Dariusz PAŹDZIUR
Dowództwo Wojsk Obrony Terytorialnej

DZIAŁANIA HYBRYDOWE FEDERACJI ROSYJSKIEJ A ZAGROŻENIA DLA BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ NA MORZU BAŁTYCKIM

STRESZCZENIE

Niniejsza praca została opracowana przy zastosowaniu krytycznej analizy literatury, z wykorzystaniem analizy dostępnych informacji z zakresu rosyjskich działań hybrydowych oraz syntezy obszaru problemowego który obejmuje wyjaśnienie definicji bezpieczeństwa, działań hybrydowych oraz infrastruktury krytycznej, opis zagrożeń dla bezpieczeństwa infrastruktury krytycznej na Morzu Bałtyckim, model działań hybrydowych 8P, katalog oraz potencjalnych działań hybrydowych FR oraz fazy działań hybrydowych FR. W artykule podkreślono wzrastające znaczenie zagadnień związanych z różnymi aspektami zagrożeń jak terroryzm morski, zorganizowana przestępczość, czy podwodne działania dywersyjne FR. Podsumowanie opracowania stanowią wnioski, że działania hybrydowe zalicza się do działań poniżej progu wojny zgodnie z prawem międzynarodowym, że punktem zwrotnym jeśli chodzi o znaczące wzmocnienie gospodarki FR oraz związanej z tym aktywności militarnej tego państwa może być wydobycie ropy naftowej i gazu z rosyjskiej części szelfu kontynentalnego w Arktyce.

Słowa kluczowe:
bezpieczeństwo, model działań hybrydowych, infrastruktura krytyczna.

WSTĘP

Wydarzenia, które miały miejsce na początku XXI wieku, w tym atak zorganizowany przez organizację terrorystyczną Al-Kaidę na World Trade Centre z 11 września 2001 r. oraz działania Federacji Rosyjskiej (FR) na Krymie i wschodniej Ukrainie przyniosły zmiany w podejściu do zagadnień bezpieczeństwa globalnego, które w istotny sposób determinują również stan bezpieczeństwa zarówno Europy jak i Polski, z infrastrukturą krytyczną włącznie. Zasadnym wydaje się zdefiniowanie pojęć użytych na potrzeby niniejszego artykułu jak *bezpieczeństwo*, *działania hybrydowe oraz infrastruktura krytyczna*. Etymologia słowa *bezpieczeństwo* wywodzi się od łacińskiego *sine cura*, które oznaczało polityczną stabilność.[1] Bezpieczeństwo to stan i proces jednocześnie. Bezpieczeństwo to „stan, proces chwilowego spokoju i porządku którego dynamika stanowi funkcję mniej lub bardziej zdeterminowanego zbioru zagrożeń i bieżącego czynnika czasowego(…) stan i poczucie pewności, wolności od zagrożeń, strachu czy jakiegoś ataku, a także spokoju i stabilnego kształtowania przyjętej strategii rozwoju".[2]

Nieco inną definicję *bezpieczeństwa* proponuje Waldemar Kitler, według którego bezpieczeństwo w znaczeniu ogólnym jest „wewnętrzną ufnością, spokojem ducha i pewnością, właściwie lub fałszywie uzasadnioną w okolicznościach rodzących podstawy do obaw. Jest też przekonaniem (...), że w obliczu różnorodnych trudności, słabości, wyzwań i zagrożeń, lub przynajmniej ich symptomów, stan rzeczy w jakim się znajduje określony podmiot pozwala się czuć bezpiecznie, tzn. wolnym i zabezpieczonym przed potencjalnymi lub realnymi zagrożeniami, pewnym niezakłóconego bytu i rozwoju, z pomocą wszelkich dostępnych środków, a także działającym twórczo na rzecz osiągania takiego stanu."[3]Z powyższych definicji wynika, że bezpieczeństwo bywa utożsamiane z subiektywnym poczuciem braku zagrożenia lub choćby poczuciem uzyskania akceptowanego poziomu ryzyka zarówno w kontekście zagwarantowania podstawowych potrzeb człowieka, jak i grup społecznych czy państw. Oznacza to również potrzebę szerszego podejścia do pojmowania bezpieczeństwa i oparcia go nie tylko na zdolnościach wojskowych i wysiłkach politycznych, ale również uwzględnienia w jego ramach takich składników jak pomoc gospodarcza, technologiczna, edukacyjna czy kształtowanie świadomości społecznej w zakresie szeroko rozumianego bezpieczeństwa. Tak rozumiane bezpieczeństwo jest procesem ciągłym podlegającym permanentnym zmianom, ewolucji.[4]

[1] Wojtaszczyk K. Bezpieczeństwo państwa- konceptualizacja pojęć. Oficyna wydawnicza ASPRA-JR, Warszawa 2009, s.11.

[2] Ficoń K, Bezpieczeństwo jako systemowa kategoria ontologiczna. Kwartalnik Bellona 2013, nr 1, s.11

[3] Kitler W. Bezpieczeństwo Narodowe RP. Podstawowe kategorie, uwarunkowania, system. AON Warszawa 2011, s.22

[4] Ficoń K, Bezpieczeństwo jako systemowa kategoria ontologiczna. Kwartalnik Bellona 2013, nr 1, s.10

Przechodząc do zdefiniowania pojęć: działania hybrydowe należy stwierdzić, że nie ma jednolitej definicji tychże. Warto więc wyjaśnić etymologię pojęcia *hybryda.* Hybryda jest to osobnik powstały ze skrzyżowania dwóch genetycznie różnych osobników należących do różnych odmian, ras, gatunków."[5] Natomiast etymologia terminu *hybrydowy* oznacza „będący wynikiem połączenia co najmniej dwóch różnych elementów, gatunków, pojęć itp."[6] Jak zatem należy rozumieć pojęcie działań hybrydowych? Wydaje się być uzasadnionym przytoczenie definicji tzw. konfliktu nowej generacji[7] zaproponowanej przez Szefa Sztabu Generalnego FR gen. Walerego Gierasimowa. Opisując konflikt nowej generacji mówi on, że "metody konfliktu zmieniły się i obejmują obecnie szerokie zastosowanie środków militarnych, politycznych, gospodarczych, informacyjnych a nawet z zakresu działań humanitarnych."[8]

Działania hybrydowe na potrzeby niniejszego opracowania zostały zdefiniowane jako kombinacja działań polityczno-dyplomatycznych, propagandowych, ekonomicznych, o charakterze sabotażowym oraz wywrotowym, przy zastosowaniu metody faktów dokonanych w długiej perspektywie czasu, o pulsacyjnym natężeniu, przy wykorzystaniu poparcia mniejszości narodowych, grup niezadowolenia społecznego mających na celu podważanie autorytetu władz państwowych innego państwa i docelowo zajęcie jego części lub całego terytorium np. działania Rosji we wschodniej Ukrainie.[9] Powyższa definicja bezpośrednio związana jest z modelem działań hybrydowych 8P, który zostanie przedstawiony w dalszej części opracowania.

Definiując pojęcie infrastruktury krytycznej na potrzeby niniejszego opracowania przyjęto definicję infrastruktury krytycznej**,** która obejmuje „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"[10].

Infrastruktura krytyczna obejmuje następujące systemy:

1. Zaopatrzenia w energię, surowce energetyczne i paliwa.
2. Łączności.
3. Sieci teleinformatycznych.
4. Finansowe.
5. Zaopatrzenia w wodę.

---

5 Wielki słownik języka polskiego, s. 184.

6 Tamże

7 tak określany jest przez stronę rosyjską to co w NATO i UE nazywamy konfliktem hybrydowym. Termin zostanie wyjaśniony w dalszej części opracowania.

8 Szefa Sztabu Generalnego FR gen. Gierasimow W. podczas wykładów Akademii Sztabu Generalnego w Moskwie w 2013 r.

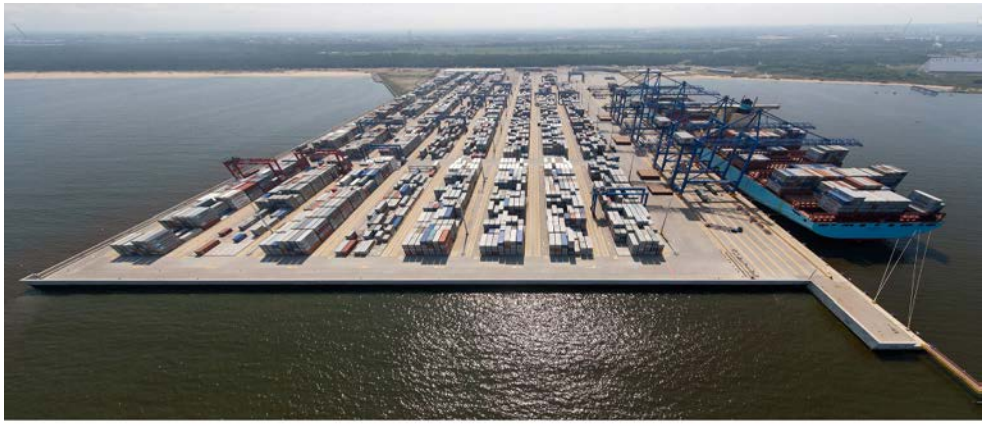
9 Opracowanie własne dr. Tyślewicz R. Model działań hybrydowych 8P AMW w Gdyni.

10 Ustawa z dn.26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.nr 89, poz.590 z późn.zm.s.1.

6. Zaopatrzenia w żywność.
7. Ochrony zdrowia.
8. Transportowe.
9. Ratownicze.
10. Zapewniające ciągłość działania administracji publicznej.
11. Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[11].

Ze względu na fakt, że w literaturze nauk o bezpieczeństwie nie występuje definicja morskiej infrastruktury krytycznej, na potrzeby tego artykułu przyjęto tą, opartą na przytoczonej powyżej definicji infrastruktury krytycznej, która obejmuje wszystkie wyszczególnione systemy, które zlokalizowane są na morzu. Przyjęto, że morską infrastrukturę krytyczną stanowią:

1. Porty morskie.
2. Jednostki pływające (tankowce, promy pasażerskie, okręty).
3. Morskie terminale przeładunkowe.
4. Platformy wiertnicze ropy naftowej i gazu ziemnego.
5. Rurociągi.
6. Kable podwodne.
7. Obiekty służące do nawigacji[12].



Rys. 1. Morski terminal przeładunkowy w Gdańsku

[11] Tamże, s.5. oraz Ustawa z dn.26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.nr 89, poz.590 z późn.zm.s.2.

[12] Polska ustanowiła wyłączną strefę ekonomiczną (ang. External Economic Zone) na podstawie ustawy z 21 marca 1991 r. o obszarach morskich RP i administracji morskiej (tekst jedn. Dz. U. z 2013 r. Nr 0, poz. 934). Wyłączna strefa ekonomiczna Polski obejmuje obszar ok. 22,5 tys. km^2.

Rys. 2. Platforma wiertnicza ropy naftowej i gazu ziemnego na Bałtyku

Zagrożenie dla bezpieczeństwa infrastruktury krytycznej w rejonie południowej części Morza Bałtyckiego

Intensywność procesu globalizacji w stosunkach międzynarodowych umożliwia z jednej strony współpracę państw i regionów leżących w znacznej od siebie odległości oraz sprawia, że system międzynarodowy jest bardziej współzależny i zintegrowany. Z drugiej strony globalizacja powoduje, że polityka międzynarodowa staje się wypadkową skomplikowanych powiązań politycznych, gospodarczych i finansowych. Środowisko bezpieczeństwa charakteryzuje się współwystępowaniem i wzajemnym przenikaniem się zagrożeń militarnych i pozamilitarnych. Cały czas pozostaje aktualnym groźba konfliktów o charakterze regionalnym i lokalnym. Konflikt na Ukrainie potwierdził aktualność tradycyjnych zagrożeń militarnych i znaczenie siły zbrojnej, także w bliskim otoczeniu Polski. Istotnym zagrożeniem dla bezpieczeństwa nie tylko dla polskiej infrastruktury krytycznej, ale również dla bezpieczeństwa międzynarodowego pozostają programy rozwoju technologii nuklearnych oraz rakietowych realizowane w sprzeczności z rezolucjami Rady Bezpieczeństwa ONZ. Powstałe w ich wyniku naruszenie regionalnej równowagi wojskowej może stanowić istotne zagrożenie dla bezpieczeństwa obiektów infrastruktury krytycznej na Bałtyku . Dalekosiężne konsekwencje może mieć też wstrzymywanie się niektórych państw np. Rosji od realizacji porozumień międzynarodowych w dziedzinie nieproliferacji broni masowego rażenia np. rozmieszczenie wyrzutni rakiet typu Iskander-M w Obwodzie Kaliningradzkim o zasięgu około 500 km czy korwet rakietowych typu BUJAN- M z pociskami Kalibr-NK o zasięgu nawet do 2500 km. To oznacza, że w ich zasięgu są m.in. Polska, Litwa, Łotwa i Estonia, a Morze Bałtyckie może stać się terenem kluczowym do prowadzenia tego typu działań przez Federację Rosyjską.

Rys. 3. Skuter podwodny Seabob Black Shadow 730[13]

Pojazdy podwodne Seabob Black Shadow 730 mają zasięg do 60 km i możliwość transportu do trzech żołnierzy oraz kilkanaście kilogramów materiałów wybuchowych i może być wykorzystywany do podwodnych działań dywersyjnych np. przeciwko portom, terminalom kontenerowym czy platformom wiertniczym ropy naftowej i gazu ziemnego. Zasięg pojazdu pozwala na użycie żołnierzy SpecNaz[14] spoza granicy polskiego morza terytorialnego dlatego sprzedaż rosyjskim płetwonurkom bojowym nowoczesnych skuterów podwodnych Sea Bob Black Shadow 730 to dowód kompletnego lekceważenia zagrożenia, jakie może nadejść ze strony morskiego SpecNazu FR.[15]

Rys. 4. Rosyjski dron startujący ze zdalnie sterowanej łodzi[16]

[13] http://www.peztco.com/fileup/upload/blackshadow_eng.pdf: dostęp 22.11.2017 r.

[14] Określenie SpecNaz (z j. ros. specjalnowo naznacienja) oznacza szeroko rozumiane siły specjalne FR.

[15] Polskie morze terytorialne sięga na 12 mil morskich(ok.22 kilometów) od tzw. linii podstawowej czyli najniższego poziomu wód np. przy odpływie.

[16] http://www. mil.ru_ Podwodny Specnaz Rosji rośnie w siłę. Dezinformacja ukrywa realne zagrożenie; Dostęp 22.11.2017 r.

Rosjanie testują drony o zasięgu do kilkudziesięciu kilometrów startującymi ze zdalnie sterowanych łodzi motorowych, ponadto SpecNaz posiada na swoim na swoim wyposażeniu szybkie łodzie motorowe co stanowić może zagrożenie dla infrastruktury krytycznej w polskiej części Wyłącznej Strefy Ekonomicznej.[17]Ze względu na specyfikę państw z dostępem do Morza Bałtyckiego, występujące na ich wodach terytorialnych oraz w Wyłącznej Strefie Ekonomicznej (z ang. EEZ) zagrożenia są nieco zróżnicowane, posiadając przy tym zasięg regionalny. Jest to akwen dostępny dla różnego rodzaju niezgodnych z prawem działań, które mogą sprzyjać wywołaniu różnorodnych zagrożeń zarówno dla infrastruktury morskiej jak i ludności. Na potrzeby tego opracowania przyjęto podział zagrożeń, które mogą potencjalnie wystąpić na Morzu Bałtyckim zaproponowany przez prof. Szubrychta T. oraz Rokicińskiego K., należą do nich[18]:

1. Terroryzm morski:

a) atak na instalacje morskie do których zaliczamy: opanowanie obiektu przez terrorystów z rozmieszczeniem ładunków wybuchowych, staranowanie obiektu przez jednostkę pływającą, samobójczy atak z użyciem statku powietrznego, użycie płetwonurków do zaminowania obiektu;

b) terroryzm państwowy/ międzynarodowy.

2. Proliferacja broni masowego rażenia.
3. Piractwo morskie.
4. Zorganizowana przestępczość:

a) zbrojne napady na statki/obiekty na morzu przez zorganizowane grupy przestępcze np. grupy abordażowe, grupy prowadzące negocjacje celem pozyskania okupu za uprowadzoną załogę;

b) przemyt nielegalnych towarów np.broni i narkotyków;

c) przemyt ludzi.

5. Nielegalna emigracja.
6. Zagrożenia ekologiczne/ celowe zanieczyszczenie środowiska naturalnego.
7. Oszustwa ubezpieczeniowe,
8. Pospolite przestępstwa kryminalne (kradzieże, wymuszenia, rabunki, morderstwa).
9. Naruszenie zasad bezpieczeństwa żeglugi (zamierzone i niezamierzone np. błąd człowieka).
10. Stosowanie lub groźba użycia sił zbrojnych:

a) własnego państwa i państw koalicyjnych/ sprzymierzonych,

[17] http://www.defence24.pl/494351,rosyjski-specnaz-podwodny-rosnie-w-sile-dezinformacja-ukrywa-realne-zagrozenie-foto; dostęp 22.11.2017 r.

[18] Szubrycht T. Bezpieczeństwo morskie państwa. Zarys problemu, Szubrycht T. Bałtyckie wymiary bezpieczeństwa. AMW.Gdynia 2010 s.167-207 oraz prof. Szubrycht T. , Rokiciński K. Gospodarka morska w świetle wybranych zagrożeń współczesnego świata. AMW. Gdynia 2006 s.43 i 62. por. Makowski A. Terroryzm morski. AMW. Gdynia 2008 r.

b) przez stronę przeciwną celem wykonywania działań sabotażowo-dywersyjnych, wywrotowych, kampanii informacyjnych, przejęcia obiektów na morzu, działań asymetrycznych i hybrydowych, itp.[19]
11. Łamanie postanowień prawa międzynarodowego z zakresu swobody żeglugi.
12. Zagrożenia generowane przez siły natury np. sztormy, szkwały:
a) eko-terroryzm- członkowie organizacji ekologicznych np. „Green Peace"[20] przykuwający się do obiektów zlokalizowanych na morzu celem organizacji protestu;
13. Inne np. błędy gospodarcze, błędy ludzkie, błędy dotyczące planowania przestrzennego, zapewnienia bezpieczeństwa państwa, błędne decyzje, ekonomiczne, społeczne, itp.

Zagrożenia te mogą wynikać zarówno z oddziaływania sił przyrody jak i działalności zorganizowanych grup przestępczych, w tym terrorystycznych.

Podobny podział zagrożeń dla infrastruktury na morzu bałtyckim proponuje Mickiewicz P., który dzieli je na zagrożenia związane z:

1. Zapleczem logistycznym dla działalności międzynarodowych organizacji przestępczych.
2. Handlem ludźmi.
3. Handlem bronią.
4. Nielegalną imigracją.
5. Próbami zawładnięcia jednostek pływających (promy, wieże wiertnicze).
6. Atakami samobójczymi np. przy pomocy szybkich łodzi motorowych.
7. Doprowadzeniem do kolizji jednostek pływających (kontenerowce, zbiornikowce).
8. Atakami przy użyciu min morskich, czy podwodnej dywersji np. przy użyciu pojazdów podwodnych typu sea bob black shadow 730.
9. Fizyczne oddziaływanie na jednostki pływające (taranowanie, przerywanie rurociągów i kabli podwodnych)[21].

Na czele listy zagrożeń pozamilitarnych znajdują się zagrożenia związane z bezpieczeństwem gospodarczym, a zwłaszcza energetycznym. Rosnące zapotrzebowanie na surowce energetyczne sprawia, że używane są one do wywierania nacisku politycznego i coraz częściej zastępują siłę militarną w realizacji celów polityki państwa. Napięcia wywołane czasowymi ograniczeniami w dostawach gazu do niektórych krajów wskazują na słabość rynku energetycznego i negatywny wpływ polityki na gospodarkę. Do tych celów

[19] Przypis autora
[20] Przypis autora
[21] Mickiewicz P. Przeciwdziałanie zagrożeniu terrorystycznemu i konsekwencji ataku terrorystycznego na polskich akwenach morskich. wyd. Dolnośląska szkoła wyższa we Wrocławiu, s. 135

może zostać w przyszłości użyty przez FR rurociąg Nord Stream I i II zlokalizowane na Bałtyku, które posiadają docelową przepustowość 55 milionów metrów sześciennych każdy, (Gazprom wykorzystuje przepustowość około 30- 35 milionów metrów sześciennych w zakresie dostaw paliw płynnych do Niemiec. Obecnie istotną rolę nie tylko w rozwoju gospodarczym FR odgrywa Gazprom, który również jest wykorzystywany przez administrację Kremla jako instrument do uzależnienia gospodarczego niektórych państw UE np. Polski. Poniżej zilustrowano wielkość sprzedaży gazu (w mln. metrów sześć.) do państw UE w latach 2013 i 2014. Największą sprzedaż tego surowca odnotowano do takich krajów jak Niemcy, Włochy, Wielka Brytania czy Francja.

Podsumowując działania FR w stosunku nie tylko do Ukrainy lecz również Polski można zaryzykować tezę, że kluczowym dla prowadzenia wszelkiego rodzaju działań hybrydowych, włączając w to działania typowo militarne może być możliwość rozbudowy przez FR przemysłu wydobywczego głównie ropy naftowej i gazu ziemnego w Arktyce, co może dać jej możliwość wzrostu PKB[22], co z kolei FR może przeznaczyć na zakup uzbrojenia oraz kontynuację konfliktów zarówno w stosunku do krajów - byłych republik radzieckich, jak i innych krajów przy zastosowaniu różnych metod i technik nazywanych działaniami hybrydowymi celem odbudowy imperium rosyjskiego. O bezpieczeństwie infrastruktury zlokalizowanej w południowej części Morza Bałtyckiego decydują więc procesy i zjawiska zachodzące przede wszystkim w jej otoczeniu. Stabilność Europy Środkowej i Wschodniej, ale też całego obszaru euroatlantyckiego i jego sąsiedztwa rzutuje na bezpieczeństwo Polski. Nie bowiem wykluczyć wystąpienia w pobliżu granic RP konfliktu o charakterze lokalnym, związanym choćby z konfliktem Ukraińskim, czy działaniami hybrydowymi podejmowanymi na coraz większą skalę przez FR przeciwko państwom bałtyckim. Stąd też Polska powinna utrzymywać zdolności zarówno militarne jak i pozamilitarne pozwalające na reagowanie na takie zagrożenia. Zagrożenia bezpieczeństwa infrastruktury na Morzu Bałtyckim RP pozostają w ścisłym związku z zagrożeniami globalnymi. Katalog zagrożeń rzutujący na bezpieczeństwo Polski jest w zasadzie tożsamy z zagrożeniami, jakie w otaczającym świecie widzą jej sojusznicy. Różnice dotyczą jedynie odmiennego określenia priorytetów, co ma związek z położeniem geopolitycznym naszego kraju. Priorytetem powinno pozostać przeciwdziałanie zagrożeniom bezpieczeństwa energetycznego oraz potencjalnemu osłabieniu więzów łączących wspólnotę europejską i transatlantycką realizowanym głównie przez FR.

Model Działań Hybrydowych 8P

Propaganda- wykorzystywanie przez FR do celów propagandowych skutecznych społecznie haseł celem usprawiedliwienia swoich działań na Krymie i we wschodniej Ukrainie np. ochrona obywateli rosyjskich

[22] PKB- Produkt Krajowy Brutto

Provocation- prowokowanie incydentów militarnych.
Progressive act- dynamiczny charakter podejmowanych działań.
Perspective-długoterminowość i nieprzypadkowa sekwencyjność działań, zbieżnych w czasie i przestrzeni.
Pulsate-pulsacyjny charakter, zmienne natężenie działań.
Pressure- presja medialna, militarna, ekonomiczno-polityczna, społeczna, religijna, itp.
Permition- wykorzystanie „stanu przyzwolenia" NATO tzn. praktycznego braku reakcji NATO na aneksję Krymu wykorzystana przez FR jako uzasadnienie do dokonania przedmiotowej aneksji oraz wsparcia „separatystów" czego skutkiem było postawienie społeczności międzynarodowej przed faktami dokonanymi od których nie ma odstępstwa przy jednoczesnym wytworzeniu wrażenia, że zarówno Ukraina jak i społeczność międzynarodowa nie ma możliwości zmiany zaistniałej sytuacji.
Proxy forces - wykorzystanie mniejszości rosyjskojęzycznej, grup niezadowolenia społecznego jako tzw. „ zielonych ludzików" na Krymie, czy „ separatystów" we wschodniej Ukrainie.[23]
Aby lepiej zrozumieć istotę powyższego modelu należy zadać pytanie; jaki jest potencjalny katalog działań podejmowanych przez FR oraz na czym polegają współczesne działania działania hybrydowe FR?

Na potrzeby niniejszego opracowania przyjęto, że ów katalog działań nazywanych *działaniami hybrydowymi* oddziałuje na wszystkie możliwe dziedziny czy też domeny życia społeczno - politycznego, militarnego, ekonomicznego, przekazu informacji, czy też na infrastrukturę państwa przeciwko któremu działania hybrydowe są prowadzone.[24] Na potrzeby tego artykułu istotnym wydaje się przedstawienie katalogu działań hybrydowych w domenach: militarnej, ekonomicznej oraz w obszarze działań przeciwko infrastrukturze krytycznej i w obszarze działań informacyjnych. Nie jest to zamknięta lista działań hybrydowych FR, szczególnie istotnych z punktu widzenia bezpieczeństwa obiektów infrastruktury krytycznej zlokalizowanej ma Morzu Bałtyckim oraz na polskim morzu terytorialnym w zdefiniowanych obszarach, m.in. z powodu wielkości, położenia geopolitycznego Polski oraz nieprzewidywalności działań FR. Ponadto, należy zauważyć, że działania FR przedstawione poniżej są ze sobą powiązane, zsynchronizowane i zbieżne w czasie i przestrzeni.

[23] P Model działań hybrydowych. Opracowanie własne dr Tyślewicz Radosław – AMW w Gdyni. Model został początkowo opracowany w j. angielskim, dlatego wyrazy tworzące ten akronim są w tym języku.

[24] w NATO przyjęto model analizy PMESII (analiza zagrożeń/działań potencjalnego przeciwnika w domenach; politycznej, militarnej, ekonomicznej, społecznej, informacyjnej, infrastrukturalnej)

Katalog potencjalnych działań hybrydowych FR

M - w obszarze działań militarnych :

- niestosowanie się do zasad zawartych w Kodeksie Postępowania Państw dotyczących polityczno-militarnych aspektów bezpieczeństwa;
- obecność obcych wojsk bez zgody władz państwa przyjmującego;
- stosowanie niedozwolonych i nieakceptowalnych form walki zbrojnej poprzez stosowanie demonstracji siły, działań dywersyjnych, prowokacji militarnej, napaść zbrojna grup nieformalnych tzw. separatystów inicjowanie incydentów granicznych z Ukrainą, państwami bałtyckimi;
- stosowanie aktów terroru;
- brak współpracy z Ukrainą w sytuacjach kryzysowych
- położenie nacisku na politykę zastraszana np. użyciem rakiet operacyjno –taktycznych Iskander- M o zasięgu około 500 km .

E - w obszarze działań ekonomicznych:

- ograniczanie dostępu innych państw do rynku wewnętrznego i zasobów naturalnych Ukrainy;
- korumpowanie władz banków państwowych, firm energetycznych celem uzależnienia ich od FR;
- zakłócenie systemu finansowego państwa (np. manipulacja kursem waluty, zakłócenie swobodnego przepływu środków pieniężnych);
- wywieranie presji gospodarczych w celu realizacji celów politycznych np. ograniczanie przesyłu energii elektrycznej, ropy naftowej i gazu ziemnego;
- obecność w gospodarce ukraińskiej rosyjskich grup przestępczych;
- wywieranie nacisku gospodarczego poprzez organizowanie blokad gospodarczych na dostawy produktów spożywczych, artykułów pierwszej potrzeby.

I - w obszarze działań przeciwko infrastrukturze krytycznej[25]:

- zakłócenie systemu transportowego i zaopatrzenia (wprowadzenie ograniczeń w wymianie handlowej z Polską - w wyniku których istnieje możliwość zakłócenia produkcji w przedsiębiorstwach/fabrykach,w konsekwencji zmniejszenie produkcji określonych artykułów lub świadczenia usług;
- wspieranie działań o charakterze lobbingowym na rzecz rodzimych firm funkcjonujących na terenie Polski. Inspirowanie do działań zgodnych
- z interesami swoich państw (np. częściowe wstrzymanie dostaw ropy naftowej i gazu do Polski);

[25] Infrastruktura krytyczna – systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Źródło Dz.U. 2007, nr 89 poz. 590 z późn. zm.

– działania przeciwko bezpieczeństwu teleinformatycznemu poprzez włamanie się do sieci. Paraliż systemów telekomunikacyjnych, brak łączności i usług transmisji danych, paraliż systemów bankowych, brak dostępu do bankowości elektronicznej;
– działania o charakterze terrorystycznym np. niszczenie obiektów administracji państwowej, zakładów produkcyjnych, systemów zaopatrywania w wodę, energię elektryczną i paliwa płynne we wschodniej Ukrainie;
– zakłócanie działania sieci informacyjnych poprzez inicjowanie ataków w cyberprzestrzeni.

I - w obszarze działań informacyjnych[26]**:**

– wykonywanie anty ukraińskich działań informacyjnych;
– ograniczenie wolności mediów;
– manipulowanie informacją;
– zakłócanie działania sieci informacyjnych;
– prowadzenie kampanii propagandowych i operacji psychologicznych z wykorzystaniem usług oferowanych przez media społecznościowe i sieci telefonii komórkowej;
– działania skierowane przeciwko infrastrukturze krytycznej państwa w tym: przełamanie zabezpieczeń;
– nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji lub nieuprawniona zmiana informacji mające na celu pogłębianie zjawiska patologii informacji;[27]
– cyberterroryzm, cyberprzestępczość.

Oprócz zdefiniowania katalogu działań hybrydowych FR istotnym i wręcz nieodzownym wydaje się być identyfikacja faz tychże działań.

[26] Bezpieczeństwo informacyjne (w tym cyber bezpieczeństwo) – obszar bezpieczeństwa, którego treść (cele, warunki, sposoby, treści) odnoszą się do środowiska informacyjnego, w tym cyberprzestrzeni. Biała Księga Bezpieczeństwa Narodowego RP. BBN, Warszawa 2013 r.
Lewandowska Anita. Patologia informacji- jeden z elementów wojny hybrydowej. Wyd. Uniwersytet Gdański „AntePortas- Studia nad Bezpieczeństwem nr 1(6) 2016 r.
por. Darczewska Jolanta. Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska- studium przypadku. Ośrodek studiów wschodnich nr 42, Warszawa maj 2014 r.

Fazy działań hybrydowych

Wiele krajów dostrzega zmiany w kontekście nowych wyzwań i zagrożeń, przede wszystkim w wykorzystaniu metod i skali ich występowania. Widoczne jest to na przykład w opracowaniu Gierasimowa W.[28] który przedstawił swój model w postaci schematu składającego się z sześciu etapów narastania konfliktu oraz diagramu obrazującego połączenie działań militarnych i niemilitarnych. Wyróżnia on następujące fazy:

- działania utajnione;
- zaostrzenie;
- rozpoczęcie działań sygnalizujących konflikt;
- kryzys;
- rozstrzygnięcie;
- przywrócenie pokoju.

Dla porównania w opracowaniu łotewskiej Narodowej Akademii Obrony wymieniono osiem faz tzw. wojny nowej generacji, które zawierają poniższe działania:

- niemilitarne, wpływające negatywnie na społeczność, ekonomię i działania polityczne;
- ukierunkowane na wprowadzenie w błąd ośrodków dyplomatycznych, politycznych oraz medialnych;
- mające na celu zastraszenie ludności i wskazanie bezcelowości dalszego oporu;
- destabilizacyjne i propagandowe;
- wprowadzające strefy zakazu lotów;
- oznaczające rozpoczęcie działań militarnych poprzez intensyfikację rozpoznania
i użycie sił specjalnych;
- wielopłaszczyznowe, w tym informacyjne, dyplomatyczne oraz militarne jako wywarcie presji z użyciem paramilitarnych i regularnych sił zbrojnych;
- mające na celu zniszczenie sił przeciwnika przez siły specjalne i precyzyjne uderzenia oraz wojska lądowe.[29]

Konflikty w ramach których można zaobserwować oznaki implementacji działań hybrydowych zazwyczaj toczą się na pograniczu kilku państw np. FR i państwa bałtyckie(Litwa, Łotwa i Estonia), co jest trudne do kontroli, skutecznego przeciwdziałania zagrożeniom hybrydowym przez poszczególne państwa w stosunku do których działania hybrydowe są prowadzone. Przeciwdziałanie działaniom hybrydowym wymaga koordynacji wysiłków polityczno-dyplomatycznych, militarnych, informacyjnych itp. na arenie między-

[28] Gierasimow W.- Szef Sztabu Federacji Rosyjskiej.

[29] Berzins J., Rassia's New Generation Warfare in Ukraine: Implikations for Latvian. Defense Policy. National Defence Academy of Latvia. Policy Paper nr 2. Riga 2014 r.

narodowej oraz pomiędzy zaangażowanymi państwami lub siłami militarnymi zarówno graniczącymi ze sobą jak i oddalonymi od siebie koalicjantami, co czyni ten konflikt bardziej skomplikowanym, znacznie trudniejszym do uniknięcia lub zażegnania na drodze rozmów pokojowych. Trudniejszym również niż w przypadku „konwencjonalnego" konfliktu jest osiągnięcie konsensusu politycznego i militarnego.

WNIOSKI

Dokonując podsumowania działań o charakterze hybrydowym Federacji Rosyjskiej nie tylko w Ukrainie, lecz również w innych rejonach np. w stosunku do państw bałtyckich (Litwa, Łotwa i Estonia) można zaryzykować wyszczególnienie poniższych wniosków:

– działania hybrydowe zalicza się do działań poniżej progu wojny zgodnie z prawem międzynarodowym;
– działania hybrydowe są z reguły prowadzone przeciwko państwom podatnym na korupcję, z nieefektywnymi mechanizmami zarządzania państwem, gdzie istnieje słabo prosperująca gospodarka, skorumpowana administracja i wojsko, niska stopa życiowa ludności a co za tym idzie kryzys polityczny, co w rezultacie ma doprowadzić do upadłości tak „zainfekowanego" państwa;
– wpływanie przez FR na administrację rządową wybranego państwa, na jej decyzje polityczne, gospodarcze, korumpowanie władz, administracji;
– użycie tzw. proxy forces jak np. „zielone ludziki", (z j. ros. dosłownie oznacza przyjaźni ludzie) użyci na Krymie tzn. żołnierzy bez przynależności państwowej oraz oznaczeń stopni i jednostek wojskowych, co jest obowiązującym w przypadku konfliktu zbrojnego zgodnego z prawem międzynarodowym. Jest to prawdopodobne do zastosowania przez FR w państwach bałtyckich, mało prawdopodobne do zastosowania w Polsce;
– łatwiejszym niż w przypadku konwencjonalnego konfliktu jest uwolnienie się od FR od odpowiedzialności politycznej i militarnej poprzez przekierowanie odpowiedzialności w wyniku działań propagandowych za działania destabilizacyjne na inne państwo np. Ukrainę lub separatystów. FR w stosunkowo prosty sposób może zaprzeczać wszelakim działaniom poprzez umiejętne prowadzenie działań o charakterze dezinformacyjnym, co określane jest mianem patologii informacji tzn. takim celowym zniekształceniu informacji niekorzystnych dla agresora, aby finalnie informacja była korzystna z jego punktu widzenia. Rosja oficjalnie zaprzecza udziałowi w konflikcie we wschodniej Ukrainie, co nieco w zmodyfikowanej formie FR może zastosować przeciwko Polsce.
– obecnie FR wykorzystuje tzw. nacjonalizm historyczny związany z działalnością band UPA we wschodniej Małopolsce w czasie i po II wojnie światowej, wykorzystywanie haseł typu „ukraińscy banderowcy" do skłócenia narodów polskiego i ukraińskiego;

– stosowanie narracji przez FR używanej w Unii Europejskiej do opisywania sytuacji we wschodniej Ukrainie np. zapewnienie praw i wolności obywatelskich dla obywateli rosyjskich, „demokratyczne" republiki Ługańska i Doniecka;
– wykorzystywanie mniejszości narodowych, grup niezadowolenia społecznego, partii opozycyjnych państwa przeciwko któremu są prowadzone działania hybrydowe celem destabilizacji sytuacji. Jest to prawdopodobne do zastosowania przez FR w Polsce;
– Rosjanie posiadają zdolności operacyjne do użycia dronów o zasięgu do kilkudziesięciu kilometrów startującymi ze zdalnie sterowanych łodzi motorowych, ponadto SpecNaz posiada na swoim na swoim wyposarzeniu szybkie łodzie motorowe co stanowić może zagrożenie dla infrastruktury krytycznej w polskiej części Wyłącznej Strefy Ekonomicznej;
– użycie pojazdu Sea Bob Black Shadow 730 pozwala na jego użycie przez żołnierzy SpecNaz spoza granicy polskiego morza terytorialnego przeciwko infrastrukturze krytycznej;
– budowa przez FR rurociągów Nord Stream w bezpośrednim sąsiedztwie polskiej części Wyłącznej Strefy Ekonomicznej daje jej możliwość dozorowania praktycznie całego Morza Bałtyckiego, co stanowi poważne zagrożenie dla bezpieczeństwa Polski;
– rozmieszczenie wyrzutni rakiet typu Iskander-M w Obwodzie Kaliningradzkim czy korwet rakietowych typu BUJAN-M z pociskami Kalibr-NK oznacza, że stanowią one zagrożenie dla Polski czy państw bałtyckich, ale również dla NATO i UE;
– punktem zwrotnym jeśli chodzi o znaczące wzmocnienie gospodarki FR może być wydobycie ropy naftowej i gazu z rosyjskiej części szelfu kontynentalnego w Arktyce. Niezbędnym do tego jest utrzymanie całorocznej drożności tranzytu morskiego z Chinami co mają zapewnić nowo budowane w Chinach dla FR lodołamacze nowej generacji, które mają kruszyć grubą do kilku nawet metrów taflę lodu wślizgując się na nią (nie jak dotychczas krusząc lód kadłubem) przy odpowiednim wyprofilowaniu kadłuba.

Katalog zidentyfikowanych metod i technik zastosowanych w konfliktach hybrydowych we wschodniej Ukrainie nie będzie prawdopodobnie możliwy do zastosowania dokładnie w takiej samej formie przeciwko Polsce, chociażby ze względu na brak w naszym kraju mniejszości rosyjskojęzycznej. Jednakże należy przypuszczać, że ów katalog pozostaje ograniczony jedynie przez wyobraźnię i pomysłowość FR i będzie prawdopodobnie kombinacją działań o charakterze militarnym, pozamilitarnym a nawet z zastosowaniem pomocy humanitarnej jako pretekstu do dostarczania wsparcia logistycznego i militarnego np. dla prorosyjskich separatystów we wschodniej Ukrainie, na co wskazuje cytowana w niniejszym opracowaniu wypowiedź rosyjskiego gen. Gierasimowa.

BIBLIOGRAFIA

[1] Berzins J. Rassia's New Generation Warfare in Ukraine: Implikations for Latvian.

[2] Biała Księga Bezpieczeństwa Narodowego RP. BBN, Warszawa 2013 r.

[3] Darczewska J. Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska-studium przypadku. Ośrodek studiów wschodnich nr 42, Warszawa maj 2014 r.

[4] Ficoń K. Bezpieczeństwo jako systemowa kategoria ontologiczna. Kwartalnik Bellona 2013, nr 1.

[5] Gierasimow W. Szef Sztabu Generalnego FR podczas wykładów w Akademii Sztabu Generalnego. Moskwa 2013 r.

[6] Kitler W. Bezpieczeństwo Narodowe RP. Podstawowe kategorie, uwarunkowania, system. AON Warszawa 2011.

[7] Kustra W. red. Obronność państwa na obszarach morskich. wyd. Stowarzyszenie Ruch Wspólnot Obronnych, Warszawa 2015 r. s.33-35.

[8] Lewandowska A. Patologia informacji- jeden z elementów wojny hybrydowej. wyd. Uniwersytet Gdański „Ante Portas- Studia nad Bezpieczeństwem nr 1(6) 2016 r.

[9] Makowski A. Terroryzm morski. AMW. Gdynia 2008 r.

[10] Mickiewicz P. Przeciwdziałanie zagrożeniu terrorystycznemu i konsekwencji ataku terrorystycznego na polskich akwenach morskich. wyd. Dolnośląska szkoła wyższa we Wrocławiu.

[11] Narodowy program ochrony infrastruktury krytycznej. Warszawa 2013 r.

[12] Racz A. Russia's Hybrid War in Ukraine. Fiński Instytut Stosunków Międzynarodowych Raport 43 z 2015.

[13] Szubrycht T. Bezpieczeństwo morskie państwa. Zarys problemu. AMW. Gdynia 2006 r.

[14] Szubrycht T. Rokiciński K. Gospodarka morska w świetle wybranych zagrożeń współczesnego świata. AMW. Gdynia 2006 r.

[15] Szubrycht T. Bałtyckie wymiary bezpieczeństwa. AMW. Gdynia 2010 s.167-207.

[16] Ustawa z dn.26.04.2007 r. o zarządzaniu kryzysowym (Dz.U.nr 89, poz.590 z późn.zm.s.1.

[17] Wojtaszczyk K. Bezpieczeństwo państwa- konceptualizacja pojęć. wyd. Oficyna wydawnicza ASPRA-JR, Warszawa 2009.

[18] Wielki słownik języka polskiego.

[19] http://pl.blastingnews.com/europa/2015/09/kim-jest-uchodzca-a-kim-imigrant-00552235.html dostęp 20.03.2016 r.

[20] http://www.defence24.pl/494351,rosyjski-specnaz-podwodny-rosnie-w-sile-dezinformacja-ukrywa-realne-zagrozenie-foto; dostęp 22.11.2017 r.

[21] http://www.peztco.com/fileup/upload/blackshadow_eng.pdf: 22.11.2017 r.

[22] http://www. mil.ru_ Podwodny Specnaz Rosji rośnie w siłę. Dezinformacja ukrywa realne zagrożenie; dostęp 22.11.2017 r.

[23] http://wiadomosci.gazeta.pl/wiadomosci/1,114871,17932395,Iskandery_przy_granicy_z_Polską:dostęp 05.03.2015 r.

RUSSIAN FEDERATION ACIVITIES AND THREATS FOR SEURITY OF THE CTITIAL INFRASTRUCTURE AT BALTIC SEA.

ABSTRACT

The critical literature analysis was use in this article as a research methodology to complete the following scientific problems:
- Description definitions of security, critical infrastructure and maritime critical infrastructure;
- Identification of the critical infrastructure threats at south part of Baltic Sea, 8P hybrid model and catalogue of potential hybrid Russian activities and RF fazes of hybrid activities.
As a result of an analysis was underlined increasing significance of issue associated with different aspect of Russian threats starting from maritime terrorism, organized crime and RF's underwater demolition activities.

Kkey words:

safety, hybrid activities, hybrid model, critical infrastructure.