AUTOR
płk dr Mirosław Banasik
rawenna2309@interia.pl
Wydział Bezpieczeństwa Narodowego, ASzWoj

POLSKIE SPOJRZENIE NA WOJNĘ HYBRYDOWĄ

Słowa kluczowe: wojna hybrydowa, zagrożenia hybrydowe, współczesne konflikty zbrojne

Wstęp

Konfrontacyjna postawa Federacji Rosyjskiej (FR) w wymiarze militarnym, stałe podnoszenie wydatków na siły zbrojne i interwencja w Syrii w połączeniu z antyzachodnią retoryką i niepewną polityką wewnętrzną budzi uzasadniony niepokój w państwach sąsiadujących, a zarazem obawy NATO co do dalszych zamiarów Kremla. Wydaje się, że największe zagrożenia ukierunkowane są na państwa bałtyckie, ze względu na historyczne uwarunkowania i znaczną ilość obywateli rosyjskojęzycznych. Przeprowadzona pomiędzy latem 2014 a wiosną 2015 roku przez Rand Corporation symulacja uderzenia FR na te byłe republiki Związku Radzieckiego uwidoczniła szereg słabości Sojuszu. Zasadnicze wnioski prowadziły do konkluzji, że NATO nie jest w stanie skutecznie obronić terytorium swoich członków przed agresją FR. Okazało się, że do zrealizowania takiego zadania konieczne jest posiadanie co najmniej siedmiu brygad ogólnowojskowych, w tym trzech brygad pancernych wspieranych ogniem artylerii i lotnictwa[1]. Rezultaty przeprowadzonej gry wojennej stanowiły dodatkowy argument do zmiany strategii NATO, rozmieszczenia wojsk i sposobu prowadzenia działań obronnych w odpowiedzi na agresję FR. Udowodniły również, że Europa nie może obronić się bez Stanów Zjednoczonych[2].

W opinii P. Goble'a, tempo przygotowywania się do globalnej konfrontacji z otaczającym Rosję zachodnim światem nie tylko nie zatrzymało się, ale nawet zwiększyło[3]. Obecnie brak jest jakichkolwiek symptomów świadczących o tym, że nastąpiły fundamentalne zmiany kursu rosyjskiej polityki.

[1] D. A. Shlapak, M. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank*. Wargaming the Defense of the Baltics, Santa Monica, 2015, s. 1 i 2, http://www.rand.org/pubs/research_reports/RR1253.html [dostęp: 11.11.2016].

[2] R. Lyman, *Eastern Europe Cautiously Welcomes Larger U.S. Military Presence*, The New York Times, 02.02.2016; http://www.nytimes.com/2016/02/03/world/europe/eastern-europe-us-military.html?_r=0 [dostęp: 11.11.2016].

[3] P. Goble*, Putin's Longstanding Plan for Long-Term Confrontation with the West Being Implemented Ever More Rapidly, Illarionov Says*, Window on Eurasia - New Series, Saturday, May 28, 2016, http://windowoneurasia2.blogspot.ca/2016/05/putins-longstanding-plan-for-long-term.html [dostęp: 01.11.2016].

Wręcz przeciwnie, potwierdzeniem jego utrzymania są próby wciągnięcia Białorusi w konfrontację z państwami Zachodu. Analitycy białoruskiego Centrum Badań Strategicznych i Politycznych twierdzą, że Białoruś, zachowując neutralną pozycję wobec kryzysu na Ukrainie oraz pełną kontrolę nad swoim terytorium, wnosi znaczący wkład w stabilność regionu. Jednak w ostatnim czasie widać *bezprecedensowe naciski wojskowe i polityczne* na Białoruś ze strony Rosji, co może świadczyć o tym, że Rosja może stworzyć na Białorusi *szarą strefę*[4], z której Federacja Rosyjska (FR) *będzie sterowała konfliktami w regionie i prowadziła konfrontację z Zachodem*[5].

W Moskwie pojawiają się coraz częściej myśli na temat realnej wojny prowadzonej z Zachodem i nie jest to tylko propaganda politycznych liderów czy mediów. Idee te mają wymiar realnych posunięć ukierunkowanych na osiąganie przewagi rosyjskich sił zbrojnych i w konsekwencji na odniesienie zwycięstwa w przyszłej, hipotetycznej konfrontacji[6]. Stosunkowo łatwo odniesione sukcesy w Gruzji w 2008 roku i na Ukrainie w 2014 roku, a także efektywna projekcja sił zbrojnych w Syrii oraz bezkolizyjne dostosowanie do tamtejszych uwarunkowań strategii wojskowej sprawia poczucie u niektórych, wysoko postawionych dowódców, że prawdopodobne jest również w przyszłości zwycięstwo z NATO.

Aktualne oceny ekspertów polityczno – wojskowych wskazują, że przekroczenie granicy NATO przez regularne siły zbrojne FR jest raczej mało prawdopodobne, tym niemniej przeciwko Polsce może być prowadzona przez Moskwę wojna hybrydowa. Celem artykułu jest dokonanie oceny zagrożeń i wykazanie potrzeby dokonania działań zabezpieczających. Jego treści są rezultatem rozwiązania następujących problemów szczegółowych:

1) W jaki sposób i w jakim celu FR wykorzystuje wojnę hybrydową?

2) Jak w Polsce rozumie się wojnę hybrydową?

3) Jak ocenia się zagrożenia dla Polski związane z prowadzeniem wojny hybrydowej?

4) W jaki sposób należy w Polsce przeciwstawiać się zagrożeniom wojny hybrydowej?

---

[4] Szerzej o szarej strefie: M. Banasik, *Unconventional war and warfare in the gray zone. The new spectrum of modern conflicts, Journal of Defense Resources Management*, Volume 7, Issue no. 1 (12), April 2016, Brasov Romania 2016, http://journal.dresmara.ro/issues/volume7_issue1/00_jodrm_vol7_issue1.pdf [dostęp: 31.10.2016].

[5] *Białoruski raport o naciskach Rosji*, Portal Interia, 21.08.2016, http://fakty.interia.pl/swiat/news-bialoruski-raport-o-naciskach-rosji,nId,2255464 [dostęp: 21.08.2016].

[6] Е Крутиков, *Военная тактика России имеет преимущества перед тактикой США и НАТО*, 13 мая 2016, http://vz.ru/politics/2016/5/13/810243.html [dostęp: 20.08.2016].

Rosyjska percepcja wojny hybrydowej

W kontekście geopolitycznym wojna hybrydowa jest nowym pojęciem. Rosyjscy stratedzy rozumieją wojnę hybrydową jako koncepcję stosowaną głównie w sferze operacji specjalnych, połączonych z działaniami sił opozycyjnych, a także wykorzystaniem doświadczeń walki z ekstremizmem państwowym i aktorami niepaństwowymi stanowiącymi zagrożenia dla bezpieczeństwa międzynarodowego[7]. Ze względu na niebezpośrednie oddziaływanie na wszystkie możliwe sfery funkcjonowania państwa i we wszystkich jej wymiarach za pomocą militarnych i niemilitarnych instrumentów oddziaływania wojna hybrydowa jest doskonałym mechanizmem destabilizacji państw sąsiadujących z FR. W ocenie amerykańskich teoretyków rosyjska wojna hybrydowa w sposób dynamiczny integruje *hard* i *soft power,* który oddziałuje na całe społeczeństwo[8], uwzględniając jego aspekty kulturowe i fizyczne. Wojna hybrydowa łączy ze sobą stan końcowy działań, zdolności, uwzględnia ryzyko i, przewidując zachowanie adwersarza, zapewnia osiąganie zamierzonych celów politycznych. Tak postrzegana konceptualizacja wojny hybrydowej może świadczyć, że jest strategią w rękach polityków i w opinii F. Hoffmana pozwala zarówno na zapobieganie niekorzystnemu postępowaniu potencjalnego przeciwnika, jak i kształtowanie własnego[9].

Na wymiar geopolityczny wojny hybrydowej wskazują В. А. Киселев i И. Н. Воробьев. Wprowadzają pojęcie operacji hybrydowej jako formy prowadzenia działań wojennych. W ich rozumieniu operacje hybrydowe prowadzi się w celu oderwania części terytorium państwa i przyłączenia do drugiego. Dokonuje się tego przy pomocy kompleksowych przedsięwzięć polityczno - dyplomatycznych, informacyjno - propagandowych, finansowo- ekonomicznych oraz o charakterze wojennym. Przy czym nie prowadzi się kampanii wojennej *sensu stricte*. Działania na terytorium strony przeciwnej mogą być wspierane operacjami specjalnymi i uzbrojonymi strukturami, wcześniej zorganizowanymi i przygotowanymi do działania na terytorium podlegającym oderwaniu, a ich zadaniem jest neutralizacja sił zbrojnych strony przeciwnej[10].

[7] А. А. Бартош, *Гибридные войны как проявление глобальной критичности современного мира, Геополитика и безопасность*, No 1 *(29*), 2015*,* s. 73, http://www.paodkb.ru/upload/iblock/38e/2015_geopolitika-i-bezopasnost-_zhurnal_.pdf [dostęp: 15.02.2016].

[8] Diego, R. Palmer, *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons*, Research Paper NATO Defense College, Rome – No. 120 – October 2015, s. 8, https://www.files.ethz.ch/isn/194718/rp_120.pdf [dostęp: 20.08.2016].

[9] O. Manea, *The Strategy of Hybrid Warfare*, Small Wars Journal, 02.02.2016; http://smallwarsjournal.com/jrnl/art/the-strategy-of-hybrid-warfare [dostęp: 10.08. 2016].

[10] В. А. Киселев, И. Н. Воробьев, *Гибридные операции как новый вид военного противоборства*, Военная мысль № 5, Москва, 2015 г., s. 1.

Dla zrozumienia istoty wojny hybrydowej ważne jest uświadomienie sobie, w jaki sposób Rosjanie w ogóle postrzegają wojnę. Rosyjskie pojmowanie wojny osadza się *na społeczno - politycznym fenomenie radykalnych zmian w charakterze relacji pomiędzy państwami i narodami i przejściem strony opozycyjnej od użycia niemilitarnych i niesiłowych form i metod rywalizacji do bezpośredniego zastosowania środków walki zbrojnej dla osiągnięcia określonych celów politycznych i ekonomicznych*[11]. Inne środki przytoczone w definicji można rozumieć jako hybrydowe, ukierunkowane na silne i słabe punkty strony przeciwnej. Wojna jest hybrydowa w takim sensie, że łączy aspekty działań powstańczych traktowanych jako element wojny nieregularnej z działaniami konwencjonalnych sił zbrojnych. Zagrożenia stale wzrastają, jednak poziom agresji utrzymuje się zawsze poniżej progu otwartego konfliktu zbrojnego. Taka sytuacja powoduje narastanie napięcia we wzajemnych relacjach międzynarodowych. Dominacja działań hybrydowych prowadzi do lokalnej eskalacji konfliktu i odsłania kolejne wrażliwości. Zagrożenie użyciem regularnych sił zbrojnych kreuje też przewagę strategiczną Federacji Rosyjskiej w takich miejscach jak Krym czy Syria, co sprawia, że w obawie przed bezpośrednią konfrontacją brak jest zdecydowanej odpowiedzi nie tylko strony przeciwnej, lecz także organizacji międzynarodowych.

Polska percepcja wojny hybrydowej

Zdefiniowanie wojny hybrydowej w Polsce wzięło na siebie Biuro Bezpieczeństwa Narodowego (BBN). W propozycji nowych terminów z dziedziny bezpieczeństwa wojna hybrydowa rozumiana jest jako *wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.*[12] Uzupełnieniem powyższej definicji pozwalającej lepiej zrozumieć zagrożenia hybrydowe jest pojęcie agresji podprogowej. W opinii prof. S. Kozieja w konfrontacji z NATO Federacja Rosyjska może posłużyć się metodą agresji poniżej progu otwartej, regularnej wojny, czyli tzw. agresji podprogowej, jako jednego z elementów wojny hybrydowej[13]. Agresja podprogowa rozumiana jest jako *działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na*

[11] Д. Рогозин, *Военно-политический словарь*, Глава 1. Государство и безопасность, мир и война, 1.47. Война; http://www.voina-i-mir.ru/article/47 [dostęp: 20.08.2016].

[12] *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*, http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINI-SLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 31.10.2016].

poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej, jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa[14]. Pracownik BBN M. Fryc uważa, że wojna jest hybrydowa ukierunkowana na osiąganie celów strategicznych. *Wykorzystuje się do tego całą gamę różnorodnych środków zarówno materialnych, jak i niematerialnych, militarnych i niemilitarnych, legalnych i nielegalnych, bezpośrednich i pośrednich. W swojej istocie przybiera więc wymiar totalny. Następnie odpowiednio je dobiera i łączy w działania tak, aby przyniosły one zamierzone efekty. Wykorzystywane są zatem wszelkie dostępne środki (polityczne, dyplomatyczne, militarne, informacyjne, gospodarcze i kulturowe), które składają się na groźbę bezpośrednią i nacisk pośredni z ograniczonymi działaniami przy użyciu siły zbrojnej*[15]. Ważnym podkreślenia jest to, że w wojnie hybrydowej duże znaczenie ma przestrzeń oddziaływania. W odróżnieniu od tradycyjnej wojny nie ogranicza się ona do wymiaru fizycznego, a jest obecna w innych wymiarach, w których do tej pory nie oddziaływały regularne siły zbrojne. W wojnie hybrydowej istotne jest wywoływanie zaplanowanych i pożądanych efektów, akcentowanych przez M. Fryca, które są ze sobą synchronizowane. W opinii amerykańskiego teoretyka A. Deepa efekty osiągane dzięki zastosowaniu asymetrycznych technik i taktyki są synchronizowane na wielowymiarowym polu walki[16]. Na efekt synergii w fizycznym i psychologicznym wymiarze konfliktu wskazuje inny amerykański naukowiec F. Hofman, który uważa, że może być on osiągany poprzez wielomodalne aktywności realizowane przez odrębne podmioty (a nawet jeden podmiot), ale generalnie są one operacyjnie i taktycznie kierowane w głównej przestrzeni prowadzonej wojny hybrydowej[17]. Biorąc pod uwagę wszystkie przytoczone argumenty, należy sądzić, że wojna hybrydowa jest kategorią strategiczną. Wojnę hybrydową należy rozumieć jako wojnę ukierunkowaną na osiąganie celów politycznych dzięki wywoływaniu zsynchronizowanych efektów kinetycznych i behawioralnych poprzez wielowymiarowe zastosowanie instrumentów oddziaływania i zdolności będących w dys-

[13] H. A. Pach, *Rozmowa z gen. Stanisławem Koziejem o wojnie i pokoju*, http://www.wiadomosci24.pl/artykul/z_gen_stanislawem_koziejem_o_wojnie_i_pokoju_332111.html [dostęp: 31.10.2016].

[14] *(Mini)Słownik….*

[15] M. Fryc, *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej”*, Bezpieczeństwo Narodowe 2015/I, Warszawa 2015, s. 65, https://www.bbn.gov.pl/ftp/dok/03/FRYC_33-2015.pdf [dostęp: 31.10.2016].

[16] A. Deep, *Hybrid War: Old Concept*, New Techniques, Small Wars Journal, March 2, 2015, s. 1, http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques [dostęp :28.10.2016].

[17] F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* Arlington, 2007, s. 8, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 30.10.2016].

pozycji strony atakującej. Z powyższej definicji wynika, że wojny hybrydowej nie należy utożsamiać tylko z zagrożeniem o nowym charakterze. Należy rozumieć, że jest raczej nowym rodzajem wojny, przez niektórych teoretyków uważanych za wojnę nowej generacji, w której oprócz starych wykorzystywane są nowe narzędzia, często niemilitarne, np. oddziaływania w cyberprzestrzeni dla osiągania efektów strategicznych.

Zagrożenia wojną hybrydową w Polsce

W opinii polskich decydentów polityczno-militarnych i ekspertów wojskowych jawne przekroczenie granicy Sojuszu przez Federację Rosyjską i agresja na dużą skalę są raczej mało prawdopodobne. Wywołanie wojny z NATO jest niewyobrażalną decyzją, ale nie można jej wykluczać. Wojna na pełną skalę, a szczególnie z użyciem broni masowego rażenia byłaby jednak pewnym samobójstwem. Rosyjska doktryna strategiczna zakłada przecież atakowanie wroga na całej głębokości jego terytorium, we wszystkich możliwych wymiarach oddziaływania. Konsekwencją takiego działania byłoby zagrożenie dla sojuszników Polski. Ocenia się, że nie tylko z uwagi na zobowiązania traktatowe, lecz także w swoim bezpośrednim interesie strategicznym państwa sojusznicze byłyby zainteresowane powstrzymaniem agresji jak najdalej od swoich terytoriów. *Racjonalna kalkulacja strategiczna podpowiadałaby im, aby wysyłać wojska do zatrzymania agresora w Polsce, pobicia go jak najszybciej, aby nie toczyć bojów u siebie i nie ponosić strat w przeciągającej się wojnie*[18]. W realiach Polski bardziej prawdopodobne jest zagrożenie wojną hybrydową z ograniczonymi działaniami kinetycznymi.

W Polsce uważa się, że największym zagrożeniem, również dla NATO, są sytuacje trudno konsensusowe. FR celowo utrzymuje poziom agresji poniżej czerwonej linii, określającej granicę wojny. Świadomie unika pogwałcenia artykułu 5, gdyż w interesie Rosji jest unikanie bezpośredniej konfrontacji z przeciwnikiem posiadającym globalną przewagę sił konwencjonalnych. W okolicznościach niesprzyjającego klimatu politycznego, przy umiejętnym doborze i stosowaniu przez potencjalnego agresora instrumentów i metod oddziaływania może uniemożliwić społeczności międzynarodowej jednoznaczne stwierdzenie, czy rzeczywiście ma już do czynienia z wojną czy agresją podprogową. Ocenia się, że w takich sytuacjach Polska musiałby reagować samodzielnie. Zagrożenia mogą się wyrażać agresją ograniczoną czasowo, przestrzennie i co do zaangażowanych sił. Ponadto może być stosowana *skryta, nieregularna, dywersyjna, asymetryczna i rajdowa działalność, z selektywnymi precyzyjnymi uderzeniami nieznanego autorstwa, aktami terrorystycznymi, w połączeniu z wykorzysta-*

[18] H. A. Pach, *Rozmowa…*, s. 50.

niem pozamilitarnych środków przemocy, do których zaliczyć można wojnę informacyjną, cyberataki, szantaż energetyczny itp., a także ewentualnych miejscowych kolaborantów[19]. Równie poważne zagrożenia związane z wojną hybrydową mogą stanowić niezidentyfikowani osobnicy, którzy pojawili się na Ukrainie, obiegowo nazywani *zielonymi ludzikami*. Jest to pojęcie *potocznie stosowane do określenie uzbrojonych żołnierzy nieposiadających dystynkcji wojskowych, ani innych wyróżników, które pozwalałyby na określenie ich narodowości, prowadzących zbrojne działania regularne i nieregularne na terytorium wschodniej Ukrainy, wymierzone przeciwko jej integralności i niezawisłości*[20].

W Polsce uważa się, że kwestii bezpieczeństwa państwa nie można sprowadzać wyłącznie do powiększania potencjału militarnego. Trzeba spojrzeć na nie z perspektywy funkcjonalności całego mechanizmu państwowego, a szczególnie tych procesów, które zabezpieczają nas przed skutkami związanymi z zagrożeniem wewnętrznym. Zagrożenia hybrydowe mogą wyrażać się działaniami ofensywnymi w cyberprzestrzeni, presją ekonomiczną, wielokierunkowymi działaniami dyplomatycznymi oraz groźbą przeprowadzenia akcji terrorystycznych i operacji dezinformacyjnych. Równie poważne zagrożenie stwarzają próby destabilizacji sytuacji politycznej i ekonomicznej, poprzez kompilację działań wymierzonych w strategiczne cele państwa, dywersję polityczną oraz działalność wrogich ośrodków propagandy[21].

W Polsce wyraźnie nasila się intensywność aktywności rosyjskich służb. Szpiegostwo jest jedną z form bardzo skutecznych właśnie w ramach wojny hybrydowej. W opinii S. Kozieja wojna hybrydowa trwa już dzisiaj w postaci pewnej presji politycznej i strategicznej. *Cały czas pod tą presją jesteśmy, tej wojny informacyjnej na przykład, tego straszenia, szantażowania lotami, przemieszczaniem rakiet, to wszystko się odbywa*[22].

Spektakularnym przykładem prowadzenia wojny hybrydowej z zastosowaniem punktowego uderzenia w interesy państwa było przeprowadzenie ataku z wykorzystaniem ośrodków antypolskiej propagandy na ministra obrony narodowej. Poprzez fałszywe i całkowicie irracjonalne oskarżenia, wykreowanie atmosfery podejrzeń i pomówień, wywołano zainteresowanie opinii publicznej. Kolejny krok polegał na wykorzystaniu publikacji do sformułowania wniosku o odwołanie ministra. A. Ścios uważa, że *korelacja poszczególnych etapów oddziaływania dowodzi, że mieliśmy do czynienia z*

[19] Tamże.

[20] *(Mini)Słownik*….

[21] A. Ścios, Bez *dekretu: przegrana wojna – (1) Diagnoza*, 06.07.2015; http://bezdekretu.blogspot.com/2016/07/przegrana-wojna-1-diagnoza.html, [dostęp: 31.10. 2016].

[22] *I kto tu straszy Polaków? Gen. Koziej: wojna przeciwko Polsce trwa, zaś rosyjskiej inwazji wykluczyć nie można*, Polityka, 19.02.2015, http://wpolityce.pl/polityka/234372-i-kto-tu-straszy-polakow-gen-koziej-wojna-przeciwko-polsce-trwa-zas-rosyjskiej-inwazji-wykluczyc-nie-mozna [dostęp: 31.10.2016].

działaniem zsynchronizowanym i całkowicie zamierzonym, którego kulminacja miała nastąpić w przededniu warszawskiego szczytu NATO. Celem tej operacji było podważenie zaufania do osoby ministra i kierownictwa MON, przekierunkowanie uwagi opinii publicznej, wywołanie chaosu i zamętu informacyjnego, osłabienie pozycji negocjacyjnej Polski podczas szczytu i tworzenie negatywnego wizerunku grupy rządzącej w oczach natowskich partnerów[23].

Raport Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT) prezentujący dane za 2014 rok nie pozostawia wątpliwości, że Polska stała się celem jednego z elementów wojny hybrydowej, jakim jest wojna informacyjna. Dostrzegalna jest wyraźna dynamika wzrostu uporczywych, długofalowych ataków bazujących na zaawansowanych narzędziach. Oznacza to, że oprócz wzrostu ilościowego obserwowany jest także istotny postęp jakościowy w prowadzonych atakach. Upraszczając, nie dość, że ataków jest więcej, to mogą one teraz być także znacznie groźniejsze. Istotnym czynnikiem pozostaje tu udział grup kierowanych i sponsorowanych przez obce państwa. Odnotowano ataki przeprowadzone na strony internetowe Prezydenta RP i giełdę papierów wartościowych, a także na niektóre witryny instytucji administracji państwowej. Do wspomnianych ataków przyznała się na swojej stronie grupa przedstawiająca się jako „Cyber Berkut", podając jako powód rzekome zaangażowanie Polski w konflikt związany z sytuacją na Ukrainie[24]. CERT podkreśla, że Internet i media społecznościowe – ze względu na dostępność i łatwość korzystania z nich – stają się także narzędziem stosowanym do wspomagania militarnych i wywiadowczych działań prowadzonych przez państwa poprzez uskutecznianie szeroko rozumianej akcji propagandowo - dezinformacyjnej. Analiza dyskusji internetowych, również w sieciach społecznościowych na przestrzeni ostatniego roku wskazała na gwałtowny i nienaturalny w stosunku do innych tematów wzrost aktywności internautów w tym zakresie, a także zjawiska tzw. *trollingu* w komentowaniu działań Federacji Rosyjskiej związanych z aneksją Krymu i konfliktem na Ukrainie. Tego typu wpisy dosłownie „zalewały" polskie portale informacyjne w początkowej fazie konfliktu[25].

Sposoby przeciwstawiania się zagrożeniom hybrydowym

Hybrydowy charakter działań zbrojnych, w tym spektrum środków zastosowanych w konflikcie rosyjsko - ukraińskim, stanowi dziś poważne wyzwanie dla władz państwowych, reaktywności systemów obronnych czy

[23] A. Ścios, *Bez dekretu*….

[24] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, CERT.GOV.PL, marzec 2015, s. 38, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html, [dostęp: 31.10.2016].

[25] *Raport*…, s. 48.

decyzyjności międzynarodowych instytucji bezpieczeństwa. Odpowiedź na takie zagrożenie z reguły musi przybrać charakter wielowymiarowy, w tym międzynarodowy. Wymaga kreatywnego myślenia i odpowiednio skoordynowanych, połączonych działań różnorodnych podmiotów, służb, a także zastosowania nietypowych narzędzi i zdolności[26]. Na zagrożenia hybrydowe w Polsce zwrócono uwagę zarówno w *Strategii Bezpieczeństwa Narodowego RP*, jak i w *Białej Księdze Bezpieczeństwa Narodowego RP*. W Strategii stwierdza się, że w niesprzyjających okolicznościach mogą wystąpić zagrożenia militarne dla bezpieczeństwa Polski, które mogą przybrać postać *konfliktów zbrojnych o różnej skali – od działań zbrojnych poniżej progu klasycznej wojny, do mniej prawdopodobnego konfliktu na dużą skalę*[27]. W Białej Księdze wyartykułowano, że w dającej się przewidzieć perspektywie istnieje duże prawdopodobieństwo wystąpienia konfliktu aterytorialnego. A zatem takiej formy zagrożenia, w ramach której przeciwnik nie dąży do opanowania zaatakowanego terytorium, lecz stosuje środki o świadomie ograniczonej skali, zasięgu i nieznanego autorstwa, które obliczone są na „rozbrojenie" prawnych mechanizmów bezpieczeństwa i w ten sposób zmuszenie zaatakowanego do prowadzenia samodzielnych działań zbrojnych w warunkach międzynarodowej izolacji w wyniku tworzenia tzw. sytuacji trudno konsensusowych[28].

W kontekście wojny hybrydowej ważne zapisy w Strategii dotyczą tworzenia strategicznej odporność kraju na agresję. Składają się na nią działania militarne i niemilitarne mające na celu zwiększanie niedostępności terytorium, powszechność przygotowań obronnych struktur pozamilitarnych, a także skuteczność wsparcia sił zbrojnych, w tym możliwość zorganizowanego oporu na terenach zajętych przez agresora[29]. Poprzez strategiczną odporność kraju rozumie się *zdolność do oporu i przetrwania agresji poprzez: a) obronne przygotowanie społeczeństwa (świadomość obronna, patriotyczna narodu, umiejętności zachowania się w obliczu agresji zbrojnej); b) zwiększanie niedostępności operacyjnej terytorium (operacyjne przygotowanie terytorium, bezpieczna infrastruktura); c) działania nieregularne i wspierające różnych struktur państwowych wzmacniające działania regularne wojsk operacyjnych*[30]. Prowadzenie oraz organizowanie działań nieregularnych na terytorium zajętym przez hybrydowego przeciwnika powinno być realizowane przede wszystkim przez Wojska Specjalne. W opinii S. Kozieja *nie ma dziś miejsca na myślenie o tym w kategoriach*

[26] M. Fryc, *Polska*…, s. 66.

[27] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2014, pkt 36, s. 20.

[28] *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013, s. 128.

[29] S. Koziej, *Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych*, „Krytyka Prawa", tom 8, nr 1/2016, s. 84.

[30] *(Mini)Słownik*….

dawnych, tradycyjnych formacjach partyzanckich. W związku z tym należy rozważyć ukierunkowanie Wojsk Specjalnych na obronę kraju, zwiększenie ich liczebności oraz organizowanie szkolenia ich na terytorium kraju z pozostałymi strukturami państwa[31]. Zapewnianie bezpieczeństwa struktur państwa, obywateli i infrastruktury krytycznej przed zagrożeniami hybrydowymi zapewniać powinny również niewojskowe formacje bezpieczeństwa. Wiązać się to będzie z koniecznością określenia zadań oraz przygotowania Policji, służb specjalnych, straży samorządowych czy agencji ochroniarskich i formacji ochrony obiektów[32]. Uogólniając, można skonstatować, że ideą tworzonego w Polsce systemu odporności kraju jest *skoordynowanie różnych działań (legislacyjnych, operacyjnych, szkoleniowych, organizacyjnych, technicznych itp.) w wielu sektorach bezpieczeństwa mające służyć zwiększeniu strategicznej odporności kraju na zagrożenia, jako jednego z ważnych wymiarów współczesnego odstraszania (powstrzymywania, odstręczania), w tym także przed próbami „miękkiej", asymetrycznej agresji*[33].

Polska liczy się z tym, że w sytuacjach prowadzenia przez FR agresji pomiędzy binarnymi granicami wojny i pokoju będzie musiała przez dłuższy czas, a w niektórych przypadkach przez cały czas reagować samodzielnie. W związku z tym uważa się, że należy przygotować się na zagrożenia hybrydowe, szczególnie te podprogowe. Podstawą do zapewnienia bezpieczeństwa zewnętrznego państwa jest odpowiedni potencjał odstraszania, który może mieć wymiar zarówno ofensywny (odwetowy), jak i defensywny (zniechęcający). W zakresie odstraszania ofensywnego należy maksymalnie korzystać z potencjału sojuszniczego (nuklearnego i konwencjonalnego) i selektywnie budować własne zdolności[34]. Wydaje się, że najlepszym środkiem powstrzymywania, hamowania i odstraszania potencjalnego przeciwnika od sięgania po taką metodę strategiczną jest rozmieszczanie wojsk innych państw NATO na terytoriach państw brzegowych[35]. Ze względu jednak na czas reagowania najbardziej korzystne byłoby na stałe rozlokowanie baz ze sprzętem i wyposażeniem. Wtedy potencjalny agresor musi wkalkulować w swoje plany, że jeśli wtargnie na terytorium kraju NATO, to wejdzie od razu w konflikt nie tylko z siłami zaatakowanego podprogowo państwa, ale także z siłami innych jego sojuszników. To powinno w istotnym stopniu mitygować jego agresywne zamiary[36]. Od-

[31] S. Koziej, *Strategiczna*…, s. 87.

[32] Tamże, s. 87.

[33] Tamże, s. 87.

[34] S. Koziej, *Dekalog priorytetów strategicznych w dziedzinie bezpieczeństwa narodowego*, Warszawa 2015, s. 4, https://www.bbn.gov.pl/ftp/dok/01/Dekalog_priorytetow_w_dziedzinie_bezpieczenstwa_RP.pdf [dostęp: 01.11.2016].

[35] H. A. Pach, *Rozmowa*….

[36] Tamże.

straszanie bronią konwencjonalną może się jednak okazać niewystarczające. Skuteczniejsze jest odstraszanie bronią jądrową, szczególnie w sytuacji braku zgody Sojuszu na stałe stacjonowanie pokaźnych sił na terytorium nowych członków. Wydaje się, że w obecnych uwarunkowaniach politycznych najlepsze efekty przyniesie odstraszanie konwencjonalne zintegrowane z odstraszaniem nuklearnym. Sygnałem do zmian w polityce nuklearnej było, uczestniczenie polskich samolotów F-16, po raz pierwszy w historii, w ćwiczeniach nuklearnych NATO w 2014 roku oraz pod koniec ubiegłego roku nieformalna propozycja zastępcy ministra obrony narodowej Tomasza Szatkowskiego o rozmieszczeniu w Polsce amerykańskiej taktycznej broni nuklearnej[37]. W reagowaniu na szantaż bronią nuklearną najlepszą strategią jest stworzenie równowagi między potencjalnymi zyskami z szantażu a skalą ryzyka, jakie się z tym wiąże[38].

W Polsce proces budowania zdolności do wiarygodnego odstraszania militarnego ujęty został pod hasłem „polskie kły". Transformacyjno-modernizacyjne wysiłki, podejmowane w ramach potencjału militarnego, prowadzą do wykształcenia wyselekcjonowanych zdolności, które – w przestrzeni lądowej, powietrznej, morskiej oraz cyberprzestrzeni – będą w stanie skutecznie zagrozić adwersarzowi i odwieść go od zamiaru czy też prób zbrojnych działań przeciwko Rzeczypospolitej. W tym wypadku istotą klasycznego wymiaru odstraszania ma być osiągnięcie przez SZ RP zdolności do precyzyjnego rażenia wybranych celów oraz przeciwdziałania szerokiemu spektrum zagrożeń asymetrycznych[39].

Oprócz budowania systemu strategicznej odporności kraju na agresję i odstraszania, wydaje się, że w przeciwdziałaniu kompleksowym w swoim charakterze zagrożeniom hybrydowym najistotniejsze jest wykorzystanie siły narodowej[40]. Dokonać tego będzie można poprzez integrację systemu bezpieczeństwa narodowego. W Polsce planuje się utworzenie Komitetu Rady Ministrów ds. Bezpieczeństwa Narodowego i wzmocnienie Rządowego Centrum Bezpieczeństwa (RCB) jako ciała sztabowego tego komitetu. Niestety Bezpieczeństwo Polski jest wciąż zarządzane resortowo. Istnieją odrębne systemy planowania i zarządzania reagowaniem obronnym oraz kryzysowym sięgające od centrali, przez resorty, województwa, aż do sa-

[37] T. Sauer, *Just Leave It: NATO's Nuclear Weapons Policy at the Warsaw Summit*, Arms Control Today, Volume 46: June 2016, s. 2, https://www.armscontrol.org/ACT/2016_06/Features/Just-Leave-It-NATOs-Nuclear-Weapons-Policy-at-the-Warsaw-Summit, [dostęp: 30.08.2016].

[38] H. A. Pach, *Rozmowa*….

[39] M. Fryc, *Polska*…, s. 69.

[40] Siła narodowa to dynamiczny zbiór czynników materialno-ekonomicznych, społecznych i kulturowych w wymiarze jednostkowym, narodowym (państwowym) i międzynarodowym, wraz z efektami substytucji i synergii zachodzącymi między nimi, tworzący podstawę sukcesu narodu (państwa) w zakresie realizacji jego celów i interesów narodowych. W. Kitler, *Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji*, „Zeszyty Problemowe TWO" 2010, nr 1 (61), s. 118.

morządów. Niestety brakuje zintegrowanego oraz kompleksowego podejścia do rozwiązywania problemów bezpieczeństwa. Celowe jest również merytoryczne integrowanie głównych dokumentów strategicznych w państwie dotyczących bezpieczeństwa. Integrowanie systemu kierowania bezpieczeństwem narodowym wymaga też uporządkowania przepisów prawnych, co można osiągnąć poprzez przygotowanie ustawy dotyczącej kierowania bezpieczeństwem narodowym[41].

Biorąc pod uwagę największe wrażliwości Polski na zagrożenia hybrydowe, wyrażające się presją polityczno - militarną realizowaną głównie w sferze informacyjnej, także w cyberprzestrzeni, to wydaje się, że kolejnym priorytetem powinno być budowanie skutecznego systemu bezpieczeństwa informacyjnego z dobrze zorganizowanym sektorem cyberbezpieczeństwa[42]. Celem strategicznym w obszarze bezpieczeństwa informacyjnego jest zapewnienie bezpiecznego funkcjonowania RP w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych (zwłaszcza administracji publicznej, służb bezpieczeństwa i porządku publicznego, służb specjalnych i sił zbrojnych), sektora prywatnego i społeczeństwa obywatelskiego[43]. Należy stworzyć i rozwinąć jednostki bezpieczeństwa informacyjnego (w tym cyberbezpieczeństwa) w obronnych i ochronnych (militarnych i pozamilitarnych) ogniwach systemu bezpieczeństwa narodowego. Powinny to być struktury zdolne do realizacji zadań zarówno o charakterze defensywnym, jak i ofensywnym[44]. Z kolei strategicznym celem w obszarze cyberbezpieczeństwa RP, sformułowanym w Strategii Bezpieczeństwa Narodowego RP, jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia[45]. Szczególnie istotne jest także zapewnienie suwerennego panowania operacyjnego oraz technicznego nad wysoce zinformatyzowanymi systemami walki i wsparcia, w tym systemami kierowania (dysponowanie kodami źródłowymi ich oprogramowania). Ważnym zadaniem jest ponadresortowa koordynacja tej problematyki w ramach budowania zintegrowanego systemu

[41] S. Koziej, *Dekalog*…, s. 3.

[42] Tamże, s. 4.

[43] Projekt *Doktryny bezpieczeństwa informacyjnego RP*, Warszawa 2015, s. 5; https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 01.11.2016].

[44] S. Koziej, *Dekalog*…, s. 5.

[45] *Doktryna cyberbezpieczeństwa RP*, Warszawa 2015, s. 9, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 01.11.2016].

kierowania bezpieczeństwem narodowym[46]. Przy założeniu, że jednym z najtrudniejszych aspektów zarządzania w sytuacjach kryzysowych wynikających z zagrożeń hybrydowych jest aspekt komunikacji i wypracowania wspólnej świadomości sytuacyjnej, cyberprzestrzeń i infosfera stają się najbardziej prominentnymi polami prowadzenia walki i pierwszą linią starcia. W opinii K. Liedla *poprawna detekcja aktywności przeciwnika i system wczesnego ostrzegania prawidłowo funkcjonujący w tych właśnie dwóch obszarach będą stanowić o zdolnościach do prowadzenia działań prewencyjnych w innych wymiarach dotyczących bezpieczeństwa państwa i jego obywateli*[47].

Zakończenie

W sytuacji kompleksowego oddziaływania państwa rosyjskiego przeciwko Zachodowi, który Putin traktuje jako zagrożenie, na pierwszy plan wysuwa się potrzeba posiadania strategii przeciwstawiania się zagrożeniom hybrydowym. Rozwiązaniem modelowym mogłoby być osiągnięcie porozumienia NATO z Unią Europejską (UE) i przygotowanie wspólnej, zintegrowanej strategii. Na jej podstawach celowe byłoby opracowanie strategii narodowej.

Ważna jest świadomość, że ani NATO, ani UE nie zagwarantuje nam absolutnego bezpieczeństwa i nie rozwiąże wszystkich problemów, jakie pojawiają się z zagrożeniami hybrydowymi. Organizacje międzynarodowe mogą jedynie pomóc w budowaniu odporności na nie, stosownie do priorytetów określonych przez Biuro Bezpieczeństwa Narodowego w 2015 roku. Zagrożenia hybrydowe są na tyle poważne, że należałoby zastanowić się nad fundamentalnymi zmianami strategii bezpieczeństwa narodowego i strukturami obronnymi. Dużym wyzwaniem dla planistów będzie zidentyfikowanie zdolności, jakie powinno posiadać państwo, a nie tylko jego siły zbrojne. Wynika z tego, że należy zmienić cały proces planowania obronnego tak, aby dotyczył on również obszarów niemilitarnych. Nie wiadomo też czy budżet obronny stanowiący 2% PKB w praktyce okaże się wystarczający. Na pewno należy dokonać zmian w planach obronnych NATO i Polski tak, aby uwzględniać realne zagrożenia przypisane do ukształtowania geograficznego oraz pododdziały sojusznicze przebywające w ramach odstraszania. Na pierwszy plan wysuwa się potrzeba stworzenia mechanizmów prawnych i proceduralnych szybkiego użycia sił zbrojnych, a

[46] S. Koziej, *Dekalog…,* s. 5.

[47] K. Liedel, *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?*, Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – WYDANIE SPECJALNE, Warszawa 2015*,* s. 56, http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html [dostęp: 23.11.2016].

także zsynchronizowania ich z innymi instrumentami niemilitarnymi. Tylko zcentralizowane kierowanie na szczeblu państwa zapewni integrowanie wszystkich instrumentów i skoordynowane przeciwdziałanie zagrożeniom hybrydowym.

Proponuje się, aby w systemie bezpieczeństwa państwa w celu efektywnego wykorzystania potencjału i uzyskania efektu synergii dążyć do integrowania w ramach jednej instytucji zarządzania bezpieczeństwem wszystkich podmiotów, cywilnych i wojskowych, administracji i mediów, sił zbrojnych i służb mundurowych, dyplomacji, polityki, organizacji pozarządowych, humanitarnych, informacyjnych etc. Celowe jest rozwijanie na szczeblu państwa zdolności do rozpoznania i oceny zagrożeń we współdziałaniu z NATO oraz pozyskiwania zdolności do odpowiedzi na zagrożenia hybrydowe, w tym także poprzez zintegrowane odstraszanie konwencjonalno-jądrowe. Na szczeblu resortu obrony narodowej zasadna jest zmiana dotychczasowych uregulowań prawnych w celu umożliwienia wykorzystania całego potencjału sił zbrojnych w czasie pokoju. Konieczne jest nadanie priorytetu rozwijaniu zdolności bezpilotowych systemów rozpoznania oraz komunikacji niejawnej do działań defensywnych i ofensywnych, w obszarze cyberprzestrzeni, komunikacji strategicznej. Celowe jest rozwijanie współpracy z organizacjami paramilitarnymi i innymi podmiotami cywilnymi działającym w obszarze obronności w celu wykorzystania ich potencjału i zdolności do przeciwdziałania zagrożeniom hybrydowym[48].

Bibliografia

1. Banasik Mirosław, *Siły zbrojne we współczesnych uwarunkowaniach środowiska bezpieczeństwa*, [w:] Kopczewski Marian, Sienkiewicz Dariusz (red.), *Edukacja warunkiem bezpieczeństwa w XXI w. – instytucje publiczne w systemie bezpieczeństwa*, Koszalin 2016.

2. Banasik Mirosław, *Unconventional war and warfare in the gray zone. The new spectrum of modern conflicts*, Journal of Defense Resources Management, Volume 7, Issue no. 1 (12), April 2016, Brasov Romania 2016, http://journal.-dresmara.ro/issues/volume7_issue1/00_jodrm_vol7_issue1.pdf.

3. Banasik Mirosław, *Wyzwania dla bezpieczeństwa wynikające z koncepcji prowadzenia wojny nowej generacji przez Federację Rosyjską*, [w:] Szmidka Tadeusz, Kozioł Jerzy (red.), *Zarządzanie Bezpieczeństwem Państwa – Wyzwania i Ryzyka*, Piotrków Trybunalski 2016.

4. Бартош Александр Александрович, *Гибридные войны как проявление глобальной критичности современного мира,* Геополитика и безопасность,

[48] M. Banasik, *Siły zbrojne we współczesnych uwarunkowaniach środowiska bezpieczeństwa*, [w:] M. Kopczewski, D. Sienkiewicz (red.), *Edukacja warunkiem bezpieczeństwa w XXI w. – instytucje publiczne w systemie bezpieczeństwa*, Koszalin 2016, s. 25.

No 1 (29), 2015; http://www.paodkb.ru/upload/iblock/38e/2015_geopolitika-i-bezopasnost-_zhurnal_.pdf.

5. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013.

6. *Białoruski raport o naciskach Rosji*, Portal Interia, 21.08.2016; http://fakty-.interia.pl/swiat/news-bialoruski-raport-o-naciskach-rosji,nId,2255464.

7. Deep Alex, *Hybrid War: Old Concept, New Techniques*, Small Wars Journal, March 2, 2015, http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques.

8. *Doktryny bezpieczeństwa informacyjnego RP*, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

9. *Doktryna cyberbezpieczeństwa RP*, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf.

10. Fryc Mariusz, *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, Bezpieczeństwo Narodowe 2015/I, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/03/FRYC_33-2015.pdf.

11. Goble Paul, *Putin's Longstanding Plan for Long-Term Confrontation with the West Being Implemented Ever More Rapidly, Illarionov Says*, Window on Eurasia – *New Series*, Saturday, May 28, 2016, http://windowoneurasia2.blogspot.ca/2016/05/putins-longstanding-plan-for-long-term.html.

12. Hoffman Frank*, Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, 2007, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

13. *I kto tu straszy Polaków? Gen. Koziej: wojna przeciwko Polsce trwa, zaś rosyjskiej inwazji wykluczyć nie można*, Portal Polityka, 19.02.2015, http://wpolityce.pl/polityka/234372-i-kto-tu-straszy-polakow-gen-koziej-wojna-przeciwko-polsce-trwa-zas-rosyjskiej-inwazji-wykluczyc-nie-mozna.

14. Kitler Waldemar, *Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji*, Zeszyty Problemowe TWO, 20, nr 1 (61), 2010.

15. Koziej Stanisław, *Dekalog priorytetów strategicznych w dziedzinie bezpieczeństwa narodowego*, Warszawa 2015, https://www.bbn.gov.pl/ftp/dok/01/Dekalog_priorytetow_w_dziedzinie_bezpieczenstwa_RP.pdf.

16. Koziej Stanisław, *Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych*, „Krytyka Prawa", tom 8, nr 1/2016.

17. Киселев Валерий Александрович, Воробьев Иван Николаевич, *Гибридные операции как новый вид военного противоборства*, Военная мысль № 5, Москва, 2015.

18. Крутиков Евгений, *Военная тактика России имеет преимущества перед тактикой США и НАТО*, 13 мая 2016, http://vz.ru/politics/2016/5/13/810243.html.

19. Liedel Krzysztof, *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?*, Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – WYDANIE SPECJALNE, Warszawa 2015, http://www.abw.gov.pl/ pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html.

20. Manea Octavian, *The Strategy of Hybrid Warfare*, Small Wars Journal, 02.02.2016. http://smallwarsjournal.com/jrnl/art/the-strategy-of-hybrid-warfare.

21. Pacha Henryk, *Rozmowa z gen. Stanisławem Koziejem o wojnie i pokoju*, http://www.wiadomosci24.pl/artykul/z_gen_stanislawem_koziejem_o_wojnie_i_pokoju_332111.html.

22. Palmer Diego Ruiz, *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons*, Research Paper NATO Defense College, Rome – No. 120 – October 2015; https://www.files.ethz.ch/isn/194718/rp_120.pdf.

23. Рогозин Дмитрий, *Военно-политический словарь*, Глава 1. Государство и безопасность, мир и война, 1.47. Война, http://www.voina-i-mir.ru/article/47.

24. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, CERT.GOV.PL, marzec 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku-.html.

25. Sauer Tom, *Just Leave It: NATO's Nuclear Weapons Policy at the Warsaw Summit*, Arms Control Today, Volume 46: June 2016.

26. *Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*, http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.

27. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2014.

28. Ścios Aleksander, *Bez dekretu: przegrana wojna – (1) Diagnoza*, portal internetowy, 06.07.2015, http://bezdekretu.blogspot.com/2016/07/przegrana-wojna-1-diagnoza.html.

POLISH VIEW ON HYBRID WARFARE

Hybrid warfare, which has been conducted since 2014 in Ukraine, has become a new geopolitical phenomenon which threatens Euro-Atlantic security that appeared after the collapse of the bipolar world. The paper discusses how the Russian Federation takes advantage of hybrid warfare to achieve its political objectives and to further its own interests. The paper also contains an assessment of the threat of hybrid warfare in Poland and determines what undertakings are necessary to effectively counter threats coming from Russia.