciem technologii informatycznych. Jest to np. także wojna między regularną armią a rebeliantami z użyciem środków konwencjonalnych.

29. P. Daniluk Współczesne wymiary konfrontacji informacyjnej, Dolnośląska Szkoła Wyższa, s. 36.

30. B. Balcerowicz Czym jest współczesna wojna?, http://files.pwi.edu.pl/files/balcerowicz.doc.

31. Według słownika BBN asymetria to niesymetryczna relacja między różnorodnymi podmiotami, o różnym charakterze i różnych potencjałach w środowisku bezpieczeństwa oraz stosowanie niesymetrycznych metod w operacjach bezpieczeństwa.

32. Carl von Clausewitz O wojnie, Kraków 2005, s. 15.

33. L. Walsh Defens do not mean a lost cyberwar, http://www.channelweb.co.uk/crn-uk/opinion/2343165/defeats-do-not-mean-a-lost-cyberwar (05-05-2015).

nie musi prowadzić do otwartej wojny[34].

Początkowe sukcesy odnoszone przez wojska amerykańskie podczas trwających ostatnich wojen spowodowały wzrost znaczenia „wojny wirtualnej", jako działania elit profesjonalistów. Sukcesy te spowodowały, że nowoczesne metody prowadzenia wojen uznano za skuteczne w rozwiązywaniu współczesnych konfliktów. Jednak atak z 11 września 2001 roku przyniósł konieczność zrewidowania takiego myślenia. Obecnie wojny wirtualne należy traktować metaforycznie, gdyż okazało się, że tradycyjne metody walki jeszcze długo nie znikną[35].

Cechą charakterystyczną ostatnich konfliktów zbrojnych jest stale rosnący poziom wykorzystania dwukierunkowych środków informacyjnych, co stanowi podstawę współczesnych konfrontacji międzynarodowych, zaś skala efektów tego typu działań często porównywana jest do użycia broni masowego rażenia[36].

Współczesne wojny charakteryzują się środowiskiem działania nie tylko w cyberprzestrzeni i za pomocą wyłącznie informacji czy narzędzi informatycznych, lecz łączą w sobie działania klasyczne wraz z innym rodzajem oddziaływania na przeciwnika. Taka hybrydowość odnosi się do współistnieniem dwóch zasadniczych płaszczyzn konfliktu – terytorialnej, odnoszącej się do klasycznie rozumianego państwa i tradycyjnych wspólnot etnicznych, klanowych lub plemiennych, zamieszkujących dane terytorium oraz wirtualnej – ponad terytorialnej, transgranicznej, posiadającej sieciową strukturę umożliwiającą komunikację w obrębie sieci, w której panują globalne wartości oraz zasady[37].

Działania w cyberprzestrzeni znacznie różnią się od tradycyjnych działań militarnych, stąd nie można polegać na mechanizmach bezpieczeństwa użytych do ochrony w przypadku konfliktu fizycznego

Wnioski

Oprócz dotychczasowych tradycyjnych zagrożeń globalnych, pojawiły się nowe wyzwania dla bezpieczeństwa, związane z rewolucją technologiczną. Różnorodność i złożoność współczesnych zagrożeń w cyberprzestrzeni i poza nią, powoduje potrzebę wypracowania nowych rozwiązań w zakresie ochrony i obrony.

Ze względu na wiele istniejących równolegle definicji, odnoszących się często do tego samego zjawiska, niezbędne wydaje się ustanowienie systemowych, jednolitych, a co ważniejsze – jednoznacznie identyfikujących zjawiska terminów, które wpłyną na jednolite postrzeganie występujących niebezpieczeństw. Jest to ważne tym bardziej, że ze względu na pogorszenie się warunków światowego bezpieczeństwa, obecna sytuacja polityczna wymaga pilnego zaangażowania się państwa w tworzenie metod walki informacyjnej oraz opracowania mechanizmów odstraszania, także w kontekście cyberbezpieczeństwa na wschodniej flance NATO[38].

Obecnie świat znajduje się na etapie wyścigu cyfrowych zbrojeń i możliwe są jeszcze negocjacje, traktaty i programy rozbrojeniowe, jednak zwiększająca się liczba i natężenie konfliktów lokalnych i rozproszonych wskazuje na początek cyberwojny światowej, w której bronią jest oprogramowanie złośliwe, niszczące infrastrukturę niezbędną do funkcjonowania współczesnych państw.

34. E. Gartzke Making Sense of Cyberwar, http://belfercenter.ksg.harvard.edu/publication/23796/making_sense_of_cyberwar.html.
35. B. Balcerowicz Czym jest współczesna wojna?, http://files.pwi.edu.pl/files/balcerowicz.doc.
36. Tamże, s. 50.
37. A. Gruszczak Hybrydowość współczesnych wojen – analiza krytyczna, http://www.bbn.gov.pl/download/Hybrydowoswspolczesnychwojenanalizakrytyczna.pdf , s. 14.
38. B. Józefiak, Cyberbezpieczeństwo na szczycie NATO. Jakie priorytety Polski i Sojuszu?, http://www.cyberdefence24.pl/399633,cyberbezpieczenstwo-na-szczycie-nato-jakie-priorytety-polski-i-sojuszu (stan na 16.08.2016).

Bibliografia

1. J. Arquilla, D. Ronfeldt Cyberwar is Coming! Comparative Strategy, 12(2) 1993, 141-165.
2. B. Balcerowicz Czym jest współczesna wojna?, http://files.pwi.edu.pl/files/balcerowicz.doc.
3. B. Bartoszek Cyberwojna – wojna XXI wieku, http://www.mojeopinie.pl/cyberwojna_wojna_xxi_wieku,3,1215862210.
4. M. Bieniek Cyberprzestrzeń, http://www.cxnews.pl/cyberprzestrzen,644.html.
5. R. Brzeski Wojna informacyjna, http://ojczyzna.pl/ARTYKULY/BRZESKI-R_Wojna-Informacyjna.htm.
6. R. Ciastoń Piąty element, [w:] Polska Zbrojna, nr 18(811) listopad 2013.
7. C. Clausewitz O wojnie, Kraków 2005.
8. P. Daniluk Współczesne wymiary konfrontacji informacyjnej, Dolnośląska Szkoła Wyższa.
9. A. Dugin Wojny sieciowe, http://geopolityka.org/analizy/112-wojny-sieciowe.
10. C. François Cyberwojna czy cyberpokój?, http://wolnemedia.net/cyberwojna-czy-cyberpokoj.
11. M. Gałązka Informacja jako broń, Bellona, 4/2009, Ministerstwo Obrony Narodowej.
12. E. Gartzke Making Sense of Cyberwar, http://belfercenter.ksg.harvard.edu/publication/23796/making_sense_of_cyberwar.html.
13. M. Górka (red), NATO a aspekty bezpieczeństwa w cyberprzestrzeni [w:] Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin, Warszawa 2014.
14. B. Grenda Sieciocentryczne zarządzanie siłami powietrznymi, AON, Journal of KONBiN 3(19) 2011.
15. A. Gruszczak Hybrydowość współczesnych wojen – analiza krytyczna, Analiza krytyczna wojen hybrydowo – społecznych.
16. T. Jemioło, P. Sienkiewicz (red.) Zagrożenia dla bezpieczeństwa informacyjnego państwa Identyfikacja, analiza zagrożeń i ryzyka. Tom I. Raport z badań, Warszawa 2004.
17. B. Józefiak Cyberbezpieczeństwo na szczycie NATO. Jakie priorytety Polski i Sojuszu?, http://www.cyberdefence24.pl/399633,cyberbezpieczenstwo-na-szczycie-nato-jakie-priorytety-polski-i-sojuszu.
18. J. Kisielnicki Po drugiej strony mocy, czyli ciemne strony informatyki, Annales Universitatis Mariae Curie-Skłodowska, Vol L,2 – 2016.
19. L. Klich, C. Sochala Bezpieczeństwo informacyjne jako współczesne wyzwania współczesnego państwa – wybrane problemy, Międzynarodowa konferencja: Україна В Процесах Глобального Інформаційного Обміну, Lwów 2016.
20. M. Lakomy Cyberwojna jako rzeczywistość XXI wieku, http://geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku
21. M.C. Libicki What is Information Warfare?, National Defense University, Center for Advanced Concepts and Technology, Washington D.C. August 1995.
22. Liedel, P. Piasecka Wojna cybernetyczna – wyzwanie XXI wieku, Bezpieczeństwo Narodowe I-2011.
23. Macmilian Dictionary, http://www.macmillandictionary.com/us/dictionary/american/cyberwar.
24. M. Madej, M. Terlikowski Bezpieczeństwo teleinformatyczne państwa, PISM 2009.
25. Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/cyberwar.
26. L. Walsh Defens do not mean a lost cyberwar, http://www.channelweb.co.uk/crn-uk/opinion/2343165/defeats-do-not-mean-a-lost-cyberwar.
27. E. Waltz Information Warfare, Principles and Operations. Norwood: Artech House Boston, London 1998.
28. M. Wrzosek Zagrożenia technologiczne a bezpieczeństwo Europy, Bellona, 3/2012 (670).